

DIN EN ISO 14620-1:2005-06 (D)

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

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	Verifikationanforderungen	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.....	42
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