

DIN EN ISO 19014-2



ICS 53.100

**Erdbaumaschinen –
Funktionale Sicherheit –
Teil 2: Entwurf und Bewertung von Hardware- und
Architekturanforderungen für sicherheitsrelevante Teile des
Steuerungssystems (ISO 19014-2:2022);
Deutsche Fassung EN ISO 19014-2:2022**

Earth-moving machinery –
Functional safety –
Part 2: Design and evaluation of hardware and architecture requirements for safety-related
parts of the control system (ISO 19014-2:2022);
German version EN ISO 19014-2:2022

Engins de terrassement –
Sécurité fonctionnelle –
Partie 2: Conception et évaluation des exigences de matériel et d'architecture pour les parties
relatives à la sécurité du système de commande (ISO 19014-2:2022);
Version allemande EN ISO 19014-2:2022

Gesamtumfang 59 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“ 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 13849-1:2015	siehe	DIN EN ISO 13849-1:2016-06
ISO 13849-2:2012	siehe	DIN EN ISO 13849-2:2013-02
ISO 19014-4:2020	siehe	DIN EN ISO 19014-4:2021-01
ISO 6165	siehe	DIN EN ISO 6165
ISO 13850	siehe	DIN EN ISO 13850
ISO 19014-1	siehe	DIN EN ISO 19014-1
ISO 19014-3	siehe	DIN EN ISO 19014-3
IEC 61508-2	siehe	DIN EN 61508-2

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 61508-2, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme — Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme*

DIN EN ISO 6165, *Erdbaumaschinen — Grundtypen — Identifizierung und Begriffe*

DIN EN ISO 13849-1:2016-06, *Sicherheit von Maschinen — Sicherheitsbezogene Teile von Steuerungen — Teil 1: Allgemeine Gestaltungsleitsätze (ISO 13849-1:2015); Deutsche Fassung EN ISO 13849-1:2015*

DIN EN ISO 13849-2:2013-02, *Sicherheit von Maschinen — Sicherheitsbezogene Teile von Steuerungen — Teil 2: Validierung (ISO 13849-2:2012); Deutsche Fassung EN ISO 13849-2:2012*

DIN EN ISO 13850, *Sicherheit von Maschinen — Not-Halt-Funktion — Gestaltungsleitsätze*

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

DIN EN ISO 19014-3, *Erdbaumaschinen — Funktionale Sicherheit — Teil 3: Umweltaforderungen und Prüfanforderungen von elektronischen und elektrischen Komponenten des sicherheitsrelevanten Steuerungssystems*

DIN EN ISO 19014-4:2021-01, *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*

— Leerseite —

Deutsche Fassung

**Erdbaumaschinen —
Funktionale Sicherheit —
Teil 2: Entwurf und Bewertung von Hardware- und
Architekturanforderungen für sicherheitsrelevante Teile des
Steuerungssystems (ISO 19014-2:2022)**

Earth-moving machinery —
Functional safety —
Part 2: Design and evaluation of hardware and
architecture requirements for safety-related parts of the
control system (ISO 19014-2:2022)

Engins de terrassement - Sécurité fonctionnelle - Partie
2: Conception et évaluation des exigences de matériel et
d'architecture pour les parties relatives à la sécurité du
système de commande (ISO 19014-2:2022)

