

DIN EN ISO 14620-1

ICS 49.140

**Raumfahrtssysteme –
Sicherheitsanforderungen –
Teil 1: Systemsicherheit (ISO 14620-1:2002);
Deutsche und Englische Fassung EN ISO 14620-1:2002**

Space systems –
Safety requirements –
Part 1: System safety (ISO 14620-1:2002);
German and English version EN ISO 14620-1:2002

Systèmes spatiaux –
Exigences de sécurité –
Partie 1: Sécurité système (ISO 14620-1:2002);
Version allemande et anglaise EN ISO 14620-1:2002

Gesamtumfang 87 Seiten

Normenausschuss Luft- und Raumfahrt (NL) im DIN

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 ISO 14620-1:2002 wurde von CEN/CS T02 auf Basis der ECSS-Q-00 unter Mitwirkung des Arbeitsausschusses 5.1.1 „Raumfahrt“ der Normenstelle Luftfahrt erarbeitet.

Entsprechend Beschluss 57/9 des Technischen Ausschusses des Beirats der Normenstelle Luftfahrt sind die europäischen Luft- und Raumfahrt-Normungsergebnisse zweisprachig, in Deutsch und Englisch, in das Deutsche Normenwerk zu überführen. Aus diesem Grund wurde in dieser nationalen Norm der Deutschen Fassung die Englische Fassung hinzugefügt.

Deutsche Fassung

**Raumfahrtssysteme – Sicherheitsanforderungen – Teil 1:
Systemsicherheit (ISO 14620-1:2002)**

Space systems – Safety requirements – Part 1: System
safety (ISO 14620-1:2002)

Systèmes spatiaux – Exigences de sécurité – Partie 1:
Sécurité système (ISO 14620-1:2002)

Diese Europäische Norm wurde vom CEN am 24. Juni 2002 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, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Portugal, Schweden, Schweiz, Spanien, der Tschechischen Republik und dem Vereinigten Königreich.



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

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

Inhalt

	Seite
Vorwort	5
Einleitung	5
1 Anwendungsbereich	6
1.1 Allgemein	6
1.2 Anwendungsbereich	6
1.3 Anpassung	7
2 Normative Verweisungen	7
3 Begriffe und Abkürzungen	7
3.1 Begriffe	7
3.2 Abkürzungen	12
4 Systemsicherheitsprogramm	13
4.1 Anwendungsbereich	13
4.2 Sicherheitsorganisation	13
4.2.1 Allgemeines	13
4.2.2 Sicherheitsvertreter	13
4.2.3 Berichterstattungslinie	13
4.2.4 Integrierte Sicherheit	13
4.2.5 Koordination mit anderen Stellen.....	13
4.3 Zugangsrecht und Befugnis des Sicherheitsvertreters	14
4.3.1 Zugang	14
4.3.2 Übertragene Befugnis zur Zurückweisung oder Unterbindung der Arbeit.....	14
4.3.3 Übertragene Befugnis zur Unterbrechung von Betriebsvorgängen.....	14
4.3.4 Übereinstimmung.....	14
4.3.5 Berichtsgenehmigung	14
4.3.6 Review	14
4.3.7 Vertretung in Ausschüssen	14
4.4 Sicherheitsrisikomanagement	14
4.4.1 Risiko.....	14
4.4.2 Gefährdungsbewertung.....	15
4.4.3 Maßnahmen	15
4.5 Projektphasen und Sicherheits-Reviewzyklus.....	15
4.5.1 Fortschrittsbesprechung.....	15
4.5.2 Projekt-Reviews	15
4.5.3 Sicherheitsprogramm	18
4.5.4 Sicherheitsdatenpaket.....	18
4.6 Sicherheitsprogrammplan.....	18
4.6.1 Durchführung	18
4.6.2 Sicherheitsaktivitäten	18
4.6.3 Definition	18
4.6.4 Beschreibung	18
4.6.5 Sicherheits- und Projektengineering-Tätigkeiten	19
4.6.6 Lieferanten und Unterlieferanten.....	19
4.6.7 Einhaltung.....	19
4.7 Sicherheitszertifizierung	19
4.8 Sicherheitstraining.....	19
4.8.1 Bestandteil	19
4.8.2 Teilnahme.....	20
4.8.3 Eingehendes technisches Training.....	20
4.8.4 Produktspezifisches Training	20
4.8.5 Aufzeichnungen	20
4.8.6 Identifizierung.....	20
4.9 Berichterstattung und Untersuchung von Unfällen/Zwischenfällen	20

4.10	Sicherheitsdokumentation.....	20
4.10.1	Allgemeines.....	20
4.10.2	Kundenzugang	20
4.10.3	Lieferant.....	20
4.10.4	Dokumentation.....	21
4.10.5	Sicherheitsdatenpaket	21
4.10.6	Sicherheitsbezogene Sonderfreigabe (vor und nach Realisierung)	21
4.10.7	Verifikationskontroll-Dokument	22
4.10.8	Erfahrungsdatei	22
5	Sicherheitstechnik	22
5.1	Sicherheitstechnische Grundsätze.....	22
5.1.1	Allgemeines.....	22
5.1.2	Elemente	23
5.1.3	Gewonnene Sicherheitserkenntnisse (lessons learnt)	23
5.2	Sicherheitsbezogene Designgrundsätze	23
5.2.1	Menschliche Überlegung	23
5.2.2	Designauswahl.....	23
5.2.3	Gefährdungsbeseitigungs- und -kontrollmaßnahmen.....	23
5.2.4	Umweltverträglichkeit	24
5.2.5	Sicher ohne externe Dienste	24
5.2.6	„Fail Safe“-Design	24
5.2.7	Gefährdungserkennung — Signalisierung und Sicherung	24
5.2.8	Zugang	25
5.3	Sicherheitsrisikoreduzierung und -kontrolle	25
5.3.1	Schweregrad	25
5.3.2	Fehlertoleranzanforderungen	26
5.3.3	Auslegung für minimales Risiko.....	27
5.3.4	Probabilistische Sicherheitsziele.....	28
5.4	Identifizierung und Kontrolle sicherheitskritischer Funktionen	29
5.4.1	Identifizierung	29
5.4.2	Unbeabsichtigtes Auslösen.....	29
5.4.3	Maßnahmen	29
5.4.4	Sichere Abschaltung und Fehlertoleranzanforderungen	29
5.4.5	Elektronische, elektrische, elektromechanische Bauelemente	29
6	Sicherheitsanalyse — Anforderungen und Techniken	29
6.1	Allgemeines.....	29
6.2	Bewertung und Zuweisung von Anforderungen	30
6.2.1	Sicherheitsanforderungen	30
6.2.2	Zusätzliche Sicherheitsanforderungen	30
6.2.3	Sicherheitsanforderungen an Funktionen	30
6.2.4	Sicherheitsanforderungen an Subsysteme	30
6.2.5	Berechtigung.....	30
6.2.6	Funktions- und Subsystemspezifikation.....	31
6.3	Sicherheitsanalyse	31
6.3.1	Allgemeines.....	31
6.3.2	Missionsanalyse	31
6.3.3	Durchführbarkeit.....	31
6.3.4	Vordefinition.....	31
6.3.5	Detaildefinition, Produktion und Qualifikation	31
6.3.6	Betrieb.....	31
6.3.7	Entsorgung.....	31
6.4	Spezielle Sicherheitsanalyse	32
6.4.1	Allgemeines.....	32
6.4.2	Gefährdungsanalyse	32
6.4.3	Sicherheitsrisikobewertung.....	33
6.4.4	Sicherheitsanalyse für Hardware-Softwaresysteme	33

