TECHNICAL REPORT

RAPPORT TECHNIQUE

TECHNISCHER BERICHT

CEN/CLC/TR 17602-80-03

October 2021

ICS 49.140; 35.240.99

English version

Space product assurance - Software dependability and safety

Assurance produit des projets spatiaux - Fiabilité et sécurité logiciel

Raumfahrtproduktsicherung - Zuverlässigkeit und Sicherheit von 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-CENELEC Management Centre:
Rue de la Science 23, B-1040 Brussels

Table of contents

Figures

European Foreword

This document (CEN/CLC/TR 17602-80-03:2021) 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 17602-80-03:2021) originates from ECSS-Q-HB-80-03A Rev.1.

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

Dependability and safety are issues of paramount importance in the development and operations of space systems. The contribution of software to system dependability and safety is a key factor, especially in view of the growing complexity of the software used in space critical applications, together with the increasing cost and schedule constraints. Hence, the need for more dependable and safe software has led to the publication of this Handbook, meant to provide guidelines on the implementation of the software dependability and safety requirements defined in ECSS-Q-ST-80C and on the application of some methods and techniques for software dependability and safety.

Analyses and activities aiming at assessing and ensuring the system dependability and safety are carried out since the early stages of the development, and software needs to be properly addressed by these system-level activities. Hardware and software products are classified based on their criticality, in order to focus engineering and product assurance activities on the most critical items. At later stages, the inherent complexity of software calls for application of specific methods and techniques, aiming at refining the software criticality classification and supporting the implementation and verification of measures for critical software handling.

This handbook provides an overall description of the entire software dependability and safety workflow, considering the different activities at system and software level, the lifecycle phases and the customer-supplier relationships, with reference to the dependability and safety requirements defined in ECSS-Q-ST-80C. Some individual software RAMS techniques are also presented. They have been selected from the list of methods and techniques mentioned in different national and international standards and literature, from which a choice has been made based on their relevance to the requirements defined in the ECSS Standards.

1 Scope

This Handbook provides guidance on the application of the dependability and safety requirements relevant to software defined in ECSS-Q-ST-80C.

This Handbook provides support for the selection and application of software dependability and safety methods and techniques that can be used in the development of software-intensive space systems.

This Handbook covers all of the different kinds of software for which ECSS-Q-ST-80C is applicable. Although the overall software dependability and safety workflow description is mainly targeted to the development of spacecraft, the described approach can be adapted to projects of different nature (e.g. launchers, ground systems).

The methods and techniques described in the scope of this Handbook are mainly focused on assessment aspects, though specific development and implementation techniques for dependability and safety (e.g. software failure propagation prevention, defensive programming) are addressed.

2 References

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

EN Reference	Reference in text	Title
EN 16602-30	[ECSS-Q-30]	ECSS-Q-ST-30C – Space product assurance - Dependability
EN 16602-30-02	[ECSS-Q-30-02]	ECSS-Q-ST-30-02C – Space product assurance – Failure modes, effects and criticality analysis (FMECA/FMEA)
EN 16602-30-09	[ECSS-Q-30-09]	ECSS-Q-ST-30-09C – Space product assurance – Availability analysis
EN 16602-40	[ECSS-Q-40]	ECSS-Q-ST-40C – Space product assurance – Safety
EN 16602-40-12	[ECSS-Q-40-12]	ECSS-Q-ST-40-12C – Space product assurance – Fault tree analysis – Adoption notice ECSS/IEC 61025
EN 16602-80	[ECSS-Q-80]	ECSS-Q-ST-80C – Space product assurance – Software product assurance
EN 16602-80-04	[ECSS-Q-80-04]	ECSS-Q-HB-80-04A – Space product assurance – Software metrication programme definition and implementation
EN 17603-40	[ECSS-E-HB-40]	ECSS-E-HB-40A – Space engineering – Software guidelines
EN 16601-00-01	[ECSS-S-ST-00-01]	ECSS-S-ST-00-01C – ECSS – Glossary of terms