

## DIN EN ISO 19014-2



ICS 53.100

**Entwurf**

Einsprüche bis 2024-04-23  
Vorgesehen als Ersatz für  
DIN EN ISO 19014-2:2022-11

**Erdbaumaschinen –  
Funktionale Sicherheit –  
Teil 2: Entwurf und Bewertung von Hardware- und  
Architekturanforderungen für sicherheitsrelevante Teile des  
Steuerungssystems (ISO/DIS 19014-2:2024);  
Deutsche und Englische Fassung prEN ISO 19014-2:2024**

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 19014-2:2024);

German and English version prEN ISO 19014-2:2024

Engins de terrassement –

Sécurité fonctionnelle –

Partie 2: Conception et évaluation des exigences de matériel et d'architecture pour les parties relatives à la sécurité du système de commande (ISO/DIS 19014-2:2024);

Version allemande et anglaise prEN ISO 19014-2:2024

**Anwendungswarnvermerk**

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

Weil das beabsichtigte Dokument von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter [www.din.de/go/entwuerfe](http://www.din.de/go/entwuerfe) bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter [www.entwuerfe.normenbibliothek.de](http://www.entwuerfe.normenbibliothek.de), sofern dort wiedergegeben;
- oder als Datei per E-Mail an [nam@vdma.org](mailto:nam@vdma.org) möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter [www.din.de/go/stellungnahmen-norm-entwuerfe](http://www.din.de/go/stellungnahmen-norm-entwuerfe) oder für Stellungnahmen zu Norm-Entwürfen der DKE unter [www.dke.de/stellungnahme](http://www.dke.de/stellungnahme) abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Maschinenbau (NAM), 60498 Frankfurt am Main, Postfach 71 08 64 oder Lyoner Str. 18, 60528 Frankfurt am Main.

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

Gesamtumfang 112 Seiten

DIN-Normenausschuss Maschinenbau (NAM)

## Nationales Vorwort

Dieser Norm-Entwurf enthält sicherheitstechnische Festlegungen.

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 wurden vom Ausschuss 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.

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

|                  |       |                            |
|------------------|-------|----------------------------|
| ISO 6165:2012    | siehe | DIN EN ISO 6165:2013-02*   |
| ISO 12100:2010   | siehe | DIN EN ISO 12100:2011-03** |
| ISO 13849-1:2023 | siehe | DIN EN ISO 13849-1:2023-12 |
| ISO 13849-2:2012 | siehe | DIN EN ISO 13849-2:2013-02 |
| ISO 19014-1:202X | siehe | DIN EN ISO 19014-1:202X    |
| ISO 19014-3:202X | siehe | DIN EN ISO 19014-3:202X    |
| ISO 19014-4:202X | siehe | DIN EN ISO 19014-4:202X    |

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

## Änderungen

Gegenüber DIN EN ISO 19014-2:2022-11 wurden folgende Änderungen vorgenommen:

- a) ausführlicher Anhang ZA hinzugefügt;
- b) Bezugsnormen datiert;
- c) Korrektur von Anhang D, MPL-Fehler und Korrektur der Satzfehler „MPLa“ und „MPL.“ in Bild D.1;
- d) 7.3.1, Diagnosedeckungsgrad, geändert.

---

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

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

## Nationaler Anhang NA (informativ)

### Literaturhinweise

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

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

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

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

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

DIN EN ISO 19014-3:202X, *Erdbaumaschinen — Funktionale Sicherheit — Teil 3: Umweltanforderungen und Prüfanforderungen von elektronischen und elektrischen Komponenten des sicherheitsrelevanten Steuerungssystems (ISO 19014-3:202X); Deutsche Fassung EN ISO 19014-3:202X*

DIN EN ISO 19014-4:202X, *Erdbaumaschinen — Funktionale Sicherheit — Teil 4: Gestaltung und Beurteilung von Software und Datenübertragung für sicherheitsrelevante Steuerungssysteme (ISO 19014-4:202X); Deutsche Fassung EN ISO 19014-4:202X*

– Leerseite –

Januar 2024

**prEN ISO 19014-2**

**Erdbaumaschinen – Funktionale Sicherheit – Teil 2: Entwurf und Bewertung von Hardware- und Architekturanforderungen für sicherheitsrelevante Teile des Steuerungssystems (ISO/DIS 19014-2:2024)**

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 19014-2:2024)

Engins de terrassement – Sécurité fonctionnelle – Partie 2: Conception et évaluation des exigences de matériel et d'architecture pour les parties relatives à la sécurité du système de commande (ISO/DIS 19014-2:2024)

## Inhalt

|                                                                                                                                                                | Seite |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| Europäisches Vorwort . . . . .                                                                                                                                 | 5     |
| Anhang ZA (informativ) Zusammenhang zwischen dieser Europäischen Norm und den<br>grundlegenden Anforderungen der abzudeckenden Richtlinie 2006/42/EG . . . . . | 6     |
| Vorwort . . . . .                                                                                                                                              | 7     |
| Einleitung . . . . .                                                                                                                                           | 9     |
| 1 Anwendungsbereich . . . . .                                                                                                                                  | 10    |
| 2 Normative Verweisungen . . . . .                                                                                                                             | 10    |
| 3 Begriffe . . . . .                                                                                                                                           | 11    |
| 4 Symbole und Abkürzungen . . . . .                                                                                                                            | 11    |
| 5 Allgemeine Anforderungen . . . . .                                                                                                                           | 12    |
| 5.1 Anwendung . . . . .                                                                                                                                        | 12    |
| 5.2 Bestehende SCS . . . . .                                                                                                                                   | 13    |
| 6 Systementwurf . . . . .                                                                                                                                      | 13    |
| 6.1 Überblick . . . . .                                                                                                                                        | 13    |
| 6.2 Allgemeine Anforderungen . . . . .                                                                                                                         | 13    |
| 6.3 Gestaltung der Hardware . . . . .                                                                                                                          | 14    |
| 7 Bewertung der Sicherheitsleistung des Systems . . . . .                                                                                                      | 15    |
| 7.1 Erreichtes Performance Level der Maschine (MPL <sub>a</sub> ) . . . . .                                                                                    | 15    |
| 7.2 Hardware-Sicherheitsbewertung . . . . .                                                                                                                    | 16    |
| 7.2.1 Allgemeines . . . . .                                                                                                                                    | 16    |
| 7.2.2 Fehlerberücksichtigung . . . . .                                                                                                                         | 16    |
| 7.2.3 Fehlerausschluss . . . . .                                                                                                                               | 16    |
| 7.2.4 Mittlere Zeit bis zum gefahrbringenden Ausfall (MTTF <sub>d</sub> ) . . . . .                                                                            | 17    |
| 7.3 Diagnosedeckungsgrad (DC) . . . . .                                                                                                                        | 17    |
| 7.3.1 DC des ESCS . . . . .                                                                                                                                    | 17    |
| 7.3.2 DC des N/ESCS . . . . .                                                                                                                                  | 17    |
| 7.4 Fehlerausschlüsse auf Systemlevel bei hydraulischen Systemen, basierend auf der<br>Robustheit des hydraulischen Systems (HSR) . . . . .                    | 17    |
| 7.4.1 Allgemeines . . . . .                                                                                                                                    | 17    |
| 7.4.2 Berechnung des HSR-Werts . . . . .                                                                                                                       | 18    |
| 7.5 Kategorie-Klassifikationen . . . . .                                                                                                                       | 19    |
| 7.5.1 Allgemeines . . . . .                                                                                                                                    | 19    |
| 7.5.2 Kategorie B/Kategorie 1 . . . . .                                                                                                                        | 23    |
| 7.5.3 Kategorie 2 . . . . .                                                                                                                                    | 25    |
| 7.5.4 Richtlinie zu in Konflikt stehenden Sicherheitsfunktionen . . . . .                                                                                      | 26    |
| 7.5.5 Überlegungen zu den SRP/CS von bei einem Ausfall betriebsfähigen Systemen . . . . .                                                                      | 27    |
| 7.6 Kombination von SCS zur Erreichung eines Gesamt-MPL . . . . .                                                                                              | 27    |
| 8 Informationen für Gebrauch und Instandhaltung . . . . .                                                                                                      | 29    |
| 8.1 Allgemeines . . . . .                                                                                                                                      | 29    |
| 8.2 Benutzerhandbuch . . . . .                                                                                                                                 | 29    |
| Anhang A (informativ) Beispielsysteme und Bewertungen . . . . .                                                                                                | 30    |
| A.1 Allgemeines . . . . .                                                                                                                                      | 30    |
| A.2 Beispiel 1 — Elektro-hydraulische Lenkung, Kategorie B . . . . .                                                                                           | 30    |
| A.3 Beispiel 2 — Hydraulisch-hydraulische Lenkung, Kategorie 1 . . . . .                                                                                       | 32    |
| A.4 Beispiel 3 — Elektrisch-hydraulische Feststellbremse, Kategorie 1 . . . . .                                                                                | 34    |
| A.5 Beispiel 4 — Elektro-hydraulische Lenkung mit automatischer Feststellbremse,<br>Kategorie 2 . . . . .                                                      | 35    |
| A.6 Beispiel 5 — Hydraulisches Lenksystem, Kategorie 2M . . . . .                                                                                              | 40    |
| A.7 Beispiel 6 — Elektro-hydraulische Betriebsbremse, Kategorie 3 . . . . .                                                                                    | 43    |
| Anhang B (informativ) Beispiele für Auswertungen mithilfe der HSR-Bewertung . . . . .                                                                          | 47    |
| B.1 Hydraulischer Lenkkreis eines Radladers . . . . .                                                                                                          | 47    |

