

DIN EN 16602-40

ICS 49.140

Einsprüche bis 2017-09-14
Vorgesehen als Ersatz für
DIN EN ISO 14620-1:2005-06

Entwurf

**Raumfahrtsysteme –
Sicherheit;
Englische Fassung FprEN 16602-40:2017**

Space product assurance –
Safety;
English version FprEN 16602-40:2017

Systèmes spatiaux –
Sécurité;
Version allemande FprEN 16602-40:2017

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2017-07-14 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an nl@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Luft- und Raumfahrt (NL), 10772 Berlin, Burggrafenstr. 6, 10787 Berlin.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 83 Seiten

DIN-Normenausschuss Luft- und Raumfahrt (NL)

Nationales Vorwort

Dieses Dokument (FprEN 16602-40:2017) wurde im Technischen Komitee CEN/CLC/TC 5 „Raumfahrt“, dessen Sekretariat von DIN (Deutschland) gehalten wird, erarbeitet.

Das zuständige deutsche Normungsgremium ist der Arbeitsausschuss NA 131-06-02 AA „Interoperabilität von Informations-, Kommunikations- und Navigationssystemen“ im DIN-Normenausschuss Luft- und Raumfahrt (NL).

Dieses Dokument (FprEN 16602-40:2017) basiert auf ECSS-Q-ST-40C Rev.1.

Dieses Dokument enthält unter Berücksichtigung des DIN-Präsidialbeschlusses 1/2004 nur die englische Originalfassung von FprEN 16602-40:2017.

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

Änderungen

Gegenüber DIN EN ISO 14620-1:2005-06 wurden folgende Änderungen vorgenommen:

- a) Norm-Nummer geändert;
- b) Inhalt technisch überarbeitet.

Nationaler Anhang NA (informativ)

Begriffe und Abkürzungen

Die Benummerung der folgenden Begriffe und Abkürzungen ist identisch mit der Benummerung in der englischen Fassung.

3.1 Begriffe aus anderen Normen

a) Für die Anwendung dieses Dokuments gelten die Begriffe nach ECSS-S-ST-00-01 (Unterschiede bei den Begriffen „ausfallsicher“ und „System“, siehe 3.2), insbesondere die folgenden Begriffe:

- 1) Unfall;
- 2) Ausfall;
- 3) katastrophal;
- 4) kritisch <KONTEXT: Sicherheit>;
- 5) Notfall;
- 6) Bodensegment;
- 7) Gefährdung;
- 8) Gefährdungsereignis;
- 9) Sperre;
- 10) Risiko;
- 11) Sicherheit;
- 12) Sicherungsmaßnahme;
- 13) Schweregrad;
- 14) sicherheitskritische Funktion;
- 15) Raumsegment;
- 16) System.

3.2 Für diese Norm spezifische Begriffe

3.2.1

Ursache

Handlung oder Bedingung, durch die ein Gefährdungsereignis ausgelöst wird (ein Initialereignis)

Anmerkung 1 zum Begriff: Die Ursache kann das Ergebnis eines Ausfalls, menschlichen Versagens, eines fehlerhaften Designs, einer induzierten oder natürlichen Umgebung, einer Systemkonfiguration oder einer oder mehrerer Betriebsart(en) sein.

Anmerkung 2 zum Begriff: Diese Definition gilt nur für diese Norm bei Verwendung im Kontext der Gefahrenanalyse.

3.2.2

Kritikalität

Klassifizierung einer Funktion oder einer Software, Hardware oder Operation entsprechend dem Schweregrad der möglichen Konsequenzen ihres Ausfalls

Anmerkung 1 zum Begriff: Siehe 6.4.1 und 6.5.6.

Anmerkung 2 zum Begriff: Dieser Begriff der Kritikalität, angewendet auf eine Funktion oder eine Software, Hardware oder Operation, berücksichtigt nur den Schweregrad, im Unterschied zur Kritikalität eines Ausfalls oder einer Ausfallart (oder eines Risikos), welche auch die Wahrscheinlichkeit des Auftretens berücksichtigt.

