

DIN EN ISO 19014-4



ICS 53.100

**Erdbaumaschinen –
Funktionale Sicherheit –
Teil 4: Gestaltung und Beurteilung von Software und Datenübertragung für
sicherheitsrelevante Steuerungssysteme (ISO 19014-4:2020);
Deutsche Fassung EN ISO 19014-4:2020**

Earth-moving machinery –

Functional safety –

Part 4: Design and evaluation of software and data transmission for safety-related parts of the control system (ISO 19014-4:2020);

German version EN ISO 19014-4:2020

Engins de terrassement –

Sécurité fonctionnelle –

Partie 4: Conception et évaluation du logiciel et de la transmission des données pour les parties relatives à la sécurité du système de commande (ISO 19014-4:2020);

Version allemande EN ISO 19014-4:2020

Gesamtumfang 55 Seiten

DIN-Normenausschuss Maschinenbau (NAM)

Nationales Vorwort

Diese Norm enthält sicherheitstechnische Festlegungen.

Die nationalen Interessen bei der Erarbeitung wurden vom Ausschuss NA 060-13-01 AA „Erdbau-/Straßenbaumaschinen (SpA ISO/TC 127)“ im Fachbereich „Bau- und Baustoffmaschinen“ des DIN-Normenausschusses Maschinenbau (NAM) wahrgenommen. Vertreter der Hersteller und Anwender von „Erdbaumaschinen“ sowie der Berufsgenossenschaften waren an der Erarbeitung beteiligt.

Für die in diesem Dokument zitierten Dokumente wird im Folgenden auf die entsprechenden deutschen Dokumente hingewiesen:

ISO 12100:2010	siehe	DIN EN ISO 12100:2010-11
ISO 13849-1	siehe	DIN EN ISO 13849-1
ISO 19014-1	siehe	DIN EN ISO 19014-1
ISO 19014-2:—*	siehe	DIN EN ISO 19014-2:—**

Aktuelle Informationen zu diesem Dokument können über die Internetseiten von DIN (www.din.de) durch eine Suche nach der Dokumentennummer aufgerufen werden.

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN EN ISO 12100:2011-03, *Sicherheit von Maschinen — Allgemeine Gestaltungsleitsätze — Risikobeurteilung und Risikominderung (ISO 12100:2010)*

DIN EN ISO 13849-1, *Sicherheit von Maschinen — Sicherheitsbezogene Teile von Steuerungen — Teil 1: Allgemeine Gestaltungsleitsätze*

DIN EN ISO 19014-1, *Erdbaumaschinen — Funktionale Sicherheit — Teil 1: Methodik zur Bestimmung sicherheitsbezogener Teile der Steuerung und deren Leistungsanforderungen*

E DIN EN ISO 19014-2:2019-11, *Erdbaumaschinen — Funktionale Sicherheit — Teil 2: Entwurf und Bewertung von Hardware- und Architektur Anforderungen für sicherheitsrelevante Teile des Steuerungssystems (ISO/DIS 19014-2:2019); Deutsche und Englische Fassung prEN ISO 19014-2:2019*

* Die ISO befindet sich in Vorbereitung und ist momentan als Entwurf ISO/DIS 19014-2:2019 verfügbar.

** Liegt derzeit als Entwurf E DIN EN ISO 19014-2:2019-11 vor.

Deutsche Fassung

Erdbaumaschinen —
Funktionale Sicherheit —
Teil 4: Gestaltung und Beurteilung von Software und
Datenübertragung für sicherheitsrelevante
Steuerungssysteme (ISO 19014-4:2020)

Earth-moving machinery —
Functional safety —
Part 4: Design and evaluation of software and data
transmission for safety-related parts of the control
system (ISO 19014-4:2020)

Engins de terrassement —
Sécurité fonctionnelle —
Partie 4: Conception et évaluation du logiciel et de la
transmission des données pour les parties relatives à la
sécurité du système de commande (ISO 19014-4:2020)

Diese Europäische Norm wurde vom CEN am 29. Juni 2020 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 CEN-CENELEC-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, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, der Republik Nordmazedonien, Rumänien, Schweden, der Schweiz, Serbien, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.