6.5	Unterstützende Bewertung und Analyse	34
6.5.1	Allgemeines	34
6.5.2	Warnzeitanalyse	34
6.5.3	Vorsicht- und Warnanalyse	34
6.5.4	Analyse der gemeinsamen Ausfall-/Fehlerarten und -ursachen	35
6.5.5	Fehlzustandsbaumanalyse (FTA)	35
6.5.6	Analyse der menschlichen Zuverlässigkeit	35
6.5.7	Fehlerart-, -auswirkungs- und -kritikalitätsanalyse (FMECA)	36
6.5.8	Sneak-Analyse	36
6.5.9	Zonenanalyse	36
6.5.10	Energieverlaufsanalyse	37
7	Sicherheitsverifikation	37
7.1	Allgemeines	37
7.2	Gefährdungsverfolgung	37
7.2.1	Gefährdungsberichtssystem	37
7.2.2	Status	37
7.2.3	Sicherheitsfortschrittsbesprechung	37
7.2.4	Überprüfung und Verfügung	37
7.2.5	Dokumentation	38
7.2.6	Prüfpunkt	38
7.3	Sicherheitsverifikationsmethoden	38
7.3.1	Verifikationstechnik und Planung	38
7.3.2	Berichte und Methoden	38
7.3.3	Verifikationsanforderungen	38
7.3.4	Analyse	38
7.3.5	Inspektion	38
7.3.6	Tests	39
7.3.7	Verifikation und Genehmigung	39
7.4	Qualifikation sicherheitskritischer Funktionen	39
7.4.1	Gültigkeit	39
7.4.2	Qualifikation	39
7.4.3	Fehlertests	39
7.4.4	Verifikation des Design oder Betriebsmerkmale	39
7.4.5	Sicherheitsverifikationstest	40
7.5	Beglaubigung des Gefährdungsausschlusses	40
7.5.1	Sicherheitssicherungsstelle	40
7.5.2	Sicherheitszertifizierungsstelle	40
7.6	Restrisikoreduzierung	40
8	Betriebssicherheit	40
8.1	Anforderungsgrundlage	40
8.2	Flugbetriebs- und Missionskontrolle	41
8.2.1	Trägersystem	41
8.2.2	Verschmutzung	41
8.2.3	Flugregeln	41
8.2.4	Kontrolle gefährdender Befehlsgebungen	41
8.2.5	Änderungskontrolle des Missionsbetriebs	42
8.2.6	Sicherheitsüberwachung und Kontrolle von Anomalien	42
8.3	Bodenbetrieb	42
8.3.1	Anwendbarkeit	42
8.3.2	Einleitung	42
8.3.3	Reviews und Prüfungen	42
8.3.4	Gefährdender Betrieb	43
8.3.5	Start- und Landeplatzanforderungen	43
8.3.6	Anforderungen an Bodendienstgeräte (Servicing-Geräte, Checkout- und Testgeräte, Handhabungs- und Transportgeräte, Nabelverbindungen, Hilfsgeräte)	43
	Literaturhinweise	44

Vorwort

Dieses Dokument (EN ISO 14620-1:2002) wurde vom Technischen Komitee CEN/SS T02 „Luft- und Raumfahrt“, in Zusammenarbeit mit dem Technischen Komitee ISO/TC 20 „Luft- und Raumfahrzeuge“, erarbeitet, dessen Sekretariat vom CMC gehalten wird.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis Juni 2003, und etwaige entgegenstehende nationale Normen müssen bis Juni 2003 zurückgezogen werden.

Die Europäische Norm EN ISO 14620-1 wurde von der ECSS-Arbeitsgruppe (European cooperation for Space Standardization) für CEN in Zusammenarbeit mit dem Technischen Komitee ISO/TC 20, *Luft- und Raumfahrzeuge*, Unterkomitee SC 14, *Raumfahrtsysteme*, WG 5, *Managementprogramm*, erarbeitet.

EN ISO 14620 besteht aus den folgenden Teilen mit dem gemeinsamen Titel *Raumfahrtsysteme — Sicherheitsanforderungen*:

— Teil 1: *Systemsicherheit*

— Teil 2: *Abschussbasisoperationen*

Entsprechend der CEN/CENELEC-Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Europäische Norm zu übernehmen: Belgien, Dänemark, Deutschland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Portugal, Schweden, Schweiz, Spanien, die Tschechische Republik und das Vereinigte Königreich.

Einleitung

Diese Europäische Norm ist eine der Serien der Raumfahrt, die zusammen mit dem Management, der Technik und Produktsicherheit in Raumfahrtprojekten und Anwendung benutzt wird.

1 Anwendungsbereich

1.1 Allgemein

Diese Europäische Norm legt das Sicherheitsprogramm und die sicherheitstechnischen Anforderungen fest, die in Übereinstimmung mit der in ISO 14300-2 festgelegten Sicherheitsleitlinien umzusetzen sind, um Flug- und Bodenpersonal, Träger, zugehörige Nutzlasten, Bodendienstgeräte, die allgemeine Öffentlichkeit, öffentliches und privates Eigentum sowie die Umwelt vor Gefährdungen im Zusammenhang mit europäischen Raumfahrtssystemen zu schützen. Abschussbasisoperationen sind in ISO 14620-2 beschrieben.

Die Sicherheitsleitlinien werden durch Umsetzung eines Sicherheitsprogramms, unterstützt durch eine Risikobewertung, verwirklicht, das sich wie folgt zusammenfassen lässt:

- a) Gefährdungsmerkmale (System- und Umweltgefährdungen) und Funktionen mit potentiell gefährdenden Ausfall-/Fehlerauswirkungen werden identifiziert und schrittweise durch iterative Durchführung systematischer, deterministischer Sicherheitsanalysen bewertet;
- b) potentielle Gefährdungsfolgen im Zusammenhang mit den Merkmalen und Funktionsausfällen/-fehlern des Systems werden einer Gefährdungsreduzierungssequenz unterzogen, wobei:
 - 1) Gefährdungen aus dem Systemdesign und –betrieb beseitigt;
 - 2) Gefährdungen minimiert;
 - 3) Gefährdungskontrollmaßnahmen angewandt und verifiziert werden.
- c) Die nach Durchführung des Gefährdungs-beseitigungs- und -reduzierungsprozesses verbleibenden Risiken werden schrittweise bewertet und einer Risikobewertung unterzogen, um:
 - 1) die Übereinstimmung mit den Sicherheitszielen aufzuzeigen;
 - 2) vergleichende Designbewertungen zu unterstützen;
 - 3) Risikoverursacher festzustellen und einzustufen;
 - 4) die Zuteilung von Projektmitteln zur Risikoreduzierung zu unterstützen;
 - 5) den Fortschritt der Risikoreduzierung zu beurteilen;
 - 6) den Prozess von Sicherheits- und Projektentscheidungsfindungen (z. B. Sonderfreigaben, Restriktionsbilligung) zu unterstützen.
- d) Die Angemessenheit der Gefährdungs- und Risikokontrollmaßnahmen wird formal verifiziert, um die Beglaubigung der Sicherheit und die Risikobilligung zu unterstützen.
- e) Die Sicherheitskonformität ist für das Produkt zu beurteilen und die Sicherheit von den zuständigen Stellen zu erlangen.

1.2 Anwendungsbereich

Diese Europäische Norm gilt für alle Raumfahrtprojekte, bei denen in irgendeiner Projektphase die Möglichkeit von Gefährdungen für Personal oder die allgemeine Öffentlichkeit, Raumflugsysteme, Bodendienstgeräte, Einrichtungen, öffentliches oder privates Eigentum oder die Umwelt besteht.

Die Vorgabe dieser Anforderungen für die Projektstätigkeiten der Lieferanten setzt voraus, dass die Projekt-Produktsicherungs- und -Sicherheitsorganisation des Kunden ebenfalls diesen Anforderungen in einer der Sicherheitskritikalität des Projekts angemessenen Weise entspricht.

1.3 Anpassung

Im Hinblick auf den Kontext eines speziellen Programms oder Projekts sollten die in dieser Europäischen Norm festgelegten Anforderungen an die tatsächlichen Anforderungen für das jeweilige Profil und die Gegebenheiten eines Programms oder Projekts angepasst werden.

ANMERKUNG Anpassung ist der Prozess, durch den einzelne Anforderungen von Spezifikationen, Normen und verwandten Dokumenten bewertet und für ein spezifisches Programm oder Projekt durch Auswahl und in einigen Ausnahmefällen durch Änderung von bestehenden oder Zufügung von neuen Anforderungen anwendbar gemacht werden.

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).

ISO 14300-1, *Space systems — Programme management — Part 1: Structuring of a programme*.

ISO 14300-2, *Space systems — Programme management — Part 2: Product assurance*.

ISO 14620-2, *Space systems — Safety requirements — Part 2: Launch site operations*.

3 Begriffe und Abkürzungen

3.1 Begriffe

Für die Anwendung dieser Europäischen Norm gelten die folgenden Begriffe.

3.1.1

Unfall

unerwünschtes Ereignis, das sich aus dem Einsatz von projektspezifischen Einheiten ergibt und Folgendes bewirkt:

- a) Tod oder Verletzung von Personen;
- b) Verlust oder Beschädigung von Projekt-Hardware, -Software oder -Einrichtungen, wodurch die Erfüllung der Mission beeinträchtigt werden könnte;
- c) Verlust oder Beschädigung von öffentlichem oder privatem Eigentum; oder
- d) schädliche Auswirkungen für die Umwelt

[EN 13701:2001]

ANMERKUNG Unfall und Panne sind Synonyme.

3.1.2

Ursache

das, was eine Wirkung hervorruft; das, was eine Aktion, eine Erscheinung oder einen Zustand zur Folge hat

ANMERKUNG 1 Ursache und Wirkung sind korrelative Begriffe (Oxford Englisch Dictionary).

ANMERKUNG 2 Speziell für diese Europäische Norm, im Zusammenhang mit der Gefährdungsanalyse: Vorgang oder Zustand, durch den ein Gefährdungsereignis ausgelöst wird (auslösendes Ereignis). Die Ursache kann durch einen Ausfall/Fehler, menschliches Fehlverhalten, Designmangel, induzierte oder natürliche Umgebungsbedingungen, Systemkonfigurations- oder -betriebsart(en) entstehen.

ANMERKUNG 3 In Anlehnung an EN 13701:2001.

