

DIN EN ISO 19014-1



ICS 53.100

Einsprüche bis 2016-11-23

Entwurf**Erdbaumaschinen –****Funktionale Sicherheit –****Teil 1: Methodik zur Bestimmung sicherheitsbezogener Teile einer Steuerung und von Leistungsanforderungen (ISO/DIS 19014-1:2016); Deutsche und Englische Fassung prEN ISO 19014-1:2016**

Earth moving machinery –

Safety –

Part 1: Methodology to determine safety related parts of the control system and performance requirements (ISO/DIS 19014-1:2016);

German and English version prEN ISO 19014-1:2016

Engins de terrassement –

Sécurité –

Partie 1: Méthodologie permettant de déterminer les parties du système de commande et les exigences de performance liés à la sécurité (ISO/DIS 19014-1:2016);

Version allemande et anglaise prEN ISO 19014-1:2016

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2016-09-23 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 des 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 48 Seiten

DIN-Normenausschuss Maschinenbau (NAM)

Nationales Vorwort

Dieser Norm-Entwurf enthält sicherheitstechnische Festlegungen.

Er beinhaltet die Deutsche Fassung der vom Technischen Komitee ISO/TC 127 „Earth-moving machinery – Safety“ in Zusammenarbeit mit dem Technischen Komitee CEN/TC 151 „Bau- und Baustoffmaschinen - Sicherheit“ im Europäischen Komitee für Normung (CEN) ausgearbeiteten prEN ISO 19014-1:2016.

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung der prEN ISO 19014-1 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 Erdbaumaschinen 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.

Für die zitierten Internationalen Normen und Dokumente, sofern sie nicht als DIN ISO-Normen mit gleicher Zählnummer veröffentlicht sind, gibt es keine nationalen Entsprechungen.

Erdbaumaschinen — Funktionale Sicherheit — Teil 1: Methodik zur Bestimmung sicherheitsbezogener Teile einer Steuerung und von Leistungsanforderungen (ISO/DIS 19014-1:2016)

Engins de terrassement — Sécurité — Partie 1 : Méthodologie permettant de déterminer les parties du système de commande et les exigences de performance liés à la sécurité (ISO/DIS 19014-1:2016)

Earth-moving machinery — Safety — Part 1: Methodology to determine safety-related parts of the control system and performance requirements (ISO/DIS 19014-1:2016)

ICS:

Deskriptoren:

Inhalt

	Seite
Europäisches Vorwort	3
Vorwort	4
Einleitung	5
1 Anwendungsbereich	6
2 Normative Verweisungen	6
3 Begriffe	7
4 Verfahren zur Bestimmung von MPLr für SRP/CS von EMM	9
4.1 Allgemeines	9
4.2 Verfahren	9
5 Bestimmung der Grenzen der Maschine	10
5.1 Allgemeines	10
5.2 Identifizierung von Gefährdungen	10
5.3 Risikoeinschätzung	10
6 Verfahren zur Bestimmung des Performance Levels	11
6.1 Anforderungen	11
6.1.1 Allgemeines	11
6.1.2 Aufgaben der Risikoanalyse	11
6.1.3 Teilnehmer der Risikobeurteilung	11
6.1.4 Bewertung und Klassifizierung eines potenziellen Schadens	11
6.1.5 Bewertung der Aufenthaltsdauer in der beobachteten Situation	12
6.1.6 Bewertung einer Möglichkeit zur Vermeidung von Schäden	14
6.1.7 Auswahl des erforderlichen MPL	15
7 Benutzerinformationen	16
7.1 Informationen für Bediener/Bedienungsanleitung	16
7.2 Informationen für Service-/Wartungsanleitungen	16
Anhang A (informativ) Flussdiagramm für das Verfahren	17
Anhang B (normativ) Tabelle mit Warn-/Betriebsanzeigen	18
Anhang C (informativ) Liste mit Gefährdungen aus 12100 (EMM-spezifisch)	20
C.1 Beim Entwerfen der Maschine zu berücksichtigende Gefährdungen	20
C.1.1 Allgemeines	20
C.1.2 Mechanische Gefährdungen	20
C.1.3 Durch die EMM erzeugte mechanische Gefährdungen	20
C.2 Elektrische Gefährdung	21
C.3 Thermische Gefährdungen	21
C.4 Gefährdungen durch Lärm	22
C.5 Gefährdungen durch Vibration	22
C.6 Gefährdungen durch Werkstoffe und Substanzen	22
C.7 Gefährdungen, die sich durch die Vernachlässigung der Grundsätze der Ergonomie bei der konstruktiven Ausführung der Maschine ergeben	22
C.8 Gefährdung durch Rutschen, Stolpern und Hinfallen	23
C.9 Kombinationen von Gefährdungen	23
C.10 Gefährdungen in Verbindung mit der Umgebung, in der die Maschine verwendet wird	23
Literaturverzeichnis	24