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

CEN-CENELEC Management-Zentrum: Rue de la Science 23, B-1040 Brüssel

Inhalt

	Seite
Europäisches Vorwort	4
Vorwort	5
Einleitung	6
1 Anwendungsbereich	7
2 Normative Verweisungen	7
3 Begriffe	7
4 Software-Entwicklung	11
4.1 Allgemeines	11
4.2 Planung	11
4.3 Artefakte	13
4.4 Spezifikation der Sicherheitsanforderungen an die Software	14
4.5 Gestaltung der Software-Architektur	15
4.6 Software-Modulgestaltung und Codierung	16
4.7 Sprache und Tool-Auswahl	18
4.8 Prüfen von Software-Modulen	18
4.9 Software-Modulintegration und -prüfung	20
4.10 Software-Validierung	21
5 Softwarebasierte Parametrierung	21
5.1 Allgemeines	21
5.2 Datenintegrität	22
5.3 Verifizierung softwarebasierter Parametrierung	22
6 Schutz der Übertragung sicherheitsbezogener Nachrichten in Bussystemen	22
7 Unabhängigkeit durch Software-Partitionierung	24
7.1 Allgemeines	24
7.2 Mehrere Partitionen in einem einzelnen Mikrocontroller	25
7.3 Mehrere Partitionen im Rahmen eines ECU-Netzwerks	27
8 Benutzerinformationen	27
8.1 Allgemeines	27
8.2 Betriebsanleitung	28
Anhang A (informativ) Beschreibung der Software-Methoden/Maßnahmen	29
A.1 Spezifikation der Anforderungen in natürlicher Sprache	29
A.2 Rechnergestützte Spezifikationstools	29
A.3 Informelle Methoden	29
A.4 Halbformelle Methoden	29
A.5 Formelle Methoden	29
A.6 Nachverfolgbarkeit der Sicherheitssoftware	30
A.7 Walkthrough	31
A.8 Inspektion	31
A.9 Rechnergestützte Gestaltungstools	32
A.10 Sicherheitsleistung in Echtzeit	32
A.11 Gestaltungsregeln	33
A.12 Dynamische Variablen oder Objekte ohne Online-Prüfung	33
A.13 Dynamische Variablen oder Objekte mit Online-Prüfung	34

A.14	Modularisierung	34
A.15	Strukturierte Programmierung	35
A.16	Defensive Programmierung	35
A.17	Verwendung vertrauenswürdiger/verifizierter Software-Elemente	36
A.18	Geeignete Programmiersprache	37
A.19	Unterstützung der Sprachteilmenge	37
A.20	Tools mit zunehmender Bewährtheit im Betrieb oder in der Validierung	38
A.21	Zertifizierte Tools und zertifizierte Übersetzungsprogramme	38
A.22	Grenzwertanalyse	39
A.23	Kontrollflussanalyse	39
A.24	Datenflussanalyse	39
A.25	Prüffallausführung anhand der Grenzwertanalyse	40
A.26	Funktions-/Black-Box-Prüfung	40
A.27	Strukturabhängige Prüfungen	40
A.28	Äquivalenzklassen und Eingabe-Partitionsprüfungen	41
A.29	Prüffallausführung aus modellbasierter Prüffallgenerierung	41
A.30	Leistungsnachweis	42
A.31	Software-Modulschnittstellenprüfung	43
A.32	Direkte Vergleichsprüfung	43
Anhang B (normativ) Prüfumgebungen für Softwarevalidierung		44
B.1	Maschinennetzwerkprüfung	44
B.2	Hardware-in-the-Loop-Prüfung	45
B.3	Prüfung der Maschinenebene	46
Anhang C (informativ) Berechnung der Datenintegritätssicherung		47
Anhang D (informativ) Methoden und Maßnahmen zum Übertragungsschutz		49
D.1	Keep-Alive-Nachrichten	49
D.2	Alive Counter	49
D.3	CRC	49
D.4	Sequenznummer	49
D.5	Nachrichtenwiederholung	49
D.6	Watchdog	49
D.7	Zeitgesteuerter Datenbus	50
D.8	Buswächter	50
D.9	Minislotting	50
Anhang E (informativ) Methoden und Maßnahmen für Mikrocontroller-internen Datenschutz		51
E.1	Eindeutiges bidirektionales Kommunikationsobjekt	51
E.2	Ausschließlich zwei unidirektionale Kommunikationsobjekte	51
E.3	IDs zur Identifizierung und Quittierung	51
E.4	Asynchrone Datenkommunikation	51
E.5	Streng prioritätsbasierte Planung	51
E.6	Zeitscheibenmethode	51
E.7	Speicherschutzmechanismen	51
E.8	Verifizierung sicherheitskritischer Daten	52
E.9	Statische Analyse	52
E.10	Statische Zuweisung	52
Literaturhinweise		53

Europäisches Vorwort

Dieses Dokument (EN ISO 19014-4:2020) wurde vom Technischen Komitee ISO/TC 127 „Earth-moving machinery“ in Zusammenarbeit mit dem Technischen Komitee CEN/TC 151 „Bau- und Baustoffmaschinen - Sicherheit“ erarbeitet, dessen Sekretariat von DIN gehalten wird.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis Februar 2021, und etwaige entgegenstehende nationale Normen müssen bis Februar 2021 zurückgezogen werden.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können, ohne dass diese vorstehend identifiziert wurden. CEN ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Entsprechend der CEN-CENELEC-Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Europäische Norm zu übernehmen: Belgien, Bulgarien, Dänemark, Deutschland, die Republik Nordmazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, Schweiz, Serbien, Slowakei, Slowenien, Spanien, Tschechische Republik, Türkei, Ungarn, Vereinigtes Königreich und Zypern.

Anerkennungsnotiz

Der Text von ISO 19014-4:2020 wurde von CEN als EN ISO 19014-4:2020 ohne irgendeine Abänderung genehmigt.

