Masterarbeit

ANALYSE UND OPTIMIERUNG DES SICHERHEITSKONZEPTES EINER MOBILEN SCHIFFSHÜLLENBEARBEITUNGS- UND INSPEKTIONSPLATTFORM

ausgeführt am

Fachhochschul-Masterstudiengang
Automatisierungstechnik-Wirtschaft

von
Ing. Thomas Moßhammer, BSc
1610322025

betreut und begutachtet von
Dipl.-Ing. Franz Gregor Blasge

Graz, im Jänner 2018 .....

Unterschrift

EHRENWÖRTLICHE ERKLÄRUNG

Ich erkläre ehrenwörtlich, dass ich die vorliegende Arbeit selbstständig und ohne fremde Hilfe verfasst, andere als die angegebenen Quellen nicht benützt und die benutzten Quellen wörtlich zitiert sowie inhaltlich entnommene Stellen als solche kenntlich gemacht habe.

.....

Unterschrift

DANKSAGUNG

Ich möchte all jenen danken, die durch ihre persönliche Unterstützung und ihre Expertise zu dieser Masterarbeit beigetragen haben.

Besonderer Dank gilt meinem Betreuer seitens der Fachhochschule CAMPUS 02, Herrn Dipl.-Ing. Franz Blasge, für die ausgezeichnete Betreuung bei der Erstellung dieser Masterarbeit. Ich danke für die konstruktive Kritik und die fachliche Diskussion. Vielen Dank für die Zeit und Mühen, die Sie in meine Arbeit investiert haben.

Ein weiterer Dank gilt meinen Arbeitskollegen bei der Hubert Palfinger Technologies GmbH. Stellvertretend möchte ich hier Herrn Dipl.-Ing. Christian Thöni und Herrn Werner Fritz erwähnen, die mir speziell bei mechanischen Themen immer mit Rat zur Verfügung gestanden sind.

Weiters danke ich meinen Eltern Rudolf und Gerlinde für die großartige Unterstützung.

Zuletzt ist es mir ein großes Anliegen mich bei meiner Freundin Sabrina zu bedanken. Sie hat mir während des Studiums den nötigen Rückhalt gegeben. Danke für das Verständnis und die motivierenden Worte.

Die vorliegende Masterarbeit widme ich meiner Freundin Sabrina und meinem Sohn Vincent, der kurz vor Fertigstellung dieser Arbeit das Licht der Welt erblickt hat.

KURZFASSUNG

Die manuelle Bearbeitung von Schiffshüllen verliert aus Gründen der Effizienz und des Umweltschutzes immer mehr an Bedeutung. Stattdessen kommen hochautomatisierte Maschinen zum Einsatz, die diese Arbeit übernehmen oder Maschinen, die Personen an exponierte Stellen transportieren, um dort diverse Arbeiten zu verrichten. Mit steigendem Automatisierungsgrad steigen auch die Anforderungen an die Sicherheit von Maschinen, speziell im Bereich der Personensicherheit.

Das Ziel dieser Masterarbeit war die Analyse und Optimierung eines Sicherheitskonzeptes für eine fahrbare Maschine der Hubert Palfinger Technologies GmbH zur manuellen Bearbeitung und Inspektion von Schiffshüllen in Schwimm- und Trockendocks. Auf Grund der rauen Umgebungsbedingungen und einer Bearbeitungshöhe von bis zu 30 Metern, wurden höchste Anforderungen an die Sicherheit des Bedienpersonals gestellt.

Die Analyse des Sicherheitskonzeptes umfasste neben der Auswahl der Steuerung und der Optimierung der elektrischen und hydraulischen Bauteile auch einen rechnerischen Nachweis zur Vermeidung von Fehlern in sicherheitsbezogenen Teilen von Steuerungen. Die in dieser Masterarbeit durchgeführten Berechnungen zur Validierung der Sicherheitsfunktionen wurden einer akkreditieren Prüfstelle, mit dem Ansuchen einer CE-Zulassung für diese Maschine vorgelegt.

Die Hubert Palfinger Technologies GmbH entwickelt mehrere Maschinen für die Schiffsbearbeitungsindustrie, die in ihrer Konstruktion sehr ähnlich sind. Das analysierte Sicherheitskonzept für die Personensicherheit ist somit vielseitig auch in anderen Maschinen anwendbar. Durch die Anwendung des fertigen Konzeptes gäbe es Potential für Einsparungen in der Entwicklung und bei Zertifizierungen. Außerdem könnten gewonnene Kenntnisse aus dem Betrieb in den Schiffswerften rasch und effektiv in zukünftige Planungen einfließen und so die Sicherheit aller Maschinen der Hubert Palfinger Technologies GmbH erhöhen.

ABSTRACT

The manual ship hull treatment loses more and more importance for reasons of efficiency and environmental protection. Instead highly automated machines are used and will be used in the future. These machines will do the work or will be used to bring workers to exposed areas to perform their tasks there. As the level of automation is increasing the demand on safety is also increasing especially as far as human safety is concerned.

The aim of this master thesis was the analysis and optimization of a safety concept for a machine of the Hubert Palfinger Technologies GmbH for a hull treatment machine used in floating and dry docks. Due to harsh environmental conditions and a processing height up to 30 meters the highest demands were placed on safety of operating staff.

The analysis of the safety concept did not only include the selection of sensors and the programmable logic controller but also a computational proof to avoid errors in safety-related parts of control systems. The validation of the safety functions out of this master thesis were submitted to an accredited testing laboratory. The accredited testing laboratory is presently auditing the safety concept.

The product portfolio of Hubert Palfinger Technologies GmbH is very large, but some parts are very similar, as far as their principle construction is concerned. As a result, the analysed safety concept for human safety could be used for different machines. This would save money for development and certification costs. Furthermore, knowledge gained from shipyard operations could be quickly and effectively incorporated into future planning. As a result, the safety of all Hubert Palfinger Technologies GmbH machines could be increased.

INHALTSVERZEICHNIS

1 EINLEITUNG

Automatisierte Maschinen gewinnen immer mehr an Komplexität. Der Anteil an elektrischen und elektronischen Systemen steigt kontinuierlich an. Die Anforderungen an die Personensicherheit erhöhen sich ebenfalls. Als logische Konsequenz steigt auch die Möglichkeit von Fehlfunktionen bei diesen Maschinen. Diese führen zu Maschinenschäden und im schlimmsten Fall sogar zu Personenschäden. Deshalb muss oberste Priorität in der Gewährleistung der funktionalen Sicherheit neuer Maschinen liegen. Das Ziel der funktionalen Sicherheit liegt darin, kritische Funktionen einer Maschine oder eines Systems gegen Fehlfunktionen zu sichern. Im Hinblick auf den Entwicklungsprozess einer neuen Maschine, ist es unumgänglich das Thema der funktionalen Sicherheit zu integrieren. Das spart Entwicklungszeiten und vor allem Entwicklungskosten. Ein Sicherheitskonzept dient dabei als Grundlage und stellt die Weichen für eine sichere Maschine.

Die vorliegende Arbeit beschäftigt sich mit der Erstellung eines solchen Sicherheitskonzeptes einer Schiffsbearbeitungs- und Inspektionsplattform für die Schifffahrts-Industrie. Das Ergebnis dieser Masterarbeit soll zum einen bei der Entscheidungsfindung der einen oder anderen Problemstellung in der Steuerungstechnik behilflich sein und zum anderen auch als Grundlage für die bevorstehende Baumusterprüfung durch den TÜV dienen.

1.1 Themenvorstellung

Die Firma Hubert Palfinger Technologies GmbH (HPT) hat sich unter anderem auf Gesamtlösungen zur Außenhaut-Sanierung von Schiffsrümpfen – Hull Treatment – mit Höchstdruckwasser bis 3.000 bar fokussiert. Dabei wird unter anderem die Schiffshülle völlig vom Lack befreit und danach wieder beschichtet. Jedes Schiff, vom Tanker bis zum Kreuzfahrtsschiff macht diesen Vorgang mehrere Male während seiner Verwendung durch. Gründe dafür sind die Sanierung beschädigter Bereiche, die Lösung von Speed Claims sowie Treibstoffeinsparungen. Neben automatisierten Maschinen, die mit Abtragswerkzeugen bestückt sind, gibt es auch Maschinen, die eine manuelle Bearbeitung durch Werftpersonal aus Arbeitskörben in bis zu 30 Meter Höhe ermöglichen. Um ein sicheres Arbeiten in solchen Höhen zu ermöglichen, liegt höchste Priorität auf der Sicherheit der Maschine.

1.2 Ziel der Arbeit

In der Masterarbeit wird das Sicherheitskonzept des Prototypen einer „Ship Treatment and Elevating Platform“ (STEP) in Bezug auf zutreffende Gesetze, Richtlinien und Normen analysiert und bewertet. In der Folge soll für ein überarbeitetes Nachfolgemodell ein mögliches Optimierungspotential entwickelt und auf dessen Umsetzbarkeit geprüft werden. Bei der Entwicklung eines Sicherheitskonzeptes liegt natürlich die Sicherheit von Personen im Fokus. Darüber hinaus geht es zusätzlich um eine Auseinandersetzung mit den anfallenden Kosten. Das Hauptaugenmerk soll dabei auf die wichtigsten Komponenten der Maschine gelegt werden. Das sind zum einen die Brücken und die Schubarme mit den angeflanschten Arbeitskörben und zum anderen der Teleskopturm. Des Weiteren wird speziell auf die Abstützvorrichtung eingegangen, auf welche eine besonders wichtige Rolle zukommt.

Zum Einsatz kommen die Maschinen der Firma HPT in Docks in China und Singapur sowie in Deutschland. Diese Docks werden von Werften betrieben um Arbeiten an trockengelegten Schiffen durchzuführen. Dabei wird grundsätzlich zwischen Trockendocks und Schwimmdocks unterschieden. Der jeweilige Dockboden ergibt unterschiedliche Anforderungen an die Fahrwerke der Maschinen der HPT.

Außerdem soll die Anwendung einzelner Sicherheitsmechanismen in anderen Maschinen im Portfolio der HPT geprüft werden. Abschließend werden gewonnene Erkenntnisse der Masterarbeit zusammengefasst und ein Ausblick über zukünftige Möglichkeiten gegeben.

1.3 Motivation

Mit der Entwicklung neuer Technologien ergeben sich nicht nur andere und mehrere Möglichkeiten, sondern auch neue Risiken. Um sicher zu gehen, dass neue Produkte keine Gefahr für Mensch und Umwelt darstellen, ist es von besonderer Bedeutung neue, relevante Risiken zu identifizieren und zu bewerten. Unter dem Begriff der funktionalen Sicherheit im Maschinen- und Anlagenbau gilt es den Schutz von Mensch und Umwelt, sowie die Gefahren für die technischen Komponenten zu minimieren. Eine Störung der funktionalen Sicherheit kann mit enormen Haftungsansprüchen einhergehen. Aus diesen Gründen ist es von besonderer Bedeutung in einer möglichst frühen Phase der Projektentwicklung bereits das Thema der funktionalen Sicherheit zu berücksichtigen. Wird das Thema vernachlässigt, kann das zu sehr hohen Kosten führen. Im schlimmsten Fall können Maschinen- oder Anlagenteile in der geplanten Form nicht umgesetzt werden.

Funktionale Sicherheit ist das zuverlässige Erbringen von Sicherheitsfunktionen von sicherheitsgerichteten Steuerungen. In der Norm IEC 61508-4:2010 ist der Begriff der funktionalen Sicherheit wie folgt definiert:

„Teil der Gesamtsicherheit, bezogen auf die EUC und das EUC-Leit- oder Steuerungssystem, der von der korrekten Funktion des E/E/PE-sicherheitsbezogenen Systems und anderer risikomindernder Maßnahmen abhängt“[1].

Die Abkürzung EUC (Equipment under control) steht dabei für den Begriff Einrichtung, Maschine, Apparat oder Anlage. Das EUC-Leit- oder Steuerungssystem ist jedoch getrennt und unterschiedlich zum EUC.

1.4 Methodik

Einführend werden zunächst theoretische Grundlagen und rechtliche Aspekte der funktionalen Sicherheit aufgezeigt. So soll der Einstieg in die zu untersuchende Thematik erleichtert werden. Dazu zählen neben der Maschinenrichtlinie auch harmonisierte Normen wie die EN 280 – Fahrbare Hubarbeitsbühnen sowie die EN 1495 – Hebebühnen - Mastgeführte Kletterbühnen. Ein weiterer Teil der theoretischen Grundlage wird die CE-Kennzeichnung sein und der Zweck und die Erstellung einer Risikobeurteilung.

Nachfolgend wird das Projekt STEP umfassend im Hinblick auf die Funktion und die funktionale Sicherheit beschrieben. Daraus hervorgehende Sicherheitsmechanismen werden in einem weiteren Schritt der Arbeit spezifiziert und mit dem bereits bestehenden Sicherheitskonzept eines Prototyps verglichen.

[1] IEC 61508-4:2010 (2010), S. 11.

Als Quellen für die vorliegende Masterarbeit dienen Fachliteratur, Richtlinien und Normen sowie Internetrecherchen. Technische Details basieren auf Gesprächen mit Fachverantwortlichen sowie externen Partnern der Hubert Palfinger Technologies GmbH.

1.5 Die Hubert Palfinger Technologies GmbH

Das Unternehmen Hubert Palfinger Technologies GmbH ist ein international agierendes Unternehmen in einem speziellen Segment des Sondermaschinenbaus. Die Tätigkeitsschwerpunkte sind die Entwicklung, Herstellung und der Vertrieb von spezifischen Zugangs- und Bearbeitungssystemen für die Schifffahrts- und Offshore-Industrie.

Der Palfinger Marine Sektor wurde im Jahr 1992 gegründet. Dieser umfasste anfangs die Herstellung von Marinekränen. Im Jahr 2000 wurde HTC-Systems gegründet, eine Entwicklungsabteilung innerhalb der Palfinger AG, die sich mit innovativen Korrosionsschutzmethoden und Zugangssystemen im maritimen Bereich beschäftigt hat. Die Abkürzung HTC steht für Hull Treatment Carrier. Aus diesen beiden Bereichen entstand nach diversen Namensänderungen im Jahr 2008 die Palfinger Systems GmbH als eigenständiges Unternehmen außerhalb der Palfinger-Gruppe mit Produktionsstätten in Marburg/Slowenien, Rijeka/Kroatien und Admont/Österreich. Im November 2010 wurde die Marinekran-Abteilung inklusive der Werke in Marburg und Rijeka in die Palfinger-Gruppe eingegliedert. Seitdem fokussiert das Unternehmen ausschließlich die Entwicklung und Herstellung von innovativen Zugangs- und Wartungssystemen für die Schifffahrts- und Offshore-Industrie. Die Zugangssysteme werden, abhängig vom jeweiligen Produkt, auch zur Miete angeboten. Im Herbst 2015 wurde das Unternehmen in Hubert Palfinger Technologies GmbH umfirmiert.[2]

Im Mai 2017 beschäftigte das Unternehmen 76 Mitarbeiterinnen und Mitarbeiter aus sieben Nationen, davon 34 Angestellte und 42 Arbeiter. Lehrlinge werden derzeit nicht ausgebildet. Der Hauptsitz der Hubert Palfinger Technologies GmbH ist in Salzburg. Zudem verfügt das Unternehmen über ein Produktions- und Montagewerk in Weng bei Admont in der Steiermark. Weitere Standorte befinden sich in Hamburg/Deutschland und in Singapur.

[2] Vgl. Hubert Palfinger Technologies GmbH (2017), Online-Quelle [12.09.2017]

2 GESETZE, RICHTLINIEN UND NORMEN

Die EU-Kommission beziehungsweise der Rat der Europäischen Union hat verschiedene Richtlinien erlassen, um die Grundgedanken der Europäischen Gemeinschaft, nämlich den Schutz der Bürgerinnen und Bürger im privaten sowie im beruflichen Umfeld und den freien Warenverkehr zu verwirklichen. Diese Richtlinien müssen von den 28 Mitgliedsstaaten in nationale Gesetze umgesetzt werden. Grundsätzliche Ziele und Anforderungen sind in den Richtlinien definiert und so weit wie möglich technologieneutral gehalten. So wurden im Bereich der Maschinensicherheit und im Arbeitsschutz unter anderem folgende Richtlinien erlassen:[3]

- die Maschinenrichtlinie 2006/42/EG, die sich an den Hersteller von Maschinen richtet
- die Arbeitsmittelbenutzungsrichtlinie 89/655/EWG, die sich an den Betreiber von Maschinen richtet
- zusätzliche Richtlinien, wie zum Beispiel die Niederspannungsrichtlinie, die EMV-Richtlinie oder die ATEX-Richtlinie

Veröffentlicht werden diese im Amtsblatt der Europäischen Union.