Europäisches Vorwort

Dieses Dokument (prEN ISO 19014-1:2016) 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 vom DIN gehalten wird.

Dieses Dokument ist derzeit zur parallelen Umfrage vorgelegt.

Anerkennungsnotiz

Der Text von ISO/DIS 19014-1:2016 wurde vom CEN als prEN ISO 19014-1:2016 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/TC 127.

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

- *Part 1: Methodology to determine safety-related parts of the control system and performance requirements*
- *Part 2: Design and evaluation of safety-related electrical and electronic machine control systems*
- *Part 3: Environmental performance and test requirements of electronic and electrical components used in safety-related parts of the control system*
- *Part 4: Design and evaluation of software and data transmission for safety related parts of the control system*

Die ISO 19014-Reihe ersetzt ISO 15998.

Einleitung

Die vorliegende Internationale Norm beschäftigt sich mit Systemen, die sämtliche Energietypen für die funktionale Sicherheit bei Erdbaumaschinen umfassen.

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-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-B Norm, wie in ISO 12100 bezeichnet.

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 Gefahr anhand einer Risikobeurteilung identifiziert wurde und ein Stellteil als sicherheitsbezogener Teil der Steuerung (SRP/CS) bestimmt wurde.

Die Gefahrenidentifizierung wird anhand einer Risikobeurteilung mithilfe des in ISO 12100 beschriebenen Verfahrens oder anderer Mittel bestimmt und wird nicht von diesem Dokument abgedeckt.

Wo ein Stellteil als sicherheitsbezogen bestimmt wird, wird ein Performance Level einer Maschine (MPL) durch das beschriebene Verfahren festgelegt.

ANMERKUNG 1 Der Begriff MPL wird verwendet, um das von einem sicherheitsbezogenen Teil einer Steuerung erforderliche Leistungsniveau zu beschreiben. Das "M" bezieht sich auf Maschinen und gilt für alle Erdbaumaschinen, die im Anwendungsbereich dieses Dokuments behandelt werden.

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.

Ein sicherheitsbezogenes Steuersystem, das die durch eine Maschinen- oder Systemrisikobeurteilung identifizierten Gefahren angeht, umfasst insbesondere Systeme, die die Bewegung der Maschine steuern. (beispielsweise angetriebene Bewegungen, Bremsen, Lenken, Zusatzeinrichtungen und Steuerungen der Arbeitsausrüstung).

Steuerungen, die vor rapiden thermischen Ereignissen, elektrischen Schlägen, Anforderungen für explosionsfähige Atmosphären, usw. schützen, sind ebenfalls mit eingeschlossen.

Die Grundsätze der vorliegenden Norm können ebenfalls auf Warnanzeigen für Sofortmaßnahmen angewandt werden, die den Bediener vor einer möglichen Gefahr warnen und eine unmittelbare Handlung von Bediener erfordern, um eine solche Gefahr zu korrigieren und ihr vorzubeugen.

Andere sicherheitsbezogene Geräte, die den Bediener auf Ausfälle aufmerksam machen, sind von dieser Norm ausgeschlossen (z. B. Scheibenwischer, Scheinwerfer usw.).

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

Die vorliegende Norm ersetzt ISO 15998:2008.

2 Normative Verweisungen

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

ISO 3411, *Earth-moving machinery — Physical dimensions of operators and minimum operator space envelope*

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 14121-1:2007, *Safety of machinery — Principles of risk assessment*

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 — General Requirements*

3 Begriffe

Für die Zwecke dieses Dokuments gelten zusätzlich zu den unten aufgeführten Definitionen die folgenden Begriffe aus ISO 6165, ISO 13849-1, ISO 12100 und ISO 20474-1.

3.1.

