DIN EN ISO 19014-4

ICS 53.100

Einsprüche bis 2024-04-23
Vorgesehen als Ersatz für
DIN EN ISO 19014-4:2021-01

Entwurf

Erdbaumaschinen – Funktionale Sicherheit – Teil 4: Gestaltung und Beurteilung von Software und Datenübertragung für sicherheitsrelevante Steuerungssysteme (ISO/DIS 19014-4:2024); Deutsche und Englische Fassung prEN ISO 19014-4:2024

Earth-moving machinery –
Functional safety –
Part 4: Design and evaluation of software and data transmission for safety-related parts of the control system (ISO/DIS 19014-4:2024);
German and English version prEN ISO 19014-4:2024

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/DIS 19014-4:2024);
Version allemande et anglaise prEN ISO 19014-4:2024

Anwendungswarnvermerk

Dieser Entwurf mit Erscheinungsdatum 2024-02-23 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil das beabsichtigte Dokument 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 nam@vdma.org 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 Maschinenbau (NAM), 60498 Frankfurt am Main, Postfach 71 08 64 oder Lyoner Str. 18, 60528 Frankfurt am Main.

Es wird gebeten, mit den Kommentaren zu diesem Entwurf jegliche relevanten Patentrechte, die bekannt sind, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 103 Seiten

DIN-Normenausschuss Maschinenbau (NAM)

Documents
Document Sharing Hub

Full document details: E DIN EN ISO 19014-4:2024-04

Nationales Vorwort

Dieser Norm-Entwurf enthält sicherheitstechnische Festlegungen.

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung beigefügt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen Text.

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

Dieser Norm-Entwurf konkretisiert einschlägige Anforderungen von Anhang I der EU-Maschinenrichtlinie 2006/42/EG an erstmals im Europäischen Wirtschaftsraum (EWR) in Verkehr gebrachte Maschinen, um den Nachweis der Übereinstimmung mit diesen Anforderungen zu erleichtern.

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

ISO 6165:2012	siehe	DIN EN ISO 6165:2013-02*
ISO 12100:2010	siehe	DIN EN ISO 12100:2011-03**
ISO 13849-1:2023	siehe	DIN EN ISO 13849-1:2023-12
ISO 13849-2:2012	siehe	DIN EN ISO 13849-2:2013-02
ISO 19014-1:202X	siehe	DIN EN ISO 19014-1:202X
ISO 19014-2:202X	siehe	DIN EN ISO 19014-2:202X

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

Änderungen

Gegenüber DIN EN ISO 19014-4:2021-01 wurden folgende Änderungen vorgenommen:

a) ausführlicher Anhang ZA hinzugefügt;

b) Bezugsnormen datiert.

---

* Dokument wurde zurückgezogen und durch DIN EN ISO 6165:2023-03 ersetzt.

** Korrigiert durch DIN EN ISO 12100 Berichtigung 1:2013-08.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO 19014-4:2024-04

Nationaler Anhang NA
(informativ)

Literaturhinweise

DIN EN ISO 6165:2013-02, *Erdbaumaschinen — Grundtypen — Identifizierung und Begriffe (ISO 6165:2012); Deutsche Fassung EN ISO 6165:2022*

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

DIN EN ISO 13849-1:2023-12, *Sicherheit von Maschinen — Sicherheitsbezogene Teile von Steuerungen — Teil 1: Allgemeine Gestaltungsleitsätze (ISO 13849-1:2023); Deutsche Fassung EN ISO 13849-1:2023*

DIN EN ISO 19014-1:202X, *Erdbaumaschinen — Funktionale Sicherheit — Teil 1: Methodik zur Bestimmung sicherheitsbezogener Teile der Steuerung und deren Leistungsanforderungen (ISO 19014-1:202X; Deutsche Fassung EN ISO 19014-1:202X)*

DIN EN ISO 19014-2:202X, *Erdbaumaschinen — Funktionale Sicherheit — Teil 2: Entwurf und Bewertung von Hardware- und Architekturanforderungen für sicherheitsrelevante Teile des Steuerungssystems (ISO 19014-2:202X); Deutsche Fassung EN ISO 19014-2:202X*

Documents
Document Sharing Hub

Full document details: E DIN EN ISO 19014-4:2024-04

– Leerseite –

Documents
Document Sharing Hub

Full document details: E DIN EN ISO 19014-4:2024-04

Januar 2024

prEN ISO 19014-4

Erdbaumaschinen – Funktionale Sicherheit – Teil 4: Gestaltung und Beurteilung von Software und Datenübertragung für sicherheitsrelevante Steuerungssysteme (ISO/DIS 19014-4:2024)

Earth-moving machinery – Functional safety – Part 4: Design and evaluation of software and data transmission for safety-related parts of the control system (ISO/DIS 19014-4:2024)

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/DIS 19014-4:2024)

Documents
Document Sharing Hub

Full document details: E DIN EN ISO 19014-4:2024-04

E DIN EN ISO 19014-4:2024-04
prEN ISO 19014-4:2024 (D)

