

DIN EN ISO 19014-1

ICS 53.100

Entwurf

Einsprüche bis 2017-08-31
Ersatz für
E DIN EN ISO 19014-1:2016-10

**Erdbaumaschinen –
Funktionale Sicherheit –
Teil 1: Methodik zur Bestimmung sicherheitsbezogener Teile einer
Steuerung und von Leistungsanforderungen (ISO/DIS 19014-1.2:2017);
Deutsche und Englische Fassung prEN ISO 19014-1:2017**

Earth-moving machinery –
Functional safety –
Part 1: Methodology to determine safety-related parts of the control system and performance requirements (ISO/DIS 19014-1.2:2017);
German and English version prEN ISO 19014-1:2017

Engins de terrassement –
Sécurité fonctionnel –
Partie 1: Méthodologie permettant de déterminer les parties du système de commande et les exigences de performance liés à la sécurité (ISO/DIS 19014-1.2:2017);
Version allemande et anglaise prEN ISO 19014-1:2017

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2017-06-30 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm 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@din.de 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, Lyoner Str. 18, 60528 Frankfurt am Main.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 61 Seiten

DIN-Normenausschuss Maschinenbau (NAM)

Nationales Vorwort

Dieser Norm-Entwurf enthält sicherheitstechnische Festlegungen.

Dieses Dokument (prEN ISO 19014-1:2017) wurde vom Technischen Komitee ISO/TC 127 „Earth-moving machinery - Safety“ in Zusammenarbeit mit dem Technischen Komitee CEN/TC 151 „Bau- und Baustoffmaschinen - Sicherheit“ erarbeitet, dessen Sekretariat von DIN (Deutschland) gehalten wird.

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

Die nationalen Interessen bei der Erarbeitung werden vom Arbeitsausschuss NA 060-13-01 AA „Erdbau-/ Straßenbaumaschinen“ im Fachbereich „Bau- und Baustoffmaschinen“ des DIN-Normenausschusses Maschinenbau (NAM) wahrgenommen. Vertreter der Hersteller und Anwender von Erdbau- und Straßenbaumaschinen sowie der Berufsgenossenschaften sind 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.

Die im Abschnitt 2 und den Literaturhinweisen zitierten Internationalen Normen sind, sofern diese gleichzeitig als Europäische Normen übernommen worden sind, als DIN EN ISO-Normen mit gleicher Zählnummer veröffentlicht.

Erdbaumaschinen — Funktionale Sicherheit — Teil 1: Methodik zur Bestimmung sicherheitsbezogener Teile einer Steuerung und von Leistungsanforderungen (ISO/DIS 19014-1.2:2017)

Engins de terrassement — Sécurité fonctionnel — Partie 1 : Méthodologie permettant de déterminer les parties du système de commande et les exigences de performance liés à la sécurité (ISO/DIS 19014-1.2:2017)

Earth-moving machinery — Functional safety — Part 1: Methodology to determine safety-related parts of the control system and performance requirements (ISO/DIS 19014-1.2:2017)

ICS:

Deskriptoren:

Dokument-Typ: Europäische Norm
Dokument-Untertyp:
Dokumentstufe: zweite parallele Umfrage
Dokumentsprache: D

STD Version 2.8l

Inhalt

	Seite
Europäisches Vorwort	4
Vorwort	5
Einleitung	6
1 Anwendungsbereich	7
2 Normative Verweisungen	7
3 Begriffe	8
4 Verfahren zur Bestimmung des MPL_T für das SRP/CS von Erdbaumaschinen	11
4.1 Allgemeines	11
4.2 Verfahren	12
5 Bestimmung der Grenzen der Maschine	12
5.1 Allgemeines	12
5.2 Identifizierung von Gefährdungen	13
6 Verfahren zur Bestimmung des Performance Levels	13
6.1 Allgemeines	13
6.1.1 Aufgaben im Rahmen der Risikoanalyse	13
6.1.2 Teilnehmer der Risikobeurteilung	13
6.1.3 Bewertung und Klassifizierung eines potenziellen Schadens	13
6.1.4 Bewertung der Aufenthaltsdauer in der beobachteten Situation	14
6.1.5 Bewertung einer Möglichkeit zur Vermeidung von Schäden	15
6.1.6 Auswahl des erforderlichen MPL	17
Anhang A (informativ) Flussdiagramm der Risikobeurteilung einer Maschine	19
Anhang B (normativ) Tabelle mit Warn-/Betriebsanzeigen	20
Anhang C (informativ) Liste der Gefährdungen aus ISO 12100 (EMM-spezifisch)	22
C.1 Bei der Konstruktion der Maschine zu berücksichtigende Gefährdungen	22
C.1.1 Allgemeines	22
C.2 Mechanische Gefährdungen	22
C.2.1 Mit der EMM in Verbindung stehende mechanische Gefährdungen	22
C.2.2 Durch die EMM erzeugte mechanische Gefährdungen	22
C.3 Elektrische Gefährdungen	23
C.4 Thermische Gefährdungen	23
C.5 Gefährdungen durch Lärm	23
C.6 Gefährdungen durch Vibration	24
C.7 Gefährdungen durch Werkstoffe und Substanzen	24
C.8 Gefährdungen durch Vernachlässigung ergonomischer Prinzipien bei der konstruktiven Ausführung der Maschine	24
C.9 Gefährdungen durch Rutschen, Stolpern und Stürzen	24
C.10 Kombinationen von Gefährdungen	24
C.11 Gefährdungen in Verbindung mit der Umgebung, in der die Maschine verwendet wird	24
Anhang D (informativ) Beispiele zur Berechnung der Variablen A, H und P für die Aufenthaltsdauer	25
D.1 Allgemeines	25
D.2 Beispiele der Variablen H und P	25

