

DIN EN 16602-40-02

ICS 49.140

Ersatz für
DIN EN 14738:2004-08**Raumfahrtproduktsicherung –
Gefahrenanalyse;
Englische Fassung EN 16602-40-02:2014**

Space product assurance –
Hazard analysis;
English version EN 16602-40-02:2014

Assurance produit des projets spatiaux –
Analyse de risques;
Version anglaise EN 16602-40-02:2014

Gesamtumfang 41 Seiten

DIN-Normenausschuss Luft- und Raumfahrt (NL)

Nationales Vorwort

Dieses Dokument (EN 16602-40-02:2014) wurde vom Technischen Komitee CEN/CLC/TC 5 „Raumfahrt“ erarbeitet, dessen Sekretariat vom DIN (Deutschland) gehalten wird.

Das zuständige deutsche Normungsgremium ist der Arbeitsausschuss NA 131-10-01 AA „Interoperabilität von Informations-, Kommunikations- und Navigationssystemen“ im DIN-Normenausschuss Luft- und Raumfahrt (NL).

Dieses Dokument ersetzt DIN EN 14738:2004-08.

Dieses Dokument (EN 16602-40-02:2014) basiert auf ECSS-Q-ST-40-02C.

Dieses Dokument enthält unter Berücksichtigung des DIN-Präsidialbeschlusses 1/2004 nur die englische Originalfassung von EN 16602-40-02:2014.

Dieses Dokument wurde speziell zur Behandlung von Raumfahrtsystemen erarbeitet und hat daher Vorrang vor jeglicher Europäischer Norm, da es denselben Anwendungsbereich hat, jedoch über einen größeren Geltungsbereich (z. B. Luft- und Raumfahrt) verfügt.

Änderungen

Gegenüber wird DIN EN 14738:2004-08 wurden folgende Änderungen vorgenommen:

- a) Norm-Nummer geändert;
- b) keinerlei Änderungen des Textes.

Frühere Ausgaben

DIN EN 14738: 2004-08

Nationaler Anhang NA (informativ)

Begriffe

3 Begriffe und Abkürzungen

3.1 Begriffe aus anderen Normen

Für die Anwendung dieses Dokuments gelten die Begriffe und Definitionen nach ECSS-S-ST-00-01 und besonders für den folgenden Begriff:

Anforderung

3.2 Für diese Norm spezifische Begriffe

3.2.1

Konsequenzenbaum

Vielzahl von Gefahrenszenarios, die zur gleichen Konsequenz (Unfallart) führen

3.2.2

Nachweisdauer

Zeitspanne zwischen dem Eintritt des Initialereignisses und dem Nachweis durch die sichtbaren Anzeichen

3.2.3

Gefahr

Gefährdung

tatsächlicher oder potentieller Zustand eines Bauteils, der zu einem Unfall führen kann

ANMERKUNG 1 [ISO 14620-2]

ANMERKUNG 2 Dieser Zustand kann mit dem Design, der Fertigung, dem Betrieb oder der Umgebung des Bauteils zusammenhängen und birgt ein Unfallpotential. [ISO 14620-2]

ANMERKUNG 3 Gefahren sind potentielle Bedrohungen für die Sicherheit eines Systems. Sie sind keine Ereignisse, aber die Voraussetzungen für den Eintritt von Gefahrenszenarios mit deren negativen Auswirkungen auf die Sicherheit in Bezug auf die sicherheitsrelevanten Konsequenzen.

3.2.4

Gefahrenakzeptanz

Entscheidung, die Konsequenzen der Gefahrenszenarios zu tolerieren, wenn sie eintreten

3.2.5

Gefahrenanalyse

systematischer und iterativer Prozess der Identifizierung, Klassifizierung und Reduzierung von Gefahren

3.2.6

Gefahrenabwehr

mit einem Gefahrenszenario verbundene präventive oder mildernde Maßnahme, die beim Design und beim Betrieb des Systems implementiert wird, um die Ereignisse zu verhindern oder um deren Ausweitung zu einer Konsequenz zu unterbrechen

3.2.7

Gefahrenbeseitigung

Entfernen einer Gefahr bei Sichtbarwerdung einer speziellen Gefahr

3.2.8

Sichtbarwerdung der Gefahr

Vorhandensein spezieller Gefahren beim technischen Design, bei Betrieb und in der Umgebung eines Systems

3.2.9

Gefahrenminimierung

Substitution einer Gefahr bei Sichtbarwerdung der Gefahr durch eine andere Gefahr der gleichen Art, aber mit einer niedrigeren potentiellen Bedrohung

ANMERKUNG Zum Beispiel Substitution einer hohen Toxizität durch eine niedrige Toxizität.