Inhalt

Seite

Europäisches Vorwort 5
Anhang ZA (informativ) Zusammenhang zwischen dieser Europäischen Norm und den grundlegenden Anforderungen der abzudeckenden Richtlinie 2006/42/EG 6
Vorwort 7
Einleitung 8
1 Anwendungsbereich 9
2 Normative Verweisungen 9
3 Begriffe 9
4 Software-Entwicklung 13
4.1 Allgemeines 13
4.2 Planung 13
4.3 Artefakte 15
4.4 Spezifikation der Sicherheitsanforderungen an die Software 16
4.5 Gestaltung der Software-Architektur 17
4.6 Software-Modulgestaltung und Codierung 17
4.7 Sprache und Tool-Auswahl 19
4.8 Prüfen von Software-Modulen 19
4.9 Software-Modulintegration und -prüfung 20
4.10 Software-Validierung 21
5 Softwarebasierte Parametrierung 22
5.1 Allgemeines 22
5.2 Datenintegrität 22
5.3 Verifizierung softwarebasierter Parametrierung 23
6 Schutz der Übertragung sicherheitsbezogener Nachrichten in Bussystemen 23
7 Unabhängigkeit durch Software-Partitionierung 25
7.1 Allgemeines 25
7.2 Mehrere Partitionen in einem einzelnen Mikrocontroller 26
7.3 Mehrere Partitionen im Rahmen eines ECU-Netzwerks 28
8 Benutzerinformationen 28
8.1 Allgemeines 28
8.2 Betriebsanleitung 28
Anhang A (informativ) Beschreibung der Software-Methoden/Maßnahmen 30
A.1 Spezifikation der Anforderungen in natürlicher Sprache 30
A.2 Rechnergestützte Spezifikationstools 30
A.3 Informelle Methoden 30
A.4 Halbformelle Methoden 30
A.5 Formelle Methoden 30
A.6 Nachverfolgbarkeit der Sicherheitssoftware 30
A.7 Walkthrough 32
A.8 Inspektion 32
A.9 Rechnergestützte Gestaltungstools 33
A.10 Sicherheitsleistung in Echtzeit 33
A.11 Gestaltungsregeln 33
A.12 Dynamische Variablen oder Objekte ohne Online-Prüfung 34
A.13 Dynamische Variablen oder Objekte mit Online-Prüfung 34
A.14 Modularisierung 34
A.15 Strukturierte Programmierung 35
A.16 Defensive Programmierung 36
A.17 Verwendung vertrauenswürdiger/verifizierter Software-Elemente 36
A.18 Geeignete Programmiersprache 37
A.19 Unterstützung der Sprachteilmenge 37

Documents
Document Sharing Hub

Full document details: E DIN EN ISO 19014-4:2024-04

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 . . . 39
A.26 Funktions-/Black-Box-Prüfung . . . 40
A.27 Strukturabhängige Prüfungen . . . 40
A.28 Äquivalenzklassen und Eingabe-Partitionsprüfungen . . . 40
A.29 Prüffallausführung aus modellbasierter Prüffallgenerierung . . . 41
A.30 Leistungsnachweis . . . 41
A.31 SW-Modulschnittstellenprüfung . . . 42
A.32 Direkte Vergleichsprüfung . . . 43
Anhang B (normativ) **Prüfumgebungen für Softwarevalidierung . . . 44**
B.1 Maschinennetzwerkprüfung . . . 44
B.2 Hardware-in-the-Loop-Prüfung . . . 44
B.3 Prüfung der Maschinenebene . . . 45
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

Bilder

Bild 1 — V-Modell der Software-Entwicklung . . . 14
Bild 2 — Mikrocontroller-Netzwerk aus elektronischen Steuereinheiten auf einem Datenbus . . . 24
Bild 3 — Mehrere Partitionen in einem einzelnen Mikrocontroller . . . 27
Bild B.1 — Maschinennetzwerkprüfung . . . 44
Bild B.2 — Hardware-in-the-Loop-Prüfung . . . 45
Bild B.3 — Prüfung der Maschinenebene . . . 46

Documents
Document Sharing Hub

Full document details: E DIN EN ISO 19014-4:2024-04

Tabellen

Tabelle ZA.1 — Übereinstimmung zwischen dieser Europäischen Norm und Anhang I der Richtlinie 2006/42/EG 6
Tabelle 1 — Spezifikation der Sicherheitsanforderungen an die Software 14
Tabelle 2 — Beispielspezifikation der Sicherheitsanforderungen an die Software 15
Tabelle 3 — Spezifikation der Sicherheitsanforderungen an die Software 16
Tabelle 4 — Gestaltung der Software-Architektur 17
Tabelle 5 — Software-Modulgestaltung und Codierung 18
Tabelle 6 — Sprache und Tool-Auswahl 19
Tabelle 7 — Prüfen von Software-Modulen 20
Tabelle 8 — Software-Modulintegration und -prüfung 21
Tabelle 9 — Software-Validierung 22
Tabelle 10 — Steuerung von Übertragungsfehlern und Performance Level 23
Tabelle 11 — Steuerung von Übertragungsfehlern und Performance Level 25
Tabelle 12 — Methoden und Maßnahmen innerhalb des Mikrocontrollers 28
Tabelle C.1 — Definition der Datenintegritätsparameter 47
Tabelle C.2 — Datenintegrität in Abhängigkeit vom MPL 48

Documents
Document Sharing Hub

Full document details: E DIN EN ISO 19014-4:2024-04

Europäisches Vorwort

Dieses Dokument (prEN ISO 19014-4:2024) 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.

Dieses Dokument ist derzeit zur parallelen Umfrage vorgelegt.

Dieses Dokument wird EN ISO 19014-4:2020 ersetzen.

Rückmeldungen oder Fragen zu diesem Dokument sollten an das jeweilige nationale Normungsinstitut des Anwenders gerichtet werden. Eine vollständige Liste dieser Institute ist auf den Internetseiten von CEN abrufbar.

Anerkennungsnotiz

Der Text von ISO/DIS 19014-4:2024 wurde von CEN als prEN ISO 19014-4:2024 ohne irgendeine Abänderung genehmigt.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO 19014-4:2024-04

Anhang ZA
(informativ)

Zusammenhang zwischen dieser Europäischen Norm und den grundlegenden Anforderungen der abzudeckenden Richtlinie 2006/42/EG

Tabelle ZA.1 — Übereinstimmung zwischen dieser Europäischen Norm und Anhang I der Richtlinie 2006/42/EG

Die relevanten grundlegenden Anforderungen der Richtlinie 2006/42/EG	Abschnitt(e)/Unterabschnitt(e) dieser EN	Anmerkungen/Hinweise
1.2.1	4	
1.7.4.2 (g)	8	

Documents
Document Sharing Hub

Full document details: E DIN EN ISO 19014-4:2024-04

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 Directives, 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 Directives, Teil 2, erarbeitet (siehe www.iso.org/directives).

