SLOVENSKI STANDARD
SIST-TP CEN/CLC/TR 17602-80-01:2021

01-december-2021

Zagotavljanje kakovosti proizvodov v vesoljski tehniki - Ponovna uporaba obstoječe programske opreme

Space product assurance - Reuse of existing software

Raumfahrt-Produktsicherung - Wiederverwendung vorhandener Software

Assurance produit des projets spatiaux - Réutilisation de logiciels existants

Ta slovenski standard je istoveten z: **CEN/CLC/TR 17602-80-01:2021**

ICS:

03.120.99	Drugi standardi v zvezi s kakovostjo	Other standards related to quality
35.080	Programska oprema	Software
49.140	Vesoljski sistemi in operacije	Space systems and operations

SIST-TP CEN/CLC/TR 17602-80-01:2021 **en,fr,de**

TECHNICAL REPORT

RAPPORT TECHNIQUE

TECHNISCHER BERICHT

CEN/CLC/TR 17602-80-01

October 2021

ICS 49.140; 35.240.99

English version

Space product assurance - Reuse of existing software

Assurance produit des projets spatiaux - Réutilisation de logiciels

Raumfahrtproduktsicherung - Wiederverwendung existierender Software

This Technical Report was approved by CEN on 13 September 2021. 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/CLC/TR 17602-80-01:2021) 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 16602-80.

This Technical report (CEN/CLC/TR 17602-80-01:2021) originates from ECSS-Q-HB-80-01A .

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

This handbook provides guidance on the approach that can be taken when defining the implementation of activities for the reuse of existing software within a space project.

Existing software is defined in ECSS-Q-ST-80 as follows:

- Any software from previous developments that is used for the project development as is or with adaptation. It also includes software supplied by the customer for use in the project development.
- Any software including any software developed outside the contract to which ECSS software standards are applicable.
- Any software including products such as freeware and open source software products.

In the development of software systems or products, different types of existing software artefacts can be reused, such as:

- Requirements, when reused early in the software product requirements definition.
- Components, when reused early in the software product architecture definition.
- Modules, when reused at detailed design level.
- Libraries and source code, when reused at coding level.
- Documents, plans, tests, and data are other software items that can be reused.

This handbook adopts a broader interpretation of the term ‘existing software’, and assumes that it can comprise the ‘reuse’ of tools for the development of any space software product.

Furthermore, the effective reuse existing software is based on the possibility to fully understand it with respect to properties such as functionality, quality, performance, dependability or safety and to find and adopt it to the development faster than it otherwise can be constructed.

However, whatever is the level of reuse, the quality of the reused existing software is of utmost importance, as low quality can easily lead to system failure and thus loss of mission even for the lowest reuse level. Consequently, significant analyses should be carried out when using existing software. Furthermore, policies that favour reuse of existing software should be adopted with an understanding of the complex impacts of using the already available software.

1 Scope

This handbook provides recommendations, methods and procedures that can be used for the selection and reuse of existing software in space software systems.

This handbook is applicable to all types of software of a space system, including the space segment, the launch service segment and the ground segment software (including EGSEs) whenever existing software is intended to be reused within them.

This handbook covers the following topics:

- Software reuse approach including guidelines to build the Software Reuse File
- Techniques to support completion of existing software qualification to allow its reuse in a particular project
- Tool qualification
- Risk management aspects of reusing existing software

Existing software can be of any type: Purchased (or COTS), Legacy-Software, open-source software, customer-furnished items (CFI's), etc.

NOTE Special emphasis is put on guidance for the reuse of COTS software often available as-is and for which no code and documentation are often available.

Legal and contractual aspects of reuse are in principle out of scope; however guidelines to help in determine the reusability of existing software from a contractual point of view is provided in [ESA/REG/002].

