

	DIN IEC 62138 (VDE 0491 Teil 3-3)	DIN
	Diese Norm ist zugleich eine VDE-Bestimmung im Sinne von VDE 0022. Sie ist nach Durchführung des vom VDE-Präsidium beschlossenen Genehmigungsverfahrens unter der oben angeführten Nummer in das VDE-Vorschriftenwerk aufgenommen und in der „etz Elektrotechnik + Automation“ bekannt gegeben worden.	VDE
ICS 27.120.20; 35.080 Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorien B oder C (IEC 62138:2004) Nuclear power plants – Instrumentation and control important for safety – Software aspects for computer-based systems performing category B or C functions (IEC 62138:2004) Centrales nucléaires – Instrumentation et contrôle-commande importants pour la sûreté – Aspects logiciels des systèmes informatisés réalisant des fonctions de catégorie B ou C (CEI 62138:2004) Gesamtumfang 48 Seiten DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE		

Beginn der Gültigkeit

Diese Norm gilt ab 2004-09-01.

Nationales Vorwort

Vorausgegangener Norm-Entwurf: E DIN IEC 62138 (VDE 0491 Teil 3-3):2002-11.

Für die vorliegende Norm ist das nationale Arbeitsgremium GUK 967.1 „Leittechnik für kerntechnische Anlagen“ und dessen Arbeitskreis AK 967.1.10 „Sicherheitsleittechnik“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE zuständig. Bei Fragen der Interpretation von Aussagen wird empfohlen, ergänzend auf die zugrunde liegende, in englischer und französischer Sprache erschienene IEC-Publikation zurückzugreifen.

Diese Norm, deren Anwendung international empfohlen wird, gibt das höchstmögliche Maß internationaler Übereinstimmung für das behandelte Sachgebiet wieder. Die Auslegung kerntechnischer Anlagen in Deutschland wird wesentlich durch die Strahlenschutzverordnung, die BMI-Kriterien, die KTA-Regeln und die RSK-Leitlinien bestimmt.

In der Reihe VDE 0491 sind als Norm erschienen:

- **DIN IEC 61226 (VDE 0491 Teil 1):1997-07**, *Kernkraftwerke – Sicherheitsleittechnik – Kategorisierung (IEC 61226:1993).*
- **DIN IEC 61513 (VDE 0491 Teil 2):2002-10**, *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Allgemeine Systemanforderungen (IEC 61513:2001).*
- **DIN IEC 60880-2 (VDE 0491 Teil 3-2):2001-12**, *Kernkraftwerke – Software für Rechner mit sicherheitstechnischer Bedeutung – Teil 2: Vorkehrungen gegen Versagen aufgrund von Softwarefehlern, Verwendung von Software-Werkzeugen und von vorgefertigter Software (IEC 60880-2:2000).*
- **DIN IEC 62138 (VDE 0491 Teil 3-3):2004-09**, *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorien B oder C (IEC 62138:2004).*
- **DIN IEC 62117 (VDE 0491 Teil 4):2001-10**, *Kernkraftwerke – Druckwasserreaktoren – Überwachung ausreichender Kühlung des Kerns im abgeschalteten Zustand des Reaktors (IEC 62117:1999).*
- **DIN IEC 61839 (VDE 0491 Teil 5):2002-09**, *Kernkraftwerke – Auslegung von Warten – Analyse und Zuordnung der Funktionen (IEC 61839:2000).*

Als Norm-Entwürfe liegen vor:

- **E DIN IEC 61226 (VDE 0491 Teil 1):2003-07**, *Kernkraftwerke – Leittechnische Systeme mit sicherheitstechnischer Bedeutung – Kategorisierung (IEC 45A/481/CDV:2003).*
- **E DIN IEC 61513/A100 (VDE 0491 Teil 2/A100):2004-04**, *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Allgemeine Systemanforderungen – Nationaler Anhang ND (informativ): Mitgeltende Festlegungen.*
- **E DIN IEC 60880 (VDE 0491 Teil 3-2):2004-07**, *Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorie A (IEC 45A/523/CD:2003).*
- **E DIN IEC 60568 (VDE 0491 Teil 6):2003-11**, *Kernkraftwerke – Kern-Instrumentierung zur Messung der Neutronenflussdichte (IEC 45A/480/CD:2003).*

Nationaler Anhang NA (informativ)

Zusammenhang mit Europäischen und Internationalen Normen

Für den Fall einer undatierten Verweisung im normativen Text (Verweisung auf eine Norm ohne Angabe des Ausgabedatums und ohne Hinweis auf eine Abschnittsnummer, eine Tabelle, ein Bild usw.) bezieht sich die Verweisung auf die jeweils neueste gültige Ausgabe der in Bezug genommenen Norm.

Für den Fall einer datierten Verweisung im normativen Text bezieht sich die Verweisung immer auf die in Bezug genommene Ausgabe der Norm.

Eine Information über den Zusammenhang der zitierten Normen mit den entsprechenden Deutschen Normen ist nachstehend wiedergegeben.