3.1.3

"Vorsicht"-Zustand

Zustand, der das Potential hat, sich in einen "Warn"-Zustand zu verschlechtern, und spezifische Maßnahmen erfordern könnte, einschließlich der Durchführung besonderer Verfahren oder Einschränkungen für den Betrieb des Systems

[EN 13701:2001]

3.1.4

Ausfall (Fehler) mit gemeinsamer Ausfall(Fehler)ursache

Ausfälle (Fehler) von mehreren Einheiten, die eine einzelne Ursache haben, die allen gemeinsam ist

[NUREG/CR-2300 PRA:1982]

3.1.5

Ausfall (Fehler) mit gemeinsamer Ausfall(Fehler)art

Ausfälle (Fehler) von mehreren identischen Einheiten, die auf dieselbe Art und Weise versagen

ANMERKUNG 1 Ausfälle(Fehler) mit gemeinsamer Ausfall(Fehler)art sind ein besonderer Fall von Ausfällen(Fehlern) mit gemeinsamer Ausfall(Fehler)ursache.

ANMERKUNG 2 In Anlehnung an NUREG/CR-2300 PRA:1982.

3.1.6

Störfallverfahren

ein vorausgeplantes Verfahren, das im Falle einer Abweichung von einem festgelegten Verhalten zur Anwendung gelangt

[EN 13701:2001]

3.1.7

kritischer Fehlzustand

Fehlzustand, der als Gefahr eingestuft wird, Personenschäden, beträchtliche Sachschäden oder andere unvermeidbare Folgen zu verursachen

[IEC 60050:1992]

3.1.8

Not(fall)

Zustand, in dem potentiell katastrophale oder kritische Gefährdungsereignisse eingetreten sind und sofortige vorausgeplante Sicherungsmaßnahmen zum Schutz von Personen möglich und zwingend sind

ANMERKUNG In Anlehnung an EN 13701:2001.

3.1.9**sicher bei Ausfall (fail safe)**

Konstruktionseigenschaft einer Einheit, die verhindert, dass deren Ausfälle zu kritischen Fehlzuständen führen

[IEC 60050:1992]

3.1.10**Ausfall**

Beendigung der Fähigkeit einer Einheit, eine geforderte Funktion zu erfüllen

[IEC 60050:1992]

3.1.11**Fehlzustand, m**

<Zustand> Zustand einer Einheit, in dem sie unfähig ist, eine geforderte Funktion zu erfüllen, wobei die durch Wartung oder andere geplante Handlungen bzw. durch das Fehlen äußerer Mittel verursachte Unfähigkeit ausgeschlossen ist

ANMERKUNG 1 Ein Fehlzustand ist oft das Ergebnis eines Ausfalls(Fehlers) der Einheit selbst, er kann aber auch ohne vorherigen Ausfall vorhanden sein.

ANMERKUNG 2 In Anlehnung an IEC 60050:1992.

3.1.12**Fehlzustand, m**

<Ereignis> unplanmäßiges Vorkommnis oder Fehler in einer Einheit, das bzw. der zu einem oder mehreren Ausfällen (Fehlern) der Einheit selbst oder anderer zugehöriger Ausrüstung führen kann

[IEC 60050:1992]

ANMERKUNG Eine Einheit kann einen Fehlzustand eines Teilelements aufweisen, einen Fehler, der sich nur unter bestimmten Umständen zeigt. Wenn diese Umstände eintreten, führt der Fehler im Teilelement zum Ausfall der Einheit, was eine Fehlaussage zur Folge hat. Diese Fehlaussage kann sich auf andere Einheiten ausdehnen, die dadurch ihrerseits zum Ausfall führen. Nach dem Eintreten des Ausfalls gilt, dass die Einheit als Ganzes einen Fehlzustand hat oder in einem fehlerhaften Zustand ist (Definition 3.1.11 oben)

[EN 13701:2001]

3.1.13**Gefährdung**

bestehender oder potentieller Zustand einer Einheit, die zu einer Panne führen kann

ANMERKUNG Dieser Zustand kann mit Design, Herstellung, Betrieb oder Umgebung einer Einheit im Zusammenhang stehen und hat das Potential für Pannen.

[ISO 14620-2]

3.1.14**Gefährdungseignis**

Ereignis, das zu unerwünschten Folgen führt und durch Auslösung einer oder mehreren Gefährdungen aufgrund eines oder mehrerer Auslöseereignisse hervorgerufen wird

ANMERKUNG In Anlehnung an EN 13701:2001.

3.1.15**Zwischenfall**

ungeplantes Ereignis, das ein Unfall hätte sein können, es jedoch nicht war

[EN 13701:2001]

3.1.16

Sperre

Designmerkmal, das eine physische Unterbrechung zwischen einer Energiequelle und einem Funktionsauslöser herstellt

BEISPIEL Relais oder Transistor zwischen einer Batterie und einem pyrotechnischen Auslöser, Sperrventil zwischen Treibstofftank und Triebwerk.

ANMERKUNG 1 Zwei Sperren gelten als unabhängig, wenn ein Einzelfehler nicht mehr als eine Sperre beseitigen kann.

ANMERKUNG 2 In Anlehnung an EN 13701:2001.

3.1.17

Fehlverhalten des Betriebspersonals

Versagen des Betriebspersonals, eine Handlung anforderungs- oder anleitungsgemäß auszuführen oder die unabsichtliche oder fehlerhafte Handlung des Betriebspersonals

3.1.18

Organisation

Gruppe von Personen und Einrichtungen mit einem Gefüge von Verantwortungen, Befugnissen und Beziehungen

BEISPIELE Gesellschaft, Körperschaft, Firma, Unternehmen, Institution, gemeinnützige Organisation, Einzelunternehmer, Verband oder Teile oder Mischformen solcher Einrichtungen.

ANMERKUNG 1 Das Gefüge ist üblicherweise geordnet.

ANMERKUNG 2 Eine Organisation kann öffentlich-rechtlich oder privatrechtlich sein.

ANMERKUNG 3 Diese Definition gilt im Rahmen von Normen zu Qualitätsmanagementsystemen. Der Begriff „Organisation“ ist im ISO/IEC-Leitfaden 2 anders definiert.

[EN ISO 9000:2000]

3.1.19

Programm

koordinierter Satz von nicht notwendigerweise voneinander abhängigen Tätigkeiten, die über einen Zeitraum bestehen und zur Erlangung weitgefasster wissenschaftlicher oder technischer Ziele oder vermehrter Kenntnis über ein bestimmtes Thema dienen

BEISPIEL Das Verteidigungsprogramm; das Apollo-Programm; das Erdbeobachtungsprogramm.

ANMERKUNG 1 Ein Programm kann mehrere Projekte umfassen.

ANMERKUNG 2 Ein Programm kann mehrere Jahre laufen.

ANMERKUNG 3 „program“ ist die amerikanische Standard-Schreibweise für „programme“.

ANMERKUNG 4 „program“ ist der britische Standard-Ausdruck für „eine Reihe kodierter Anweisungen, um die Arbeit eines Rechners oder einer Maschine zu kontrollieren“ — Oxford English Dictionary.

3.1.20

Projekt

Gesamtheit von koordinierten Tätigkeiten mit bestimmten Start- und Zielpunkten, die von einer Person oder Organisation durchgeführt werden, um spezifische Ziele im Rahmen festgelegter Zeit-, Kosten- und Leistungsparameter zu erreichen

[BS 6079:1996]

3.1.21

Auftraggeber

Kunde in einer Vertragssituation

ANMERKUNG Der Auftraggeber wird manchmal als die „business second party“ bezeichnet.

3.1.22

Restrisiko

Risiko, das in einem System nach Ausführung des Gefährdungsreduzierungs- und -überwachungsprozesses bestehen bleibt

[EN 13701:2001]

3.1.23

Risiko

quantitatives Maß für die Größe eines potentiellen Verlusts und die Eintrittswahrscheinlichkeit eines solchen Verlusts

[EN 13701:2001]

3.1.24

sicherer Zustand

Zustand, der nicht zu kritischen oder katastrophalen Folgen führt

3.1.25

sicherheitskritische Funktion

Funktion, die bei Verlust oder Minderung oder durch unsachgemäßen oder unbeabsichtigten Betrieb zu katastrophalen oder kritischen Folgen führen könnte

ANMERKUNG In Anlehnung an EN 13701:2001.

3.1.26

Sicherung(Maßnahme)

Maßnahme, die durchgeführt wird, um Not- und Warnsituationen einzugrenzen oder unter Kontrolle zu bringen oder ein System (oder einen Teil davon) in einen vorausbestimmten sicheren Zustand zu versetzen

ANMERKUNG In Anlehnung an EN 13701:2001.

3.1.27

Lieferant

Organisation oder Person, die ein Produkt bereitstellt

BEISPIEL Hersteller, Vertriebseinrichtung, Einzelhändler, Verkäufer eines Produkts oder Erbringer einer Dienstleistung oder Bereitsteller von Informationen.

