

DIN EN ISO 19014-2

ICS 53.100

Einsprüche bis 2019-12-04

Entwurf

**Erdbaumaschinen –
Funktionale Sicherheit –
Teil 2: Entwurf und Bewertung von Hardware- und
Architekturanforderungen für sicherheitsrelevante Teile des
Steuerungssystems (ISO/DIS 19014-2:2019);
Deutsche und Englische Fassung prEN ISO 19014-2:2019**

Earth-moving machinery –
Functional safety –
Part 2: Design and evaluation of hardware and architecture requirements for safety-related
parts of the control system (ISO/DIS 19014-2:2019);
German and English version prEN ISO 19014-2:2019

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2019-10-04 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 88 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“ in Zusammenarbeit mit dem Technischen Komitee CEN/TC 151 „Baumaschinen und Baustoffmaschinen - Sicherheit“ im Europäischen Komitee für Normung (CEN) ausgearbeiteten EN ISO 19014-2:2019.

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

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

Ab dem Zeitpunkt ihrer Bezeichnung als Harmonisierte Norm im Amtsblatt der Europäischen Union kann der Hersteller bei ihrer Anwendung davon ausgehen, dass er die von der Norm behandelten Anforderungen der Maschinenrichtlinie eingehalten hat (so genannte Vermutungswirkung).

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 2: Entwurf und Bewertung von Hardware- und Architektur Anforderungen für sicherheitsrelevante Teile des Steuerungssystems (ISO/DIS 19014-2:2019)

Earth-moving machinery — Functional safety — Part 2: Design and evaluation of hardware and architecture requirements for safety-related parts of the control system (ISO/DIS 19014-2:2019)

ICS:

Deskriptoren:

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

STD Version 2.9p

Inhalt

	Seite
Europäisches Vorwort	3
Vorwort	4
Einleitung	5
1 Anwendungsbereich	6
2 Normative Verweisungen	6
3 Begriffe	7
4 Symbole und Abkürzungen	8
5 Allgemeine Anforderungen	9
5.1 Bestehende SCS	9
6 Systementwurf	9
6.1 Allgemeines	9
6.1.1 Interaktion zwischen verschiedenen SRP/CS	10
6.1.2 Unterschiede zwischen Sicherheitsfunktionen mobiler und statischer Maschinen	10
6.1.3 Beurteilungsprozess	11
6.2 Gestaltung der Hardware	11
7 Bewertung der Sicherheitsleistung des Systems	12
7.1 Erreichtes Performance Level der Maschine (MPLa)	12
7.2 Hardware-Sicherheitsbewertung	12
7.2.1 Allgemeines	12
7.2.2 Fehlerberücksichtigung	13
7.2.3 Fehlerausschluss	13
7.2.4 Mittlere Zeit bis zum gefahrbringenden Ausfall (MTTFd)	13
7.3 Diagnosedeckungsgrad (DC)	13
7.3.1 DC des ESCS	13
7.3.2 DC des N/ESCS	14
7.4 Fehlerausschlüsse auf Systemlevel bei hydraulischen Systemen, basierend auf der Robustheit des hydraulischen Systems (HSR)	14
7.5 Kategorie-Klassifikationen	15
7.5.1 Allgemeines	15
7.5.2 Kategorie 1	18
7.5.3 Kategorie 2	20
7.5.4 Richtlinie zu in Konflikt stehenden Sicherheitsfunktionen	21
7.5.5 Überlegungen zu den SRP/CS von bei einem Ausfall betriebsfähigen Systemen	22
7.6 Kombination von SCS zur Erreichung eines Gesamt-MPL	22
8 Informationen für Gebrauch und Instandhaltung	24
Anhang A (informativ) Beispielsysteme und Bewertungen	25
Anhang B (normativ) Beispiele für Auswertungen mithilfe der HSR-Bewertung	39
Anhang C (normativ) Kompatibilität mit anderen funktionalen Sicherheitsnormen	42
Anhang D (informativ) Bewertung der Sicherheitsfunktion	43
Anhang E (informativ) Ausnahmen, Ausschlüsse, Ergänzungen zu ISO 13849-1 und ISO 13849-2	44
Literaturhinweise	45

Europäisches Vorwort

Dieses Dokument (prEN ISO 19014-2:2019) wurde vom Technischen Komitee ISO/TC 127 „Earth-moving machinery“ in Zusammenarbeit mit dem Technischen Komitee CEN/TC 151 „Bau- und Baustoffmaschinen - Sicherheit“ erarbeitet, dessen Sekretariat von DIN gehalten wird.

Dieses Dokument ist derzeit zur parallelen Umfrage vorgelegt.

Dieses Dokument wird ISO 15998 ersetzen.

Anerkennungsnotiz

Der Text von ISO/DIS 19014-2:2019 wurde von CEN als prEN ISO 19014-2:2019 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. 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. 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 WTO-Grundsätze zu technischen Handelshemmnissen (TBT, en: Technical Barriers to Trade) durch ISO enthält der folgende Link: Foreword - Supplementary information.

Das für dieses Dokument verantwortliche Komitee ist ISO/TC 127.

Die Normenreihe ISO 19014 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 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.

Dieser Teil von ISO 19014 ist eine Typ-C-Norm entsprechend ISO 12100.

ISO 19014-2 ist die Anpassung von ISO 13849 zur Schaffung einer Typ-C-Norm, die die spezifische Anwendung funktionaler Sicherheit auf Erdbaumaschinen behandelt.

ISO 19014-2 ergänzt die Aktivitäten bezüglich des Sicherheitslebenszyklus von Sicherheitssteuerungen nach ISO 13849-1:2015 und ISO 13849-2:2012 bei Erdbaumaschinen, wie in ISO 6165 festgelegt.

1 Anwendungsbereich

Dieser Teil von ISO 19014 legt allgemeine Grundsätze für die Entwicklung und Beurteilung des erreichten Leistungsniveaus 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 angetrieben werden, fest. Dieses Dokument wird in Verbindung mit den anderen Teilen der Reihe verwendet.

In Bezug auf Erdbaumaschinen (EMM) ist ISO 19014 in Verbindung mit ISO 13849 zu verwenden und ersetzt ISO 15998. Wenn in ISO 19014 spezifische Anforderungen angegeben werden, haben diese gegenüber den in angegebenen ISO 13849 Anforderungen Vorrang.

Die Grundsätze dieser Norm gelten 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 untersucht.

Folgende Systeme sind vom Anwendungsbereich von ISO 19014 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 etc.) oder die primär dem Schutz von Eigentum dienen, sind von diesem Dokument ausgeschlossen. Akustische Signale sind von den Anforderungen des Diagnosedeckungsgrads ausgeschlossen. Siehe 7.4.3.

2 Normative Verweisungen

Die folgenden zitierten Dokumente sind für die Anwendung dieses Dokuments 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 6165, *Earth-moving machinery — Basic types — Identification and terms and definitions*

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, *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*

IEC 61508-2, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach ISO 19014-1, ISO 12100, ISO 13849-1:2015 und die folgenden Begriffe.

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

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

3.1 elektronische Sicherheitssteuerung ESCS

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 der kontrollierte Ausrüstungsprozess 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 der Sicherheitssteuerung (z. B. Lenkung) beim Auftreten eines Einzelfehlers gehören.

[QUELLE: ISO 3450:2011 3.15 mod.] geändert — Anmerkung 1 zum Begriff wurde ergänzt.