Vorwort

ISO (die Internationale Organisation für Normung) ist eine weltweite Vereinigung nationaler Normungsinstitute (ISO-Mitgliedsorganisationen). Die Erstellung von Internationalen Normen wird üblicherweise von Technischen Komitees von ISO durchgeführt. Jede Mitgliedsorganisation, die Interesse an einem Thema hat, für welches ein Technisches Komitee gegründet wurde, hat das Recht, in diesem Komitee vertreten zu sein. Internationale staatliche und nichtstaatliche Organisationen, die in engem Kontakt mit ISO stehen, nehmen ebenfalls an der Arbeit teil. ISO arbeitet bei allen elektrotechnischen Normungsthemen eng mit der Internationalen Elektrotechnischen Kommission (IEC) zusammen.

Die Verfahren, die bei der Entwicklung dieses Dokuments angewendet wurden und die für die weitere Pflege vorgesehen sind, werden in den ISO/IEC-Direktiven, Teil 1 beschrieben. Es sollten insbesondere die unterschiedlichen Annahmekriterien für die verschiedenen ISO-Dokumentenarten beachtet werden. Dieses Dokument wurde in Übereinstimmung mit den Gestaltungsregeln der ISO/IEC-Direktiven, Teil 2 erarbeitet (siehe www.iso.org/directives).

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. ISO ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren. Details zu allen während der Entwicklung des Dokuments identifizierten Patentrechten finden sich in der Einleitung und/oder in der ISO-Liste der erhaltenen Patenterklärungen (siehe www.iso.org/patents).

Jeder in diesem Dokument verwendete Handelsname dient nur zur Unterrichtung der Anwender und bedeutet keine Anerkennung.

Für eine Erläuterung des freiwilligen Charakters von Normen, der Bedeutung ISO-spezifischer Begriffe und Ausdrücke in Bezug auf Konformitätsbewertungen sowie Informationen darüber, wie ISO die Grundsätze der Welthandelsorganisation (WTO, en: World Trade Organization) hinsichtlich technischer Handelshemmnisse (TBT, en: Technical Barriers to Trade) berücksichtigt, siehe www.iso.org/iso/foreword.html.

Dieses Dokument wurde vom Technischen Komitee ISO/TC 127, Earth-moving machinery, Unterkomitee SC 2, *Safety, ergonomics and general requirements*, in Zusammenarbeit mit dem Europäischen Komitee für Normung (CEN), Technisches Komitee CEN/TC 151, *Bau- und Baustoffmaschinen — Sicherheit*, gemäß der Vereinbarung über technische Kooperation zwischen ISO und CEN (Wiener Vereinbarung) erarbeitet.

Diese erste Ausgabe von ISO 19014-4 ersetzt zusammen mit anderen Teilen der Normenreihe ISO 19014, ISO 15998:2008 und ISO/TS 15998-2:2012, die technisch überarbeitet wurden.

Die wesentlichen Änderungen im Vergleich zu den vorherigen Dokumenten sind folgende:

- weitere Anforderungen für Software-Entwicklung;
- Anforderungen für die Entwicklung mit softwarebasierter Parametrierung;
- Anforderungen für die Übertragung von sicherheitsbezogenen Nachrichten in einem Kommunikationsbus und
- Anforderungen an die Software-Validierung und -Verifizierung der Performance Level der Maschine.

Eine Auflistung aller Teile der Normenreihe ISO 19014 ist auf der ISO-Internetseite abrufbar.

Rückmeldungen oder Fragen zu diesem Dokument sollten an das jeweilige nationale Normungsinstitut des Anwenders gerichtet werden. Eine vollständige Auflistung dieser Institute ist unter www.iso.org/members.html zu finden.

Einleitung

Dieses Dokument behandelt Systeme, die aus jeder möglichen Kombination elektrischer, elektronischer und programmierbarer elektronischer Bauteile [elektrische/elektronische/programmierbare elektronische Systeme (E/E/PES)], die zur Funktionssicherheit von Erdbaumaschinen verwendet werden, bestehen.

Sicherheitsnormen im Bereich des Maschinenbaus sind wie folgt aufgebaut:

Typ-A-Normen (Grundnormen) liefern Grundkonzepte, Auslegungs- und Konstruktionsgrundsätze und allgemeine Aspekte, die auf Maschinen angewendet werden können.

Typ-B-Normen (Fachgrundnormen) behandeln einen oder mehrere Sicherheitsaspekte oder eine oder mehrere Arten von Schutzeinrichtungen, die bei einer Reihe von Maschinen angewendet werden können:

- Typ-B1-Normen behandeln bestimmte Sicherheitsaspekte (z. B. Sicherheitsabstände, Oberflächentemperatur, Geräusch);
- Typ B2-Normen behandeln Schutzeinrichtungen (z. B. Zweihandschaltungen, Verriegelungseinrichtungen, Kontaktmatten, trennende Schutzeinrichtungen).

Typ-C-Normen (Maschinensicherheitsnormen) behandeln detaillierte Sicherheitsanforderungen für eine bestimmte Maschine oder Gruppe von Maschinen.

Diese Internationale Norm ist eine Typ-C-Norm wie in ISO 12100 angegeben.