ANMERKUNG 1 Ein Lieferant kann der Organisation angehören oder ein Außenstehender sein.

ANMERKUNG 2 In einer Vertragssituation wird ein Lieferant manchmal als „Auftragnehmer“ bezeichnet.

[EN ISO 9000:2000]

3.1.28

System

Zusammenstellung von zusammenhängenden Elementen zum Erreichen eines vorgegebenen Ziels durch Ausführung einer festgelegten Funktion

ANMERKUNG Das System wird von der Umgebung und anderen externen Systemen durch eine imaginäre Oberfläche getrennt betrachtet, die die Verbindungen zwischen diesen und dem betrachteten System trennt. Über diese Verbindungen wird das System durch die Umgebung beeinflusst, der Einwirkung externer Systeme ausgesetzt oder wirkt selbst auf die Umgebung oder externe Systeme ein.

[IEC 60050:1992]

3.1.29

Systemsicherheit

Anwendung von Engineering- und Managementgrundsätzen, -kriterien und -techniken, um alle sicherheitsbezogenen Aspekte innerhalb der Grenzen von Funktionsfähigkeit, Zeit und Kosten während aller Lebenszyklusphasen des Systems zu optimieren

3.1.30

Warnzustand

Zustand, in dem potentiell katastrophale oder kritische Gefährdungsereignisse unmittelbar bevorstehen und vorausgeplante Sicherungsmaßnahmen innerhalb einer begrenzten Zeit durchgeführt werden müssen

ANMERKUNG In Anlehnung an EN 13701:2001.

3.1.31

Zonenanalyse

systematische Prüfung der geographischen Lage der Elemente und der Wechselwirkungen eines Systems, Bewertung der potentiellen Wechselwirkungen zwischen Subsystemen mit und ohne Ausfall/Fehler und Beurteilung der Schwere der möglichen systeminstallationseignen Gefährdungen

3.2 Abkürzungen

Die folgenden Abkürzungen werden in dieser Europäischen Norm entsprechend benutzt.

Abkürzung	Bedeutung
CCB	Konfigurations-Überwachungsausschuss
ECSS	European Cooperation for Space Standardization
EEE	elektronisch, elektrisch, elektromechanisch
FMECA	Fehlerart-, -auswirkungs- und -kritikalitätsanalyse
FTA	Fehlzustandsbaumanalyse
GEO	geostationäre Umlaufbahn
GSE	Bodendienstgerät
IEC	Internationale Elektrotechnische Kommission
LEO	niedrige Erdumlaufbahn
MIL STD	militärische Norm (US Verteidigungsministerium)
MIP	verbindlich vorgeschriebener Prüfpunkt
NRB	Nichtkonformitäts-Untersuchungsausschuss
NUREG-CR	US-Atomaufsichtskommission — Contractor Report (Bericht des Auftragnehmers)
TRB	Test-Untersuchungsausschuss
VTL	Verifikations-Nachweisverzeichnis

4 Systemsicherheitsprogramm

4.1 Anwendungsbereich

- a) Ziel und Zweck des Sicherheitsprogramms ist die Erstellung eines Sicherheitsmanagementsystems zur Umsetzung der Festlegungen dieser Europäischen Norm im Einklang mit den Programmanforderungen.
- b) Das Systemsicherheitsprogramm sollte vom Kunden je nach Projekttyp, Sicherheitskritikalität, Komplexität und Entwicklungsphase in Übereinstimmung mit den Anforderungen von ISO 14300-1 und ISO 14300-2 angepasst werden.
 - 1) Der Lieferant muss ein Sicherheitsprogramm für das System erstellen und aufrechterhalten.
 - 2) Der Lieferant muss die Sicherheitsanforderungen und -vorschriften für Startplatz und Träger entsprechend den Projektanforderungen anwenden, um die effiziente und effektive Durchführung der Systemsicherheitszielsetzungen zu ermöglichen.
 - 3) Die entsprechenden Anforderungen an das Systemsicherheitsprogramm nach dieser Europäischen Norm sind zur Umsetzung der für Startplatz und Träger anzuwendenden Anforderungen und Vorschriften heranzuziehen.
- c) Die Einhaltung der hierin festgelegten Sicherheitsanforderungen entbindet den Lieferanten keineswegs von der Einhaltung nationaler oder internationaler Sicherheitsvorschriften.
- d) Bei der Anpassung darf die Zielsetzung , Flug- und Bodenpersonal, Träger, zugehörige Nutzlasten, Bodendienstgeräten, die allgemeine Öffentlichkeit, öffentliches und privates Eigentum sowie die Umwelt vor Gefährdungen im Zusammenhang mit Raumfahrtssystemen zu schützen, nicht gemindert werden.

4.2 Sicherheitsorganisation

4.2.1 Allgemeines

Jeder Lieferant ist für die Sicherheit seines Produktes verantwortlich. Deshalb gelten folgende Anforderungen.

4.2.2 Sicherheitsvertreter

Jeder Lieferant muss entsprechend ISO 14300-2 einen Sicherheitsvertreter benennen, der aufgrund seiner Ausbildung oder Erfahrung qualifiziert ist, Systemsicherungsfunktionen durchzuführen.

4.2.3 Berichterstattungslinie

Die Sicherheitsvertreter müssen Berichterstattungslinien zum Projektleiter und zur obersten Unternehmensleitung haben, die unabhängig von der hierarchischen Berichterstattungslinie innerhalb des Projekts sind.

4.2.4 Integrierte Sicherheit

Die Sicherheit ist in alle Projektaktivitäten zu integrieren.

4.2.5 Koordination mit anderen Stellen

Die Sicherheitsvertreter müssen bestehende Zugänge zu allen betroffenen medizinischen Ausschüssen, Strahlungsschutzkommissionen und industriellen Sicherheitsorganen, soweit zweckmäßig, haben.

4.3 Zugangsrecht und Befugnis des Sicherheitsvertreters

4.3.1 Zugang

Der Sicherheitsvertreter muss das Zugangsrecht zu allen für die Projektsicherheit relevanten Daten haben und frei und ohne Organisationszwang über alle Aspekte der Projektsicherheit berichten dürfen.

4.3.2 Übertragene Befugnis zur Zurückweisung oder Unterbindung der Arbeit

Dem Sicherheitsvertreter muss die Befugnis übertragen sein, Projektdokumente zurückzuweisen oder Projektaktivitäten zu unterbinden, die nicht den genehmigten Sicherheitsanforderungen oder –vorschriften entsprechen.

4.3.3 Übertragene Befugnis zur Unterbrechung von Betriebsvorgängen

Zur korrekten Risikokontrolle muss dem Sicherheitsvertreter die Befugnis übertragen sein, gefährdende Betriebsvorgänge zu unterbrechen und das betreffende System wieder in einen sicheren Zustand zu versetzen, wenn sich zeigt, dass der Betrieb nicht den Maßnahmen entspricht.

4.3.4 Übereinstimmung

Der Lieferant muss die Übereinstimmung seiner eigenen und der Projektaktivitäten seiner Unterlieferanten mit den Sicherheitsgrundsätzen des Projektes und den Anforderungen sicherstellen.

4.3.5 Berichtsgenehmigung

Der Lieferant darf ohne unterzeichnete Genehmigung des Sicherheitsvertreters keinen Projektbericht herausgeben lassen, der Aspekte der Sicherheitszertifizierung berührt.

4.3.6 Review

Ohne vorheriges Sicherheits-Review und die schriftliche Zustimmung des Sicherheitsvertreters dürfen gefährdende Projektbetriebsvorgänge oder Systemeinsätze nicht vorgenommen werden.

4.3.7 Vertretung in Ausschüssen

Die Sicherheit muss in den Konfigurations-Überwachungsausschüssen (CCB's), den Material-Untersuchungsausschüssen (MRB's), den Test-Untersuchungsausschüssen (TRB's), bei den Qualifikations- und Abnahme-Reviews vertreten sein, wenn Sicherheitsanforderungen und sicherheitskritische Funktionen und/oder sicherheitskritische Einheiten betroffen sind. Die Sicherheit muss weiterhin in allen medizinischen oder vergleichbaren Ausschüssen vertreten sein, wenn Grenzen der Belastbarkeit/Ausdauer für die Flug- und Bodenmannschaften festgelegt werden.

4.4 Sicherheitsrisikomanagement

4.4.1 Risiko

Das Risiko für Menschenleben, Investitionen, Mission und Umwelt ist im gesamten Projektverlauf durch Ausübung folgender Tätigkeiten zu steuern:

- a) Zuweisung von Sicherheitsanforderungen;
- b) Gefährdungsidentifizierung;
- c) Gefährdungsbewertung;
- d) Gefährdungsverhütung, -reduzierung und -kontrolle;
- e) Gefährdungsausschluss einschließlich Restrisikobilligung.