Diese Europäische Norm wurde vom CEN am 25. Mai 2022 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	8
2 Normative Verweisungen	8
3 Begriffe	9
4 Symbole und Abkürzungen	10
5 Allgemeine Anforderungen	11
5.1 Anwendung	11
5.2 Bestehende SCS	11
6 Systementwurf	11
6.1 Überblick	11
6.2 Allgemeine Anforderungen	12
6.3 Gestaltung der Hardware	12
7 Bewertung der Sicherheitsleistung des Systems	13
7.1 Erreichtes Performance Level der Maschine (MPL _a)	13
7.2 Hardware-Sicherheitsbewertung	14
7.2.1 Allgemeines	14
7.2.2 Fehlerberücksichtigung	14
7.2.3 Fehlerausschluss	14
7.2.4 Mittlere Zeit bis zum gefahrbringenden Ausfall (MTTF _d)	15
7.3 Diagnosedeckungsgrad (DC)	15
7.3.1 DC des ESCS	15
7.3.2 DC des N/ESCS	15
7.4 Fehlerausschlüsse auf Systemlevel bei hydraulischen Systemen, basierend auf der Robustheit des hydraulischen Systems (HSR)	15
7.4.1 Allgemeines	15
7.4.2 Berechnung des HSR-Werts	16
7.5 Kategorie-Klassifikationen	17
7.5.1 Allgemeines	17
7.5.2 Kategorie B/Kategorie 1	21
7.5.3 Kategorie 2	23
7.5.4 Richtlinie zu in Konflikt stehenden Sicherheitsfunktionen	24
7.5.5 Überlegungen zu den SRP/CS von bei einem Ausfall betriebsfähigen Systemen	25
7.6 Kombination von SCS zur Erreichung eines Gesamt-MPL	25
8 Informationen für Gebrauch und Instandhaltung	27
8.1 Allgemeines	27
8.2 Benutzerhandbuch	27
Anhang A (informativ) Beispielsysteme und Bewertungen	28
A.1 Allgemeines	28
A.2 Beispiel 1 — Elektro-hydraulische Lenkung, Kategorie B	28
A.3 Beispiel 2 — Hydraulisch-hydraulische Lenkung, Kategorie 1	30
A.4 Beispiel 3 — Elektrisch-hydraulische Feststellbremse, Kategorie 1	32
A.5 Beispiel 4 — Elektro-hydraulische Lenkung mit automatischer Feststellbremse, Kategorie 2	33

A.6	Beispiel 5 — Hydraulisches Lenksystem, Kategorie 2M	39
A.7	Beispiel 6 — Elektro-hydraulische Betriebsbremse, Kategorie 3	41
Anhang B (informativ) Beispiele für Auswertungen mithilfe der HSR-Bewertung		44
B.1	Hydraulischer Lenkkreis eines Radladers.....	44
B.2	Beispiel für die Berechnung der HSR-Bewertung für eine federbetätigte hydraulische Feststellbremse	47
Anhang C (normativ) Kompatibilität mit anderen funktionalen Sicherheitsnormen		49
Anhang D (informativ) Bewertung der Sicherheitsfunktion.....		50
Anhang E (normativ) Ausnahmen, Ausschlüsse, Ergänzungen zu ISO 13849-1 und ISO 13849-2		52
Literaturhinweise.....		55

Europäisches Vorwort

Dieses Dokument (EN ISO 19014-2:2022) 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 Dezember 2022, und etwaige entgegenstehende nationale Normen müssen bis Dezember 2022 zurückgezogen werden.

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

Dieses Dokument wurde im Rahmen eines Normungsauftrages erarbeitet, den die Europäische Kommission und die Europäische Freihandelsassoziation CEN erteilt haben.

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.

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 19014-2:2022 wurde von CEN als EN ISO 19014-2:2022 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*, in Übereinstimmung mit der Vereinbarung zur technischen Zusammenarbeit zwischen ISO und CEN (Wiener Vereinbarung) erarbeitet.

Diese erste Ausgabe ersetzt zusammen mit ISO 19014-1, ISO 19014-3, ISO 19014-4 und ISO 19014-5 die ersten Ausgaben (ISO 15998:2008 und ISO/TS 15998-2:2012), die technisch überarbeitet wurden.

Die wesentlichen Änderungen sind folgende:

- Streichung der alternativen Verfahren ECE R79, Anhang 6, und IEC 62061;
- Anwendung von ISO 13849-1 auf mobile Erdbaumaschinen, einschließlich der Analyse von nichtelektronischen Steuerungen, die in Erdbaumaschinen zum Einsatz kommen.

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 beschäftigt sich mit Systemen sämtlicher Energietypen für die funktionale Sicherheit bei Erdbaumaschinen.