Dieses Dokument ist insbesondere für die folgenden Interessengruppen von Relevanz, die die Marktakteure im Hinblick auf die Sicherheit von Maschinen repräsentieren:

- Maschinenhersteller (kleine, mittlere und große Unternehmen);
- Gesundheits- und Sicherheitsinstitutionen (Aufsichtsbehörden, Berufsgenossenschaften, Marktaufsicht usw.).

Andere Interessengruppen können durch das in diesem Dokument durch die oben genannten interessierten Kreise festgeschriebene Sicherheitsniveau betroffen sein. Es handelt sich dabei um:

- Maschinenanwender/Arbeitgeber (kleine, mittlere und große Unternehmen);
- Maschinenanwender/Mitarbeiter (z. B. Gewerkschaften, Organisationen für Personen mit besonderen Bedürfnissen);
- Dienstleister, z. B. für Wartungsarbeiten (kleine, mittelständische und große Unternehmen);

Den oben angeführten Interessengruppen wurde die Möglichkeit gegeben, sich an dem Entwurfsprozess zu diesem Dokument zu beteiligen.

Die behandelten Maschinen und Gefährdungen, Gefährdungssituationen und Gefährdungsereignisse sind im Anwendungsbereich dieses Dokumentes angegeben.

Für Maschinen, die nach den Anforderungen dieser Typ-C-Norm konzipiert und gebaut worden sind, gilt: Wenn die Anforderungen in dieser Typ-C-Norm von den Anforderungen in Typ-A- oder B-Normen abweichen, haben die Anforderungen dieser Typ-C-Norm Vorrang gegenüber den Anforderungen der anderen Normen.

1 Anwendungsbereich

Dieses Dokument legt allgemeine Grundsätze für Anforderungen an Software-Entwicklung und Signalübertragung von sicherheitsbezogenen Teilen von Maschinensteuerungssystemen (MCS, en: machine-control systems) in Erdbaumaschinen (EMM, en: earth-moving machinery) und deren Ausrüstung, wie in ISO 6165 definiert, fest. Zudem behandelt dieses Dokument die in ISO 12100 festgelegten signifikanten Gefährdungen in Bezug auf die im Maschinensteuerungssystem eingebettete Software. Bei den behandelten signifikanten Gefährdungen handelt es sich um das falsche Ansprechen der Ausgabe von Maschinensteuerungssystemen auf Eingaben in Maschinensteuerungssystemen.

Cybersicherheit liegt außerhalb des Anwendungsbereichs dieses Dokuments.

ANMERKUNG Hinweise zur Cybersicherheit sind in einer geeigneten Sicherheitsnorm zu finden.

Dieses Dokument gilt nicht für EMM, die vor dem Veröffentlichungsdatum dieses Dokuments hergestellt wurden.

2 Normative Verweisungen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. 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).

ISO 6750-1, *Earth-moving machinery — Operator's manual — Part 1: Contents and format*

ISO 12100:2010, *Safety of machinery — General principles for design — Risk assessment and risk reduction*

ISO 13849-1, *Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design*

ISO 19014-1, *Earth-moving machinery — Functional safety — Part 1: Methodology to determine safety-related parts of the control system and performance requirements*

ISO 19014-2:—¹, *Earth-moving machinery — Functional safety — Part 2: Design and evaluation of hardware and architecture requirements for safety-related parts of the control system*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach ISO 12100, ISO 19014-1, ISO 13849-1 und die folgenden Begriffe.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

- ISO Online Browsing Platform: verfügbar unter <https://www.iso.org/obp>
- IEC Electropedia: verfügbar unter <http://www.electropedia.org/>

¹ In Vorbereitung. Stufe zum Zeitpunkt der Veröffentlichung: ISO/DIS 19014-2:2020.

3.1

Bussystem

in einem elektronischen Steuerungssystem für die Übertragung von *Nachrichten* (3.6) verwendetes Subsystem

Anmerkung 1 zum Begriff: Das Bussystem besteht aus der Systemeinheit (Sources und Sinks of Information), einem Übertragungspfad/Übertragungsmedium (z. B. elektrische Leitungen, faseroptische Leitungen, Hochfrequenzübertragung) und der Schnittstelle zwischen Nachrichten-Source/Sink und Buselektronik (z. B. Protokoll-ASICs (anwendungsspezifische integrierte Schaltung), Empfänger).

3.2

gekapseltes Bussystem

Bussystem (3.1) bestehend aus einer festen Anzahl oder vorbestimmter Höchstanzahl von Busteilnehmern, die miteinander über ein Übertragungsmedium mit sorgfältig definierter und fester Leistungsstärke/Funktion verbunden sind

3.3

Ausfall der Partnerkommunikation

Situation, in der der Kommunikationspartner nicht verfügbar ist

3.4

unbeabsichtigte Nachrichtenwiederholung

Situation, in der die gleiche *Nachricht* (3.6) versehentlich erneut versendet wird

3.5

Nachrichtenwiederholung

Situation, in der die gleiche *Nachricht* (3.6) absichtlich erneut versendet wird

Anmerkung 1 zum Begriff: Dieses Verfahren, bei dem die gleiche Nachricht erneut gesendet wird, behandelt Ausfälle wie Nachrichtenverlust (3.10).