4.4.2 Gefährdungsbewertung

Bei allen Gefährdungsbewertungen müssen in erster Linie das Gefährdungspotential betrachtet und alle Gefährdungen je nach Schweregrad eingestuft werden. Entsprechende Kontrollmaßnahmen sind vorzuschlagen. Das ursprüngliche Design ist so zu wählen, dass das Gefährdungspotential und der jeweilige Schweregrad der Folgen minimiert werden. Die Wahrscheinlichkeit eines Gefährdungsereignisses ist folglich immer dann in Betracht zu ziehen, wenn Methoden zur Schweregradreduzierung von Gefährdungsfolgen allein als unzureichend angesehen werden, d. h. alle Mindestrisiko-Designbereiche oder die Zuverlässigkeit von Sicherheitsgeräten.

4.4.3 Maßnahmen

Maßnahmen zur Reduzierung des Gefährdungspotentials, durch die zumindest die Zuverlässigkeit nicht eingeschränkt wird, sind vorzuziehen. Wahrscheinlichkeits- und somit risikobezogenen Reduzierungsmaßnahmen, die nicht zu einer erhöhten Kritikalität führen, ist der Vorzug zu geben.

4.5 Projektphasen und Sicherheits-Reviewzyklus

4.5.1 Fortschrittsbesprechung

Im Rahmen dieser Europäischen Norm festgelegten Projektfortschrittsbesprechungen muss der Lieferant regelmäßig Sicherheitsfortschrittsbesprechungen mit dem Kunden und seinen Unterlieferanten abhalten. Auf den Besprechungen müssen die jeweiligen Experten des Kunden und Lieferanten vertreten sein und der Stand der Sicherheitsprogrammtätigkeiten nach den Festlegungen dieser Norm und des Vertrags überprüft werden.

4.5.2 Projekt-Reviews

4.5.2.1 Allgemeines

- a) Der Lieferant muss die Sicherheits-Reviews des Projektsicherheitsstatus durch den Kunden und gegebenenfalls die zuständige Startorganisation, wie in dieser Norm gefordert, unterstützen.
- b) Sicherheits-Reviews sind auf allen Ebenen abzuhalten, die zur Sicherstellung der zufriedenstellenden Umsetzung des Sicherheitsprogramms und der sicherheitstechnischen Anforderungen notwendig sind.
- c) Für jedes Review ist in der Regel ein Sicherheitsdatenpaket zu erstellen.
- d) Sicherheits-Reviews sollten in Verbindung mit den folgenden Projektmeilensteinen, soweit zutreffend, und den im jeweiligen Unterabschnitt beschriebenen Zielsetzungen durchgeführt werden.

4.5.2.2 Missiondefinitions-Review

Beim Missiondefinitions-Review muss der Lieferant den folgenden Nachweis führen:

- a) Die Sicherheitsanforderungen und Erfahrungen aus früheren Projekten wurden analysiert. Vergleichende Design- und Betriebskonzeptbewertungen wurden unterstützt.
- b) Die wichtigsten Sicherheitsanforderungen auf Systemebene wurden identifiziert.

4.5.2.3 Vorläufiges Anforderungs-Review

Beim vorläufigen Anforderungs-Review muss der Lieferant den folgenden Nachweis führen:

- a) Die Gefährdungen, Gefährdungszustände und -ereignisse auf Systemebene, zusammen mit den sicherheitskritischen Aspekten und dem Sicherheitsrisiko der analysierten Konzepte, wurden identifiziert und verglichen.
- b) Die Projektsicherheitsanforderungen auf Systemebene wurden verfeinert.

4.5.2.4 Systemanforderungs-Review

Beim Systemanforderungs-Review muss der Lieferant den folgenden Nachweis führen:

- a) Die Sicherheitsanforderungen wurden ausreichend detailliert spezifiziert, um die Definition der technischen Lösungen für das in Phase A gewählte Systemkonzept zu ermöglichen.
- b) Die Ergebnisse der Sicherheitsanalyse sind zur Bestätigung der Übereinstimmung der empfohlenen Lösung mit den Projektsicherheitsanforderungen verfügbar.

4.5.2.5 Vorläufiges Design-Review

Beim vorläufigen Design-Review muss der Lieferant den folgenden Nachweis führen:

- a) Die Gefährdungskontrollmaßnahmen und Sicherheitsanforderungen wurden hinreichend definiert, um mit dem Detaildesign beginnen zu können.
- b) Das vorgestellte Design entspricht den Sicherheitsanforderungen in dem für das Review geforderten Detailumfang.
- c) Die Verifikationsmethoden für die Gefährdungskontrollmaßnahmen wurden vorgeschlagen.
- d) Die Definition der Sicherheitsanforderungen auf System- und nachgeordneten Ebenen wurde zum Abschluss gebracht.
- e) Die geforderten Tätigkeiten wurden in das Projektverifikationsprogramm aufgenommen.
- f) Abweichungen von den Sicherheitsanforderungen wurden identifiziert.

4.5.2.6 Kritisches Design-Review

Beim kritischen Design-Review muss der Lieferant den folgenden Nachweis führen:

- a) Die Ergebnisse der Sicherheitsanalysen an der in der vorangegangenen Phase erzielten Lösung wurden zur Verfügung gestellt, um verifizieren zu können, dass das Detaildesign mit den Projektsicherheitsanforderungen übereinstimmt und als Basis für die Herstellung von Qualifikationsmodellen benutzt werden kann.
- b) Alle an technischen Anforderungen vorgenommenen Änderungen wurden bewertet, um festzustellen, welche Änderungen sich daraus für die Gefährdungskontrollmaßnahmen ergeben.
- c) Die Sicherheitsverifikationsmethoden für alle Gefährdungskontrollmaßnahmen wurden vereinbart und die erforderlichen Tätigkeiten wurden in das Verifikationsprogramm aufgenommen.

4.5.2.7 Qualifikations-Review

Beim Qualifikations-Review muss der Lieferant den folgenden Nachweis führen:

- a) Alle Designqualifikationstätigkeiten in Bezug auf sicherheits- und bruchkritische Einheiten sowie sicherheitskritische Funktionen wurden der Review-Ebene entsprechend abgeschlossen und die zugehörigen Berichte wurden genehmigt.
- b) Alle sicherheitskritischen Einheiten und sicherheitskritischen Funktionen wurden qualifiziert.

4.5.2.8 Abnahme-Review

Beim Abnahme-Review muss der Lieferant den folgenden Nachweis führen:

- a) Alle späteren Änderungen an Design und technischen Anforderungen wurden auf eventuelle Folgeänderungen für Gefährdungskontrollmaßnahmen und deren Verifikationen bewertet.
- b) Die Verifikation für alle festgelegten Gefährdungskontrollmaßnahmen wurde abgeschlossen und gebilligt.
- c) Jede noch offene Verifikation wurde zu diesem Zeitpunkt im Verifikationskontroll-Dokument (VCD) vermerkt. Die Verifikationsverfahren für zum Zeitpunkt der Abnahme noch offene Verifikationen wurden qualifiziert und gegebenenfalls zur späteren Ausführung gegenseitig vereinbart.
- d) Alle sicherheitsbezogenen Nichtkonformitäten, Fehler, Ausfälle, Sonderfreigaben sowie Unfall/Zwischenfallberichte wurden formal gebilligt und abgeschlossen oder in einer Liste offener Punkte mit Angabe eventueller Einschränkungen dokumentiert.

4.5.2.9 Flugbereitschafts-Review

Beim Flugbereitschafts-Review muss der Lieferant den folgenden Nachweis führen:

- a) Das Verifikationskontroll-Dokument (VCD) weist keine weiteren offenen Verifikationen auf.
- b) Verifikationen, die plangemäß zu einem späteren Zeitpunkt durchzuführen sind, d. h. Spätzugangs-Inspektionen usw., wurden auf der Grundlage einer existierenden Startorganisationsvorschrift, welche von entsprechend angeleitetem Personal durchzuführen ist, förmlich abgeschlossen.
- c) Alle offenen Arbeiten im Zusammenhang mit sicherheitskritischen Einheiten und sicherheitskritischen Funktionen wurden abgeschlossen oder als Teil der normalen Startvorbereitungs-Tätigkeiten terminlich vorgesehen.
- d) Alle sicherheitsbezogenen Nichtkonformitäten, Fehler, Ausfälle, Sonderfreigaben und Unfall/Zwischenfallberichte wurden formal gebilligt und abgeschlossen.
- e) Alle sicherheitsrelevanten Fluganomalien an bereits früher im Flug eingesetzten ähnlichen Designs oder erneut im Flug eingesetzter Hardware wurden gelöst und zum Abschluss gebracht.

4.5.2.10 Betriebsbereitschafts-Review

Die Ergebnisse der Träger/Boden-Kompatibilitätstests und der Betriebsqualifikationstests (in deren Verlauf die Betriebsvorschriften verifiziert sein müssen) sind zu bewerten, um festzustellen, ob der kombinierte Betrieb von Träger und Bodeneinrichtungen nicht zu neuen Gefährdungen führt oder zusätzliche Kontrollmaßnahmen erfordert.