Sicherheitsnormen im Maschinenbau sind wie folgt aufgebaut:

- Typ-A-Normen (grundlegende Normen) liefern Grundkonzepte, Auslegungs- und Konstruktionsgrundsätze und allgemeine Aspekte, die auf Maschinen angewendet werden können.
- Typ-B-Normen (allgemeine Sicherheitsnormen) behandeln einen oder mehrere Sicherheitsaspekte oder eine oder mehrere Arten an Schutzeinrichtungen, die auf eine Vielzahl von Maschinen angewandt werden können:
 - Typ-B1-Normen behandeln bestimmte Sicherheitsaspekte (z. B. Sicherheitsabstände, Oberflächentemperatur, Geräusch);
 - Typ-B2-Normen behandeln Schutzeinrichtungen (z. B. Zweihandschaltungen, Verriegelungen, Kontaktmatten, trennende Schutzeinrichtungen).
- Typ-C-Normen (Maschinensicherheitsnormen) behandeln detaillierte Sicherheitsanforderungen für eine bestimmte Maschine oder Gruppe von Maschinen.

Dieses Dokument ist eine Typ-C-Norm, wie in ISO 12100 angegeben.

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

- Maschinenhersteller (kleine, mittlere und große Unternehmen);
- Organisationen des Arbeits- und Gesundheitsschutzes (Gesetzgeber, Unfallversicherungen, Marktaufsicht usw.).

Andere interessierte Kreise können durch das in diesem Dokument (durch die oben genannten interessierten Kreise) festgeschriebenen Sicherheitsniveau betroffen sein. Es handelt sich dabei um:

- Maschinenanwender/Arbeitgeber (kleine, mittlere und große Unternehmen);
- Maschinenanwender/Angestellte (z. B. Gewerkschaften, Organisationen für Personen mit besonderen Bedürfnissen);
- Dienstleister, z. B. für die Wartung (kleine, mittlere und große Unternehmen);
- Verbraucher (falls die behandelten Maschinen für die Nutzung durch Verbraucher bestimmt sind).

Den oben genannten interessierten Kreisen wurde die Möglichkeit eingeräumt, sich an der Erarbeitung dieses Dokuments zu beteiligen.

Auf die betreffenden Maschinen und die behandelten Gefährdungen, Gefährdungssituationen und Gefährdungsereignisse wird im Anwendungsbereich dieses Dokumentes hingewiesen.

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.

Dieses Dokument ist die Anpassung von ISO 13849, um eine Typ-C-Norm für die spezifische Anwendung der funktionalen Sicherheit bei Erdbaumaschinen zu schaffen.

In Bezug auf Erdbaumaschinen (EMM) muss dieses Dokument in Verbindung mit ISO 13849 verwendet werden, und es ersetzt ISO 15998.

Dieses Dokument ergänzt die Aktivitäten bezüglich des Sicherheitslebenszyklus von Sicherheitssteuerungen nach ISO 13849-1:2015 und ISO 13849-2:2012 für Erdbaumaschinen in Übereinstimmung mit der Definition in ISO 6165.

1 Anwendungsbereich

Dieses Dokument legt allgemeine Grundsätze für die Entwicklung und Beurteilung des erreichten Performance Level der Maschine (MPL_a) bei Sicherheitssteuerungen (SCS), unter Verwendung von Komponenten, die durch sämtliche, bei Erdbaumaschinen und deren Ausrüstung, wie in ISO 6165 festgelegt, Energiequellen (z. B. elektronisch, elektrisch, hydraulisch, mechanisch) angetrieben werden, fest.

Die Grundsätze dieses Dokuments sind anwendbar für Steuerungssysteme zur Steuerung von Maschinenbewegungen oder Verminderung von Gefährdungen. Solche Systeme werden nach ISO 19014-1 oder ISO/TS 19014-5 hinsichtlich der Anforderungen an das Performance Level (MPL_r) untersucht.

Folgende Systeme sind vom Anwendungsbereich dieses Dokuments ausgeschlossen:

- Wahrnehmungssysteme, die die Maschinenbewegung nicht beeinflussen (z. B. Kameras und Radardetektoren);
- Löschanlagen, sofern die Aktivierung des Systems kein anderes SCS beeinflusst oder aktiviert.

Weitere Systeme oder Komponenten, die den Bediener auf Ausfälle aufmerksam machen (z. B. Scheibenwischer oder Scheinwerfer usw.) oder die primär dem Schutz von Eigentum dienen, sind von diesem Dokument ausgeschlossen. Akustische Signale sind von den Anforderungen des Diagnosedeckungsgrads ausgeschlossen.