3.6

Nachricht

elektronische Datenübertragung

Anmerkung 1 zum Begriff: Übertragung können Nutzerdaten, Adresse und Daten zur Gewährleistung der Übertragungsintegrität umfassen.

3.7

ECU

elektronische Steuereinheit

in einem Steuerungssystem in einer Erdbaumaschine verwendetes elektronisches Gerät (elektronische programmierbare Steuerung)

[QUELLE: ISO 22448:2010, 3.3, modifiziert — Die zugelassenen Begriffe „ECM“ und „elektronisches Steuermodul“ wurden entfernt.]

3.8

Ansprechzeit

Zeit von der Erkennung eines sicherheitsrelevanten Ereignisses bis zur Einleitung einer Sicherheitsmaßnahme

3.9

Artefakt

Arbeitsprodukte, die während eines Projekts zum Erfassen und Weiterleiten von Informationen erstellt und verwendet werden

3.10

Nachrichtenverlust

unbeabsichtigte Löschung einer *Nachricht* (3.6) aufgrund des Versagens eines Busteilnehmers

3.11

falsche Abfolge

unbeabsichtigte Änderung der Reihenfolge der *Nachrichten* (3.6) aufgrund des Versagens eines Busteilnehmers

Anmerkung 1 zum Begriff: *Bussysteme* (3.1) können Elemente mit gespeicherten Nachrichten (First In - First Out (FIFO) usw.) enthalten, die die richtige Abfolge abändern können.

3.12

Falsifizierung von Nachrichten

unbeabsichtigte Änderung von *Nachrichten* (3.6) aufgrund eines Fehlers eines Busteilnehmers oder eines Fehlers im Übertragungskanal

3.13

Nachrichtenverzögerung

unbeabsichtigte Verzögerung oder Verhinderung der Sicherheitsfunktion, hervorgerufen durch eine Überlast auf dem Übertragungspfad durch normalen Datenaustausch oder Versenden inkorrekt *Nachrichten* (3.6)

3.14

Alive Counter

Zählelement, das mit „0“ initialisiert wird, sobald das zu überwachende Objekt erstellt oder wiederhergestellt wurde

Anmerkung 1 zum Begriff: Der Zähler erhöht sich von Zeit $t-1$ bis Zeit t , solange das Objekt aktiv ist. Zum Schluss zeigt der Alive Counter den Zeitraum an, in dem das Objekt in einem Netzwerk aktiv war.

3.15

Black-Box-Prüfung

Prüfung eines Objekts, die keine Kenntnis seiner internen Struktur oder seiner konkreten Implementierung erfordert

3.16

Partition

Ressourceneinheit, die einen Anteil eines Speichers, E/A-Geräte und CPU-Verwendung einem oder mehreren *Systemaufträgen* (3.21) zuteilt

Anmerkung 1 zum Begriff: Die Partitionen können einem oder mehreren Subsystemen im Mikrocontroller-Netzwerk zugewiesen werden.

3.17

Software-Partitionierung

Methode zur Eindämmung von *Software-Fehlern* (3.26), die darin besteht, Ressourcen spezifischen Software-Komponenten zuzuweisen, um die Verbreitung eines Software-Fehlers auf mehrere *Partitionen* (3.16) zu verhindern

3.18

Software-Komponente

ein oder mehrere *Software-Module* (3.19)

[QUELLE: ISO 26262-1:2018, 3.157, modifiziert — Das Wort „Einheiten“ wurde durch „Module“ ersetzt.]

3.19

Software-Modul

unabhängiges Teil der Software, das unabhängig geprüft und auf eine Spezifikation zurückgeführt werden kann

Anmerkung 1 zum Begriff: Das Software-Modul ist eine unteilbare Software-Komponente.

3.20

Software-Partitionen

Laufzeitumgebung mit separat zugewiesenen Systemressourcen

3.21

Systemaufgabe

Laufzeiteinheiten, die innerhalb des Ressourcenbudgets der *Partitionen* (3.16) und mit unterschiedlichen Prioritäten ausgeführt werden

3.22

Unabhängigkeit der Software

Ausschluss unbeabsichtigter Interaktionen zwischen Software-Komponenten sowie die Vermeidung von Auswirkungen auf den einwandfreien Betrieb einer Software-Komponente durch Fehler einer anderen Software-Komponente

3.23

Betriebshistorie

Betriebsdaten über eine Software-Komponente oder ein *Software-Modul* (3.19) während dessen Betriebszeit

3.24

gesamte Zykluszeit

feststehende Zeit zum Zugriff auf einen Kommunikationsbus zwischen Knoten auf Bus- oder Knotenebene

Anmerkung 1 zum Begriff: Die Anwendung eines zeitgesteuerten Protokolls sorgt dafür, dass diese Zykluszeit nicht überschritten wird.