D.3	Beispielberechnung.....	27
Anhang E (informativ)	LISTE MÖGLICHER SICHERHEITSFUNKTIONEN VON ERDBAUMASCHINEN	28
Anhang ZA (informativ)	Zusammenhang zwischen dieser Europäischen Norm und den grundlegenden Anforderungen der abzudeckenden EU-Richtlinie 2006/42/EC	30
Literaturhinweise.....		31

Europäisches Vorwort

Dieses Dokument (prEN ISO 19014-1:2017) wurde vom Technischen Komitee ISO/TC 127 „Earth-moving machinery - Safety“ 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 zweiten parallelen Umfrage vorgelegt.

Anerkennungsnotiz

Der Text von ISO/DIS 19014-1.2:2017 wurde von CEN als prEN ISO 19014-1:2017 ohne irgendeine Abänderung genehmigt.

Vorwort

ISO (die Internationale Organisation für Normung) ist eine weltweite Vereinigung von Nationalen Normungsorganisationen (ISO-Mitgliedsorganisationen). Die Erstellung von Internationalen Normen wird normalerweise von ISO Technischen Komitees 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 Organisationen, staatlich und nicht-staatlich, in Liaison mit ISO, nehmen ebenfalls an der Arbeit teil. ISO arbeitet eng mit der Internationalen Elektrotechnischen Kommission (IEC) bei allen elektrotechnischen Themen 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. Im Besonderen sollten die für die verschiedenen ISO-Dokumentenarten notwendigen Annahmekriterien 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 empfangenen Patenterklärungen (siehe www.iso.org/patents).

Jeder in diesem Dokument verwendete Handelsname wird als Information zum Nutzen der Anwender angegeben und stellt keine Anerkennung dar.

Eine Erläuterung der Bedeutung ISO-spezifischer Benennungen und Ausdrücke, die sich auf Konformitätsbewertung beziehen, sowie Informationen über die Beachtung der Grundsätze der Welthandelsorganisation (WTO) zu technischen Handelshemmnissen (TBT, en: Technical Barriers to Trade) durch ISO enthält der folgende Link: www.iso.org/iso/foreword.html.

Das für dieses Dokument verantwortliche Komitee ist ISO/127.

ISO 19014 besteht unter dem allgemeinen Titel *Earth-moving machinery — Functional Safety* aus folgenden Teilen:

- *Part 1: Risk assessment methodology to determine control system performance requirements*
- *Part 2: Design and Evaluation of Safety-Related Machine Control Systems*
- *Part 3: Environmental Testing Requirements*
- *Part 4: Design and evaluation of software and data transmission for safety-related parts of the control system*
- *Part 5: Technical report: Guidance and table of MPLr for EMM*

Die ISO 19014-Reihe ersetzt ISO 15998.

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 sowie 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-B 1 Normen behandeln bestimmte Sicherheitsaspekte (z. B. Sicherheitsabstände, Oberflächentemperaturen, Lärm);
- Typ-B 2 Normen behandeln Schutzeinrichtungen (z. B. Zweihandbedienungen, Verriegelungseinrichtungen, druckempfindliche Geräte, trennende Schutzeinrichtungen).

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

Dieser Teil der ISO 19014 ist eine Typ-C Norm, wie in ISO 12100 angegeben.

1 Anwendungsbereich

Dieser Teil der ISO 19014 stellt Leitfäden und eine Methodik zur Bestimmung der für Erdbaumaschinen (en: earth moving machinery, EMM) erforderlichen Performance Level, wie in ISO 6165 beschrieben, bereit, nachdem eine Gefährdung anhand einer Risikobeurteilung identifiziert wurde.

ANMERKUNG Diese Reihe kann auch für funktionale Sicherheitsanforderungen anderer mobiler Geländemaschinen verwendet werden.

Die Gefährdungsidentifizierung wird anhand einer Risikobeurteilung (auch bekannt als Sicherheitsanalyse der Maschinensteuerung, MCSSA) mithilfe des in ISO 12100 beschriebenen Verfahrens oder anderer Mittel bestimmt und wird nicht von diesem Dokument abgedeckt.

Wenn ein Untersystem als Sicherheitssteuerung (en: safety control system, SCS) festgelegt wird, wird diesem Untersystem ein Performance Level der Maschine (MPL) zugewiesen.

ANMERKUNG Der Begriff MPL wird verwendet, um das von einem sicherheitsbezogenen Teil einer Steuerung erforderliche Performance Level zu beschreiben. „M“ steht für Maschine und bezeichnet Erdbaumaschinen, die vom Anwendungsbereich dieses Dokuments abgedeckt werden und wird zur Abgrenzung zu anderen Normen über funktionale Sicherheit (z. B. PL, AgPL, ASIL usw.) verwendet.