|                       |                                                                                                    |    |
|-----------------------|----------------------------------------------------------------------------------------------------|----|
| B.2                   | Beispiel für die Berechnung der HSR-Bewertung für eine federbetätigte hydraulische Feststellbremse | 49 |
| Anhang C (normativ)   | Kompatibilität mit anderen funktionalen Sicherheitsnormen                                          | 52 |
| Anhang D (informativ) | Bewertung der Sicherheitsfunktion                                                                  | 53 |
| Anhang E (normativ)   | Ausnahmen, Ausschlüsse, Ergänzungen zu ISO 13849-1 und ISO 13849-2                                 | 55 |
| Literaturhinweise     |                                                                                                    | 58 |

## Bilder

|           |                                                                                                                                                                                   |    |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| Bild 1    | V-Modell der Hardwareentwicklung                                                                                                                                                  | 15 |
| Bild 2    | Beispiel für zwei analoge Lenksysteme der Kategorien B/Kategorie 1 unterschiedlicher Technologien: hydraulisches Lenksystem (oben) und analoges elektronisches Lenksystem (unten) | 24 |
| Bild 3    | Beispiel für ein hydraulisches Lenksystem der Kategorie 2M                                                                                                                        | 26 |
| Bild 4    | Beispiel für ein Blockdiagramm eines hydraulischen Systems                                                                                                                        | 26 |
| Bild 5    | Beispiel für die Reduktion eines parallel kombinierten $MPL_a$ in Reihe                                                                                                           | 28 |
| Bild A.1  | Schema einer elektro-hydraulischen Lenkung, Kategorie B                                                                                                                           | 31 |
| Bild A.2  | Logikdiagramm einer elektro-hydraulischen Lenkung, Kategorie B                                                                                                                    | 31 |
| Bild A.3  | Schema einer hydraulisch-hydraulischen Lenkung, Kategorie 1                                                                                                                       | 33 |
| Bild A.4  | Logikdiagramm einer hydraulisch-hydraulischen Lenkung, Kategorie 1                                                                                                                | 33 |
| Bild A.5  | Schema einer elektrisch-hydraulischen Feststellbremse, Kategorie 1                                                                                                                | 34 |
| Bild A.6  | Logikdiagramm einer elektrisch-hydraulischen Feststellbremse, Kategorie 1                                                                                                         | 35 |
| Bild A.7  | Schema für eine elektro-hydraulische Lenkung mit automatischer Feststellbremse, Kategorie 2                                                                                       | 36 |
| Bild A.8  | Logikdiagramm einer elektro-hydraulischen Lenkung mit automatischer Feststellbremse, Kategorie 2                                                                                  | 37 |
| Bild A.9  | Schema eines hydraulischen Lenksystems, Kategorie 2M                                                                                                                              | 41 |
| Bild A.10 | Logikdiagramm eines elektro-hydraulischen Lenksystems, Kategorie 2M                                                                                                               | 42 |
| Bild A.11 | Schema einer elektro-hydraulischen Betriebsbremse, Kategorie 3                                                                                                                    | 44 |
| Bild A.12 | Logikdiagramm einer elektro-hydraulischen Betriebsbremse Kategorie 3                                                                                                              | 46 |
| Bild B.1  | Schema eines hydraulischen Lenkkreises                                                                                                                                            | 48 |
| Bild D.1  | Bewertung der Sicherheitsfunktion                                                                                                                                                 | 54 |

## Tabellen

|              |                                                                                          |    |
|--------------|------------------------------------------------------------------------------------------|----|
| Tabelle ZA.1 | Übereinstimmung zwischen dieser Europäischen Norm und Anhang I der Richtlinie 2006/42/EG | 6  |
| Tabelle 1    | Bewertungskriterien für die Robustheit des hydraulischen Systems                         | 18 |
| Tabelle 2    | Korrelation zwischen HSR und DC zur Bestimmung des $MPL_a$                               | 19 |
| Tabelle 3    | Zusammenfassung der Kategorie-Anforderungen                                              | 20 |
| Tabelle 4    | Kategorien für verschiedene Technologien                                                 | 23 |
| Tabelle A.1  | In diesem Anhang dargestellte Beispiele für die Berechnung des $MPL_a$                   | 30 |
| Tabelle A.2  | Beispiel für eine $MTTF_d$ -Berechnung mithilfe der Teile-Zählmethode                    | 32 |
| Tabelle A.3  | $MTTF_d$ -Berechnung für eine hydraulisch-hydraulische Lenkung, Kategorie 1              | 33 |
| Tabelle A.4  | Beispiel für eine $MTTF_d$ -Berechnung mithilfe der Teile-Zählmethode                    | 35 |
| Tabelle A.5  | Beispiel für eine $MTTF_d$ -Berechnung mithilfe der Teile-Zählmethode für den Hauptkanal | 37 |
| Tabelle A.6  | Beispiel für eine $MTTF_d$ -Berechnung mithilfe der Teile-Zählmethode für den Prüfkanal  | 37 |
| Tabelle A.7  | Bewertung von Ausfällen infolge gemeinsamer Ursache                                      | 38 |
| Tabelle A.8  | Berechnung des $DC_{avg}$ für das System                                                 | 39 |
| Tabelle A.9  | Beispiel für eine $MTTF_d$ -Berechnung mithilfe der Teile-Zählmethode für den Hauptkanal | 42 |

|                                                                                                                                 |           |
|---------------------------------------------------------------------------------------------------------------------------------|-----------|
| <b>Tabelle A.10 — Beispiel für eine MTTF<sub>d</sub>-Berechnung mithilfe der Teile-Zählmethode für den Prüfkanal . . . . .</b>  | <b>42</b> |
| <b>Tabelle A.11 — Beispiel für eine MTTF<sub>d</sub>-Berechnung mithilfe der Teile-Zählmethode . . . . .</b>                    | <b>44</b> |
| <b>Tabelle A.12 — Beispiel für eine MTTF<sub>d</sub>-Berechnung mithilfe der Teile-Zählmethode . . . . .</b>                    | <b>45</b> |
| <b>Tabelle B.1 — HSR-Bewertung für einen hydraulischen Lenkkreis . . . . .</b>                                                  | <b>48</b> |
| <b>Tabelle B.2 — Beispiel für Kriterien für die HSR-Bewertung einer federbetätigten hydraulischen Feststellbremse . . . . .</b> | <b>50</b> |
| <b>Tabelle C.1 — MPL<sub>r</sub> im Vergleich zu Parametern aus anderen Normen . . . . .</b>                                    | <b>52</b> |
| <b>Tabelle E.1 — Vergleich für den Vorrang zwischen ISO 13849-1:2015 und der Normenreihe ISO 19014 . . . . .</b>                | <b>55</b> |
| <b>Tabelle E.2 — Vergleich für den Vorrang zwischen ISO 13849-2:2012 und der Normenreihe ISO 19014 . . . . .</b>                | <b>57</b> |

## Europäisches Vorwort

Dieses Dokument (prEN ISO 19014-2:2024) wurde vom Technischen Komitee ISO/TC 127 „Earth-moving machinery“ in Zusammenarbeit mit dem Technischen Komitee CEN/TC 151 „Bau- und Baustoffmaschinen — Sicherheit“ erarbeitet, dessen Sekretariat von DIN gehalten wird.