Performance Level der Maschine (en: Machine Performance Level, MPL)

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

3.2

Funktionale Sicherheit

Teil der Gesamtsicherheit, der von der korrekten Betriebsweise eines Systems oder einer Ausrüstung als Reaktion auf seine Eingaben abhängt

3.3.1

Steuerung der Maschine (en: Machine Control System, MCS)

System, das aus den Bauteilen besteht, die zur Erfüllung der Funktion des Systems erforderlich sind, einschließlich Messfühlern, Signalverarbeitungseinheiten, Monitoren, Stellteilen und Stellantrieben oder mehreren davon

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.

3.3.2

Sicherheitsbezogener Teil einer Steuerung (en: safety related part of the control system, SRP/CS)

Teil einer Steuerung, die auf sicherheitsbezogene Eingangssignale reagiert und sicherheitsbezogene Ausgangssignale erzeugt

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 Auftragnehmers).

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

3.4

Bedienperson

Person, die eine EMM auf einem hohen Niveau an Fähigkeiten, Übung und Kenntnis bedient

3.5

Mitarbeiter

Person, die in der Nähe einer Maschine arbeitet und von der angenommen wird, dass sie ein mittleres Niveau an Übung (Einarbeitung vor Ort) und Kenntnis besitzt

3.6

Umstehende Person

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

3.7

Instandhalter

Person, deren Funktion es ist, Wartungsarbeiten auf der analysierten Maschine durchzuführen. Dieses Personal ist normalerweise geschult und mit der Maschine vertraut

3.8

Beherrschbarkeit

involviert die Möglichkeit einer Einzelperson, Schaden in der Situation zu vermeiden, die ihn/ihr einem Risiko aussetzt

3.9

Aufenthaltsdauer

Dauer und Häufigkeit, in der sich eine Einzelperson in einer Situation befindet, in der eine potenzielle Gefährdung besteht

3.10

Schwere

Ausmaß des Schadens an einer gefährdeten Einzelperson

3.11

Warnanzeige

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

Anmerkung 1 zum Begriff: Die erforderliche Handlung kann umgehend für dringende Warnungen wie Umkippp-Anzeigen oder Warnhinweise wie niedriger Ölstand erfolgen – erforderliche Handlungen werden normalerweise durch die Farbe der Anzeige oder der Dringlichkeit des Alarms bestimmt.

3.11.1

Warnanzeige für Sofortmaßnahmen

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

Anmerkung 1 zum Begriff: Anhang C bietet eine Liste mit Warnanzeigen und Leitfäden für diejenigen, die eine umgehende Handlung erfordern.

3.12

Betriebsanzeige

Visuelle Anzeige zur Darstellung der Betriebsart

3.13

Anwendungsprofil

Auflistung der Zeit, in der eine Maschine für eine gegebene Anwendung in einem Arbeitszyklus verwendet wird (ausgedrückt in %)

BEISPIEL Anwendungsprofil der Maschine = 100 %:

20 % Nutzung auf der Straße;

40 % Anwendung Schaufel/Baustelle;

30 % Nutzung des Tieflöffels;

10 % Leerlauf.

4 Verfahren zur Bestimmung von MPLr für SRP/CS von EMM

4.1 Allgemeines

In den meisten Situationen wird die Sicherheit durch eine Anzahl an Schutzsystemen erreicht, die auf vielen Technologien basieren (z. B. mechanisch, hydraulisch, pneumatisch, elektrisch, elektronisch, programmierbar elektronisch). Die Sicherheitsstrategien berücksichtigen nicht nur sämtliche Elemente ohne individuelles System, wie beispielsweise Sensoren, Steuergeräte und Stellantriebe, sondern auch sämtliche sicherheitsbezogenen Teile einer Steuerung.

Die Reihe ISO 19014 legt einen Ansatz für das Design und die Bewertung von sicherheitsbezogenen Steuerungen sämtlicher Energietypen für sämtliche Aktivitäten von Sicherheitslebenszyklen von Erdbaumaschinen dar, die in ISO 6165 definiert werden. Sie deckt die möglichen Gefährdungen ab, die durch das funktionale Verhalten sicherheitsbezogener Systeme verursacht werden, mit Ausnahme von Gefährdungen, die aufgrund der Ausrüstung selbst entstehen (elektrische Schläge, Brände, Nenn-Performance Level von Bauteilen für die aktive und passive Sicherheit usw.).

