ECSS–E–00A
19 April 1996

Space Engineering

Policy and Principles

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

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

Price: 35 Dutch Guilders

Printed in the Netherlands

Foreword

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

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

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

This standard has been prepared by the ECSS Engineering Standards Working Group, reviewed by the ECSS Technical Panel and approved by the ECSS Steering Board.

(This page is intentionally left blank)

Contents List

Foreword **3**

Introduction **7**

1 Scope **9**

2 Normative References **11**

3 Definitions and Abbreviations **13**

3.1 Definitions 13
3.2 Abbreviations 14

4 Space Project Engineering **15**

5 The Engineering Domain **19**

5.1 Introduction to the Engineering Domain 19
5.2 The System Engineering Process 23
5.3 Engineering Disciplines 24
5.4 Levels of Decomposition 25
5.5 Development 28

6 Overview of the System Engineering Process 29

6.1 System Engineering Integration and Control 29
6.2 Requirements Engineering 30
6.3 Analysis 31
6.4 Design and Configuration Engineering 31
6.5 Verification Engineering 32

7 Other Activities within the Engineering Domain 35

7.1 Production Engineering 35
7.2 Operations Engineering 36

8 Overview of ECSS Engineering Standards 39

9 Domain of Application of ECSS–E Standards 43

9.1 Space Product Classification 43
9.2 Space Project Criticality Classes 43

10 Use of ECSS–E Standards to Define Project Requirements .. 45

Figures

Figure 1: Illustration of the Scope of a Typical Space System 17
Figure 2: Representation of the Engineering Domain 21
Figure 3: Example Variation with Time of the Intensity of Possible Activities within the Engineering Domain related to Formal Project Phases 22
Figure 4: Simplified Representation of the System Engineering Process 24
Figure 5: Levels of Decomposition 27
Figure 6: Architecture of the ECSS Engineering Standards 41

Tables

Table 1: Scope of Level 3 Engineering Standard Sets 42
Table 2: Space Product Types 44

Introduction

The production of complex products requires the co–operation of several organisations which share a common goal : to provide a product which satisfies the consumer's needs (technical performance) under cost, schedule constraints.

To reach this goal, corresponding technical activities, human and financial resources, shall be organised and co–ordinated in a structured manner in order to obtain the end product a.k.a. system. This structure, together with related processes, constitutes a project. It implies a target (system), a time frame, and actions to be performed under resources constraints.

Project management consists of the definition, implementation and execution of such actions including the verification that corresponding obtained results match with the expected ones.

Project management requires thinking carefully about what shall be accomplished, laying out all the steps needed to build that future, and obtaining the resources required to carry out those steps. But most important, it requires dealing with reality, problems, delays, changes, obstacles and, sometimes, opportunities that arise as a project takes place.

(This page is intentionally left blank)

1

Scope

This standard, which is informative in nature, contains the basic rules and overall principles to be applied to all engineering activities during performance of a space project. It addresses the establishment, based on customer needs, of mission objectives, requirements, and specifications for space systems, and the design, definition, production, verification, operation, and eventual disposal of the systems themselves. It defines the scope and interfaces of these activities relative to the domains of management and product assurance which are addressed in the Management (– M) and Product Assurance (– Q) branches of the ECSS system, and explains how they may apply in different ways depending on the type of space system concerned. It also introduces the lower level engineering standards within the ECSS system, and proposes how they may be used (after “tailoring” if required) to facilitate space project operations.

This standard is intended to help customers in formulating their needs and suppliers in preparing their response and implementing the work.

(This page is intentionally left blank)

2

Normative References

This ECSS Standard incorporates by dated or undated reference, provisions from other publications. These normative references are cited at the appropriate places in the text, and publications are listed hereafter. For dated references, subsequent amendments to or revisions of any of these apply to this ECSS Standard only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies.

This 'Policy and Principles' standard ECSS–E–00 calls up the standards in the Space Project Management series. The standards listed below shall be considered in association with this document.

ECSS–M–00	Space Project Management – Policy and Principles.
ECSS–M–10	Space Project Management – Project Breakdown Structures.
ECSS–M–30	Space Project Management – Project Phasing and Planning.
ECSS–M–70	Space Project Management – Integrated Logistic Support.
ECSS–P–001	Glossary of Terms.
ECSS–Q–20	Space Product Assurance – Quality Assurance.
ECSS–Q–30	Space Product Assurance – Dependability.
ECSS–Q–40	Space Product Assurance – Safety.

(This page is intentionally left blank)

3

Definitions and Abbreviations

3.1 Definitions

For the purposes of this standard, the definitions given in ECSS–P–001 Issue 1 apply. In particular, it should be noted that the following terms have a specific definition for use in ECSS standards.

Analysis

Assembly

Contract

Demonstration

Development

Development Model

Disposal

Element

Equipment

Hazard

Inspection

Item

Mission

Model Philosophy

Part

Production

Project

Prototype

Purchaser

Risk

Set

Space Project

Space System

Software Module

Subsystem

Supplier

Support System

Supported System

System

Tailoring

Test

Validation

Verification

3.2 Abbreviations

The following abbreviations are defined and used within this standard.

Abbreviation	Meaning
DJF:	Design Justification File
ECLS:	Environmental Control and Life Support
ECSS:	European Cooperation for Space Standardization
RE:	Requirements Engineering

4

Space Project Engineering

The purpose of a space project is to deliver to a customer (and subsequently support or operate if required) a system which includes one or more elements intended for operation in outer space. The activities carried out by the system supplier are conveniently and conventionally categorised into five domains:

- project management, responsible for achievement of the totality of the project objectives, and specifically for organisation of the project, and its timely and cost–effective execution.
- engineering, responsible for definition of the system, verification that the customer's technical requirements are achieved, and compliance with the applicable project constraints.
- production, responsible for manufacture, assembly and integration of the system, in accordance with the design defined by engineering
- operations, responsible for exercising and supporting the system in order to achieve the customer's objectives during the operational phases (note; operations may be carried out by the customer, by the supplier or a third party on the customer's behalf, or by a combination of these)
- product assurance, responsible for the implementation of the quality assurance element of the project and also for certain other specialist activities.

The boundaries between these activities are not always clearly defined; for example:

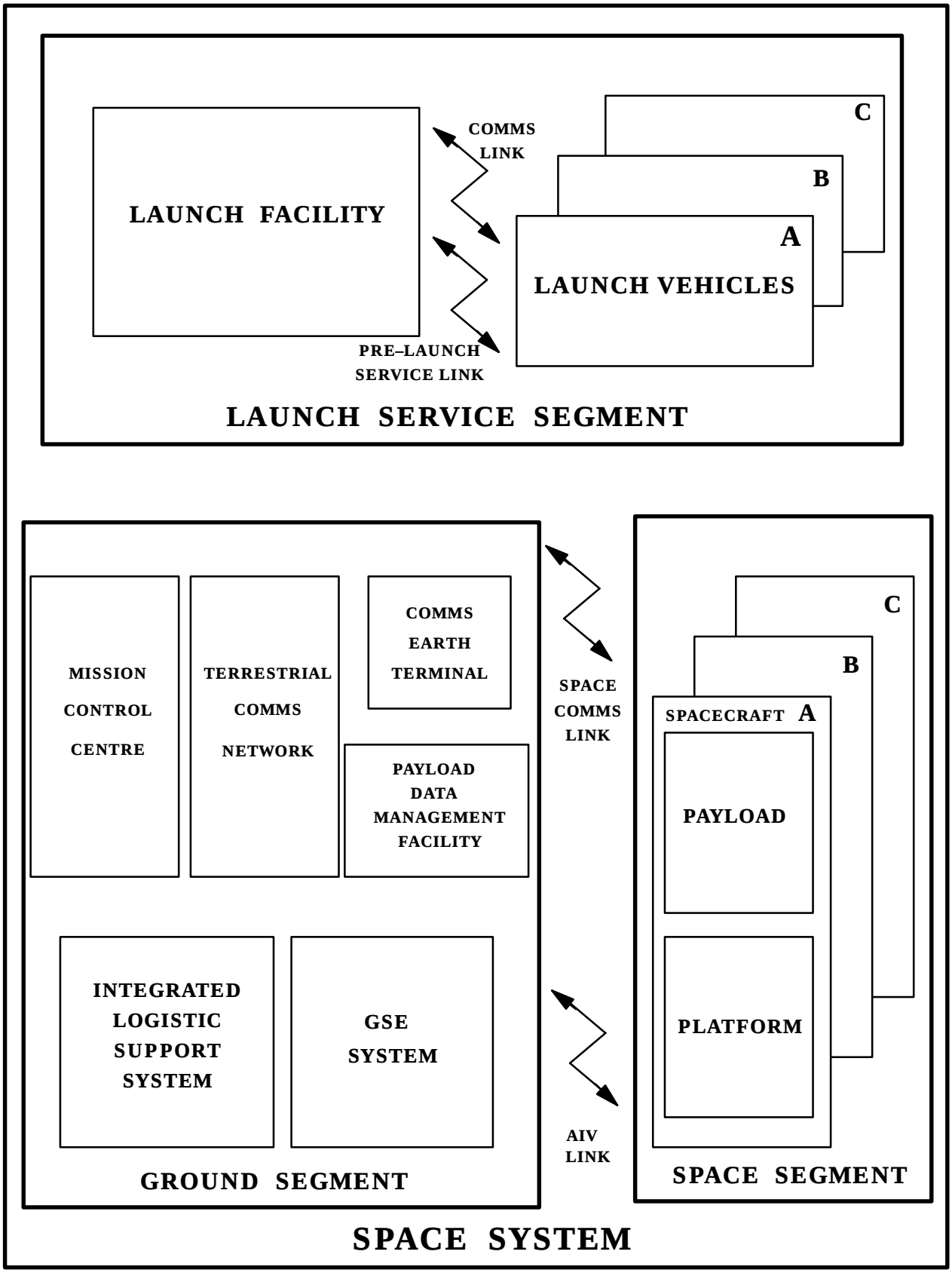
- the engineering, production, operations and product assurance domains each include an element of management which overlaps with the project management domain proper
- production and operations include preparatory and supportive engineering activities, which may also be considered as part of the engineering domain
- product assurance includes reliability, availability, maintainability and safety activities, which form an essential part of the design process in the engineering domain.