3.2.3

ausfallsicher

Eigenschaft eines Systems (oder Systemteils), die verhindert, dass es bei seinem Ausfall zu kritischen oder katastrophalen Konsequenzen kommt

3.2.4

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

3.2.5

gefährlicher Befehl

Befehl, der eine Sperre einer sicherheitskritischen Funktion beseitigen oder ein gefährliches Subsystem aktivieren kann

3.2.6

Gefahrenreduzierung

Prozess der Eliminierung oder Minimierung und Abwehr von Gefahren

3.2.7

Gefahrenszenario

Abfolge von Ereignissen von der auslösenden Ursache zur unerwünschten Konsequenz

Anmerkung 1 zum Begriff: Die Ursache kann ein einzelnes Initialereignis, eine zusätzliche Handlung oder die Änderung einer Bedingung sein, die ein verborgenes Problem aktiviert.

3.2.8

Fehlverhalten des Betriebspersonals

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

[QUELLE: ISO 14620-1]

3.2.9

Sicherheitszulassungsgremium

Instanzen, die detaillierte technische Sicherheitsanforderungen, für ein bestimmtes Projekt, festlegt oder aufstellt und deren Implementierung bewertet

3.2.10

Sicherheitsaudit

unabhängige Prüfung, um festzustellen, ob die spezifischen Verfahrensweisen im Rahmen der Sicherheitsanforderungen wirksam implementiert werden und zur Umsetzung der spezifizierten Ziele geeignet sind

3.2.11

Sicherheitsrisiko

Maß für die Bedrohung der Sicherheit durch Gefahrenszenarien und ihre Konsequenzen

Anmerkung 1 zum Begriff: Ein Sicherheitsrisiko ist immer mit einem bestimmten Gefahrenszenario oder einer bestimmten Gruppe von Gefahrenszenarien verbunden. Das mit einem einzelnen Gefahrenszenario verbundene Risiko heißt Einzelrisiko. Das mit einer Gruppe von Gefahrenszenarien mit der gleichen Hauptkonsequenz verbundene Risiko heißt Gesamtrisiko.

Anmerkung 2 zum Begriff: Die Stärke eines Sicherheitsrisikos ergibt sich aus dem Schweregrad kombiniert mit der Wahrscheinlichkeit der Konsequenz.

3.2.12

Sicherheitsstatusparameter

Parameter, der eine Beurteilung des Status einer implementierten Gefahrenabwehr ermöglicht

3.3 Abkürzungen

Für die Anwendung dieses Dokuments gelten die Abkürzungen nach ECSS-S-ST-00-01 und die folgenden Abkürzungen:

Abkürzung	Bedeutung	
------------------	------------------	--

AR	Abnahmebewertung	(en: acceptance review)
CCB	Konfigurationslenkungsausschuss	(en: configuration control board)
CDR	Bewertung des kritischen Designs	(en: critical design review)
CE	CE-Kennzeichnung (Europäische Konformität)	(fr: Conformité Européenne)
CRR	Inbetriebnahme-Abschlussbewertung	(en: commissioning result review)
EEE	elektronisch, elektrisch, elektromechanisch	(en: electronic, electrical, electromechanical)
ELR	Ausmusterungsbewertung	(en: end-of-life review)
EMC	elektromagnetische Verträglichkeit	(en: electro-magnetic compatibility)
FMEA	Fehlermöglichkeits- und Einflussanalyse	(en: failure modes and effects analysis)
FMECA	Fehlermöglichkeits-, Einfluss- und Kritikalitäts-Analyse	(en: failure modes, effects and criticality analysis)
FSDP	Flugsicherheitsdatenpaket	(en: flight safety data package)
FRR	Bewertung der Flugbereitschaft	(en: flight readiness review)
FTA	Fehlerbaumanalyse	(en: fault tree analysis)
GSDP	Bodensicherheitsdatenpaket	(en: ground safety data package)