3.2.10

Gefahrenreduzierung

Prozess der Eliminierung oder Minimierung und Abwehr von Gefahren

3.2.11

Gefahrenszenario

Abfolge von Ereignissen, die vom ersten Auslöser bis zur unerwünschten sicherheitsrelevanten Konsequenz führen

ANMERKUNG Der Auslöser kann ein einzelnes Initialereignis, eine zusätzliche Aktivität oder die Änderung einer Bedingung sein, die ein verborgenes Problem aktivieren.

3.2.12

Gefahrenbaum

Vielzahl von Gefahrenszenarios, die aus der gleichen Gruppe sichtbarer Gefahren stammen

3.2.13

gefährlich

Eigenschaft eines Bauteils und der Bauteilumgebung, die ein Unfallpotential birgt

ANMERKUNG [ISO 14620-2]

3.2.14

sichtbare Anzeichen

Anhaltspunkte, die darauf hinweisen, dass ein unerwünschtes Ereignis eingetreten ist

ANMERKUNG Sichtbare Anzeichen treten während der Ausbreitungsdauer auf.

3.2.15

Reaktionsdauer

Zeitspanne zwischen dem Erkennen und dem Eintritt der Konsequenz

ANMERKUNG Das ist die Zeitspanne, die für risikomindernde Maßnahmen nach dem Erkennen des Eintritts des Initialereignisses zur Verfügung steht.

3.2.16

Restgefahr

Gefahr, die nach der Implementierung der Gefahrenreduzierung bestehen bleibt

3.2.17

beseitigte Gefahr

Gefahr, die reduziert ist, bei der die Reduzierung verifiziert und die Gefahr als akzeptabel angesehen wird

ANMERKUNG Beseitigte Gefahren werden zur formellen Annahme vorgelegt.

3.2.18**Ausbreitungsdauer des Szenarios**

Zeitspanne zwischen dem Eintritt des Initialereignisses und dem Eintritt der Konsequenz

3.2.19**Schwere der sicherheitsrelevanten Konsequenz**

Maß für die Schwere des Schadens in Bezug auf die Sicherheit

3.3 Abkürzungen

Für die Anwendung dieser Norm gelten die Abkürzungen nach ECSS-S-ST-00-01 und die folgenden Abkürzungen.

Abkürzung	Bedeutung	
CC&M	Analyse von Ausfällen aufgrund gemeinsamer Ursache	(en: common cause and common failure mode analysis)
DRD	Dokumenten-Anforderungsdefinition	(en: document requirements definition)
FMECA	Fehlerart-, auswirkungs- und -kritizitätsanalyse	(en: failure modes, effects and criticality analysis)
GSE	Bodendienstgerät	(en: ground support equipment)
NASA	Nationale Luft- und Raumfahrtbehörde	(en: National Aeronautics and Space Administration)
OHA	Betriebliche Gefahrenanalyse	(en: operating hazard analysis)
PHA	Vorläufige Gefahrenanalyse	(en: preliminary hazard analysis)
SHA	Systembezogene Gefahrenanalyse	(en: system hazard analysis)
SSHA	Subsystembezogene Gefahrenanalyse	(en: subsystem hazard analysis)

— Leerseite —

English version

Space product assurance - Hazard analysis

Assurance produit des projets spatiaux - Analyse de
risques

Raumfahrtproduktsicherung - Gefahrenanalyse

This European Standard was approved by CEN on 13 March 2014.

CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN and CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

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



**CEN-CENELEC Management Centre:
Avenue Marnix 17, B-1000 Brussels**

Table of contents

Foreword	4
Introduction.....	5
1 Scope.....	6
2 Normative references	7
3 Terms, definitions and abbreviated terms.....	8
3.1 Terms from other standards.....	8
3.2 Terms specific to the present standard	8
3.3 Abbreviated terms.....	10
4 Principles of hazard analysis	11
4.1 Hazard analysis concept.....	11
4.2 Role of hazard analysis	14
4.3 Hazard analysis process.....	14
4.3.1 Overview	14
4.3.2 Overview of the hazard analysis process	15
4.4 Hazard analysis implementation	17
4.4.1 Overview	17
4.4.2 General considerations	17
4.4.3 Type of project considerations	17
4.4.4 Documentation of hazard analysis	17
4.5 Hazard analysis documentation	18
4.6 Integration of hazard analysis activities.....	18
4.7 Objectives of hazard analysis	18
5 Requirements.....	20
5.1 Hazard analysis requirements	20
5.2 Hazard analysis steps and tasks.....	20
5.2.1 Step 1: Define hazard analysis implementation requirements	20
5.2.2 Step 2: Identify and assess the hazards.....	22
5.2.3 Step 3: Decide and act.....	25
5.2.4 Step 4: Track, communicate and accept the hazards	27