3.5 bewährte Komponenten

eine 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 folgende 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)
DCavg	durchschnittlicher Diagnosedeckungsgrad (en: average diagnostic coverage)
ECM	Elektronische Steuermodul (en: electronic control module)
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)
ILO	Eingang Logik Ausgang (en: input logic output)
MCS	Maschinensteuerungssystem (en: machine control system)
MPL	Performance Level der Maschine (en: machine performance level)
MPLa	erreichter Performance Level der Maschine (en: achieved machine performance level)
MPLr	erforderlicher Performance Level der Maschine (en: required machine performance level)
MTTF	mittlere Zeit bis zum Ausfall (en: mean time to failure)
MTTFd	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)
QM	Qualitätsmanagement (en: quality management)
RC	Zuverlässigkeitsabdeckung (Reliability Coverage)
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

In Bezug auf Erdbaumaschinen (EMM) muss ISO 19014 in Verbindung mit ISO 13849 verwendet werden und ersetzt ISO 15998. Wenn in ISO 19014 spezifische Anforderungen angegeben werden, haben diese gegenüber den in angegebenen ISO 13849 Anforderungen Vorrang.

Die Grundsätze dieser Norm müssen für Steuerungssysteme zur Steuerung von Maschinenbewegungen oder Verminderung von Gefährdungen gelten. Solche Systeme müssen nach der Normenreihe ISO 19014-1 oder ISO/TS 19014-5 hinsichtlich der Anforderungen an das Performance Level untersucht werden. Weiteren Maschinensteuerungssystemen, die eine Sicherheitsfunktion der Sicherheitssteuerung beeinflussen oder stummschalten, muss der gleiche Performance Level zugeordnet werden wie dem System, das sie beeinflussen oder stummschalten.

5.1 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 durchgeführt und ein Aktionsplan entwickelt und umgesetzt werden, um sicherzustellen, dass die Sicherheitsanforderungen eingehalten werden.

6 Systementwurf

6.1 Allgemeines

Eine Sicherheitsfunktion, die darauf angewiesen ist, dass ein Steuerungssystem die notwendige Gefährdungsminderung für die Maschine liefert, kann innerhalb des Anwendungsbereiches von ISO 19014-2 durch eine SCS implementiert werden. Eine SCS kann ein oder mehrere SRP/CS enthalten und mehrere SCS können ein oder mehrere SRP/CS (z. B. eine Logikeinheit, Leistungssteuerungselemente), wie in Bild 1 dargestellt, teilen. Es ist auch möglich, dass ein SRP/CS sowohl Sicherheitsfunktionen als auch Standard-Steuerungsfunktionen implementiert.

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

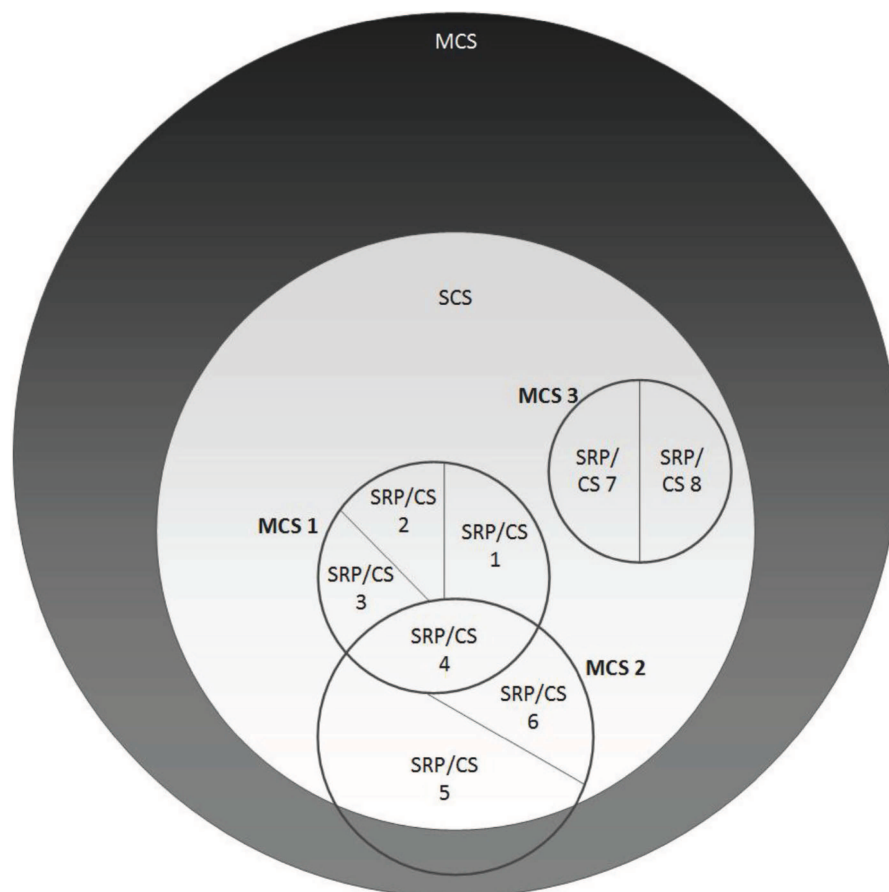


Bild 1 — Zusammenstellung sicherheitsbezogener MCS

Nach der Identifizierung der Sicherheitsfunktionen des Steuerungssystems, muss der Konstrukteur die Anforderungen jeder SCS, die eine Sicherheitsfunktion erfüllt, bestimmen und dokumentieren. 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.

6.1.1 Interaktion zwischen verschiedenen SRP/CS

Wenn Maschinenfunktionen für die synchrone Verwendung entworfen werden (z. B. Aufgabenautomatisierung), muss das Steuerungssystem so konstruiert werden, dass Gefährdungen aufgrund mangelnder Synchronisation vermindert werden.

ANMERKUNG Ein EMM-Beispiel für die Synchronisation wäre ein Baggerausleger, -arm und eine Ladeschaufel, die mithilfe eines Neigungs-Steuerungssystems simultan gesteuert werden.

6.1.2 Unterschiede zwischen Sicherheitsfunktionen mobiler und statischer Maschinen

Viele Sicherheitsfunktionen an mobilen Maschinen haben keine Start-/Stopp-Ausgänge, wie sie stationäre Maschinen für gewöhnlich aufweisen und werden eine Maschine nicht immer zur reinen 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 inkorrektur Anwendungsmengen einen geschlossenen statt eines offenen Regelkreises, muss das System Gefährdungen im Zusammenhang mit selbständiger Aktivierung sowie Ausfall nach Aufforderung adressieren etc.).

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

Die folgenden Gestaltungserwägungen müssen berücksichtigt werden:

- in 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 ECMs);
- in Konflikt stehende sichere Zustände, die von mehreren, durch das System adressierten Fehlertypen benötigt werden;
- Systeme, die ein bei einem Ausfall betriebsfähiges Sicherheitskonzept benötigen

6.1.3 Beurteilungsprozess

Beurteilungsprozesse sollten unabhängig vom Konstruktionsprozess sein.

6.2 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 auf der Systemebene beginnen, auf der Sicherheitsfunktionen und die damit verbundenen Anforderungen identifiziert werden (siehe Bild 2). Das System kann in Teilsysteme zerlegt werden, um die Entwicklung zu vereinfachen.