Teile der Steuerung der betroffenen Maschine, die Sicherheitsfunktionen bieten, werden sicherheitsbezogene Teile von Steuerungen (SRP/CS) genannt. Diese können aus Hardware oder Software bestehen, separate oder integrierte Teile einer Steuerung sein und entweder ausschließlich kritische Funktionen durchführen oder Teil einer Betriebsfunktion darstellen.

Allgemein darf der Designer (und zu einem gewissen Maß der Anwender) die Konstruktion und Validierung dieser SRP/CS als Teil der Risikobeurteilung kombinieren. Das Ziel ist es, die mit einer gegebenen Gefährdung (oder Gefahrensituationen) verbundenen Risiken unter sämtlichen Gebrauchsbedingungen der Maschine zu reduzieren. Dies kann erreicht werden, indem verschiedene Schutzmaßnahmen (sowohl SRP/CS als auch Nicht-SRP/CS) angewendet werden. Das Endergebnis ist das Erzielen einer sicheren Bedingung.

Um den Designer durch die Konstruktion zu führen und die Bewertung des erreichten Performance Level zu vereinfachen, definiert ISO 19014 einen Ansatz, der auf einer Klassifizierung der Strukturen mit verschiedenen Designfunktionen und spezifischem Verhalten im Falle eines Ausfalls basiert.

Die Performance Levels und Kategorien können auf die Steuerungen sämtlicher Arten an mobilen 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 auf dem Kundenrisiko basierenden 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 (Design, 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 MPLr für sicherheitsbezogene Teile von Steuerungen (SRP/CS):

- a) Bestimmung der vorgesehenen EMM-Einschränkungen gemäß EN ISO 12100:2010. (Abschnitt 5);
- b) Durchführung einer Risikobeurteilung mithilfe eines geeigneten Werkzeugs und Identifizierung der mit der Funktion oder Anwendung der Maschine verbundenen Gefährdungen;

- c) Festlegung, wie die im Risikobeurteilungsverfahren identifizierten Gefährdungen abgeschwächt oder sich davor geschützt werden kann. (Dies kann zusätzliche Steuerungen oder Mittel zur Sicherstellung der Integrität inhärenter Steuerungen erfordern.);
- d) Bestimmung, ob die genutzte Gefährdungsminderung/Schutzmaßnahme von einer Steuerung abhängt und ob dies ein SRP/CS ist. (Dies muss Steuerungen umfassen, die zur Maschine hinzugefügt wurden, um eine Gefährdung zu mindern, sowie Steuerungen, welche die Bewegung der Maschine oder Steuerungen regeln, die verwendet werden, wenn Ausfälle zu einer Gefahrensituation führen.);
- e) Wenn eine Steuerung nicht als SRP/CS bestimmt wird, wird das Verfahren angehalten und eine MPL-Bestimmung ist nicht erforderlich. Die Steuerungen, 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 die folgenden Qualitätsmanagementwerkzeuge, die relevanten technischen Anforderungen sowie die geltenden Normen gewährleistet werden;
- f) Wenn die Schutzmaßnahme von einem SRP/CS abhängt, muss die Berechnungsmethode zur Bestimmung des Performance Levels verwendet werden, um die MPL(s) auszuwählen, die für die SRP/CS erforderlich sind, um die Sicherheitsfunktion durchzuführen. (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 muss für alle Phasen des Lebenszyklus des Maschinensystems dokumentiert werden, einschließlich der Merkmale und der erwarteten Leistungen der Maschine.

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

Weitere Leitsätze zu den Grenzen der Maschinenverwendung können ISO 12100:2010 entnommen werden.

Eine Risikobeurteilung muss Informationen berücksichtigen, die den Gesamtumfang der Anwendung der EMM definieren.

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 Designer die vom Bediener geforderten Reaktionen versteht, um eine Gefährdung abzuschwächen, wenn eine Warnung gegeben wurde. Anhang C bietet eine normative Liste an Anzeigen, wenngleich diese nicht vollständig ist.

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

5.3 Risikoeinschätzung

Die Risikoeinschätzung wird verwendet, um die wahrscheinliche Schwere des Schadens (S) und die Wahrscheinlichkeit seines Auftretens zu definieren (E).