2.1 Harmonisierte Normen

Die Maschinenrichtlinie sieht folgende Definition für harmonisierte Normen vor:[4]

Eine harmonisierte Norm ist eine nicht verbindliche technische Spezifikation, die von einer europäischen Normenorganisation aufgrund eines Auftrages der Europäischen Kommission, nach einem festgelegten Verfahren, angenommen wurde.

Zu den europäischen Normenorganisationen gehören:

- Das Europäische Komitee für Normen (CEN)
- Das Europäische Komitee für Elektrotechnische Normung (Cenelec)
- Das Europäische Institut für Telekommunikationsnormen (ETSI)

Harmonisierte Normen dienen der Umsetzung der produktbezogenen Europäischen Richtlinien, wie es die Maschinenrichtlinie zum Beispiel ist. Im Amtsblatt der Europäischen Union werden harmonisierte Normen bekannt gegeben. Für den Inhalt der Normen sind die oben aufgelisteten europäischen Normenorganisationen verantwortlich. Die harmonisierten Normen müssen dann als nationale Normen umgesetzt werden. Sollten zu diesem Zeitpunkt nationale Normen im Widerspruch zu den harmonisierten Normen stehen, müssen diese zurückgezogen werden. Veröffentlicht werden harmonisierte Normen in Österreich im Bundesgesetzblatt.

Wird für die Herstellung einer Maschine eine harmonisierte Norm herangezogen, die im Amtsblatt der Europäischen Union veröffentlicht wurde, so kann von einer Konformitätsvermutung ausgegangen werden.

[3] Vgl. European Commission (2017), Online-Quelle [13.11.2017]

[4] Vgl. Maschinenrichtlinie (2006), S. 28.

Die grundlegenden Sicherheits- und Gesundheitsschutzanforderungen entsprechen dieser harmonisierten Norm.[5]

2.2 Klassifizierung von Normen

Grundsätzlich werden Normen im Amtsblatt der Europäischen Union veröffentlicht. Mögliche Änderungen in Normen werden ebenso im Amtsblatt kundgetan und sind auch im Namen der jeweiligen Norm vermerkt.

Normen werden im Rahmen der MRL, ausgehend vom Amtsblatt der Europäischen Union wie folgt klassifiziert:[6]

- **Typ-A-Normen** (Sicherheitsgrundnormen) behandeln Grundbegriffe, Gestaltungsleitsätze und allgemeine Aspekte, die auf Maschinen angewandt werden können;
  Als Beispiel sei hier in Bezug auf die Maschinenrichtlinie die EN ISO 12100:2010 erwähnt.
- **Typ-B-Normen** (Sicherheitsfachgrundnormen) behandeln einen Sicherheitsaspekt oder eine Art von Schutzeinrichtungen, die für eine ganze Reihe von Maschinen verwendet werden können:
  - **Typ-B1-Normen** für bestimmte Sicherheitsaspekte (z. B. Sicherheitsabstände, Oberflächentemperatur, Lärm);
  - **Typ-B2-Normen** für Schutzeinrichtungen (z. B. Zweihandschaltungen, Verriegelungseinrichtungen, druckempfindliche Schutzeinrichtungen, trennende Schutzeinrichtungen);

  Beispiel für Typ-B-Normen sind die EN ISO 13849-1:2015 sowie die EN ISO 13849-2:2012. Beide Normen sind essentielle Normen bei der Erstellung dieser Arbeit.
- **Typ-C-Normen** (Maschinensicherheitsnormen) behandeln detaillierte Sicherheitsanforderungen an eine bestimmte Maschine oder Gruppe von Maschinen.
  Beispiele für Typ-C-Normen, die auch im Projekt STEP von großer Bedeutung sind, sind die EN 280:2013 (Fahrbare Hubarbeitsbühnen - Berechnung - Standsicherheit - Bau - Sicherheit - Prüfungen) sowie die EN 1495:1997 (Hebebühnen - Mastgeführte Kletterbühnen)

Typ-A und Typ-B Normen sind sogenannte Grundnormen und lassen sich immer anwenden. Sie sind allgemeingültig, können aber oft nur schwer bei speziellen Maschinen umgesetzt werden. Dafür gibt es Typ-C-Normen. Diese Art der Normen sind auf spezielle Risiken einer Maschinenart ausgerichtet und bieten somit zielgerichtete Ansätze zur Risikoreduzierung. Im Fall des STEPs sind die EN 280:2013 und die EN 1495:1997 zutreffend.

[5] Vgl. Maschinenrichtlinie (2006), S. 29.

[6] Vgl. EN ISO 12100:2010 (2010), S. 5.

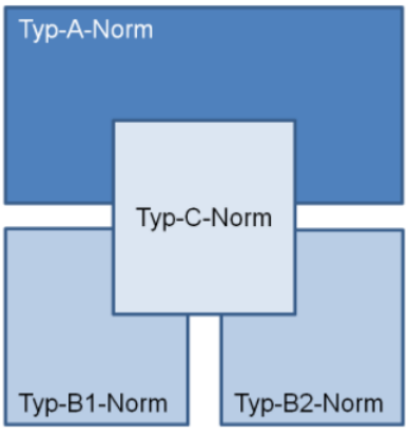


Abbildung 1: Klassifizierung von Normen und deren Zusammenspiel, Quelle: Ingenieurbüro Vogt (2017), Online-Quelle [20.08.2017]

Kommt es in einer Typ-C-Norm zu Unterscheidungen mit den Grundnormen, gelten für eine in Typ-C-Norm behandelte Maschine nicht mehr die Anforderungen aus Typ-A- oder Typ-B-Normen, sondern diejenigen aus der speziell für diesen Maschinentyp geltenden Norm. Dabei ist es auch möglich, dass nur bestimmte Teile einer Maschine in eine Typ-C-Norm fallen. Dies ist dann sachlich gut begründet zu dokumentieren.[7]

2.3 Wer ist für die Sicherheit einer Maschine verantwortlich?

Unterschiedliche Lebensphasen einer Maschine ergeben auch unterschiedliche, sicherheitstechnische Verantwortlichkeiten und Aufgaben. Dies betrifft sowohl den Hersteller als auch den Betreiber einer Maschine.

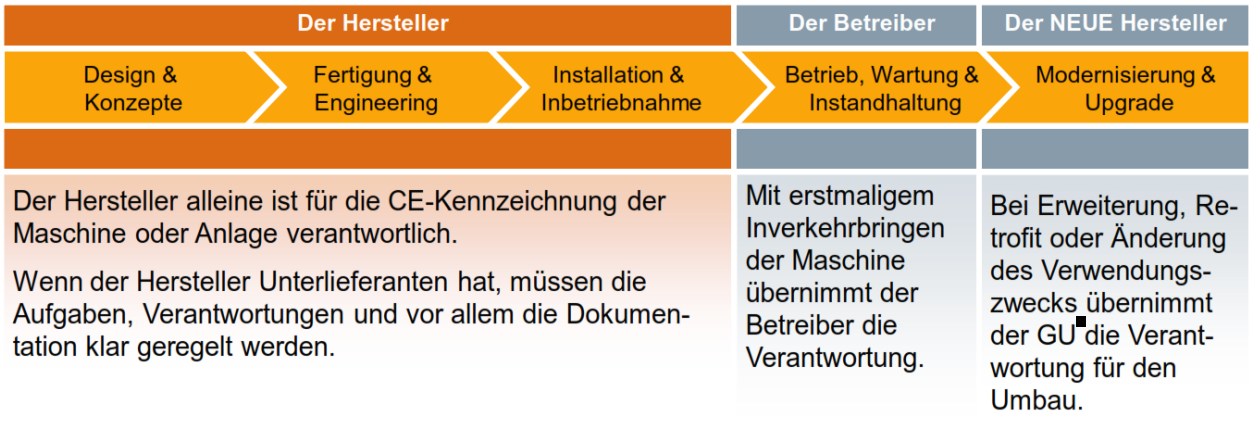


Abbildung 2: Die Abbildung zeigt die sicherheitstechnischen Aufgaben und Verantwortungen in jeder Lebensphase einer Maschine oder Anlage. Quelle: Siemens AG (2014), Online-Quelle [08.08.2017]

[7] Vgl. Ingenieurbüro Vogt (2017), Online-Quelle [20.08.2017]

* Generalunternehmer

2.4 Änderungen an einer Maschine

Grundsätzlich wird zwischen Umbau und Austausch unterschieden, wobei ein Austausch keine Änderung an der Maschine darstellt. Unter Austausch wird zum Beispiel das Tauschen von Verschleißteilen oder das Tauschen von Werkzeug verstanden.

Beispiele für einen Umbau sind der Austausch nicht gleichwertiger Teile oder vom Hersteller nichtvorgesehene Veränderungen. Auch der Austausch einer Schutztüre durch ein Lichtgitter stellt einen Umbau dar. Entscheidend bei Umbauten ist immer ob der Umbau zu einer neuen Gefahr führt oder nicht.

Werden Umbauten an einer Maschine durchgeführt, die unter Anhang IV der MRL fallen, ist die benannte Stelle, in deren Besitz sich die technischen Unterlagen der EG-Baumusterprüfbescheinigung befinden, zu informieren. Nach einer Prüfung durch die benannte Stelle wird die Gültigkeit der EG-Baumusterprüfbescheinigung bestätigt oder gegebenenfalls eine neue Bescheinigung ausgestellt.[8]

2.5 Der Weg zur sicheren Maschine

In Abbildung 3 ist der Weg zur sicheren Maschine skizziert. Sowohl für den Hersteller als auch für den Betreiber. Geregelt ist dies im Vertrag über die Arbeitsweise der Europäischen Union im Artikel 114 beziehungsweise im Artikel 153.

[8] Vgl. Maschinenrichtlinie (2006), S. 74.

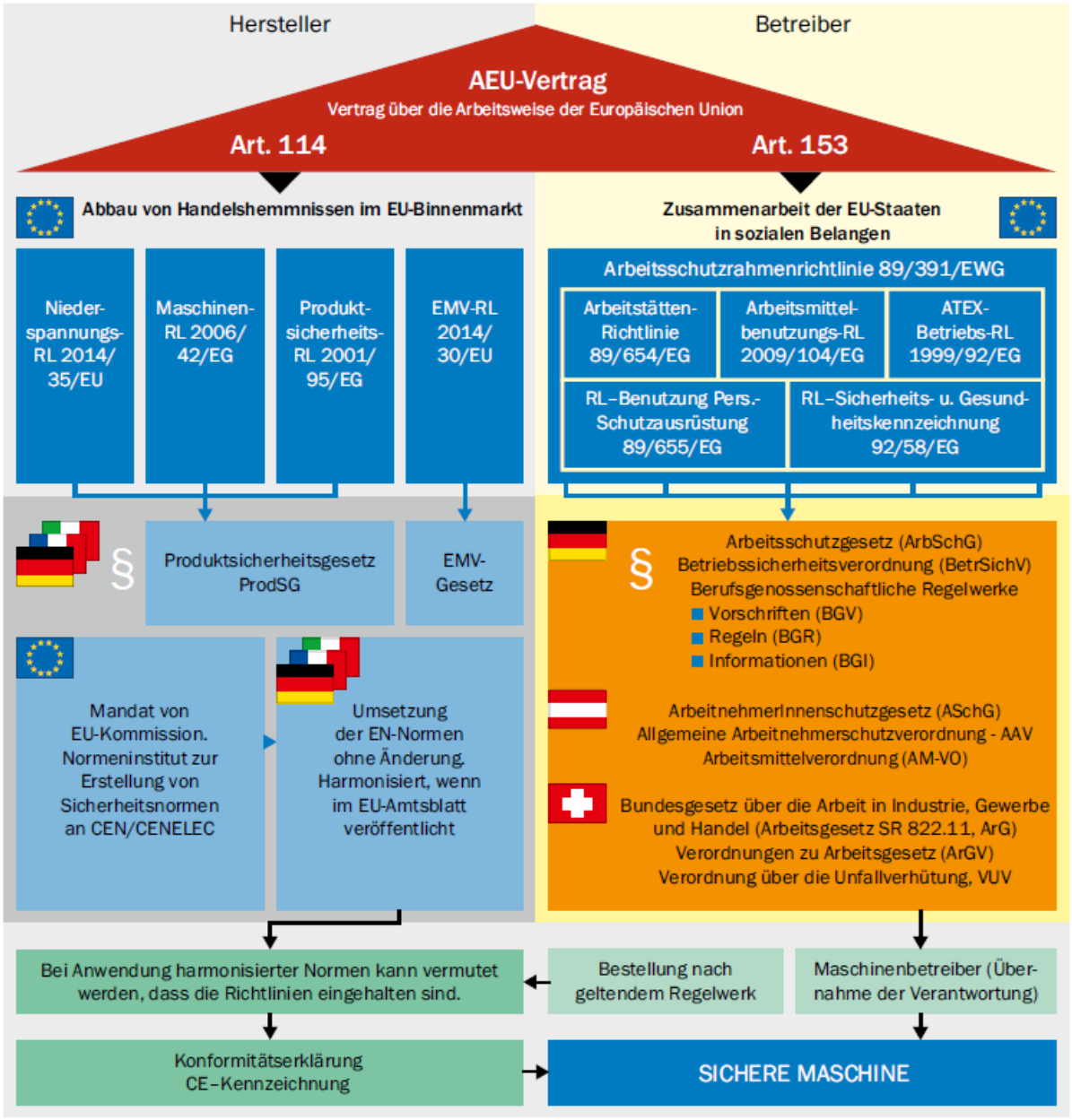


Abbildung 3: Diese Abbildung zeigt den Weg zu einer sicheren Maschine, Quelle: Kurrus/u.a. (2016), Online-Quelle [08.08.2017], S. 4.

Die nationale Umsetzung der Maschinenrichtlinie (MRL) erfolgt in Deutschland über das Produktsicherheitsgesetz, siehe Abbildung 3. In Österreich wird die Umsetzung der MRL über die Maschinensicherheitsverordnung 2010 sichergestellt. Im Detail wird darauf im Kapitel 3 - Die Maschinenrichtlinie - Richtlinie 2006/42/EG – eingegangen.

3 DIE MASCHINENRICHTLINIE - RICHTLINIE 2006/42/EG

Die MRL wurde im Juni 1989 unter dem Namen „Richtlinie 89/392/EG“ das erste Mal veröffentlicht. Das damalige Ziel war die technischen Rechtsvorschriften und Normen europaweit zu vereinheitlichen. Mittlerweile wurde die Richtlinie mehrfach erneuert und dient als Rechtsrahmen bei der Konstruktion von Maschinen. Sie regelt das einheitliche Schutzniveau zur Unfallverhütung für Maschinen und unvollständigen Maschinen bei der Inverkehrbringung. Gültigkeit hat die Maschinenrichtlinie innerhalb des europäischen Wirtschaftsraumes (EWR) und über bilaterale Verträge auch unter anderem in der Türkei und der Schweiz. Über die Jahre wurde mit zunehmender Komplexität der Maschinen die Richtlinie immer wieder erweitert. Im Jahr 1993 wurde der Begriff der CE-Kennzeichnung eingeführt.[9]

Im Mai 2006 wurde die jetzt gültige MRL unterzeichnet und ein Monat später im Amtsblatt der Europäischen Union veröffentlicht. Die MRL musste zwei Jahre nach Inkrafttreten in die nationalen Regelungen aufgenommen werden. 18 Monate später musste die neue MRL angewandt werden. Maschinen, die dann nicht der neuen MRL entsprachen, durften nicht mehr in Verkehr gebracht werden.[10]

3.1 Ziele der Maschinenrichtlinie

Die Philosophie der Maschinenrichtlinie bezüglich Konstruktion, Fertigung, Bau und sicherem Betrieb einer Maschine wird im Absatz 1.1.2 a) folgendermaßen zusammengefasst:[11]

„Die Maschine ist so zu konstruieren und zu bauen, dass sie ihrer Funktion gerecht wird und unter den vorgesehenen Bedingungen — aber auch unter Berücksichtigung einer vernünftigerweise vorhersehbaren Fehlanwendung der Maschine — Betrieb, Einrichten und Wartung erfolgen kann, ohne dass Personen einer Gefährdung ausgesetzt sind.