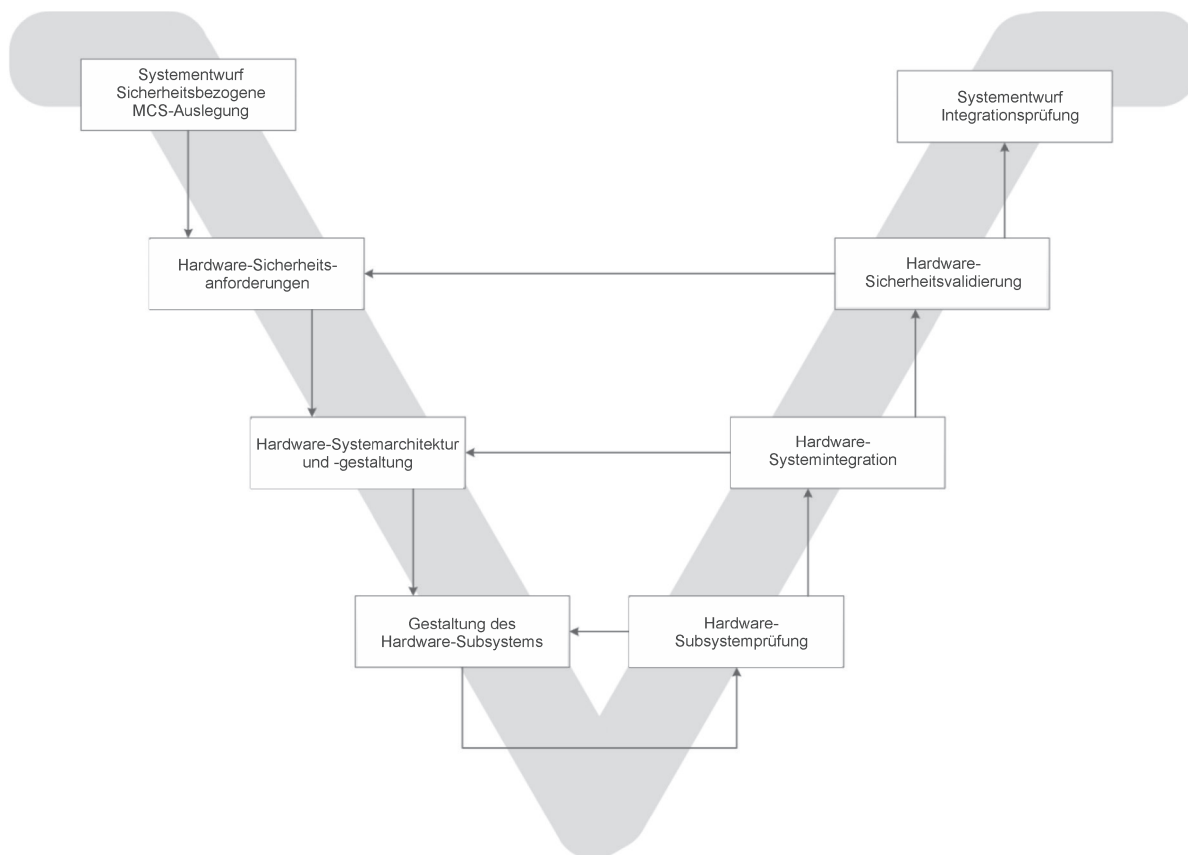
Sofern anwendbar, muss jede Phase des Entwicklungszyklus validiert werden.

Siehe Bild 2 für eine Abbildung des Hardware-Entwicklungsprozesses in Form eines V-Modells.

Die Vorgehensweise für den Entwurf der Hardware-Systemarchitektur umfasst die folgenden Schritte:

- a) Identifizierung der Betriebsumgebung und der Beanspruchungshöhe von Bauteilen;
- b) Auswahl der Bauteile;
- c) Identifizierung und Dokumentierung von Fehlerausschlüssen (Verw. 7.2.1) oder durch Verwendung einer passenden Systemanalyse (z. B. FMEA, Fehlerbaumanalyse etc.);
- d) Berechnung der $MTTF_d$ (siehe Anhang D, ISO 13849-1:2015) und Prüfung, ob die $MTTF_d$ den erforderlichen Level erreicht (siehe ISO 13849-1:2015);
- e) Prüfung, ob die Hardware den erforderlichen Level an DC bieten kann (Anhang E, ISO 13849-1:2015). 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 Anhang F, ISO 13849-1:2015), sofern erforderlich;
- g) Betrachtung von systematischen Ausfällen (Anhang G, ISO 13849-1:2015);
- h) Betrachtung möglicher Interaktionen von anderen Sicherheitsfunktionen;
- i) bei FPGA- und ASIC-Auslegung, (siehe Anhang E oder Anhang F, IEC 61508-2).

Siehe Anhang D für zusätzliche Informationen zur Bewertung von Sicherheitsfunktionen.



ANMERKUNG 1 Dieses Bild stellt nur eine der Gestaltungsmethoden dar (V-Modell). Jeder organisierte, bewährte Entwurfsprozess, der die Anforderungen in ISO 19014 erfüllt, sollte für den Entwurfsprozess verwendet werden

Bild 2 — V-Modell der Hardwareentwicklung

7 Bewertung der Sicherheitsleistung des Systems

7.1 Erreichtes Performance Level der Maschine (MPLa)

Für die Zwecke dieses Teils von ISO 19014 wird die erreichte Integrität sicherheitsbezogener Teile zur Ausführung einer Sicherheitsfunktion durch die Bestimmung des MPL_a ausgedrückt.

Die Fähigkeit, eine Sicherheitsfunktion unter den, in ISO 19014-3 dargelegten, erwarteten Umgebungsbedingungen auszuführen, muss demonstriert und dokumentiert werden.

7.2 Hardware-Sicherheitsbewertung

7.2.1 Allgemeines

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

Bei nicht bewährten Komponenten muss eine Fehlermöglichkeits- und Einflussanalyse (FMEA), eine Fehlerbaumanalyse oder eine gleichwertige Systemanalyse 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 dazu, Ausfallmechanismen zu mindern, die gemäß anerkannter industrieller Vorgehensweisen 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 zwei Leveln angewendet werden.

- 1) Teil-für-Teil-Basis – Nachdem alle Fehler identifiziert wurden, können manche Fehler ausgeschlossen werden. Andere können mit Diagnosemitteln innerhalb des Steuerungssystems behandelt werden.
- 2) Komponentenlevel – Sofern der Fehlerausschluss auf alle bekannten SCS-Fehler auf Komponentenlevel angewendet werden kann, kann der Fehlerausschluss für die gesamte Komponente gelten.

7.2.4 Mittlere Zeit bis zum gefahrbringenden Ausfall (MTTFd)

Siehe 4.5.2, ISO 13849-1:2015. Während ISO 13849-1 die grundlegende Annahme von 50 % für die Rate gefährlicher Ausfälle (z. B., $B10d = 2 \times B10$) empfiehlt, können niedrigere Ausfallraten angewandt werden, sofern sie durch Analysen (z. B. empirische Daten, FMEA) gestützt werden.

7.3 Diagnosedeckungsgrad (DC)

7.3.1 DC des ESCS

Siehe ISO 13849-1:2015, 4.5.3.