GSE	Luftfahrt-Bodengerät	(en: ground support equipment)
IEC	Internationale Elektrotechnische Kommission	(en: International Electrotechnical Commission)
LRR	Bewertung der Startbereitschaft	(en: launch readiness review)
LVD	Niederspannungsrichtlinie	(en: low voltage directive)
MIP	obligatorischer Prüfpunkt	(en: mandatory inspection point)
NRB	Ausschuss für die Bewertung der Nichtkonformität	(en: nonconformance review board)
NUREG-CR	Auftragnehmerbericht der US-Atomaufsichtsbehörde	(en: US Nuclear Regulatory Commission contractor report)
ORR	Bewertung der Betriebsbereitschaft	(en: operational readiness review)
PDR	Bewertung des vorläufigen Designs	(en: preliminary design review)
PED	Druckgeräte-richtlinie	(en: pressure equipment directive)
PGSE	Druck-Bodendienstgerät	(en: pressure ground support equipment)
PRR	Bewertung der vorläufigen Anforderungen	(en: preliminary requirements review)
QR	Qualifikationsbewertung	(en: qualification review)
R&TTE	Funkanlagen & Telekommunikationsendeinrichtungen	(en: radio & telecommunications terminal equipment)
RoHS	Beschränkung der Verwendung bestimmter gefährlicher Stoffe (in Elektro- und Elektronikgeräten)	(en: restriction of certain hazardous substances)
SDP	Sicherheitsdatenpaket	(en: safety data package)
SRR	Bewertung der Systemanforderungen	(en: system requirements review)
SVTL	Sicherheitsprüfprotokoll	(en: safety verification tracking log)
TRB	Ausschuss für die Bewertung der Prüfung	(en: test review board)
WEEE	Elektro- und Elektronikaltgeräte	(en: waste electrical and electronic equipment)

English version

Space product assurance - Safety

Systèmes spatiaux - Sécurité

Raumfahrtssysteme - Sicherheit

This draft European Standard is submitted to CEN members for unique acceptance procedure. It has been drawn up by the Technical Committee CEN/CLC/TC 5.

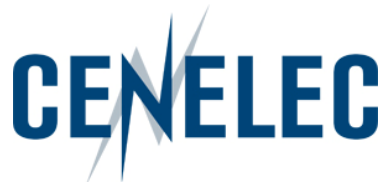
If this draft becomes a European Standard, CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

This draft European Standard was established by CEN and CENELEC 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, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

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

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



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

Table of contents

European foreword.....	7
1 Scope.....	8
2 Normative references	9
3 Terms, definitions and abbreviated terms.....	10
3.1 Terms from other standards.....	10
3.2 Terms specific to the present standard	10
3.3 Abbreviated terms.....	12
3.4 Nomenclature	13
4 Safety principles.....	14
4.1 Objective	14
4.2 Policy.....	14
4.2.1 General	14
4.2.2 Implementation	14
4.3 Safety programme	15
5 Safety programme	16
5.1 Scope	16
5.2 Safety programme plan	16
5.3 Conformance	17
5.4 Safety organization	17
5.4.1 Safety manager.....	17
5.4.2 Safety manager access and authority	17
5.4.3 Safety audits	18
5.4.4 Approval of documentation.....	18
5.4.5 Approval of hazardous operations.....	18
5.4.6 Representation on boards	18
5.4.7 Safety approval authority.....	19
5.5 Safety risk assessment and control	19
5.6 Safety critical items.....	19
5.7 Project phases and safety review cycle	19

5.7.1	Safety program tasks and reviews	19
5.7.2	Progress meetings	23
5.7.3	Safety reviews.....	23
5.8	Safety compliance demonstration	24
5.9	Safety training.....	24
5.9.1	General	24
5.9.2	Product specific training	24
5.9.3	General awareness briefings.....	25
5.9.4	Basic technical training	25
5.9.5	Training records	25
5.10	Accident-incident reporting and investigation	25
5.11	Safety documentation	25
5.11.1	General	25
5.11.2	Safety data package	26
5.11.3	Safety deviations and waivers	26
5.11.4	Safety lessons learned.....	27
5.11.5	Documentation of safety critical items	27
6	Safety engineering	28
6.1	Overview	28
6.2	Safety requirements identification and traceability	28
6.3	Safety design objectives	28
6.3.1	Safety policy and principles.....	28
6.3.2	Design selection.....	28
6.3.3	Hazard reduction precedence	29
6.3.4	Environmental compatibility.....	31
6.3.5	External services.....	31
6.3.6	Hazard detection - signalling and safing.....	31
6.3.7	Space debris mitigation.....	32
6.3.8	Atmospheric re-entry.....	32
6.3.9	Safety of Earth return missions	32
6.3.10	Safety of human spaceflight missions	33
6.3.11	Access	33
6.4	Safety risk reduction and control.....	33
6.4.1	Severity of hazardous event and function criticality	33
6.4.2	Failure tolerance requirements.....	35
6.4.3	Design for minimum risk.....	36
6.4.4	Probabilistic safety targets	37