Für diese als sicherheitsbezogen festgelegten Stellteile werden die Merkmale für die Architektur, die Hardware, die Umgebungsanforderungen für die Software und die Leistung von anderen Teilen dieser Reihe abgedeckt.

ISO 19014 deckt die Gefährdungen ab, die durch das funktionale Verhalten sicherheitsbezogener Systeme verursacht werden, mit Ausnahme von Gefährdungen, die aufgrund der Ausrüstung selbst entstehen (z. B. elektrische Schläge, Brände usw.).

Die Grundsätze der vorliegenden Norm müssen ebenfalls auf Warnanzeigen für Sofortmaßnahmen angewandt werden, die den Bediener vor einer möglichen Gefährdung warnen und eine unmittelbare Handlung vom Bediener erfordern, um eine solche Gefährdung zu korrigieren und ihr vorzubeugen (z. B. Bilderkennungssysteme, Abstandswarnsysteme usw.).

ANMERKUNG Eine normative Liste mit Warnanzeigen für Sofortmaßnahmen ist in Anhang B enthalten.

Andere Stellteile, die keine Sicherheitssteuerungen (SCS) darstellen, eine Gefährdung nicht mindern oder keine Steuerfunktion ausüben und die den Bediener auf Ausfälle aufmerksam machen, sind von dieser Norm ausgeschlossen (z. B. Scheibenwischer, Scheinwerfer usw.).

ANMERKUNG 1 Eine informative Liste mit Sicherheitsfunktionen ist in Anhang E enthalten.

ANMERKUNG 2 Akustische Signale sind von den Anforderungen des Diagnosedeckungsgrads ausgeschlossen.

Die vorliegende Norm ersetzt ISO 15998:2008.

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

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

ISO 19014-2, *Earth-moving machinery — Safety — Control system performance level architecture and requirements*

ISO 19014-3, *Earth-moving machinery — Safety — Control system performance level environmental requirements*

ISO 19014-4, *Earth-moving machinery — Safety — Design and evaluation of software and data transmission for safety-related parts of the control system*

ISO 20474-1, *Earth-moving machinery — Safety — Part 1: General requirements*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach ISO 12100 und die folgenden Begriffe.

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

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

3.1

Performance Level der Maschine

MPL

diskretes Niveau zur Spezifizierung der Fähigkeit sicherheitsbezogener Teile von Steuerungen, unter vernünftigerweise vorhersehbaren Bedingungen eine Sicherheitsfunktion durchzuführen

3.1.1

erforderliches Performance Level der Maschine

MPL_r

erforderliches diskretes Niveau, wie durch Verfahren in diesem Dokument festgelegt

3.1.2

erreichtes Performance Level der Maschine

MPL_a

erreichtes diskretes Niveau, wie durch Verfahren in ISO 19014-2 und ISO 19014-4 festgelegt

3.2

funktionale Sicherheit

Teil der mit der zu steuernden Ausrüstung und ihrem Stellteil in Bezug stehenden Gesamtsicherheit, der von der korrekten Betriebsweise des sicherheitsbezogenen Systems und anderen risikomindernden Maßnahmen abhängt

[QUELLE: IEC 61508-4:2010, 3.1.12]

3.3

Maschinensteuerung

MCS

System, das auf Eingangssignale von Teilen der Maschine, Bedienern, externer Steuerungseinrichtungen oder einer Kombination dieser reagiert und Ausgangssignale erzeugt, damit sich die Maschine in der vorgesehenen Art und Weise verhält

[QUELLE: ISO 13849-1:2015, 3.1.32]

Anmerkung 1 zum Begriff: Der Umfang des Systems ist nicht auf die elektronische Steuerung beschränkt, sondern wird durch die maschinenbezogene Funktion des kompletten Systems definiert. Es besteht deshalb allgemein aus elektronischen, nicht elektronischen und Verbindungsgeräten. Diese können mechanische, hydraulische, optische oder pneumatische Bauteile/Systeme umfassen.

3.3.1

Sicherheitssteuerung

SCS

ein Untersystem oder Bauteil, das von einer MCS verwendet wird, um funktionale Sicherheit durch Beeinflussung des Maschinenverhaltens oder Mindern der Gefährdung zu erreichen

Anmerkung 1 zum Begriff: Ein System, durch dessen Ausfall eine Gefährdung entstehen kann, gilt als SCS.

Anmerkung 2 zum Begriff: z. B. darf eine SCS für den Antrieb Drossel, Gangschaltung, Start/Stopp usw. umfassen.

3.3.2

sicherheitsbezogener Teil der Steuerung

SRP/CS

Teil einer SCS, das auf sicherheitsbezogene Eingangssignale reagiert und sicherheitsbezogene Ausgangssignale erzeugt

[QUELLE: ISO 13849-1:2015, 3.1.1]

Anmerkung 1 zum Begriff: Die kombinierten sicherheitsbezogenen Teile einer Steuerung beginnen an dem Punkt, an dem die sicherheitsbezogenen Eingangssignale initiiert werden (beispielsweise einschließlich der Antriebsnocke und der Rolle des Positionsschalters) und enden am Ausgang der Leistungssteuerungselemente (beispielsweise einschließlich der Hauptkontakte eines Aufnehmers).