Nevertheless, categorisation into these five principal domains provides a useful first–level partition of space–project activities, enabling a complex activity to be split into less complex elements which can be addressed separately and in parallel. This categorisation is adopted as the first–level breakdown of the European Cooperation for Space Standardization (ECSS) standards architecture, except that no standards are defined which address the totality of the production and operations domains; requirements for relevant aspects of production and oper-

ations are, however, addressed within the project management, engineering, and product assurance standards.

This document, ECSS–E–00, which is the top–level standard in the Engineering branch of the ECSS standards system, serves to introduce and define the engineering domain within a space project, and to describe the principal activities within it. It also serves as an introduction to the lower level standards in the ECSS Engineering branch, which define the requirements for these engineering activities, and also provides guidance in the use of the engineering standards in project applications.

It is emphasised that this standard is applicable to all the elements of a space system, including the space segment, the launch service segment, and the ground segment (see Figure 1).



NOTE GSE = Ground Support Equipment
AIV = Assembly, Integration, Verification

Figure 1: Illustration of the Scope of a Typical Space System

(This page is intentionally left blank)

5

The Engineering Domain

5.1 Introduction to the Engineering Domain

The project engineering process aims at a satisfactory response to a user's needs by the creation and delivery of a product for the intended mission; it occurs within a domain which can be represented as illustrated in Figure 2. Three orthogonal axes can be identified within this domain :

- the **"system engineering process"** axis, which includes the function within the domain which guides and powers the engineering process (called "integration and control"), and those processes which are exercised iteratively through the project in order to design and verify a product which meets the customers requirements. The functions within the system engineering process are introduced in clause 5.2 below, and described in more detail in clause 6.
- the **"engineering disciplines"** axis which includes those engineering disciplines (systems, electrical, mechanical, software, communications, control and operations engineering) which contribute their expertise to the engineering process. The engineering disciplines are addressed in clause 5.3.
- the **"levels of decomposition"** axis, which indicates the level (part, assembly, equipment, subsystem, system) at which the engineering process is being exercised. Levels of decomposition are addressed in clause 5.4.

Each cell within the domain in Figure 2 represents a potential project engineering activity; it can be identified by means of three labels, which indicate :

- the type of system engineering activity
- the engineering discipline concerned
- the level of decomposition

For example, the cell marked in Figure 2 indicates mechanical analysis at equipment level.

The activities on the system engineering process axis should not be confused with the phases in the project life cycle, (defined in ECSS–M–30) even though similar nomenclature may be adopted. Rather, they should be thought of as activities in a process which may need to be iterated several times during the course of a project, in order to achieve a satisfactory outcome at each stage. The way in which these activities are arranged, their relative importance and the amount of effort devoted to each activity will vary according to the type of project, its complexity and the extent of the technological advance and innovation required to implement it; generally, however, each activity should be considered and exercised concurrently during each project phase, with its relative importance adjusted ap-

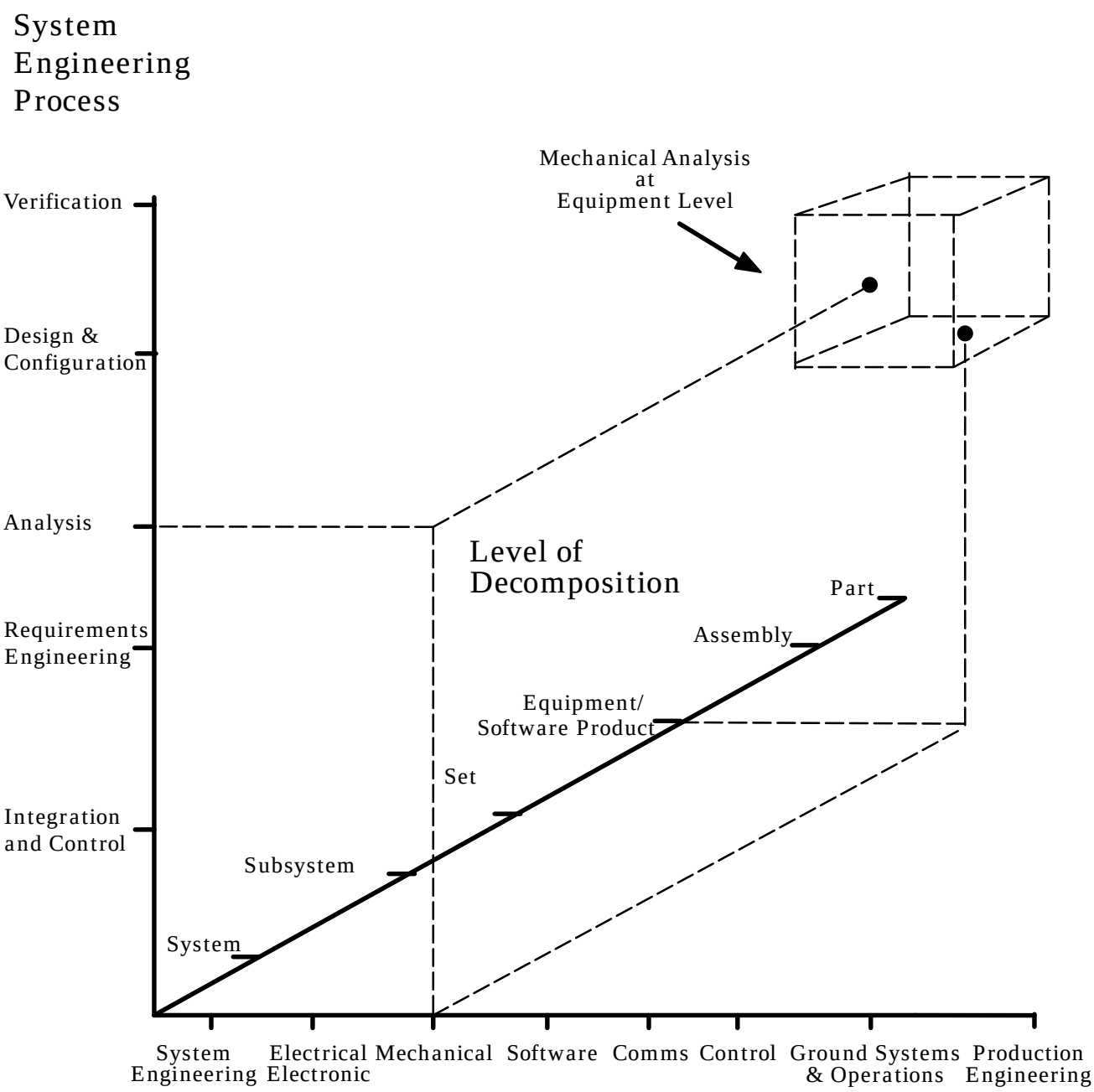
propriately, so that the downstream implications of each decision are fully assessed and recognised.