Die getroffenen Maßnahmen müssen darauf abzielen, Risiken während der voraussichtlichen Lebensdauer der Maschine zu beseitigen, einschließlich der Zeit, in der die Maschine transportiert, montiert, demontiert, außer Betrieb gesetzt und entsorgt wird.“[12]

Bei der Lösungsfindung zur Integration der Sicherheit hat der Hersteller folgende Grundsätze in der angegebenen Reihenfolge einzuhalten:

- Beseitigung oder Minderung der Risiken durch konstruktive Maßnahmen
- Ergreifen von Schutzmaßnahmen gegen Risiken, die sich nicht beseitigen lassen
- Unterrichten der Benutzer über etwaige Restrisiken

Das Risiko ist in der Norm wie folgt definiert:

„[…] die Kombination aus der Wahrscheinlichkeit und der Schwere einer Verletzung oder eines

[9] Vgl. Kringf (2014), Online-Quelle [25.08.2017]

[10] Vgl. Kirchberg (2006), S. 3.

[11] Vgl. Maschinenrichtlinie (2006), S. 36.

[12] Maschinenrichtlinie (2006), S. 36.

Gesundheitsschadens, die in einer Gefährdungssituation eintreten können;“[13]

In der Betriebsanleitung muss der Hersteller unter anderem die bestimmungsgemäße Verwendung der Maschine beschreiben beziehungsweise muss der Hersteller jede vernünftigerweise vorhersehbare Fehlanwendung der Maschine berücksichtigen.

3.2 Aufbau der Maschinenrichtlinie

Die MRL in ihrer aktuellen gültigen Fassung besteht aus 29 Artikeln und zwölf Anhängen. In den Artikeln sind allgemeine Informationen, Begriffsbestimmungen, Anwendungsbereiche und dergleichen zu finden. In den zwölf Anhängen der MRL werden unter anderem allgemeine Grundsätze zu grundlegenden Sicherheits- und Gesundheitsschutzanforderungen für Konstruktion und Bau von Maschinen angeführt.

3.3 Anwendung der Maschinenrichtlinie

Die richtlinienkonforme Anwendung der MRL bringt etliche Vorteile mit sich:[14]

Die Anwendung der MRL ist in allen EU-Mitgliedstaaten vorgeschrieben, da sie ein europäisches Gesetz darstellt. Neben den unbestreitbaren Vorteilen, die die MRL mit sich bringt, kann die Nichteinhaltung schwerwiegende Folgen nach sich ziehen. So gilt die Einhaltung der gemeinsamen Richtlinie als Schlüssel für den freien Warenverkehr innerhalb des EWR und zum Teil auch über die Grenzen hinaus, Stichwort bilaterale Abkommen. Der Hersteller profitiert auch von der damit einhergehenden Rechtssicherheit, da bei richtlinienkonformer Herstellung die Konformitätsvermutung gilt.

Des Weiteren schützt die Anwendung harmonisierter Normen vor unsicheren Billigprodukten. So dürfen Produkte, die keine CE-Kennzeichnung besitzen, die Binnenmarktgrenzen nicht überschreiten. Zu guter Letzt erspart die Einhaltung der MRL und deren Sicherheitsprozesse während der Konstruktion und dem Bau der Maschine teure Schutzmaßnahmen und kann im gesamten EWR auf den Markt gebracht werden, ohne teure Anpassungen an nichtharmonisierte Standards durchführen zu müssen.

3.3.1 Welche Maschinen fallen unter die Maschinenrichtlinie

Unter den Anwendungsbereich der MRL fallen laut Artikel 1.1 folgende Erzeugnisse:[15]

- Maschinen
- Auswechselbare Ausrüstung
- Sicherheitsbauteile
- Lastaufnahmemittel
- Ketten, Seile und Gurte
- Abnehmbare Gelenkwellen

[13] Maschinenrichtlinie (2006), S. 35.

[14] Vgl. Walther (2015), Online-Quelle [26.08.2017]

[15] Vgl. Maschinenrichtlinie (2006), S. 26.

- Unvollständige Maschinen

Ausgenommen vom Anwendungsbereich der MRL sind neben anderen zum Beispiel:[16]

- Spezielle Einrichtungen auf Jahrmärkten und Vergnügungsparks
- Waffen einschließlich Feuerwaffen
- Seeschiffe und bewegliche Offshore-Anlagen
- Kraftfahrzeuge und Kraftfahrzeuganhänger
- Maschinen für militärische Zwecke

3.3.2 Maschine laut Maschinenrichtlinie

Ein Erzeugnis gilt nach Artikel 2 a) der MRL als Maschine, wenn gewisse Kriterien erfüllt werden. Zum Beispiel gelten Produkte mit Teilen oder Vorrichtungen, die nicht in ihrer Gesamtheit miteinander verbunden sind, nicht als Maschine. Werden Teile einer Maschine nur wegen Transportgründen abgebaut, gilt sie sehr wohl als Maschine. In diesem Fall muss sie jedoch so konstruiert werden, dass Montagefehler beim Aufbau der Maschine ausgeschlossen sind, selbst wenn die Montage von Laien durchgeführt wird. Der Hersteller ist verpflichtet eine Montageanleitung mitzuliefern.[17]

Eine Maschine gilt laut MRL nicht als Maschine, wenn sie keine beweglichen Teile hat. Außerdem müssen die beweglichen Teile der Maschine mindestens durch ein oder mehrere Antriebssysteme angetrieben werden. Ob die Maschine dabei von einem Motor angetrieben wird oder mechanische Energie von einer anderen Maschine bereitgestellt wird, spielt dabei keine Rolle.

Im Fall, dass die Maschine ohne Antriebssystem geliefert wird, muss der Hersteller:[18]

- sämtliche Risiken, auch jene die auf das Antriebssystem bezogen sind, in der Risikobeurteilung anführen
- in der Betriebsanleitung sämtliche Spezifikationen für das zu montierende Antriebssystem anführen
- die technischen Einzelheiten des Antriebssystems sowie die Montageanleitung in die Konformitätsbewertung miteinbeziehen
- dafür Sorge tragen, dass die CE-Kennzeichnung an der Maschine die technischen Einzelheiten und die Betriebsanleitung des Antriebssystems abdeckt

Werden die Punkte nicht erfüllt, gilt die Maschine als unvollständige Maschine, siehe MRL Artikel 2, Buchstabe g.

Bewegte Teile im Anwendungsbereich der MRL dürfen nicht von unmittelbarer menschlicher oder tierischer Kraft angetrieben werden. Somit fallen geschobene Rasenmäher, Handbohrmaschinen und von Hand geschobene Transportkarren nicht in den Anwendungsbereich der MRL. Diese Maschinen funktionieren

[16] Vgl. Maschinenrichtlinie (2006), S. 27.

[17] Vgl. Maschinenrichtlinie (2006), S. 27.

[18] Vgl. Fraser/u.a. (2010), S. 31.

nicht mehr, sobald die manuelle Kraft nicht mehr wirkt. Hebezeuge sind von dieser Regel ausgenommen. Wirkt die manuelle Krafteinwirkung nicht direkt, sondern wird gespeichert, zum Beispiel in hydraulischen oder pneumatischen Systemen, kommt die MRL sehr wohl zum Einsatz.[19]

3.3.3 Unvollständige Maschine

Eine unvollständige Maschine laut MRL ist eine Maschine, die in ihrer Gesamtheit aber keine bestimmte Funktion erfüllen kann. Außerdem kann sie die grundlegenden Sicherheits- und Gesundheitsschutzanforderungen in Anhang I nicht in vollem Umfang erfüllen. Eine unvollständige Maschine ist dazu bestimmt in anderen Maschinen oder anderen unvollständigen Maschinen eingebaut beziehungsweise mit ihnen zusammengefügt zu werden und bildet dann eine Maschine im Sinne der MRL. An einer unvollständigen Maschine müssen also weitere Montagearbeiten durchgeführt werden. In einer Einbauerklärung muss der Hersteller angeben, welche der grundlegenden Sicherheits- und Gesundheitsschutzanforderungen erfüllt wurden.[20]

3.3.4 Maschinen nach Anhang IV der Maschinenrichtlinie

Im Anhang IV der MRL sind Maschinen angeführt, bei denen von einem besonderen Gefahrenpotential auszugehen ist beziehungsweise Maschinen, die eine kritische Schutzfunktion erfüllen. Für diese Maschinen gilt auch ein besonderes Verfahren zur Erlangung der CE-Kennzeichnung. Unter Punkt 17 im Anhang IV der MRL fällt auch der STEP. Das umfassende Thema der CE-Kennzeichnung wird im Kapitel 4 aufgegriffen. Ebenso wird in diesem Kapitel auf die Unterschiede in der Erlangung der CE-Kennzeichnung für aufgelistete Maschinen im Anhang IV der MRL eingegangen.

3.4 Umsetzung der Maschinenrichtlinie

Die Umsetzung der MRL stellt viele Unternehmen vor große Herausforderungen. Die MRL ist sehr umfassend und doch sehr allgemein gehalten. Je komplexer und vor allem je spezieller die Maschine in ihrer Anwendung ist, desto schwerer wird die Umsetzung der MRL. Auf jeden Fall braucht der Hersteller einer Maschine fachkundiges Personal mit dem nötigen Know-how um die rechtskonforme Umsetzung der MRL zu gewährleisten.

3.5 Nationale Umsetzung – Maschinensicherheitsverordnung 2010

In Österreich wird mit der Maschinensicherheitsverordnung - 2010 (MSV) die MRL umgesetzt. Genauer gesagt ist es die 282. Verordnung des Bundesministers für Wirtschaft und Arbeit über die Sicherheit von Maschinen und von Sicherheitsbauteilen für Maschinen. Die MSV wurde am 31. Juli 2008 ausgegeben und ist mit 29. Dezember 2009 in Kraft getreten[21]. Die MSV besteht aus 22 Paragraphen, in der MRL Artikel benannt, und 15 Anhängen.

---

[19] Vgl. Fraser/u.a. (2010), S. 31 f.

[20] Vgl. Maschinenrichtlinie (2006), S. 28, 65, 72.

[21] Maschinensicherheitsverordnung (2008), S. 1, 10.

4 DIE CE-KENNZEICHNUNG

Das Anbringen der CE-Kennzeichnung ist für viele Produkte im Europäischen Binnenmarkt verpflichtend. Mit der CE-Kennzeichnung sollen die gleichen Anforderungen an Produkte gewährleistet sein und der freie Warenverkehr innerhalb der Europäischen Union nicht behindert werden. Die CE-Kennzeichnung wird durch Harmonisierungsvorschriften der Europäischen Union geregelt und durch das Konformitätsbewertungsverfahren festgestellt. Es muss vom Hersteller oder einem befugten Bevollmächtigen und vor Inverkehrbringen oder der Inbetriebnahme am Europäischen Binnenmarkt angebracht werden.[22]

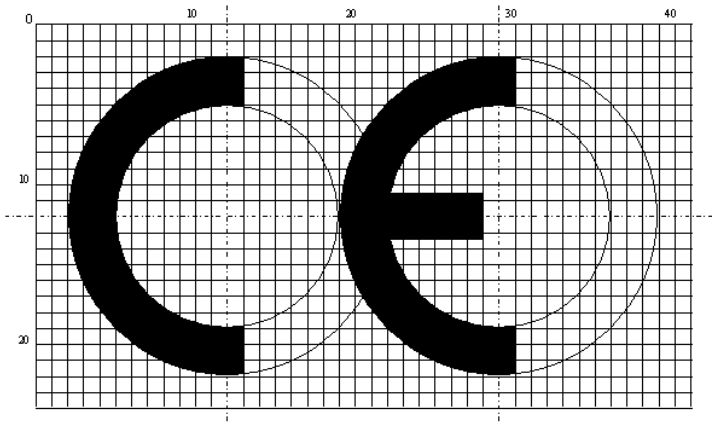


Abbildung 4: Richtlinienkonforme Darstellung der CE-Kennzeichnung;
Quelle: Unbekannt (2017), Online-Quelle [21.08.2017]

Wird die CE-Kennzeichnung kleiner oder größer dargestellt, müssen die gezeigten Proportionen eingehalten werden. Die Mindesthöhe beträgt 5 mm, Ausnahmen bestehen bei kleineren Maschinen. In diesem Fall kann es an der Verpackung und den Begleitunterlagen angebracht werden. Es ist in unmittelbarer Nähe der Angabe des Herstellers gut sichtbar, lesbar und dauerhaft anzubringen.[23]

4.1 Hersteller einer Maschine

In der Regel ist der Hersteller einer Maschine der Maschinen- und Anlagenbauer. Er ist verantwortlich für die Konstruktion und den Bau einer unter die Richtlinie fallenden Maschine oder unvollständigen Maschine. In den meisten Fällen ist der Hersteller der, der die Maschine in seinem Namen in Verkehr bringt. Aber auch wer den Verwendungszweck einer Maschine ändert oder eine Funktionserweiterung durchführt gilt als Hersteller. Das können Betreiber oder ein von ihm beauftragter Modernisierer sein. Wer eine Maschine aus einem Drittland importiert und somit die in der Richtlinie festgelegten Herstellerverpflichtungen übernimmt, gilt ebenfalls als Hersteller. Existiert kein Hersteller im Sinne dieser Definition, gilt als Hersteller jener, der die Maschine in Verkehr bringt oder in Betrieb nimmt.[24]

[22] Vgl. Wirtschaftskammer Österreich (2017), Online-Quelle [21.08.2017]

[23] Vgl. Maschinenrichtlinie (2006), S. 67.

[24] Vgl. Maschinenrichtlinie (2006), S. 28.

4.2 CE-Kennzeichnungspflicht für Produkte

EU-Richtlinien und Verordnungen schreiben fest welche Produkte, die im EWR in Verkehr gebracht werden, unter die CE-Kennzeichnungspflicht fallen.[25] Gibt es für eine Produktgruppe eine europäische Richtlinie oder Verordnung, gilt auch die CE-Kennzeichnungspflicht. Gilt für ein Produkt keine einzige CE-Rechtsvorschrift, ist die Anbringung der CE-Kennzeichnung nicht legitim. Als Ausnahme seien an dieser Stelle Verpackungen oder Verpackungsabfälle erwähnt.

„Sicher ist ein Produkt, das keine oder nur geringe mit der Verwendung des Erzeugnisses zu vereinbarende und unter Wahrung eines hohen Schutzniveaus für die Gesundheit und Sicherheit von Personen vertretbare Gefahren birgt.“[26]

Was nicht bedeutet, dass die Verwendung eben dieses Produktes nicht gefährlich ist. In manchen Fällen sind nicht alle Gefahrenstellen durch mechanische, elektrische beziehungsweise steuerungstechnische Lösungen zu entschärfen. Was bleibt ist ein Restrisiko, auf das zum Beispiel durch Piktogramme aufmerksam gemacht werden muss. Auf jeden Fall sind solche Restrisiken in der Betriebsanleitung zu dokumentieren.

4.3 Richtlinien und Verordnungen zur CE-Kennzeichnung

Wesentliche Anforderungen an die Sicherheit, Gesundheit, elektromagnetische Verträglichkeit, Energieeffizienz und so weiter werden für zahlreiche Produkte in den EU-Richtlinien und EU-Verordnungen zur CE-Kennzeichnung festgelegt. Diese müssen zur Erlangung der CE-Kennzeichnung von den Produkten erfüllt werden. Jeder Mitgliedstaat führt die EU-Richtlinien in nationale Richtlinien über. So ist zum Beispiel die Maschinenrichtlinie in Österreich in der Maschinensicherheitsverordnung umgesetzt.[27]

So gibt es Richtlinien für zum Beispiel folgende Produkte:[28]

- Aufzüge und Sicherheitsbauteile für Aufzüge – 2014/33/EU
- Druckbehälter – 2014/39/EU
- Druckgeräte – 2014/68/EU
- Explosionsschutz von Geräten und Schutzsystemen – 2014/34/EU
- Elektrische Betriebsmittel – 2014/35/EU
- Messgeräte – 2014/32/EU
- Maschinen – 2006/42/EC

Fehlen spezielle Rechtsvorschriften für die Sicherheit bestimmter Produkte oder weisen die CE-Bestimmungen bezüglich Produktsicherheit für ein gewisses Produkt Lücken auf, gilt für Verbraucherprodukte die EU-Richtlinie betreffend die Allgemeine Produktsicherheit.