Anmerkung 2 zum Begriff: Wenn Überwachungssysteme für die Diagnose verwendet werden, werden sie ebenfalls als SRP/CS angesehen.

Anmerkung 3 zum Begriff: SRP/CS ist ein Teil oder eine Komponente innerhalb des jeweiligen MCS.

3.4

Bediener

Person, die die EMM bedient

3.5

Mitarbeiter

Person, die in der Nähe der Maschine arbeitet

3.6

umstehende Person

Person, einschließlich Nicht-Mitarbeiter, Kinder oder Mitglieder der Öffentlichkeit, mit wenig oder keiner Kenntnis der Maschinengefährdungen und keinerlei Übung

3.7

Instandhalter

Person, deren Funktion es ist, Wartungsarbeiten an der Maschine durchzuführen

Anmerkung 1 zum Begriff: Ein Instandhalter ist geschult und mit der Maschine vertraut.

3.8

Beherrschbarkeit

Fähigkeit, Schaden an der Personengruppe, die einem Risiko ausgesetzt ist, durch zeitnahes Reagieren des Bedieners, möglicherweise mithilfe alternativer Steuerungen, zu vermeiden

3.9

Aufenthaltsdauer

Prozentsatz der Zeit, dem eine Personengruppe der Gefährdung ausgesetzt ist

3.10

Schwere

geschätztes Ausmaß des Schadens für eine oder mehrere Einzelpersonen, das in einer potenziellen Gefährdungssituation eintreten kann

[QUELLE: ISO 26262-1:2011, 3.120]

3.11

Warnanzeige

visuelle, sensorische oder akustische Anzeigen, für die eine Handlung vom Bediener oder der Steuerung erforderlich ist

3.11.1

Warnanzeige für Sofortmaßnahmen

Warnanzeige, die eine umgehende Handlung vom Bediener erfordert, um Gefährdungen oder Systemausfälle zu mindern

3.12

Anzeige

Mittel, durch das einem Beobachter der Zustand der Ausrüstung oder Maschine dargestellt wird

[QUELLE: ISO 22555:2007, 3.2]

3.13

Anwendung

unterschiedliche Branchen, in denen eine Maschine eingesetzt wird, die jeweils unterschiedliche Gefährdungen aufweisen können

Anmerkung 1 zum Begriff: Anwendungen können Allgemeinbau, Straßenbau, Abfallmanagement, Steinbruch usw. umfassen

3.14

Nutzungsfall

Nutzungen einer Maschine innerhalb einer Anwendung

Anmerkung 1 zum Begriff: Eine Planiermaschine kann beispielsweise innerhalb einer Anwendung die Nutzungsfälle Planieren, Aufreißen, Fahren und Instandhalten aufweisen.

3.15

Nutzungsfall einer Anwendung

höchster Prozentsatz der Zeit, den eine Maschine in einem Nutzungsfall innerhalb einer gegebenen Anwendung während des bestimmungsgemäßen Gebrauchs im Lebenszyklus der Maschine zum Einsatz kommt

Anmerkung 1 zum Begriff: Da der Nutzungsfall der Anwendung den höchsten Prozentsatz der Zeit darstellt, den eine Maschine in einem Nutzungsfall verbringt, kann die Summe der Nutzungsfälle der Anwendung über die gesamte Anwendung hinweg mehr als 100 % betragen.

3.16

Gefährdungszeit

Prozentsatz der Zeit innerhalb des Arbeitszyklus, bei dem es vernünftigerweise vorhersehbar ist, dass eine Gefährdung bestehen könnte, wenn die zu bewertende Steuerung ausfallen sollte

Anmerkung 1 zum Begriff: Beispielsweise ist eine Planiermaschine, die Material von einer hohen Mauer wegschiebt, nur innerhalb des Anhaltewegs der Maschine und in der Zeit, in der die Maschine auf die hohe Mauer zufährt, der Gefährdung ausgesetzt, sich über die hohe Mauer hinweg zu bewegen.

3.16.1

Gefährdungsbereich

jeder Bereich innerhalb oder um die Maschine, in dem eine Person einer Gefährdung durch die zu analysierende SCS ausgesetzt sein kann

[QUELLE: ISO 12100:2010, 3.11 (MOD)]

3.17

Sicherheitsanalyse der Maschinensteuerung

MCSSA

Risikobeurteilung, die zur Bestimmung der erforderlichen MPL_T für die SCS auf einer Maschine verwendet wird, wie in diesem Dokument beschrieben

3.18

Personengruppe

Gruppe von Menschen, die in der MCSSA analysiert werden

Anmerkung 1 zum Begriff: Die vier Personengruppen sind Bediener, Instandhalter, umstehende Personen und Mitarbeiter.

3.19

Aufenthaltsdauer der Personengruppe

höchster Prozentsatz der Zeit, den sich jemand aus der Personengruppe, die bewertet wird, innerhalb des Gefährdungsbereichs aufhält

Anmerkung 1 zum Begriff: Die Analyse stellt die Summe aller sich im Gefährdungsbereich aufhaltenden Personen und nicht eine Einzelperson innerhalb der Gruppe dar, d. h. kein einzelnes vorbeifahrendes Auto, sondern der Verkehrsfluss.