Wo kein Verletzungsrisiko vorliegt, wird der Prozess angehalten, die Risikobeurteilung muss Teil der technischen Dokumentation sein und die Anforderungen für ein QM wie in ISO 19014-2 definiert werden wie in Anhang B gezeigt befolgt.

Wo es ein Verletzungsrisiko gibt, das nicht ausgeschlossen werden kann, und der Anwender dieses Dokuments zu Schritt 2 in Anhang B springt, muss Abschnitt 6 verwendet werden, um das erforderliche Performance Level des sicherheitsbezogenen Teils einer Steuerung zu bestimmen.

6 Verfahren zur Bestimmung des Performance Levels

6.1 Anforderungen

6.1.1 Allgemeines

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

Entscheidungen, die später im Lebenszyklus getroffen werden, die den Grundsatz ändern, auf dem frühere Entscheidungen beruhen, müssen eine neue Risikobeurteilung initiieren.

Die Architektur des SRP/CS dürfen nicht als Teil der Risikobeurteilung angesehen werden.

ANMERKUNG Die Integrität der Steuerungen, die kein MPLr erfordern, müssen durch die folgenden anerkannten Regeln der Technik, die relevanten technischen Anforderungen, Qualitätsmanagementsysteme (QM) und geltende Normen gewährleistet werden.

6.1.2 Aufgaben der Risikoanalyse

Die Betriebsbedingungen, bei denen die EMM bei korrekter Verwendung Gefährdungen initiieren kann (einschließlich vernünftigerweise vorhersehbarer menschlicher Bedienungsfehler und Teileausfällen) müssen berücksichtigt werden.

Bei risikobewerteten und in verschiedenen Anwendungen oder Szenarien verwendeten Systemen, bei denen die Schwere, Beherrschbarkeit oder Aufenthaltsdauer variieren kann, muss jede Anwendung individuell bewertet und das höchste Performance Level für eine gegebene Anwendung aus dem Risikographen in diesem System verwendet werden.

6.1.3 Teilnehmer der Risikobeurteilung

Die Risikobeurteilung muss verschiedene Einzelpersonen aus unterschiedlichen Abteilungen involvieren, z. B. elektronische oder elektrische Entwicklung, Prüfung oder Validierung, Maschinen- oder Hydraulikdesign, Wartung, Vertrieb und Marketing.

Ein informatives Beispiel einer Risikobeurteilungsmethode wird in Anhang A gegeben.

6.1.4 Bewertung und Klassifizierung eines potenziellen Schadens

Potenziell schädliche Auswirkungen können ermittelt werden, indem mögliche Fehlfunktionen und systematische Ausfälle unter relevanten Betriebsbedingungen ermittelt werden. Die potenzielle Schwere der Schäden wird für jedes relevante Szenario so präzise wie möglich beschrieben.

ANMERKUNG Die Einschätzung der Schwere hat ihren Schwerpunkt normalerweise auf dem schlimmsten und schwersten Schaden, der realistischere auftreten kann (schlimmster glaubwürdiger Fall), anstatt der schlimmsten erdenklichen Konsequenz. (siehe ISO/TR 14121-2:2012, Abschnitt 6.2.2.3) Welche Schadensschwere angenommen werden soll, ist nicht immer einfach. 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 Risikobeurteilung durchgeführt wird, muss das Risiko der schlimmsten glaubwürdigen Schwere des Schadens genutzt 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 involvierten Maschine und andere Parteien (z. B. Personen, die Unterstützung anbieten, andere Bedienungspersonen des Maschinensystems, umstehende Personen, Mitarbeiter usw.) müssen in der detaillierten Beschreibung des Schadens verwendet werden.

Eine Untersuchung des Risikos für Sicherheitsfunktionen legt ihren Schwerpunkt auf die Ursache der Verletzungen von Personen. Wenn in der Analyse des potenziellen Schadens etabliert werden kann, dass der Schaden eindeutig auf Besitztümer beschränkt ist und keine Verletzungen von Personen umfasst, wäre es nicht erforderlich, eine Regelungseinrichtung des Systems als Sicherheitsfunktion zu klassifizieren. Dies wird durch die Einführung einer S0-Schadensklassifizierung und eines QM ermöglicht.