4.5.2.11 Startfreigabebesprechung

Ein Delta-Sicherheitsbericht ist vorzulegen, der den aktuellen Sicherheitsstatus dokumentiert, einschließlich aller potentiellen Auswirkungen von Countdown-Anomalien, Wetter- und Hardware- oder Personalzuständen. In dem Bericht ist anzugeben, ob der Sicherheitsstatus für den Startvorgang annehmbar ist. Der Bericht ist vom Kunden und der zuständigen Startorganisation zu überprüfen und formal zu billigen.

4.5.2.12 Orbitaltest-Review

Die Gültigkeit einer früheren Gefährdungs- und Risikobilligung ist unter Berücksichtigung aller eingeführten Design- oder Betriebsänderungen neu zu bestätigen. Dazu gehören auch eine Bewertung der fortdauernden Gültigkeit von früher gebilligten Betriebsreserven und Sonderfreigaben für sicherheitskritische Funktionen. Aktualisierte Sicherheitsanalysen sind, soweit erforderlich, zur Unterstützung der Entscheidung über die Zulassung des weiteren Gebrauchs des Systems zu liefern.

4.5.2.13 Bewertung des Lebensdauerendes

Ein Sicherheitsdatenpaket ist zu liefern, in dem der Sicherheitsstatus des Systems im Hinblick auf seine Tauglichkeit für die geplanten Lebensdauerabschluss- und Entsorgungsvorgänge und deren Konformität mit den geltenden Anforderungen, einschließlich jedweder internationaler Sicherheitsvorschriften, dokumentiert wird.

4.5.3 Sicherheitsprogramm

Das Sicherheitsprogramm ist je nach Projektkritikalität entweder:

- a) als Teil der planmäßigen Projektmeilenstein-Reviews; oder
- b) als Teil eines gezielten Sicherheits-Reviews zu überprüfen.

4.5.4 Sicherheitsdatenpaket

Der Lieferant muss das Sicherheitsdatenpaket ausarbeiten und bereitstellen. Der Inhalt des Sicherheitsdatenpaketes muss für jedes Projekt oder Programm von der zuständigen Sicherheitszertifizierungsstelle festgelegt werden.

4.6 Sicherheitsprogrammplan

4.6.1 Durchführung

Der Lieferant muss aufzeigen, wie das Sicherheitsprogramm im Sicherheitsprogrammplan nach ISO 14300-2 umgesetzt wird. Der Plan kann entweder als Teil eines Gesamtproduktsicherungsplans des Projekts oder als separater Sicherheitsprogramm-Teilplan aufgenommen werden.

4.6.2 Sicherheitsaktivitäten

Die Sicherheitsplanung muss die Sicherheitstätigkeiten für die Projektphasen nach ISO 14300-1 enthalten.

4.6.3 Definition

Der Plan muss Folgendes festlegen:

- a) die durchzuführenden Sicherheitsprogrammaufgaben;
- b) Personal/Lieferant, das/der für die Durchführung der Aufgaben zuständig ist;
- c) Zeitplan der Sicherheitsprogrammaufgaben bezogen auf Projektmeilensteine;
- d) Schnittstellen der Sicherheitsprogrammtätigkeiten mit dem Projektengineering und anderen Produktsicherungstätigkeiten;
- e) (gegebenenfalls durch Hinweis auf interne Verfahren) wie der Lieferant die Aufgaben erfüllen und ihre zufriedenstellende Erfüllung verifizieren wird.

4.6.4 Beschreibung

Der Plan muss beinhalten: Beschreibung der Projektsicherheitsorganisation, ihrer Zuständigkeiten und ihrer Arbeitsbeziehungen zu den Produktsicherungsdisziplinen Zuverlässigkeit, Instandhaltbarkeit, Softwareproduktsicherung, Teile, Materialien und Prozesse und Qualitätssicherung, zum Konfigurationsmanagement und zur Systemtechnik sowie zu Design und anderen Projektfunktionen und Unternehmensabteilungen.

4.6.5 Sicherheits- und Projektengineering-Tätigkeiten

Der Plan muss aufzeigen, wie die Projektsicherheitsorganisation die parallel laufenden Sicherheits- und Projektengineering-Tätigkeiten zur ständigen Unterstützung des Projektdesign- und -entwicklungsprozesses verwirklichen wird.

4.6.6 Lieferanten und Unterlieferanten

Der Plan muss beschreiben, wie die sicherheitsbezogenen Tätigkeiten und Anforderungen für die Unterlieferanten und Lieferanten festgelegt und an ihren Standorten überwacht werden. Es sind nur solche Anforderungen verbindlich vorzugeben, die für die Tätigkeiten und Verantwortlichkeiten der Unterlieferanten und Lieferanten relevant sind.

4.6.7 Einhaltung

Der Plan muss Vorkehrungen zur Sicherstellung der Einhaltung der Sicherheitsanforderungen und -bestimmungen, die für jede zusätzliche im Projektverlauf zu benutzende Einrichtung und Dienstleistung gelten, vorsehen.

4.7 Sicherheitszertifizierung

- a) Für alle Projekte muss zertifiziert werden, dass die Flug- und Bodensystemprodukte sicher sind und den Anforderungen dieser Norm sowie allen geltenden projektspezifischen Sicherheitsanforderungen entsprechen.
- b) Der Zertifizierungsprozess muss abgeschlossen sein, bevor eine Auslieferung an irgendeine Partei, außer dem Käufer, erfolgt.
- c) Die Zertifizierung muss einen Hinweis enthalten, dass noch offene Verifikationen gemäß dem geführten Verifikations-Nachweisverzeichnis abgeschlossen werden und die sichere Weiterführung auf dem Gelände von Drittparteien nicht beeinträchtigen.
- d) Bei jedem Projekt ist der Kunde, der detaillierte sicherheitstechnische Anforderungen festlegt oder verbindlich vorgibt, die zuständige Sicherheitszertifizierungsstelle oder Teil davon.
- e) Die Projektorganisation muss der zuständigen Zertifizierungsstelle alle sicherheitsbezogenen Informationen zur Verfügung stellen, die erforderlich sind, um die Sicherheitskonformitätserklärung billigen und verstehen zu können.

4.8 Sicherheitstraining

4.8.1 Bestandteil

- a) Das Sicherheitstraining ist Bestandteil des nach ISO 14300-1 und ISO 14300-2 geforderten Gesamttrainings.
- b) Jedes sicherheitsbezogene Training von Personen, die — ständig oder vorübergehend — mit Produkten arbeiten, die Gefährdungsmerkmale haben können, hat drei Hauptaspekte zum Inhalt:
 - 1) allgemeine Übersicht zur Bewusstseinsbildung über Sicherheitsmaßnahmen, die in einem bestimmten Ort oder Arbeitsumfeld zu treffen sind;
 - 2) technisches Grundtraining in den geforderten Sicherheitstechniken und Fertigkeiten, z. B. Prüfung, Test, Instandhaltung oder Integration, die zur Erfüllung der betreffenden Aufgabenstellung erforderlich sind;
 - 3) produktspezifisches Training, das sich schwerpunktmäßig mit den für das Produkt spezifischen Gefährdungen befasst.

4.8.2 Teilnahme

Die Teilnahme an den allgemeinen Einweisungen ist für alle Personen verbindlich, die Zugang zu dem Bereich haben müssen, in dem das Produkt be- oder verarbeitet wird.

4.8.3 Eingehendes technisches Training

Ein eingehendes technisches Training ist dem Projektengineering- und Sicherheitspersonal zu erteilen, das mit gefährdenden Produkten zu tun hat.

4.8.4 Produktspezifisches Training

Ein produktspezifisches Training ist von Sicherheitsexperten allen neuen Projektingenieuren sowie den Flug- und Bodenmannschaften zu erteilen.

4.8.5 Aufzeichnungen

Aufzeichnungen über die Personen, die ein Training erhalten haben, sind zu führen.

4.8.6 Identifizierung

Wenn ein Sicherheitstraining für die Flugbetriebsmannschaft oder für das Missionskontrollpersonal als erforderlich angesehen wird, ist dies dem Kunden unter Angabe von Art und Umfang des erforderlichen Trainings mitzuteilen. Der Lieferant muss die Verwirklichung des Trainingsprogramms, wie vom Kunden festgelegt, unterstützen.

4.9 Berichterstattung und Untersuchung von Unfällen/Zwischenfällen

- a) Der Lieferant muss dem Kunden über alle Unfälle und Zwischenfälle berichten, die während der Projekt-tätigkeiten, die in seinem Verantwortungsbereich oder dem seiner Unterlieferanten liegen, auftreten.
- b) Der Sicherheitsvertreter des Lieferanten ist verantwortlich für die Untersuchung aller zu meldenden Zwischenfälle und für die Unterstützung des Kunden bei der Untersuchung von Unfällen, wie dies angewiesen wird.

4.10 Sicherheitsdokumentation

4.10.1 Allgemeines

Der Lieferant muss sicherheitsrelevante Daten zur Unterstützung der Reviews und der Sicherheitszertifizierung bereithalten.