6.5	Identification and control of safety-critical functions	38
6.5.1	Identification.....	38
6.5.2	Inadvertent operation	38
6.5.3	Status information	38
6.5.4	Safe shutdown and failure tolerance requirements.....	38
6.5.5	Electronic, electrical, electromechanical components.....	39
6.5.6	Software functions.....	39
6.6	Operational Safety	41
6.6.1	Basic requirements	41
6.6.2	Flight operations and mission control	41
6.6.3	Ground operations	42
7	Safety analysis requirements and techniques.....	45
7.1	Overview	45
7.2	General.....	45
7.3	Assessment and allocation of requirements.....	46
7.3.1	Safety requirements	46
7.3.2	Additional safety requirements	46
7.3.3	Define safety requirements - functions	46
7.3.4	Define safety requirements - subsystems.....	46
7.3.5	Justification	46
7.3.6	Functional and subsystem specification	46
7.4	Safety analyses during the project life cycle.....	46
7.5	Safety analyses	47
7.5.1	General	47
7.5.2	Hazard analysis	47
7.5.3	Safety risk assessment	48
7.5.4	Supporting assessment and analysis	48
8	Safety verification.....	52
8.1	General.....	52
8.2	Hazard reporting and review	52
8.2.1	Hazard reporting system	52
8.2.2	Safety status review	52
8.2.3	Documentation.....	52
8.3	Safety verification methods.....	53
8.3.1	Verification engineering and planning	53
8.3.2	Methods and reports	53
8.3.3	Analysis	53

8.3.4	Inspections.....	53
8.3.5	Verification and approval.....	54
8.4	Verification of safety-critical functions	54
8.4.1	Validation	54
8.4.2	Qualification	54
8.4.3	Failure tests	55
8.4.4	Verification of design or operational characteristics.....	55
8.4.5	Safety verification testing	55
8.5	Hazard close-out	55
8.5.1	Safety assurance verification	55
8.5.2	Hazard close-out verification	56
8.6	Declaration of conformity of ground equipment.....	56
Annex A (informative) Analyses applicability matrix		57
Annex B (normative) Safety programme plan - DRD.....		59
B.1	DRD identification	59
B.1.1	Requirement identification and source document.....	59
B.1.2	Purpose and objective.....	59
B.2	Expected response	59
B.2.1	Contents	59
B.2.2	Special remarks	60
Annex C (normative) Safety verification tracking log (SVTL) DRD		61
C.1	DRD identification	61
C.1.1	Requirement identification and source document.....	61
C.1.2	Purpose and objective.....	61
C.2	Expected response	61
C.2.1	Contents	61
C.2.2	Special remarks	63
Annex D (normative) Safety analysis report including hazard reports - DRD		65
D.1	DRD identification	65
D.1.1	Requirement identification and source document.....	65
D.1.2	Purpose and objective.....	65
D.2	Expected response	65
D.2.1	Contents	65
D.2.2	Special remarks	66
Annex E (informative) Criteria for probabilistic safety targets.....		67

E.1 Objectives of probabilistic safety targets	67
E.2 Criteria for probabilistic safety targets	67
Annex F (informative) Applicability guidelines	68
Annex G (informative) European legislation and ‘CE’ marking	74
G.1 Overview	74
G.2 CE mark	74
G.3 Responsibility of the design authority	74
G.4 Declaration of conformity	75
G.5 References	75
Bibliography	77
 Figures	
Figure C-1 : Safety verification tracking log (SVTL)	64
 Tables	
Table 6-1: Severity categories	35
Table 6-2: Criticality of functions	35
Table 6-3: Criticality category assignment for software products vs. function criticality	40
 Table A-1 : Safety deliverable documents	 58

European foreword

This document (FprEN 16602-40:2017) has been prepared by Technical Committee CEN/CLC/TC 5 “Space”, the secretariat of which is held by DIN (Germany).

This document (FprEN 16602-40:2017) originates from ECSS-Q-ST-40C Rev.1.

This document is currently submitted to the Unique Acceptance Procedure

This document will supersede EN ISO 14620-1:2002 Space systems - Safety requirements - Part 1: System safety.

This document has been developed to cover specifically space systems and will therefore have precedence over any EN covering the same scope but with a wider domain of applicability (e.g.: aerospace).

1

Scope

This European Standard defines the safety programme and the safety technical requirements aiming to protect flight and ground personnel, the launch vehicle, associated payloads, ground support equipment, the general public, public and private property, the space system and associated segments and the environment from hazards associated with European space systems.

