

DIN EN 14738



ICS 49.140

**Raumfahrtproduktsicherung –
Gefahrenanalyse;
Deutsche Fassung EN 14738:2004**

Space product assurance –
Hazard analysis;
German version EN 14738:2004

Assurance produit des projets spatiaux –
Analyse des dangers;
Version allemande EN 14738:2004

Gesamtumfang 34 Seiten

Normenausschuss Luft- und Raumfahrt (NL) im DIN

Die Europäische Norm EN 14738:2004 hat den Status einer Deutschen Norm.

Nationales Vorwort

Die *European Cooperation for Space Standardization (ECSS)*, eine Einrichtung zur Erstellung eines kohärenten, einheitlichen Normenwerkes zur Anwendung in allen europäischen Raumfahrtprojekten, hat am 1996-11-13 vom *Europäischen Komitee für Normung (CEN)* das Mandat (M/237) erhalten, für den CEN-Subsector T02 „Aerospace“ Europäische Normen (EN) auszuarbeiten.

Aufgrund der zwischen ISO/TC 20/SC 14 „Raumfahrt“ und ECSS vereinbarten A-Liaison werden die Normungsprogramme dieser Partner abgestimmt und die Abstimmungsregeln gemäß Abschnitt 5.2 der Wiener-Vereinbarung angewendet.

Die vorliegende Norm EN 14738:2004 wurde von CEN/CS T02 auf Basis der ECSS-Q-40-02 erarbeitet und in das einstufige Annahmeverfahren gegeben.

Deutsche Fassung

Raumfahrtproduktsicherung — Gefahrenanalyse

Space product assurance —
Hazard analysis

Assurance produit des projets spatiaux —
Analyse des dangers

Diese Europäische Norm wurde vom CEN am 2. Februar 2004 angenommen.

Die CEN-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist. Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim Management-Zentrum oder bei jedem CEN-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CEN-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem Management-Zentrum mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CEN-Mitglieder sind die nationalen Normungsinstitute von Belgien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, Schweden, der Schweiz, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, Ungarn, dem Vereinigten Königreich und Zypern.



EUROPÄISCHES KOMITEE FÜR NORMUNG
EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION

Management-Zentrum: rue de Stassart, 36 B-1050 Brüssel

Inhalt

	Seite
Vorwort	3
1 Anwendungsbereich	5
2 Normative Verweisungen	5
3 Begriffe und Abkürzungen	5
4 Prinzipien der Gefahrenanalyse	8
5 Zielsetzung der Gefahrenanalyse	12
6 Anforderungen an die Gefahrenanalyse und Durchführung	12
7 Durchführung der Gefahrenanalyse	21
Anhang A (informativ) Beispiele für allgemeine Gefahren	22
Anhang B (normativ) Gefahrenbericht — Definition der Anforderungen an Dokumente (DRD)	24
Anhang C (informativ) Hintergrundinformationen	30
Literaturhinweise	32

Vorwort

Dieses Dokument (EN 14738:2004) wurde von CEN/CS erstellt.

Diese Europäische Norm muss bis spätestens September 2004 entweder durch Veröffentlichung einer gleichlautenden Fassung oder durch Einführung den Status einer nationalen Norm erhalten; entgegenstehende nationale Normen müssen bis spätestens September 2004 zurückgezogen werden.

Diese Norm basiert auf einer früheren Version¹⁾, die von der ECSS-Arbeitsgruppe für Anpassung erstellt, vom Technischen Ausschuss geprüft und vom ECSS-Lenkungsgremium verabschiedet wurde. ECSS (European Cooperation for Space Standardization) ist ein Gremium, in dem die Europäische Raumfahrtagentur ESA, nationale Raumfahrtagenturen sowie europäische Industrieverbände mit dem Ziel zusammenarbeiten, einheitliche Normen zu erstellen und zu pflegen.

Diese Europäische Norm gehört zu einer Reihe von ECSS-Normen, die sich auf das Management, die Technik (Engineering) und die Produktsicherung bei Projekten und Anwendungen der Raumfahrt beziehen.

Diese Europäische Norm legt Anforderungen in Form von Zielen fest, und nicht in Bezug auf die Organisation und Durchführung der erforderlichen Arbeiten. Dies ermöglicht es, bewährte Organisationsstrukturen und -verfahren beizubehalten und erlaubt gleichzeitig deren Weiterentwicklung, ohne dass die Normen überarbeitet werden müssen.