Tabelle NA.1

Europäische Norm	Internationale Norm	Deutsche Norm	Klassifikation im VDE-Vorschriftenwerk
–	IEC 60880:1986 *)	DIN IEC 60880:1987-08 *)	–
–	IEC 60880-2:2000 *)	DIN IEC 60880-2 (VDE 0491 Teil 3-2):2001-12 *)	VDE 0491 Teil 3-2
EN 61131-3:2003	IEC 61131-3:2003	DIN EN 61131-3:2003-12	–
–	IEC 61226:1993 *)	DIN IEC 61226 (VDE 0491 Teil 1):1997-07 *)	VDE 0491 Teil 1
EN 61508-3:2001	IEC 61508-3:1998 + Corr. 1999	DIN EN 61508-3 (VDE 0803 Teil 3):2002-12	VDE 0803 Teil 3
EN 61508-4:2001	IEC 61508-4:1998 + Corr. 1999	DIN EN 61508-4 (VDE 0803 Teil 4):2002-11	VDE 0803 Teil 4
–	IEC 61511-1:2003	DIN IEC 61511-1 (VDE 0810 Teil 1):2004-02	VDE 0810 Teil 1
–	IEC 61513:2001	DIN IEC 61513 (VDE 0491 Teil 2):2002-10 *)	VDE 0491 Teil 2
EN ISO 9001:2000	ISO 9001:2000	DIN EN ISO 9001:2000-12	–
EN ISO 9000-3:1997	ISO 9000-3:1997	DIN EN ISO 9000-3:1998-08	–
–	ISO/IEC 12207	–	–
–	IAEA NS-G-1.1	–	–
–	IAEA NS-G-1.3	–	–
–	IAEA NS-R-1	–	–
–	IAEA 50-C/SG-Q	–	–
*) Siehe Aufstellung auf Seite 2.			

Nationaler Anhang NB (informativ)

Literaturhinweise

DIN IEC 60880:1987-08, *Software für Rechner im Sicherheitssystem von Kernkraftwerken; Identisch mit IEC 60880:1986.*

DIN IEC 60880-2 (VDE 0491 Teil 3-2):2001-12, *Kernkraftwerke – Software für Rechner mit sicherheitstechnischer Bedeutung – Teil 2: Vorkehrungen gegen Versagen aufgrund von Softwarefehlern, Verwendung von Software-Werkzeugen und von vorgefertigter Software (IEC 60880-2:2000).*

DIN EN 61131-3:2003-12, *Speicherprogrammierbare Steuerungen – Teil 3: Programmiersprachen (IEC 61131-3:2003); Deutsche Fassung EN 61131-3:2003.*

DIN IEC 61226 (VDE 0491 Teil 1):1997-07, *Kernkraftwerke – Sicherheitsleittechnik – Kategorisierung (IEC 61226:1993).*

DIN EN 61508-3 (VDE 0803 Teil 3):2002-12, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 3: Anforderungen an Software (IEC 61508-3:1998 + Corrigendum 1999); Deutsche Fassung EN 61508-3:2001.*

DIN EN 61508-4 (VDE 0803 Teil 4):2002-11, *Funktionale Sicherheit elektrischer/elektronischer/programmierbarer elektronischer sicherheitsbezogener Systeme – Teil 4: Begriffe und Abkürzungen (IEC 61508-4:1998 + Corrigendum 1999); Deutsche Fassung EN 61508-4:2001.*

DIN IEC 61511-1 (VDE 0810 Teil 1):2004-02, *Funktionale Sicherheit – Sicherheitstechnische Systeme für die Prozessindustrie – Teil 1: Allgemeines, Begriffe, Anforderungen an System, Hardware und Software (IEC 61511-1:2003).*

DIN IEC 61513 (VDE 0491 Teil 2):2002-10, *Kernkraftwerk – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Allgemeine Systemanforderungen (IEC 61513:2001).*

DIN EN ISO 9001:2000-12, *Qualitätsmanagementsysteme – Anforderungen (ISO 9001:2000-09); EN ISO 9001:2000.*

DIN EN ISO 9000-3:1998-08, *Normen zum Qualitätsmanagement und zur Qualitätssicherung/QM-Darlegung – Teil 3: Leitfaden für die Anwendung von ISO 9001:1994 auf Entwicklung, Lieferung, Installation und Wartung von Computer-Software (ISO 9000-3:1997); EN ISO 9000-3:1997.*

Deutsche Übersetzung

Kernkraftwerke
Leittechnik für Systeme mit sicherheitstechnischer Bedeutung
Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen
der Kategorien B oder C

Inhalt

	Seite
Vorwort.....	6
Einleitung	7
1 Anwendungsbereich	8
2 Normative Verweisungen	8
3 Begriffe und Abkürzungen	9
4 Grundsätzliche Konzepte und Annahmen	15
4.1 Arten von Software	15
4.2 Datentypen	16
4.3 Software- und System-Sicherheitslebenszyklen	16
4.4 Abstufungsprinzipien	19
5 Anforderungen an die Software leittechnischer Systeme, die Funktionen der Kategorie C ausführen	20
5.1 Allgemeine Anforderungen	20
5.2 Auswahl vorgefertigter Software.....	24
5.3 Software-Anforderungsspezifikation.....	25
5.4 Softwareauslegung	27
5.5 Realisierung neuer Software	28
5.6 Softwareaspekte der Systemintegration.....	28
5.7 Softwareaspekte der Systemvalidierung	29
5.8 Einrichtung der Software in der Anlage.....	30
5.9 Anomalie-Berichte	30
5.10 Softwaremodifizierung	30
6 Anforderungen an die Software leittechnischer Systeme, die Funktionen der Kategorie B ausführen.....	31
6.1 Allgemeine Anforderungen	31
6.2 Auswahl vorgefertigter Software.....	35
6.3 Software-Anforderungsspezifikation.....	39
6.4 Softwareauslegung	41
6.5 Realisierung neuer Software	43
6.6 Softwareaspekte der Systemintegration.....	45
6.7 Softwareaspekte der Systemvalidierung	45
6.8 Einrichtung der Software in der Anlage.....	46
6.9 Anomalie-Berichte	46
6.10 Softwaremodifizierung	46
Literaturhinweise.....	48
 Bild 1 – Typische Softwareteile in rechnerbasierten leittechnischen Systemen.....	15
Bild 2 – Tätigkeiten im System-Sicherheitslebenszyklus (nach IEC 61513)	16