Any organization with the business objective of systematic reuse may need to implement the organizational reuse processes presented in [ISO12207]. These processes will support the identification of reusable software products and components within selected reuse domains, their classification, storage and systematic reuse within the projects of that organization, etc. But these processes are out of scope of this handbook as the handbook is centred on the specific project activities to reuse an existing software product, not part of those organizational reuse processes more oriented to 'design for reuse' processes.

In addition, this handbook provides guidelines to be used for the selection and analysis of tools for the development, verification and validation of the operational software.

2 References

For each document or Standard listed, a *mnemonic* (used to refer to that source throughout this document) is proposed in the left side, and then the *complete reference* is provided in the right one.

EN Reference	Reference in text	Title
EN 16601-00-01	ECSS-S-ST-00-01	ECSS - Glossary of terms
EN 16602-80	ECSS-Q-ST-80	Space product assurance – Software product assurance
EN 16603-40	ECSS-E-ST-40	Space engineering – Software
	BSCC(2004)	ESA software Intellectual Property Rights and Licensing
	DO178B	Software considerations in airborne systems and equipment certification. RTCA DO178B/EUROCAE ED-12B. Radio Technical Commission for Aeronautics/European Organization for Civil Aviation Equipment. 1992.
TR 17602-80-04	ECSS-Q-HB-80-04	Space product assurance - Software metrication programme definition and implementation
TR 17602-80-02	ECSS-Q-HB-80-02	Space product assurance - Software process assessment and improvement
	ESA/REG/002	General clauses and conditions for ESA contracts (clauses 41-43).
	FAA-COTS	DOT/FAA/AR-01/26 COTS avionics Study, May 2001
	FAA-DOT-handbook	DOT/FAA/AR-01/116 Software Service History Handbook. January 2002. FAA.
	FAA-DOT-report	DOT/FAA/AR-01/125 Software Service History report. January 2002. FAA.
	FAA-N8110.91	FAA Notice N 8110.91. Guidelines for the qualification of software tools using RTCA/DO-178B. 16/01/2001
	GSWS	GAL-SPE-GLI-SYST-A/0092. Galileo Software Standard
	IEC 61508	Functional safety: safety-related systems. (Parts 1-7) Ed 2.0. 2010
	IEEE 1517	IEEE Standard for Information Technology - Software Life Cycle Processes-Reuse Processes
	ISO 12207	Systems and software engineering -- Software life cycle

EN Reference	Reference in text	Title
		processes. Edition: 2. 2008. ISO.
	ISO FDIS 26262	Road vehicles -- Functional safety. FDIS Parts 1-10. 2010. ISO.

3 Terms, definitions and abbreviated terms

3.1 Terms from other documents

For the purpose of this document, the terms and definitions from ECSS-S-ST-00-01 and ECSS-Q-ST-80 apply.

3.2 Terms specific to the present document

3.2.1 asset

item that has been designed for use in multiple contexts

[ISO 24765]

NOTE 1 an asset may be such as design, specification, source code, documentation, test suites or manual procedures.

NOTE 2 "asset" is used in this handbook as synonym of "existing software".

3.2.2 domain engineering

reuse-based approach to defining the scope (i.e., domain definition), specifying the structure (i.e., domain architecture), and building the assets for a class of systems, subsystems, or applications

[ISO 24765]

3.2.3 operational software

software product which contributes directly to the mission

[GSWS]

NOTE Contractual aspects are not considered in this definition.

3.2.4 reuse

building a software system at least partly from existing pieces to perform a new application

[ISO 24765]

NOTE Traditionally achieved using program libraries. Object-oriented programming offers reusability of code via its techniques of inheritance and genericity. Class libraries with intelligent browsers and application generators are under development to help in this process. Polymorphic functional languages also supports reusability while retaining the benefits of strong typing.

3.2.5 reuse software

see “existing software” in ECSS-Q-ST-80.