This Standard is applicable to all European space projects.

This standard may be tailored for the specific characteristic 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 16601-00-01	ECSS-S-ST-00-01	ECSS system – Glossary of terms
EN 16603-10	ECSS-E-ST-10	Space engineering – System engineering general requirements
EN 16603-32-01	ECSS-E-ST-32-01	Space engineering – Fracture control
EN 16603-32-10	ECSS-E-ST-32-10	Space engineering – Structural factors of safety for spaceflight hardware
EN 16603-40	ECSS-E-ST-40	Space engineering – Software general requirements
EN 16601-10	ECSS-M-ST-10	Space project management – Project planning and implementation
EN 16601-40	ECSS-M-ST-40	Space project management – Configuration and information management
EN 16601-80	ECSS-M-ST-80	Space project management – Risk management
EN 16602-10	ECSS-Q-ST-10	Space product assurance – Product assurance management
EN 16602-10-04	ECSS-Q-ST-10-04	Space product assurance – Critical-item control
EN 16602-20	ECSS-Q-ST-20	Space product assurance – Quality assurance
EN 16602-30	ECSS-Q-ST-30	Space product assurance – Dependability
EN 16602-60	ECSS-Q-ST-60	Space product assurance – Electrical, electronic and electromechanical (EEE) components
EN 16602-70	ECSS-Q-ST-70	Space product assurance – Materials, mechanical parts and processes
EN 16602-80	ECSS-Q-ST-80	Space product assurance – Software product assurance

Terms, definitions and abbreviated terms

3.1 Terms from other standards

- a. For the purpose of this Standard, the terms and definitions from ECSS-S-ST-00-01 apply (see in clause 3.2 differences for "fail safe" and "system"), in particular for the following terms:
1. accident
 2. failure
 3. catastrophic
 4. critical <CONTEXT: safety>
 5. emergency
 6. ground segment
 7. hazard
 8. hazardous event
 9. inhibit
 10. risk
 11. safety
 12. safing
 13. severity
 14. safety-critical function
 15. space segment
 16. system

3.2 Terms specific to the present standard

3.2.1 cause

action or condition by which a hazardous event is initiated (an initiating event)

NOTE 1 The cause can arise as the result of failure, human error, design inadequacy, induced or natural environment, system configuration or operational mode(s).

NOTE 2 This definition is specific to this Standard, when used in the context of hazard analysis.

3.2.2 criticality

classification of a function or of a software, hardware or operation according to the severity of the consequences of its potential failures

NOTE 1 Refer to clauses 6.4.1 and 6.5.6.

NOTE 2 This notion of criticality, applied to a function or a software, hardware or operation, considers only severity, differently from the criticality of a failure or failure mode (or a risk), which also considers the likelihood or probability of occurrence.

3.2.3 fail safe

property of a system (or part of it), which prevents its failures from resulting in critical or catastrophic consequences

3.2.4 hazard control

preventive or mitigation measure, associated to a hazard scenario, which is introduced into the system design and operation to avoid the events or to interrupt their propagation to consequence

3.2.5 hazardous command

command that can remove an inhibit to a safety-critical function or activate a hazardous subsystem

3.2.6 hazard reduction

process of elimination or minimization and control of hazards

3.2.7 hazard scenario

sequence of events leading from the initial cause to the unwanted safety consequence

NOTE The cause can be a single initiating event, or an additional action or a change of condition activating a dormant problem.

3.2.8 operator error

failure of an operator to perform an action as required or trained or the inadvertent or incorrect action of an operator

[ISO 14620-1]

3.2.9 safety approval authority

entity that defines or makes applicable, for a given project, detailed technical safety requirements, and reviews their implementation

3.2.10 safety audit

independent examination to determine whether the procedures specific to the safety requirements are implemented effectively and are suitable to achieve the specified objectives

3.2.11 safety risk

measure of the threat to safety posed by the hazard scenarios and their consequences

NOTE 1 Safety risk is always associated with a specific hazard scenario or a particular set of scenarios. The risk posed by a single scenario is called individual scenario risk. The risk posed by a set of scenarios with the same top consequence is called overall risk.

NOTE 2 The magnitude of a safety risk is a combination of the severity and the likelihood of the consequence.