4.10.2 Kundenzugang

Während der beim Lieferanten abgehaltenen Audits, Sicherheits-Reviews und Besprechungen müssen die in der Sicherheitserfahrungsdatei enthaltenen Daten dem Kunden auf Wunsch zugänglich gemacht werden.

4.10.3 Lieferant

Der Lieferant muss die Projektdokumentation einschließlich Spezifikationen, Zeichnungen, Analysen, Verfahren und Berichten, Nichtkonformitätenberichten, Fehler-/Ausfallberichten, Sonderfreigaben und Dokumentationsänderungen einem Review unterziehen, um Folgendes zu überprüfen oder ihre Auswirkung zu beurteilen auf:

- a) Umsetzung der Sicherheitsanforderungen und Gefährdungs- und Risikokontrollmaßnahmen;
- b) Einarbeitung der Gefährdungs- und Risikokontrollmaßnahmen in das Design oder Verifikationsprogramm;

- c) Abschluss der Verifikationstätigkeiten;
- d) Design- und Betriebssicherheit des Systems;
- e) Gültigkeit der durchgeführten und dokumentierten Sicherheitsanalysen.

4.10.4 Dokumentation

- a) Es sind Aufzeichnungen über die überprüften Dokumente zu führen.
- b) Die Sicherheitsdokumentation ist gegebenenfalls zu aktualisieren, um dem neuesten Stand zu entsprechen.
- c) Der Lieferant muss zertifizieren, dass die Sicherheitsdokumentation genau, gültig, umfassend und vollständig ist, bevor sie auf dem Startgelände weitergeführt wird.

4.10.5 Sicherheitsdatenpaket

- a) Der Lieferant muss für die Reviews ein Sicherheitsdatenpaket vorlegen (siehe 4.5.4). Dies kann ein separates Paket oder Bestandteil des Gesamtdatenpaketes sein, wenn das Sicherheits-Review Teil eines Gesamtprojektreviews ist.
- b) Der Inhalt des Datenpaketes ist zu spezifizieren, um für die inhaltliche Bestimmung von Sicherheitsdatenpaketen herangezogen zu werden.
- c) Die Design- und Betriebsgrundlage, die Gegenstand des Sicherheitsdatenpaketes ist, muss durch Bezug auf die entsprechende Dokumentation festgelegt werden.
- d) Alle bei früheren Sicherheitsreviews geforderten Daten sind in das Sicherheitsdatenpaket aufzunehmen.
- e) Der Lieferant muss die Sicherheitsdaten, die sich auf die einzelnen Subsysteme oder Geräte des Systems beziehen, in das beim Sicherheitsreview vorzulegende Sicherheitsdatenpaket einbeziehen.
- f) Alle Sicherheitsdaten müssen vom Sicherheitsdatenpaket zurückverfolgbar sein und für das Review zur Verfügung stehen, sofern zutreffend.

4.10.6 Sicherheitsbezogene Sonderfreigabe (vor und nach Realisierung)

4.10.6.1 Abweichung

Sicherheitsanforderungen, die nicht eingehalten werden können, sind zu identifizieren, und es muss eine Sonderfreigabe erwirkt werden.

4.10.6.2 Beschreibung, Analyse und Begründung

Die Sonderfreigabe muss darlegen, warum die Anforderung nicht eingehalten werden kann, und eine ausreichende Analyse und Begründung zur Unterstützung der Abweichung von der Anforderung liefern.

4.10.6.3 Identifizierung und Review

Der Lieferant muss alle Sonderfreigaben (vor und nach Realisierung) identifizieren, die die anzuwendenden Projektsicherheitsanforderungen beeinflussen. Diese Sonderfreigaben sind vom Projektsicherheitsvertreter zu überprüfen, um sicherzustellen, dass eventuelle Auswirkungen auf die Sicherheit vollständig analysiert und jede vom Lieferanten als vertretbar angesehene Abweichung ausreichend begründet ist.

4.10.6.4 Bewertung der Sonderfreigaben

Die kumulierten Sonderfreigaben (vor und nach Realisierung), die die Sicherheit betreffen, sind zu bewerten, um sicherzustellen, dass die Auswirkungen einzelner Sonderfreigaben die für die Annahme anderer Sonderfreigaben gelieferte Begründung nicht ungültig machen. Der Lieferant muss eine Übersichtsliste führen, in der alle überprüften sicherheitsbezogenen Sonderfreigaben festgehalten sind.

4.10.6.5 Review und Disposition

Sonderfreigaben, die Projektsicherheitsanforderungen oder sicherheitskritische Funktionen und Einheiten betreffen und vom Lieferanten als annehmbar angesehen werden, müssen von der zuständigen Sicherheitsstelle des Kunden überprüft und entschieden werden.

4.10.6.6 Genehmigung der Sicherheitsstelle

Die sicherheitsbezogenen Sonderfreigaben bedürfen der Genehmigung durch die zuständigen Sicherheitszertifizierungsstellen einschließlich der zuständigen Startorganisation, soweit wie angemessen.

4.10.7 Verifikationskontroll-Dokument

Ein Verifikationskontroll-Dokument (VCD) ist zu führen, aus dem eindeutig die zum Abschluss führenden Schritte für die Verifikationspunkte nach dem Gefährdungsbericht hervorgehen. Sobald die Verifikationsmethoden zur gegenseitigen Zufriedenheit der Projekt- und Zertifizierungsstellen in den Gefährdungsberichten dokumentiert sind, billigt das Verifikations-Nachweisverzeichnis den zugehörigen Beglaubigungseintrag.

4.10.8 Erfahrungsdatei

- a) Der Lieferant muss die im Projektverlauf gewonnenen Sicherheitserfahrungen sammeln. Der Lieferant muss sicherstellen, dass die gewonnenen Erfahrungen, soweit sie von Belang sind, noch während der Projektlaufzeit in das Projekt einfließen.
- b) Die gewonnenen Sicherheitserfahrungen müssen mindestens Folgendes erfassen:
 - 1) Auswirkungen neu vorgegebener Anforderungen;
 - 2) Bewertung aller Funktionsstörungen, Unfälle, Anomalien, Sonderfreigaben;
 - 3) Effektivität der Sicherheitsstrategien des Projektes;
 - 4) neue Sicherheitswerkzeuge und -methoden, die entwickelt oder dargelegt wurden;
 - 5) Vergleich von durchgeführten wirksamen und unwirksamen Verifikationen;
 - 6) Änderungsvorschläge zu Sicherheitsgrundsätzen, Sicherheitsstrategie oder sicherheitstechnischen Anforderungen, einschließlich Begründung.

5 Sicherheitstechnik

5.1 Sicherheitstechnische Grundsätze

5.1.1 Allgemeines

Die Sicherheit ist integraler Bestandteil aller Produktsicherungs- und Engineering-Tätigkeiten des Projektes und somit keine isolierte Tätigkeit. Die Qualität aller Arbeiten im Zusammenhang mit der Sicherheitstechnik beruht auf der Sicherstellung, dass Design, Qualifikation, Herstellung und Betrieb des Systems den Produktsicherungsanforderungen entsprechen.

5.1.2 Elemente

Die Sicherheitstechnik umfasst das Management der Gefährdungs- und Risikoreduzierungsprozesse, Gefährdungs- und Risikopotentialbewertung, Design-Sicherung und Gefährdungs- und Risikokontrolltätigkeiten.

5.1.3 Gewonnene Sicherheitserkenntnisse (lessons learnt)

Die während des Designprozesses gewonnenen Erkenntnisse sollten weitgehend zur Anwendung kommen.

5.2 Sicherheitsbezogene Designgrundsätze

5.2.1 Menschliche Überlegung

Die Bewahrung der Sicherheit des Personals muss bei der Entwicklung und dem Betrieb von Raumfahrtssystemen die höchste Priorität haben.

5.2.2 Designauswahl

Hauptziel in der Designphase ist die Sicherstellung einer inhärenten Sicherheit durch Auswahl angemessener Designmerkmale. Schadensbegrenzung, Eingrenzung und Isolierung potentieller Gefährdungen sind in die Designüberlegungen einzubeziehen.