Zudem behandelt dieses Dokument die in ISO 12100 festgelegten signifikanten Gefährdungen, die durch die Hardwarekomponenten der SCS gemindert werden.

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

ISO 13849-1:2015, *Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design*

ISO 13849-2:2012, *Safety of machinery — Safety-related parts of control systems — Part 2: Validation*

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

ISO 19014-3, *Earth-moving machinery — Functional safety — Part 3: Environmental performance and test requirements of electronic and electrical components used in safety-related parts of the control system*

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/TS 19014-5, *Earth-moving machinery — Functional safety — Part 5: Table of Machine Performance Levels*

3 Begriffe

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

ESCS

elektronische Sicherheitssteuerung

aus elektronischen Komponenten bestehende Maschinensteuerung vom Eingabegerät zum Ausgabegerät

3.2

Funktion

definiertes Verhalten einer oder mehrerer Steuereinheiten

Anmerkung 1 zum Begriff: Eine Steuereinheit (elektronische Steuereinheiten) kann mehr als eine Funktion ausführen. Wenn eine Steuereinheit mehrere Sicherheitsfunktionen umfasst, wird jede Sicherheitsfunktion sowie der zugehörige Stromkreis separat analysiert.

3.3

N/ESCS

nicht elektronische Sicherheitssteuerung

aus nicht elektronischen Komponenten bestehende Maschinensteuerung vom Eingabegerät zum Ausgabegerät

3.4

sicherer Zustand

Zustand, in dem nach einem Fehler der Sicherheitssteuerung die gesteuerte Ausrüstung, der Prozess oder das System automatisch oder manuell angehalten oder in einen Modus geschaltet wird, der unbeabsichtigtes Verhalten oder die potenziell gefährliche Freigabe gespeicherter Energie verhindert

Anmerkung 1 zum Begriff: Zu einem sicheren Zustand kann auch, abhängig von der verminderten Gefährdung, die Aufrechterhaltung der *Funktion* (3.2) der Sicherheitssteuerung (z. B. Lenkung) beim Auftreten eines Einzelfehlers gehören.

[QUELLE: ISO 3450:2011, 3.15, modifiziert – „Fehlfunktion“ wurde durch „Fehler“, „Maschinensteuerungssystem“ durch „Sicherheitssteuerung“, „die gesteuerte Ausrüstung, der Betriebsprozess oder das Gesamtsystem“ wurde durch „die gesteuerte Ausrüstung, der Prozess oder das System“, „unexpected performance“ wurde durch „unintended behaviour“ ersetzt; Anmerkung 1 zum Begriff wurde hinzugefügt.]

3.5

bewährte Komponenten

Komponente für eine Sicherheitsanwendung, die in der Vergangenheit in großem Umfang und mit erfolgreichen Ergebnissen für ähnliche oder gleiche Anwendungen genutzt wurde und die unter Verwendung von Grundsätzen, die ihre Eignung und Zuverlässigkeit für Sicherheitsanwendungen belegt, hergestellt und geprüft wurde