Bei der Erarbeitung dieser Europäischen Norm wurde die Normenreihe EN ISO 9000 berücksichtigt.

Die Anhänge A und C dienen zur Information. Der Anhang B hat normativen Charakter.

In Übereinstimmung mit der CEN/CENELEC-Geschäftsordnung sind folgende Staaten verpflichtet, diese Europäische Norm anzuwenden: Belgien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Schweden, Schweiz, Slowakei, Slowenien, Spanien, Tschechische Republik, Ungarn, Vereinigtes Königreich und Zypern.

1) ECSS-Q-40-02A

Einleitung

Zur Sicherheitsanalyse gehören die Gefahrenanalyse, die Sicherheitsrisikobewertung und Supportanalysen, die in EN ISO 14620-1 definiert sind. Die Sicherheitsanalyse hat den Zweck, im Rahmen des Gesamtrisikomanagements Gefahren für die Sicherheit und die damit verbundenen Sicherheitsrisiken auf systematische, proaktive, vollständige und kosteneffiziente Weise aufzuzeigen, zu bewerten, zu verringern und zu akzeptieren. Die Sicherheitsanalyse kann als Schrittprozess durchgeführt werden, wobei die einzelnen Schritte durch den Projektfortschritt in den einzelnen Phasen und durch Änderungen gegenüber einer vorgegebenen Projektbasis festgelegt werden.

Die Gefahrenanalyse umfasst die Identifikation, die Klassifizierung und die Verringerung von Gefahren. Die Gefahrenanalyse kann auf jeder Ebene des Kunden-Lieferanten-Netzwerks implementiert werden. Die Aktivitäten der Gefahrenanalyse auf unterer Ebene können zur Sicherheitsanalyse auf Systemebene beitragen. Die Sicherheitsanalyse auf Systemebene kann wiederum Aktivitäten der Gefahrenanalyse auf unterer Ebene auslösen.

Die Gefahrenanalyse hat eine Schnittstelle zur Zuverlässigkeitsanalyse, insbesondere FMECA. Die Gefahrenanalyse legt auch die Grundlage für die Sicherheitsrisikobewertung fest.

1 Anwendungsbereich

Diese Europäische Norm legt Anforderungen an die Gefahrenanalyse von EN ISO 14620-1:2002 6.4.2 fest; sie enthält Vorgaben für die Prinzipien, den Prozess, die Umsetzung und die Anforderungen an die Gefahrenanalyse.

Sie kommt bei europäischen Raumfahrtprojekten zur Anwendung, bei denen in sämtlichen Projektphasen ein Gefahrenpotential für Mitarbeiter, Öffentlichkeit, Raumfahrtflugsysteme, Bodensupportgeräte, Strukturen, öffentliches oder privates Eigentum oder die Umwelt besteht.

2 Normative Verweisungen

Diese Europäische Norm enthält durch datierte oder undatierte Verweisungen Festlegungen aus anderen Publikationen. Diese normativen Verweisungen sind an den jeweiligen Stellen im Text zitiert, und die Publikationen sind nachstehend aufgeführt. Bei datierten Verweisungen gehören spätere Änderungen oder Überarbeitungen dieser Publikationen nur zu dieser Europäischen Norm, falls sie durch Änderung oder Überarbeitung eingearbeitet sind. Bei undatierten Verweisungen gilt die letzte Ausgabe der in Bezug genommenen Publikation (einschließlich Änderungen).

EN 13290-5:2001, *Raumfahrt-Projektmanagement — Allgemeine Anforderungen — Teil 5: Konfigurationsmanagement*.

EN 13701:2001, *Raumfahrtsysteme — Glossar*.

EN ISO 14620-1:2002, *Raumfahrttechnik — Sicherheitsanforderungen — Teil 1: Sicherheitssystem (ISO 14620-1:2002)*.

EN ISO 17666:2003, *Raumfahrtsysteme — Risikomanagement (ISO 17666:2003)*.