ISO weist auf die Möglichkeit hin, dass die Anwendung dieses Dokuments mit der Verwendung eines oder mehrerer Patente verbunden sein kann. 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*, in Übereinstimmung mit der Vereinbarung zur technischen Zusammenarbeit zwischen ISO und CEN (Wiener Vereinbarung) erarbeitet.

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

Die wesentlichen Änderungen sind folgende:

— ausführlicher Anhang ZA hinzugefügt;

— Bezugsnormen datiert;

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.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO 19014-4:2024-04

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 12100:2010 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);

— Verbraucher (falls die behandelten Maschinen für die Nutzung durch Verbraucher bestimmt sind).

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 Typ-B-Normen abweichen, haben die Anforderungen dieser Typ-C-Norm Vorrang gegenüber den Anforderungen der anderen Normen.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO 19014-4:2024-04

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 6165:2012 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 6165:2012, *Earth-moving machinery — Basic types — Identification and terms and definitions*

ISO 6750-1:2019, *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 13849-1:2023, *Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design*

ISO 19014-1:202X, *Earth-moving machinery — Functional safety — Part 1: Methodology to determine safety-related parts of the control system and performance requirements*

ISO 19014-2:202X, *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 https://www.electropedia.org/

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, Hochfrequenz-

AVA Documents Document Sharing Hub

Full document details: E DIN EN ISO 19014-4:2024-04

übertragung) 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 Kommunikation zwischen Teilnehmern
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

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO 19014-4:2024-04

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 inkorrekter *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.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO 19014-4:2024-04

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 Konten 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

Documents
Document Sharing Hub

Full document details: E DIN EN ISO 19014-4:2024-04

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, darf es keine Anforderung an die Aktualisierung der Dokumentation des Software-Lebenszyklus auf der Software-Modulebene geben.

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 konstruiert und entwickelt sein.

4.2 Planung

Es muss ein Plan 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 die Parallelschaltung 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.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO 19014-4:2024-04

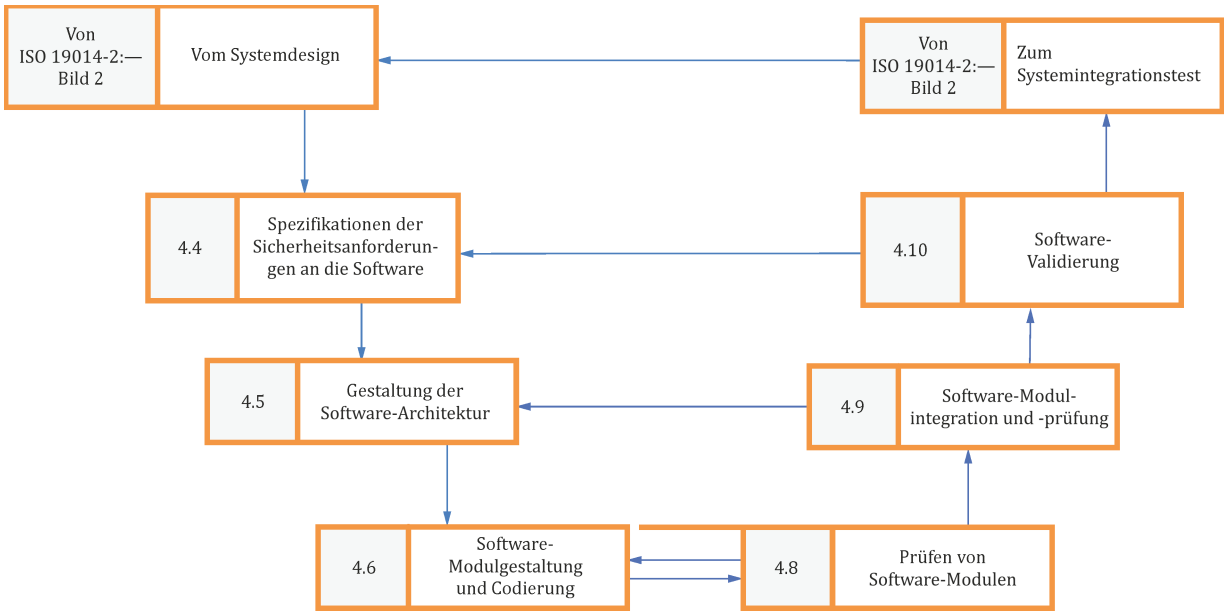

Bild 1 — V-Modell der Software-Entwicklung

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 darf 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.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO 19014-4:2024-04

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.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO 19014-4:2024-04

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	+	+	+	+

Documents
Document Sharing Hub

Full document details: E DIN EN ISO 19014-4:2024-04

Tabelle 3 (*fortgesetzt*)

Methode/Maßnahme		Referenz	MPLr = a	MPLr = b, c	MPLr = d	MPLr = e
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.

