SLOVENSKI STANDARD
SIST-TP CEN/TR 17603-40:2022

01-september-2022

Vesoljska tehnika - Priročnik o programski opremi

Space engineering - Software engineering handbook

Raumfahrttechnik - Handbuch zur Softwareentwicklung

Ingénierie spatiale - Guide d’ingénierie logiciel

Ta slovenski standard je istoveten z: CEN/TR 17603-40:2022

ICS:

35.080	Programska oprema	Software
49.140	Vesoljski sistemi in operacije	Space systems and operations

SIST-TP CEN/TR 17603-40:2022 en,fr,de

TECHNICAL REPORT

RAPPORT TECHNIQUE

TECHNISCHER BERICHT

CEN/TR 17603-40

June 2022

ICS 49.140; 35.080

English version

Space engineering - Software engineering handbook

Ingénierie spatiale - Guide d'ingénierie logiciel

Raumfahrttechnik - Handbuch zur Softwareentwicklung

This Technical Report was approved by CEN on 20 April 2022. It has been drawn up by the Technical Committee CEN/CLC/JTC 5.

CEN and CENELEC members are the national standards bodies and national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

CEN-CENELEC Management Centre:
Rue de la Science 23, B-1040 Brussels

Table of contents

Figures

Tables

European Foreword

This document (CEN/TR 17603-40:2022) has been prepared by Technical Committee CEN/CLC/JTC 5 “Space”, the secretariat of which is held by DIN.

It is highlighted that this technical report does not contain any requirement but only collection of data or descriptions and guidelines about how to organize and perform the work in support of EN 16603-40.

This Technical report (CEN/TR 17603-40:2022) originates from ECSS-E-HB-40A.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN [and/or CENELEC] shall not be held responsible for identifying any or all such patent rights.

This document has been prepared under a mandate given to CEN by the European Commission and the European Free Trade Association.

This document has been developed to cover specifically space systems and has therefore precedence over any TR covering the same scope but with a wider domain of applicability (e.g.: aerospace).

Introduction

The ECSS-E-ST-40C Standard defines the principles and requirements applicable to space software engineering. This ECSS-E-HB-40A handbook provides guidance on the use of the ECSS-E-ST-40C.

History of the ECSS-E-40

At the beginning was ESA PSS-05. It was a prescriptive list of requirements ordered all along a waterfall lifecycle. It was necessary to improve it because it was too prescriptive and not flexible enough to apply new technologies such as UML.

ECSS was created in the 90's, and ECSS-E-40A was published in 1999. It was derived from ISO 12207, which is a process model. A process model proposes a set of abstract processes, and the software developer defines its own lifecycle that enters and leaves and re-enters the various processes. The process model was very abstract, with sort of meta-processes that were "invoking" other sub-processes. The new ECSS-E-40A was not prescriptive and very flexible to any kind of lifecycle.

ECSS-E-40A was improved because it was too abstract and it was not clear what had to be done. ECSS-E-40B was worked out in order to downsize the abstraction. The invocation was simplified, some processes were grouped. ECSS-E-40B was sent for public review.

The public review recommended improving further the pragmatic aspects of the standard. Therefore another ECSS-E-40B version was produced where the process model was streamlined.

At a workshop in 2004 on the use of ECSS-E-40B, it was recognised that some of the requirements left room for interpretation, which in turn lead to many discussions in the project reviews (especially when they were overlooked during the Software Development Plan review). Therefore the version C of ECSS-E-ST-40 was produced to improve the usability of the standard, refining and streamlining the open requirements, and somehow coming closer to the ESA PSS-05 spirit.

1 Scope

This Handbook provides advice, interpretations, elaborations and software engineering best practices for the implementation of the requirements specified in ECSS-E-ST-40C. The handbook is intended to be applicable to both flight and ground. It has been produced to complement the ECSS-E-ST-40C Standard, in the area where space project experience has reported issues related to the applicability, the interpretation or the feasibility of the Standard. It should be read to clarify the spirit of the Standard, the intention of the authors or the industrial best practices when applying the Standard to a space project.

The Handbook is not a software engineering book addressing the technical description and respective merits of software engineering methods and tools.

ECSS-E-HB-40A covers, in particular, the following:

a. In section 4.1, the description of the context in which the software engineering standard operates, together with the explanation of the importance of following standards to get proper engineering.

b. In section 4.2, elaboration on key concepts that are essential to get compliance with the Standard, such as the roles, the software characteristics, the criticality, the tailoring and the contractual aspects.

c. In section 5, following the table of content of the ECSS-E-ST-40C Standard, discussion on the topics addressed in the Standard, with the view of addressing the issues that have been reported in projects about the interpretation, the application or the feasibility of the requirements. This includes in particular:

   1. Requirement engineering and the relationship between system and software

   2. Implementation of the requirements of ECSS-E-ST-40 when different life-cycle paradigms are applied (e.g., waterfall, incremental, evolutionary, agile) and at different levels of the Customer-Supplier Network

   3. Architecture, design and implementation, including real-time aspects

   4. Unit and integration testing considerations, testing coverage

   5. Validation and acceptance, including software validation facility and ISVV implementation

   6. Verification techniques, requirements and plan

   7. Software operation and maintenance considerations.

d. In section 6 and 7, more information about selected topics addressed in section 5 such as (in section 6) use cases, life cycle, model based engineering, testing, automatic code generation, and (in section 7) technical budget and margin, computational model and schedule analysis.

