PD CEN/TR 17602-30-03:2021

BSI Standards Publication

Space product assurance — Human dependability handbook

bsi.

National foreword

This Published Document is the UK implementation of CEN/TR 17602-30-03:2021.

The UK participation in its preparation was entrusted to Technical Committee ACE/68, Space systems and operations.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

Published by BSI Standards Limited 2022

ISBN 978 0 539 17711

ICS 49.140

Compliance with a British Standard cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 31 May 2022.

Amendments/corrigenda issued since publication

Date	Text affected

TECHNICAL REPORT

RAPPORT TECHNIQUE

TECHNISCHER BERICHT

CEN/TR 17602-30-03

December 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 Technical Report was approved by CEN on 22 November 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

Ref. No. CEN/TR 17602-30-03:2021 E

Table of contents

European Foreword **5**

Introduction **6**

References 6

1 Scope and objectives **8**

1.1 Scope 8

1.2 Objectives 9

2 References **10**

3 Terms, definitions and abbreviated terms **11**

3.1 Terms from other standards 11

3.2 Terms specific to the present handbook 11

3.3 Abbreviated terms 13

4 Objectives of human dependability **14**

5 Principles of human dependability **15**

5.1 Human dependability concept 15

5.1.1 Introduction 15

5.1.2 Failure scenario integrating human errors 16

5.1.3 Human error and error type 16

5.1.4 Error precursors and error mitigators 16

5.2 Human role in the system 24

5.2.1 Overview 24

5.2.2 Human contribution to safety and mission success 24

5.2.3 Fundamental principles driving function allocation 25

5.2.4 Some principles driving user interfaces design 26

5.2.5 Automated processes and operator tasks in space systems 28

5.3 References 29

6 Human dependability processes **31**

6.1 General 31

6.2 Human error analysis 32

6.2.1 Objectives of human error analysis 32

6.2.2 Principles of human error analysis 33

6.2.3 Human error analysis process 37
6.3 Human error reporting and investigation 41
6.3.1 Objectives of human error reporting and investigation 41
6.3.2 Principles of human error reporting and investigation 41
6.3.3 Human error reporting and investigation process 43
6.4 References 45

7 Implementation of human dependability in system life cycle 46
7.1 General 46
7.2 Human dependability activities in project phases 47
7.2.1 Overview 47
7.2.2 Phase A: Feasibility 47
7.2.3 Phase B: Preliminary Definition 48
7.2.4 Phase C: Detailed Definition 49
7.2.5 Phase D: Qualification and Production 50
7.2.6 Phases: E Operations/Utilization and F Disposal 52
7.3 References 53

Annex A (informative) Human error analysis data - examples 54
A.1 Overview 54
A.2 Examples of the Evolution of PSFs 55
A.3 Examples of Human Error Scenario Data 58
A.4 References 58

Annex B (informative) Human error analysis documentation 59

Annex C (informative) Human error analysis example questions 61
C.1 Examples of questions to support a risk analysis on anomalies and human error during operations 61
C.2 References 63

Annex D (informative) Human dependability in various domains 64
D.1 Human dependability in industrial sectors 64
D.2 References 66

Bibliography 68

Figures

Figure 5-1: Examples of human error in failure scenarios 16
Figure 5-2: Error precursors, error mitigators and human error in failure scenarios 17
Figure 5-3: HFACS model 20

Figure 5-4: Levels of human performance 21
Figure 5-5: Basic error types 23
Figure 5-6: MABA-MABA principle 25
Figure 5-7: Small portion of Chernobyl nuclear power plant control room (from http://www.upandatom.net/Chernobyl.htm).....26
Figure 5-8: Example of a computer-based, concentrated control room (Large Hadron Collider at CERN).....27
Figure 5-9. Example of a computer-based, concentrated user interface – the glass cockpit (transition to glass cockpit for the Boeing 747) 27
Figure 6-1: Human error reduction examples 33
Figure 6-2: Human error analysis and reduction process.....37
Figure 6-3: Human error analysis iteration.....41
Figure 6-4: Human error reporting and investigation process 44
Figure 7-1: Human dependability in system life cycle 46

Tables

Table A-1 : SPAR_H PSF modelling considerations for MIDAS [57].....55
Table B-1 : Example of an “Human Error Analysis Form sheet 60
Table D-1 : Examples of Comparable External Domains 65

European Foreword

This document (CEN/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 (CEN/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).

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,