3.3 Abbreviated terms

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

Abbreviation	Meaning
ESA	European Space Agency
FAA	U.S. Federal Aviation Authority
PSH	product service history
SCMP	software configuration management plan
SDP	software development plan
SFMECA	software failure mode effect and criticality analysis
SFTA	software fault tree analysis
SQA	software quality assurance
SRF	software reuse file
SVVP	software verification and validation plan
V&V	verification and validation

4 Overview of the handbook

4.1 Introduction

This clause 4 contains an introduction of the content of this handbook, the intended audience and how to use this handbook.

The organization of this handbook is reflected in detail in Figure 4-1. This handbook is organized in ten main parts:

- Section 1. Scope
- Section 2: References
- Section 3: Terms, definitions and abbreviated terms
- Section 4: Overview of the handbook
- Section 5: Software reuse approach
- Section 6: Tool qualification
- Section 7: Techniques to support qualification when reusing existing software

Annexes include detailed information about:

- Annex A: Content of Software Reuse File (SRF)
- Annex B: Content of the Product Service History file
- Annex C: Risk management considerations

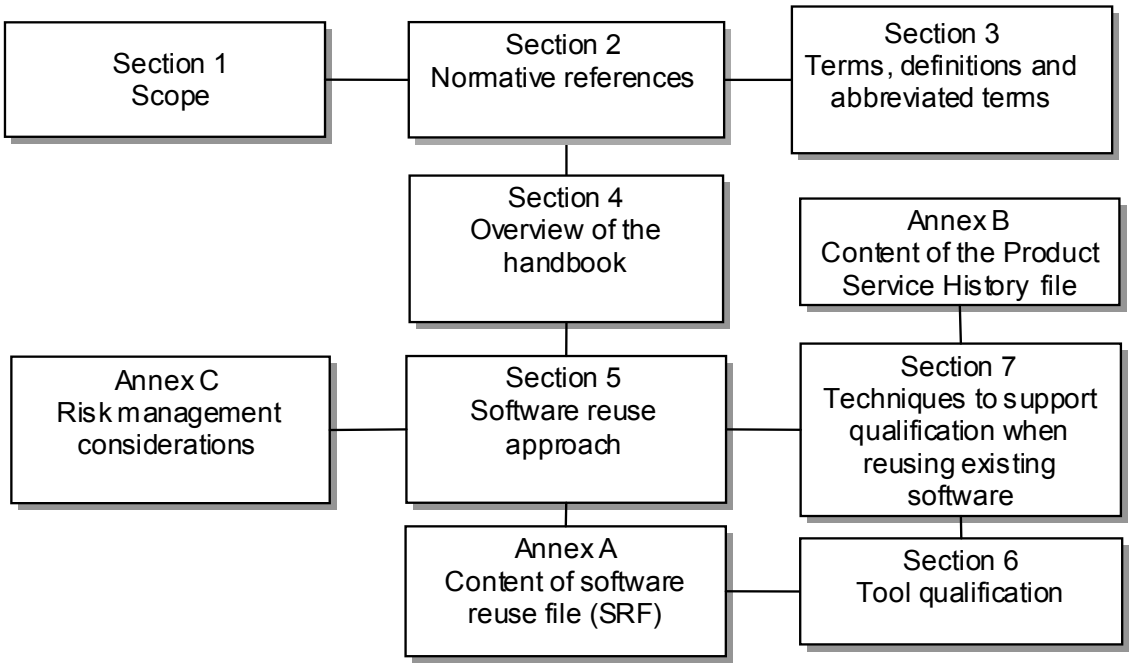

Figure 4-1: Organization of the handbook

4.2 Relation to other ECSS Standards

4.2.1 General

Section 4.2 discusses how this handbook interfaces with other ECSS series, namely the ECSS-Q series of standards (product assurance), ECSS-E series of standards (engineering) and the ECSS-M series of standards (management).

The interface of this handbook to the ECSS-Q branch is via ECSS-Q-ST-80; equally, the interface of this handbook to the ECSS-E branch is ECSS-E-ST-40.