4 Symbole und Abkürzungen

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

a, b, c, d, e	Graduierung der Performance Level der Maschine
ASIC	anwendungsspezifischer integrierter Stromkreis (en: application specific integrated circuit)
B, 1, 2, 3, 4	Kategoriebezeichnungen
CCF	Ausfall infolge gemeinsamer Ursache (en: common-cause failure)
DC	Diagnosedeckungsgrad (en: diagnostic coverage)
DC _{avg}	durchschnittlicher Diagnosedeckungsgrad (en: average diagnostic coverage)
ECU	elektronische Steuereinheit (en: electronic control unit)
EMM	Erdbaumaschine (en: earth moving machine)
ESCS	elektronische Sicherheitssteuerung (en: electronic safety control system)
FMEA	Fehlermöglichkeits- und Einflussanalyse (en: failure modes and effects analysis)
FMEDA	Fehlermöglichkeits-, Einfluss- und Diagnostikanalyse (en: failure mode, effects and diagnostics analysis)
FPGA	feldprogrammierbares Gatterfeld (en: field programmable gate array)
HFT	Hardware-Fehlertoleranz (en: hardware fault tolerance)
HSR	Robustheit des hydraulischen Systems (en: hydraulic system robustness)
MCS	Maschinensteuerungssystem (en: machine control system)
MPL	Performance Level der Maschine (en: machine performance level)
MPL _a	erreichtes Performance Level der Maschine (en: achieved machine performance level)
MPL _r	erforderliches Performance Level der Maschine (en: required machine performance level)
MTTF	mittlere Zeit bis zum Ausfall (en: mean time to failure)
MTTF _d	mittlere Zeit bis zum gefahrbringenden Ausfall (en: mean time to dangerous failure)
N/ESCS	nicht elektronische Sicherheitssteuerung (en: non-electronic safety control system)
OTE	Ausgang des Prüfgeräts (en: output of test equipment)
SCS	Sicherheitssteuerung (en: safety control system)
SRP/CS	sicherheitsbezogene Teile der Steuerung (en: safety related parts of control system)
TE	Prüfgerät (en: test equipment)

5 Allgemeine Anforderungen

5.1 Anwendung

In Bezug auf Erdbaumaschinen (EMM) muss die Reihe ISO 19014 in Verbindung mit der Reihe ISO 13849 verwendet werden und ersetzt ISO 15998. Wenn in diesem Dokument spezifische Anforderungen angegeben werden, haben diese Vorrang gegenüber den in der Normenreihe ISO 13849 enthaltenen Anforderungen; wenn jedoch in diesem Dokument keine spezifischen Anforderungen angegeben werden, gilt die Normenreihe ISO 13849, wobei PL anstelle von MPL verwendet wird (z. B. ist $MPL = b$ gleichwertig zu $PL = b$). Eine Zusammenfassung der anwendbaren Abschnitte der Normenreihe ISO 13849 oder dieses Dokuments ist in Tabelle E.1 und Tabelle E.2 in Anhang E enthalten.

Die Grundsätze dieses Dokuments müssen auf MCS angewendet werden, die in ISO 19014-1 oder ISO/TS 19014-5 als SCS eingestuft werden. Weiteren Maschinensteuerungssystemen, die eine Sicherheitsfunktion der Sicherheitssteuerung beeinflussen oder stummschalten, muss das gleiche Performance Level zugeordnet werden wie dem System, das sie beeinflussen oder abschalten.

Maschinen müssen den Sicherheitsanforderungen und/oder Schutz-/Risikominderungsmaßnahmen dieses Abschnittes entsprechen. Zusätzlich müssen die Maschinen den Grundsätzen von ISO 12100:2010 in Bezug auf die relevanten, aber nicht signifikanten Gefährdungen entsprechen, die in diesem Dokument nicht behandelt werden. Sicherheitsbezogene Software in allen Komponenten innerhalb der SCS muss die Anforderungen von ISO 19014-4:2020 erfüllen.

5.2 Bestehende SCS

Wenn eine bestehende SCS nach einer früheren Norm entwickelt und durch Anwendung, Verwendung und Validierung nachgewiesen wurde, dass sie die Wahrscheinlichkeit einer Gefährdung so gering wie praktisch möglich hält, gibt es keine Anforderung an die Aktualisierung der Lebenszyklus-Dokumentation. Wenn die zuvor verwendete SCS geändert wird, muss eine Bewertung der Auswirkungen (siehe ISO 19014-4:2020, 3.28) durchgeführt und ein Aktionsplan entwickelt und umgesetzt werden, um sicherzustellen, dass die Sicherheitsanforderungen eingehalten werden.