Annex A (informative) Examples of generic hazards	28
Annex B (informative) Hazard and safety risk register (example) and ranked hazard and safety risk log (example)	30
Annex C (informative) Background information	33
C.1 Preliminary hazard analysis (PHA)	33
C.2 Subsystem hazard analysis (SSHA)	33
C.3 System hazard analysis (SHA)	34
C.4 Operating hazard analysis (OHA)	34
Bibliography.....	35

Figures

Figure 4-1: Hazards and hazard scenarios	12
Figure 4-2: Example of a hazard tree	12
Figure 4-3: Example of a consequence tree	12
Figure 4-4: Reduction of hazards	13
Figure 4-5: Interface to FMECA and CC&M analysis	13
Figure 4-6: The process of hazard analysis	15
Figure 4-7: The steps and cycles in the hazard analysis process	16
Figure 4-8: The nine tasks associated with the four steps of the hazard analysis process	16
Figure B-1 : Example of a hazard and safety risk register (see also ECSS-M-ST-80).....	31
Figure B-2 : Example of a ranked hazard and safety risk log	32

Tables

Table 5-1: Example of a safety consequence severity categorization	21
Table 5-2: Example of a hazard matrix	23
Table 5-3: Example of a hazard manifestation list	23
Table 5-4: Example of a hazard scenario list	25

Foreword

This document (EN 16602-40-02:2014) has been prepared by Technical Committee CEN/CLC/TC 5 "Space", the secretariat of which is held by DIN.

This standard (EN 16602-40-02:2014) originates from ECSS-Q-ST-40-02C.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by March 2015, and conflicting national standards shall be withdrawn at the latest by March 2015.

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 supersedes EN 14738:2004.

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 EN covering the same scope but with a wider domain of applicability (e.g. : aerospace).

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Introduction

Safety analysis comprises hazard analysis, safety risk assessment and supporting analyses as defined in ECSS-Q-ST-40. The objective of safety analysis is to identify, assess, reduce, accept, and control safety hazards and the associated safety risks in a systematic, proactive, complete and cost effective manner, taking into account the project's technical and programmatic constraints. Safety analysis can be implemented through an iterative process, with iterations being determined by the project progress through the different project phases, and by changes to a given project baseline.

Hazard analysis comprises the identification classification and reduction of hazards. Hazard analysis can be implemented at each level of the customer-supplier network. Hazard analysis activities at lower level can contribute to system level safety analysis. System level safety analysis can determine lower level hazard analysis activities.

Hazard analysis interfaces with dependability analysis, in particular FMECA. Safety risk assessment interfaces with quantitative dependability analysis, in particular reliability analysis. Safety risk assessment contributes to project risk management. Ranking of safety risks according to their criticality for project success, allowing management to direct its attention to the essential safety issues, is part of the major objectives of risk management.

Safety risk assessment is further addressed in ECSS-Q-ST-40.

1

Scope

This Standard details the hazard analysis requirements of ECSS-Q-ST-40; it defines the principles, process, implementation, and requirements of hazard analysis.

It is applicable to all European space projects where during any project phase there exists the potential for hazards to personnel or the general public, space flight systems, ground support equipment, facilities, public or private property or the environment.

This standard may be tailored for the specific characteristics and constraints of a space project in conformance with ECSS-S-ST-00.

2

Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this ECSS Standard. For dated references, subsequent amendments to, or revision of any of these publications do not apply. However, parties to agreements based on this ECSS Standard are encouraged to investigate the possibility of applying the more recent editions of the normative documents indicated below. For undated references, the latest edition of the publication referred to applies.

EN reference	Reference in text	Title
EN 16001-00-01	ECSS-S-ST-00-01	ECSS system — Glossary of terms
EN 16601-80	ECSS-M-ST-80	Space project management — Risk management
EN 16602-40	ECSS-Q-ST-40	Space product assurance — Safety