As examples :

- a feasibility study should address operations as well as requirements and architectural design.
- it is important to verify that requirements have been realistically allocated in a way which satisfies all participants during a project definition phase.
- it is imperative that production and verification are addressed during design engineering activities, to ensure that the product is manufacturable and verifiable.
- it is necessary to exercise the complete system engineering process if modifications to the design are introduced during the project operations phase.

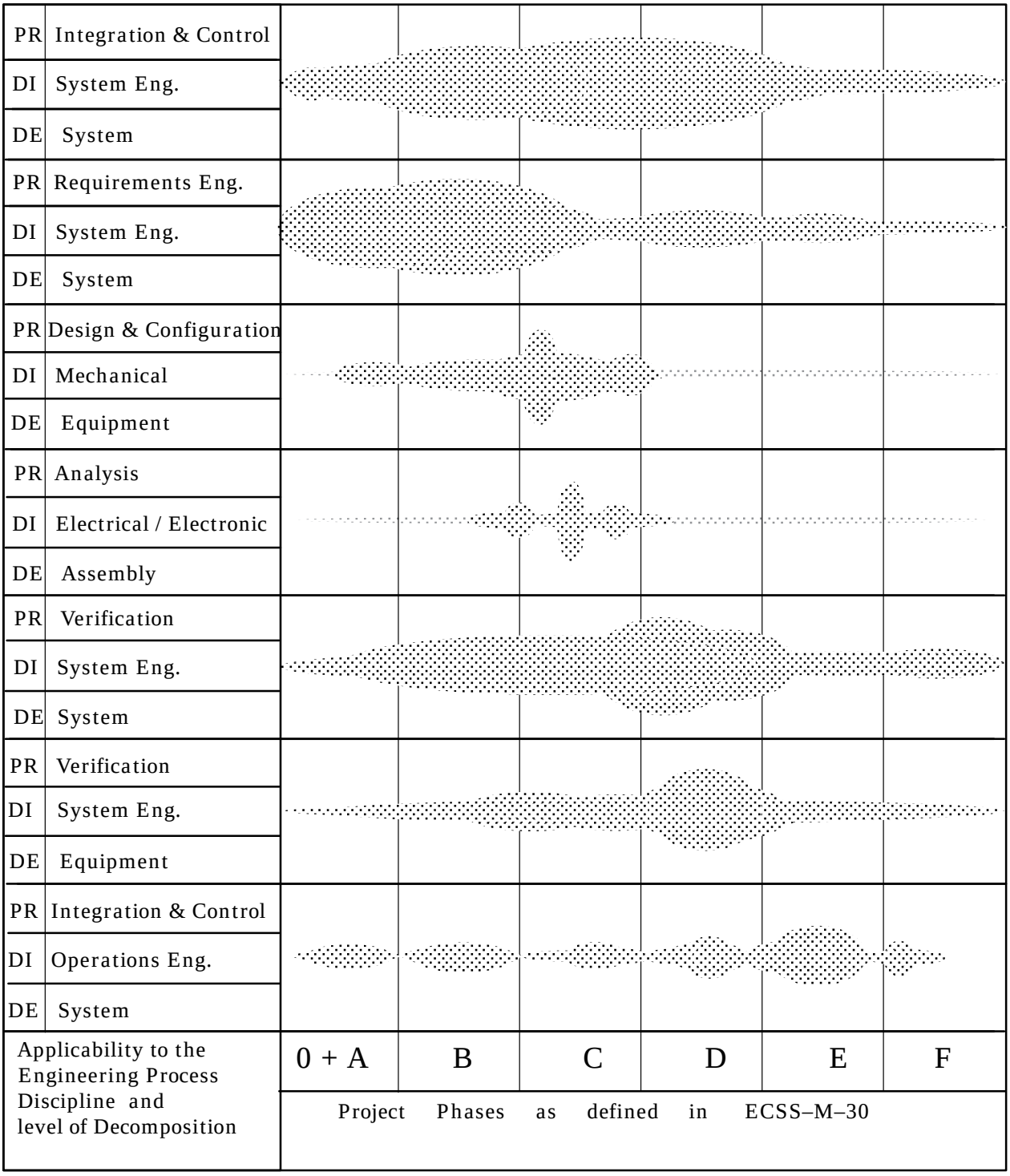
Equally, the predominant level of assembly at which engineering activities take place, and the involvement of the engineering disciplines, will vary with time in a way which depends on the nature of the product.

Consequently, the activity level in each cell in the engineering domain will vary in a complex way with time. Figure 3 illustrates the typical variation of the level of engineering activity with time, related to project phases, for sample cells within the engineering domain.



NOTE The sequence of the items along the axes is not significant.

Figure 2: Representation of the Engineering Domain



NOTE 1 The width of each trace represents the relative intensity of the engineering activity

NOTE 2 PR = System Engineering Process DI = Engineering Discipline
DE = Level of Decomposition

Figure 3: Example Variation with Time of the Intensity of Possible Activities within the Engineering Domain related to Formal Project Phases

5.2 The System Engineering Process

A simplified representation of the system engineering process is presented in Fig ure 4, in which five functions can be identified:

- the integration and control function, which manages the concurrent contributions of all participating functions, of all disciplines, throughout all project phases, in order to optimise the total system definition and implementation
- the requirements engineering function which ensures that the product requirements are complete, unambiguous, and properly express the customer's need
- the analysis function, which comprises two subfunctions which although related are rather different in nature:
  - definition, documentation, modelling and optimisation of a functional representation of the system (functional analysis)
  - analytic support to the requirements, design, and verification functions
- the design and configuration function, which generates a physical architecture for the product, and defines it in a configured set of documentation which forms an input to the production process
- the verification engineering function, which iteratively compares the outputs from other functions with each other, in order to converge upon satisfactory requirements, functional architecture, and physical configuration, and defines and implements the processes by which the finalised product design is proved to be compliant with its requirements.

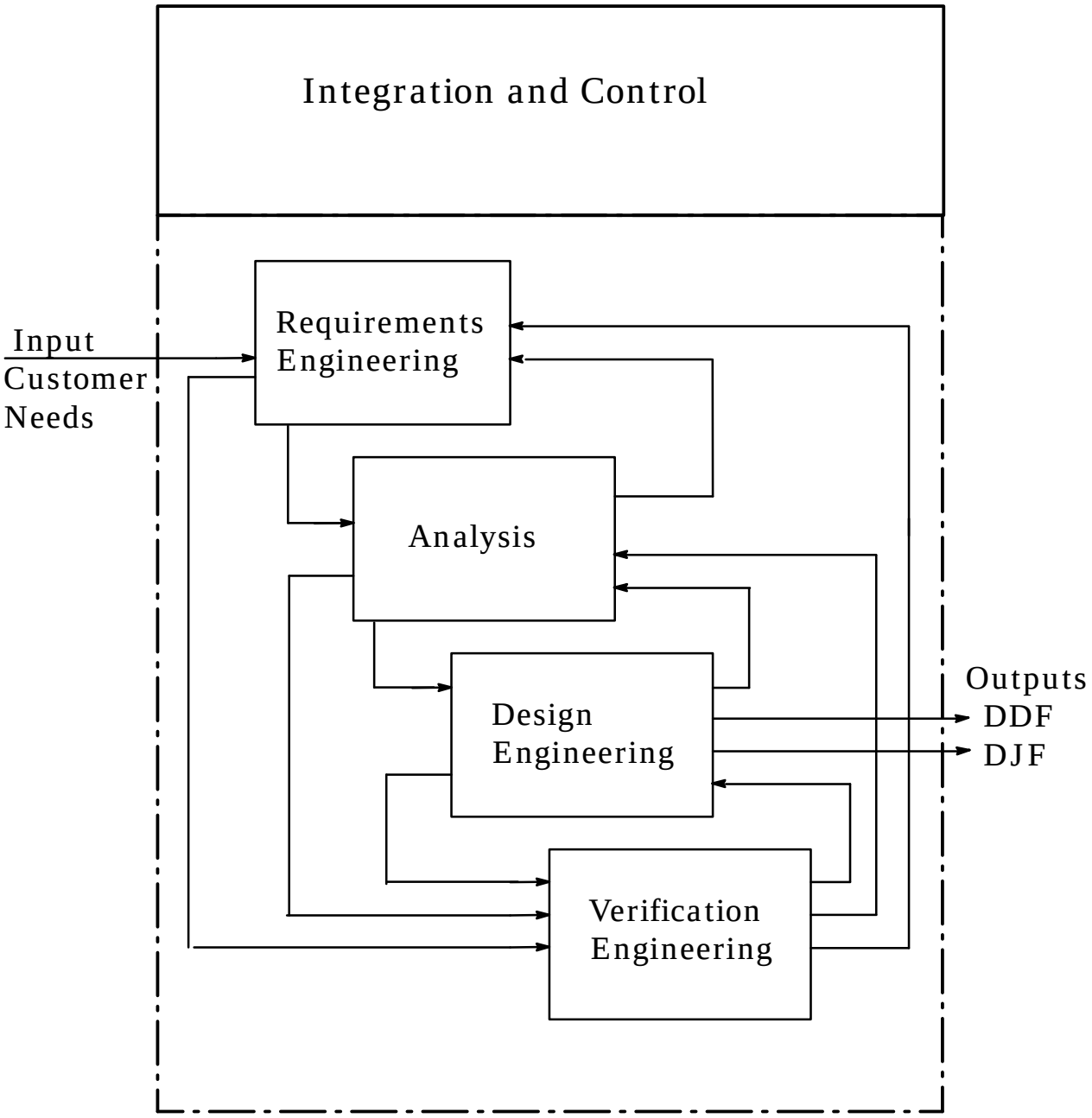
The system engineering activities illustrated above are equally valid and necessary at all levels of decomposition within the space product. The process is commonly called "system engineering" when applied at the top ("system") level; however, each responsible designer of a lower item should recognise himself as the system engineer for his product, and ensure that the system engineering process is fully exercised. The process is generally exercised primarily at top level during the early stages of a project, and addresses lower levels with greater thoroughness as the project progresses.