Dieses Dokument ist derzeit zur parallelen Umfrage vorgelegt.

Dieses Dokument wird EN ISO 19014-2:2022 ersetzen.

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

### Anerkennungsnotiz

Der Text von ISO/DIS 19014-2:2024 wurde von CEN als prEN ISO 19014-2:2024 ohne irgendeine Abänderung genehmigt.

**Anhang ZA**  
(informativ)

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

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

| Die relevanten grundlegenden<br>Anforderungen der<br>Richtlinie 2006/42/EG | Abschnitt(e)/Unterabschnitt(e)<br>dieser EN | Anmerkungen/Hinweise |
|----------------------------------------------------------------------------|---------------------------------------------|----------------------|
| 1.2.1                                                                      | 5, 6, 7                                     |                      |
| 1.6.1                                                                      | 8                                           |                      |
| 1.7.4.2 (g)                                                                | 8                                           |                      |

## Vorwort

ISO (die Internationale Organisation für Normung) ist eine weltweite Vereinigung nationaler Normungsinstitute (ISO-Mitgliedsorganisationen). Die Erstellung von Internationalen Normen wird üblicherweise von Technischen Komitees von ISO durchgeführt. Jede Mitgliedsorganisation, die Interesse an einem Thema hat, für welches ein Technisches Komitee gegründet wurde, hat das Recht, in diesem Komitee vertreten zu sein. Internationale staatliche und nichtstaatliche Organisationen, die in engem Kontakt mit ISO stehen, nehmen ebenfalls an der Arbeit teil. ISO arbeitet bei allen elektrotechnischen Normungsthemen eng mit der Internationalen Elektrotechnischen Kommission (IEC) zusammen.

Die Verfahren, die bei der Entwicklung dieses Dokuments angewendet wurden und die für die weitere Pflege vorgesehen sind, werden in den ISO/IEC Directives, Teil 1, beschrieben. Es sollten insbesondere die unterschiedlichen Annahmekriterien für die verschiedenen ISO-Dokumentenarten beachtet werden. Dieses Dokument wurde in Übereinstimmung mit den Gestaltungsregeln der ISO/IEC Directives, Teil 2, erarbeitet (siehe [www.iso.org/directives](http://www.iso.org/directives)).

ISO weist auf die Möglichkeit hin, dass die Anwendung dieses Dokuments mit der Verwendung eines oder mehrerer Patente verbunden sein kann. ISO ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren. Details zu allen während der Entwicklung des Dokuments identifizierten Patentrechten finden sich in der Einleitung und/oder in der ISO-Liste der erhaltenen Patenterklärungen (siehe [www.iso.org/patents](http://www.iso.org/patents)).

Jeder in diesem Dokument verwendete Handelsname dient nur zur Unterrichtung der Anwender und bedeutet keine Anerkennung.

Für eine Erläuterung des freiwilligen Charakters von Normen, der Bedeutung ISO-spezifischer Begriffe und Ausdrücke in Bezug auf Konformitätsbewertungen sowie Informationen darüber, wie ISO die Grundsätze der Welthandelsorganisation (WTO, en: World Trade Organization) hinsichtlich technischer Handelshemmnisse (TBT, en: Technical Barriers to Trade) berücksichtigt, siehe [www.iso.org/iso/foreword.html](http://www.iso.org/iso/foreword.html).

Dieses Dokument wurde vom Technischen Komitee ISO/TC 127, *Earth-moving machinery*, Unterkomitee SC 2, *Safety, ergonomics and general requirements*, in Zusammenarbeit mit dem Europäischen Komitee für Normung (CEN), Technisches Komitee CEN/TC 151, *Bau- und Baustoffmaschinen — Sicherheit*, in Übereinstimmung mit der Vereinbarung zur technischen Zusammenarbeit zwischen ISO und CEN (Wiener Vereinbarung) erarbeitet..

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

Die wesentlichen Änderungen sind folgende:

- ausführlicher Anhang ZA hinzugefügt;
- Bezugsnormen datiert;
- Korrektur von Anhang D, MPL-Fehler und Korrektur der Satzfehler „MPLa“ und MPL.“ in Bild D.1;
- 7.3.1, Diagnosedeckungsgrad, geändert.

Eine Auflistung aller Teile der Normenreihe ISO 19014 ist auf der ISO-Internetseite abrufbar.

**E DIN EN ISO 19014-2:2024-04**  
**prEN ISO 19014-2:2024 (D)**

Rückmeldungen oder Fragen zu diesem Dokument sollten an das jeweilige nationale Normungsinstitut des Anwenders gerichtet werden. Eine vollständige Auflistung dieser Institute ist unter [www.iso.org/members.html](http://www.iso.org/members.html) zu finden.

## Einleitung

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

Sicherheitsnormen im Maschinenbau sind wie folgt aufgebaut:

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

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

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

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

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

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

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

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

Für Maschinen, die nach den Anforderungen dieser Typ-C-Norm konzipiert und gebaut worden sind, gilt: Wenn die Anforderungen in dieser Typ-C-Norm von den Anforderungen in Typ-A- oder Typ-B-Normen abweichen, haben die Anforderungen dieser Typ-C-Norm Vorrang gegenüber den Anforderungen der anderen Normen.

## 1 Anwendungsbereich

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

Die Grundsätze dieses Dokuments sind anwendbar für Steuerungssysteme zur Steuerung von Maschinenbewegungen oder Verminderung von Gefährdungen. Solche Systeme werden nach ISO 19014-1:202X oder ISO 19014-5:202X hinsichtlich der Anforderungen an das Performance Level (MPL<sub>r</sub>) untersucht.

Folgende Systeme sind vom Anwendungsbereich dieses Dokuments ausgeschlossen:

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

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

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

Dieses Dokument gilt nicht für EMM, die vor dem Veröffentlichungsdatum dieses Dokuments hergestellt wurden.

## 2 Normative Verweisungen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

ISO 6165:2012, *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 13849-1:2023, *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 19014-1:202X, *Earth-moving machinery — Functional safety — Part 1: Methodology to determine safety-related parts of the control system and performance requirements*

ISO 19014-3:202X, *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 19014-4:202X, *Earth-moving machinery — Functional safety — Part 4: Design and evaluation of software and data transmission for safety-related parts of the control system*

ISO 19014-5:202X, *Earth-moving machinery — Functional safety — Part 5: Table of Machine Performance Level*

### 3 Begriffe

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

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

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

#### 3.1

##### **ESCS**

elektronische Sicherheitssteuerung

aus elektronischen Komponenten bestehende Maschinensteuerung vom Eingabegerät zum Ausgabegerät

#### 3.2

##### **Funktion**

definiertes Verhalten einer oder mehrerer Maschinensteuerungen

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

#### 3.3

##### **N/ESCS**

nicht elektronische Sicherheitssteuerung

aus nicht elektronischen Komponenten bestehende Maschinensteuerung vom Eingabegerät zum Ausgabegerät

#### 3.4

##### **sicherer Zustand**

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

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

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

#### 3.5

##### **bewährte Komponenten**

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

### 4 Symbole und Abkürzungen

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

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

## 5 Allgemeine Anforderungen

### 5.1 Anwendung

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

Die Grundsätze dieses Dokuments müssen auf MCS angewendet werden, die in ISO 19014-1:202X oder ISO 19014-5:202X als SCS eingestuft werden. Weiteren Maschinensteuerungssystemen, die eine Sicherheitsfunktion der Sicherheitssteuerung beeinflussen oder stummschalten, muss das gleiche Performance Level zugeordnet werden wie dem System, das sie beeinflussen oder abschalten.