3.2.12 safety status parameter

parameter that makes it possible to assess the status of an implemented hazard control

3.3 Abbreviated terms

For the purpose of this Standard, the abbreviated terms from ECSS-S-ST-00-01 and the following apply:

Abbreviation	Meaning
AR	acceptance review
CCB	configuration control board
CDR	critical design review
CE	Conformité Européenne
CRR	commissioning result review
EEE	electronic, electrical, electromechanical
ELR	end-of-life review
EMC	electro-magnetic compatibility
FMEA	failure modes and effects analysis
FMECA	failure modes, effects and criticality analysis
FSDP	flight safety data package
FRR	flight readiness review
FTA	fault tree analysis
GSDP	ground safety data package
GSE	ground support equipment
IEC	International Electrotechnical Commission
LRR	launch readiness review
LVD	low voltage directive

MIP	mandatory inspection point
NRB	nonconformance review board
NUREG-CR	US Nuclear Regulatory Commission contractor report
ORR	operational readiness review
PDR	preliminary design review
PED	pressure equipment directive
PGSE	pressure ground support equipment
PRR	preliminary requirements review
QR	qualification review
R&TTE	radio & telecommunications terminal equipment
RoHS	restriction of certain hazardous substances
SDP	safety data package
SRR	system requirements review
SVTL	safety verification tracking log
TRB	test review board
WEEE	waste electrical and electronic equipment

3.4 Nomenclature

The following nomenclature applies throughout this document:

- a. The word “shall” is used in this Standard to express requirements. All the requirements are expressed with the word “shall”.
- b. The word “should” is used in this Standard to express recommendations. All the recommendations are expressed with the word “should”.

NOTE It is expected that, during tailoring, recommendations in this document are either converted into requirements or tailored out.

- c. The words “may” and “need not” are used in this Standard to express positive and negative permissions, respectively. All the positive permissions are expressed with the word “may”. All the negative permissions are expressed with the words “need not”.
- d. The word “can” is used in this Standard to express capabilities or possibilities, and therefore, if not accompanied by one of the previous words, it implies descriptive text.

NOTE In ECSS “may” and “can” have completely different meanings: “may” is normative (permission), and “can” is descriptive.

- e. The present and past tenses are used in this Standard to express statements of fact, and therefore they imply descriptive text.

Safety principles

4.1 Objective

The objective of safety assurance is to ensure that all safety risks associated with the design, development, production and operations of space product are adequately identified, assessed, minimized, controlled and finally accepted through the implementation of a safety assurance programme.

4.2 Policy

4.2.1 General

The ECSS safety policy is to:

- ensure that space systems do not cause a hazard to, in order of priority:
 - human life,
 - the environment,
 - public and private property (including launch facilities),
 - spacecraft and launcher,
 - ground support equipment and facilities,
- determine and evaluate the safety risks associated with project activities,
- minimize safety risks in a technically effective and cost effective manner,
- ensure adequate verification of safety control measures.

4.2.2 Implementation

The ECSS safety policy is implemented by applying a safety programme which ensures that:

- safety is designed into the system,
- safety controls are adequately implemented in the verification plan,
- safety requirements including launch centre safety regulations are met,
- hazards are identified, and eliminated or, where this is not possible, minimized, ranked and controlled in accordance with project objectives in a manner acceptable to the customer and to the safety organisations involved in the implementation of the mission.

4.3 Safety programme

The safety programme comprises the:

- identification and control of all safety related risks with respect to the design, development and operations of space products,
- assessment of the risks based on qualitative and quantitative analysis as appropriate,
- application of a hazard reduction precedence and of control measures of the residual risks.

5

Safety programme

5.1 Scope

- a. The supplier shall establish and maintain a safety programme to assure conformance with project safety policy and requirements.
- b. The safety programme shall establish a safety management system to implement provisions of this Standard - commensurate with the programme requirements and tailored by the customer

NOTE 1 For tailoring, refer to clause 1.

NOTE 2 The system safety programme requirements are subject to tailoring, without diminishing the intent to protect flight and ground personnel, the launch vehicle, associated payloads, ground support equipment, the general public, public and private property, the space system and associated segments and the environment from hazards associated with space systems.

NOTE 3 As support to tailoring, informative Annex F provides a guideline for determining the applicability of this standard depending on the type of project.

5.2 Safety programme plan

- a. The supplier shall establish and maintain a safety programme plan in conformance with the DRD in Annex B.