In real projects, the customer's needs may evolve as the project progresses; the system engineering process should be prepared for this, and be robust enough to respond to it in a timely way through controlled iterations for affected product areas. In all cases, revised requirements enter the system engineering process as shown in Figure 4, and all functions are exercised to the necessary extent.

Because of their fundamental importance in the space project engineering process, the system engineering functions (and integration and control requirements engineering, analysis, design and verification) are described in more detail in clause 6.

Quality assurance requirements relating to the system engineering process are defined in ECSS–Q–20.

It will be noted that "development" is not included as a primary function within the system engineering process; nevertheless, activities often loosely categorised as "development" play an important part in space projects. The place of development within the engineering domain is explained in clause 5.5 below.



NOTE DDF = Design Definition File
DJF = Design Justification File

Figure 4: Simplified Representation of the System Engineering Process

5.3 Engineering Disciplines

Space project engineering is a multidisciplinary activity employing a wide range of technologies, with no one person able to master all of the disciplines at the level of expertise required to ensure a successful outcome. Consequently, resources from a number of engineering disciplines generally contribute to the engineering process, at least at the higher levels of complexity.

Those disciplines are:

- the “generalist” discipline of system engineering, which is responsible for integrating and controlling activities in the system engineering process; it also contributes strongly to the other system engineering functions, in which it is supported by the specialist disciplines listed below.

- the electrical/electronic discipline, which addresses all aspects of the electrical and electronic design of space products, including functions such as power generation, storage, conversion and distribution, optical, avionics, and microwave technologies, electromagnetic compatibility, and electrical interfaces and interconnections.
- the mechanical discipline, which addresses all aspects of the mechanical design of space products (where mechanical in this context includes structural, thermal and material selection aspects), propulsion for spacecraft and launch vehicles, pyrotechnic and environmental control/life support functions, and mechanical parts, interfaces and interconnections.
- the software discipline, which addresses the requirements definition, architectural design, detailed design, coding, integration and test of software products.
- the communications engineering discipline, which addresses spacecraft–to–ground, spacecraft–to–spacecraft, ground–to–ground and on–board communications links, including aspects such as link budgets and protocols.
- the control engineering discipline, which covers all aspects of automatic control in space systems
- the production engineering discipline, also part of the “production” domain, which covers all aspects of preparation for efficient manufacture, assembly and integration; production engineering is addressed in clause 7.1.
- the operations engineering discipline, also part of the “operations” domain, which covers the preparations for efficient operation of the system after delivery, and for its eventual safe disposal. Operations engineering is addressed in clause 7.2.

The requirements placed on the activities of each of these engineering disciplines (except for production engineering) is addressed in a branch of the ECSS Engineering Standards, as explained in clause 8 of this standard.

A separate branch is not devoted to production engineering requirements, as these generally depend on the specific methods and resources available to the supplier; however, the engineering requirements of the assembly and integration of complex products (essentially the production engineering for subsystems and systems) are addressed in the systems engineering branch of the ECSS standards.

5.4 Levels of Decomposition

Definition of a space product generally proceeds from a functional to a physical description. The physical description is formalised in the Product Tree, which is a structure resulting from the orderly and exhaustive breakdown of the end product into successive levels of partial products. These partial products change in nature as the breakdown progresses from the top level through to lower levels of decomposition; they generally become less complex functionally, more compact and self–contained physically, and include fewer different technologies.

The “levels of decomposition” used in the ECSS system, with their essential characteristics, are summarised in Figure 5, and defined and explained below.

- The top level of decomposition recognised within ECSS is the ***system***. It is defined as a set of interdependent elements constituted to achieve a given objective by performing a specified function. The physical form of the entities may include any combination of hardware, software and personnel. It is the system–level product which fulfils the customer’s need.
- The next–lower level of decomposition is the ***subsystem***. It consists of a set of interdependent elements constituted to achieve a given objective by performing a specified function, but it does not, on its own, provide sufficient functionality to satisfy the customer’s need. In space projects, subsystems and lower levels of decomposition usually consist of hardware and software only.
- The next lower level of decomposition is designated a ***set***. This is a group of physically or functionally related elements, which are usefully considered to-

gether for technical or organisational reasons, but whose association does not increase their functionality.

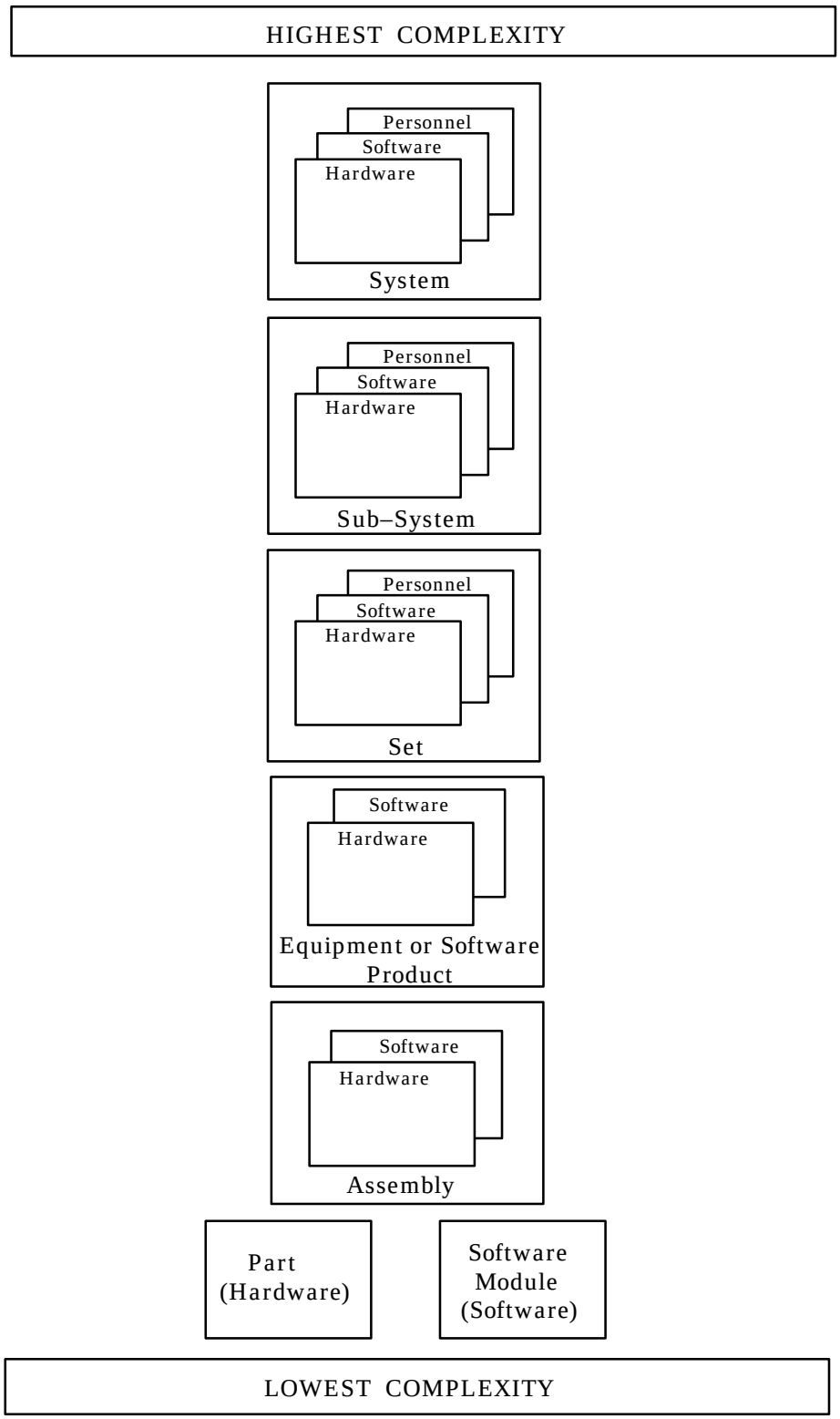
- The next lower level of decomposition is an item designed and built to achieve a specific purpose, which is implemented as a single entity. It is designated an ***equipment*** when it consists of a hardware element (which may include embedded software), and called a ***software product*** when it comprises software only.
- The next lower level of decomposition is called an ***assembly***. It consists of two or more parts or software modules (as defined below) joined together to form an item with defined physical characteristics, but which does not by itself achieve a specific purpose. Typically, an equipment or software product will consist of a number of assemblies; a hardware assembly may include embedded software.
- The lowest defined level of decomposition is a hardware item which cannot be disassembled without permanent destruction (designated a ***part***), or any software item which is discrete and identifiable with respect to compiling, combining with other items, and loading (designated a ***software module***).