---

[25] Vgl. Wirtschaftskammer Österreich (2017), Online-Quelle [21.08.2017]

[26] Wirtschaftskammer Österreich (2017), Online-Quelle [22.08.2017]

[27] Vgl. Wirtschaftskammer Österreich (2017), Online-Quelle [21.08.2017]

[28] Vgl. Kramer (2016), Online-Quelle [24.08.2017]

EU-Richtlinie betreffend die Allgemeine Produktsicherheit

Wie in Kapitel 4.3 angeführt, gilt die EU-Richtlinie betreffend die Allgemeine Produktsicherheit für Produkte, in denen das europäische Recht keine speziellen Vorschriften für die Sicherheit bestimmter Produktkategorien vorsieht. Erfasst sind allerdings nur Verbraucherprodukte wie Fahrräder, Möbel, Feuerzeuge oder zum Beispiel Grillgeräte und umgesetzt ist diese Richtlinie in Österreich im Produktsicherheitsgesetz.[29]

Wenn keine Vorschriften und keine Norm für ein Produkt bestehen, so ist es möglich die Beurteilung der Konformität anhand folgender Punkte durchzuführen: „

- der nicht bindenden nationalen Normen zur Durchführung anderer relevanter Europäischer Normen oder der Empfehlungen der Kommission zur Festlegung von Leitlinien für die Beurteilung der Produktsicherheit; oder
- der Normen des Mitgliedstaats, in dem das Produkt hergestellt worden ist oder vermarktet wird; oder
- der Verhaltensregeln zur Sicherheit und Gesundheit; oder
- des aktuellen Standes der Kenntnisse und der Technik; oder
- des Sicherheitsniveaus, das die Verbraucher erwarten können."[30]

4.4 Schritte zur CE-Kennzeichnung einer Maschine

Es gibt mehrere Möglichkeiten die CE-Kennzeichnung einer Maschine, die unter Anhang IV der Maschinenrichtlinie fällt oder auch nicht, zu erlangen. In der folgenden Abbildung sind die verschiedenen Wege dargestellt:

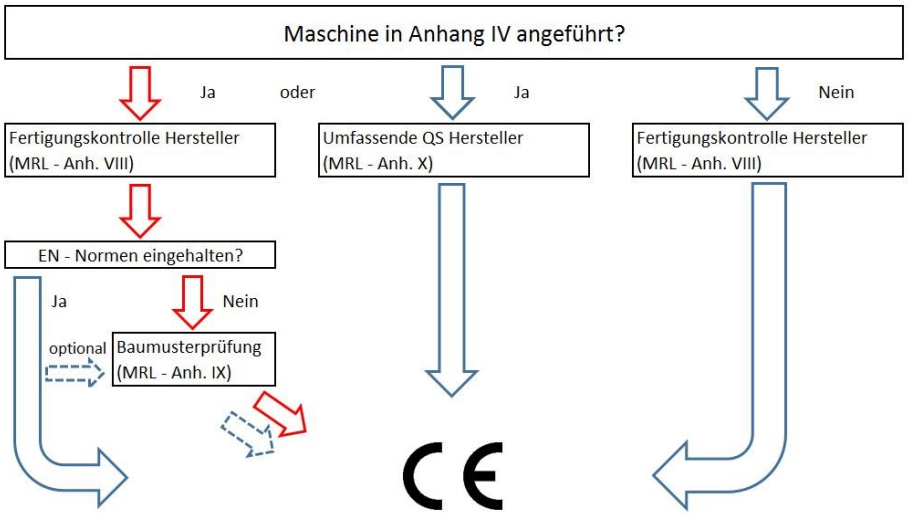


Abbildung 5: Möglichkeiten zur Erlangung der CE-Kennzeichnung, der rote Pfad ist bezogen auf den STEP, Quelle: Eigene Darstellung

[29] Vgl. Wirtschaftskammer Österreich (2017), Online-Quelle [22.08.2017]

[30] Wirtschaftskammer Österreich (2017), Online-Quelle [22.08.2017]

4.4.1 STEP – der Weg zur CE-Kennzeichnung

Am Beginn eines jeden Konformitätsbewertungsverfahrens müssen zutreffende Gesetze, Richtlinien und Normen eruiert werden. In Bezug auf den STEP können andere Richtlinien außer der Maschinenrichtlinie ausgeschlossen werden. Auch unter die von der MRL ausgenommenen Maschinen, siehe Punkt 3.3.1 fällt der STEP nicht.

Somit ist geklärt, dass der STEP unter Anhang IV der Maschinenrichtlinie, nämlich unter Punkt 17 fällt:

„Maschinen zum Heben von Personen oder von Personen und Gütern, bei denen die Gefährdung eines Absturzes aus einer Höhe von mehr als 3 m besteht.“[31]

Da die Firma HPT kein umfassendes Qualitätssicherungsverfahren nach Anhang X der Maschinenrichtlinie vorweisen kann und die Maschine keiner eindeutigen EN Norm zuzuordnen ist, bleibt nur die Möglichkeit einer Baumusterprüfung, nach Anhang IX der Maschinenrichtlinie um eine CE-Kennzeichnung für den STEP zu erhalten. Siehe dazu auch Abbildung 5.

4.4.2 STEP – EG-Baumusterprüfung

Wie schon in Kapitel 4.4.1 festgestellt, ist zur Erlangung der CE-Kennzeichnung beim STEP eine EG-Baumusterprüfung nach Maschinenrichtlinie - Anhang IX notwendig. Eine EG-Baumusterprüfung ist eine Art Prüfverfahren einer benannten Stelle, zum Beispiel TÜV. Dieses Verfahren wird zur Feststellung und Bescheinigung eines repräsentativen Musters, einer in Anhang IV der Maschinenrichtlinie genannten Maschine durchgeführt. Es bescheinigt, dass die Bestimmungen dieser Richtlinie erfüllt werden.

4.4.2.1 Benannte Stelle

Eine benannte Stelle ist eine akkreditierte Einrichtung, die eine Baumusterprüfung durchführen darf. Des Weitern darf eine benannte Stelle eine Baumusterprüfbescheinigung ausstellen. Benannte Stellen werden im Ministerium für Wissenschaft, Forschung und Wirtschaft gelistet.

4.4.2.2 Ablauf der EG-Baumusterprüfung

Die Maschinenrichtlinie sieht folgende Vorgehensweise vor:[32]

Die Firma HPT, als Hersteller, erstellt für den STEP die in Anhang VII Teil A geforderten technischen Unterlagen und reichen bei einer benannten Stelle ihrer Wahl einen Antrag ein. Der Antrag hat Name und Anschrift der Firma HPT, eine schriftliche Erklärung, dass nur diese benannte Stelle konsultiert wurde, sowie die technischen Unterlagen zu enthalten. Des Weiteren hat die Firma HPT das Baumuster, also die gesamte Maschine der benannten Stelle zur Verfügung zu stellen. Die benannte Stelle prüft daraufhin die technischen Unterlagen und führt erforderliche Prüfungen, Messungen und Versuche durch. Dadurch kann die benannte Stelle feststellen, ob grundlegende Sicherheits- und Gesundheitsschutzanforderungen beziehungsweise die zutreffenden harmonisierten Normen gewissenhaft angewandt wurden.

[31] Maschinenrichtlinie (2006), S. 68.

[32] Vgl. Maschinenrichtlinie (2006), S. 74.

Entspricht die Maschine laut der benannten Stelle den Bestimmungen, wird eine EG-Baumusterprüfbescheinigung ausgestellt. Sämtliche Unterlagen sowie eine Kopie der EG-Baumusterprüfbescheinigung werden sowohl vom Hersteller als auch von der benannten Stelle für 15 Jahre archiviert. Alle fünf Jahre hat der Hersteller bei der benannten Stelle eine Überprüfung der Gültigkeit der EG-Baumusterprüfbescheinigung zu beantragen.

Im Fall einer negativen Begutachtung wird die Ausstellung einer EG-Baumusterprüfbescheinigung verwehrt. In diesem Fall hat die benannte Stelle eine detaillierte Begründung abzuliefern. Des Weiteren werden die anderen benannten Stellen als auch der Mitgliedstaat darüber in Kenntnis gesetzt.

Werden Änderungen an der Maschine mit gültiger EG-Baumusterprüfbescheinigung vorgenommen, ist die benannte Stelle, die im Besitz der technischen Unterlagen ist, über diese Umbauten zu informieren. Änderungen werden geprüft und die Gültigkeit der EG-Baumusterprüfbescheinigung bestätigt beziehungsweise eine neue Bescheinigung ausgestellt.

Die benannte Stelle hat den Hersteller über Änderungen, die Auswirkungen auf die Gültigkeit der Bescheinigung haben könnten, zu informieren und kann gegebenenfalls auch Bescheinigungen zurückziehen. Vice versa hat der Hersteller die Verpflichtung die Maschine auf dem aktuellen Stand der Technik zu halten. Verliert die EG-Baumusterprüfbescheinigung ihre Gültigkeit, darf die Maschine nicht mehr in Verkehr gebracht werden.

4.5 EG-Konformitätserklärung

Wurde ein Konformitätsbewertungsverfahren durchgeführt und nachgewiesen, dass das Produkt den CE-Rechtsvorschriften entspricht, kann eine EG-Konformitätserklärung vom Hersteller ausgestellt werden. Die technischen Unterlagen sowie die Konformitätserklärung sind die wesentlichen Unterlagen für die CE-Kennzeichnung.

Die Konformität wird nicht nur für die MRL ausgestellt, sondern auch für andere zutreffende Richtlinien, wie zum Beispiel die Richtlinien für die Elektromagnetische Verträglichkeit, kurz EMV. Die Bestätigung der Konformität für verschiedene Richtlinien erfolgt in einem Dokument oder in mehreren. Eine Ausnahme gibt es bei der Niederspannungsrichtlinie. Diese ist bereits in der MRL enthalten. Dazu steht in der MRL im Anhang I - Grundlegende Sicherheits- und Gesundheitsschutzanforderungen für Konstruktion und Bau von Maschinen unter Punkt 1.5.1. folgende Anmerkung:

„Eine mit elektrischer Energie versorgte Maschine muss so konstruiert, gebaut und ausgerüstet sein, dass alle von Elektrizität ausgehenden Gefährdungen vermieden werden oder vermieden werden können.

Die Schutzziele der Richtlinie 73/23/EWG gelten für Maschinen. In Bezug auf die Gefährdungen, die von elektrischem Strom ausgehen, werden die Verpflichtungen betreffend die Konformitätsbewertung und das Inverkehrbringen und/oder die Inbetriebnahme von Maschinen jedoch ausschließlich durch die vorliegende Richtlinie geregelt.“[33]

[33] Maschinenrichtlinie (2006), S. 44.

5 DIE RISIKOBEURTEILUNG

Die MRL fordert dezidiert, dass der Hersteller einer Maschine eine Risikobeurteilung und die damit einhergehende Risikominderung durchzuführen hat. Dies wird im Anhang I – Allgemeine Grundsätze der MRL gefordert und die Risikobeurteilung ist Teil der technischen Dokumentation nach MRL Anhang VII.

Die entsprechenden Grundlagen für die Risikobeurteilung liefert die Grundnorm EN ISO 12100:2010 – Sicherheit von Maschinen. In dieser harmonisierten europäischen Norm werden Gestaltungsleitsätze und Begriffsbestimmungen angeführt. Sicherheit von Maschinen bedeutet in Bezug auf die Risikobeurteilung, dass in jeder Lebensphase der Maschine die Funktion erfüllt ist und mögliche Risiken reduziert wurden.[34]

5.1 Zweck einer Risikobeurteilung

Durch die Durchführung einer Risikobeurteilung soll die Konstruktion sicherer Maschinen gewährleistet werden. Durch die systematische Methode der Risikobeurteilung sollen bereits während der Konzeptphase einer Maschine Gefährdungen und Risiken erkannt werden. Die Identifizierung von Gefährdungen und Risiken noch während der Entwurfsphase, sind in der Regel kostengünstiger und vor allem wirkungsvoller. Änderungen an der Maschine zu einem späteren Zeitpunkt können die Kosten in die Höhe treiben und führen meist zu aufwendigen Schutzvorrichtungen oder schränken die Einsatzmöglichkeiten der Maschine ein. Die Inverkehrbringung einer Maschine darf nur im sicheren Zustand erfolgen. Restrisiken lassen sich nicht vermeiden. Diese müssen allerdings in einem akzeptablen Bereich unter einer Grenze liegen, siehe Abbildung 6.

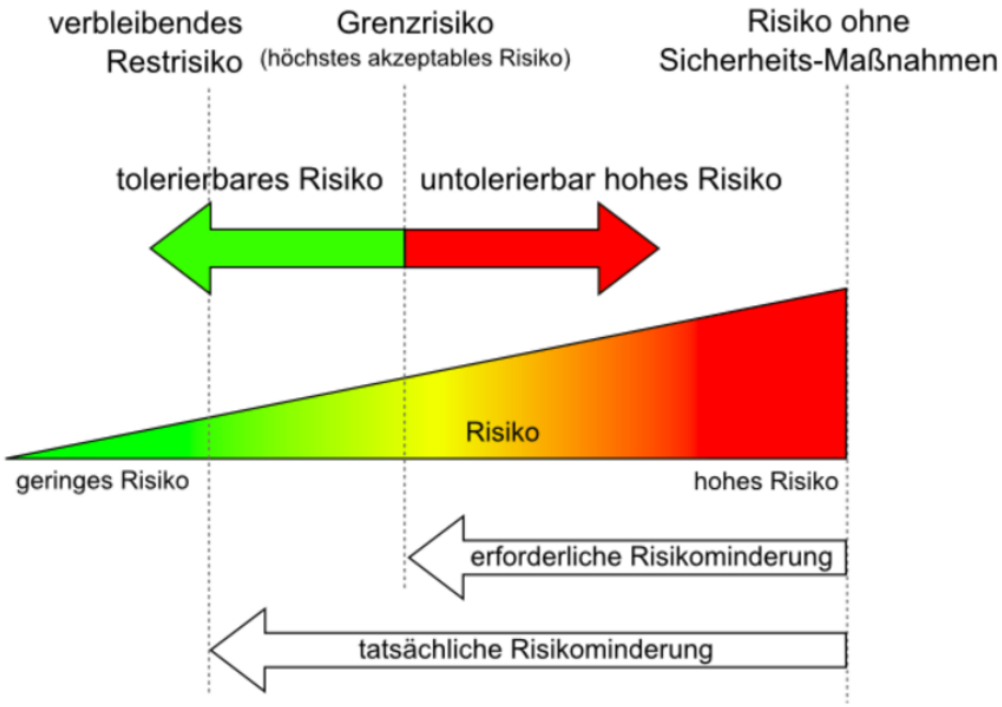


Abbildung 6: Grenzrisiko bei der Risikobeurteilung, Quelle: Agerer (2016), Online-Quelle [31.08.2017]

[34] Vgl. Agerer (2016), Online-Quelle [31.08.2017]

Akzeptables Grenzrisiko

Zu klären gilt wo das akzeptable Grenzrisiko liegt. Am Arbeitsplatz setzt sich niemand freiwillig einem Risiko aus, im Gegensatz zu manchen Freizeitaktivitäten. Deswegen muss differenziert unterschieden werden. Am Arbeitsplatz erfolgt die Festlegung des Grenzrisikos deshalb anhand von gültigen Wertvorstellungen der Gesellschaft. In technischen Regeln, Unfallverhütungsvorschriften und Normen wird der Grenzwert für das Grenzrisiko definiert.[35]

5.2 Ablauf einer Risikobeurteilung

In Abbildung 9 ist der Prozess der Risikobeurteilung dargestellt. Wichtig in diesem Zusammenhang ist die Terminologie. Risikoanalyse ist nicht gleich Risikobeurteilung. Die Risikobeurteilung besteht aus einer Risikoanalyse und einer Risikobewertung. Im Detail wird in den folgenden Kapiteln auf die unterschiedlichen Stufen der Risikobeurteilung eingegangen.

5.2.1 Risikoanalyse

Bei der Risikoanalyse werden jene Informationen erhoben, welche zur Risikobewertung benötigt werden. Die Risikoanalyse besteht aus folgenden drei Punkten:

1. Festlegung der Grenzen der Maschine
2. Identifizierung der Gefährdungen
3. Risikoeinschätzung

Diese Informationen liefern die Basis zur Entscheidung ob eine Risikominderung erforderlich ist oder nicht.