Maschinen müssen den Sicherheitsanforderungen und/oder Schutz-/Risikominderungsmaßnahmen dieses Abschnittes entsprechen. Zusätzlich müssen die Maschinen den Grundsätzen von ISO 12100:2010 in Bezug auf die relevanten, aber nicht signifikanten Gefährdungen entsprechen, die in diesem Dokument nicht behandelt werden. Sicherheitsbezogene Software in allen Komponenten innerhalb der SCS muss die Anforderungen von ISO 19014-4:202X erfüllen.

## 5.2 Bestehende SCS

Wenn eine bestehende SCS nach einer früheren Norm entwickelt und durch Anwendung, Verwendung und Validierung nachgewiesen wurde, dass sie die Wahrscheinlichkeit einer Gefährdung so gering wie praktisch möglich hält, darf es keine Anforderung an die Aktualisierung der Lebenszyklus-Dokumentation geben. Wenn die zuvor verwendete SCS geändert wird, muss eine Bewertung der Auswirkungen (siehe ISO 1901-4:202X, 3.28) durchgeführt und ein Aktionsplan entwickelt und umgesetzt werden, um sicherzustellen, dass die Sicherheitsanforderungen eingehalten werden.

# 6 Systementwurf

## 6.1 Überblick

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

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

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

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

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

## 6.2 Allgemeine Anforderungen

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

Die folgenden Gestaltungserwägungen müssen berücksichtigt werden:

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

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

### **6.3 Gestaltung der Hardware**

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

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

Sofern anwendbar, muss jede Phase des Entwicklungszyklus validiert werden.

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

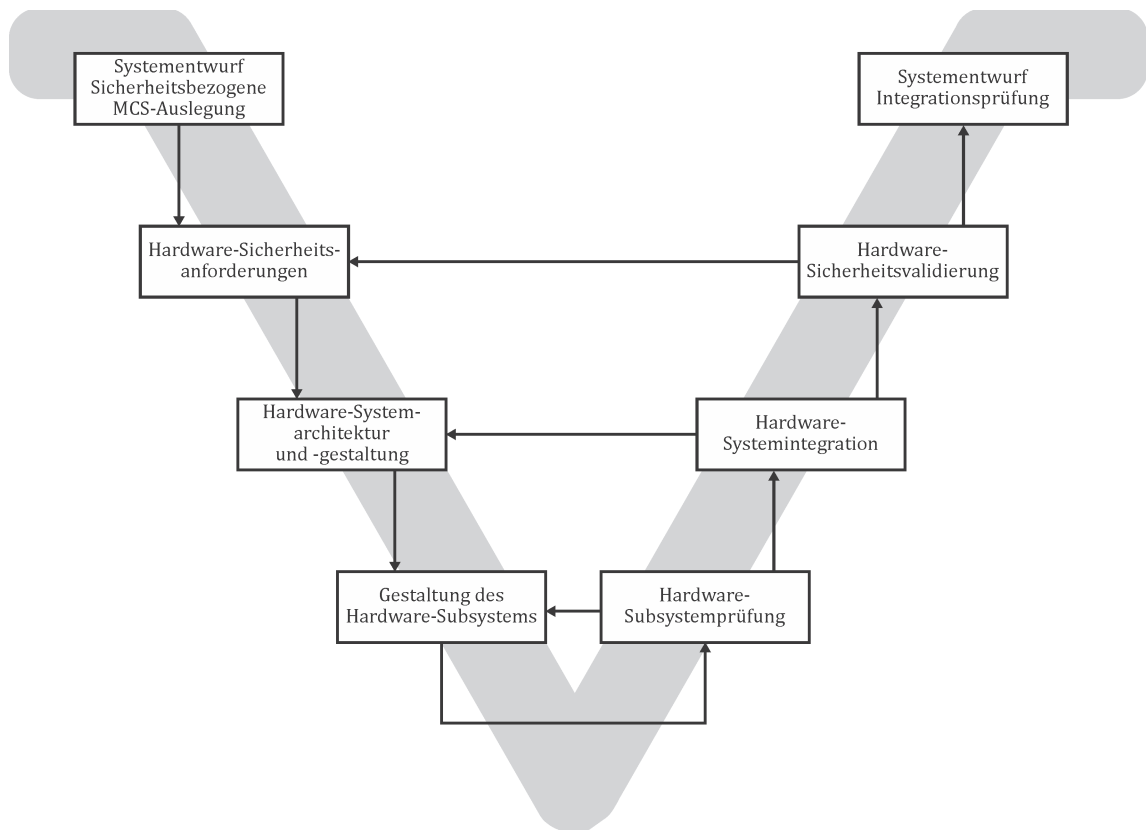


Bild 1 — V-Modell der Hardwareentwicklung

## 7 Bewertung der Sicherheitsleistung des Systems

### 7.1 Erreichtes Performance Level der Maschine (MPL<sub>a</sub>)

Die erreichte Integrität von sicherheitsbezogenen Teilen zur Erfüllung einer Sicherheitsfunktion wird durch die Bestimmung des MPL<sub>a</sub> angegeben.

Die Fähigkeit, eine Sicherheitsfunktion unter den erwarteten Umgebungsbedingungen, wie sie in ISO 19014-3:202X festgelegt sind, auszuführen, muss nachgewiesen und dokumentiert werden.

Das folgende Verfahren wird zur Bewertung des MPL<sub>a</sub> verwendet:

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

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

Bei Systemen, die in der MCSSA für die Qualifizierung zur QM beurteilt werden, müssen ein Qualitätsmanagementsystem (z. B. ISO 9001 oder gleichwertig) verwenden.

Siehe Anhang D für zusätzliche Informationen zur Bewertung von Sicherheitsfunktionen.

## **7.2 Hardware-Sicherheitsbewertung**

### **7.2.1 Allgemeines**

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

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

### **7.2.2 Fehlerberücksichtigung**

Im Allgemeinen können folgende Fehlerkriterien berücksichtigt werden:

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

### **7.2.3 Fehlerausschluss**

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

Der Fehlerausschluss kann auf Folgendem basieren:

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

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

Fehlerausschlüsse können auf anhand der folgenden Hierarchie angewendet werden.

- 1) Fehler-für-Fehler-Basis – Nachdem alle Fehler identifiziert wurden, können manche Fehler auf Basis der oben genannten Kriterien ausgeschlossen werden. Andere können mit Diagnosemitteln innerhalb des Steuerungssystems behandelt werden.
- 2) Komponentenebene – Sofern der Fehlerausschluss auf alle bekannten SCS-Fehler auf Komponentenebene angewendet werden kann, kann der Fehlerausschluss für die gesamte Komponente gelten.
- 3) Systemebene – Sofern alle Fehler in allen Komponenten durch Fehlerausschluss behoben wurden, darf die Analyse von hydraulischen Systemen mithilfe des HSR-Verfahrens in 7.4 durchgeführt werden. Rein mechanische Systeme können auf Systemebene fehlerfrei sein, wenn die Komponenten mit einem angemessenen Sicherheitsfaktor gestaltet sind und die Wartungsanforderungen zur Aufrechterhaltung der korrekten Funktionalität des Systems in der Serviceliteratur nach Abschnitt 8 enthalten sind.