3.25

maximale Ansprechzeit

einer Systemaktivität zugewiesene feste Zeit zum Austausch global synchronisierter *Nachrichten* (3.6) auf einem Bus in einer zeitgesteuerten Architektur

3.26

Softwarefehler

falscher Schritt, Prozess oder falsche Datendefinition in Software, der/die dafür sorgt, dass das System unerwartete Ergebnisse hervorbringt

3.27

Auswirkungsanalyse

Dokumentation, die das Verständnis für und die Auswirkungen einer vorgeschlagenen Änderung aufzeichnet

3.28

Konfigurationsmanagementprozess

Aufgabe, Änderungen an den *Artefakten* (3.9) im Entwicklungsprozess nachzuverfolgen und zu kontrollieren

3.29

ständige Übertragung von Nachrichten

Situation, in der der fehlerhafte Knoten ständig *Nachrichten* (3.6) überträgt, die den Betrieb des Bus beeinträchtigt

3.30

Zugangssperre zum Datenbus

Situation, in der der fehlerhafte Knoten sich nicht an die erwarteten Nutzungsmuster hält und übermäßig Dienste anfordert; damit verringert er seine für die anderen Knoten zur Verfügung stehenden Dienste

4 Software-Entwicklung

4.1 Allgemeines

Das Hauptziel der folgenden Anforderungen besteht darin, mittels lesbarer, verständlicher, prüfbarer und wartbarer Software die Zuverlässigkeit der Software sicherzustellen. In diesem Abschnitt werden Empfehlungen für die Gestaltung von Software und den folgenden dazugehörigen Prüfungen gegeben. Die Vermeidung von Software-Fehlern muss während des gesamten Software-Entwicklungsprozesses berücksichtigt werden.

Wenn eine bestehende Software-Komponente nach einer früheren Norm entwickelt und durch Anwendung, Verwendung und Validierung nachgewiesen wurde, dass sie das Risiko so gering wie praktisch möglich hält, gibt es keine Anforderung an die Aktualisierung der Dokumentation des Software-Lebenszyklus auf der Software-Modulebene.

Die Maschinensteuerungssoftware muss den Sicherheitsanforderungen dieses Abschnitts entsprechen. Darüber hinaus muss die Maschinensteuerungssoftware im Hinblick auf die Gefährdungen, die relevant, aber nicht signifikant sind und die nicht in diesem Dokument behandelt werden, nach den Leitsätzen der ISO 12100:2010 konstruiert und entwickelt sein.

4.2 Planung

Es muss ein Zeitplan erstellt werden, welcher die Beziehung zwischen den einzelnen Phasen der Software-Entwicklung und der zugehörigen Artefakte definiert.

Geeignete Methoden und Maßnahmen von Tabelle 3 bis Tabelle 9 müssen nach dem erforderlichen Performance Level der Maschine (MPLr, en: machine performance level required) für die Software-Entwicklung ausgewählt werden.

Der MPLr des Systems kann durch paralleles Hinzufügen von zwei Systemen eines niedrigeren Performance Levels erzielt werden. Bei parallelem Hinzufügen (nach ISO 19014-2) kann die Software in jedem System nach den niedrigeren MPLr-Anforderungen entwickelt werden. Dies ist nur zulässig, wenn es zwischen beiden Systemen keine gemeinsamen Ausfallursachen gibt.

Die Eignung der gewählten Methoden oder Maßnahmen für die Anwendung muss gerechtfertigt und zu Beginn jeder geplanten Entwicklungsphase durchgeführt werden. Für eine bestimmte Anwendung ist die passende Kombination von Methoden oder Maßnahmen während der Entwicklungsplanung anzugeben. Nicht in Tabelle 3 bis Tabelle 9 angeführte Methoden oder Maßnahmen dürfen angewendet werden.