Tabelle 4 — Gestaltung der Software-Architektur

Methode/Maßnahme		Referenz	MPLr = a	MPLr = b, c	MPLr = d	MPLr = e
1.a	Informelle Methoden	A.3	+	+	+	—
1.b	Halbformelle Methoden	A.4	+	+	+	+
1.c	Formelle Methoden	A.5	+	+	+	+
2.	Rechnergestützte Gestaltungstools	A.9	o	o	o	+
3.a	Zyklisches Verhalten, mit garantierter maximaler Zykluszeit	A.10	o	o	+	+
3.b	Zeitgesteuerte Architektur		o	o	+	+
3.c	Ereignisgesteuert, mit garantierter maximaler Ansprechzeit		o	o	+	+
4.	Nachverfolgbarkeit nach vorn zwischen den Software-Sicherheitsanforderungen und der Software-Architektur	A.6	o	o	o	+
5.	Rückverfolgbarkeit zwischen der Software-Architektur und der Spezifikation der Software-Sicherheitsanforderungen		o	o	o	+
6.a	Walkthrough der Software-Architektur	A.7	+	+	+	—
6.b	Inspektion der Software-Architektur	A.8	+	+	+	+
ANMERKUNG Die detaillierte Beschreibung dieser Methoden/Maßnahme findet sich in Anhang A.						

4.6 Software-Modulgestaltung und Codierung

Die Ziele dieser Phase der Software-Entwicklung lauten:

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO 19014-4:2024-04

— detaillierte Spezifizierung des Verhaltens der sicherheitsbezogenen Software-Module, die von der Software-Architektur vorgeschrieben sind;

— Erstellung lesbarer, prüfbarer und wartbarer Software-Module (z. B. manueller Code, Modell usw.);

— Verifizierung, dass die Software-Architektur vollständig und richtig implementiert wurde.

Geeignete Methoden oder Maßnahmen müssen aus Tabelle 5 ausgewählt werden, um den angegebenen MPLr einzuhalten. Es ist nicht erforderlich, den automatisch erzeugten Code zu überprüfen.

Tabelle 5 — Software-Modulgestaltung und Codierung

Methode/Maßnahme		Referenz	MPLr = a	MPLr = b, c	MPLr = d	MPLr = e
1.a	Informelle Methoden	A.3	+	+	—	—
1.b	Halbformelle Methoden	A.4	+	+	+	+
1.c	Formelle Methoden	A.5	+	+	+	+
2.	Rechnergestütztes Gestaltungstool	A.9	o	o	o	+
3.	Verwendung von Gestaltungs- und Codierungsnormen	A.11	o	+	+	+
4.	Kein unstrukturierter Steuerungsablauf in Programmen in übergeordneten Sprachen[b]		o	o	+	+
5.	Begrenzte automatische Typkonvertierung[b]		o	o	+	+
6.	Eingeschränkte Verwendung von Interrupts[b]		o	o	o	+
7.	Begrenzte Verwendung von Zeigern[b]		o	o	o	+
8.	Eingeschränkte Verwendung von Rekursionen		o	o	o	+
9.a	Dynamische Variablen oder Objekte ohne Online-Prüfung[b]	A.12	o	o	—	—
9.b	Dynamische Variablen oder Objekte mit Online-Prüfung[b]	A.13	o	o	+	+
10.	Größenbeschränkung von Software-Modulen	A.14	+	+	+	+
11.	Ein Eintritts-/ein Austrittspunkt in Unterprogrammen und Funktionen[b]		o	+	+	+
12.	Vollständig festgelegte Schnittstelle		o	+	+	+
13.	Verbergen/Kapseln von Informationen		o	o	+	+
14.	Software-Komplexitätskontrolle		o	o	o	+
15.	Strukturierte Gestaltung oder Codierung	A.15	o	+	+	+
16.	Defensive Gestaltung oder Codierung	A.16	o	o	o	+
17.	Verwendung vertrauenswürdiger/verifizierter Software-Elemente[a]	A.17	o	o	o	o
18.	Nachverfolgbarkeit nach vorn zwischen den Software-Sicherheitsanforderungen und der Software-Gestaltung	A.6	o	o	o	+
19.a	Walkthrough der Software-Gestaltung, des Quellcodes oder von beidem	A.7	+	+	+	—

Documents
Document Sharing Hub

Full document details: E DIN EN ISO 19014-4:2024-04

Tabelle 5 (*fortgesetzt*)

Methode/Maßnahme		Referenz	MPLr = a	MPLr = b, c	MPLr = d	MPLr = e
19.b	Inspektion der Software-Gestaltung, des Quellcodes oder von beidem	A.8	+	+	+	+
ANMERKUNG Die detaillierte Beschreibung dieser Methoden/Maßnahmen findet sich in Anhang A.						
[a] Es werden dringend vertrauenswürdige und verifizierte Software-Elemente empfohlen. [b] Diese Methoden oder Maßnahmen sind nicht immer für in der modellbasierten Entwicklung verwendete grafische Modellierungsnotationen anwendbar.						

4.7 Sprache und Tool-Auswahl

Die Sicherheitsintegrität der zu entwickelnden Software kann direkt von der ausgewählten Programmiersprache, dem für Entwicklung und Prüfung verwendeten Tool und der Verwendung bestehender, vertrauenswürdiger, verifizierter Software-Module beeinflusst werden. Geeignete Methoden oder Maßnahmen müssen aus Tabelle 6 ausgewählt werden, um den angegebenen MPLr einzuhalten.

Tabelle 6 — Sprache und Tool-Auswahl

Methode/Maßnahme		Referenz	MPLr = a	MPLr = b, c	MPLr = d	MPLr = e
1.	Geeignete Programmiersprache	A.18	+	+	+	+
2.	Unterstützung der Sprachteilmenge	A.19	o	o	o	+
3.a	Tools und Übersetzungsprogramme mit erhöhter Bewährtheit im Betrieb oder in der Validierung	A.20	o	+	+	+
3.b	Zertifizierte Tools und zertifizierte Übersetzungsprogramme	A.21	o	+	+	+
ANMERKUNG Die detaillierte Beschreibung dieser Methoden/Maßnahmen findet sich in Anhang A.						