3.20

Ausfallart

Beschreibung der Art des Ausfalls, der in einer SCS auftreten kann

Anmerkung 1 zum Begriff: Zu berücksichtigende Ausfallarten beinhalten Nichtanwenden, Nichtlösen, ungewolltes Anwenden, ungewolltes Lösen, inkorrekte Anwendungsgeschwindigkeit, inkorrekte Lösegeschwindigkeit oder inkorrekte Richtung usw.

4 Verfahren zur Bestimmung des MPL_T für das SRP/CS von Erdbaumaschinen

4.1 Allgemeines

Funktionale Sicherheit wird durch eine oder mehrere SCS erreicht, die auf vielen Technologien basieren (z. B. mechanisch, hydraulisch, pneumatisch, elektrisch, elektronisch, programmierbar elektronisch). Eine Sicherheitsstrategie muss sämtliche Elemente innerhalb einer SCS wie Sensoren, Steuergeräte und Stellantriebe berücksichtigen.

Teile der SCS, die Sicherheitsfunktionen bieten, werden sicherheitsbezogene Teile von Steuerungen (SRP/CS) genannt. Diese können aus Hardware oder Software bestehen und separate oder integrierte Teile einer Steuerung sein, die im MCSSA-Verfahren enthalten sein muss.

Der Konstrukteur (und in gewissem Maße der Anwender) muss die Konstruktion und Validierung dieser SRP/CS als Teil der Risikobeurteilung kombinieren. Ziel ist es, die mit einer gegebenen Gefährdung (oder Gefährdungssituation) verbundenen Risiken während des bestimmungsgemäßen Gebrauchs oder einer vernünftigerweise vorhersehbaren Fehlanwendung der Maschine zu reduzieren. Dies muss erreicht werden, indem verschiedene Schutzmaßnahmen (sowohl SRP/CS als auch Nicht-SRP/CS) angewendet werden, sodass als Endergebnis eine sichere Bedingung erreicht wird.

Um den Konstrukteur durch die Konstruktion zu führen und die Bewertung des erreichten Performance Levels zu vereinfachen, definiert ISO 19014 einen Ansatz, der auf einer Klassifizierung von Strukturen mit verschiedenen Konstruktionsmerkmalen und spezifischem Verhalten im Falle eines Ausfalls basiert. Die Performance Levels und Kategorien können auf die SCS aller Arten mobiler Maschinen angewendet werden: von einfachen Systemen (z. B. Hilfsventilen) über komplexe Systeme (z. B. Steer-by-Wire) bis hin zu Steuerungen von Schutzausrüstungen (z. B. Verriegelungsvorrichtungen, druckempfindliche Geräte).

ISO 19014 übernimmt einen risikobasierten Ansatz für die Bestimmung der Risiken und bietet gleichzeitig ein Mittel zur Spezifizierung des Ziel-Performance Levels für die mithilfe von sicherheitsbezogenen Kanälen zu implementierenden Sicherheitsfunktionen. Sie beinhaltet Anforderungen für den gesamten Sicherheitslebenszyklus der SRP/CS (Konstruktion, Validierung, Produktion, Betrieb, Wartung, Außerbetriebsetzung), die zum Erreichen der erforderlichen Funktionssicherheit für SRP/CS in Verbindung mit den Performance Levels notwendig sind.

4.2 Verfahren

Die folgenden wichtigen Stufen gelten für die Bestimmung von MPL_r für sicherheitsbezogene Teile von Steuerungen (SRP/CS):

- a) Bestimmung der vorhergesehenen EMM-Einschränkungen in Übereinstimmung mit EN ISO 12100:2010. (Abschnitt 5)
- b) Durchführung einer MCSSA mithilfe eines geeigneten Werkzeugs und Identifizierung der mit der Funktion oder Anwendung der Maschine verbundenen Gefährdungen.
- c) Festlegung, wie die im MCSSA-Verfahren identifizierten Gefährdungen abgeschwächt werden können oder sich vor diesen geschützt werden kann. (Dies kann zusätzliche MCS oder Mittel zur Sicherstellung der Integrität inhärenter Steuerungen erfordern.)
- d) Bestimmung, ob die genutzte Gefährdungsminderung/Schutzmaßnahme von einer SCS abhängt und ob dies ein SRP/CS ist. (Dies muss MCS umfassen, die zur Maschine hinzugefügt wurden, um eine Gefährdung zu mindern, sowie Steuerungen, die die Bewegung der Maschine regeln oder Steuerungen, die verwendet werden, wenn Ausfälle zu einer Gefährdungssituation führen.)
- e) Wenn eine MCS nicht als eine SCS bestimmt wird, ist das MCSSA-Verfahren nicht erforderlich. Die MCS, die nicht den Anforderungen von ISO 19014-1 MPL unterliegen, werden durch die Anforderungen für Qualitätsmanagementsysteme (QM) (Abschnitt 6.1.7) abgedeckt, und die Integrität muss durch Anwendung der Qualitätsmanagementwerkzeuge und technischen QM-Normen wie in ISO 19014-2 definiert sichergestellt werden und andere Teile der ISO 19014-Reihe finden keine Anwendung.
- f) Wenn die Schutzmaßnahme von einer SCS abhängt, die MCSSA verwenden, um die MPL auszuwählen, die für die SCS erforderlich ist. (Abschnitt 6)
- g) Damit ein System ein bestimmtes MPL erreicht, muss auf die anderen Teile in dieser Reihe Bezug genommen werden.