7.3.2 DC des N/ESCS

Der DC nicht elektrischer Systeme wird durch einen oder mehrere der folgenden Faktoren bestimmt:

- 1) Auswahl des geeignetsten analogen Typs des Diagnosedeckungsgrad-Wertes in ISO 13849-1:2015, Anhang E. Ein Wechselventil, das Öldruckwerte vergleicht und auf Grundlage dieser Druckwerte agiert ist zum Beispiel mit kontinuierlicher Überwachung vergleichbar, sodass ein Wert von 99 % zugeordnet werden kann.
- 2) Berechnung des DC-Prozentsatzes mithilfe einer FMEDA.
- 3) Fehlerausschluss kann für alle oder manche Fehler gelten. Falls dieser auf manche, jedoch nicht alle Fehler angewandt wird, müsste der entsprechende DC berechnet werden.
- 4) Direkte mechanische Verbindungen zwischen Komponenten können mit einem DC von 99 % betrachtet werden.

7.4 Fehlerausschlüsse auf Systemlevel bei hydraulischen Systemen, basierend auf der Robustheit des hydraulischen Systems (HSR)

Einen alternativen Ansatz zur Bewertung des MPLa bei aus Hydraulikkomponenten bestehenden N/ESCS stellt die Bewertung des Werts der Robustheit des hydraulischen Systems (HSR) für die Systemauslegung gemäß der in Tabelle 1 angegebenen Kriterien dar. Grundlage dieser Bewertung ist die Ausgereiftheit der Auslegung des hydraulischen Systems bezüglich Sicherheitsanwendungen an Erdbaumaschinen. Die Kriterien in Tabelle 1 basieren auf den grundlegenden Sicherheitsprinzipien, Fehlerausschlüssen und bewährten Sicherheitsprinzipien in ISO 13849-2:2012 sowie bewährten Vorgehensweisen zu Auslegung, Entwicklung und Herstellung hydraulischer SCS.

Der HSR-Wert wird mithilfe der folgenden Formel als Prozentsatz festgelegt:

$$HSR = \frac{Wert}{100 - Q} \times 100$$

Q ist der Gesamtwert der Kriterien, die die Sicherheit des zu bewertenden Systems nicht verbessern; (eine alternative Energiequelle wäre zum Beispiel kein anwendbares Kriterium für ein federbetätigtes, hydraulisch freigegebenes System, bei dem der sichere Zustand dem betätigten Zustand entspricht). Ein Kriterium, das das System nicht erfüllt, das jedoch das Risiko eines gefährbringenden Ausfalls des Systems verringern würde, darf nicht in Q einbezogen werden.

Jedes SRP/CS im auszuwertenden N/ESCS muss die Anforderungen der vorgegebenen Kriterien erfüllen, um einen Wert zu erhalten. Teilwerte sind nicht zulässig; (Falls zum Beispiel drei Spulen vorhanden sind, von denen nur zwei die Anforderungen eines vorgegebenen Kriteriums erfüllen, wäre der Wert für dieses Kriterium Null).

Die Anforderungen von ISO 13849-2:2012, C.1 und C.2 gelten für diese N/ESCS. Die Fehlerausschlüsse in ISO 13849-2:2012, C.3 können auf Komponentenlevel angewandt werden.

Tabelle 2 legt den maximalen MPLa fest, bei dem der Fehlerausschluss auf das N/ESCS, basierend auf dem HSR-Wert, angewandt werden kann.

Tabelle 1 — Bewertungskriterien für die Robustheit des hydraulischen Systems

Kriterien	Bewertung
Überdimensionierung (z. B. ausreichender Spulen-Freiraum, -Geradheit und -Zylindrizität)	+10
Gegenmaßnahmen für das Hängenbleiben oder Durchdrehen von Spulen	+10
Gegenmaßnahmen für störenden Hydraulikeingang (z. B. unmittelbarer Hochdruck an beiden Anschlüssen des Hydraulikmotors)	+10
Sekundäre Energiequelle (z. B. Steuerakku) oder ausfallsichere Auslegung bei Verlust der primären Energiequelle.	+20
Langsamer oder schrittweise voranschreitender Fehler (z. B. Verminderung der Lenkunterstützung vor dem erheblichen Fehler)	+10
Schlauchplatzsicherung (z. B. Verlegung zur Verhinderung scharfkantiger Verunreinigungen/Verschleiß)	+10
Systemauslegung zur Aufrechterhaltung der erforderlichen Sauberkeit der Hydraulikflüssigkeit	+10
Gegenmaßnahmen für Erosion durch Luftbeimischung in der Hydraulikflüssigkeit	+10
Gegenmaßnahmen für durch Luftbeimischung in der Hydraulikflüssigkeit verursachte Probleme bei der Druckübertragung (z. B. Entlüftungskreis)	+10

Tabelle 2 — Maximaler MPLa, bei dem der Fehlerausschluss auf das N/ESCS angewandt werden kann.

HSR-Wert	Maximaler Fehlerausschluss	
	MTTF _d = Mittel	MTTF _d = Hoch
≤ 80 %	MPL _a = b	MPL _a = c
> 80 %	MPL _a = c	MPL _a = d
ANMERKUNG 1 Die Definition der und der Prozess zur Festlegung der MTTF _d -Levels sind in ISO 13849-1 und ISO 13849-2 zu finden. ANMERKUNG 2 Die Miteinbeziehung der MTTF _d dient als Nachweis für SRP/CS, bei denen kein Fehlerausschluss auf Komponentenlevel erfolgen kann.		

7.5 Kategorie-Klassifikationen

7.5.1 Allgemeines

Der Konstrukteur muss die zur Einhaltung der Anforderungen an das System geeignete Architektur auswählen. Obwohl die Vielfalt möglicher Strukturen groß ist, sind die Basiskonzepte oft ähnlich. Daher können die meisten bestehenden Strukturen einer der in ISO 13849-1 beschriebenen Kategorien zugeordnet werden. Für jede Kategorie wird eine typische Ausführung in Form eines sicherheitsbezogenen Blockdiagramms angegeben. Diese typischen Umsetzungen werden als vorgesehene Architekturen bezeichnet und im Kontext jeder der folgenden Kategorien aufgelistet.

Manche SCS sind hochkomplex und stimmen nicht notwendigerweise exakt mit einer der vorgesehenen Architekturen überein. Auslegungen, die die Eigenschaften der jeweiligen Kategorie im Allgemeinen aufweisen, entsprechen der jeweiligen vorgesehenen Architektur dieser Kategorie. Die folgenden Bilder zeigen allgemeine Architekturen, keine spezifischen Beispiele. Eine Abweichung von diesen Architekturen ist jederzeit möglich, wobei jede Abweichung mithilfe geeigneter Analysewerkzeuge, die die Entsprechung des Systems mit dem erforderlichen Performance Level beweisen, begründet werden muss. Bei alternativen Architekturen muss die Hardware-Fehlertoleranz (HFT) und jede weitere Anforderung weiterhin der relevanten Kategorie entsprechen. Die vorgesehenen Architekturen müssen als Logikdiagramme und nicht als einfache Schaltpläne, betrachtet werden. Bei den Kategorien 3 und 4 bedeutet dies, dass nicht alle Teile zwangsläufig physikalisch redundant sind, aber redundante Mittel vorhanden sind, um sicherzustellen, dass ein Fehler nicht zu einem Verlust der Sicherheitsfunktion führen kann. (z. B. ein ECM mit paralleler Bearbeitung, Querüberwachung und externen Überwachungen würde der Kategorie 3 oder 4 zugeordnet werden).