4.8 Prüfen von Software-Modulen

Software-Modulprüfungen haben zum Ziel, zu verifizieren, dass die entworfenen und implementierten Software-Module die Software-Sicherheitsanforderungen korrekt erfüllen. In dieser Phase muss ein Verfahren für das Prüfen der Software-Module gegen ihre Anforderungen erstellt und die Prüfungen entsprechend diesem Verfahren durchgeführt werden.

Für eine systematische Herangehensweise an die Prüfung von Software-Modulen hilft die Verwendung geeigneter Tools für die Prüfungsverwaltung und Prüfungsautomatik, die arbeitsintensiven und fehleranfälligen Aufgaben beim Prüfen von Software-Modulen zu unterstützen. Da Support-Tools verfügbar sind, bietet sich eine umfassendere Herangehensweise sowohl an normale als auch Regressionsprüfungen an.

Für eine einfachere Verifizierung, Validierung, Bewertung und Wartung sollten alle Daten, Entscheidungen und Begründungen im gesamten Software-Projekt dokumentiert werden. Die Dokumentation der Software-Module sollte Folgendes beinhalten:

— durchgeführte Prüfungen;

— Entscheidungen und deren Begründung;

Documents
Document Sharing Hub
Full document details: E DIN EN ISO 19014-4:2024-04

— Probleme und deren Lösungen.

ANMERKUNG Die Aufzeichnung von Daten ist wichtig für die Wartung von Computersystemen, da die Begründung für bestimmte während des Entwicklungsprojekts getroffene Entscheidungen den Wartungsingenieuren nicht immer bekannt ist.

Geeignete Methoden oder Maßnahmen müssen aus Tabelle 7 ausgewählt werden, um den angegebenen MPLr einzuhalten. Die Prüfung von Software-Modulen darf in verschiedenen Umgebungen durchgeführt werden, zum Beispiel:

— Model-in-the-Loop-Prüfungen,

— Software-in-the-Loop-Prüfungen,

— Processor-in-the-Loop-Prüfungen,

— Hardware-in-the-Loop-Prüfungen.

Tabelle 7 — Prüfen von Software-Modulen

Methode/Maßnahme		Referenz	MPLr = a	MPLr = b, c	MPLr = d	MPLr = e
1.	Grenzwertanalyse	A.22	o	o	+	+
2.	Kontrollflussanalyse	A.23	o	o	+	+
3.	Datenflussanalyse	A.24	o	o	+	+
4.	Prüffallausführung anhand der Grenzwertanalyse	A.25	o	o	o	+
5.	Funktions-/Black-Box-Prüfung [einschließlich Fehlersimulationsprüfung (FI, en: Fault Insertion)]	A.26	+	+	+	+
6.a	Umfang der Strukturprüfung (Eintrittspunkte)	A.27	o	+	—	—
6.b	Umfang der Strukturprüfung (Anweisungen)		o	+	+	—
6.c	Umfang der Strukturprüfung (Verzweigungen)		o	+	+	+
7.	Äquivalenzklassen und Eingabe-Partitionsprüfungen[a]	A.28	o	o	+	+
8.	Prüffallausführung aus modellbasierter Prüffallgenerierung	A.29	o	o	o	+
9.	Prüfung der Ansprechzeiten und Speicherbeschränkungen[a]	A.30	o	+	+	+
10.	Leistungsanforderungsprüfung[a]		o	+	+	+
11.	Belastungs-/Stressprüfung[a]		o	o	o	+
12.	SW-Modulschnittstellenprüfung	A.31	o	o	o	+
13	Direkte Vergleichsprüfung	A.32	o	o	+	+
14.	Nachverfolgbarkeit nach vorn zwischen der Software-Modulgestaltung und den Modul-Prüfspezifikationen	A.6	o	o	o	+

ANMERKUNG Die detaillierte Beschreibung dieser Methoden/Maßnahmen findet sich in Anhang A.

[a] Der Prüfer darf sich dafür entscheiden, dieses Prüfverfahren nicht durchzuführen, muss es aber auf Integrationsebene durchführen, wenn es erforderlich ist.

4.9 Software-Modulintegration und -prüfung

Die Ziele dieser Phase der Software-Entwicklung lauten:

Documents
Document Sharing Hub

Full document details: E DIN EN ISO 19014-4:2024-04

— Integration der Software-Module in Software-Komponenten über die gesamte systemintegrierte Software der Sicherheitssteuerung;

— Verifizierung, dass die Anforderungen an die Software von der systemintegrierten Software korrekt umgesetzt werden.

In dieser Phase werden die einzelnen Integrationsstufen auf die Software-Sicherheitsanforderungen geprüft. Die Schnittstellen zwischen den Software-Modulen und zwischen Software-Modulen und Software-Komponenten werden ebenfalls geprüft. Die Integrationsschritte und Prüfungen der Software-Komponenten müssen direkt der hierarchischen Architektur der Software entsprechen.

Geeignete Methoden/Maßnahmen müssen aus Tabelle 8 ausgewählt werden, um den angegebenen MPLr einzuhalten. Der Prüfer darf sich jedoch dafür entscheiden, ein Prüfverfahren oder eine Maßnahme auf der Integrationsebene nicht anzuwenden, muss die Methode oder Maßnahme aber auf Modulebene durchführen, wenn es erforderlich ist.

Eine Software-Modulintegrationsprüfung darf in verschiedenen Umgebungen durchgeführt werden, zum Beispiel:

— Model-in-the-Loop-Prüfungen,

— Software-in-the-Loop-Prüfungen,

— Processor-in-the-Loop-Prüfungen,

— Hardware-in-the-Loop-Prüfungen.