5.2.1.1 Festlegung der Grenzen der Maschine

Am Beginn der Risikobeurteilung steht das Festlegen der Grenzen der Maschine. Dabei müssen sämtliche Phasen der Lebensdauer der Maschine berücksichtigt werden. Genau bestimmt werden müssen die Merkmale, die Leistung der Maschine sowie die am Maschinenprozess beteiligten Personen, die Umgebung und die im Zusammenhang mit der Maschine stehenden Produkte.[36]

Bei der Festlegung der Grenzen werden laut EN ISO 12100:2010 folgende Unterscheidungen gemacht:

- Verwendungsgrenzen z.B.: verschiedene Betriebsarten der Maschine, Einsatzbereich der Maschine wie Industrie oder Gewerbe, Bedienpersonal usw.
- Räumliche Grenzen z.B.: Bewegungsraum, Platzbedarf von Personen und Wechselwirkung zwischen Mensch und Maschine
- Zeitliche Grenzen z.B.: Grenze der Lebensdauer der Maschine und beziehungsweise oder deren Bauteile
- Weitere Grenzen z.B.: Eigenschaften des zu verarbeiteten Materials, Sauberkeit der Maschine, Umgebung: Innenraum oder im Freien, Sonneneinstrahlung udg.

[35] Vgl. Agerer (2016), Online-Quelle [02.09.2017]

[36] Vgl. EN ISO 12100:2010 (2010), S. 19.

5.2.1.2 Identifizierung der Gefährdungen

Zur Identifizierung der Gefährdungen ist der Norm folgendes zu entnehmen:[37]

Wurden die Grenzen festgelegt, muss im nächsten Schritt die systematische Identifizierung der vorhersehbaren dauerhaften und unerwartet auftretenden Gefährdungen, Gefahrensituationen und Gefährdungsereignisse erfolgen und zwar in allen Phasen der Lebensdauer der Maschine.

Die zu berücksichtigenden Phasen der Lebensdauer sind:

- Transport
- Montage, Programmierung
- Inbetriebnahme
- Verwendung, Normalbetrieb
- Fehlerfall, Fehlersuche, Wartung
- Reinigung, Instandhaltung
- Demontage, Außerbetriebnahme und die Entsorgung

Erst nach der Identifizierung der Gefährdungen können entsprechende Maßnahmen zur Minderung von Gefahren eingeleitet werden. Dazu müssen auch Arbeitsvorgänge, Aufgaben, die von Personen erfüllt werden, das Umfeld und dergleichen analysiert werden.

Im Besonderen sind dabei folgende Punkte zu berücksichtigen:

- Das Eingreifen durch Personen während der gesamten Lebensdauer der Maschine wie z.B.: das Umrüsten, das Prüfen, das Einrichten, das Reinigen oder das Stillsetzen der Maschine
- Mögliche Betriebszustände der Maschine wie z.B.: Normalbetrieb, Versagen der Maschine durch Störung von außen, Ausfall der Energieversorgung oder Software-Fehler
- Unbeabsichtigtes Verhalten des Bedienpersonals oder vernünftigerweise vorhersehbare Fehlanwendung der Maschine, wie Verlust der Kontrolle des Bedienpersonals, Verhalten durch Unachtsamkeit sowie Verhalten von bestimmten Personengruppen z.B.: Kinder

5.2.1.3 Risikoeinschätzung

Der letzte Schritt der Risikoanalyse ist die Risikoeinschätzung. Für die Risikoeinschätzung sieht die Norm folgendes vor:[38]

Der Zusammenhang zwischen Gefährdungssituation und Risiko hängt von folgenden Elementen ab:

1. dem Schadensausmaß
2. der Eintrittswahrscheinlichkeit dieses Schadens als Funktion
    a. der Gefährdungsexposition einer Person/von Personen
    b. des Eintritts eines Gefährdungsereignisses, sowie

[37] Vgl. EN ISO 12100:2010 (2010), S. 20 ff.

[38] Vgl. EN ISO 12100:2010 (2010), S. 23 ff.

c. der technischen und menschlichen Möglichkeiten zur Vermeidung oder Begrenzung des Schadens

In Abbildung 7 sind die Risikoelemente aus der EN ISO 12100:2010 dargestellt.

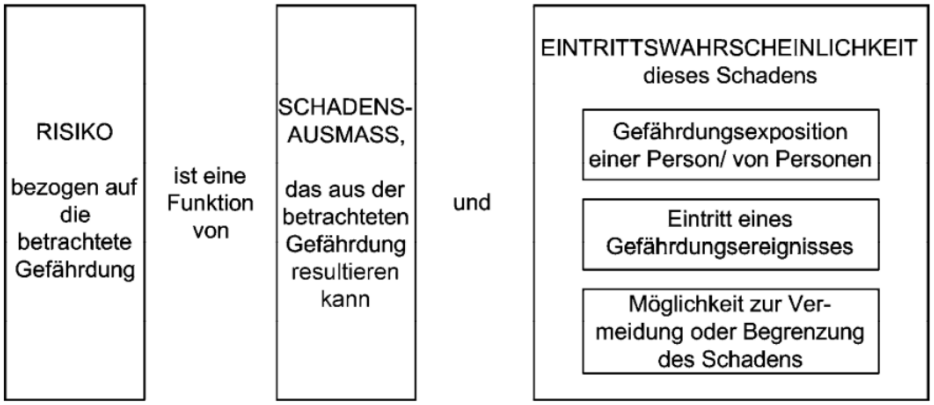


Abbildung 7: Risikoelemente nach EN ISO 21100:2010, Quelle: EN ISO 12100:2010 (2010), S. 24.

Das Schadensausmaß kann mittels folgender Kriterien eingestuft werden:[39]

- nach dem Ausmaß der Verletzungen beziehungsweise der Gesundheitsschädigung
  - leicht (reversible Verletzungen wie z.B.: Schnittwunden, Quetschungen)
  - schwer (irreversible Verletzungen wie z.B. der Verlust eines Fingers oder eines Arms)
  - tödlich
- dem Schadensumfang
  - eine Person
  - mehrerer Personen betroffen

5.2.1.4 Instrument zur Risikoeinschätzung

Zur Einschätzung des Risikos können mehrere Methoden herangezogen werden. Im Folgenden wird auf die Einschätzung mittels Risikograph eingegangen.

Zur Ermittlung des Risiko Index, der zwischen eins – niedriges Risiko und sechs – sehr hohes Risiko liegt, wird in vier Kategorien zwischen jeweils zwei Möglichkeiten unterschieden. Wurde eine Entscheidung getroffen, kann der Risiko Index direkt abgelesen werden, siehe Abbildung 8.

Unterschieden wird in folgenden Kategorien:[40]

- S: Schwere des Schadens
  - S1: leichte Verletzung (Kratzer, Schnitte, Quetschungen, kleine Wunden)
  - S2: schwere Verletzung, inklusive Todesfolge (gebrochene oder abgetrennte Gliedmaßen)
- F: Häufigkeit und/oder Dauer der Gefährdungsexposition
  - F1: zweimal oder weniger pro Arbeitsschicht oder weniger als 15 min pro Arbeitsschicht
  - F2: mehr als zweimal pro Arbeitsschicht oder mehr als insgesamt 15 min pro Arbeitsschicht

[39] Vgl. EN ISO 12100:2010 (2010), S. 24.

[40] Vgl. Blasge (2016), S. 57 ff.

- O: Wahrscheinlichkeit des Eintretens eines Gefährdungsereignisses
    - O1: bewährte Technik, geprüft und anerkannt sicher anwendbar
    - O2: technisches Versagen wurde in den vergangenen zwei Jahren festgestellt
    - O3: technisches Versagen wird regelmäßig festgestellt (alles sechs Monate oder öfter)
- A: Möglichkeit der Abwendung oder Minderung des Schadens
    - A1: möglich unter bestimmten Bedingungen
    - A2: unmöglich

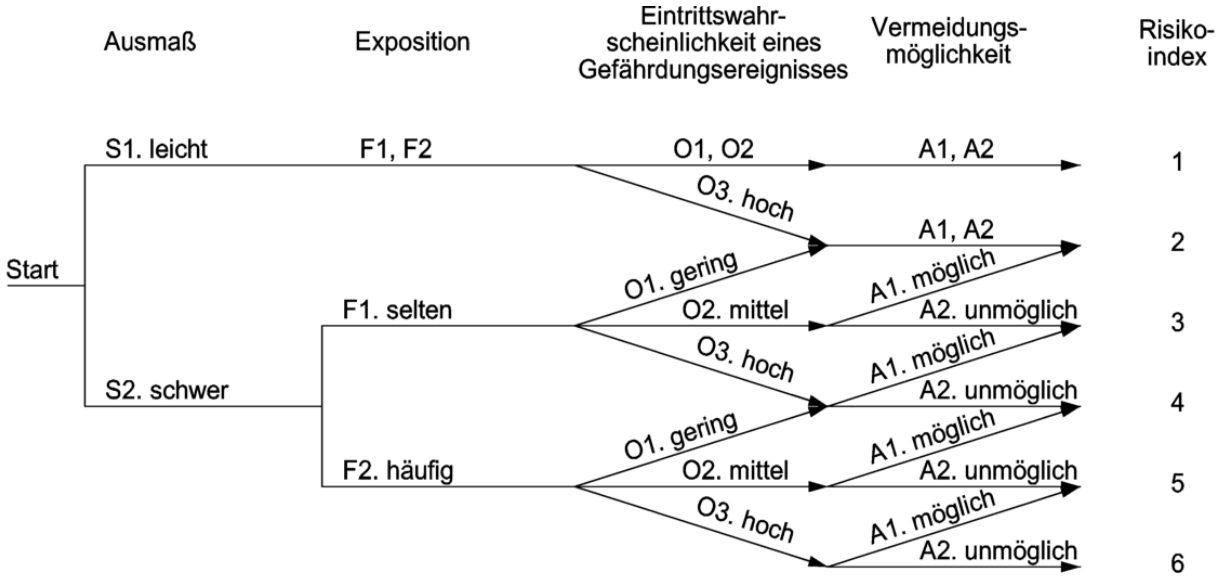


Abbildung 8: Risikograph als Hilfestellung für die Risikoeinschätzung, Quelle: ISO/TR 14121-2:2012 (2013), S. 19.

5.2.2 Risikobewertung

Bei der Risikobewertung wird für jedes bekannte Risiko eine Gefährdungsanalyse hinsichtlich Schadensausmaß, Eintrittswahrscheinlichkeit und Vermeidbarkeit durchgeführt und somit das Risiko eingestuft. Anhand dieser Einstufung wird bewertet, ob Maßnahmen zur Risikominderung erforderlich sind oder ob von einem akzeptablen Restrisiko ausgegangen wird.[41]

Liegt das jeweilige Risiko über dem akzeptablen Grenzrisiko, siehe Abbildung 6, muss eine Risikominderung durchgeführt werden. Dazu müssen risikomindernde Maßnahmen generiert werden bevor eine neuerliche Risikobewertung durchgeführt wird. Wurde das Risiko hinreichend minimiert, ist der Fall für dieses Risiko erledigt. Sollte dies nicht der Fall sein, startet der Prozess von vorne. Siehe dazu Abbildung 9.

Bei Risikominderung kommt das „Drei-Stufen-Verfahren“ zur Anwendung, siehe dazu auch Abbildung 10:

- 1. Stufe: Inhärent sichere Konstruktion
- 2. Stufe: Technische Schutzmaßnahmen und ergänzende Schutzmaßnahmen
- 3. Stufe: Benutzerinformation

[41] Vgl. Agerer (2016), Online-Quelle [02.09.2017]

5.3 Informationen zur Risikobeurteilung

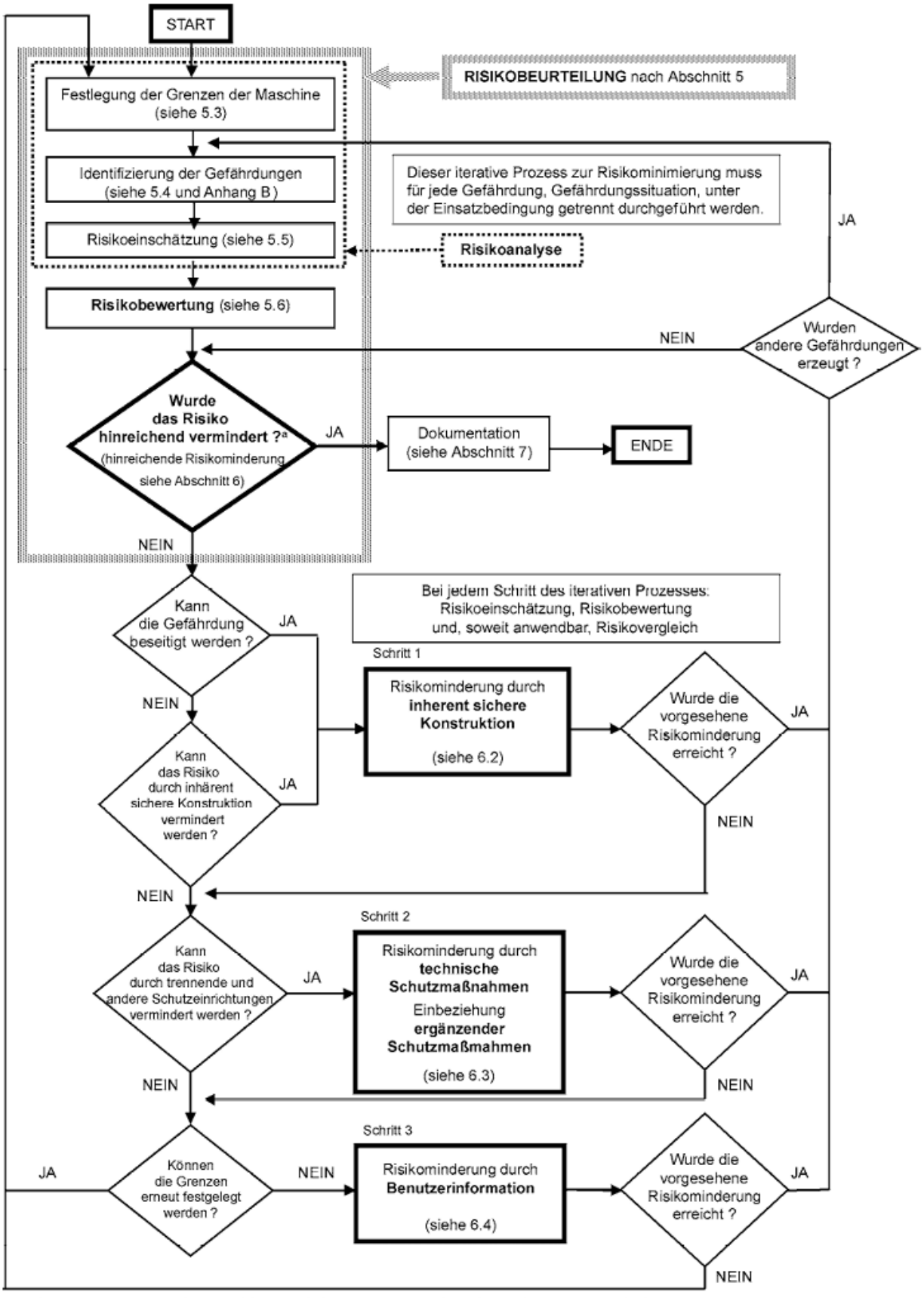
Die Informationen zur Risikobeurteilung sollen laut EN ISO 12100:2010 unter anderem folgendes beinhalten:[42]

- Beschreibung der Maschine
    - Benutzerspezifikationen
    - Erwartete Maschinenspezifikationen, einschließlich:
        - Beschreibung der verschiedenen Phasen der gesamten Lebensdauer
        - Konstruktionszeichnungen
        - erforderliche Energiequellen und deren Versorgung
    - Benutzerinformationen zur Maschine
- Vorschriften, Normen und weitere anwendbare Dokumente
    - anwendbare Vorschriften
    - relevante Normen
    - relevante, technische Spezifikationen
    - relevante Sicherheitsdatenblätter
- Erfahrungen im Einsatz
    - Unfall-, Zwischenfall-, oder Fehlfunktionsgeschichte
    - dokumentierte Gesundheitsschäden durch zum Bespiel Lärm, Vibrationen oder Staub
    - Erfahrungen von Benutzern ähnlicher Maschinen
- relevante ergonomische Grundsätze

Alle diese Informationen müssen bei Weiterentwicklungen oder Neugestaltungen berücksichtigt werden. Ähnliche Gefährdungssituationen bei verschiedenen Maschinentypen sind häufig und können durchaus verglichen werden.