#### 7.2.4 Mittlere Zeit bis zum gefahrbringenden Ausfall (MTTF<sub>d</sub>)

Das Verfahren zur Bestimmung der MTTF<sub>d</sub> ist in ISO 13849-1:2015, 4.5.2 beschrieben. Während ISO 13849-1 die grundlegende Annahme von 50 % für die Rate gefährlicher Ausfälle (z. B.  $B_{10d} = 2 \times B_{10}$ ) empfiehlt, dürfen 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 bestimmte Fehler gelten. Falls dieser auf einige, 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)

#### 7.4.1 Allgemeines

Die Bewertung des MPL<sub>a</sub> von hydraulischen Lenk- und Bremssystemen erfordert eine Bewertung von Fehlern innerhalb der Komponenten im primären Kanal. Aufgrund der Eigenschaften von Hydraulikkomponenten und ihrer Anwendung bei Erdbaumaschinen können deren Fehler nicht mit den in elektronischen Systemen verwendeten Fehlererkennungstechniken adressiert werden. Die Bewertungspunktzahl der Robustheit des hydraulischen Systems (HSR) wird anhand der Kriterien in Tabelle 1 ermittelt. Grundlage für diese Bewertung ist die Robustheit des hydraulischen Systems bei Sicherheitsanwendungen an Erdbewegungsmaschinen. Die Kriterien in Tabelle 1 basieren auf den grundlegenden Sicherheitsprinzipien, Fehlerausschlüssen und bewährten Sicherheitsprinzipien (z. B. nach ISO 13849-2:2012), sowie bewährten Vorgehensweisen zu Auslegung, Entwicklung und Herstellung hydraulischer SCS und bauen darauf auf.

**ANMERKUNG** Diese Kriterien können ebenfalls auf hydraulische Systeme angewandt werden, die nicht für Lenk- und Bremsanwendungen verwendet werden. Da diese Systeme jedoch in der Regel der Kategorie 1 angehören, wäre die Anwendung von Tabelle 2 zur Berechnung eines DC-Werts für die Analyse eines Systems der Kategorie 1 nicht erforderlich.

#### **7.4.2 Berechnung des HSR-Werts**

Der HSR-Score wird als Prozentsatz nach der folgenden Gleichung definiert:

$$r = \frac{t}{100 - q} \times 100$$

Dabei ist

- r* die Robustheit des hydraulischen Systems (HSR);
- q* die Summe der Kriterien, die die Wahrscheinlichkeit des gefährlichen Ausfalls für die beabsichtigte Sicherheitsfunktion, die die Sicherheitsfunktion abschwächt, nicht verringert;
- t* die Gesamtheit der verbleibenden anwendbaren Kriterien, die vom System erfüllt werden.

Ein Kriterium, das das System nicht erfüllt, darf nicht in *q* einbezogen werden. (Eine alternative Energiequelle wäre zum Beispiel kein anwendbares Kriterium für ein federbetätigtes, hydraulisch freigegebenes System, bei dem der sichere Zustand dem betätigten Zustand entspricht.)

Jedes SRP/CS im hydraulischen System 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 hydraulischen Systeme. Die Fehlerausschlüsse dürfen auf Komponentenebene angewandt werden, wenn alle anwendbaren Fehler nach ISO 13849-2:2012, Anhang C, ausgeschlossen werden können.

**Tabelle 1 — Bewertungskriterien für die Robustheit des hydraulischen Systems**

| <b>Ref.</b> | <b>Kriterien</b>                                                                                                                | <b>Be-<br/>wertung</b> |
|-------------|---------------------------------------------------------------------------------------------------------------------------------|------------------------|
| A           | Überdimensionierung<br>(z. B. ausreichender Spulen-Freiraum, -Geradheit und -Zylindrizität)                                     | 10                     |
| B           | Gegenmaßnahmen für das Hängenbleiben oder Durchdrehen von Spulen                                                                | 10                     |
| C           | Gegenmaßnahmen für störenden Hydraulikeingang<br>(z. B. der unmittelbare Hochdruck an beiden Anschlüssen eines Hydraulikmotors) | 10                     |
| D           | Sekundäre Energiequelle (z. B. Steuerakku) oder ausfallsichere Auslegung bei Verlust der primären Energiequelle                 | 20                     |
| E           | Langsamer oder schrittweise voranschreitender Fehler<br>(z. B. Verminderung der Lenkunterstützung vor dem erheblichen Fehler)   | 10                     |
| F           | Schlauchplatzsicherung (z. B. Verlegung zur Verhinderung scharfkantiger Verunreinigungen/Verschleiß)                            | 10                     |
| G           | Systemauslegung zur Aufrechterhaltung der erforderlichen Sauberkeit der Hydraulikflüssigkeit                                    | 10                     |
| H           | Gegenmaßnahmen für Erosion durch Luftbeimischung in der Hydraulikflüssigkeit                                                    | 10                     |

**Tabelle 1 (fortgesetzt)**

| Ref. | Kriterien                                                                                                                                   | Be-<br>wertung |
|------|---------------------------------------------------------------------------------------------------------------------------------------------|----------------|
| I    | Gegenmaßnahmen für durch Luftbeimischung in der Hydraulikflüssigkeit verursachte Probleme bei der Druckübertragung (z. B. Entlüftungskreis) | 10             |
|      | <b>Gesamtwert</b>                                                                                                                           |                |

Tabelle 2 definiert den DC-Wert, mit dem ein bestimmter HSR-Wert korreliert ist. Mit diesem DC-Wert, der Kategorie der Systemarchitektur,  $MTTF_d$  und CCF aus ISO 13849-1:2015, Tabelle 6 kann ein  $MPL_a$  bestimmt werden. Siehe Tabelle 3 für eine Erläuterung der Kategorie 2M.

**Tabelle 2 — Korrelation zwischen HSR und DC zur Bestimmung des  $MPL_a$**

| HSR-Wert        | DC-<br>Entsprechung | MPL               |              |                 |              |
|-----------------|---------------------|-------------------|--------------|-----------------|--------------|
|                 |                     | $MTTF_d$ = Mittel |              | $MTTF_d$ = Hoch |              |
|                 |                     | Kategorie B       | Kategorie 2M | Kategorie 1     | Kategorie 2M |
| 50 % bis ≤ 80 % | 60 %                | $MPL_a = b$       | $MPL_a = b$  | $MPL_a = c$     | $MPL_a = c$  |
| > 80 %          | 90 %                | $MPL_a = b$       | $MPL_a = c$  | $MPL_a = c$     | $MPL_a = d$  |

Siehe Anhang B für Beispiele von Bewertungen, bei denen die HSR-Bewertung angewandt wurde.

## **7.5 Kategorie-Klassifikationen**

### **7.5.1 Allgemeines**

Die zur Einhaltung der Anforderungen des Systems geeignete Architektur muss ausgewählt werden. Obwohl die Vielfalt möglicher Strukturen groß ist, sind die Basiskonzepte oft ähnlich. Daher können die meisten bestehenden Strukturen einer der in ISO 13849-1:2015, 6.2 beschriebenen Kategorien zugeordnet werden. Bei einigen Strukturen, die in Lenk- und Bremssystemen verwendet werden, ist jedoch eine Anpassung aufgrund der Eigenschaften des hydraulischen Systems erforderlich, die speziell für die Anwendung bei Erdbewegungsmaschinen gelten. 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 vorgeschlagenen Architekturen überein. Auslegungen, die die Eigenschaften der jeweiligen Kategorie im Allgemeinen aufweisen, entsprechen der jeweiligen vorgesehenen Architektur dieser Kategorie. Die Bilder 2 und Bild 3 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. eine ECU 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 19014-3:202X;
  - Unterstützung der erforderlichen MTTF<sub>d</sub>.

MCS, die eine Sicherheitsfunktion des SCS beeinflussen oder abschalten, muss das gleiche Performance Level wie dem SCS zugeordnet werden, sofern nicht belegt werden kann, dass nach ISO 19014-1:202X oder ISO 19014-5:202X ein anderer MPL<sub>r</sub> erforderlich ist.