Tabelle 3 liefert eine Übersicht der SCS-Kategorien, Anforderungen und dem Systemverhalten bei Fehlern. Die Verwendung bewährter Bauteile wird empfohlen. Ein bewährtes Bauteil für eine sicherheitsbezogene Anwendung muss ein Bauteil sein, das:

- a) in der Vergangenheit weithin erfolgreich in vergleichbaren Anwendungen eingesetzt wurde oder
- b) unter Verwendung von Prinzipien und Technologien hergestellt und verifiziert wurde, die seine Eignung und Zuverlässigkeit für sicherheitsbezogene Anwendungen nachweisen. Die verwendeten Auslegungs- und Verifizierungsaktivitäten sollten (sofern anwendbar) Folgendes umfassen:
 - Übereinstimmung mit der in diesem Dokument angegebenen Definition für bewährte Komponenten;
 - Prüfung der Belastbarkeit und Funktionalität mithilfe einer Prüfbank;
 - Belastungsprüfungen zu einem angemessenen Sicherheitsfaktor;
 - beschleunigte Haltbarkeitsprüfung;
 - Computergestützte Analyse und Studien zu physikalischen Zusammenhängen;
 - Umweltprüfungen nach ISO 19014-3;
 - Unterstützt die erforderliche $MTTF_d$.

MCS, die eine Sicherheitsfunktion des SCS beeinflussen oder stummschalten, muss der gleiche Performance Level wie dem SCS zugeordnet werden, sofern nicht gezeigt werden kann, dass nach ISO 19014-1 oder ISO/TS 19014-5 MPLr ein anderer MPLr erforderlich ist.

Tabelle 3 — Zusammenfassung der Kategorie-Anforderungen

Kategorie	Systemverhalten	$MTTF_d$	DC	CCF Eval	HFT
B	Das Auftreten eines Fehlers kann zum Verlust der Sicherheitsfunktion führen.	niedrig bis mittel	keine	NA	0
1	Das Auftreten eines Fehlers kann zum Verlust der Sicherheitsfunktion führen. Das sichere Betriebsverhalten der Maschine liegt über den Anforderungen an ein System der Kategorie B.	hoch	keine	NA	0

Kategorie	Systemverhalten	MTTF _d	DC	CCF Eval	HFT
2	Das Auftreten eines Fehlers kann zum Verlust der Sicherheitsfunktion führen, es wird jedoch eine Maßnahme zur Minderung des mit dem Fehler verbundenen Risikos ergriffen. Fehler an den Eingangs- und Ausgangsgeräten werden angemessen und wie praktisch möglich bei oder vor dem nächsten Abruf der Sicherheitsfunktion erkannt.	niedrig	niedrig bis mittel	erforderlich ^a	0
3	Wenn ein Einzelfehler auftritt, wird die Sicherheitsfunktion stets ausgeführt, jedoch kann eine Anhäufung unerkannter Fehler zum Verlust der Sicherheitsfunktion führen. Manche Fehler an den Eingangs-, Logik- und Ausgangsgeräten werden während oder vor dem nächsten Abruf der Sicherheitsfunktion erkannt. Warnung der Bedienungsperson ist erforderlich.	niedrig bis hoch	niedrig bis mittel	erforderlich	1
4	Wenn ein Einzelfehler auftritt, wird die Sicherheitsfunktion stets ausgeführt, jedoch kann eine Anhäufung unerkannter Fehler zum Verlust der Sicherheitsfunktion führen. Das sichere Betriebsverhalten der Maschine liegt über den Anforderungen an ein System der Kategorie 3. Alle Fehler an den Eingangs-, Logik- und Ausgangsgeräten werden während oder vor dem nächsten Abruf der Sicherheitsfunktion erkannt oder die Fehleransammlung kann nicht zum Verlust der Sicherheitsfunktion führen. Warnung der Bedienungsperson ist erforderlich.	hoch	hoch	erforderlich	1
^a Eine Architektur der Kategorie 2 könnte gegenüber einem CCF empfindlich sein					

Hinsichtlich der in der unteren Tabelle 4 beschriebenen vorgesehenen Architekturen bestehen folgende Annahmen:

- Gebrauchsdauer, 20 Jahre;
- konstante Ausfallraten innerhalb der Gebrauchsdauer;
- bei Kategorie 2, Anforderungsrate $\leq 1/100$ Testrate (siehe auch Anmerkung in ISO 13849-1:2015, Anhang K); oder der Prüfung findet direkt bei Aufruf der Sicherheitsfunktion statt und die Gesamtzeit, die benötigt wird, um den Fehler zu erkennen und die Maschine in einen ungefährlichen Zustand zu bringen (normalerweise Maschinenstopp), ist kürzer als die zum Erreichen der Gefährdung benötigte Zeit;
- bei Kategorie 2, $MTTF_{d,TE} > MTTF_{d,L}/2$.

Tabelle 4 — Kategorien für verschiedene Energietypen

Kategorie	Mechanisch	Pneumatisch	Hydraulisch	Elektronisch	Elektrisch
1	✓	✓	✓	✓	✓
2	N/A	✓	✓	✓	N/A
3	P/A	P/A	P/A	✓	P/A
4	P/A	P/A	P/A	✓	P/A
N/A – Nicht anwendbar P/A – Parallele Hinzufügung (en: parallel add) ✓ – Anwendbar					

ANMERKUNG Für weitere Informationen zur parallelen Hinzufügung, siehe 7.6.2 und Beispiele in Anhang A.

7.5.2 Kategorie 1

7.5.2.1 Erklärung zur Anwendung der Kategorie 1 für N/ESCS

Die meisten hydraulischen und pneumatischen Ventile und mechanischen Verbindungen haben Architekturen der Kategorie 1. Im Falle von hydraulischen Ventilen werden die Eingangs-, Logik- und Ausgangsfunktion intrinsisch in der Auslegung mit Feder und Spule innerhalb des Ventils umgesetzt. Diese kann als Eingangs-, Logik- und Ausgangskomponenten in Einem angesehen werden. Diese Systeme sind insofern analog zu ihren elektrischen Gegenstücken, als dass sie dieselbe Funktion erfüllen können, aber einen anderen Energietyp zur Signalübertragung verwenden.

ANMERKUNG Eine Art, die Grenzen von Eingang, Logik und Ausgang innerhalb eines Systems festzulegen besteht darin, zu betrachten, wo sich der Energietyp in der Signalverarbeitung ändert.

Im Folgenden eine nicht inklusive Liste mit Beispielen;

- Eine Bedienungsperson drückt ein Pedal herunter – die Energie verändert sich von kinetisch zu hydraulisch.
- Eine Bedienungsperson drückt ein Pedal herunter – die Energie verändert sich von kinetisch zu elektrisch. Das Signal bleibt durch die Komponenten I - L hindurch elektrisch und wird dann in hydraulischen Druck umgewandelt.
- Ein vorgesteuertes hydraulisches System ist a) sehr ähnlich. Das Steuersignal ist jedoch nicht elektrisch, sondern besteht in niedrigem Hydraulikdruck. Am Ausgang entsteht Hochdruck-Hydraulikenergie.