5 Bestimmung der Grenzen der Maschine

5.1 Allgemeines

Die Grenzen des Maschinensystems müssen für alle Phasen des Lebenszyklus des Maschinensystems dokumentiert werden, einschließlich der Merkmale und der erwarteten Leistungen der Maschine.

Grenzen müssen die zugehörigen Personen, Umgebungen und Produkte umfassen, die jeweils hinsichtlich der Grenzen des Maschinensystems identifiziert werden müssen.

Die Bestimmung der Grenzen der Maschine muss nach ISO 12100 erfolgen.

5.2 Identifizierung von Gefährdungen

Sobald die Grenzen bestimmt wurden, müssen sämtliche Gefährdungen in Verbindung mit der verwendeten EMM überprüft werden.

Es sollte ebenfalls eine Überprüfung der Warnanzeigen für Sofortmaßnahmen durchgeführt werden, um sicherzustellen, dass der Konstrukteur die vom Bediener geforderten Reaktionen versteht, um eine Gefährdung abzuschwächen, wenn eine Warnung gegeben wurde. Anhang B bietet eine normative Liste an Anzeigen, wenngleich diese nicht vollständig ist.

Anhang C bietet eine informative Liste von Gefährdungen, wenngleich diese nicht vollständig ist und jede Gefährdung bewertet werden muss, um die Nutzungsbedingungen wie im Flussdiagramm in Anhang A zu berücksichtigen.

6 Verfahren zur Bestimmung des Performance Levels

6.1 Allgemeines

Mithilfe des Flussdiagramms in Anhang A muss dieser Abschnitt (6) angewendet werden, wenn Schritt 2 gilt und ein sicherheitsbezogener Teil einer Steuerung erforderlich ist (d. h. Schutzeinrichtung).

Die Architektur (z. B. redundante Kanäle) dieser zu überprüfenden SCS darf nicht als Teil der MCSSA angesehen werden.

Entscheidungen, die später im Lebenszyklus getroffen werden und den Grundsatz ändern, auf dem frühere Entscheidungen beruhen, müssen eine neue MCSSA und Beurteilung des Systems in Übereinstimmung mit allen Teilen der ISO 19014-Reihe initiieren.

6.1.1 Aufgaben im Rahmen der Risikoanalyse

Die Betriebsbedingungen, bei denen die EMM bei korrekter Verwendung Gefährdungen initiieren kann, müssen berücksichtigt werden.

Bei in verschiedenen Szenarien verwendeten SCS, bei denen die Schwere, Beherrschbarkeit oder Aufenthaltsdauer variieren kann, muss jedes Szenario berücksichtigt werden. Das höchste durch die MCSSA bestimmte Performance Level muss für diese SCS verwendet werden.

6.1.2 Teilnehmer der Risikobeurteilung

An der MCSSA sollte ein funktionsübergreifendes Team aus beispielsweise folgenden Bereichen beteiligt sein: elektronische oder elektrische Entwicklung, Prüfung oder Validierung, Maschinen- oder Hydraulikdesign, Bediener, Wartung, Vertrieb und Marketing.

6.1.3 Bewertung und Klassifizierung eines potenziellen Schadens

Schädliche Auswirkungen können ermittelt werden, indem sowohl die Geschichte vergangener Vorfälle als auch das potenzielle Ergebnis von Fehlfunktionen der analysierten SCS verwendet werden. Die potenzielle Schwere der Schäden oder Verletzung muss für jedes relevante Szenario in der MCSSA so präzise wie möglich beschrieben werden.

ANMERKUNG Die Einschätzung der Schwere hat ihren Schwerpunkt normalerweise auf dem schlimmsten und schwersten Schaden, der realistischereweise auftreten kann (schlimmster glaubwürdiger Fall), und nicht auf der schlimmsten erdenklichen Konsequenz. Es ist jedoch nicht immer einfach zu bestimmen, welche Schadensschwere angenommen werden soll. Der schwerste Fall kann sehr unwahrscheinlich sein und der wahrscheinlichste Fall kann belanglos sein, sodass die Verwendung eines der beiden Fälle zu einer unangemessenen Einschätzung des Risikos führen könnte.

Wenn eine MCSSA durchgeführt wird, muss das Risiko der schlimmsten glaubwürdigen Schwere des Schadens verwendet werden. Andere Schwere, die häufiger auftreten, müssen ebenfalls in der Bewertung überprüft werden, um zu prüfen, ob ein höheres Performance Level erzeugt wird.

In der Beschreibung der Schäden muss eine bestimmte Kategorisierung verwendet werden. Aus diesem Grund wird die Klassifizierung der Schwere des Schadens in vier Kategorien dargestellt: S0, S1, S2 und S3 (siehe Tabelle 1).

Der Bediener der betreffenden Maschine und andere Parteien (z. B. Personen, die Unterstützung anbieten, andere Bediener des Maschinensystems, umstehende Personen, Mitarbeiter usw.) müssen in der detaillierten Beschreibung des Schadens aufgenommen werden.