The following information provides further clarification of the use of “levels of decomposition” in space systems:

- Not all levels of decomposition are necessary in every product. For example, the subsystem and/or set level may be omitted, leading to a system that is broken down immediately into equipments.
- Equally, some of the levels of decomposition may be repeated; for example, an overall space system may contain a satellite and a ground segment, both also considered as systems. The term “element” is sometimes used specifically to describe these “systems within systems”. Elements which operate entirely in space or on the ground are often designated the “space segment” and “ground segment” respectively. Subsystems, equipments, and assemblies may also contain elements of the same name; parts cannot, however, by definition, contain other parts, and software modules cannot contain other software modules.
- In the early stages of a project, attention is focused on the top level product; as the project matures, lower levels of decomposition are addressed in successively greater detail. It is, however, necessary that critical lower level items be identified and submitted to the system engineering process in sufficient detail at an early stage, to ensure that no problems are encountered later which cannot be resolved within the project cost and schedule constraints.

It is common practice to give each type of item within the system a unique proper name, in addition to its configuration identifier, for ease of reference and to aid comprehension of its function; the proper name may indicate the level of complexity (e.g. Propulsion Subsystem, Frequency Generator Equipment) but this is not essential. A numerical suffix is generally used to distinguish between repeated interchangeable items (e.g. Power Amplifier N°7).

Terms such as, for example, “payload”, “instrument”, “platform”, “module” and “stage”, are used to form proper names, and do not represent levels of complexity additional to those defined above.



NOTE 1 All levels of decomposition are not necessarily used in a specific system

NOTE 2 Any level of decomposition except the lowest may be repeated hierarchically in a specific system

NOTE 3 Any level of decomposition including the lowest may be repeated at the same level in a specific system

Figure 5: Levels of decomposition

5.5 Development

The term “development” is commonly used in a number of different senses:

- to describe the process in which new technologies are made available for use in future projects
- to describe the generation of new products (generally at equipment or lower complexity levels) which are intended for repeated use in future projects
- to describe the process by which confidence is established in a design before production of a deliverable product commences.

It is clear from the above that development is not a separable activity within the system engineering process, comparable with “analysis” or “design”; it is rather a term describing all or part of a project in which activities may take place in all of the five project domains identified in clause 4 above. The first two types of “development” cited above are essentially projects in themselves, to which the complete set of ECSS–E standards a priori applies; the third type of development is explained in more detail below.

In the sense of elaboration of a design in preparation for production, development engineering may include, for more complex products, the production of development models and prototypes and their testing and operation. It contributes significantly to the verification process, and activities should be coherent with the verification plan. The construction and test of the development models and prototypes confirms that the required level of design maturity has been achieved and permits the final design to be frozen.

The organisation of this activity depends considerably on the complexity of the product and on the technological advance to be achieved with respect to past experience. Generally speaking, development may have the following objectives :

- to develop any new technologies that may be necessary within the project context
- to improve development model design by iterative loops of manufacture, test and evaluation when theoretical design work and simulation alone are not sufficient.
- to gather performance data for characteristics that are difficult to simulate (for example ageing, endurance).
- to gain experience that will improve estimates of design margins and reliability (using, for example, over tests, limit tests, or failure mode tests).
- to validate and improve simulation models; these models may be purely numerical, or may be combinations of numerical models and real elements. They may represent all the functions of the product, or a subset of the total functionality (for example, dynamic functions only). Some tests may be performed on reduced scale models.
- to develop and qualify manufacturing processes
- to adjust and validate assembly, handling and operational procedures and in general all user procedures for the entire life cycle.

Development activities will not generally produce new categories of documentation; rather they will permit documents generated within the fundamental processes of system, production and operations engineering to be increased in maturity

6

Overview of the System Engineering Process

6.1 System Engineering Integration and Control

The system engineering integration and control process manages the contributions of all participants, through all project phases, in order to optimise the total system definition and implementation. It can be identified with the common volume of the engineering and management domains, responsible for:

- overall management of engineering activities
- planning the engineering activities, including generation of key plans defining the intended requirements engineering, analysis, design, and verification activities (sometimes collected together to form a document called the Design and Verification Plan)
- production and maintenance of the project engineering data base
- definition of rules for the control and exchange of engineering data within the project, using recognised standards wherever possible
- management of external and internal systems interfaces
- a set of maintained system budgets, utilising a margin strategy which is coherent at all levels, and allows for margin reallocation as the design evolves and matures
- collation of the engineering inputs to the risk assessment and management process described in ECSS–M–00

The system engineering process often progresses at different speeds for different elements of the product, because (for example) of the use of both slightly modified and newly developed hardware, because of technical problems in some areas, and because of differences in emphasis of the same process stages for hardware and software. It is an important part of the integration and control function to manage this situation in such a way that the global system engineering process achieves its objectives.

The system engineering integration and control process is assisted in its operations by other system engineering functions, and by the specialist technical disciplines.

6.2 Requirements Engineering

The principal input to the requirements engineering (RE) process is a statement from the customer of his **perceived** requirements or needs. The purpose of RE is to provide designers with all the necessary data to accurately specify an approach which will satisfy these perceived needs. As the outputs from the RE process may have significant impacts on project cost and schedule, each requirement should be necessary, attainable, traceable, unique, clear, concise, properly referenced, and verifiable unambiguously.

Requirements are structured in different levels of decomposition, as defined in clause 5.4 above, depending on the nature of the product and on the sharing of activities between participants with development responsibilities. As a result of the RE process, each element identified in the product tree (defined in ECSS–M–10) has a technical specification.

A comprehensive RE activity should achieve:

- A statement of mission objectives
- The incorporation of statutory requirements imposed by European Union or national legislation, even if not explicitly specified by the customer
- A description of operational life of the product from delivery to disposal, and derivation of reliability, availability, and maintainability requirements
- Characterisation of external interfaces including interfaces with elements of a higher–level system, and constraints resulting from the external environment
- An assessment of environmental conditions and derived operating loads
- A statement of requirements for characteristics of different functions (performances, constraints, ...)
- A definition of design to cost and schedule objectives
- A definition of any mandatory design safety factors and margins
- A definition of any requirements on verification
- An understanding of the possible rates of exchange between characteristics (cost, performance, reliability...), including definition of order of preference and weighting factors.

In addition, the possible imposition of specific designs and technologies should be considered; for example, the use of an existing standard spacecraft platform to achieve a short time scale may influence major aspects of the design.

An optimised RE activity needs careful phasing and will generally require iterative trade–off studies with other system engineering activities and with adjacent levels of decomposition. The extent to which iterative trade studies are necessary will depend primarily on the complexity and the innovative content of the project.