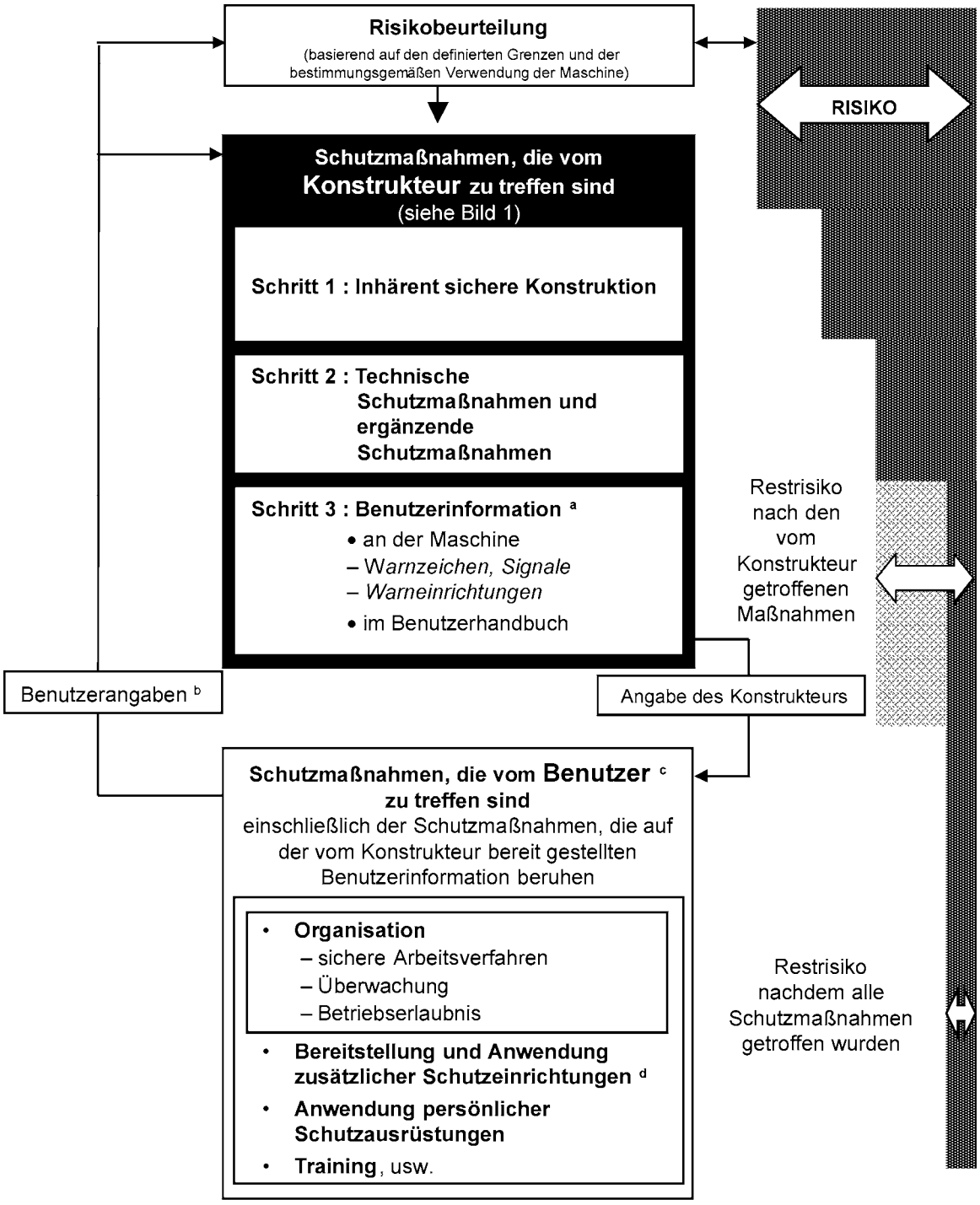
[42] Vgl. EN ISO 12100:2010 (2010), S. 18 f.

5.4 Der Prozess der Risikobeurteilung



[a] Beim erstmaligen Stellen der Frage, wird diese mit dem Ergebnis der Ausgangsrisikobewertung beantwortet.

Abbildung 9: Schematische Darstellung des dreistufigen iterativen Prozesses zur Risikominderung, Quelle: EN ISO 12100:2010 (2010), S. 16.



[a] Die Bereitstellung einer angemessenen Benutzerinformation ist Teil des Beitrages des Konstrukteurs zur Risikominderung; die betreffenden Schutzmaßnahmen werden jedoch erst mit deren Umsetzung durch den Benutzer wirksam.

[b] Benutzerangaben sind Informationen, die dem Konstrukteur entweder von den Benutzern hinsichtlich der bestimmungsgemäßen Verwendung der Maschine im Allgemeinen oder von einem bestimmten Benutzer gegeben werden.

[c] Bei den verschiedenen vom Benutzer zu treffenden Schutzmaßnahmen besteht keine bestimmte Hierarchie. Diese Schutzmaßnahmen liegen außerhalb des Anwendungsbereiches dieser Internationalen Norm.

[d] Schutzmaßnahmen, die für besondere, im Rahmen der bestimmungsgemäßen Verwendung der Maschine nicht vorgesehene Prozesse oder für besondere, durch den Konstrukteur nicht beeinflussbare Installationsbedingungen erforderlich sind

Abbildung 10: Prozess zur Risikominderung aus Sicht des Konstrukteurs, Quelle: EN ISO 12100:2010 (2010), S. 17.

5.5 Das Ergebnis einer Risikobeurteilung

Eine Risikobeurteilung liefert eine detaillierte Auflistung aller denkbaren Gefährdungen in allen Phasen der Lebensdauer einer Maschine und dies in einer möglichst frühen Phase einer Entwicklung. Außerdem werden für sämtliche Gefährdungen die nötigen Schutzmaßnahmen dokumentiert beziehungsweise die sich daraus ergebenden Maßnahmen zur Risikominderung beschrieben.

Kurzum, das Ergebnis einer Risikobeurteilung ist Konstruktionshandbuch, Wissensdokumentation und Vorlage für neue konstruktive Ansätze. Das Ergebnis der Risikobeurteilung ist außerdem die Basis für die Bestimmung des PL. Ein PL wird benötigt um eine technische Schutzmaßnahme der Sicherheitssteuerung zu bewerten.

5.6 Der Performance Level – PL

In der Norm EN ISO 13849-1:2015 ist der PL wie folgt definiert: „diskreter Level, der die Fähigkeit von sicherheitsbezogenen Teilen einer Steuerung spezifiziert, eine Sicherheitsfunktion unter vorhersehbaren Bedingungen auszuführen“[43].

In anderen Worten bedeutet das: Der Performance Level ist ein Maß für die Zuverlässigkeit einer Sicherheitsfunktion. Der Performance Level wird dabei auf einer Skala von „a“ (geringster PL) bis „e“ (höchster PL) bemessen. Die Sicherheit einer Funktion oder auch eines Bauteils kann anhand des PL angegeben werden. Je höher der PL, desto sicherer und zuverlässiger, auch im Sinne der Ausfallswahrscheinlichkeit ist die betrachtete Funktion beziehungsweise das Bauteil.

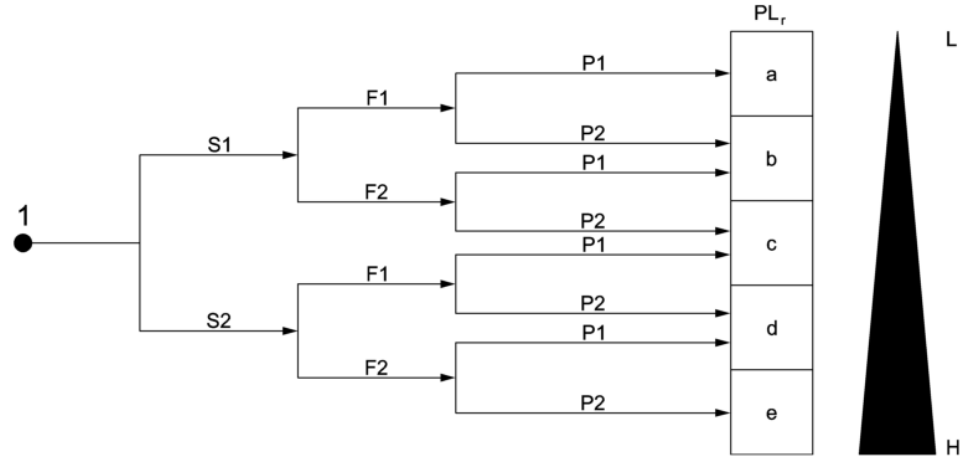
Dabei wird unterschieden zwischen einem erforderlichen Performance Level (PL_r), der für die Sicherheitsfunktion die erforderliche Risikominderung erzielt und einem Performance Level (PL), der die Fähigkeit der sicherheitsbezogenen Teile einer Steuerung beschreibt. Das bedeutet, dass der PL mindestens das gleiche oder ein höheres Level als der PL_r erreichen muss. Das Erreichen des PL_r muss validiert werden, dies gilt sowohl für Hardwareaspekte als auch für Softwareaspekte derartiger Systeme[44].

Zur Bestimmung des PL_r gibt es zwei Möglichkeiten. Zum einen kann der PL_r mit Hilfe des Graphen aus der EN ISO 13849-1:2015, Anhang A (siehe Abbildung 11) bestimmt werden oder er kann den zutreffenden Typ-C-Normen entnommen werden. Im Fall des STEPs sind die zutreffenden Typ-C-Normen zum einen die EN 280 – Fahrbare Hubarbeitsbühnen - Berechnung - Standsicherheit - Bau - Sicherheit - Prüfungen sowie die EN 1495 – Hebebühnen - Mastgeführte Kletterbühnen.

Ist die Eintrittswahrscheinlichkeit als niedrig einzustufen, kann der PL_r um eine Stufe verringert werden.

[43] EN ISO 13849-1:2015 (2015), S. 13.

[44] Vgl. Blasge (2016), S. 77.



Legende

1 Startpunkt zur Bewertung des Sicherheitsfunktionsbeitrags zur Risikominderung
L niedriger Beitrag zur Risikoreduzierung
H hoher Beitrag zur Risikominderung
PL_r erforderlicher Performance Level

Risikoparameter:
S Schwere der Verletzung
S1 leichte (üblicherweise reversible Verletzung)
S2 ernste (üblicherweise irreversible Verletzung oder Tod)
F Häufigkeit und/oder Dauer der Gefährdungsexposition
F1 selten bis weniger häufig und/oder die Zeit der Gefährdungsexposition ist kurz
F2 häufig bis dauernd und/oder die Zeit der Gefährdungsexposition ist lang
P Möglichkeit zur Vermeidung der Gefährdung oder Begrenzung des Schadens
P1 möglich unter bestimmten Bedingungen
P2 kaum möglich

Abbildung 11: Graph zur Bestimmung des erforderlichen Performance Levels (PL_r) für Sicherheitsfunktionen. Die Bewertung des Risikos anhand von Schadensausmaß, Häufigkeit beziehungsweise Aufenthaltsdauer und Möglichkeit zur Vermeidung der Gefährdung führen zur Ermittlung des PL_r. Quelle: EN ISO 13849-1:2015 (2015), S. 61.

5.6.1 Performance Level Parameter

Anhand der folgenden Aspekte muss die Einschätzung des PL, für jedes sicherheitsbezogene Teil der Steuerung beurteilt werden:[45]

5.6.1.1 Kategorien und deren Zusammenhang

Sicherheitsbezogene Teile von Steuerungen können in Bezug auf ihre Architektur in fünf verschiedene Kategorien eingeteilt werden. Die jeweilige Kategorie ist der Basisparameter zur Erreichung eines bestimmten PL. Je nach Gestaltung legt die Kategorie das erforderliche Verhalten bezüglich der Widerstandsfähigkeit gegenüber Fehlern der sicherheitsbezogenen Teile einer Steuerung fest.

In Abbildung 12 ist der Zusammenhang zwischen Kategorie, PL, $MTTF_D$, und DC ersichtlich. So lassen sich bestimmte PL nur mit bestimmten Kategorien erreichen.

[45] Vgl. EN ISO 13849-1:2015 (2015), S. 14, 27, 40 f, 81.

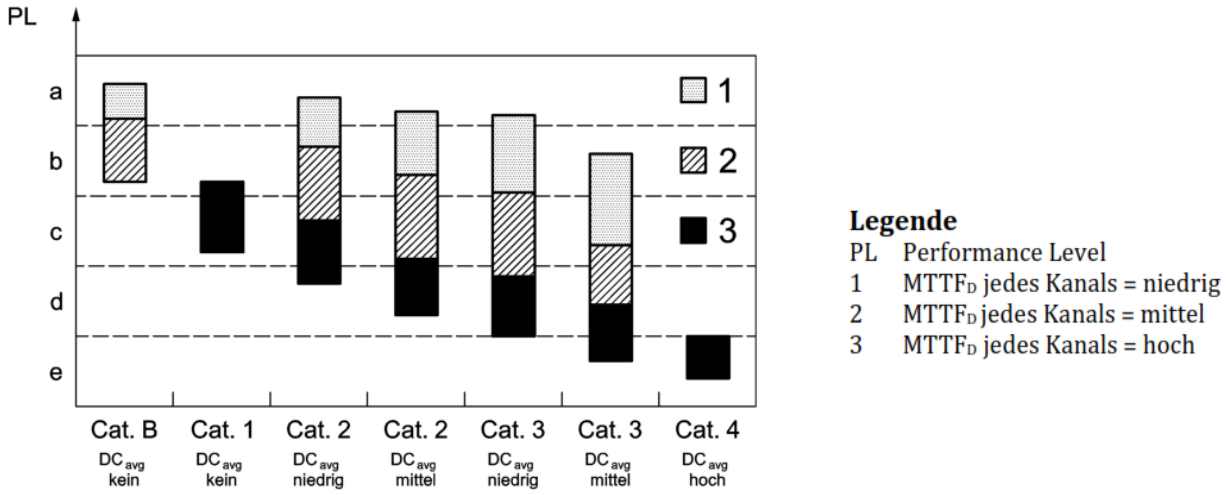


Abbildung 12: Zusammenhang zwischen Kategorie, DC_{avg}, $MTTF_D$ und PL, Quelle: EN ISO 13849-1:2015 (2015), S. 31.

Die jeweiligen Kategorien werden in Kapitel 5.7 genauer erläutert.

5.6.1.2 Mean Time to Dangerous Failure – $MTTF_D$

Der $MTTF_D$ Wert gibt jene mittlere Zeit bis zu einem gefahrbringenden Ausfall einer sicherheitsbezogenen Steuerung oder deren Teile an. Dieser Wert wird in drei Stufen angegeben, siehe Abbildung 13. Die Berücksichtigung erfolgt individuell für jeden einzelnen Kanal.

$MTTF_D$	
Bezeichnung für jeden Kanal	**Bereich für jeden Kanal**
niedrig	3 Jahre ≤ $MTTF_D$ < 10 Jahre
mittel	10 Jahre ≤ $MTTF_D$ < 30 Jahre
hoch	30 Jahre ≤ $MTTF_D$ ≤ 100 Jahre

Abbildung 13: Bezeichnung der drei $MTTF_D$ Bereiche inklusive der Bereiche, Quelle: EN ISO 13849-1:2015 (2015), S. 28.

5.6.1.3 Diagnosedeckungsgrad – DC

Der Diagnosedeckungsgrad (Diagnostic Coverage – DC) errechnet sich aus dem Verhältnis der Ausfallsrate bei erkannten gefahrbringenden Störungen zur Ausfallsrate aller gefahrbringenden Störungen. Er ist somit ein Maß für die Wirksamkeit der Diagnose. Der DC kann sowohl für die Gesamtheit als auch für Teile des sicherheitsbezogenen Systems gelten.

In Abbildung 14 sind die vier Bezeichnungen des DC beschrieben.

DC	
Bezeichnung	**Bereich**
kein	DC < 60 %
niedrig	60 % ≤ DC < 90 %
mittel	90 % ≤ DC < 99 %
hoch	99 % ≤ DC

Abbildung 14: Die vier Bezeichnungen des DC inklusive dessen Bereiche, Quelle: EN ISO 13849-1:2015 (2015), S. 29.

5.6.1.4 Common Cause Failures – CCF

Der CCF ist ein Wert, der sich auf den Ausfall verschiedener Einheiten bezieht, deren Ursache eine einzelne gemeinsame ist. Die Störungen stellen untereinander keine Folgefehler dar. Die EN ISO 13849-1:2015 enthält im Anhang F eine Tabelle mit einem Verfahren zur Punktevergabe und Quantifizierung für Maßnahmen. Bei 65 Punkten oder mehr wurden die Anforderungen erreicht, bei einer Punkteanzahl kleiner 65 ist das Verfahren gescheitert.

