SLOVENSKI STANDARD
kSIST-TP FprCEN/TR 17602-30-03:2021

01-oktober-2021

Zagotavljanje kakovosti proizvodov v vesoljski tehniki - Priročnik o človekovi zanesljivosti

Space product assurance - Human dependability handbook

Raumfahrtproduktsicherung - Handbuch zur menschlichen Zuverlässigkeit

Assurance produit des projets spatiaux - Guide sur le facteur humain

Ta slovenski standard je istoveten z: **FprCEN/TR 17602-30-03**

ICS:

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

kSIST-TP FprCEN/TR 17602-30-03:2021 **en,fr,de**

TECHNICAL REPORT

RAPPORT TECHNIQUE

TECHNISCHER BERICHT

FINAL DRAFT
FprCEN/TR 17602-30-03

July 2021

ICS 49.140

English version

Space product assurance - Human dependability handbook

Assurance produit des projets spatiaux - Guide sur le facteur humain

Raumfahrtproduktsicherung - Handbuch zur menschlichen Zuverlässigkeit

This draft Technical Report is submitted to CEN members for Vote. 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.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Warning : This document is not a Technical Report. It is distributed for review and comments. It is subject to change without notice and shall not be referred to as a Technical Report.

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

Table of contents

Figures

Tables

European Foreword

This document (FprCEN/TR 17602-30-03:2021) 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 16602-30.

This Technical report (FprCEN/TR 17602-30-03:2021) originates from ECSS-Q-HB-30-03A.

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).

This document is currently submitted to the CEN CONSULTATION.

Introduction

Space systems always have “human in the loop” such as spacecraft operators in a control centre, test or maintenance staff on a ground or astronauts on board.

Human dependability complements disciplines that concern the interaction of the human element with or within a complex sociotechnical system and its constituents and processes such as human factors engineering (see ECSS-E-ST-10-11C “Human factors engineering” [1]), human systems integration [2], human performance capabilities, human-machine interaction and human-computer interaction in the space domain [3],[4].

Human dependability captures the emerging consensus and nascent effort in the space sector to systematically include the considerations of “human behaviour and performance” in the design, validation and operations of both crewed and un-crewed systems to take benefit of human capabilities and to prevent human errors. Human behaviour and performance can be influenced by various factors, also called precursors (e.g. performance shaping factors), resulting in human errors, or error mitigators, limiting the occurrence or impact of human errors. Human errors can originate from inadequate system design i.e. that ignores or does not properly account for human factor engineering and system operation. Human errors can contribute to or be part of failure or accident scenarios leading to undesirable consequences on a space mission such as loss of mission or as worst case loss of life.

In the space domain, human dependability as a discipline first surfaced during contractor study and policy work in the early 1990s in the product assurance, system safety and knowledge management domain [5],[6] and concerned principles and practices to improve the safety and dependability of space systems by focusing on human error, related design recommendations and root cause analysis [7],[8].

The standards ECSS-Q-ST-30C “Dependability”[9] and ECSS-Q-ST-40C”Safety” [10] define principles and requirements to assess and reduce safety and dependability risks and address aspects of human dependability such as human error failure tolerance and human error analysis to complement FMECA and hazard analysis. The objective of human error analysis is to identify, assess and reduce human errors involved failure scenarios and their consequences. Human error analysis can be implemented through an iterative process, with iterations being determined by the project progress through the different project phases. Human error analysis is not to be seen as the conclusion of an investigation, but rather as a starting point to ensure safety and mission operations success.

The main focus of the handbook is on human dependability associated with humans directly involved in the operations of a space system (“humans” understood here as individual human operator or astronaut or groups of humans i.e. e.g. a crew, a team or an organization including AIT (assembly, integration and test)and launch preparation). This includes and concerns especially the activities related to the planning and implementation of space system control and mission operations from launch to disposal, and can be extended to cover operations such as AIT and launch preparation.

References

[1] ECSS-E-ST-10-11C - Space engineering - Human factors engineering, 31 July 2008 (*Number of EN version: EN 16603-10-11*)

[2] Booher, Harold R. (Ed.) (2003) Handbook of Human Systems Integration. New York: Wiley.

[3] NASA (2010) Human Integration Design Handbook NASA/SP-2010-3407 (Baseline). Washington, D.C.: NASA.

[4] NASA (2011) Space Flight Human-System Standard Vol. 2: Human Factors, Habitability, and Environmental Health NASA-STD-3001,Vol. 2. Washington, D.C.: NASA.

[5] Atkins, R. K. (1990) Human Dependability Requirements, Scope and Implementation at the European Space Agency. Proceedings of the Annual Reliability and Maintainability Symposium, IEEE, pp. 85-89.

[6] Meaker, T. A. (1992) Future role of ESA R&M assurance in space flight operation. Proceedings of the Annual Reliability and Maintainability Symposium, IEEE, pp. 241-242.

[7] Alenia Spazio (1994) Human Dependability Tools, Techniques and Guidelines: Human Error Avoidance Design Guidelines and Root Cause Analysis Method (SD-TUN-AI-351, -353, -351). Noordwijk: ESTEC.

[8] Cojazzi, G. (1993) Root Cause Analysis Methodologies: Selection Criteria and Preliminary Evaluation, ISEI/IE/2443/93, JRC Ispra, Italy: Institute for System Engineering and Informatics.

[9] ECSS-Q-ST-30 – Space product assurance - Dependability, 6 March 2009 (*Number of EN version: EN 16602-30*)

[10] ECSS-Q-ST-40 – Space product assurance - Safety, 6 March 2009 (*Number of EN version: EN 16602-40*)

1 Scope and objectives

1.1 Scope

The handbook defines the principles and processes of human dependability as integral part of system safety and dependability. The handbook focuses on human behaviour and performance during the different operation situations as for example in a control centre such as handover to routine mission operation, routine mission operation, satellite maintenance or emergency operations.