Requirements engineering may be considered as having been satisfactorily completed when all lower levels have accepted their statement of requirements and their consequences have been sufficiently evaluated. Customers should agree that the product defined by these requirements will fulfil their needs, and the means to demonstrate that the product will comply with them must have been correctly identified.

The primary output of the RE process is a detailed Statement of Requirements (or Technical Specification or Requirements Baseline) agreed between the author and the user of these requirements, supported by sufficient lower level documentation demonstrating the feasibility and acceptability of all critical areas of the proposed design solution.

6.3 Analysis

Analysis is performed at various stages throughout the product life cycle, at all levels of complexity, and for all operational modes. Objectives of the functional analysis process include:

- An identification of the functionality required to meet the requirements, captured in a functional model of the system; the optimum approach is selected following trade studies of alternative solutions
- Assessments of predicted performance, in operational, test and failure conditions, based on stimulation of the system model, which are updated as appropriate during the project life cycle. They can be used to facilitate dialogue with users, and hence clarify their needs, and to confirm the required characteristics of lower level assemblies.
- Identification of feared events (originating from characteristics of the product itself, or caused by the product's environment), through dependability and safety engineering activities, with risks reduced according to their probability and gravity. Generally based on past experience at the beginning of the project, these activities subsequently focus more and more on analysis of the actual design and anomalies encountered during the development phase. Dependability and safety requirements are defined in ECSS–Q–30 and ECSS–Q–40.
- Allocation of requirements to lower levels

The principal objectives of the analysis process which supports requirements, design, and verification engineering are:

- Generation of analyses covering all technical disciplines relevant to the product (mechanical, thermal, electrical, ...). These analyses, which contribute to the verification process described in clause 6.4, should consider factors such as:
  - the limitations and validity of the simulation methods
  - the application of design safety factors, margins and contingencies
- An integration of all analyses performed at all levels, and by all disciplines, to produce a coherent whole, which is adequately documented and controlled; generation and maintenance of this overall analysis is sometimes called "technical performance management"

The analysis function uses established methodologies and tools wherever possible.

6.4 Design and Configuration Engineering

In the design and configuration activity, the functional model of the product is defined in a physical architecture (hardware and software). This physical synthesis process, which proceeds from the highest level of complexity to lower levels, is iterated interactively with analysis and verification, to confirm that the required output has been obtained. The principal objectives are:

- a physical architecture, selected after design trade–off studies
- preparation of data for system budgets
- a Product Tree which defines the product architecture
- a design for each item within the Product Tree, responding to the required functional characteristics and specifications, which complies with the requirements, and can be produced, operated and maintained at minimum cost. Design elaboration will, in general require working using concurrent engineering methods with engineering specialists representing the technical disciplines required to realise the product, (and especially with production engineers) prioritisation of characteristics with functional designers, and analyses carried out by dependability and safety specialists.

Two important constraints during the design process are that:

- **Where deemed beneficial** suitably qualified equipment and standard space–qualified components should be employed, as they offer a warranty of validation by experience (provided that their qualification level is consistent with the specific project requirements). Exceptions to this principle are the evaluation, demonstration or qualification of new innovative elements intended for future operational use (refer to development in 5.5 above).
- **During the design engineering process**, the production and operation implications of designs should be considered through processes such as (for example) Design for Manufacturing and Assembly and Design for Operations, following a life–cycle optimisation.

The outputs from the design engineering activity are a Design Definition File which contains all of the information, including drawings and schematics, required to define the characteristics of the product at all levels of assembly, and a Design Justification File (DJF) which provides the rationale supporting the design choices which have led to the design captured in the Design Definition File, and the analysis and test data which show that the design meets all requirements.

6.5 Verification Engineering

Verification is the process of confirmation that the considered system meets the applicable requirements during the course of the product life cycle. The objectives of the verification process are to:

- iteratively check that users needs are properly captured (this activity is also commonly known as validation),
- confirm that design constraints are respected, and that all requirements are met (or are predicted to be met) throughout the operational life of the product; this constitutes “design qualification”,
- accept flight hardware and software (workmanship),
- validate production processes equipment and facilities,
- validate operations tools, procedures and personnel,
- confirm integrity and performance after particular steps of the life cycle.

The verification process is active throughout the complete product life cycle, and consequently should be planned as early as possible. As an example, main verification activities will generally be performed at least during the following phases of a space project : requirements engineering, development, qualification, acceptance, pre–launch, on–orbit, post–flight. Results acquired during each project phase contribute to the global verification process.

A successful verification process starts with a satisfactory set of requirements. To facilitate verification implementation, each requirement should be traceable, unique, clear, concise, properly referenced and verifiable unambiguously. A verification plan should be established showing, for each requirement, the selected verification methods for the different verification levels in the applicable verification phases for each type of system model. The verification strategy should be consistent with the model philosophy.

The verification process should be implemented during the project life cycle through the following steps:

- establishment of verification criteria against applicable requirements, including consideration of required accuracies and methods, and equipment and facility calibration requirements.
- derivation of the planning for the associated verification activities,
- bottom–up execution of the verification activities
- monitoring of the implementation and the execution of all verification activities at all levels (part, module, equipment, subsystem, element of a system, system)
- preparation and approval of the verification close–out documentation.

Methods of verification are :

- test (on–ground, in–flight, on–orbit),
- analysis (including performance simulations),
- review of design (including assessment of similarity with other previously qualified designs),
- inspection,
- demonstration (including operations rehearsals).

For more complex products, taking into account that requirements, design features, and production processes may evolve during development, it is generally necessary to implement a formal design verification campaign, called “qualification”, when the product is frozen. The qualification plan, which is approved at “customer” level, may necessitate deployment of any of the above verification methods. The qualification article(s) is(are) manufactured and tested using the same documentation as will subsequently be used for production, and qualification is granted on the basis of approval of a qualification report.

It is emphasised that, to achieve successful verification, management guidelines have to be applied; in particular, “verification” should be addressed from the earliest phases of a project as a specific programme organisational element.

(This page is intentionally left blank)

7

Other Activities within the Engineering Domain

This clause addresses two areas of space engineering:

- Production Engineering
- Operations Engineering

which lie outside the system engineering process (although they interface with it) and are also related to project phases.

7.1 Production Engineering

Production engineering covers all the preparatory work necessary to ensure that the product will be manufactured, assembled and integrated at the lowest cost, in the defined timescale, and in accordance with the requirements specified.

The objectives of production engineering are:

- an assessment of the environmental impact of manufacturing processes,
- production of manufacturing documentation,
- procurement planning activities, including supplier evaluation and selection, and preparation of procurement documents,
- trade off studies of possible production technologies in coordination with designers, and their evaluation against the criteria to be considered (cost, reproducibility, ...),
- identification and optimisation of critical fabrication and assembly procedures,
- optimisation of the production plant when the product is to have a long production life and uses specific or dedicated facilities,
- evaluation and selection of standard tooling, and identification and design of special tools when required,
- elimination or control through dependability and safety activities of possible hazards, arising either from the product or from the production environment, so that the risks of accidents and nonconformances are reduced.

The production engineering function also provides support to the production process, through solution of problems relating to the product itself or to the production environment, and optimisation of the in–process inspection and acceptance test activities during the production cycle.

The output from the production engineering process is a set of manufacturing documents: the Manufacturing File which will permit efficient production of a quality product; with the Design Definition File, it forms the Production Master File.

7.2 Operations Engineering

In the project context, the word “operations” includes all activities leading to the production of the ground facilities required to support operations, the preparation activities leading up to operations, conduct of operations themselves and all post–operational activities.

In this scheme, project operation activities can be partitioned as follows :

- operations preparation,
- training,
- system validation,
- operation execution, including logistics support
- disposal
- post–operation activities

The first two of these activities will generally be more or less concurrent.

The logistics support may be exercised using a specific support system, which together with the supported system forms the space system itself.

The ground segment is an element of the space system, and all the activities within the engineering domain are in principle applicable. The degree to which they are practised depends on the nature of the requirement and of the solution. The ground segment is addressed as part of “operations” because of its intimate relationship with this function

The major elements of a space system ground segment subject to engineering standards are included in product categories G to K inclusive in Table 9–1. These elements may be part of a multi–mission ground infrastructure, adapted and configured to meet the needs of a specific project. In this case the engineering process and standards will be applied to the infrastructure development itself.

In contrast to the space segment, the ground segment will make use of equipment or will consist itself of services not originally intended for use in a space system, and offered off–the–shelf. Requirements and standards will, in the case of such equipment and services, apply primarily to the as–is product and only in a limited way to the engineering process.