6 Systementwurf

6.1 Überblick

Viele Sicherheitsfunktionen an mobilen Maschinen haben keine Start-/Stopp-Ausgänge, wie sie stationäre Maschinen für gewöhnlich aufweisen, und werden einer Maschine nicht immer nur zur Gefährdungsverminderung hinzugefügt. Lenkung, Betriebsbremsen, Schwenk- und Ausrüstungssteuerungen können innerhalb eines bestimmten Bereichs über modulierte oder variable Ausgänge verfügen. Während diese Systeme den Architekturen nach ISO 13849 entsprechen können, müssen Konstrukteure berücksichtigen, inwiefern die Sicherheitskonzepte und Sicherheitsfunktionen an einer mobilen Maschine abweichen können (z. B. benötigt das System zur Adressierung inkorrekturer Anwendungsmengen einen geschlossenen statt eines offenen Regelkreises, muss das System Gefährdungen im Zusammenhang mit selbständiger Aktivierung sowie Ausfall nach Aufforderung adressieren usw.).

Eine Sicherheitsfunktion, die sich auf ein Steuerungssystem stützt, um die erforderliche Gefährdungsminimierung für die Maschine sicherzustellen, kann durch eine SCS im Rahmen dieses Dokuments umgesetzt werden. Eine SCS kann ein oder mehrere SRP/CS enthalten, und mehrere SCS können sich ein oder mehrere SRP/CS teilen (z. B. eine Logikeinheit, Leistungssteuerungselemente). Es ist auch möglich, dass mit einem SRP/CS sowohl Sicherheits- als auch Nicht-Sicherheitsfunktionen umgesetzt werden.

ANMERKUNG Für Warnanzeigen für Sofortmaßnahmen siehe ISO 19014-1:2018, Anhang B.

Manche Systeme an mobilen Maschinen müssen während eines Ausfalls einen betriebsfähigen Zustand aufrechterhalten. Obwohl ISO 13849-1:2015 dies prinzipiell erlaubt, müssen zusätzliche Maßnahmen ergriffen werden, um sicherzustellen, dass dies auf sichere Weise geschehen kann und parallele Kanäle zueinander nicht in Konflikt stehen und die Systeme nach den für die angegebene Architektur festgelegten Anforderungen funktionieren.

In Anhang C sind die Mindestanforderungen festgelegt, die für die Nutzung von Systemen, Subsystemen und SRP/CS erfüllt werden müssen, die nach anderen Verfahren als denen der Normenreihe ISO 19014 entwickelt und bewertet wurden.

6.2 Allgemeine Anforderungen

Nachdem die Sicherheitsfunktionen der SCS ermittelt wurden, müssen die Anforderungen an die Sicherheitsfunktionen dokumentiert werden. Während des Sicherheitslebenszyklus werden die Sicherheitsanforderungen in näheren Einzelheiten in hierarchischen Ebenen detailliert und spezifiziert. Alle Sicherheitsanforderungen müssen so geschrieben werden, dass sie eindeutig, mit anderen Anforderungen konsistent und umsetzbar sind.

Die folgenden Gestaltungserwägungen müssen berücksichtigt werden:

- im Konflikt stehende Eingangs- oder Ausgangssignale;
- Verlust des Signals oder der Auslöseenergien an einem der Systeme (z. B. separate Ölversorgungen für jeden Kanal, redundante Stromversorgungen für ECU);
- in Konflikt stehende sichere Zustände, die von mehreren, durch das System adressierten Fehlertypen benötigt werden;
- Systeme, die ein bei einem Ausfall ein betriebsfähiges Sicherheitskonzept benötigen;
- Beurteilungsprozesse sind unabhängig vom Konstruktionsprozess;
- wenn SCS für die synchronisierte Nutzung gestaltet sind (z. B. Aufgabenautomatisierung), muss das Steuerungssystem so ausgelegt sein, dass Gefährdungen aufgrund mangelnder Synchronisierung reduziert werden.

ANMERKUNG Ein EMM-Beispiel für diese Synchronisation sind Baggerausleger, -arm und -schaufel, die gleichzeitig von einem Steuerungssystem für die Neigung gesteuert werden.

6.3 Gestaltung der Hardware

Der Hardware-Aufbau des SCS kann Maßnahmen zur Vermeidung, Erkennung oder Tolerierung von Fehlern liefern. Zu den praktischen Maßnahmen können Redundanz, Diversität und Überwachung zählen.

Der Hardware-Entwicklungsprozess muss ISO 13849-1:2015 entsprechen, wie in Anhang E beschrieben. Der Konstrukteur sollte auf der Systemebene beginnen, wo die Sicherheitsfunktionen und die damit verbundenen Anforderungen identifiziert werden. Das System kann in Subsysteme zerlegt werden, um die Entwicklung zu vereinfachen.