The ECSS-M branch defines the requirements to be applied to the management of space projects. ECSS-E-ST-40 and ECSS-Q-ST-80 describe how the ECSS-M standards apply to the management of software projects. In addition, requirements that cannot be found in the M-branch because they are specific to software product assurance are defined in ECSS-Q-ST-80.

Therefore, this clause contains an analysis of ECSS-E-ST-40 and ECSS-Q-ST-80 requirements related to the reuse of software in space systems.

4.2.2 Software engineering

The interface of this handbook to the ECSS-E branch is via ECSS-E-ST-40; in turn, the interface of ECSS-E-ST-40 to this handbook is via the ECSS-Q-ST-80.

ECSS-E-ST-40 covers all aspects of space software engineering from requirements definition to retirement. It defines the scope of the space software engineering processes, including details of the verification and validation processes, and their interfaces with management and product assurance, which are addressed in the management (-M) and product assurance (-Q) branches of the ECSS system.

ECSS-E-ST-40 contains some specific clauses applicable to projects that intend to reuse software products from other space projects and third-party "commercial off-the-shelf" products to be part of the software product

ECSS-E-ST-40 clauses 5.4.2.1 and 5.4.3.7, respectively, invokes clause 6.2.7 of ECSS-Q-ST-80 for requirements on the use of existing software. Clause 5.4.3.7 of ECSS-E-ST-40 requires the evaluation of the reuse potential of the software to be performed through the identification of the reuse components with respect to the functional requirements baseline.

ECSS-E-ST-40 contains a DRD for the Software Reuse File (SRF) as a constituent of the design justification file (DJF). Its purpose is to document the identification and analysis to be performed on existing software intended to be reused.

This handbook also provides guidance for gaining confidence of the qualification status of any tool used for the development, verification or validation of the space operational software. This handbook will explicitly complement the implementation of ECSS-E-ST-40 tool related clauses, such as: 5.3.2.1 with requirements about development techniques (often supported by the use of tools) and testing environment, 5.3.2.4 containing requirements about supporting tools for automatic code generation, 5.6.2 mentioning validation tools, 5.8.2.1 mentioning verification tools.

4.2.3 Software product assurance

ECSS-Q-ST-80 Standard defines software product assurance requirements for the development of software in space projects in order to provide confidence to the customer and to the suppliers that developed or reused software satisfies the requirements throughout the system lifetime. In particular, ECSS-Q-ST-80 specifies requirements to ensure the software is developed to perform as expected and safely in the operational environment meeting the quality objectives agreed for the project.

Clause 6.2.7 in ECSS-Q-ST-80 contains requirements about reuse of existing software and specifies the term reuse software as it is used in the handbook. This handbook supports the implementation of the requirements contained in ECSS-Q-ST-80 Clause 6.2.7.

Assessing the impact and deriving extra requirements to ensure any deactivated code or configurable code, potentially happening when reusing existing software, do not harm the operational software and system (as required by requirements 6.2.6.5 and 6.2.6.6 of ECSS-Q-ST-80) is also mentioned in this handbook.

This handbook also provides guidance to cope with the selection of suppliers of existing software as required ECSS-Q-ST-80 in Clause 5.4.1.2.

As this handbook also provides guidance for gaining confidence in the qualification status of any tool used for the development, verification or validation of the operational space software, it supports the implementation of clause 5.6 in ECSS-Q-ST-80, about tools and supporting environment detailing development environment requirements.

4.2.4 Project management

The ECSS-M branch defines the requirements to be applied to the management of space projects. ECSS-E-ST-40 and ECSS-Q-ST-80 describe how the ECSS-M series of standards apply to the management of software projects. In addition, requirements that cannot be found in the M-branch because they are specific to software product assurance are defined in ECSS-Q-ST-80.

These management-related processes are directly handled in this handbook through the interfaces to ECSS-E-ST-40 and ECSS-Q-ST-80.