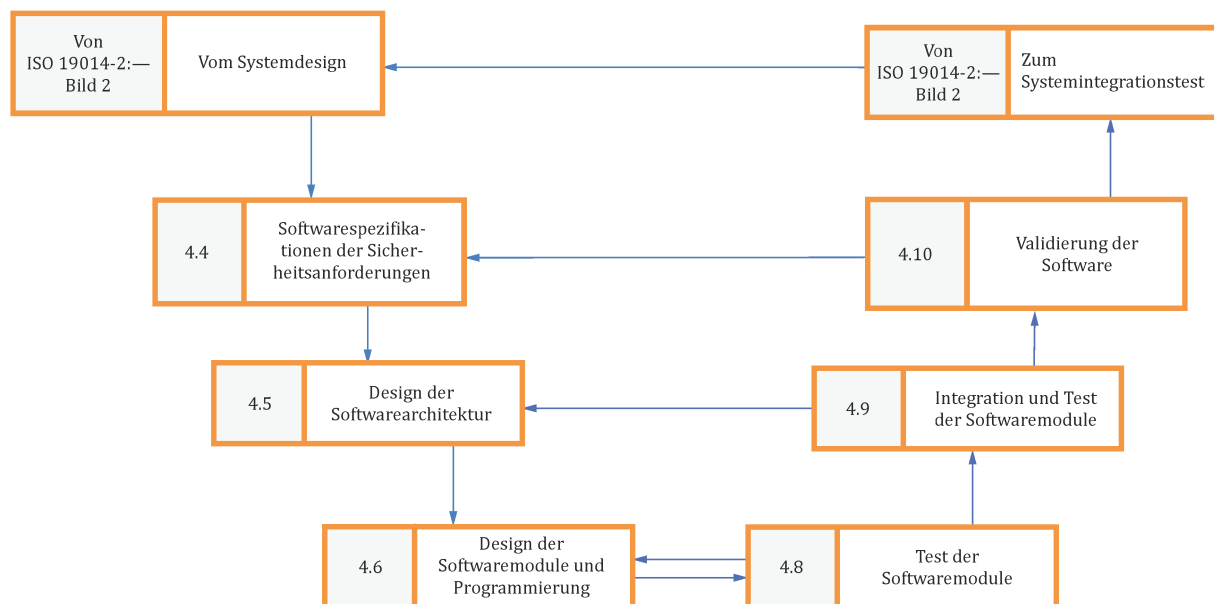


Bild 1 — V-Modell der Software-Entwicklung

Bild 1 ist eine Darstellung einer möglichen Gestaltungsmethode (V-Modell). Jeder organisierte, bewährte Entwicklungsprozess, der die Anforderungen in diesem Dokument erfüllt, darf zur Software-Entwicklung verwendet werden.

Bei der Auswahl der Methoden und Maßnahmen darf neben der manuellen Codierung eine modellbasierte Entwicklung durchgeführt werden, bei der der Quellcode automatisch aus Modellen generiert wird.

Bei jeder Methode oder jeder Maßnahme in den Tabellen gibt es eine unterschiedliche Bestimmung für jeden Performance Level. Tabelle 1 gibt die Anforderungen an.

Tabelle 1 — Spezifikation der Sicherheitsanforderungen an die Software

Symbol	Spezifikation der Sicherheitsanforderungen an die Software
+	Die Methode oder Maßnahme muss für diesen MPLr angewendet werden. Wenn diese Methode oder Maßnahme nicht angewendet wird, muss die Begründung dafür während der Sicherheitsplanungsphase dokumentiert werden.
o	Die Methode oder Maßnahme kann für diesen MPLr angewendet werden.
—	Die Methode oder Maßnahme ist nicht für die Einhaltung dieses MPLr geeignet.

Es müssen die dem jeweiligen MPLr entsprechenden Methoden und Maßnahmen gewählt werden. Alternative oder gleichwertige Methoden und Maßnahmen sind durch Buchstaben nach der Zahl gekennzeichnet. Es muss mindestens eine der alternativen oder gleichwertigen Methoden und Maßnahmen gewählt werden, die mit einem „+“ gekennzeichnet sind. In einem solchen Fall ist es nicht erforderlich, eine Begründung anzugeben. Ein Beispiel hierfür ist Tabelle 2.

Tabelle 2 — Beispielspezifikation der Sicherheitsanforderungen an die Software

Methode/Maßnahme		MPLr = a	MPLr = b, c	MPLr = d	MPLr = e
1.a	Maßnahme 1	+	+	–	–
1.b	Maßnahme 2	+	+	+	+
1.c	Maßnahme 3	+	+	+	+

In diesem Fall gilt:

- eine Maßnahme von Maßnahme 1, Maßnahme 2 oder Maßnahme 3 muss für MPLr = a, b, c erfüllt werden;
- eine Maßnahme von Maßnahme 2 oder Maßnahme 3 muss für MPLr = d, e erfüllt werden;
- andernfalls muss eine Begründung für die nicht spezifizierte alternative Methode/Maßnahme angegeben werden, um die Anforderung der Norm für den spezifischen MPLr zu erfüllen.

Es muss eine Begründung oder Rechtfertigung angegeben werden, wenn andere gleichwertige Methoden statt der angeführten Methoden oder Maßnahmen verwendet werden.

Wenn eine Software-Komponente sich auf verschiedene Sicherheitsfunktionen mit einem anderen MPLr auswirkt, dann gelten die Anforderungen im Zusammenhang mit dem höchsten MPLr.

Wenn die Software sicherheitsbezogene und nicht sicherheitsbezogene Komponenten enthält, dann muss der gesamtintegrierte erreichte Performance Level der Maschine (MPLa, en: machine performance level achieved) auf die Software-Komponente mit dem niedrigsten MPLa begrenzt werden; diese Anforderung gilt nicht, wenn eine ausreichende Unabhängigkeit zwischen den Software-Komponenten in Übereinstimmung mit Abschnitt 7 nachgewiesen werden kann.

Wenn eine Software-Komponente wiederverwendet wird, die modifiziert werden soll, muss eine Auswirkungsanalyse durchgeführt werden. Ein Maßnahmenplan muss erstellt und für den Software-Gesamtlebenszyklus umgesetzt werden, basierend auf den Ergebnissen der Auswirkungsanalyse, um die Einhaltung der Sicherheitsziele zu sicherstellen.