7.5.2.2 Anwendungsbeispiele für Kategorie 1

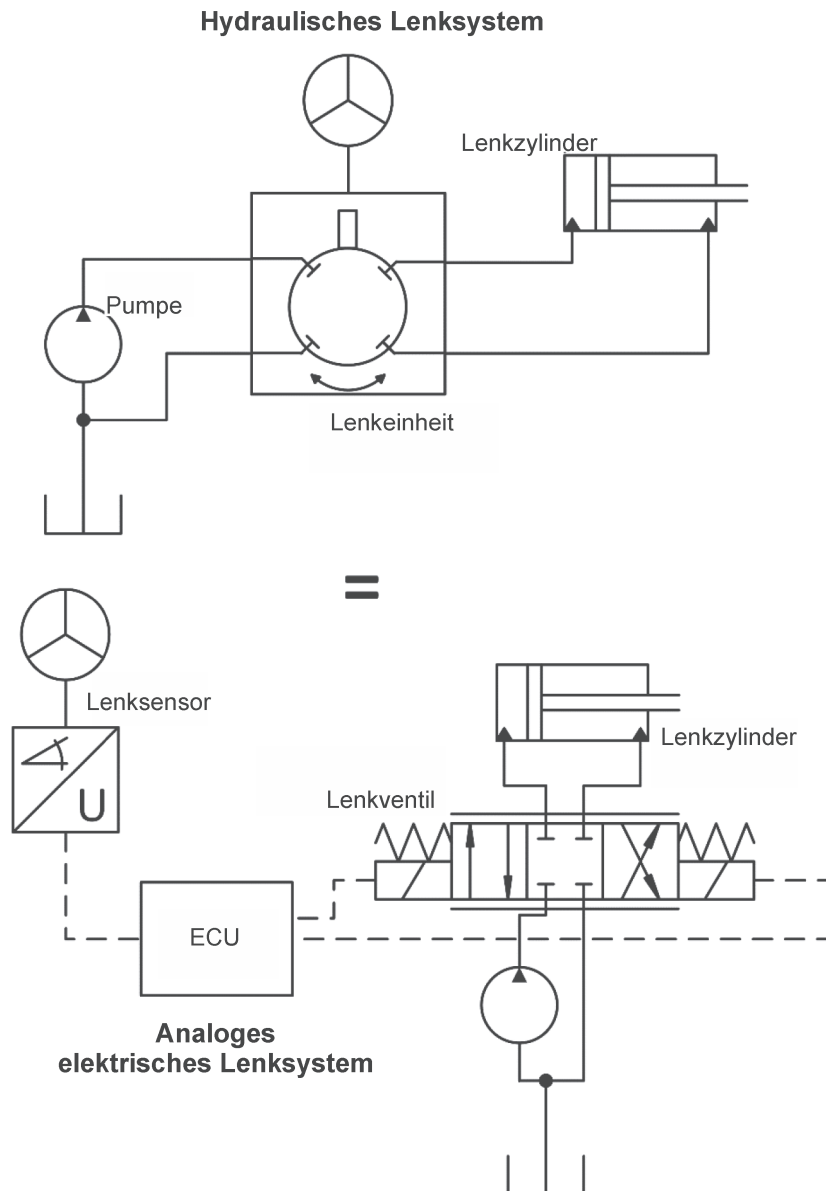


Bild 3 — Beispiel für zwei analoge Steuerungssysteme der Kategorie 1 mit verschiedenen Energietypen

ANMERKUNG Elektronische Systeme entscheiden für gewöhnlich darüber, wie die Eingangsleistung geleitet wird und steuern die Ausgangsleistung auf dieser Basis. Bei N/ESCS wird die Ausgangsleistung durch die ILO-Komponenten geleitet und dann wird die Energie entweder zurück zum Tank gesendet oder für die Steuerung der Maschine verwendet.

7.5.3 Kategorie 2

7.5.3.1 Allgemeines

Die Richtlinie aus 6.2.5 in ISO 13849-1:2015 gilt mit den in diesem Abschnitt dargelegten Ausnahmen und Erläuterungen.

- Wenn eine Risikobeurteilung ergeben hat, dass der Bedienungsperson genug Zeit für eine Reaktion bleibt, kann eine Warnanzeige für Sofortmaßnahmen als OTE in einem $MPL_r = d$ SCS verwendet werden;

ANMERKUNG Oft kann die Bedienungsperson besser als die SCS einschätzen, welche Reaktion zur Minderung der Gefährdung geeignet ist.

- der OTE muss die Maschine innerhalb eines annehmbaren Zeitraums in einen sicheren Zustand versetzen können. Der sichere Zustand muss die Gefährdung mindern, die die Sicherheitsfunktion adressiert;
- wenn 2 oder mehr Komponenten innerhalb eines Funktionsblocks parallel (ILO) sind und für den Verlust der Sicherheitsfunktion ein Fehler an mehr als einer Komponente erforderlich ist, kann dieser Block als eine Funktion der Kategorie 3 betrachtet werden (siehe 7.6 für parallele Hinzufügung)

7.5.3.2 Erklärung zur Anwendung der Kategorie 2 für N/ESCS (Mechanisch)

Die Anwendung einer Architektur der Kategorie 2 auf N/ESCS folgt den Prinzipien und Anforderungen einer Architektur der Kategorie 2, sieht aber aufgrund der verschiedenen Komponententypen etwas anders aus.

Hydraulische Systeme bestehen normalerweise aus einem System der Kategorie 1 mit hinzugefügtem TE und OTE, um jegliche Ausfälle der ILO-Komponente zu adressieren. Da die Ausfallarten bei diesen Komponententypen wohlbekannt sind und ihre Zuverlässigkeit nachgewiesen ist, können auf die meisten Ausfallarten Fehlerausschlüsse angewandt werden. Im Gegensatz zu elektronischen Systemen der Kategorie 2, überwachen der TE und OTE von hydraulischen Systemen der Kategorie 2 die ILO-Komponenten nicht direkt hinsichtlich Fehlern, sondern überwachen die Fähigkeit des Systems, seine Funktion zu erfüllen.

ANMERKUNG Eine typische Ausfallart, auf die kein Fehlerausschluss angewendet werden kann, ist ein Mangel an Öl. Die Ölversorgung wird für gewöhnlich von einem elektronischem System, einem Wechselventil oder ähnlichem, überwacht und, falls die primäre Ölquelle unterbrochen wird, von einem Akkumulator oder einer Ersatzpumpe übernommen.

Ähnlich wie das Beispiel zu Kategorie 1, ist dieses System komplett analog zu einem elektrischen System, das die gleichen Funktionen erfüllt.

ANMERKUNG Dies ist ein Beispiel für ein „bei Ausfall betriebsfähiges“ System. Der sichere Zustand besteht darin, die Lenkfähigkeit über die sekundäre Ölversorgung aufrechtzuerhalten; auf alle anderen Fehler im Hinblick auf die betroffenen Blöcke wird der Fehlerausschluss angewendet. In diesem Fall wurden die Ölversorgung und die Lenksteuerung zu einer einzigen Sicherheitsfunktion kombiniert.