Sofern anwendbar, muss jede Phase des Entwicklungszyklus validiert werden.

Siehe Bild 1 für eine Abbildung des Hardware-Entwicklungsprozesses in Form eines V-Modells. Jeder organisierte, bewährte Entwurfsprozess, der die Anforderungen in ISO 19014 erfüllt, darf für den Entwurfsprozess verwendet werden.

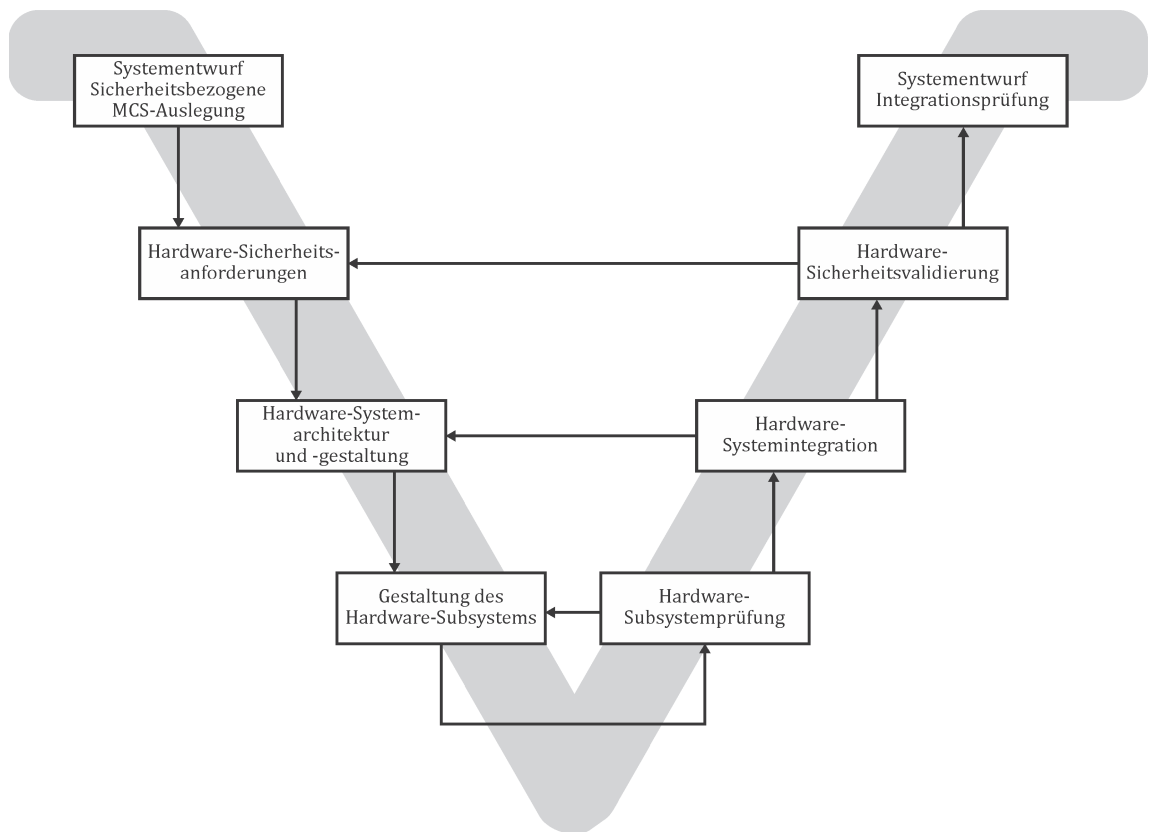


Bild 1 — V-Modell der Hardwareentwicklung

7 Bewertung der Sicherheitsleistung des Systems

7.1 Erreichtes Performance Level der Maschine (MPL_a)

Die erreichte Integrität von sicherheitsbezogenen Teilen zur Erfüllung einer Sicherheitsfunktion wird durch die Bestimmung des MPL_a angegeben.