Tabelle 8 — Software-Modulintegration und -prüfung

	Methode/Maßnahme	**Referenz**	**MPLr = a**	**MPLr = b, c**	**MPLr = d**	**MPLr = e**
1.	Funktions-/Black-Box-Prüfung [einschließlich Fehlersimulationsprüfung (FI, en: Fault Insertion)]	A.26	+	+	+	+
2.	Äquivalenzklassen und Eingabe-Partitionsprüfungen	A.28	o	o	+	+
3.	Ansprechzeiten und Speicherbeschränkungen	A.30	o	+	+	+
4.	Leistungsanforderungsprüfung		o	+	+	+
5.	Belastungs-/Stressprüfung		o	o	o	+
6.	Direkte Vergleichsprüfung	A.32	o	o	+	+
7.	Nachverfolgbarkeit nach vorn zwischen der Software-Architekturgestaltung und den Prüfspezifikationen für Integration	A.6	o	o	o	+
ANMERKUNG Die detaillierte Beschreibung dieser Methoden/Maßnahmen findet sich in Anhang A.						

4.10 Software-Validierung

Das Ziel dieser Phase der Software-Entwicklung ist es, zu zeigen, dass die Software-Sicherheitsanforderungen von der integrierten Software korrekt umgesetzt sind.

Testen muss die wichtigste Methode zur Verifizierung von Software sein. Animation und Modellierung dürfen als Ergänzung der Verifizierungsaktivitäten verwendet werden.

Die Software muss durch Simulation von Folgendem ausgeführt werden:

AVA Documents Document Sharing Hub

Full document details: E DIN EN ISO 19014-4:2024-04

— im Normalbetrieb vorhandene Eingabesignale;

— erwartete Vorkommnisse;

— unerwünschte Umstände, die eine Systemaktion erfordern.

Die Wirksamkeit der angewendeten Prüfverfahren und aller anderen verwendeten Maßnahmen muss anhand der Spezifikationen der Sicherheitsanforderungen nach Abschluss des Verifizierungsverfahrens ausgewertet werden.

Geeignete Methoden/Maßnahmen müssen aus Tabelle 9 ausgewählt werden, um den angegebenen MPLr einzuhalten.

Tabelle 9 — Software-Validierung

Methode/Maßnahme		Referenz	MPLr = a	MPLr = b, c	MPLr = d	MPLr = e
1.a	Maschinennetzwerkprüfung	B.1	+	+	+	+
1.b	Hardware-in-the-Loop-Prüfung	B.2	+	+	+	+
1.c	Prüfung der Maschinenebene	B.3	+	+	+	+
2.	Nachverfolgbarkeit nach vorn zwischen den Software-Sicherheitsanforderungen und dem Software-Verifizierungsplan (einschließlich Datenverifizierung)	A.6	o	o	o	+
3.	Rückverfolgbarkeit zwischen dem Software-Verifizierungsplan (einschließlich Datenverifizierung) und den Software-Sicherheitsanforderungen		o	o	o	+
ANMERKUNG Die detaillierte Beschreibung dieser Methoden/Maßnahmen findet sich in Anhang B.						

Das Prüfverfahren muss nach den Festlegungen in Anhang B durchgeführt werden.

5 Softwarebasierte Parametrierung

5.1 Allgemeines

Die softwarebasierte Parametrierung bezieht sich auf die Möglichkeit, das Software-System nach Abschluss der Entwicklung an unterschiedliche Anforderungen anzupassen, indem Parameter zur Modifizierung der Funktionalität der Software geändert werden. Die softwarebasierte Parametrierung sicherheitsbezogener Parameter muss als Teil des SRP/CS betrachtet werden, und muss in der Spezifikation der Software-Sicherheitsanforderungen beschrieben werden.

Softwarebasierte Parameter umfassen:

— Variantencodierung (z. B. Ländercode, Links-/Rechtslenkung usw.);

— Systemparameter (z. B. Wert für niedrige Leerlaufdrehzahl, Motorkennliniendiagramme usw.);

— Kalibrierungsdaten (z. B. maschinenspezifisch, Endanschlag für Gaseinstellung usw.).

5.2 Datenintegrität

Die Integrität der für die Parametrierung verwendeten Daten muss erhalten bleiben, und Modifizierungen durch Unbefugte müssen verhindert werden. Dies muss durch Anwendung von Methoden oder Maßnahmen erreicht werden, um Folgendes zu überwachen:

Documents
Document Sharing Hub

Full document details: E DIN EN ISO 19014-4:2024-04

— den Bereich gültiger Eingaben;

— Datenkorruption vor und nach der Übertragung;

— die Fehler aus dem Parameterübertragungsprozess;

— die Auswirkungen einer unvollständigen Parameterübertragung und

— die Fehler- und Ausfallwirkungen der Hardware und Software des für die Parametrierung verwendeten Tools.

5.3 Verifizierung softwarebasierter Parametrierung

Folgende Verifizierungsaktivitäten müssen für die softwarebasierte Parametrierung durchgeführt werden:

— Verifizierung der gültigen Einstellung jedes sicherheitsbezogenen Parameters (Minimum, Maximum und repräsentative Werte);

— Verifizierung, dass die sicherheitsbezogenen Parameter durch Verwendung ungültiger in die Software eingeschriebener Werte während der Konfigurationsphase zur Verifizierung deren Verhaltens auf Plausibilität überprüft wurden;

— Verifizierung, dass eine unbefugte Modifizierung sicherheitsbezogener Parameter verhindert wird;

— Verifizierung, dass die Daten/Signale für die Parametrierung so generiert und verarbeitet werden, dass Fehler nicht zu einem Verlust der sicherheitsbezogenen Funktionen führen können.