7.5.3.3 Beispiel für ein hydraulisches System der Kategorie 2

Hydraulisches Lenksystem der Kategorie 2

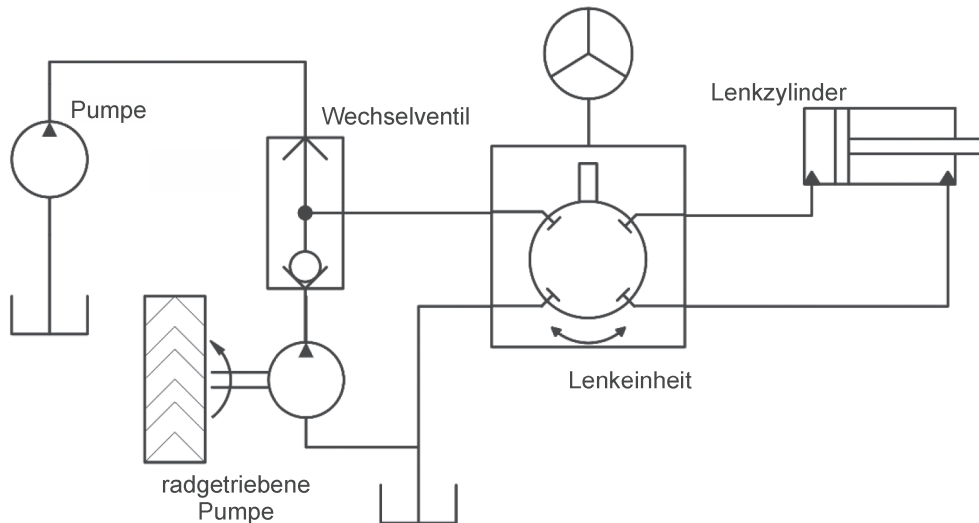


Bild 4 — Beispiel für ein hydraulisches System der Kategorie 2

Blockdiagramm des hydraulischen Lenksystems der Kategorie 2

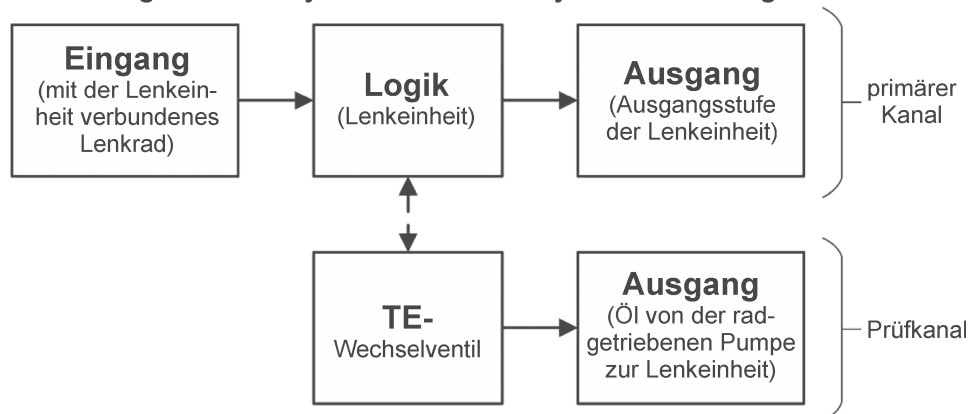


Bild 5 — Beispiel für ein Blockdiagramm eines hydraulischen Systems

ANMERKUNG 1 Der Text in Klammern betrifft Systemeigenschaften außerhalb des SRP/CS.

ANMERKUNG 2 Die Begriffe „Kugel-Koordinatenwandler“ und „Wechselventil“ sind austauschbar.

7.5.4 Richtlinie zu in Konflikt stehenden Sicherheitsfunktionen

Im Fall von zueinander in Konflikt stehenden Sicherheitsfunktionen, müssen die sicheren Zustände für manche selbstständigen Anwendungen gegen Funktionen bei Ausfall nach Aufforderung beachtet werden. Wenn dies der Fall ist, erfordern beide Ausfallarten einen MPLr und müssen ihre eigenen Sicherheitsfunktionen haben. Eine der Sicherheitsfunktionen wird vermutlich einen niedrigeren MPLr haben als die andere und der sichere Zustand der Maschine entspricht eventuell dem sicheren Zustand gemäß dem höchsten MPLr.

Ein Beispiel hierfür ist ein Bremssystem an einer Hochgeschwindigkeits-Maschine, an der sowohl die selbstständige Anwendung als auch der Ausfall bei Abruf der Bremse Sicherheitsfunktionen darstellen. Während für den Ausfall bei Abruf des Bremssystems ein höherer MPLr gilt, kann die selbstständige Anwendung der Bremse ebenfalls gefährlich sein.

Da der Ausfall bei Abruf gefährlicher ist, besteht der sicherste Zustand darin, die Maschine zum Stillstand zu bringen. Der sichere Zustand der Sicherheitsfunktion bei selbstständiger Aktivierung kann darin bestehen, die Maschine ohne einen Befehl der Bedienungsperson, sondern über den Prüfkanal anzuhalten; es sollte jedoch betrachtet werden, wie die SCS die Maschine zum Stillstand bringt (d.h. Auf eine Weise, die die Gefährdung durch unkontrolliertes Schleudern mindert).

ANMERKUNG Bei bei einem Ausfall betriebsfähigen Systemen kann es sich um gegensätzliche Sicherheitsfunktionen handeln.

Falls der MLPR der gegensätzlichen Sicherheitsfunktion gleich ist, kann eine Architektur der Kategorie 3 verwendet werden.

7.5.5 Überlegungen zu den SRP/CS von bei einem Ausfall betriebsfähigen Systemen

Systeme der Kategorie 2 können für bei einem Ausfall betriebsfähige SCS verwendet werden, sofern die Ansprechzeit der Fehlerreaktion einer angemessenen Risikobewertung unterzogen wurde (d.h. dem in der entsprechenden Typ-C-Norm dargelegten Performance Level entspricht) und unter der Anforderungsrate liegt.

Systeme der Kategorie 3, die für bei einem Ausfall betriebsfähige Anwendungen verwendet werden, können als komplett redundante Systeme arbeiten. In Fällen, in denen ein Einzelfehler zu gegensätzlichen Ausgängen führen könnte, kann die redundante Verarbeitung der Sicherheitsfunktion mit Umschaltfunktion zwischen den primären und sekundären Kanälen, abhängig vom Fehlzustand der jeweiligen Kanäle, verwendet werden.

ANMERKUNG Wenn eine solche Umschaltfunktion verwendet wird, verursacht die Senkung der Prüffrequenz keine Senkung des Diagnosedeckungsgrads, da der sekundäre Kanal nicht kontinuierlich betriebsfähig ist.

Ein Beispiel für eine SCS mit kontinuierlicher Anforderung ist ein elektro-hydraulisches Lenksystem.

7.6 Kombination von SCS zur Erreichung eines Gesamt-MPL

Folgendes kann genutzt werden, um Systeme parallel zu kombinieren; dies kann für die Bewertung von Architekturen nützlich sein, die den für die Kategorien 1-4 dargelegten nicht entsprechen. Siehe 6.3, ISO 13849-1:2015 für die Kombination von Systemen in Reihe.

Diese Architekturreduzierung gilt für qualitative Anforderungen; quantitative Anforderungen (z. B., $MTTF_d$, DC, CCF) müssen separat verifiziert werden. Zwischen den kombinierten Elementen darf es keine Ausfälle aufgrund gemeinsamer Ursache geben.