4.3 Artefakte

Sobald die einzelnen Software-Entwicklungsphasen festgelegt worden sind, müssen die Artefakte für jede durchzuführende Phase definiert werden. Weitere Phasen und dazugehörige Artefakte können durch Aufteilung der Aktivitäten und Aufgaben hinzugefügt werden. Mit Blick auf das Ausmaß und die Komplexität des Projekts dürfen alle Artefakte in den einzelnen in Bild 1 dargestellten Phasen modifiziert werden.

ANMERKUNG Es ist üblich, einzelne Phasen zu kombinieren, wenn die verwendete Methode/Maßnahme eine klare Unterscheidung zwischen den Phasen erschwert. So können beispielsweise die Gestaltung der Software-Architektur und die Software-Implementierung nacheinander mit demselben rechnergestützten Entwicklungstools generiert werden, wie dies im modellbasierten Entwicklungsprozess der Fall ist.

Im Rahmen des Software-Entwicklungsprozesses müssen die Artefakte:

- a) entsprechend der von den geplanten Phasen erwarteten Ergebnisse dokumentiert werden;
- b) als Folge einer Auswirkungsanalyse modifiziert werden, und nur die beeinträchtigte Software muss regressionsgeprüft werden;

c) von einem Konfigurationsmanagementprozess erfasst werden.

Das erste Artefakt, das für diesen Prozess angewendet wird, ist der Software-Entwicklungsplan. Die folgenden im Plan festgelegten Artefakte müssen enthalten:

- Gestaltungsspezifikation und dazugehörigen Verifizierungsbericht für jede Software-Gestaltungsphase (absteigender Ast des V-Modells in Bild 1);
- Prüfspezifikation und dazugehörigen Prüfbericht für jede Software(SW)-Designphase (aufsteigender Ast des V-Modells in Bild 1);
- ausführbare Software.

4.4 Spezifikation der Sicherheitsanforderungen an die Software

Die Spezifikation der Software-Sicherheitsanforderungen muss, falls zutreffend, die Anforderungen an die Software beschreiben:

- Funktionen, die es dem System ermöglichen, einen sicheren Zustand zu erreichen oder aufrechtzuerhalten;
- Funktionen zur Erkennung, Anzeige und Handhabung von Fehlern in den sicherheitsbezogenen Teilen des Steuersystems (SRP/CS);
- Funktionen zur Erkennung, Anzeige und Handhabung von Fehlern in der Software;
- Funktionen für die Online- und Offline-Prüfungen der Sicherheitsfunktionen;

ANMERKUNG 1 Eine Online-Prüfung wird ausgeführt, während das geprüfte System in Betrieb ist. Eine Offline-Prüfung wird ausgeführt, während das geprüfte System nicht in Betrieb ist.

ANMERKUNG 2 Ein Beispiel für eine Online-Prüfung wäre die Fehlersuche im Steuersystem während des Fahrens der Maschine. Ein Beispiel für eine Offline-Prüfung wäre die Fehlersuche im Steuersystem, bevor die Maschine zur Bewegung freigegeben wird.

- Funktionen, die Modifizierungen sicherheitsbezogener Software-Parameter zulassen;
- Schnittstellen mit nicht sicherheitsbezogenen Funktionen;
- Leistung und Ansprechzeit;
- Schnittstellen zwischen Software und Hardware des elektronischen Steuergeräts.

Geeignete Methoden oder Maßnahmen müssen aus Tabelle 3 ausgewählt werden, um den angegebenen MPLr einzuhalten.

Tabelle 3 — Spezifikation der Sicherheitsanforderungen an die Software

Methode/Maßnahme		Referenz	MPLr = a	MPLr = b, c	MPLr = d	MPLr = e
1.	Spezifikation der Anforderungen in natürlicher Sprache	A.1	+	+	+	+
2.	Rechnergestützte Spezifikationstools	A.2	o	o	o	+
3.a	Informelle Methoden	A.3	+	+	+	—
3.b	Halbformelle Methoden	A.4	+	+	+	+
3.c	Formelle Methoden	A.5	+	+	+	+
4.	Nachverfolgbarkeit nach vorn zwischen den Systemsicherheitsanforderungen und den Software-Sicherheitsanforderungen	A.6	o	o	o	+
5.	Rückverfolgbarkeit zwischen den Software-Sicherheitsanforderungen und den Systemsicherheitsanforderungen		o	o	o	+
6.a	Walkthrough der Software-Sicherheitsanforderungen	A.7	+	+	+	—
6.b	Inspektion der Software-Sicherheitsanforderungen	A.8	+	+	+	+
ANMERKUNG Die detaillierte Beschreibung dieser Methoden/Maßnahmen findet sich in Anhang A.						

4.5 Gestaltung der Software-Architektur

Es muss eine Software-Architektur entwickelt werden, die basierend auf den Software-Sicherheitsanforderungen die hierarchische Struktur für alle sicherheitsbezogenen Software-Komponenten jeder Sicherheitssteuerung (SCS, en: safety control system) beschreibt. Geeignete Methoden oder Maßnahmen müssen aus Tabelle 4 ausgewählt werden, um den angegebenen MPLr einzuhalten.