Bild 3 – Software bezogenen Tätigkeiten im System-Sicherheitslebenszyklus.....	17
Bild 4 – Entwicklungstätigkeiten im Software-Sicherheitslebenszyklus bezogen auf IEC 62138.....	18
Bild 5 – Vorgehen zum Nachweis der Zuverlässigkeit von vorgefertigter Software eines leittechnischen Systems der Klasse 2	18

Vorwort

- 1) Die IEC (Internationale Elektrotechnische Kommission) ist eine weltweite Normungsorganisation, die alle Nationalen Elektrotechnischen Komitees (Nationale Komitees der IEC) umfasst. Die IEC hat das Ziel, die internationale Zusammenarbeit in allen Fragen der Normung auf dem Gebiet der Elektrotechnik und Elektronik zu fördern. Zu diesem Zweck und neben anderen Aktivitäten veröffentlicht die IEC Internationale Normen, technische Spezifikationen, technische Berichte, öffentlich verfügbare Spezifikationen (PAS) und Leitfäden (im Folgenden als „Publikation(en) der IEC“ bezeichnet. Mit der Vorbereitung sind die Technischen Komitees beauftragt. Jedes Nationale Komitee der IEC, das an dem behandelten Thema interessiert ist, darf an dieser Vorbereitungsarbeit teilnehmen. Internationale Organisationen, Regierungs- und Nichtregierungsstellen, die mit der IEC in Verbindung stehen, nehmen ebenfalls an diesen Vorbereitungsarbeiten teil. Die IEC arbeitet eng mit der Internationalen Organisation für Normung (ISO) nach den in der Vereinbarung zwischen beiden Organisationen festgelegten Bedingungen zusammen.
- 2) Die offiziellen Beschlüsse oder Vereinbarungen der IEC über technische Fragen, die in Technischen Komitees von Vertretern aller an dem behandelten Thema besonders interessierten Nationalen Komitees erarbeitet werden, bringen das höchstmögliche Maß internationaler Übereinstimmung für das behandelte Sachgebiet zum Ausdruck.
- 3) Publikationen der IEC haben die Form von Empfehlungen zur internationalen Anwendung und werden von den Nationalen Komitees der IEC in diesem Sinne anerkannt. Obwohl alle möglichen Anstrengungen unternommen werden, um sicherzustellen, dass der fachliche Inhalt ihrer Publikationen korrekt ist, kann die IEC nicht für deren Art der Anwendung oder für eventuelle Fehlinterpretationen durch den Anwender verantwortlich gemacht werden.
- 4) Um die internationale Vereinheitlichung zu fördern, verpflichten sich die Nationalen Komitees der IEC, Publikationen der IEC so durchschaubar wie möglich in ihren nationalen und regionalen Normen anzuwenden. Jede Abweichung zwischen der Publikation der IEC und der entsprechenden nationalen oder regionalen Norm muss in dieser deutlich gekennzeichnet werden.
- 5) Die IEC hat kein Verfahren für die Kennzeichnung der Konformität festgelegt und übernimmt keine Verantwortung, wenn ein Gegenstand als konform mit einer ihrer Publikationen erklärt wird.
- 6) Alle Anwender sollten sicherstellen, dass sie über die neueste Ausgabe dieser Publikation verfügen.
- 7) Weder die IEC, deren Geschäftsführung, Angestellte oder sonstige Beteiligte oder Beauftragte der IEC noch einzelne Fachleute oder Mitglieder ihrer Technischen Komitees und Nationalen Komitees der IEC dürfen für Schäden an Personen, Sachen oder sonstige Schäden beliebiger Art, sei es direkt oder indirekt, oder für Kosten (einschließlich Gerichtskosten) oder Ausgaben, die sich aus der Veröffentlichung, Anwendung oder im Vertrauen auf diese oder jede andere Publikation der IEC ergeben, haftbar gemacht werden.
- 8) Zu beachten sind die in dieser Publikation zitierten normativen Verweisungen. Für die korrekte Anwendung dieser Publikation sind die in Bezug genommenen Normen unerlässlich.
- 9) Es besteht die Möglichkeit, dass Bestandteile dieser Publikation der IEC Gegenstand von Patentrechten sind. Die IEC hat nicht die Verantwortung, das Vorhandensein solcher Patentrechte festzustellen und auf deren Existenz hinzuweisen.

Die Internationale Norm IEC 62138 wurde vom Technischen Unterkomitee 45A „Instrumentation and control of nuclear facilities“ des Technischen Komitees 45 „Nuclear instrumentation“ der IEC ausgearbeitet.

Dieser Text basiert auf den folgenden Dokumenten:

FDIS	Report on voting
45A/507/FDIS	45A/521/RVC

Ausführliche Auskunft über die Abstimmung zur Genehmigung dieser Norm gibt der in obiger Tabelle zitierte Abstimmungsbericht.

Diese Norm wurde entsprechend den ISO/IEC-Direktiven, Teil 2 ausgearbeitet.

Das IEC-Komitee hat entschieden, dass der Inhalt dieser Publikation bis zum Jahr 2009 unverändert bleiben soll. Zu diesem Zeitpunkt wird entsprechend der Entscheidung des Komitees die Publikation

- bestätigt,
- zurückgezogen,
- durch eine Folgeausgabe ersetzt oder
- geändert.