NOTE The plan can either be included as part of an overall project product assurance plan or as a separate safety programme plan.

- b. The supplier shall cover, in his safety programme plan, the safety tasks for the project phases in conformance with 5.7.1.

5.3 Conformance

- a. The supplier shall comply with all applicable national or international safety regulations.

NOTE This includes launch site safety regulations, space debris mitigation and re-entry safety regulations, etc.

- b. <<deleted>>

- c. The implementation of safety requirements shall not be compromised by other requirements.

NOTE For example: security requirements.

5.4 Safety organization

5.4.1 Safety manager

- a. Each supplier shall appoint a safety manager who has appropriate training or experience.
- b. The safety manager shall have organisational authority and independence to:
 - 1. establish and maintain a safety programme in accordance with the project safety requirements,
 - 2. manage all safety assurance aspects of the design of the system (including software) and its operation in accordance with the Safety Plan,
 - 3. coordinate the interfaces:
 - (a) with the relevant bodies involved in the project in accordance with the safety plan,
 - (b) with the safety launcher authority.

NOTE Depending on the project safety criticality, the safety manager can be combined with other functions (e.g. PA manager) when agreed with the customer.

5.4.2 Safety manager access and authority

5.4.2.1 Access

- a. The safety manager shall:
 - 1. have the right of access to safety-related data relevant to project safety in conformance with ECSS-M-ST-40,
 - 2. have unimpeded access to any management level without organizational constraint on any aspect of project safety.

5.4.2.2 Authority

- a. The safety manager or safety relevant authority shall have the authority to:
 - 1. reject any project document, or to stop any project activity that does not conform to approved safety requirements or procedures,
 - 2. interrupt hazardous operations when it becomes clear by the Safety Manager that the operation does not conform to the agreed measures defined in the corresponding hazard report and derived approved hazard procedure.

5.4.3 Safety audits

- a. The supplier shall perform safety audits or reviews to verify compliance to project safety policy and requirements.
- b. The safety audits shall be in accordance with ECSS-M-ST-10 and ECSS-Q-ST-10.

NOTE The safety audits can be part of the project audits.

- c. The customer shall be informed of the audit schedule.

5.4.4 Approval of documentation

- a. Documentation related to safety shall be approved by the safety manager upon his verification of completeness, compliance with stated safety requirements and formal closeout of open safety verification items (as defined and agreed during safety audits and reviews).

5.4.5 Approval of hazardous operations

- a. The safety manager (or a designated representative) shall have concluded the review of, and approved, any hazardous operation before it is executed.

5.4.6 Representation on boards

- a. The safety manager or designated delegate shall be represented at configuration control boards (CCBs), nonconformance review boards (NRBs), test review board (TRBs), and at qualification, and acceptance reviews, where safety requirements and safety-critical functions are involved.
- b. The safety function shall be further represented at all boards dealing with health matters where exposure or endurance limits are defined for flight and ground crews.

5.4.7 Safety approval authority

- a. The safety approval authority shall:
 - 1. review and disposes the safety data submittals,
 - 2. approve the close-out of hazards,
 - 3. decide on deviations and waivers, and finally
 - 4. accept the statement of safety compliance.

5.5 Safety risk assessment and control

- a. The safety risk identification, reduction and control shall be part of the project's risk management process as specified in ECSS-M-ST-80.
- b. Safety risk identification, reduction and control shall be a continuous and iterative process throughout the project life cycle, encompassing
 - 1. allocation of safety requirements;
 - 2. hazard and safety risk identification;
 - 3. evaluation (including categorisation) of consequence severity;
 - 4. hazard and safety risk reduction and control;
 - 5. close out and acceptance of residual risk.
- c. For the identification of hazards and associated safety risks, consideration shall be given to past experience, studies, ground and flight tests, reviews, the industrial process as well as the operational use.

5.6 Safety critical items

- a. The safety critical items shall be part of the project's overall critical items control programme as specified in ECSS-Q-ST-10-04.

5.7 Project phases and safety review cycle

5.7.1 Safety program tasks and reviews

5.7.1.1 Mission analysis/Needs identification - Phase 0

- a. Safety analysis shall support the identification of sources of safety risk as well as the performance of preliminary trade-off analyses between alternative system concepts.
- b. The following safety programme tasks shall apply for human spaceflight programmes and safety critical systems:
 - 1. Analyse safety requirements and lessons-learnt associated with similar previous missions;