7.2.1 Operations Preparation

The operations preparation activity is performed concurrently with the space and ground segment engineering process. In particular there needs to be early interaction with space and ground segment requirements engineering, analysis, and design engineering activities (including dependability and safety studies) in order to assure operability of the product, with consideration of requirements such as observability, commandability and autonomy, definition of operational modes, and preliminary work on system data bases and user manuals. The end result of the operations preparation activity is a set of plans, schedules and procedures set up to assure safe and efficient mission operations and an optimal use of mission resources with respect to the mission objectives, including degraded modes of operation in the case of contingencies.

7.2.2 Operations Training

Training targets two distinct groups of persons involved in mission operations :

- ground personnel monitoring and controlling a space vehicle, or operating associated ground facilities,

- for manned missions, the persons piloting vehicles or conducting mission operations in orbit.

The objective of the training is the familiarisation of personnel with the plans and procedures elaborated during the mission operations phase. Frequently, training will be achieved by a participation of the trainees in the operations preparation phase and in the system validation activities, for both space and ground segments. While all training objectives need to be achieved before the start of operations execution, training will continue afterwards in order to bring new staff into operations and to reinforce the capabilities of existing staff.

7.2.3 Operations Validation

Operations validation consists of exercising the completed facilities and trained personnel in accordance with the defined plans and procedures, in scenarios which simulate (as closely as possible before operation of the space segment) the situations which will apply during mission operations. The space segment/ ground segment interfaces are exercised and validated using simulators for the space segment.

Fault conditions are simulated so that contingency procedures can be practised. The outputs from the operations validations are plans, procedures and personnel fully prepared for mission operations.

7.2.4 Operations Execution

Operations execution as a phase in the mission life cycle denotes the utilisation of the completed product for its intended purpose. The start and end points of this phase are:

- for launchers : from launcher erection to safing operations after deployment of last payload element (including controlled re–entry as applicable) or completion of retrieval of retrievable launch element, whichever comes later,
- for space vehicles : from launch to disposal in orbit, retrieval, or destruction.

The following tasks are included in this phase (the significance of the asterisked items is explained below) :

- launch sequence operations,
- in–orbit calibration, test, and commissioning
- update and refinement of mission planning and schedules (*),
- remote monitoring and control of the payload, launcher or space vehicle, including trend analysis to verify nominal operation and provide early warning of degradation,
- ground facilities operations,
- in–orbit mission operations by humans,
- ground facilities maintenance (*),
- in–orbit maintenance (major in–orbit maintenance activities may be considered as separate missions (*)),
- re–configuration of space vehicle hardware or software in response to mission evolution or faults / contingencies,
- update of flight operations procedures and plans as a result of lessons learnt, space hardware / software reconfiguration, or contingencies (*),
- retrieval/recovery of space vehicles and experiments and of re–usable launchers
- ground refurbishment and turn–around of re–usable space vehicles or elements (*)

All tasks marked with an asterisk (*) imply possible modifications to the product and will therefore be subject to all strict requirements of the engineering process, and in particular to design control, configuration control of the delivered product, and verification.

7.2.5 Disposal

Disposal constitutes the tasks, actions, and activities to be performed and system elements required to ensure that disposal of decommissioned and destroyed or irreparable system end items complies with applicable environmental regulations and directives. Additionally, disposal addresses the short–term and long–term degradation to the environment and health hazards to humans and animals.

The operations engineering process includes disposal analyses to support development of the products and processes for disposal. Factors for process wastes / outputs and used products / components are included in environmental analyses. The analysis considers alternative methods of storage, dismantling / reusing, recycling, and destruction of system parts and materials.

Requirements for new or modified disposal methods are determined. Costs, sites, responsible agencies, handling and shipping, supporting equipment, and applicable international, national and local regulations should be included in the analysis.

7.2.6 Post–operations

The post–operations execution activity, in particular the space vehicle monitoring, results in collection and analysis of information on the performance of the space and ground systems, the appropriateness of technologies used, and the quality of the human–machine interfaces. This is a pre–planned part of the overall engineering process and provides feedback to the engineering of future space mission systems.

8

Overview of ECSS Engineering Standards

Compared with the ECSS–M Standards, which relate principally to the organisation and monitoring of the work to be done within the project, and the ECSS–Q Standards, which relate principally to the organisation of activities aimed at ensuring that the work results in a quality product, the ECSS–E Standards are more specifically devoted to the products themselves. They cover:

- The engineering process as applied to space systems and their elements or functions
- Technical aspects of products used to accomplish, or associated with, space missions.

Space missions feature amongst those activities within the real or human endeavour which are highly intolerant to errors in design, production, and operation. Consequently, a thorough appreciation of the required attributes of the steps in the engineering process is essential for all participants. Within the ECSS–E architecture, standards will be found which address the totality of the engineering process in general, and specific aspects in detail. They generally apply to complex, multi–disciplinary situations.

Standards within the ECSS–E architecture which address the technological aspects of products are aimed at:

- avoiding project–specific repetition of engineering activities
- achieving interoperability of products at all relevant levels within the system, and within the external system environment
- capturing previous best practice to ensure product reliability

They are often specific to a relatively simple product employing a single dominant technology, or to the basic constituents of such products.

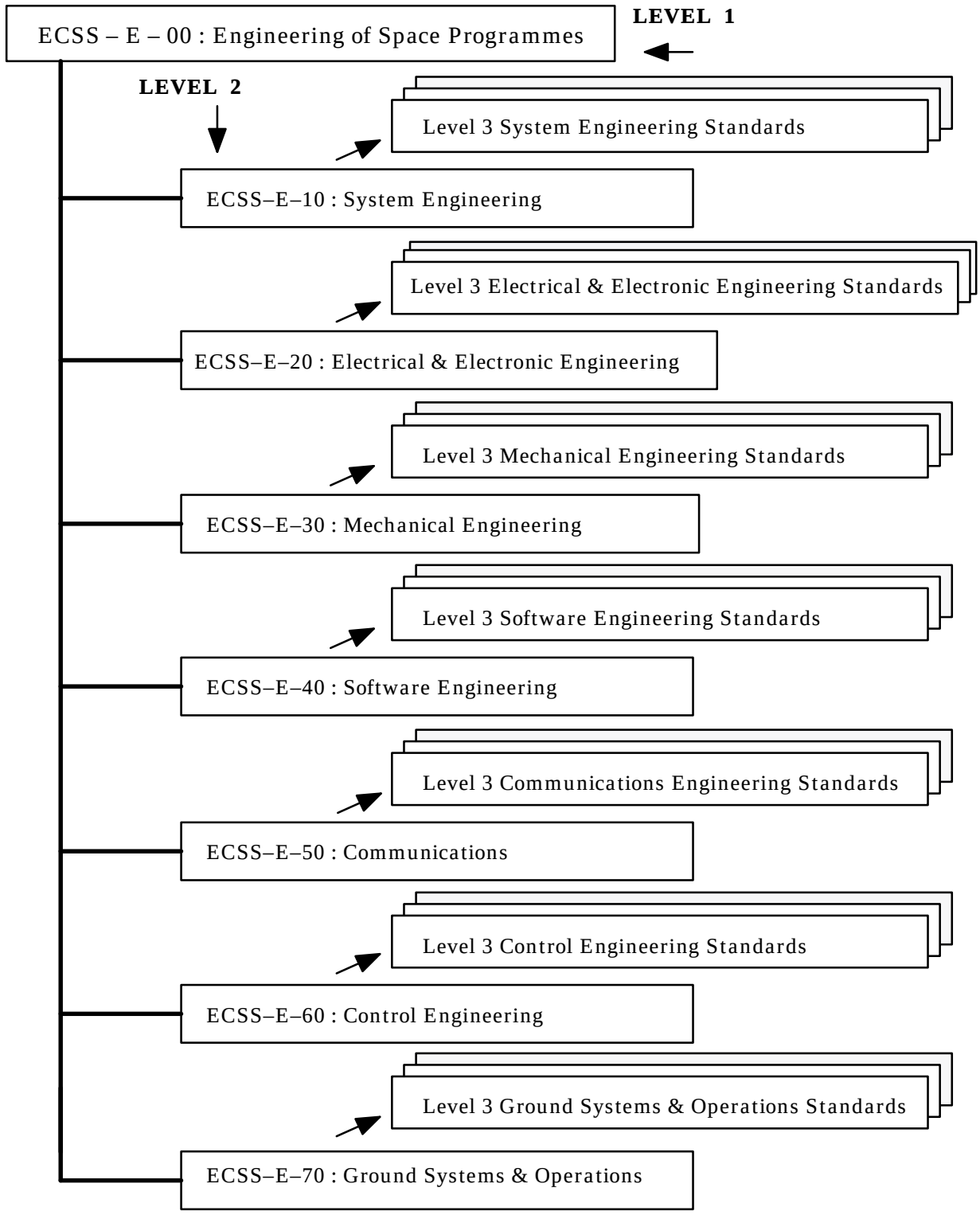
Specifications, guidelines, manuals, handbooks and procedures are all identified collectively as ECSS Standards. Their objective is to enable engineers to work as efficiently as possible and to achieve the most appropriate product for the project application.