Einleitung

Struktur der Normen des SC 45A – Beziehungen zu anderen IEC-Dokumenten sowie zu Dokumenten von IAEA und ISO

Eingangsdokument zu den Normen des SC 45A ist die **IEC 61513**, die sich mit allgemeinen Anforderungen an die leittechnischen Systeme und Geräte befasst, die zur Ausführung sicherheitstechnisch wichtiger Funktionen in Kernkraftwerken genutzt werden. Durch die **IEC 61513** werden die Normen des SC 45A strukturiert.

In **IEC 61513** wird direkt auf andere Normen des SC 45A verwiesen, die allgemeine Themen wie die Kategorisierung von Funktionen, die Klassifizierung, Qualifizierung und Trennung von Systemen, Software- bzw. Hardwareaspekte rechnerbasierter Systeme sowie die Auslegung von Warten behandeln. Die Normen, auf die direkt verwiesen wird, sind zusammen mit **IEC 61513** als ein in sich konsistenter Satz von Dokumenten zu betrachten (sie sind in Ebene 1 eingeordnet).

Andere Normen des SC 45A, auf die in **IEC 61513** nicht direkt verwiesen wird, behandeln spezielles Gerät, technische Verfahren oder spezifische Aktivitäten. Üblicherweise können diese auf Ebene 2 eingeordneten Normen, die sich auf die zuvor beschriebenen Dokumente für allgemeine Themen beziehen (Ebene 1), für sich allein benutzt werden.

Für **IEC 61513** wird ein Darstellungsformat verwendet, das dem der Sicherheitsgrundnorm IEC 61508 ähnlich ist, mit einem Sicherheits-Lebenszyklus als Gesamtrahmen und einem System-Lebenszyklus als weiteren wichtigen Rahmen. Mit **IEC 61513** werden die allgemeinen Anforderungen (für Sicherheitssysteme unterschiedlicher industrieller Anwendungen) von **IEC 61508-1**, **-2** und **-4** für die Anwendung im nuklearen Sektor umgesetzt. Die Einhaltung der **IEC 61513** erleichtert die Übereinstimmung mit IEC 61508, weil die Anforderungen der **IEC 61513** aus den Anforderungen der IEC 61508 für die Anwendung in der nuklearen Industrie entwickelt wurden. In diesem Rahmen entsprechen IEC 60880 und **IEC 62138** für den nuklearen Sektor der allgemeinen **IEC 61508-3**.

IEC 61513 stützt sich für Themen der Qualitätssicherung sowohl auf ISO als auch auf IAEA 50-C-QA (inzwischen durch IAEA 50-C/SG-Q ersetzt) ab.

In den Normen des SC 45A werden die Prinzipien und grundsätzlichen Sicherheitsaspekte des „IAEA code on the safety of nuclear power plants“ und der „IAEA safety series“, im Speziellen NS-R-1 „Safety of Nuclear Power Plants: Design“ und NS-G-1.3 „Instrumentation and control systems important to safety in Nuclear Power Plants“, umgesetzt. Terminologie und Definitionen in den Normen des SC 45A sind mit denen der IAEA konsistent.

1 Anwendungsbereich

Diese Internationale Norm enthält Anforderungen an die Software rechnerbasierter leittechnischer Systeme zur Ausführung von Funktionen der Kategorien B oder C wie in IEC 61226 definiert. Sie ergänzt die Normen IEC 60880 und IEC 60880-2, die Anforderungen für die Software rechnerbasierter leittechnischer Systeme bereitstellen, die Funktionen der Kategorie A ausführen.

Sie ist auch konsistent mit und ergänzend zu IEC 61513. Hauptsächlich auf Systemebene ablaufende Tätigkeiten (z. B. Integration, Validierung, Errichtung) sind in dieser Norm nicht erschöpfend behandelt; bezüglich nicht softwarespezifischer Anforderungen wird auf IEC 61513 verwiesen.

Die Klassen der sicherheitstechnisch wichtigen leittechnischen Systeme sind nach IEC 61513 wie folgt definiert:

- leittechnische Systeme der Klasse 1 dienen grundsätzlich der Realisierung von Funktionen der Kategorie A, können aber auch Funktionen der Kategorien B und C sowie nicht klassifizierte Funktionen ausführen;
- leittechnische Systeme der Klasse 2 dienen grundsätzlich der Realisierung von Funktionen der Kategorie B, können aber auch Funktionen der Klasse C und nicht klassifizierte Funktionen ausführen;
- leittechnische Systeme der Klasse 3 dienen grundsätzlich der Realisierung von Funktionen der Kategorie C, können aber auch nicht klassifizierte Funktionen ausführen.

Da mit einem gegebenen klassifizierten leittechnischen System Funktionen verschiedener Kategorien und auch nicht klassifizierte Funktionen ausgeführt werden können, sind die Anforderungen in dieser Norm nicht einer Kategorie der realisierten Funktionen zugeordnet, sondern der Klasse des leittechnischen Systems.

In dieser Norm werden die laufenden Praktiken bei Entwicklung und Modifizierung von Software in rechnerbasierten leittechnischen Systemen berücksichtigt, insbesondere

- die Verwendung vorgefertigter Software, Geräte und Gerätefamilien, die nicht notwendigerweise für die speziellen Gegebenheiten der Nuklearindustrie ausgelegt sind;
- die Verwendung spezieller „Black-box“-Einrichtungen mit eingebetteter Software;
- die Verwendung anwendungsorientierter Sprachen.

Diese Norm ist keine allgemeine Leitlinie für Software-Engineering. Sie enthält vielmehr Anforderungen, die Software leittechnischer Systeme der Klassen 2 und 3 zur Erreichung der Sicherheitsziele einhalten muss^{N1)}.