3 Begriffe und Abkürzungen

3.1 Begriffe

Für die Anwendung dieser Europäischen Norm gelten die in EN 13701:2001 verwendeten Begriffe mit den folgenden Definitionen:

3.1.1

Folgenbaum

Gruppe von Gefahrenszenarien, welche zu derselben Sicherheitsfolge führen

3.1.2

Feststellungszeit

Zeitraum zwischen dem Eintreten des auslösenden Ereignisses und seiner Feststellung der wahrnehmbaren Symptome

3.1.3

Gefahr

tatsächlicher oder möglicher Zustand eines Objekts, der zu einem Störfall führen kann [ISO 14620-2:2000]

ANMERKUNG 1 Dieser Zustand kann mit dem Design, der Fertigung, dem Betrieb oder der Umgebung der betreffenden Komponente zusammenhängen und kann möglicherweise Störfälle hervorrufen. [ISO 14620-2:2000]

ANMERKUNG 2 Gefahren sind potentielle Bedrohungen für die Sicherheit eines Systems. Sie sind keine Ereignisse, sondern die Voraussetzung für das Eintreten von Gefahrenszenarien, welche sich negativ auf die Sicherheit und die Sicherheitsfolgen auswirken.

3.1.4

Akzeptieren einer Gefahr

Entscheidung, die Folgen von Gefahrenszenarien zu akzeptieren, wenn diese eintreten

3.1.5

Gefahrenanalyse

systematischer und schrittweiser Prozess der Identifikation, Klassifizierung und Verringerung von Gefahren

3.1.6

Gefahrenkontrolle

Präventiv- oder Abschwächungsmaßnahme im Falle eines Gefahrenszenarios, welche in das Systemdesign und den Systembetrieb eingebracht wird, um die Gefahrenereignisse zu vermeiden oder ihre Entwicklung hin zu einer Folge zu unterbrechen

3.1.7

Gefahrenbeseitigung

Beseitigung einer Gefahr aus einer besonderen Gefahrenmanifestation

3.1.8

Gefahrenmanifestation

Vorhandensein von spezifischen Gefahren im technischen Design, im Betrieb und in der Umgebung eines Systems

3.1.9

Gefahrenminimierung

Ersatz einer Gefahr in der Gefahrenmanifestation durch eine andere Gefahr desselben Typs jedoch mit geringerem Gefahrenpotenzial

BEISPIEL Ersetzen von hoher Toxizität durch niedrigere Toxizität.

3.1.10

Gefahrenverringierung

Prozess der Beseitigung oder Minimierung und Kontrolle von Gefahren

3.1.11

Gefahrenszenario

Folge von Ereignissen, die von dem anfänglichen Grund zu der unerwarteten Folge für die Sicherheit führen

ANMERKUNG Der Grund kann ein einzelnes auslösendes Ereignis, eine zusätzliche Aktion oder eine sich verändernde Bedingung sein, die ein latent vorhandenes Problem aktiviert.

3.1.12

Gefahrenbaum

Gruppe von Gefahrenszenarien, welche bei derselben Gruppe von Gefahrenmanifestationen ihren Ausgang nehmen

3.1.13

gefährlich

Eigenschaft einer Komponente und deren Umgebung, welche das Potential für Störfälle liefert [ISO 14620-2:2000]

3.1.14

wahrnehmbare Symptome

Anzeichen dafür, dass ein unerwünschtes Ereignis eingetreten ist

ANMERKUNG Wahrnehmbare Symptome treten während der Ausbreitung des Szenarios auf.

3.1.15**Reaktionszeit**

Zeitraum zwischen der Feststellung und dem Eintreten der Folge

ANMERKUNG Hierbei handelt es sich um den Zeitraum, in dem nach der Feststellung des auslösenden Ereignisses noch abschwächende Maßnahmen ergriffen werden können.

3.1.16**Restgefahr**

Nach der Durchführung einer Gefahrenverringerng verbleibende Gefahr

3.1.17**beseitigte Gefahr**

verringerte Gefahr, wobei die Verringerung überprüft und die Restgefahr als akzeptabel eingestuft wird

ANMERKUNG Beseitigte Gefahren müssen zur formellen Annahme vorgelegt werden.

3.1.18**Ausbreitungszeit**

Zeitraum zwischen dem Eintreten des auslösenden Ereignisses und dem Eintreten der Folge

3.1.19**Schweregrad der Sicherheitsfolge**

Messung des Schweregrads eines Schadens im Hinblick auf die Sicherheit

3.2 Abkürzungen

In dieser Europäischen Norm werden die nachstehend definierten Abkürzungen verwendet.