Tabelle 1 — Beispiele für Beschreibungen von Verletzungen

S0	S1	S2	S3
Keine signifikanten Verletzungen, braucht nur erste Hilfe	Verletzungen, braucht medizinische Hilft, vollständige Genesung, reversible Verletzung ohne Verlust der Arbeitskapazität nach der Genesung	Schwer und lebensbedrohlich, permanenter teilweise Verlust von Arbeitskapazität, gilt als irreversibel	Todesfall

6.1.5 Bewertung der Aufenthaltsdauer in der beobachteten Situation

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

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

Die Variable E muss verwendet werden, um die verschiedenen Häufigkeiten oder die Aufenthaltsdauer zu kategorisieren.

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, bei der ein Ausfall zu einer Verletzung des Bedieners oder der umstehenden Person führen könnte.

Die Exposition in einer gegebenen Situation wird durch die Häufigkeit und die Dauer in einem gegebenen Anwendungsprofil bestimmt und als Prozentsatz ausgedrückt.

Das folgende Verfahren muss verwendet werden, um die Aufenthaltsdauer zu bestimmen:

- i) Festlegung des Anwendungsprofils der Maschine;
- ii) Festlegung des Prozentsatzes der Zeit in einem gegebenen Segment dieses Anwendungsprofils;
- iii) Festlegung, welchen Prozentsatz der Zeit innerhalb dieses Segments Personen jeder Gruppe (Bediener, Mitarbeiter, Wartungspersonal oder umstehende Person) der Gefährdung ausgesetzt werden.

Informatives Beispiel eines Anwendungsprofils:

- i) Anwendungsprofil der gesamten Maschine = 100 %
 - 20 % Nutzung auf der Straße,
 - 40 % Anwendung Schaufel/Baustelle,
 - 30 % Nutzung des Tieflöffels,
 - 10 % Leerlauf.
- ii) Dieses Anwendungsprofil darf weiter definiert werden als:

Nutzung des Tieflöffels 30 %

- 50 % Materialtransport = Anwendungsprofil 15 %,
- 50 % Graben = Anwendungsprofil 15 %.
- iii) Die der Gefährdung ausgesetzten Personen aus jeder Gruppe für das Anwendungsprofil des Materials:
 - Bedienerperson = keiner Gefährdung ausgesetzt;
 - Mitarbeiter = 100 % des Anwendungsprofils des Materialtransports = 15 %;
 - Umstehende Person = selten = nur 10 % der Zeit von 15 % des Materialtransports = 1,5 % des Anwendungsprofils der Maschine.

Dieses Anwendungsprofil könnte sich ändern; einige Maschinen sollen in einer einzigen Anwendung während des gesamten Lebenszyklus arbeiten, wobei dies für andere Maschinen von der vorgesehenen Arbeitsumgebung, des Arbeitszyklus, den Zusatzeinrichtungen, usw. abhängt und in der Risikobeurteilung berücksichtigt werden muss.

Wenn eine Risikobeurteilung durchgeführt wird, muss das Risiko der längsten Aufenthaltsdauer genutzt 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 sollte die Zeit zur Wartung der Maschine widerspiegeln. Für die meisten Maschinen würde dies normalerweise mit 10 % der Zeit berücksichtigt werden. Eine Ausnahme dafür wären Maschinen, die in Maschinenparkszenarien betrieben werden, in denen es mehrere Maschinen desselben Typs gibt und in denen häufigere Wartungsaufgaben oft vom selben Wartungspersonal durchgeführt werden. In der Risikobeurteilung muss berücksichtigt werden, wenn ein SRP/CS für Wartungszwecke stummgeschaltet werden.

Transportanwendungen haben beispielsweise oft 20 oder mehr Muldenkipper eines ähnlichen Typs an einem Standort. Diese Maschinen werden oft länger als eine Schicht am Tag betrieben. In diesen Fällen würde eine 250-Stunden-Wartungsaufgabe fast täglich von einer einzigen Wartungsperson durchgeführt werden.

Wo aufgrund eines Mangels an Produktgeschichte oder aufgrund eines neuen Produktdesigns kein Anwendungsprofil definiert ist, ist es akzeptabel, Tabelle 2 zur Bestimmung erwarteter Expositionsgrenzwerte zu nutzen.

ANMERKUNG Eine Gefährdung kann eine Kombination von Bedingungen der Maschine sein (z. B. umwelttechnisch und betrieblich).