2 Normative Verweisungen

Die folgenden zitierten Dokumente sind für die Anwendung dieses Dokuments erforderlich. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

IEC 61226, *Nuclear power plants – Instrumentation and control systems important for safety – Classification.*

IEC 61513:2001, *Nuclear power plants – Instrumentation and control systems important for safety – General requirements for systems.*

^{N1)} Nationale Fußnote: Auslegung bedeutet auch, Kompromisse zwischen verschiedenen Projektzielen einzugehen, z. B. hinsichtlich Instandhaltbarkeit, Diversität, niedriger Komplexität, Testbarkeit, oder der Bevorzugung bekannter und bewährter Techniken. Abweichungen von den Anforderungen in dieser Norm müssen begründet werden, indem die Fähigkeit zum Erreichen der in dieser Norm definierten fundamentalen Sicherheitsprinzipien gezeigt wird.

3 Begriffe und Abkürzungen

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe und Abkürzungen.

3.1

Animation

(en: animation)

Prozess, durch den das in einer Spezifikation festgelegte Verhalten mit aktuellen Werten angezeigt wird, abgeleitet aus den Gleichungen für dieses Verhalten und einigen Eingangswerten

[IEC 60880-2]

3.2

Anwendungsfunktion

(en: application function)

Funktion eines leittechnischen Systems, die eine Aufgabe in Verbindung mit dem Prozess und nicht mit dem Funktionieren des Systems selbst erfüllt

[IEC 61513]

3.3

anwendungsorientierte Sprache

(en: application-oriented language)

Rechnersprache, die speziell für bestimmte Anwendungsarten entwickelt und von Personen verwendet wird, die Spezialisten in diesen Anwendungsarten sind

ANMERKUNG 1 Gerätefamilien verwenden üblicherweise anwendungsorientierte Sprachen, um damit eine leicht nutzbare Möglichkeit für die Anpassung des Geräts an spezifische Anforderungen zur Verfügung zu stellen.

ANMERKUNG 2 Anwendungsorientierte Sprachen können verwendet werden, um spezielle funktionale Anforderungen an ein leittechnisches System festzulegen oder Anwendungssoftware zu spezifizieren und/oder zu entwickeln.

ANMERKUNG 3 Beispiele: Sprachen für Funktionsblockdiagramme, Sprachen definiert entsprechend IEC 61131-3.

ANMERKUNG 4 Siehe auch „allgemeine Sprache“.

3.4

Anwendungssoftware

(en: application software)

Teil der Software eines leittechnischen Systems, durch den Anwendungsfunktionen realisiert werden

[IEC 61513]

ANMERKUNG Siehe auch „Systemsoftware“, „Betriebssystem-Software“.

3.5

Kategorie einer leittechnischen Funktion

(en: category of an I&C function)

eine von drei möglichen Sicherheitszuordnungen (A, B, C) von leittechnischen Funktionen, die aus der Sicherheitsrelevanz der durchzuführenden Funktionen resultieren. Wenn die Funktion für die Sicherheit nicht signifikant ist, erfolgt keine Sicherheitszuordnung (Kategorisierung)

[IEC 61513]

ANMERKUNG Siehe auch „Klasse eines leittechnischen Systems“.

3.6

Klasse eines leittechnischen Systems

(en: class of an I&C system)

eine von drei möglichen Zuordnungen (1, 2, 3) sicherheitstechnisch wichtiger leittechnischer Systeme, entsprechend der Anforderung, leittechnische Funktionen unterschiedlicher Sicherheitsrelevanz zu realisieren. Wenn das leittechnische System keine Funktion von sicherheitstechnischer Bedeutung realisiert, wird es als unklassifiziert eingestuft

[IEC 61513]

ANMERKUNG Siehe auch „Kategorie einer leittechnischen Funktion“.

3.7

Komplexität

(en: complexity)

Schwierigkeitsgrad der Verständlichkeit und Verifizierbarkeit eines Systems oder einer Komponente aufgrund von Auslegung, Realisierung oder Verhalten

[IEC 61513]

3.8

Konfigurationsmanagement

(en: configuration management)

Disziplin, in der technische und administrative Anleitungen und Kontrollmaßnahmen angewendet werden, um die funktionalen und physikalischen Eigenschaften einer Konfigurationskomponente festzustellen und zu dokumentieren, Änderungen solcher Eigenschaften zu überwachen, Änderungsprozesse und Implementierungsstatus zu dokumentieren und die Übereinstimmung mit den spezifizierten Anforderungen zu verifizieren

[IEC 61513]

3.9

Auslegungsspezifikation

(en: design specification)

Dokument oder Dokumentenreihe zur Beschreibung der Organisation und Funktion einer Betrachtungseinheit und zur Nutzung als Grundlage für ihre Realisierung und Integration

3.10

Sicherheitsdokumentation

(en: documentation for safety)

Dokument oder Dokumentenreihe, in der spezifiziert wird, wie ein Produkt zuverlässig für sicherheitstechnisch wichtige Anwendungen eingesetzt werden kann

3.11

Gerätefamilie

(en: equipment family)

Satz von Hardware- und Softwarekomponenten, die in einer oder mehreren Architekturen (Konfigurationen) zusammenarbeiten können. Die Entwicklung von anlagenspezifischen Konfigurationen und der zugehörigen Anwendungssoftware kann durch Software-Werkzeuge unterstützt werden. Eine Gerätefamilie stellt üblicherweise eine Anzahl von Standardfunktionen zur Verfügung, die zur Erzeugung spezifischer Anwendungssoftware miteinander kombiniert werden können

[IEC 61513]

ANMERKUNG 1 Eine Gerätefamilie kann das Produkt eines speziellen Herstellers oder ein Satz von Produkten sein, die von der Lieferfirma zusammengestellt und adaptiert sind.