Eine Untersuchung des Risikos für Sicherheitsfunktionen legt ihren Schwerpunkt auf die Ursache der Verletzungen von Personen. Wenn in der Analyse des potenziellen Schadens festgestellt werden kann, dass es sich ausschließlich um Sachschaden handelt und keine Verletzungen von Personen vorliegen, wäre es nicht erforderlich, eine Regelungseinrichtung des Systems als Sicherheitsfunktion zu klassifizieren. Dies wird durch die Einführung einer S0-Schadensklassifizierung und das QM ermöglicht.

Tabelle 1 — Beispiele für Beschreibungen von Verletzungen

S0	S1	S2	S3
Keine signifikanten Verletzungen, braucht nur erste Hilfe	Verletzungen, braucht medizinische Hilfe, vollständige Genesung, reversible Verletzung ohne Verlust der Arbeitskapazität nach der Genesung	Schwere Verletzung, permanenter Verlust der Arbeitskapazität.	Todesfall

6.1.4 Bewertung der Aufenthaltsdauer in der beobachteten Situation

Folgendes spiegelt die Auswirkungen möglicher Ausfälle unter spezifischen Arbeits- und Betriebsbedingungen wider.

Diese Situationen können von täglichen Routineaktivitäten bis hin zu extremen, seltenen Situationen reichen.

Die Variable E für Aufenthaltsdauer muss verwendet werden, um die verschiedenen Häufigkeiten bzw. die jeweilige Aufenthaltsdauer zu kategorisieren. Sie wird mit der folgenden Formel berechnet:

$$\begin{bmatrix} A_1 \\ A_2 \\ \vdots \\ A_n \end{bmatrix} \times \begin{bmatrix} H_1 \\ H_2 \\ \vdots \\ H_n \end{bmatrix} \times \begin{bmatrix} P_1 \\ P_2 \\ \vdots \\ P_n \end{bmatrix} = \begin{bmatrix} E_1 \\ E_2 \\ \vdots \\ E_n \end{bmatrix}$$

Dabei ist

- A der Nutzungsfall einer Anwendung definiert als Prozentsatz der Zeit für die Aktivität der zu analysierenden Maschine
- H die Gefährdungszeit für jede Ausfallart, jedes SCS-Untersystem und jede Personengruppen-Kombination
- P die Personengruppen-Aufenthaltsdauer für jede Ausfallart, jedes SCS-Untersystem und jede Personengruppen-Kombination

Ein Beispiel zur Bestimmung der Variablen A, H und P ist in Anhang D enthalten.

Maschinen müssen so entworfen werden, dass Risiken eines jeden bestimmungsgemäßen Gebrauchs gemindert werden, selbst wenn der ungünstigste Fall des bestimmungsgemäßen Gebrauchs einen kleinen Prozentsatz der gesamten Feldpopulation ausmacht. Wenn Maschinen nur für durchschnittliche Werte der Nutzungsfälle der Anwendung, Gefährdung und Aufenthaltsdauer konstruiert sind, würden sie nicht alle Sicherheitsrisiken, die mit ihrem bestimmungsgemäßen Gebrauch in Bezug stehen, mindern.

Anwendungen, die andere Gefährdungen als Grundmaschinen aufweisen und mit anderen Steuerungen speziell für die Anwendung ausgestattet werden, können als Spezialanwendungen behandelt und aus der Analyse ausgeschlossen werden sowie in einer separaten MCSSA Berücksichtigung finden.

Der falsche Gebrauch einer Maschine kann aus der MCSSA ausgeschlossen werden, solange dies in der MCSSA und O&MM als nicht akzeptabler Gebrauch dokumentiert ist und es realistisch ist, dass die Maschine nicht auf diese Art verwendet wird, damit die Maschine eine Aufgabe beendet, die die Maschine normalerweise beenden darf.

Drei Kategorien, die als E0, E1 und E2 bezeichnet werden, werden dort verwendet, (siehe Tabelle 2), wo E als Schätzung gilt, wie oft und wie lang ein Bediener oder eine umstehende Person einer Gefährdung ausgesetzt ist, die zu einer Verletzung der sich dort aufhaltenden Personengruppe führen könnte. Wenn eine MCSSA durchgeführt wird, muss das Risiko der längsten Aufenthaltsdauer angewendet werden. Niedrigere Aufenthaltsdauern, die eine größere Schwere besitzen, müssen ebenfalls in der Bewertung überprüft werden, um zu prüfen, ob ein höheres Performance Level erzeugt wird.

Aufenthaltsdauern für Wartungspersonal sollten die Zeit für die Wartung der Maschine widerspiegeln, in der MCSSA muss berücksichtigt werden, wenn ein SRP/CS für Wartungszwecke stummgeschaltet wird.

Wenn aufgrund eines Mangels an Produktgeschichte oder aufgrund eines neuen Produktdesigns kein Anwendungsprofil definiert ist, muss der schlimmste glaubwürdige Fall des bestimmungsgemäßen Gebrauchs genutzt werden.

ANMERKUNG Eine Gefährdung kann eine Kombination aus Bedingungen (z. B. Umwelt- und Betriebsbedingungen) der Maschine sein.