CC&M	common cause and common failure mode analysis	Analyse des gemeinsamen Grunds und des gemeinsamen Ausfallmodus
DRD	document requirements definition	Definition der Anforderungen an Dokumente
ECSS	European Cooperation for Space Standardization	European Cooperation for Space Standardization
FMECA	failure modes, effects and criticality analysis	Analyse der Fehlermöglichkeiten, -auswirkungen und -einflüsse
GSE	ground support equipment	Bodensupportgeräte
OHA	operating hazard analysis	Betriebsgefahrenanalyse
PHA	preliminary hazard analysis	vorläufige Gefahrenanalyse
SHA	system hazard analysis	Systemgefahrenanalyse
SSHA	subsystem hazard analysis	Subsystemgefahrenanalyse

4 Prinzipien der Gefahrenanalyse

4.1 Konzept der Gefahrenanalyse

Die Gefahrenanalyse beruht auf dem nachstehend, in den Bildern 1 bis 4 dargestellten Konzept der Gefahrenanalyse.

Gefahren, welche durch Gefahrenmanifestationen latent im System vorhanden sind, werden durch das Eintreten von auslösenden Ereignissen (d. h. Ursachen) aktiviert. Gefahrenszenarien zeigen das Verhalten des Systems auf die aktivierten Gefahren, ausgedrückt als Ereignisausbreitung von den Gründen bis hin zu den Sicherheitsfolgen (siehe hierzu Bild 1). Das Eintreten von Ereignissen ist an wahrnehmbare Symptome im System gekoppelt. Die Sicherheitsfolgen werden durch ihren Schweregrad unterschieden.

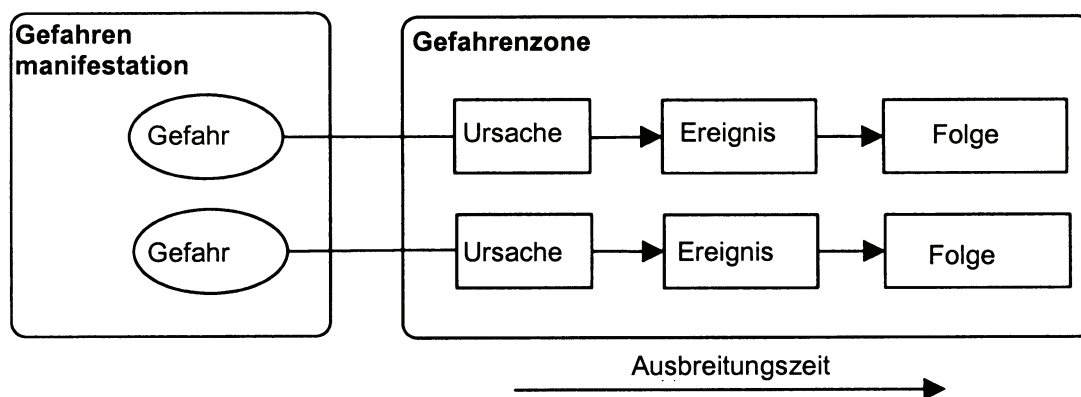


Bild 1 — Gefahr und Gefahrenszenarien

Ein und dieselbe Gefahr kann zu verschiedenen Gefahrenszenarien führen. Ferner können verschiedene Gefahrenszenarien zu derselben Sicherheitsfolge führen. Ein Beispiel ist in Tabelle 4 dargestellt. Die Gruppe von Gefahrenszenarien, welche von derselben Gefahrenmanifestation herrühren, ist im Gefahrenbaum in Bild 2 dargestellt. Die Gruppe der Gefahrenszenarien, die zur selben Sicherheitsfolge führen, ist im Folgenbaum in Bild 3 dargestellt.