ANMERKUNG 2 Der Ausdruck „Geräteplattform“ wird oft als Synonym für „Gerätefamilie“ verwendet.

3.12

Abweichung

(en: error)

Diskrepanz zwischen berechneten, beobachteten oder gemessenen Werten oder Bedingungen und den tatsächlichen, spezifizierten oder theoretischen Werten oder Bedingungen

[IEC 61513]

ANMERKUNG Siehe auch „Irrtum“, „Fehler“, „Versagen“ bzw. „Ausfall“.

3.13

ablauffähiger Code

(en: executable code)

Software, die in das Zielsystem integriert wird

ANMERKUNG Der ablauffähige Code umfasst üblicherweise Instruktionen, die von der Zielhardware auszuführen sind, und die zugehörigen Daten.

3.14

Versagen

Ausfall^{N2)}

(en: failure)

Abweichen der ausgeführten von der vorgesehenen Funktion

[IEC 61513]

ANMERKUNG Siehe auch „Irrtum“, „Fehler“, „Abweichung“.

3.15

Fehler

(en: fault)

Mangel an einer Hardware-, Software- oder Systemkomponente

[IEC 61513]

ANMERKUNG 1 Fehler können Zufallsfehler sein, z. B. bei Hardware, oder systematische Fehler, z. B. Softwarefehler, die auf Auslegungsmängel zurückgehen. Systematische Fehler resultieren aus Auslegungsfehlern (z. B. Softwarefehlern) und führen unter gleichen Bedingungen systematisch zu denselben Ausfällen.

ANMERKUNG 2 Ein Fehler (insbesondere ein Auslegungsfehler) kann in einem System unentdeckt bleiben, bis besondere Bedingungen auf dieses System so einwirken, dass die resultierende Funktion nicht mit der vorgesehenen Funktion übereinstimmt, d. h. ein Versagen eintritt.

ANMERKUNG 3 Siehe auch „Irrtum“, „Abweichung“, „Versagen“ bzw. „Ausfall“.

3.16

funktionale Validierung

(en: functional validation)

Prüfung der Übereinstimmung von Spezifikationen der Anwendungsfunktionen mit den originären funktionalen und Leistungsfähigkeitsanforderungen der Anlage. Die funktionale Validierung ist als Ergänzung zur Systemvalidierung zu sehen, bei der die Übereinstimmung des Systems mit den Spezifikationen der Anwendungsfunktionen geprüft wird

[IEC 61513]

3.17

allgemeine Sprache

(en: general-purpose language)

Rechnersprache, die für alle Arten von Anwendungen ausgelegt ist

ANMERKUNG 1 Die Systemsoftware von Gerätefamilien wird üblicherweise unter Anwendung allgemeiner Sprachen realisiert.

ANMERKUNG 2 Beispiele: ADA, C, Pascal.

ANMERKUNG 3 Siehe auch „anwendungsorientierte Sprache“.

3.18

Integration

(en: integration)

fortschreitende Zusammenfassung und Verifizierung von Komponenten zu einem kompletten System

^{N2)} Nationale Fußnote: Wenn Hardware oder Teilsysteme (z. B. ein Strang eines redundanten Systems) betroffen sind, wird „failure“ mit „Ausfall“ übersetzt.

3.19

leittechnische Architektur^{N3)}

(en: I&C architecture)

organisatorische Struktur der leittechnischen Systeme der Anlage, die sicherheitstechnische Bedeutung haben

[IEC 61513]

3.20

menschliches Fehlverhalten (Irrtum)

(en: mistake)

Handlung oder Vorgehensweise eines Menschen, die eine unbeabsichtigte Folge hat

[IEC 60880-2]

ANMERKUNG Siehe auch „Fehler“, „Abweichung“, „Versagen“ bzw. „Ausfall“.

3.21

Verhaltensart (von Software)

(en: mode of behaviour)

funktionaler Status einer Software-Einheit, in dem sie ein spezielles Betriebsverhalten zeigt

ANMERKUNG Beispiele: Startbetrieb, Normalbetrieb, eingeschränkter Betrieb mit abgestufter Funktionalität bei Fehlern in der Software-Einheit oder in ihrer Umgebung.

3.22

Betriebssoftware

(en: operational system software)

Teil der Systemsoftware, dessen ausführbarer Code während des Systembetriebs am Zielsystem läuft

[IEC 61513]

ANMERKUNG 1 Beispiele: Betriebssystem, Eingangs-/Ausgangstreiber, Ausnahmebehandlung, Scheduler, Interrupt-Manager, Online-Diagnostik, Redundanz und Management der abgestuften Reduktion von Funktionalität, anwendungsorientierte Bibliotheken.

ANMERKUNG 2 Siehe auch „Anwendungssoftware“, „Systemsoftware“.

3.23

Parameter

(en: parameter)

Einstellwerte für das Verhalten des leittechnischen Systems und/oder seiner Software, die von den Operateuren während des Betriebs verändert werden können

3.24

vorgefertigte Software

(en: pre-developed software)

Software, die – bereits vorgefertigt – als kommerzielles oder proprietäres Produkt verfügbar ist

[IEC 61513]

ANMERKUNG 1 Vorgefertigte Software (PDS) kann eingeteilt werden in allgemeine PDS, die nicht für eine spezielle Hardware-Umgebung entwickelt wurde, und in Hardwarekomponenten integrierte PDS, die zusammen mit dieser Hardware zu verwenden ist.

ANMERKUNG 2 In dieser Norm schließt dieser Ausdruck Softwarewerkzeuge nicht mit ein, auch wenn sie vorgefertigt sind.