Tabelle 2 — Aufenthaltsdauer im Gefährdungsereignis basierend auf dem Anwendungsprofil

E0	E1	E2
< 1 %	> 1 % x < 10 %	> 10 %

6.1.5 Bewertung einer Möglichkeit zur Vermeidung von Schäden

Unter Berücksichtigung menschlicher Faktoren (z. B. Panik, wiederholter Funktionsbefehl usw.) und der Reaktionszeit muss Folgendes beurteilt werden, um die Beherrschbarkeit und die Mittel zur Herbeiführung eines sicheren Halts oder sicheren Zustands für die Maschine oder Sicherheitsfunktion zu bestimmen.

Bei der Analyse eines Systems können keine anderen Merkmale dieses Systems berücksichtigt werden; diese Merkmale können alternative Steuerungen, zusätzliche Warnungen, redundante Elemente, Diagnose usw. sein.

Alternative Steuerungen können nicht berücksichtigt werden, wenn sie mit dem analysierten System einen Ausfall infolge gemeinsamer Ursache teilen.

Bei Berücksichtigung mehrerer alternativer Aktionen müssen alle diese Aktionen unabhängig voneinander sein.

Die folgenden Faktoren werden zur Bestimmung der Beherrschbarkeit verwendet:

Alternative Steuerungen

- **AC0** – keine alternativen Steuerungen oder mögliche Aktion
- **AC1** – eine oder mehr alternative Steuerungen oder mögliche Aktion

Kenntnis der Gefährdung

- **AW3 – Hoch:** Bekannt vor Funktionsaktion z. B.
- **AW2 – Mittel:** Bekannt bei Funktionsaktion, die gesamte Zeit
- **AW1 – Niedrig:** Bekannt bei Funktionsaktion, für eine gewisse Zeit
- **AW0 – Keine:** Nicht bekannt bei Funktionsaktion, z. B. ein System, das nicht sichtbar ist oder über dessen Bedienung durch eine unbeabsichtigte Aktion Unkenntnis herrscht.

Warnanzeigen sollten in der Bewertung der Kenntnis der Gefährdung nur in Betracht gezogen werden, wenn sie als eine Warnanzeige für Sofortmaßnahmen definiert sind, die über keine gemeinsamen Bauteile mit dem analysierten System verfügen.

Reaktionsfähigkeit

- **AR 3** – Bediener kann rechtzeitig reagieren, natürliche Reaktion, Bediener hat Hand auf Steuerung, z. B. Bediener kann Gefährdung umfahren, wenn Bremsen ausfallen.
- **AR 2** – Bediener kann rechtzeitig reagieren, natürliche Reaktion, Bediener muss Hand zum Bedienen bewegen, z. B. Bediener betätigt Feststellbremse, wenn Bremsen ausfallen.
- **AR 1** – Bediener kann rechtzeitig reagieren, unnatürliche Reaktion, z. B. Bediener setzt Anbaugerät auf dem Boden ab, wenn Bremsen ausfallen.
- **AR 0** – Unabhängig davon, ob es ein weiteres System gibt, mit dem reagiert werden kann, reagiert der Bediener oder das System nicht rechtzeitig, um die Gefährdung zu verhindern.

Mehrere Aktionen umfassen erwartete, beabsichtigte und/oder intuitive Aktionen und müssen dokumentiert werden. Bei einem Ausfall der Bremsen einer Planiermaschine ist es beispielsweise zu erwarten und intuitiv, dass der Bediener die Schneide oder den Aufreißer absenkt.

Beispiele anderer Sicherheitsfunktionen sind in Anhang E enthalten.

Klassifizierung der Beherrschbarkeit

- C0 – Hohe Beherrschbarkeit
- C1 – Mittlere Beherrschbarkeit
- C2 – Niedrige Beherrschbarkeit
- C3 – Keine Beherrschbarkeit

		AR0	AR1	AR2	AR3
AC0		C3	C3	C3	C3
AC1	AW0	C3	C3	C3	C3
	AW1	C3	C3	C3	C2
	AW2	C3	C3	C2	C1
	AW3	C3	C2	C1	C0

Bild 1 — Klassifizierung der Beherrschbarkeit

AC – Alternative Steuerungen

AW – Kenntnis der Gefährdung

AR – Reaktionsfähigkeit

6.1.6 Auswahl des erforderlichen MPL

Das erforderliche MPL_r wird durch die Kombination der Schwere-, Aufenthaltsdauer- und Beherrschbarkeitswerte für jede in der Risikobeurteilung identifizierte Gefährdung in Bild 1 bestimmt.

Zusätzlich zu diesen Levels gibt es eine Qualitätsmessung (QM), deren implizite Anforderung die Durchführung einer Systementwicklung in Übereinstimmung mit Qualitätsmanagementwerkzeugen, relevanten technischen Anforderungen und geltenden Normen ist. Für eine QM ist eine Gefährdungsanalyse und eine MCSSA erforderlich.

Die Integrität der Steuerungen, die kein MPL_r erfordern, muss durch die Befolgung anerkannter Regeln der Technik, relevanter technischer Anforderungen, Qualitätsmanagementsysteme (QMS) und technischer Normen gewährleistet werden, wie in ISO 19014-2 definiert. Andere Teile der ISO 19014-Reihe sind nicht anwendbar.