Die Fähigkeit, eine Sicherheitsfunktion unter den erwarteten Umgebungsbedingungen, wie sie in ISO 19014-3 festgelegt sind, auszuführen, muss nachgewiesen und dokumentiert werden.

Das folgende Verfahren wird zur Bewertung des MPL_a verwendet:

- Identifizierung der Betriebsumgebung und der Beanspruchungshöhe von Bauteilen;
- Identifizierung der Bauteile;
- Identifizierung und Dokumentierung von Fehlerausschlüssen (7.2) oder durch Verwendung einer passenden Systemanalyse (z. B. FMEA, Fehlerbaumanalyse usw.);
- Berechnung der MTTF_d (siehe ISO 13849-1:2015, Anhang D) und Prüfung, ob die MTTF_d das erforderliche Level erreicht (siehe ISO 13849-1:2015);
- Prüfung, ob die Hardware das erforderliche Level an DC bieten kann (ISO 13849-1:2015, Anhang E). Bei Systemen, die zur Bestimmung des Diagnosedeckungsgrads auf Software-Interaktion angewiesen sind, kann diese Analyse nur bestimmen, ob die Hardware zur Unterstützung des DC verfügbar ist, jedoch nicht prüfen, ob die DC-Anforderung für das System erfüllt wurde;

- f) Betrachtung von CCF (siehe ISO 13849-1:2015, Anhang F), sofern erforderlich;
- g) Betrachtung von systematischen Ausfällen (ISO 13849-1:2015, Anhang G);
- h) Betrachtung möglicher Interaktionen von anderen Sicherheitsfunktionen;
- i) bei FPGA- und ASIC-Auslegung siehe IEC 61508-2:2010, Anhang E oder F.

Siehe Anhang D für zusätzliche Informationen zur Bewertung von Sicherheitsfunktionen.

7.2 Hardware-Sicherheitsbewertung

7.2.1 Allgemeines

ISO 13849-2:2012, Anhänge A bis D listen die wichtigen Fehler, Fehlerausschlüsse und Ausfälle für verschiedene Komponententypen auf, wobei diese Listen nicht erschöpfend sind. Sofern erforderlich, müssen zusätzliche Fehler, Fehlerausschlüsse und Ausfälle betrachtet und aufgelistet werden; in solchen Fällen sollte zudem die Bewertungsmethode spezifisch präzisiert werden.

Eine Fehlermöglichkeits- und Einflussanalyse (FMEA), eine Fehlerbaumanalyse oder eine gleichwertige Systemanalyse muss durchgeführt werden, um die Fehler und Fehlerausschlüsse zu ermitteln.

7.2.2 Fehlerberücksichtigung

Im Allgemeinen können folgende Fehlerkriterien berücksichtigt werden:

- wenn infolge eines Fehlers weitere Bauteile ausfallen, müssen der erste Fehler und alle Folgefehler als Einzelfehler betrachtet werden;
- zwei oder mehr Fehler mit gemeinsamer Ursache müssen als Einzelfehler (als CCF bekannt) betrachtet werden;
- das gleichzeitige Auftreten zweier oder mehrerer Fehler mit separaten Ursachen wird als sehr unwahrscheinlich eingestuft und muss daher nicht betrachtet werden.

7.2.3 Fehlerausschluss

Fehlerausschlüsse dienen bei der Hardware-Entwicklung in Übereinstimmung mit anerkannten Regeln der Technik als Methode zur Eindämmung von Fehlerzuständen, die zu bekannten Gefährdungen führen. Der Fehlerausschluss stellt einen Kompromiss zwischen technischen Sicherheitsanforderungen und der theoretischen Möglichkeit des Auftretens eines Fehlers dar.

Der Fehlerausschluss kann auf Folgendem basieren:

- der technischen Unwahrscheinlichkeit für das Auftreten mancher Fehler;
- allgemein anerkannter technischer Erfahrung, unabhängig von der betrachteten Anwendung; und
- technischen Anforderungen in Bezug auf die Anwendung und die spezifische Gefährdung.

Falls Fehler ausgeschlossen werden, muss der technischen Dokumentation eine umfangreiche Begründung hinzugefügt werden.

Fehlerausschlüsse können auf anhand der folgenden Hierarchie angewendet werden.