This handbook illustrates the implementation of human dependability in the system life cycle, where during any project phase there exists the need to systematically include considerations of the:

- Human element as part of the space system,
- Impact of human behaviour and performance on safety and dependability.

Within this scope, the main application areas of the handbook are to support the:

a. Development and validation of space system design during the different project phases,

b. Development, preparation and implementation of space system operations including their support such as the organisation, rules, training etc.

c. Collection of human error data and investigation of incidents or accidents involving human error.

The handbook does not address:

- Design errors: The handbook intends to support design (and therefore in this sense, addresses design errors) regarding the avoidance or mitigation of human errors during operations. However, human error during design development are not considered.
- Quantitative (e.g. probabilistic) analysis of human behaviour and performance: The handbook does not address probabilistic assessment of human errors as input to system level safety and dependability analysis and consideration of probabilistic targets, and
- Intentional malicious acts and security related issues: Dependability and safety deals with "threats to safety and mission success" in terms of failures and human non malicious errors and for the sake of completeness includes "threats to safety and mission success" in terms of malicious actions, which are addressed through security risk analysis. However by definition "human dependability" as presented in this handbook excludes the consideration of "malicious actions" and security related issues i.e. considers only "non-malicious actions" of humans.

The handbook does not directly provide information on some disciplines or subjects, which only indirectly i.e. at the level of PSFs (see section 5) interface with "human dependability". Therefore the handbook does not provide direct support to "goals" such as:

- optimize information flux in control room during simulations and critical operations,
- manage cultural differences in a team,
- cope with negative group dynamics,

- present best practices and guidelines about team training needs and training methods,
- provide guidelines and best practices concerning planning of shifts,
- present basic theory about team motivation, and
- manage conflict of interests on a project.

1.2 Objectives

The objectives of the handbook are to support:

- Familiarization with human dependability (see section 5 "principles of human dependability"). For details and further reading see listed "references" at the end of each section of the handbook.
- Application of human dependability; (see section 6 "human dependability processes" and 7 "implementation of human dependability in system life cycle").

2 References

Due to the structure of the document, each section includes at its end the references called in it.

The Bibliography at the end of this document contains a list of recommended literature.

3 Terms, definitions and abbreviated terms

3.1 Terms from other standards

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

b. For the purpose of this document, the terms and definitions from ECSS-Q-ST-40 apply, in particular the following term:

1. operator error

3.2 Terms specific to the present handbook

3.2.1 automation

design and execution of functions by the technical system that can include functions resulting from the delegation of user's tasks to the system

3.2.2 error mitigator

set of conditions and circumstances that influences in a positive way human performance and the occurrence of a human error

NOTE The conditions and circumstances are best described by the **performance shaping factors** and levels of human performance.

3.2.3 error precursor

set of conditions and circumstances that influences in a negative way human performance and the occurrence of a human error

3.2.4 human dependability

performance of the human constituent element and its influencing factors on system safety, reliability, availability and maintainability

3.2.5 human error

inappropriate or undesirable observable human behaviour with potential impact on safety, dependability or system performance

NOTE Human behaviour can be decomposed into perception, analysis, decision and action.

3.2.6 human error analysis

systematic and documented process of identification and assessment of human errors, and analysis activities supporting the reduction of human errors

3.2.7 human error reduction

elimination, or minimisation and control of existing or potential conditions for human errors

NOTE The conditions and circumstances are best described by the **performance shaping factors** and levels of human performance.

3.2.8 human error type

classification of human errors into slips, lapses or mistakes

NOTE The types of human error are described in section 6.2 on the human dependability concept.

3.2.9 level of human performance

categories of human performances resulting from human cognitive, perceptive or motor behaviour in a given situation

NOTE 1 As an example, categories of human performances can be "skill based", "rule based" and "knowledge based".

NOTE 2 The level of human performance results from the combination of the circumstances and current situation (e.g. routine situation, trained situation, novel situation) and the type of control of the human action (e.g. consciously or automatically).

3.2.10 operator-centred design

approach to human-machine system design and development that focuses, beyond the other technical aims, on making systems usable

3.2.11 performance shaping factor

specific error precursor or error mitigator that influences human performance and the likelihood of occurrence of a human error.

NOTE 1 Performance shaping factors are either error precursors or error mitigators appearing in a failure scenario and enhance or degrade human performance.

NOTE 2 Different performances shaping factors are listed in section 5 of this document.

3.2.12 resilience

ability to anticipate and adapt to the potential for “surprise and error” in complex sociotechnical systems

NOTE Resilience engineering provides a framework for understanding and addressing the context of failures i.e. as a symptom of more in-depth structural problems of a system.

3.2.13 socio-technical system

holistic view of the system including the operators, the organization in which the operator is involved and the technical system operated.

NOTE A socio-technical system is the whole structure including administration, politics, economy and cultural ingredients of an organisation or a project.

3.3 Abbreviated terms

For the purpose of this document, the following abbreviated terms apply:

Abbreviation	Meaning
AIT	assembly, integration and testing
FDIR	failure detection, isolation and recovery
FMEA	failure mode effect analysis
FMECA	failure mode effect and criticality analysis
HET	human error type
HFACS	Human Factors Analysis and Classification System
HMI	human-machine interface
HUDEP	human dependability
LHP	level of human performance
O&M	organizational and management
PIF	performance influencing factors
PSF	performance shaping factor
RAMS	reliability, availability, maintainability and safety
SRK	skill, rule, knowledge
VACP	visual, auditory, cognitive and psychomotor