**Tabelle 3 — Zusammenfassung der Kategorie-Anforderungen**

| Kategorie | Zusammenfassung der Anforderungen                                                                                                                                                                                                                                                                                     | Systemverhalten                                                                                                                                                                     | MTTF <sub>d</sub>  | DC    | CCF-Eval. | HFT |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|-------|-----------|-----|
| B         | SRP/CS und/oder ihre Schutzausrüstungen sowie ihre Bauteile müssen in Übereinstimmung mit den relevanten Normen ausgelegt, konstruiert, ausgewählt, zusammengebaut und kombiniert werden, damit sie den zu erwartenden Einflüssen standhalten können. Es müssen grundlegende Sicherheitsprinzipien angewendet werden. | Das Auftreten eines Fehlers kann zum Verlust der Sicherheitsfunktion führen.                                                                                                        | niedrig bis mittel | keine | NA        | 0   |
| 1         | Es müssen die Anforderungen der Kategorie B erfüllt werden. Es müssen bewährte Komponenten und erprobte Sicherheitsprinzipien verwendet werden.                                                                                                                                                                       | 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   |

**Tabelle 3 (fortgesetzt)**

| Kate-<br>gorie | Zusammenfassung der<br>Anforderungen                                                                                                                                                                            | Systemverhalten                                                                                                                                                                                                                                                                                                                    | MTTF <sub>d</sub>                                             | DC                                                            | CCF-Eval.                 | HFT |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------|---------------------------------------------------------------|---------------------------|-----|
| 2              | Es gelten die Anforderungen der Kategorie B und die Anwendung von bewährten Sicherheitsprinzipien. Die Sicherheitsfunktion muss in angemessenen Abständen durch das Maschinensteuerungssystem überprüft werden. | 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 <sup>a</sup> | 0   |
| 2M             | Die Anforderungen der Kategorie 1 gelten für hydraulische SRP/CS. Die Anforderungen der Kategorie 2 gelten für andere Technologien.                                                                             | Das Auftreten eines Fehlers kann zum Verlust der Sicherheitsfunktion führen. Die Fähigkeit des Systems, die Funktion auszuführen, wird überwacht oder der Fehlerausschluss wird auf anwendbare Fehler angewandt. Das System reagiert, wenn ein nicht durch Fehlerausschluss ausgeschlossener Fehler vorliegt.                      | hoch für hydraulische SRP/CS, niedrig für andere Technologien | niedrig bis mittel (siehe Tabelle 2 für Hydraulikkomponenten) | erforderlich <sup>a</sup> | 0   |

**Tabelle 3** (fortgesetzt)

| Kate-<br>gorie                                                                             | Zusammenfassung der<br>Anforderungen                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Systemverhalten                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | MTTF <sub>d</sub> | DC                 | CCF-Eval.    | HFT |
|--------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|--------------------|--------------|-----|
| 3                                                                                          | Es gelten die Anforderungen der Kategorie B und die Anwendung von bewährten Sicherheitsprinzipien. Sicherheitsbezogene Teile müssen so gestaltet sein, dass „ein Einzelfehler in einem dieser Teile nicht zum Verlust der Sicherheitsfunktion führt“ und, wann immer dies nach vernünftigem Ermessen durchführbar ist, der Einzelfehler erkannt wird.                                                                                                                                            | 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.                                                                                                                                                                                  | niedrig bis hoch  | niedrig bis mittel | erforderlich | 1   |
| 4                                                                                          | Es gelten die Anforderungen der Kategorie B und die Anwendung von bewährten Sicherheitsprinzipien. Sicherheitsbezogene Teile müssen so gestaltet sein, dass „ein Einzelfehler in einem dieser Teile nicht zum Verlust der Sicherheitsfunktion führt“ und der Einzelfehler bei oder vor dem nächsten Abruf der Sicherheitsfunktion erkannt wird, dass aber, wenn diese Erkennung nicht möglich ist, eine Anhäufung von unerkannten Fehlern nicht zum Verlust der Sicherheitsfunktion führen darf. | 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 bei oder vor dem nächsten Abruf der Sicherheitsfunktion erkannt oder die Fehleransammlung kann nicht zum Verlust der Sicherheitsfunktion führen. | hoch              | hoch               | erforderlich | 1   |
| <sup>a</sup> Eine Architektur der Kategorie 2 könnte gegenüber einem CCF empfindlich sein. |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                   |                    |              |     |

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

- die Gebrauchsdauer beträgt 20 Jahre;
- konstante Ausfallraten innerhalb der Gebrauchsdauer sind zu erwarten;
- bei Kategorie 2: Anforderungsrate  $\leq 1/100$  Testrate (siehe auch ANMERKUNG in ISO 13849-1:2015, Anhang K); oder die 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 ist die  $MTTF_d$  des Prüfkanals größer als die Hälfte der  $MTTF_d$  des Basis- oder Funktionskanals.

**Tabelle 4 — Kategorien für verschiedene Technologien**

| Kategorie | Mechanisch | Pneumatisch | Hydraulisch | Elektronisch | Elektrisch |
|-----------|------------|-------------|-------------|--------------|------------|
| 1         | √          | √           | √           | N/A          | √          |
| 2         | N/A        | √           | √           | √            | N/A        |
| 3         | P/A        | P/A         | P/A         | √            | P/A        |
| 4         | P/A        | P/A         | P/A         | √            | P/A        |

**Legende**  
N/A: Nicht anwendbar  
P/A: Parallele Hinzufügung (en: parallel add)  
√: Anwendbar  
ANMERKUNG 1 Für weitere Informationen zur P/A siehe 7.6 und Beispiele in Anhang A.  
ANMERKUNG 2 Komplexe elektronische Komponenten (z. B. SPS, Mikroprozessor, anwendungsspezifischer integrierter Stromkreis) können in einer Architektur der Kategorie 1 nicht verwendet werden.

## 7.5.2 Kategorie B/Kategorie 1

### 7.5.2.1 Erklärung zur Anwendung der Kategorie 1 für N/ESCS

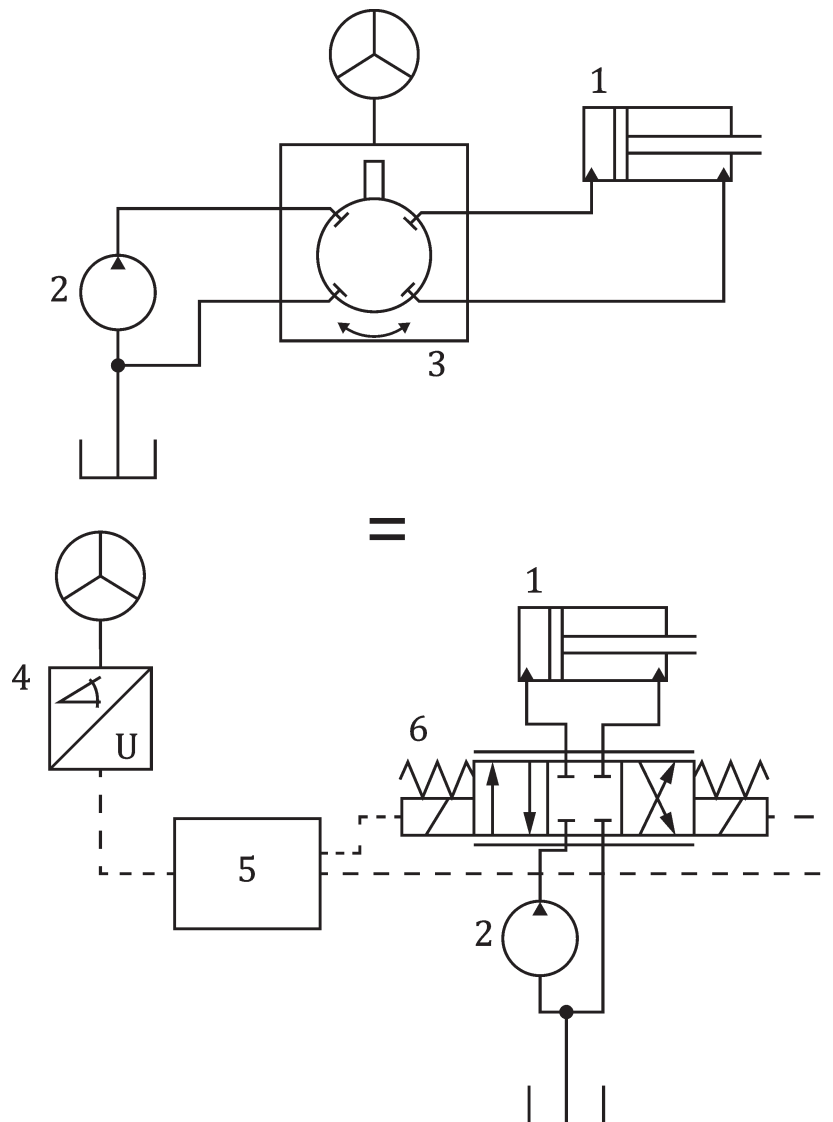
Die meisten hydraulischen und pneumatischen Ventile und mechanischen Verbindungen haben Architekturen der Kategorie 1. Im Falle von hydraulischen Ventilen werden die Eingangs-, Logik- und Ausgangsfunktion intrinsisch in der Auslegung mit Feder und Spule innerhalb des Ventils umgesetzt. Diese kann als kombinierte Eingangs-, Logik- und Ausgangskomponente 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. Bild 2 zeigt ein Beispiel für ein Lenksystem, das mit zwei verschiedenen Technologien umgesetzt wurde.