Three document levels are recognised within the ECSS Engineering Standard architecture, as illustrated in Figure 6:

- Level 1 contains only this document ECSS–E–00
- Level 2 contains the standards which head the major branches of the engineering standards architecture

- Level 3 contains the standards which address specific aspects of the engineering processes and/or technologies in each branch.

There is no defined structure below Level 2; each Level 3 standard is numbered sequentially. Table 1 gives guidance on the scope of the standards within each branch.



NOTE 1 The level 2 standard ECSS–E–10 defines the requirements for system engineering within the project life cycle, including a definition of required documentary outputs related to the project phases defined in ECSS–M–30.

NOTE 2 The ECSS–E–30 branch contains an introductory level 2 document, and eight supplementary level 2 documents, each of which addresses one of the disciplines identified in table 1.

Figure 6: Architecture of the ECSS Engineering Standards

Table 1: Scope of Level 3 Engineering Standard Sets

Number	Title	Scope of Level 3 Standard Sets	Notes
ECSS–E–10	System Engineering	System engineering process; system requirements definition and analysis; assembly, integration, verification; celestial mechanics and mission analysis; spacecraft / launcher interface; environments; human factors and ergonomics; configuration definition	1 2
ECSS–E–20	Electrical & Electronic Engineering	Electrical power; electromagnetics; optics; avionics	3
ECSS–E–30	Mechanical Engineering	Thermal control; structures; mechanisms; environmental control and file support; propulsion for both launchers and satellites; pyrotechnics; mechanical parts; materials	4 6
ECSS–E–40	Software Engineering	All aspects of software engineering including requirements definition, design, production, verification and validation, and transfer, operations and maintenance	7
ECSS–E–50	Communications	Ground communications; space to ground and interorbital links (telemetry, telecommands and data) and interfaces between items of on–board equipment	
ECSS–E–60	Control Engineering	Rendezvous and docking; attitude and orbit control; robotics	
ECSS–E–70	Ground Systems and Operations	Definition of mission operations requirements; ground system development and validation; preflight operations for spacecraft and launch vehicles; mission control; in–orbit operations; mission data description and utilisation: post–flight operations; engineering aspects of integrated logistics support.	5 8

NOTE 1 Technological aspects of communications interfaces (e.g. electrical definition of telecommand interfaces to equipments) are included in the appropriate subbranch of E–20; communications protocols are included in E–50

NOTE 2 Definition of electromagnetic compatibility environments is included in E–10, but equipment electromagnetic compatibility design aspects are included in E–20 or E–30 as appropriate

NOTE 3 Includes microwave equipment design

NOTE 4 Materials selection for specific design applications is included in E–30; acceptance of materials is included in ECSS–Q standards

NOTE 5 The primary treatment of Integrated Logistics Support is contained in the ECSS–M standards.

NOTE 6 The E–30 standards address requirements for the exchange of technical data

NOTE 7 The E–40 standard is applicable both to embedded software, reflecting the constraints of the space segment, and to software which supports the development and operation of the system on the ground

NOTE 8 The E–70 standard addresses both ground systems and operations, for the reasons explained in 7.2.

9

Domain of Application of ECSS–E Standards

This clause describes the domain of application of the ECSS–Engineering standards. This domain is characterised by:

- specific product types, defined in 9.1
- project criticality, addressed in 9.2

These classifications aid the customer in the process of selection of ECSS–E standards for application to his project through contract action (described in 10).

9.1 Space Product Classification

The Space Product classification presented in Table 2 defines the product type domain to which the ECSS Engineering standard set is applicable. Each specific engineering standard includes guidance on the product type(s) to which it may be applied.

9.2 Space Project Criticality Classes

The Level 1 Management Standard ECSS–M–00 defines four project criticality classes, ranging from a minimum cost project, to a programme where mission loss would have “unacceptable” consequences. The classification of a project according to these criteria aids the customer’s decisions on the application of ECSS standards to the project. It is envisaged that project criticality will have most effect on the selection of management and product assurance standards (especially in the area of risk identification and management); there will be relatively little effect on the selection of engineering standards, as the same basic engineering processes should be exercised in all cases but the level of detail to which the processes descend may be modified. In relevant cases, the specific standards in the ECSS–E set include guidance to the user on application to projects in different criticality classes.

Table 2: Space Product Types

Primary Reference	Space System Element	Secondary Reference	Category	Notes
A	Launch Vehicle	1 2	Man rated Unmanned	
B	Transfer Vehicle	1 2	Man rated Unmanned	
C	Re–entry Vehicle	1 2	Man rated Unmanned	
D	Spacecraft, including spacecraft platforms	1 2 3 4 5 6	Satellite (GEO) Satellite (LEO) Satellite (other) Space Station (manned element) Space Station (unmanned element) Interplanetary probe	
E	Landing Probes and Rovers			(3)
F	Payloads	1 2 3 4 5 6	Communication Payload Instrument Re–usable Space Element Space Station Facility Sounding Rocket Payload Balloon or Aircraft Payload	
G	Ground Systems	1 2 3 4 5 6	Mission Control Centre Payload Control Centre Terrestrial Comms Network Comms Earth Terminal Payload Data Management Facility Integrated Logistics Support System	
H	Launch Facility			
I	Test Facility	1 2	Static Facility Ground Support Equipment	(1) (2)
J	Training Facility			
K	Ground Refurbishment and Logistics Facility for Re–usable Space Element	1 2	Fixed to Launch Vehicle Retrievable	
L	Sounding Rocket			

NOTE 1 Fixed facility such as antenna test range, space simulation chamber

NOTE 2 Transportable equipment used for space segment tests before launch

NOTE 3 Rover includes atmospheric and ground vehicles

NOTE 4 GEO = Geostationary Earth Orbit
LEO = Low Earth Orbit

10

Use of ECSS–E Standards to Define Project Requirements

The ECSS Engineering Standards are publicly available documents, agreed as a result of consultation processes with space agencies and industry in Europe, designed to secure acceptance by users. However, publication of an ECSS–E Engineering Standard does not automatically ensure its use; it becomes applicable on a project only if the purchaser invokes it in the contractually binding documentation, or the contractor claims compliance with it. The usual methodology for application of ECSS Engineering Standards to space projects is defined in sub–clause 5.2 of ECSS–M–00.

A space product may range from a single item of ground equipment through a complex product such as a launcher to a complete space system, and may cover the complete life cycle from conception to disposal. Size, complexity, life cycle and the environment that its elements are subject to (room temperature/one atmosphere to the extremes of low temperature/high radiation/vacuum) are also factors to be considered. ECSS–E draws together a large body of space standards applicable to all classes of product and programme from which a purchaser Project Manager can select a framework to meet the requirements of the user and which is appropriate for the project needs.

Consequently, a standards selection activity will include a discretionary step–by–step tailoring process.

This process should address each facet of the specific requirements of a particular programme, project, programme phase or contractual structure. Standards should be selected and tailored by the customer, in consultation with potential suppliers.

It is important to be aware of the possible interactions between different elements of the project. Throughout, an awareness of the resource limits (including schedule) imposed by the customer should be maintained, and it follows that selected tailored standards should be appropriate to the needs of each application and should not impose unnecessary cost or complexity. The tailoring process should be recorded to facilitate traceability.

A pertinent question is “does the imposition of the standard add value to the product or process?”

This question should be addressed initially by the customer, when deciding which standards to impose and how to tailor them, and again by the supplier, in formulating his response.

Selection and tailoring of ECSS standards for specific project applications is addressed in sub–clause 5.3 of ECSS–M–00. Where necessary, each standard in the E–series contains information on how to tailor that specific standard for project use. This standard ECSS–E–00, which provides information and guidance relevant to all projects, does not require project–specific tailoring.