5.6.2 Safety Integrity Level – SIL

Grundsätzlich lassen sich Performance Level (PL) und Safety Integrity Level (SIL) vergleichen. Die unterschiedlichen Einteilungen entstammen zweier unterschiedlicher Normen. So stammt der PL aus der EN ISO 13849 und der SIL aus der IEC 61508. Im Gegensatz zur EN ISO 13849, die sich auf sicherheitsbezogene Teile von Steuerungen bezieht, wurde die IEC 61508 speziell zur Entwicklung von elektrischen, elektronischen und programmierbaren elektronischen (E/E/PE) Systemen, die eine Sicherheitsfunktion ausführen herausgegeben. Die IEC 61508 ist allerdings keine zur MRL harmonisierte Norm.

PL	SIL (IEC 61508-1, zur Information) hohe/kontinuierliche Betriebsart
a	keine Entsprechung
b	1
c	1
d	2
e	3

Tabelle 1: Beziehung zwischen dem Performance Level (PL) und dem Sicherheits-Integritätslevel (SIL), Quelle: EN ISO 13849-1:2015 (2015), S. 27.

Die MRL bezieht sich im Anhang I, Punkt 1.2.1. – Sicherheit und Zuverlässigkeit von Steuerungen – auf keine spezifische Norm. Somit können Maschinenkonstrukteure zwischen dem Gebrauch beider Normen wählen. Im Technischen Report ISO/TR 23849:2014-12 Punkt 2.5 sind Punkte angeführt, die die Auswahl der jeweiligen Normen erleichtern sollen. Besteht bereits Erfahrung oder Vorwissen mit der ISO 13849-1:1999 oder beruht die sicherheitsbezogene Steuerung nicht auf elektrischen Medien, so ist die EN ISO 13849-1:2006 geeigneter. Wünscht der Kunde den Nachweis der Sicherheit einer Maschine in SIL, so ist der EN 62061:2005 der Vorzug zu geben.[46]

5.7 Architekturen und Kategorien nach EN ISO 13849-1:2015

Die Toleranz gegenüber Fehlern wird durch die Architektur einer Sicherheitssteuerung bestimmt. Im Maschinenbau kommen zum einen einkanalige ungetestete Systeme mit in ihrer Zuverlässigkeit unterschiedlichen Bauteilen und zum anderen zweikanalige hochwertig getestete Systeme zum Einsatz.

[46] Vgl. DIN ISO/TR 23849:2014-12; DIN SPEC 33883:2014-12 (2014), S. 6.

Hilfreich neben der Einteilung in funktionale Kanäle ist auch die Einteilung in eine Ebene für Sensoren (Input „I“), Verarbeitung (Logik „L“) und Aktoren (Output „O“).[47]

Je höher die Widerstandsfähigkeit gegenüber Fehlern, desto höher ist die Möglichkeit der Risikoreduzierung. Zur Bestimmung der Ausfallswahrscheinlichkeit und des PL ist die Kategorie die Basis, die durch die Bauteilzuverlässigkeit ($MTTF_D$), die Tests (DC_{avg}) und die Widerstandsfähigkeit gegenüber Ausfällen als Folge gemeinsamer Ursache (CCF) komplettiert wird. Die Kategorie B gilt als die Basiskategorie und deren Anforderungen müssen auch in den anderen vier Kategorien eingehalten werden. Die Kategorien B und 1 werden überwiegend über die Auswahl der Bauteile bestimmt, während die Kategorien 2 bis 4 hauptsächlich über die Strukturen bestimmt werden.[48]

5.7.1 Kategorie B

Sicherheitsbezogene Teile von Steuerungen müssen nach zutreffenden Normen und unter Verwendung von grundlegenden Sicherheitsprinzipien so ausgewählt und kombiniert werden, dass

- sie den zu erwartenden Betriebsbeanspruchungen, z.B. Zuverlässigkeit bezüglich Schaltzyklen
- dem Einfluss des verwendeten Materials, z.B. Hydrauliköl in Schläuchen
- anderen relevanten äußeren Einflüssen, z.B. elektromagnetischen Störungen

standhalten.[49]

Systemverhalten	**$MTTF_D$ jedes Kanals**	**DC_{avg}**	**CCF**
Das Auftreten eines Fehlers kann zum Verlust der Sicherheitsfunktion führen	niedrig bis mittel	kein	nicht relevant

Tabelle 2: Übersicht über Kategorie B, Quelle: Hauke/u.a. (2017), S. 52.

Der maximal erreichbare PL für Systeme der Kategorie B ist der PL „b“. Die Architektur von Kategorie B Systemen ist in Abbildung 15 dargestellt.

Legende
i_m Verbindungsmittel
I Eingabeeinheit, z. B. Sensor
L Logik
O Ausgabeeinheit, z. B. Hauptschütz

Abbildung 15: Architektur der Kategorie B und 1, Quelle: EN ISO 13849-1:2015 (2015), S. 45.

[47] Vgl. Hauke/u.a. (2017), S. 49 f.

[48] Vgl. Hauke/u.a. (2017), S. 50.

[49] Vgl. EN ISO 13849-1:2015 (2015), S. 46.

5.7.2 Kategorie 1

Zusätzlich zu den Anforderungen von Kategorie B gelten für die Kategorie 1 die Verwendung bewährter Bauteile und bewährter Sicherheitsprinzipien. Bewährte Bauteile sind Bauteile, die in der Vergangenheit weit verbreitet mit erfolgreichen Ergebnissen in ähnlichen Anwendungen eingesetzt wurden beziehungsweise die eine zuverlässige Eignung in sicherheitsbezogenen Anwendungen zeigen und diese auch verifiziert wurden. Der maximal erreichbare PL in Kategorie 1 ist „c". Die Struktur der Kategorie ist gleich wie in Kategorie B, siehe Abbildung 15.[50]

Systemverhalten	**$MTTF_D$ jedes Kanals**	**DC_{avg}**	**CCF**
Das Auftreten eines Fehlers kann zum Verlust der Sicherheitsfunktion führen, die Wahrscheinlichkeit ist allerdings nicht so groß wie in Kategorie B.	hoch	kein	nicht relevant

Tabelle 3: Übersicht über Kategorie 1, Quelle: Hauke/u.a. (2017), S. 52.

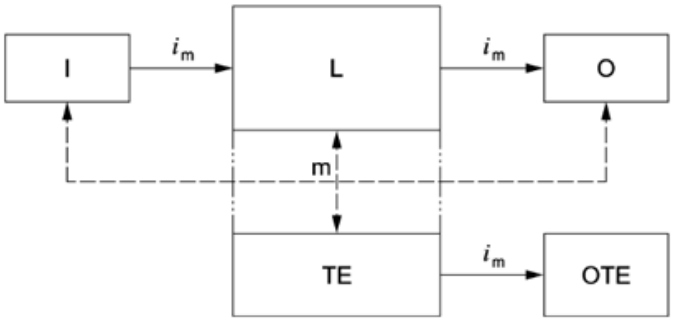
5.7.3 Kategorie 2

Sicherheitssteuerungen der Kategorie 2 müssen in angemessenen Zeitabständen durch die Maschinensteuerung getestet werden. Ein Test muss auf jeden Fall durchgeführt werden beim Anlauf der Maschine und vor dem Einleiten einer Gefährdungssituation. Dies ist zum Beispiel beim Start einer Bewegung oder vor dem Start eines neuen Zyklus notwendig. Wird kein Fehler erkannt, muss der Betrieb zugelassen werden. Bei der Erkennung eines Fehlers muss zur Erreichung des PL_r „d" ein sicherer Zustand eingeleitet werden, der bis zur Behebung des Fehlers aufrecht bleibt beziehungsweise zur Erreichung des PL_r „c" ist die Ausgabe einer Warnung ausreichend, sofern kein sicherer Zustand eingeleitet werden kann. Der Test darf zu keiner Gefährdungssituation führen.[51]

Die Kategorie 2 spielt in Maschinensteuerungen nur eine untergeordnete Rolle. Die Architektur der Kategorie 2 ist in Abbildung 16 dargestellt.

[50] Vgl. EN ISO 13849-1:2015 (2015), S. 47 f.

[51] Vgl. EN ISO 13849-1:2015 (2015), S. 48 f.



Legende

i_m	Verbindungsmittel
I	Eingabeeinheit, z. B. Sensor
L	Logik
m	Überwachung
O	Ausgabeeinheit, z. B. Hauptschütz
TE	Testeinrichtung
OTE	Ausgang der TE

Die gestrichelten Linien zeigen die vernünftigerweise durchführbare Fehlererkennung.

Abbildung 16: Architektur der Kategorie 2, Quelle: EN ISO 13849-1:2015 (2015), S. 49.

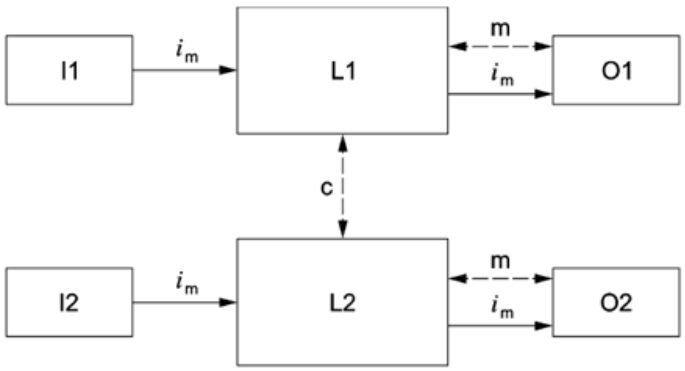
Systemverhalten	**$MTTF_D$ jedes Kanals**	**DC_{avg}**	**CCF**
Das Auftreten eines Fehlers kann zum Verlust der Sicherheitsfunktion zwischen den Tests führen. Der Verlust wird beim Test erkannt.	niedrig bis hoch	min-destens niedrig	Maßnahmen erforderlich

Tabelle 4: Übersicht über Kategorie 2, Quelle: Hauke/u.a. (2017), S. 52.

5.7.4 Kategorie 3

Die Gestaltung von Sicherheitsbezogenen Teilen von Steuerungen in Kategorie 3 hat so zu erfolgen, dass ein Fehler in einem der Teile nicht zum Verlust der Sicherheitsfunktion führt. Ein Fehler muss bei oder vor der nächsten Anforderung der Sicherheitsfunktion erkannt werden. Das Systemverhalten von Sicherheitsbezogenen Teilen von Steuerungen in Kategorie 3 ist in Tabelle 5 dargestellt.[52]

Die Architektur der Kategorie 3 ist in Abbildung 17 dargestellt.



[52] Vgl. EN ISO 13849-1:2015 (2015), S. 49 f.

Legende

i_m	Verbindungsmittel
c	Kreuzvergleich
I1, I2	Eingabeeinheiten, z. B. Sensor
L1, L2	Logik
m	Überwachung
O1, O2	Ausgabeeinheiten, z. B. Hauptschütz

Die gestrichelten Linien zeigen die vernünftigerweise durchführbare Fehlererkennung.

Abbildung 17: Architektur der Kategorie 3, Quelle: EN ISO 13849-1:2015 (2015), S. 50.

Systemverhalten	$MTTF_D$ jedes Kanals	DC_{avg}	CCF
Bei Auftreten eines einzelnen Fehlers bleibt die Sicherheitsfunktion immer erhalten. Einige Fehler werden erkannt, aber nicht alle. Eine Anhäufung von unerkannten Fehlern kann zum Verlust der Sicherheitsfunktion führen	niedrig bis hoch	min-destens niedrig	Maßnahmen erforderlich

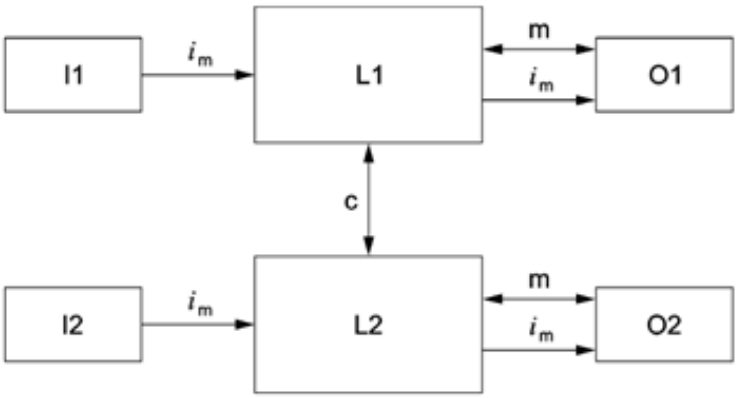
Tabelle 5: Überblick über Kategorie 3, Quelle: Hauke/u.a. (2017), S. 52.

In Kategorie 3 kann ein maximaler PL von „e“ erreicht werden.

5.7.5 Kategorie 4

Sicherheitsbezogene Teile einer Steuerung müssen in Kategorie 4 so ausgeführt werden, dass ein Fehler nicht zum Verlust der Sicherheitsfunktion führt und dieser bei oder vor der nächsten Anforderung erkannt wird. Wenn der Fehler nicht erkannt wird, darf die Anhäufung von Fehlern nicht zum Verlust der Sicherheitsfunktion führen. Die Betrachtung einer Fehlerkombination von zwei Fehlern ist in der Praxis ausreichend. Bei Ausführung in Kategorie 4 wird ein PL von „e“ erreicht.[53]

Die Architektur der Kategorie 4 ist in Abbildung 18 dargestellt.



[53] Vgl. EN ISO 13849-1:2015 (2015), S. 50 f.

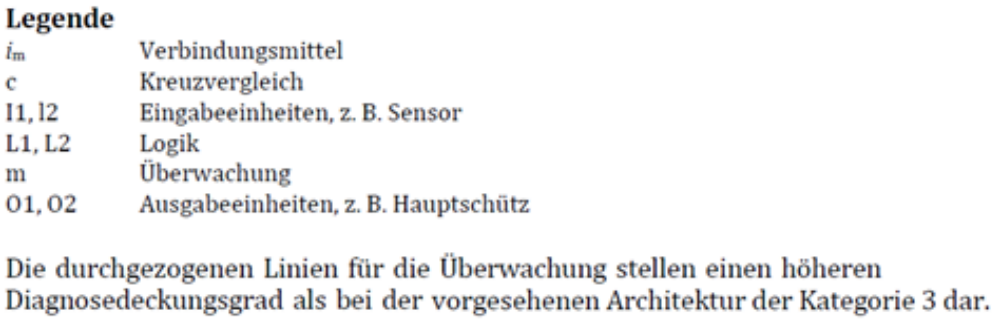


Abbildung 18: Architektur der Kategorie 4, Quelle: EN ISO 13849-1:2015 (2015), S. 51.

Systemverhalten	**$MTTF_D$ jedes Kanals**	**DC_{avg}**	**CCF**
Bei Auftreten eines einzelnen Fehlers bleibt die Sicherheitsfunktion immer erhalten. Die Erkennung von Fehleranhäufungen reduziert die Wahrscheinlichkeit des Verlustes der Sicherheitsfunktion (hoher DC_{avg}). Um den Verlust der Sicherheitsfunktion zu vermeiden, werden Fehler rechtzeitig erkannt.	hoch	hoch einschließlich der Fehler-anhäufung	Maßnahmen erforderlich

Tabelle 6: Überblick über Kategorie 4, Quelle: Hauke/u.a. (2017), S. 52.

5.8 Verifikation des Performance Levels

Wurde der PL der Sicherheitsfunktion bestimmt, muss dieser mit dem davor aus dem Risikograph ermittelten oder aus der Typ-C-Norm entnommenen PL_r übereinstimmen beziehungsweise höher sein. Ist der PL niedriger als der PL_r müssen die sicherheitsbezogenen Teile der Sicherheitsfunktion neu gestaltet oder gegebenenfalls andere Bauteile eingesetzt werden.

Ebenso gilt für jeden Bauteil einer Sicherheitsfunktion, dass der PL mindestens dem des PL_r entsprechen muss.[54]

5.9 Validierung von Sicherheitseinrichtungen nach EN 12849-2

Zweck des Validierungsverfahrens ist es, zu bestätigen, dass die Gestaltung der sicherheitsbezogenen Teile der Steuerung die Spezifikation der Sicherheitsanforderungen der Maschinen unterstützt. Dabei muss das Validierungsverfahren aufzeigen, dass jeder sicherheitsbezogene Teil einer Steuerung die Anforderungen an die EN ISO 13849-1:2015 erfüllt. Insbesondere in Bezug auf:[55]

- den festgelegten Sicherheitseigenschaften der Sicherheitsfunktionen

[54] Vgl. EN ISO 13849-1:2015 (2015), S. 39.