^{N3)} Nationale Fußnote: Durch die organisatorische Struktur werden vor allem die Hauptfunktionen, Klasse und Abgrenzung jedes Systems, Verbindungen und Grad der Unabhängigkeit von Systemen, Priorität und Abstimmung bei mehreren gleichzeitig auftretenden Signalen, die Mensch-Maschine-Kommunikation definiert.

In dieser Norm bezeichnet der Ausdruck „leittechnische Architektur“ nur eine Teilmenge der gesamten leittechnischen Architektur der Anlage. Letzterer umfasst auch die nicht klassifizierten Geräte und Systeme.

3.25**Programm**

(en: program)

von Spezialisten verfasstes Dokument, das durch automatische Werkzeuge in einen ablauffähigen Code umgesetzt wird

ANMERKUNG Dies schließt traditionelle Programme mit ein, die in einer allgemeinen Sprache geschrieben sind^{N4)}. Weiter sind Programme in anwendungsorientierten Sprachen eingeschlossen.

3.26**Zugriffsschutz**

(en: security)

Fähigkeit des rechnerbasierten Systems, Informationen und Daten so zu schützen, dass nicht autorisierte Personen oder Systeme sie nicht lesen oder ändern können, und autorisierten Personen oder Systemen der Zugriff nicht verwehrt wird

[IEC 61513]

3.27**Software**

(en: software)

Programme (d. h. Sätze geordneter Instruktionen), Daten, Regeln einschließlich zugehöriger Dokumentation, die zum Betrieb eines rechnerbasierten leittechnischen Systems gehören

[IEC 60880]

3.28**Softwaremodifikation**

(en: software modification)

Änderung eines bereits abgestimmten Dokuments, die zu einer Veränderung des ablauffähigen Codes führt

ANMERKUNG Softwaremodifikationen können während der Entwicklung von Software auftreten (z. B. bei der Behebung von Fehlern, die in einem späteren Stadium der Entwicklung gefunden wurden) oder nachdem die Software bereits in Betrieb genommen wurde.

3.29**Softwarekomponente**

(en: software component)

eine der Auslegungseinheiten, aus denen Software besteht. Sie kann in weitere Softwarekomponenten unterteilt werden

[IEC 61513]

3.30**Software-Entwicklung**

(en: software development)

Phase des Softwarelebenszyklus, die zur Erzeugung der Software für ein leittechnisches System oder eines anderen Softwareprodukts führt. Sie umfasst alle Tätigkeiten von der Anforderungsspezifikation bis zur Validierung und Installation in der Anlage

3.31**Sicherheitslebenszyklus der Software**

(en: software safety life cycle)

erforderliche Tätigkeiten im Zusammenhang mit Entwicklung und Betrieb von Software eines sicherheitstechnisch wichtigen leittechnischen Systems in einer Zeitspanne beginnend mit der Software-Anforderungsspezifikation bis zu dem Zeitpunkt, in dem die Software nicht mehr für die Nutzung zur Verfügung steht

[IEC 61513]

^{N4)} Nationale Fußnote: z. B. in C, ADA oder Assembler.

3.32

statische Analyse

(en: static analysis)

Bewertungsvorgang eines Systems oder einer Komponente, der auf dessen/deren Form, Struktur, Inhalt oder Dokumentation beruht

[IEC 60880-2]

3.33

Systemsoftware

(en: system software)

Teil der Software eines leittechnischen Systems, der für ein bestimmtes Rechnersystem oder eine Rechnerfamilie erstellt wurde, um Entwicklung, Betrieb und Modifikation des Systems und der zugehörigen Programme zu erleichtern

[IEC 61513]

ANMERKUNG 1 Die Systemsoftware der Gerätefamilien besteht üblicherweise aus der Betriebssoftware und der Software unterstützender Systeme (Softwarewerkzeuge).

ANMERKUNG 2 Siehe auch „Anwendungssoftware“ und „Betriebssoftware“.

3.34

Softwarevalidierung

(en: validation)

Test und Überprüfung der integrierten Software, um Übereinstimmung mit den in der Spezifikation des leittechnischen Systems vorgegebenen Anforderungen an Funktionalität, Leistungsfähigkeit und Schnittstellen sicherzustellen

3.35

Verifizierung

(en: verification)

durch Prüfen und Vorlegen objektiver Beweise sicherstellen, dass die Ergebnisse einer Tätigkeit den Zielen und Anforderungen entsprechen, die für diese Tätigkeit definiert wurden

[ISO 12207]

3.36

Abkürzungen

LT: Leittechnik

(en: I&C: instrumentation and control)

3.37^{N5)}

bereits verfügbare(s) Software/Hardware/System

(en: pre-existing software/hardware/system)

bei der Planung oder Auslegung bereits verfügbare(s) und kommerziell genutzte(s) Software/Hardware/System

ANMERKUNG In den neuen und überarbeiteten Normen des SC 45A hat sich „pre-developed“ gegenüber „pre-existing“ immer mehr durchgesetzt. Um Einheitlichkeit zu erreichen, wird daher in vorliegender Norm „vorgefertigt“ verwendet (siehe 3.24).

^{N5)} Nationale Fußnote: Im IEC-Original nicht enthalten; zum besseren Verständnis hier ergänzt.

4 Grundsätzliche Konzepte und Annahmen

Dieser Abschnitt enthält einige grundsätzliche Konzepte und Annahmen über die Art und Entwicklung der Software für leittechnische Systeme der Klassen 2 und 3, auf denen der normative Text beruht.