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.

Es folgt eine nicht-erschöpfende Auflistung von Beispielen:

- a) Eine Bedienperson drückt ein Pedal herunter – die Energie verändert sich von kinetisch zu hydraulisch.
- b) Eine Bedienperson 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.
- c) Ein vorgesteuertes hydraulisches System ist Beispiel b) 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 B/Kategorie 1



#### Legende

- 1 Lenkzylinder
- 2 Pumpe
- 3 Orbitalventil
- 4 Lenksensor
- 5 ECU
- 6 Lenkventil

ANMERKUNG 1 Elektronische Systeme entscheiden für gewöhnlich darüber, wie die Eingangsleistung geleitet wird und steuern die Ausgangsenergie basierend darauf. Bei einer N/ESCS wird die Ausgangsleistung durch den primären Kanal geleitet und dann wird die Energie entweder zurück an den Tank gesendet oder für die Steuerung der Maschine verwendet.

ANMERKUNG 2 Ein elektronisches System kann der Kategorie 2 angehören, wenn das ECM über eine Eingangs-/Ausgangsdiagnose und einen Ausgang zur Minderung der Gefährdung verfügt.

**Bild 2 — Beispiel für zwei analoge Lenksysteme der Kategorien B/Kategorie 1 unterschiedlicher Technologien: hydraulisches Lenksystem (oben) und analoges elektronisches Lenksystem (unten)**

### 7.5.3 Kategorie 2

#### 7.5.3.1 Allgemeines

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

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

ANMERKUNG Oft kann die Bedienperson 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 zwei oder mehr Komponenten innerhalb eines Funktionsblocks parallel (ILO) sind und für den Verlust der Sicherheitsfunktion ein Fehler an mehr als einer Komponente auftreten muss, kann dieser Block als eine Funktion der Kategorie 3 betrachtet werden (siehe 7.6 für parallele Hinzufügung).

#### 7.5.3.2 Modifizierung von Kategorie 2 für hydraulische Systeme (Kategorie 2M)

Die Anwendung einer Architektur der Kategorie 2M folgt den Prinzipien und Anforderungen einer Architektur der Kategorie 2, sieht aber aufgrund der Eigenschaften von Hydraulikkomponenten und ihrer Anwendung auf Erdbaumaschinen, z. B. Lenk- und Bremssysteme, etwas anders aus. Der Begriff „Kategorie 2M“ wird verwendet, um den unterschiedlichen Ansatz gegenüber stationären Maschinen in ISO 13849-1 zu verdeutlichen.

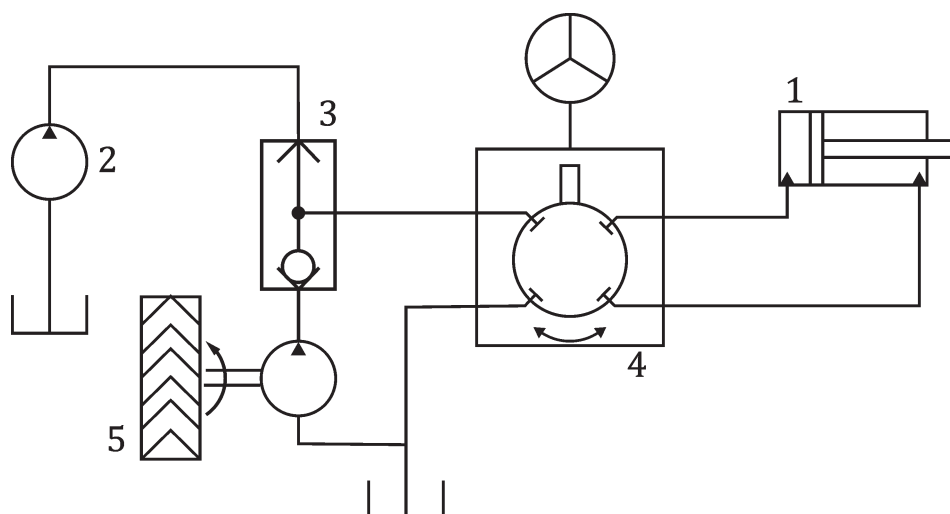
Die Prüfkä-näle von Systemen der Kategorie 2M überwachen den primären Kanal nicht direkt auf Fehler, sondern überwachen und erhalten die Fähigkeit des Systems, seine Funktion zu erfüllen (z. B. wenn die Ölversorgung nicht ausreicht und auf eine sekundäre Versorgung umschaltet). Da ihre Ausfallmodi gut untersucht sind und ihre Zuverlässigkeit erwiesen ist, werden Fehler im primären Kanal mithilfe der HSR-Bewertung in 7.4 behoben; diese Bewertung wird zur Bestimmung des DC-Werts des Systems verwendet.

ANMERKUNG 1 Die Ölversorgung wird üblicherweise durch ein elektronisches System, ein Wechselventil oder eine ähnliche Einrichtung überwacht und durch einen Druckspeicher oder eine Reservepumpe ergänzt, wenn die Hauptölquelle unterbrochen ist.

ANMERKUNG 2 Dies ist ein Beispiel für ein „bei Ausfall betriebsfähiges“ System. Der sichere Zustand besteht darin, die Lenkfähigkeit über die sekundäre Ölversorgung aufrechtzuerhalten. In diesem Fall wurden die Ölversorgung und die Lenksteuerung zu einer einzigen Sicherheitsfunktion kombiniert.

Ein System der Kategorie 2M wird in Bezug auf den Prozess und die Anforderungen zur Berechnung einer  $MPL_a$  aus ISO 13849-1:2015, Tabelle 6 als gleichwertig mit einem System der Kategorie 2 angesehen. Bild 3 ist ein Beispiel für ein Lenksystem der Kategorie 2M, während das System in Bild 4 als Blockdiagramm dargestellt ist.

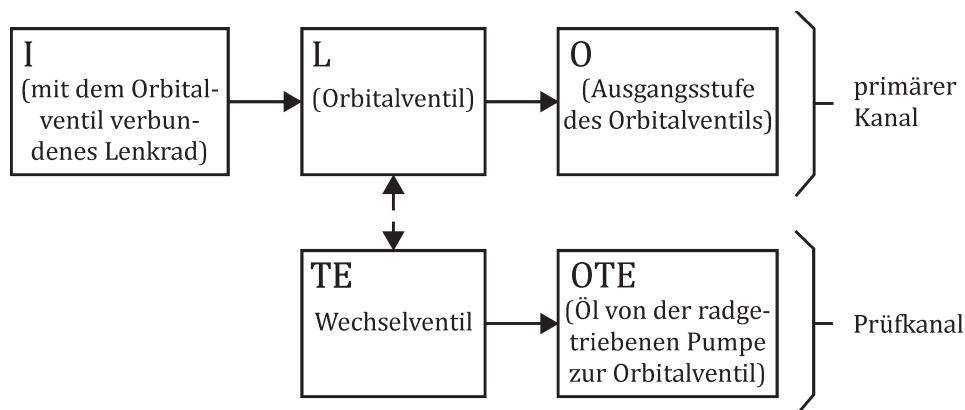
### 7.5.3.3 Beispiel für ein hydraulisches System der Kategorie 2M



#### Legende

- 1 Lenkzylinder
- 2 Pumpe
- 3 Wechselventil
- 4 Orbitalventil
- 5 radgetriebene Pumpe

**Bild 3 — Beispiel für ein hydraulisches Lenksystem der Kategorie 2M**



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

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

**Bild 4 — Beispiel für ein Blockdiagramm eines hydraulischen Systems**

### 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  $MPL_r$  und müssen eigene Sicherheitsfunktionen haben. Eine der Sicherheitsfunktionen wird vermutlich einen niedrigeren  $MPL_r$  haben als die andere und der sichere Zustand der Maschine entspricht eventuell dem sicheren Zustand entsprechend dem höchsten  $MPL_r$ .