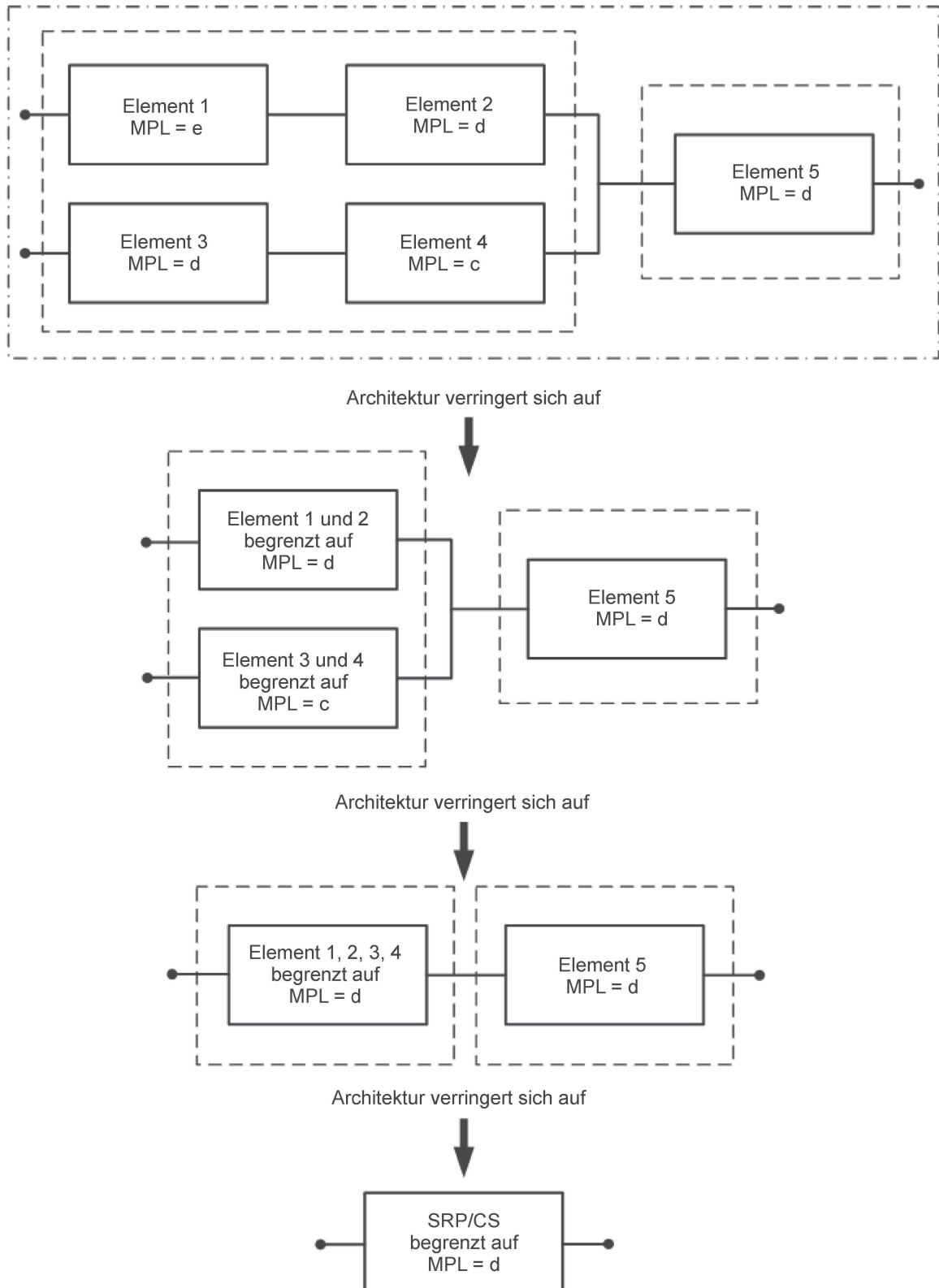


Bild 6 — Beispiel für die Reduktion eines parallelen kombinierten MPL_a in Reihe

Alternativ zur parallelen Hinzufügung von Komponenten können zwei parallele $HFT = 0$ Kanäle (Kategorie B, 1, 2) als ein System der Kategorie 3 betrachtet werden. Die Aktivierungsmaßnahme für die beiden Kanäle durch die Bedienungsperson muss der Anforderung von AR3 in 6.5, ISO 19014-1:2018 entsprechen; aufgrund der natürlichen Reaktion der Bedienungsperson ist dies jedoch nur erforderlich, sofern die beiden Kanäle tatsächlich redundant sind. Trotz der fehlenden Querüberwachung zwischen den beiden Kanälen, wird $HFT = 1$ aufrechterhalten.

Dieser Prozess ist auch für parallele, redundante Elemente in Funktionsblöcken innerhalb der Kategorien relevant, wenn diese in Reihe hinzugefügt werden. Die derartige Berücksichtigung der Blöcke kann die hinzugefügte Sicherheitsmarge erfassen und anerkennen, eine Betrachtung der Blöcke als nicht-redundante Komponenten, oder das Weglassen eines Blocks bei der Berechnung jedoch nicht.

8 Informationen für Gebrauch und Instandhaltung

ISO 6750 legt die Anforderungen an den Inhalt von Gebrauchs- und Instandhaltungshandbüchern fest. Zusätzlich können die folgenden Informationen zur funktionalen Sicherheit der EMM, die diesem Standard entsprechen, geteilt werden. Diese Informationen könnten dem Handbuch oder einer anderen Dokumentation, die der Endnutzer erhält, hinzugefügt werden.

- Eine Auflistung der Sicherheitsfunktionen auf der Maschine;
- eine Liste der sicherheitsbezogenen Teile des Steuerungssystems; besonders falls Änderungen an diesen Teilen die Konformität der funktionalen Sicherheit der Maschine ungültig machen;
- sämtliche Instandhaltungs-, Prüfungs- oder Inspektionsaktivitäten, die zur Aufrechterhaltung der Integrität der SCS über den Lebenszyklus der Maschine notwendig sind.

Es ist nicht erforderlich, den MPL oder die Kategorie zu nennen, wenn diese Systeme als eine vollständige, in die Maschine integrierte SCS zur Verfügung gestellt werden.

Anhang A (informativ)

Beispielsysteme und Bewertungen

Die Beispiele in diesem Anhang sollen dazu dienen, die Berechnung des erreichten Performance Levels der Maschine (MPLa) einer bestehenden SCS zu veranschaulichen. Diese Beispiele beginnen relativ einfach und werden zunehmend komplexer. Diese Beispiele umfassen rein hydraulische SCS-Komponenten bis Komponenten elektrohydraulischer SCS.

Tabelle A.1 — Beispiele für die Berechnung des MPL_a sind in Anhang A zu finden.

MPLa	Kategorie	Hydraulisch/ Hydraulisch	Elektrisch/ Hydraulisch	Elektro- hydraulisch	Parallele Hinzufügung
b	B			A.1 Lenkung	
c	1	A.2 Lenkung	A.3 Feststell- bremse		
c	2			A.4 Lenkung mit automatischer Feststellbremse	
d	2	A.5 Lenkung			
d	3			A.6 Bremsung	X

Beispiel A.1 Elektro-hydraulische Lenkung, Kategorie B

Gefährdungsereignis: Ausfall der Lenkung bei Abruf

Sicherer Zustand: N/A, Kategorie B verfügt über keine Fehlerreaktion

Sicherheitsfunktion: Lenkung wie befohlen

Ausfall (auslösendes Ereignis) bei Verwendung von Prüfgeräten (TE): N/A, Kategorie B verfügt über keinen Prüfkanal

Reaktionen auf einen Fehler (OTE): N/A – Kategorie B verfügt über keinen Prüfkanal