5.2.3 Gefährdungsbeseitigungs- und -kontrollmaßnahmen

Bei den identifizierten Gefährdungen, Gefährdungszuständen und Funktionen, deren Ausfall/Fehler Gefährdungsfolgen hat, ist die folgende Reihenfolge der Tätigkeiten einzuhalten:

a) Gefährdungsbeseitigung

Gefährdungen und Gefährdungszustände müssen entsprechend den Projektauflagen und Missionszielen über die Auswahl von Design-Technologie, Design-Architektur und Betriebsmerkmalen aus den Design- und Betriebskonzepten beseitigt werden.

b) Gefährdungsminimierung

Können Gefährdungen und Gefährdungszustände nicht beseitigt werden, ist die Schwere der damit verbundenen Gefährdungsereignisse und -folgen entsprechend den Projektauflagen und Missionszielen durch Auswahl der am wenigsten gefährdenden Design-Architektur, Design-Technologien und Betriebsmerkmale zu minimieren.

c) Gefährdungskontrolle — Sicherheitseinrichtungen

Gefährdungen, die über die Designauswahl nicht beseitigt werden können, müssen reduziert und mit Hilfe automatischer Sicherheitseinrichtungen als Teil des Systems, Subsystems oder Geräts kontrollierbar gemacht werden.

d) Gefährdungskontrolle — Warnvorrichtungen

Ist es nicht möglich, das Vorhandensein oder Eintreten bekannter Gefährdungen auszuschließen oder automatische Sicherheitseinrichtungen einzusetzen, sind Vorrichtungen zur rechtzeitigen Erkennung des Zustandes und Erzeugung eines geeigneten Warnsignals zu verwenden, gekoppelt mit Notfall-Kontrollen, bestehend aus Korrekturmaßnahmen durch das Betriebspersonal, um das betroffene Subsystem zu sichern oder abzuschalten.

e) Gefährdungskontrolle — Besondere Vorschriften

- 1) Ist es nicht möglich, das Ausmaß einer Gefährdung über das Design, Sicherheitseinrichtungen oder Warnvorrichtungen zu reduzieren, sind besondere Vorschriften zu entwickeln, um den Gefährdungszuständen zur Erhöhung der Sicherheit für die Besatzung entgegenzuwirken.

- 2) Besondere Vorschriften können Not- und Störfallvorschriften, Verfahrensvorschriften oder die Anwendung eines kontrollierten Instandhaltungsprogramms beinhalten.
- 3) Besondere Vorschriften sind durch Tests zu qualifizieren, und das Personal ist entsprechend einzuweisen.
- 4) Von den verfügbaren Gefährdungskontroll- und Risikoreduzierungsmaßnahmen sind die besonderen Vorschriften am wenigsten effektiv. Vorrang ist daher der Gefährdungskontrolle durch Anwendung der alternativen Gefährdungskontrollmaßnahmen in der angegebenen Reihenfolge zu geben.
- 5) Die Anforderung für die Gefährdungserkennung, -signalisierung und -sicherung durch die Besatzung zur Kontrolle zeitkritischer Gefährdungen ist zu minimieren und nur dann umzusetzen, wenn es keine alternative Lösung zur Reduzierung oder Kontrolle von Gefährdungszuständen gibt.
- 6) Um den Einsatz von Echtzeit-Monitoring-, Gefährdungserkennungs- und -sicherungssystemen für die Gefährdungskontrolle zulassen zu können, muss die Verfügbarkeit einer ausreichenden Reaktionszeit für die Besatzung verifiziert werden. Abnehmbare Sicherungsverfahren müssen entwickelt und verifiziert werden, und das Personal ist entsprechend einzuweisen.
- 7) Physische Barrieren, sichere Trennabstände, Beschränkung des Personals mit Befugnis für Zugangskontrollen, Fernüberwachung, Energieabschaltverfahren und zeitlich begrenzte Belastung sind als Mittel zur Gefährdungseindämmung und Risikominderung in Betracht zu ziehen.

5.2.4 Umweltverträglichkeit

- a) Das Systemdesign muss unter den für das Projekt definierten ungünstigsten natürlichen und induzierten Umgebungsbedingungen die geltenden Sicherheitsanforderungen erfüllen.
- b) Design- und Leistungsreserven sind festzulegen und anzuwenden unter Berücksichtigung der ungünstigsten Kombinationen von induzierten und natürlichen Umgebungsbedingungen und Betriebsmerkmalen.

5.2.5 Sicher ohne externe Dienste

Hängt der sichere Betrieb des Systems von externen Diensten (z. B. Energieversorgung) ab, muss das Systemdesign so ausgelegt sein, dass aus dem Verlust solcher Dienste (zumindest für einen bestimmten, für jedes Projekt festzulegenden Zeitraum) keine kritischen oder katastrophalen Folgen entstehen.

5.2.6 „Fail Safe“-Design

Das System und seine Bestandteile müssen so ausgelegt sein, dass bei Ausfällen das System in einen „sicheren Zustand“ übergeht.

5.2.7 Gefährdungserkennung — Signalisierung und Sicherung

- a) Bei bemannten Raumflugsystemen müssen Sicherheitsüberwachungs-, Anzeige-, Alarm- und Sicherungseinrichtungen vorhanden sein. Diese Einrichtungen müssen die notwendigen Informationen liefern, die es der Besatzung und dem Systembetriebspersonal ermöglichen, eventuell erforderliche Maßnahmen zum Schutz von Personen vor den Folgen von Ausfällen innerhalb sicherheitskritischer Funktionen und vor dem Ausfall von Gefährdungskontrollmaßnahmen zu ergreifen.
- b) Das Systemdesign muss die Möglichkeit bieten, Fehler zu erkennen, die zu einer Verschlechterung der Fehlertoleranz für die Gefährdungserkennungs-, -signalisierungs- und -sicherungsfunktion führen. Die Leistung dieser Funktionen muss nach deren Verwirklichung während der Flug- und Bodenbetriebsphasen verifizierbar sein.
- c) Die Not-, Vorsicht- und Warnfunktion muss die Not-, Vorsicht- und Warnsituationen erkennen und der Besatzung und dem Systembetriebspersonal melden.
- d) Sicherungsfunktionen und -einrichtungen müssen zur Eingrenzung oder Kontrolle von Not-, Vorsicht- und Warnsituationen vorhanden sein.
- e) Vorkehrungen zur Verfolgung der Ausführung der Sicherungsfunktion müssen vorgesehen sein.

- f) Für Notsituationen muss es gezielte Sicherungsfunktionen geben. Die Kontrolle von Vorsicht- und Warnsituationen über System-Rekonfiguration oder gezielte Sicherungsfunktionen ist je nach Fall zulässig.
- g) Kein einzelner Ausfall darf zum Verlust der Not- und Warnfunktion führen.
- h) Wenn durch den Betrieb eines Sicherungssystems neue Gefährdungen eingebracht werden, muss zumindest die unbeabsichtigte Aktivierung des Sicherungssystems in Übereinstimmung mit den Fehler-toleranzanforderungen unter Kontrolle gebracht werden.
- i) Kein einzelner Ausfall darf den Verlust der Not- und Warnfunktionen zusammen mit den überwachten Funktionen zur Folge haben.
- j) Not-, Warn- und Vorsichtdaten- und Grenzüberschreitungsmeldungen und Sicherungsbefehle müssen Vorrang vor anderen Datenverarbeitungs- und Befehlsfunktionen haben.
- k) Wenn Systeme oder Elemente in andere Systeme oder Elemente integriert oder mit diesen gekoppelt werden, muss die Not-, Warn-, Vorsicht- und Sicherungsfunktion es den verantwortlichen Kontrollstellen ermöglichen, die jeweiligen Parameter zu verfolgen und anzuzeigen und die entsprechenden Sicherungsfunktionen zu überwachen.
- l) Statusinformationen über die Not-, Warn- und Vorsichtparameter müssen in den Start- und Missionsleit-zentren „echtzeitnah“ während der relevanten Betriebsphasen zur Verfügung stehen und angezeigt werden. Die Besatzung muss die Möglichkeit haben, den Status der Not-, Warn- und Vorsichtparameter nichtbemannter Systeme oder Elemente vor dem Ankoppeln an bemannte Systeme in „Echtzeit“ festzu-stellen und zu verfolgen.

5.2.8 Zugang

Das Projektprodukt muss so ausgelegt sein, dass jeder während des Flug- oder Bodenbetriebs erforderliche Zugang zu einzelnen Produkten mit einem Minimum an Risiko für das Personal vollzogen werden kann.

5.3 Sicherheitsrisikoreduzierung und -kontrolle

5.3.1 Schweregrad

- a) Der Schweregrad der identifizierten Gefährdungseignisse ist nach folgenden Kategorien einzustufen (siehe Tabelle 1):

Tabelle 1 — Schweregrad der Gefährdungen und Folgen (1)

Schweregrad		Folge	
1)	Katastrophale Gefährdungen	i)	Verlust menschlichen Lebens, lebensbedrohende oder zu dauernder Arbeitsunfähigkeit führende Verletzung oder Berufskrankheit, Verlust eines Elementes eines angrenzenden bemannten Flugsystems;
		ii)	Verlust von Startplatzeinrichtungen;
		iii)	schädliche Langzeitauswirkungen für die Umwelt.
2)	Kritische Gefährdungen	i)	zu vorübergehender Arbeitsunfähigkeit führende, jedoch nicht lebensbedrohende Verletzung oder vorübergehende Berufs-krankheit;
		ii)	Verlust oder größere Beschädigung des Flugsystems, von Hauptelementen des Flugsystems oder von Bodeneinrich-tungen;
		iii)	größere Beschädigung von öffentlichem oder privatem Eigen-tum; oder
		iv)	größere schädliche Auswirkungen für die Umwelt.