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  $MPL_r$  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 Bedienperson über den Prüfkanal anzuhalten; es sollte jedoch betrachtet werden, wie genau 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  $MPL_r$  der gegensätzlichen Sicherheitsfunktion gleich ist, darf 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 dürfen 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, darf 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 bis 4 dargelegten nicht entsprechen. Siehe ISO 13849-1:2015, 6.3 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 infolge gemeinsamer Ursache geben. Ein Beispiel für eine Reduktion eines parallelen kombinierten  $MPL_a$  in Reihe ist in Bild 5 dargestellt.

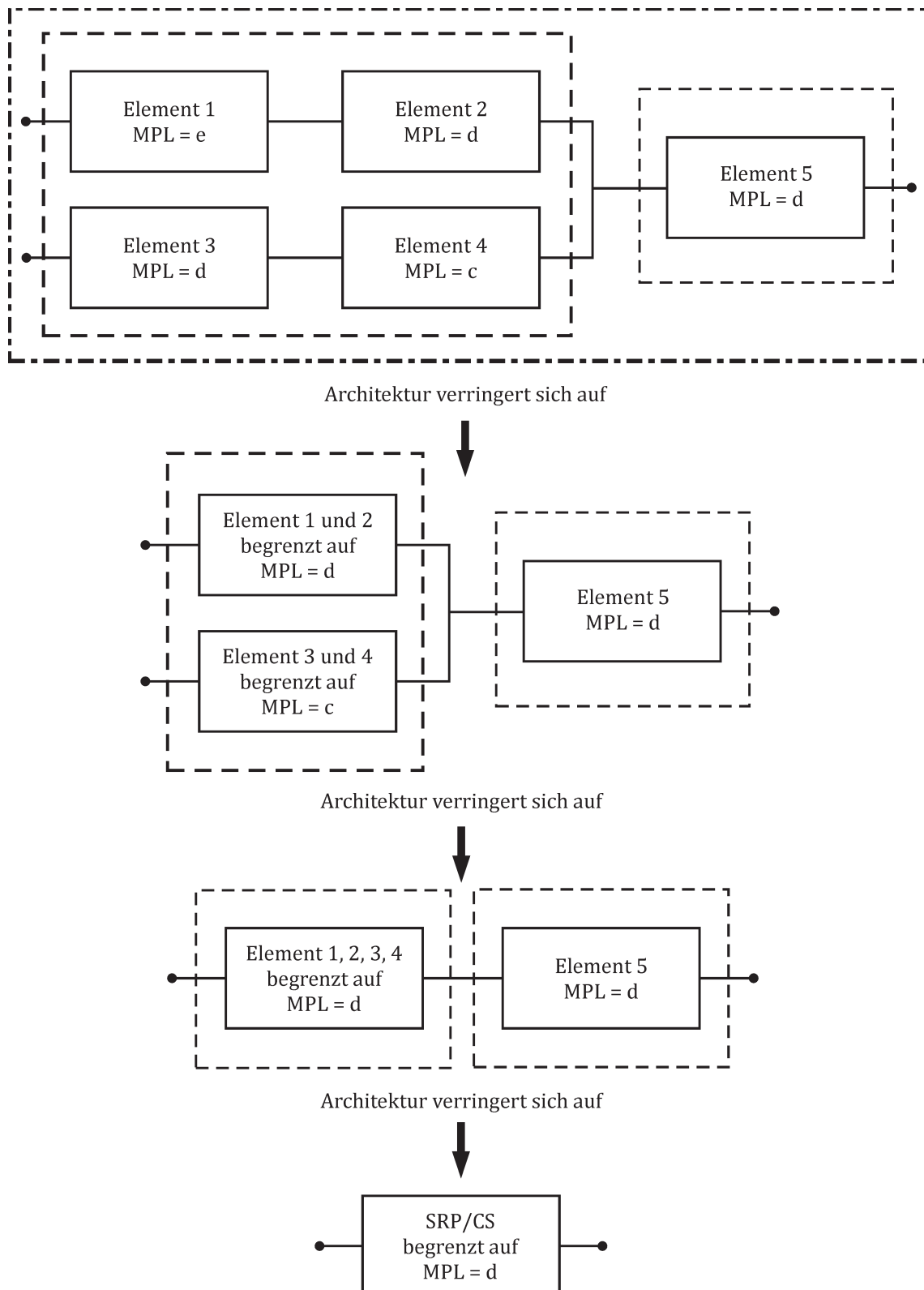


**Bild 5 — Beispiel für die Reduktion eines parallel kombinierten MPL<sub>a</sub> in Reihe**

Alternativ zur parallelen Hinzufügung von Komponenten dürfen zwei parallele Kanäle HFT = 0 (Kategorie B, 1, 2) als ein System der Kategorie 3 betrachtet werden. Die Aktivierungsmaßnahme für die beiden Kanäle durch die Bedienperson muss der Anforderung von AR3 in ISO 19014-1:2020X, 6.5 entsprechen; aufgrund der natür-

lichen Reaktion der Bedienperson 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. Eine 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

### 8.1 Allgemeines

Benutzerinformationen müssen in Übereinstimmung mit ISO 12100:2010, 6.4.5 bereitgestellt werden.

### 8.2 Benutzerhandbuch

ISO 6750-1 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

#### A.1 Allgemeines

Die Beispiele in diesem Anhang sollen dazu dienen, die Berechnungsverfahren für Systeme mit unterschiedlichen MPL, Kategorien und Technologien zu veranschaulichen, und spiegeln nicht zwingend reale Systeme wider. Daher entsprechen diese Beispiele möglicherweise nicht den Anforderungen an das Performance Level der Maschine in ISO 19014-5:202X und lassen auch nicht darauf schließen, dass ein sicherer Zustand für die Sicherheitsfunktion bei einer bestimmten Maschine geeignet wäre.

Diese Beispiele beginnen relativ einfach und werden zunehmend komplexer. Diese Beispiele umfassen rein hydraulische SCS-Komponenten bis hin zu Komponenten elektro-hydraulischer SCS. Siehe Tabelle A.1 für eine Zusammenfassung der Beispiele in diesem Anhang.

**Tabelle A.1 — In diesem Anhang dargestellte Beispiele für die Berechnung des  $MPL_a$**

| $MPL_a$ | Kategorie | Hydraulisch/<br>Hydraulisch | Elektrisch/<br>Hydraulisch | Elektro-<br>hydraulisch                             | Parallele<br>Hinzufügung |
|---------|-----------|-----------------------------|----------------------------|-----------------------------------------------------|--------------------------|
| b       | B         |                             |                            | A.1 Lenkung                                         |                          |
| c       | 1         | A.2 Lenkung                 | A.3 Feststellbremse        |                                                     |                          |
| c       | 2         |                             |                            | A.4 Lenkung mit<br>automatischer<br>Feststellbremse |                          |
| d       | 2         | A.5 Lenkung                 |                            |                                                     |                          |
| d       | 3         |                             |                            | A.6 Bremsung                                        | X                        |

**ANMERKUNG** Die  $MTTF_d$ -Werte für NES/CS können anhand der  $MTTF_d$ -Werte des Lieferanten der Komponenten oder des Herstellers der Maschine oder des  $B_{10d}$ -Wertes entsprechend ISO 13849-1:2015, C.4 berechnet werden.

#### A.2 Beispiel 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.

Bild A.1 zeigt ein Schema einer elektro-hydraulischen Lenkung der Kategorie B.