> NOTE In order to improve the readability of the Handbook, the following logic has been selected for sections 5, 6, and 7:

- section 5 follows the table of content of ECSS-E-ST-40C at least up to level 3 and generally up to level 4. For each sub clause of ECSS-E-ST-40C:
  - + either information is given fully in section 5,
  - + or there is a pointer into section 6 or section 7
  - + or the paragraph has been left intentionally empty for consistency with the ECSS-E-ST-40C table of content, in this case, only " –" is mentioned.
- section 6 expands selected parts of section 5 when:
  - + either the volume of information was considered too large to stay in section 5,
  - + or the topic is addressed in several places of section 5

  In any case, there is a pointer from section 5 to section 6, and section 6 mentions the various places in ECSS-E-ST-40C where the topic is addressed.
- section 7 follows the same principles as section 6, but gathers the topics related to margins and to real-time.

e. In Annex A, as a complement to the ECSS-E-ST-40C Annex A called Document Requirement List [DRL], the documents expected at the Technical Reviews such as SWRR, DDR, TRR and TRB.

f. In Annex B, software engineering techniques appropriate for the implementation of specific ECSS-E-ST-40C clauses and their selection criteria, covering most of the software lifecycle.

g. In Annex C, an example of the Document Requirement Definition of the Software Maintenance Plan.

2 References

EN Reference	Reference in text	Title
EN 16601-00-01	ECSS-S-ST-00-01C	ECSS system - Glossary of terms
EN 16603-10	ECSS-E-ST-10C	Space engineering – System engineering general requirements
EN 16603-40	ECSS-E-ST-40C	Space engineering - Software
EN 16603-70-01	ECSS-E-ST-70-01C	Space engineering - On board control procedures
	ECSS-E-TM-40-07A	Space engineering - Simulation modelling platform
EN 16601-40	ECSS-M-ST-40C	Space project management - Configuration and information management
EN 16602-80	ECSS-Q-ST-80C	Space product assurance - Software product assurance
	Def Stan 00-54 (March 1999)	Requirements for Safety Related Electronic Hardware in Defence Equipment" Part No: 1: Requirements: Issue 1
	ESA ISVV Guide	ESA Guide for Independent Software Verification and Validation, Version 2.0, December 29, 2008
	IEEE 610.12-1990 (Jan 1990)	IEEE Standard Glossary of Software Engineering Terminology
	IEEE 754-1985 (Aug 1985)	IEEE Standard for Binary Floating-Point Arithmetic
	ISO/IEC 12207:2008	Systems and software engineering – Software life cycle processes
	NASA Study on Flight Software Complexity (May 2009)	Final Report. NASA Study on Flight Software Complexity. Commissioned by the NASA Office of Chief Engineer. Technical Excellence Program Adam West, Program Manager
	RNC-CNES-E-HB-70-501 (September 2008)	Space engineering monitoring and control specification guide, Version 2, September 16, 2008
	NASA Lessons Learned	http://llis.nasa.gov/llis/search/home.jsp
	NASA System Engineering Handbook	NASA/SP-2007-6105 Rev1 December 2007

EN Reference	Reference in text	Title
	ESA PSS-05-0 Issue 2 (February 1991)	ESA software engineering standards Issue 2
	Flight Computer Initialisation Sequence	Space Avionics Open Interface initiative document: SAVOIR/12-007/FT http://savoir.estec.esa.int

3 Terms, definitions and abbreviated terms

3.1 Terms from other documents

For the purpose of this document, the terms and definitions from ECSS-S-ST-00-01C and ECSS-E-ST-40C apply.

3.2 Terms specific to the present document

3.2.1 software product:

set of computer programs, procedures, documentation and their associated data

3.2.2 acceptance test

test of a system or functional unit usually performed by the customer on his premises after installation, with the participation of the supplier to ensure that the contractual requirements are met

[adapted from ISO/IEC 2382--20:1990]

NOTE ECSS-E-ST-40C relies on ECSS-E-ST-00-01 for the definition of acceptance test and software product (and consequently of its synonyms "software" and "software item"). However, these two terms have disappeared in its last revision C. The definitions of ECSS-E-ST-40B (and therefore ECSS-Q-ST-80B) are restored here.

3.3 Abbreviated terms

For the purpose of this document, the abbreviated terms from ECSS-S-ST-00-01C and ECSS-E-ST-40C apply.

Abbreviation	Meaning
AR	acceptance review NOTE The term SW-AR can be used for clarity to denote ARs that solely involve software products.
CDR	critical design review NOTE The term SW-CDR can be used for clarity to denote CDRs that solely involve software products.
CMMI	capability maturity model integration
COTS	commercial-off-the-shelf

Abbreviation	Meaning
CPU	central processing unit
DDF	design definition file
DDR	detailed design review
DJF	design justification file
DRD	document requirements definition
ECSS	European Cooperation for Space Standardization
eo	expected output
GS	ground segment
HMI	human machine interface
HSIA	hardware-software interaction analysis
HW	hardware
ICD	interface control document
INTRSA	international registration scheme for assessors
IRD	interface requirements document
ISO	International Organization for Standardization
ISV	independent software validation
ISVV	independent software verification and validation
MGT	management file
MF	maintenance file
MOTS	modified off-the-shelf
OBCP	on-board control procedure
OP	operational plan
ORR	operational readiness review
OTS	off-the-shelf
PAF	product assurance file
PDR	preliminary design review NOTE The term SW-PDR can be used for clarity to denote PDRs that solely involve software products.
PRR	preliminary requirement review
QR	qualification review NOTE The term SW-QR can be used for clarity to denote QRs that solely involve software products.
RB	requirements baseline
SCAMPI	standard CMMI appraisal method for process improvement
SDE	software development environment
SOS	software operation support