6 Schutz der Übertragung sicherheitsbezogener Nachrichten in Bussystemen

In diesem Abschnitt werden Empfehlungen für den Übertragungsschutz in SCS und in der Kommunikation verwendeten sicherheitsbezogenen Nachrichten gegeben, die, wie in Bild 2 dargestellt, zwischen verschiedenen Komponenten (z. B. Mikrocontroller, intelligente Sensoren, intelligente Aktoren) eines SCS stattfinden kann.

ANMERKUNG 1 Zum Zeitpunkt der Veröffentlichung werden nur die gekapselten Bussysteme berücksichtigt, bei denen der Hersteller Anzahl und Typ der Busteilnehmer (d. h. an den Bus angeschlossene Einheiten) festgelegt hat. Daten- und Adressenbusse in den internen Geräten von CPU und ECU werden nicht berücksichtigt.

Geeignete Methoden und Maßnahmen aus Tabelle 11 müssen wie in Tabelle 10 zur Steuerung der Fehler implementiert werden.

Tabelle 10 — Steuerung von Übertragungsfehlern und Performance Level

Übertragungsfehler	MPLr = a, b, c	MPLr = d,e
Ausfall der Kommunikation zwischen Teilnehmern	JA[a]	JA
Falsifizierung von Nachrichten	JA[a]	JA
Nachrichtenwiederholung	NEIN	JA
Nachrichtenverlust	JA[a]	JA
Einfügung von Nachrichten	NEIN	JA
Falsche Abfolge	NEIN	JA
Nachrichtenverzögerung	JA[a]	JA

Documents
Document Sharing Hub
Full document details: E DIN EN ISO 19014-4:2024-04

Tabelle 10 (*fortgesetzt*)

Übertragungsfehler	MPLr = a, b, c	MPLr = d,e
Zugangssperre zum Datenbus	JA[a]	JA
Ständige Übertragung von Nachrichten	JA[a]	JA
[a] Gilt nicht für Systeme der Kategorie B oder 1, da kein Diagnosedeckungsgrad erforderlich ist.		

ANMERKUNG 2 Techniken können in Protokollen implementiert werden, wie z. B. SAE J1939, um Übertragungsfehler zu behandeln.

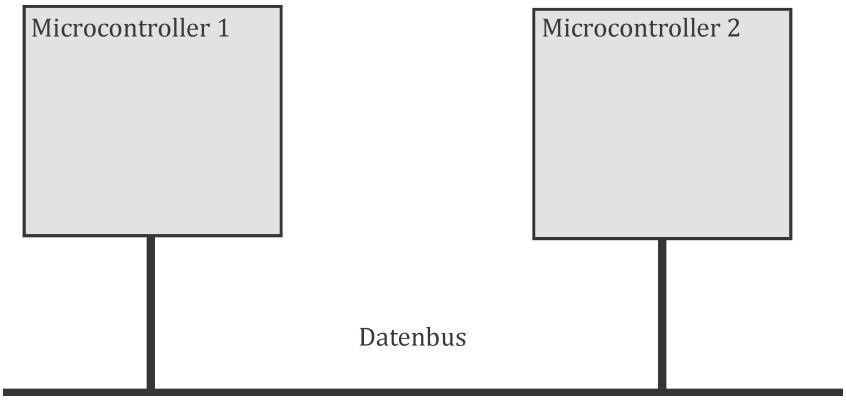

Bild 2 — Mikrocontroller-Netzwerk aus elektronischen Steuereinheiten auf einem Datenbus

In Tabelle 11 werden einige der Methoden und Maßnahmen zum Schutz vor Übertragungsfehlern definiert, indem bestimmte Fehlerwirkungen ausgeschlossen werden, die in Verbindung mit der Kommunikation oder dem Schutz der sicherheitsbezogenen Daten im SCS stehen. Es dürfen andere Methoden und Maßnahmen zum Schutz vor Fehlern verwendet werden.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO 19014-4:2024-04

Tabelle 11 — Steuerung von Übertragungsfehlern und Performance Level

			Übertragungsfehler (siehe Abschnitt 6)								
			Ausfall der Kommunikation zwischen Teilnehmern	**Ungewollte Nachrichtenwiederholung**	**Nachrichtenverlust**	**Einfügung von Nachrichten**	**Falsche Abfolge**	**Falsifizierung von Nachrichten**	**Nachrichtenverzögerung**	**Zugangssperre zum Datenbus**	**Ständige Übertragung von Nachrichten**
Methode/Maßnahme	**D.1**	**Keep-Alive-Nachrichten**	JA	NEIN	NEIN	NEIN	NEIN	NEIN	NEIN	JA	JA
	D.2	**Alive Counter**	NEIN	JA	JA	JA	NEIN	NEIN	NEIN	NEIN	JA
	D.3	**Zyklische Redundanz-prüfung (CRC, en: cyclic redundancy check)**	NEIN	NEIN	NEIN	NEIN	NEIN	JA	NEIN	NEIN	NEIN
	D.4	**Sequenz-nummer**	NEIN	JA	JA	JA	JA	NEIN	NEIN	NEIN	JA
	D.5	**Nachrichten-wiederholung**	NEIN	NEIN	JA	NEIN	JA	JA	NEIN	NEIN	NEIN
	D.6	**Watchdog**	JA	NEIN	JA	NEIN	NEIN	NEIN	JA	JA	JA
	D.7	**Zeit-gesteuerter Datenbus**	JA	NEIN	NEIN	JA	NEIN	NEIN	JA	NEIN	NEIN
	D.8	**Buswächter**	NEIN	NEIN	NEIN	NEIN	NEIN	NEIN	NEIN	NEIN	JA
	D.9	**Minislotting**	NEIN	NEIN	NEIN	NEIN	NEIN	NEIN	JA	NEIN	JA

Das Erfüllen des MPLr durch in der Netzwerkkommunikation umgesetzte Maßnahmen darf durch die Berechnung der Datenintegritätssicherung überprüft werden, wie in Anhang C angegeben. Anhang D enthält zusätzliche Informationen zu Tabelle 11.