4.1 Arten von Software

Bild 1 zeigt die Vielfalt der Dienste, die durch Software und Softwarekomponenten in einem typischen leittechnischen System oder einer leittechnischen Architektur zur Verfügung gestellt werden. Softwarekomponenten werden oft als entweder zu Systemsoftware oder Anwendungssoftware gehörend definiert. Systemsoftware wird üblicherweise in Betriebssoftware, die in sicherheitsklassifizierten leittechnischen Systemen implementiert ist, und unterstützende Software (oder Softwarewerkzeuge), die entweder offline genutzt wird oder in nicht sicherheitsklassifizierten Hilfsystemen implementiert ist, unterteilt. Software kann auch in speziellen Einrichtungen wie Messfühlern und Betätigungsbausteinen, Kommunikationsbausteinen und Einrichtungen zur unterbrechungsfreien Stromversorgung verwendet werden.

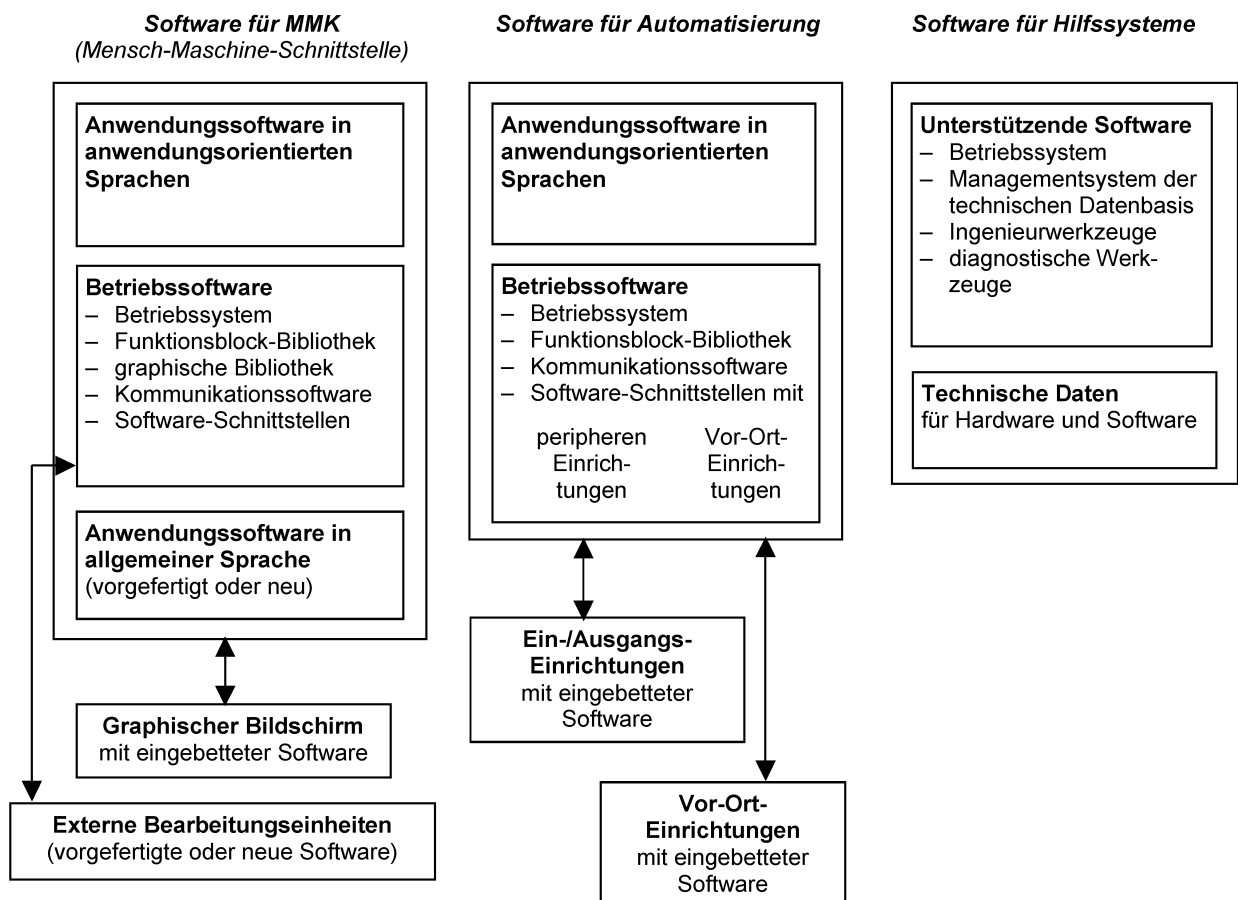


Bild 1 – Typische Softwareteile in rechnerbasierten leittechnischen Systemen

Die Software eines leittechnischen Systems kann auch in vorgefertigte Software (die üblicherweise einen für leittechnische Systeme nutzbaren Bereich umfasst) und neue Software (die entsprechend spezieller Anforderungen eines leittechnischen Systems entwickelt wird) unterteilt werden. Systemsoftware ist üblicherweise vorgefertigte Software, Anwendungssoftware ist in der Regel neu. Die Anforderungen in dieser Norm gelten für neue Software, können aber auch auf vorgefertigte Software angewendet werden. Weiter enthält diese Norm auch alternative Anforderungen, die speziell auf vorgefertigte Software oder auf spezielle Einrichtungen mit integrierter Software angewendet werden können.

Viele moderne Gerätefamilien sind mit umfangreichen anwendungsorientierten Entwicklungswerkzeugen ausgestattet, die Anlagen- oder Systemingenieuren die Spezifizierung ihrer Anforderungen mit Hilfe graphischer Techniken ermöglichen. Die Werkzeuge setzen die graphischen Programme automatisch in ablauffähige Anwendungssoftware um. Wenn die Werkzeuge hinreichende Qualität aufweisen, wird durch diese Vorgehensweise im Allgemeinen das Risiko von Fehlern reduziert.