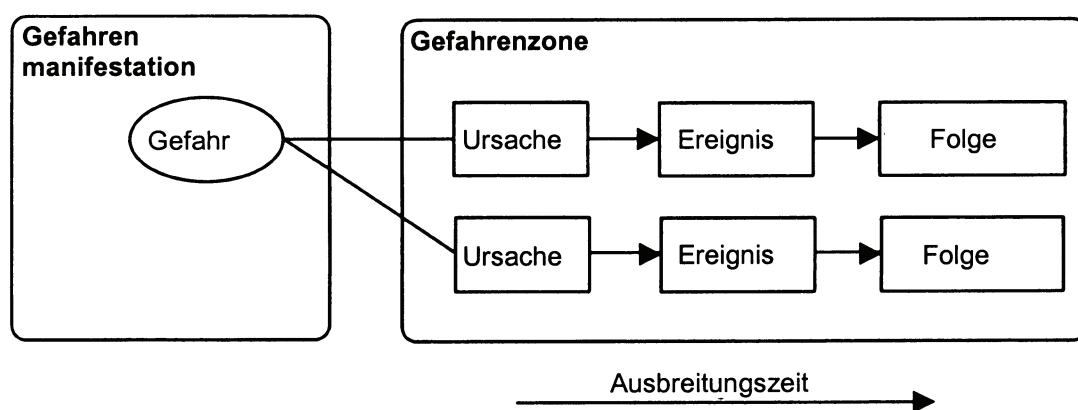


Bild 2 — Beispiel für einen Gefahrenbaum

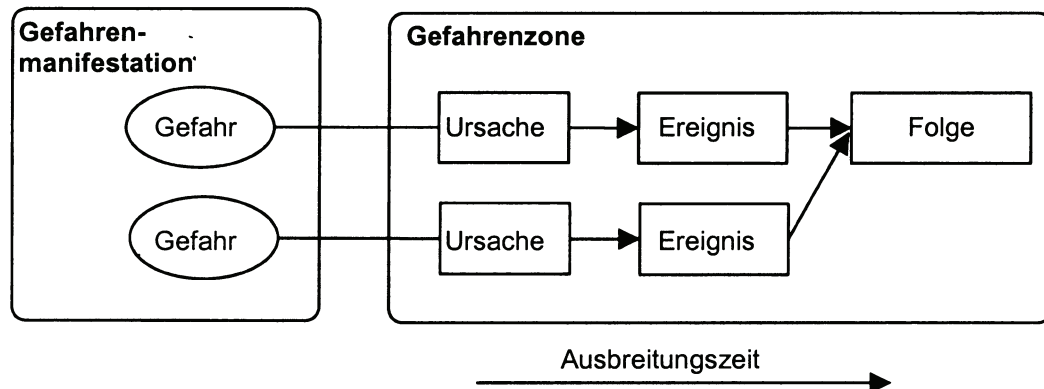


Bild 3 — Beispiel für einen Folgenbaum

Gefahren werden verringert, indem sie entweder beseitigt werden, oder, wenn das nicht möglich ist, indem sie wie in Bild 4 dargestellt minimiert und kontrolliert werden. Die Beseitigung von Gefahren erfolgt durch die Beseitigung spezifischer Systemmerkmale, von denen eine potentielle Bedrohung für die Sicherheit ausgeht. Die Minimierung von Gefahren erfolgt durch eine Verringerung der Stufe oder des Ausmaßes der Systemmerkmale, von denen eine potentielle Bedrohung für die Sicherheit ausgeht. Die Kontrolle von Gefahren erfolgt durch Verhinderung ihres Eintretens oder durch Verringerung der Wahrscheinlichkeit und Abschwächung der Auswirkungen von Ereignissen. Das Eintreten von Ereignissen kann durch ihre wahrnehmbaren Symptome festgestellt werden.

BEISPIEL Eine Gefahr beim Auto fahren ist „schlechtes Wetter“; diese Gefahr manifestiert sich als „Eis auf der Straße“. Der Grund „schneller Richtungswechsel“ kann zu dem Ereignis „Verlust der Kontrolle über das Fahrzeug“ oder „von der Straße abkommen“ und schließlich zur Folge „Tod des Fahrers“ führen. Die Gefahrenbeseitigung kann durch „Verschieben der Fahrt auf einen späteren Zeitpunkt“ erreicht werden; eine Gefahrenminimierung kann durch „Ausstreuen von Sand auf der Straße“ erreicht werden. Es gibt verschiedene Methoden für eine Gefahrenkontrolle, die einen Einfluss auf verschiedene Teile des Prozesses haben: „Langsam Fahren“ hat einen Einfluss auf die Ursache, die „Verwendung von Schneeketten“ hat einen Einfluss auf die Verbindung zwischen Ursache und Ereignis; einen „Airbag einbauen“ hat einen Einfluss auf die Verbindung zwischen Ereignis und Folge.