7 Unabhängigkeit durch Software-Partitionierung

7.1 Allgemeines

Die Software-Partitionierung ist dafür vorgesehen, den Planer durch den Nachweis der Unabhängigkeit von Software-Komponenten zu unterstützen. Eine ausreichende Unabhängigkeit von Software-Komponenten wird dadurch garantiert, dass bestimmte Softwarefehlerwirkungen, die diese Unabhängigkeit verletzen, ausgeschlossen werden.

Hierzu müssen Methoden und Maßnahmen mit angemessener Effektivität umgesetzt werden:

Documents
Document Sharing Hub

Full document details: E DIN EN ISO 19014-4:2024-04

— zur Beherrschung von Gefährdungen, die in Teilsystemen auftreten können, sodass sie andere Teilsysteme nicht negativ beeinflussen können;

— zur Gewährleistung ausreichender Unabhängigkeit von Software-Komponenten durch Software-Partitionierung.

Zum Erreichen einer ausreichenden Unabhängigkeit von Software-Komponenten sollten die Systemressourcen unabhängigen Partitionen, von denen jede eine bestimmte Laufzeitumgebung darstellt, zugewiesen werden. Der Einsatz der Software-Partitionierung ist nicht auf die Koexistenz von Software mit unterschiedlichem MPL in derselben Laufzeitumgebung beschränkt. Sie kann auch Folgendes unterstützen:

a) Änderungen einer Partition ohne Reverifizierung der unveränderten Software-Partitionen;

b) Koexistenz von Software einer anderen Art (innerbetrieblich, von Dritten).

Für Software-Partitionen mit einem MPLr = c, d, e ist Unabhängigkeit erforderlich.

ANMERKUNG Partitionen können in einem einzelnen Mikrocontroller oder mehreren Mikrocontrollern in einem Mikrocontroller-Netzwerk zugewiesen werden.

Je nach gewählter Architektur können zwei Ansätze verfolgt werden:

a) mehrere Partitionen in einem einzelnen Mikrocontroller;

b) mehrere Partitionen im Rahmen eines ECU-Netzwerks (elektronisches Steuerungssystem).

Das Konzept der Software-Partitionierung und zugehöriger Methoden und Maßnahmen für die Unabhängigkeit von Software-Komponenten muss bei der Spezifikation der Software-Architektur berücksichtigt werden.

Derjenige Teil der Software, der die Unterstützung zur Partitionierungsimplementierung umsetzt, muss denselben oder einen höheren MPLa als den mit den Software-Partitionen verbundenen höchsten MPLr aufweisen.

7.2 Mehrere Partitionen in einem einzelnen Mikrocontroller

Um eine angemessene Unabhängigkeit der Software-Komponenten innerhalb eines einzelnen Mikrocontrollers, wie in Bild 3 dargestellt, zu garantieren, muss die korrekte Ausführung der sicherheitsbezogenen Funktionen vor jeder der folgenden Fehlerwirkungen geschützt werden:

— Speicherverfälschung (unbeabsichtigtes Schreiben in den Speicher einer anderen Partition);

ANMERKUNG 1 Speicherverfälschung kann bei Memory Mapped Eingang/Ausgang (E/A), Speicherregistern usw. auftreten.

— Blockieren von Partitionen (aufgrund von Kommunikationsblockaden);

— falsche Zuweisung der Prozessorausführungszeit;

— falscher Kommunikationspartner (der Absender sendet Nachrichten an den falschen Empfänger oder missbraucht die Identifikation eines anderen Absenders);

— Verfälschung der E/A-Schnittstelle durch unbeabsichtigtes Schreiben an eine E/A-Schnittstelle einer anderen Partition.

ANMERKUNG 2 Verfälschung der E/A-Schnittstelle bezieht sich nur auf externe Geräte.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO 19014-4:2024-04

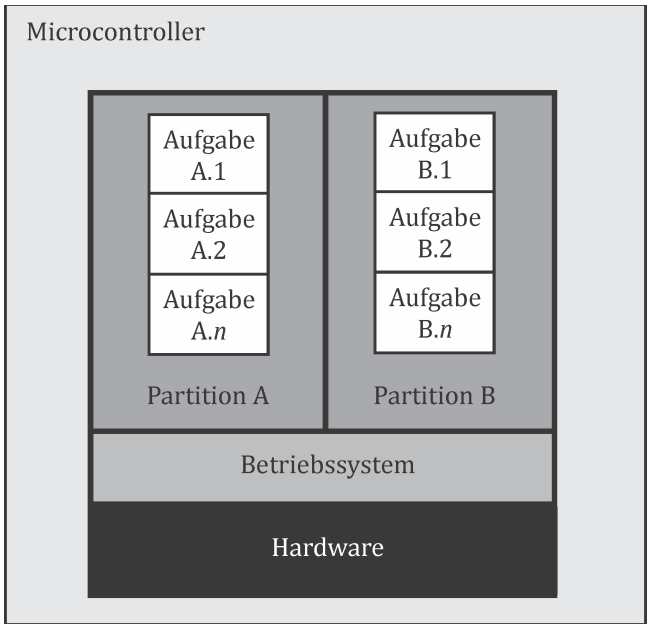

Bild 3 — Mehrere Partitionen in einem einzelnen Mikrocontroller

Tabelle 12 definiert die Maßnahmen so, dass alle oben angeführten entsprechenden Fehlerwirkungen behandelt werden können, um eine angemessene Wirksamkeit und eine angemessene Unabhängigkeit der Software-Komponenten sicherzustellen. Weitere Informationen sind Anhang E zu entnehmen.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO 19014-4:2024-04