[55] Vgl. EN ISO 13849-2:2012 (2012), S. 6.

- den Anforderungen für den festgelegte Performance Level
- den Anforderungen für die festgelegte Kategorie
- den Maßnahmen zur Beherrschung und zur Vermeidung systematischer Ausfälle
- den Anforderungen an die Software
- der Fähigkeit, eine Sicherheitsfunktion unter den erwarteten Umgebungsbedingungen zu leisten
- der ergonomischen Gestaltung der Benutzerschnittstelle

Zur Validierung der Sicherheit von Steuerungen gibt es eine Software die dabei behilflich ist. Das Windows-Tool ist kostenlos erhältlich, heißt SISTEMA und arbeitet auf Basis der EN ISO 13849-1:2015. SISTEMA steht für „Sicherheit von Steuerungen an Maschinen“[56].

Auf Basis der gewählten Architektur bildet SISTEMA die Struktur der sicherheitsbezogenen Steuerung nach und errechnet Zuverlässigkeitswerte und den erreichten PL. Die unter Punkt 5.6.1 erwähnten Parameter zur Bestimmung des erforderlichen PL_r werden erfasst und damit der PL errechnet. Der daraus resultierende Report ist Teil der Risikobeurteilung.

Die Norm EN ISO 13849-2:2012 empfiehlt, dass die Validierung Personen durchführen, die unabhängig von der Gestaltung der sicherheitsbezogenen Teile der Steuerung sind.

[56] Vgl. Deutsche Gesetzliche Unfallversicherung e.V. (2015), Online-Quelle [15.09.2017]

6 HARMONISIERTE NORMEN IN BEZUG AUF DEN STEP

In diesem Kapitel wird auf Harmonisierte Typ-C-Normen eingegangen, die auf das Projekt STEP zutreffend sind. Konkret handelt es sich hierbei um die EN 280 – Fahrbare Hubarbeitsbühnen - Berechnung - Standsicherheit - Bau - Sicherheit - Prüfungen sowie um die EN 1495 – Hebebühnen - Mastgeführte Kletterbühnen. Wie bereits in Kapitel 2.2 erwähnt, haben Festlegungen in Typ-C-Normen bei Abweichung gegenüber Typ-A-Normen beziehungsweise Typ-B-Normen Vorrang. Voraussetzung ist, dass die Maschine nach den Bestimmungen der jeweiligen Typ-C-Norm konstruiert wurde.

Durch die spezielle Konstruktion, kann der STEP nicht einer einzelnen Typ-C-Norm eindeutig zugewiesen werden. Aus diesem Grund werden einzelne Komponenten nach unterschiedlichen Normen konstruiert. So wird der Unterwagen, der Teleskopturm und der Schubarm inklusive Arbeitskorb nach der EN 280 konstruiert, die Brücke hingegen wird nach der EN 1495 geplant.

6.1 Die fahrbare Hubarbeitsbühne nach EN 280

Die ÖNORM EN 280 für fahrbare Hubarbeitsbühnen (FHAB) legt Sicherheitsanforderungen und Maßnahmen für FHABs fest, unabhängig von deren Art und Größe. Als FHAB gilt eine Maschine, die Personen zu Arbeitsplätzen bringt, an denen sie Arbeiten aus zum Beispiel Arbeitskörben verrichten. Als Bedingung gilt, dass die Arbeitsbühne nur an Zugangsstellen in Bodennähe oder wie im Falle des STEP vom Fahrgestell aus betreten und verlassen werden darf. Die EN 280 setzt voraus, dass das Bedienpersonal dementsprechend geschult ist. Aus diesem Grund werden nur Anforderungen an Material und Ausrüstung im Hinblick auf die Sicherheit erwähnt.[57]

6.1.1 Klassifizierung von fahrbaren Hubarbeitsbühnen nach der EN 280

FHABn werden in zwei Hauptgruppen eingeordnet. FHABn, bei denen sich der Mittelpunkt der Plattform in allen Stellungen innerhalb der Kippkante befindet und alle anderen FHABn. Da die Arbeitskörbe des STEPS über die Kippkante ragen, gehört der STEP eindeutig zur zweiten Gruppe von FHABn. Auch in Bezug auf das Fahren werden FHABn klassifiziert:[58]

1. Fahren nur in Grundstellung
2. Fahren, wenn der Arbeitskorb angehoben ist und vom Untergestell gesteuert wird
3. Fahren, wenn der Arbeitskorb angehoben ist und vom Arbeitskorb gesteuert wird

Eine Kombination aus Typ 2 und Typ 3 ist erlaubt und ist beim STEP auch zutreffend.

6.1.2 Liste der Gefährdungen der EN 280

Unter Kapitel 4 der NORM EN 280 wird in der Tabelle 1 eine Liste an signifikanten Gefährdungen, die durch die Risikobeurteilung ermittelt wurden angeführt und auf relevante Abschnitte in der Norm zu den jeweiligen Gefährdungen verwiesen. Die Liste der signifikanten Gefährdungen soll als Hilfe bei der Erstellung der

[57] Vgl. EN 280:2013+A1:2015 (2015), S. 5 f.

[58] Vgl. EN 280:2013+A1:2015 (2015), S. 7.

Risikobeurteilung dienen. Darüber hinaus gilt natürlich für relevante aber nicht signifikante Gefährdungen die EN ISO 12100:2010.

6.1.3 Sicherheitsanforderungen und Sicherheitsmaßnahmen nach EN 280

Im Kapitel 5 – Sicherheitsanforderungen und/oder -maßnahmen der EN 280 sind Sicherheitsanforderungen an FHABs und deren Komponenten aufgelistet die erfüllt werden müssen. Des Weiteren schreibt die Norm vor, in welchem Ausmaß die Verifikation der jeweiligen Sicherheitsfunktion zu erfolgen hat.

In Tabelle 5 der EN 280 werden Performance Level für Sicherheitsanforderungen angegeben, die erfüllt werden müssen. In der folgenden Tabelle werden die für den STEP relevanten Sicherheitsfunktionen mit dem PL_r aufgelistet.

PL_r nach EN ISO 13849-1	**Beschreibung der Sicherheitsfunktion**
c	Verfahren von mitgängergeführten FHABn verhindern
c	Überschreitung der Neigungsgrenzen verhindern
d	Überwachung der Abstützeinrichtungen
d	Kipp-Regelung oder -Verriegelung
d	Stellungsüberwachung
c	Unterbrechung von Bewegungen unter Schlaffkettenbedingungen
c	Verriegelung von Handläufen
c	Verriegelung von auswechselbaren Arbeitsbühnen
b	Verriegelung von Steuereinrichtungen
c	Verriegelung von Steuerplätzen
c	Bewegungen der lasttragenden Zylinder bei Versagen der Zuleitung verhindern

Tabelle 7: Erforderliche Performance Level für Sicherheitsfunktionen von fahrbaren Hubarbeitsbühnen nach EN 280, Quelle: EN 280:2013+A1:2015 (2015), S. 66.

6.1.4 Prüfungen nach EN 280

Zur Feststellung ob Sicherheitsmaßnahmen auch der Norm genügen, müssen Prüfungen durchgeführt werden. Deren Ergebnisse sowie Name und Anschrift des Ausführenden müssen in einem Prüfbericht angegeben und unterschrieben werden.[59] Diese Prüfungen bestehen aus folgenden Teilen:[60]

- Vorprüfung
- Bauprüfung

[59] Vgl. EN 280:2013+A1:2015 (2015), S. 67.

[60] Vgl. EN 280:2013+A1:2015 (2015), S. 67.

- Prüfungen

6.1.4.1 Vorprüfung

In der Vorprüfung muss gezeigt werden, dass die FHAB nach der Norm EN 280 berechnet und konstruiert wurde. Die Vorprüfung verlangt die Prüfung der Unterlagen:“

a) Zeichnungen mit den wesentlichen Abmessungen der FHAB;
b) Beschreibung der FHAB einschließlich der notwendigen Informationen über ihre Leistungsfähigkeit;
c) Angaben über die benutzten Werkstoffe;
d) Schaltpläne der elektrischen, hydraulischen und pneumatischen Einrichtungen;
e) Betriebshandbuch;
f) Berechnungen.“[61]

6.1.4.2 Bauprüfung

In der Bauprüfung muss gezeigt werden, dass: „

a) die FHAB in Übereinstimmung mit den geprüften Unterlagen hergestellt wird;
b) die Bauteile mit den Zeichnungen übereinstimmen;
c) die Prüfbescheinigungen über die verwendeten Arten von Seilen, Ketten sowie hydraulischer oder pneumatischer Schläuche vorliegen. Diese Bescheinigungen müssen die Mindestbruchlast oder den Berstdruck ausweisen, soweit erforderlich;
d) die Qualität der Schweißungen von insbesondere lasttragenden Bauteilen durch die Anwendung der zutreffenden Europäischen Norm(en) sichergestellt wird;
e) die Ausführung und der Einbau von Teilen (insbesondere Sicherheitseinrichtungen) entsprechend dieser Norm erfolgt.“[62]

6.1.4.3 Prüfungen

Prüfungen sind durchzuführen um zu zeigen, dass: „

a) die FHAB standsicher ist;
b) die FHAB stabil ist;
c) alle Funktionen richtig und sicher arbeiten;
d) Kennzeichnungen angebracht sind.“[63]

6.2 Die mastgeführte Kletterbühne nach EN 1495

Die Norm EN 1495 legt Sicherheitsanforderungen an Mastgeführte Kletterbühnen (MKB) fest. Angewandt wird die Norm sowohl bei vorübergehend als auch dauerhaft aufgestellten MKBn, unabhängig von deren Antrieb. Als weiteres Kriterium legt die Norm fest, dass das Heben und Senken bei MKBn über

[61] EN 280:2013+A1:2015 (2015), S. 67.

[62] EN 280:2013+A1:2015 (2015), S. 68.

[63] EN 280:2013+A1:2015 (2015), S. 68.

Zahnstangen beziehungsweise Ritzel zu erfolgen hat. Der Unterschied von MKBn zu Bauaufzügen ist laut EN 1495, dass Personen und Material von einer einzigen Einstiegsstelle und zurück befördert werden.[64]

Nach Anwendungsbereich der EN 1495 sind nur die sich auf den Teleskopturm befindlichen Brücken dieser Norm zuzuordnen. Diese werden über Zahnstangen auf und ab bewegt, dabei darf die Nenngeschwindigkeit von 0,2 m/s nicht überschritten werden. Außerdem schreibt de EN 1495 für jede Arbeitsbühne ein automatisches Bremssystem vor, das bei Ausfall der Hauptenergieversorgung beziehungsweise bei Ausfall der Energieversorgung von Steuerkreisen wirksam wird. In Bezug auf den STEP sind die Arbeitsbühnen in Form von Brücken ausgeführt, die wiederrum telekopierbare Schubarme tragen. Das Bremssystem muss elektromechanisch oder hydromechanisch ausgeführt sein.[65]

Im Gegensatz zur EN 280 wird in der EN 1495 kein PL_r für Sicherheitsfunktionen angegeben. Die Bestimmung des PL_r erfolgt also ausschließlich über den Risikograph.

[64] Vgl. EN 1495:1997+A2:2009 (2009), S. 4.

[65] Vgl. EN 1495:1997+A2:2009 (2009). S. 29.

7 SYSTEMBESCHREIBUNG STEP

Für Wartungsarbeiten kommen Schiffe mit Längen bis zu 400 m, 60 m Breite und 16 m Tiefgang regelmäßig in die Werft. Dort werden Beschädigungen im Lack und der Außenhaut, verursacht durch Salzwasser, Treibgut und Meereslebewesen repariert. Außerdem werden Ablagerungen am gesamten Schiffsrumpf entfernt. Diese führen zu sinkender Höchstgeschwindigkeit und in weiterer Folge zu niedrigerer Manövrierfähigkeit und das bei höherem Treibstoffverbrauch. Deswegen werden Schiffsrümpfe in turnusmäßigen Abständen gewaschen beziehungsweise gänzlich vom Lack befreit und neu beschichtet.

Üblicherweise wird diese schwere und gefährliche Arbeit manuell, mittels Wasserstrahllanzen von unzähligen Werftmitarbeitern im asiatischen Raum durchgeführt. Um Schiffe mit solchen Dimensionen zu bearbeiten werden Gerüste und Hubarbeitsbühnen eingesetzt. Der Arbeits- und Umweltschutz wird oftmals vernachlässigt. Nicht selten passieren schwere Arbeitsunfälle auch mit tödlichem Ausgang.

Die Firma HPT hat sich auf die Entwicklung und Herstellung vollautomatisierter Zugangs- und Bearbeitungssysteme für die Schifffahrtsindustrie spezialisiert. Als Flaggschiff in der automatisierten Schiffsbearbeitung gilt dabei der HTC. Mit dem HTC kann der Schiffsrumpf mit Hochdruckwasserstrahlen von Salzrückständen und pflanzlichen Anlagerungen befreit werden. Abhängig vom Druck der Wasserstrahlen kann auch die gesamte Beschichtung des Schiffes abgetragen werden. Das Prozesswasser wird dabei abgesaugt und das abgetragene Material gefiltert. In einem weiteren Arbeitsschritt kann das Schiff wieder beschichtet werden. Diese Bearbeitungsschritte können einzeln und parallel durchgeführt werden. Bedient wird die Maschine dabei aus einem Stellstand an der Maschine.

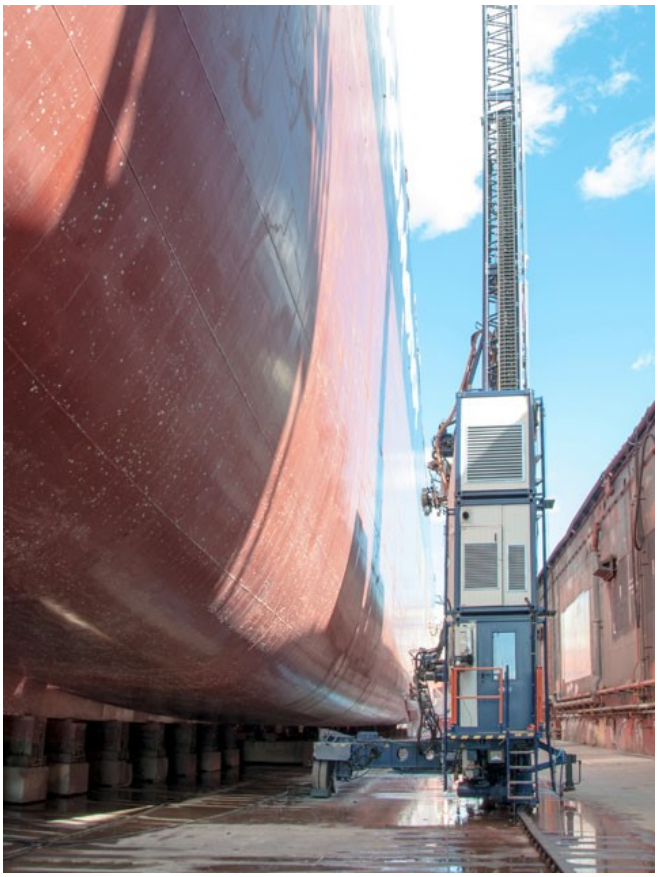


Abbildung 19: Vollautomatisierte Anlage zur Bearbeitung von Schiffsrümpfen, der HTC. Quelle: Hubert Palfinger Technologies GmbH (2017), Online-Quelle [12.09.2017]

Durch die Größe des HTCs und die geometrische Form des Schiffs können nicht alle Bereiche des zu bearbeitenden Schiffs erreicht werden. Genau für diese Bereiche wurde der STEP entwickelt. Der STEP wird neben dem HTC im Dock betrieben und deckt eben Bereiche ab die der HTC nicht erreicht. Mit dem am Arbeitskorb befestigten Werkzeug kann ebenso wie beim HTC die Beschichtung des Schiffes abgetragen werden. Eine eventuell neue Beschichtung wird vom Werftpersonal händisch aufgebracht.

Abbildung 20 zeigt den gesamten STEP im eingefahrenen Zustand, mit Ausnahme eines Arbeitskorbes, inklusive der beiden Ultrahochdruck-Pumpen.

Abbildung 20: Gesamtansicht des STEPs, Quelle: Eigene Darstellung

Es sind vor allem die Bereiche im Bug und Heck Bereich des Schiffes, die der HTC nicht erreicht. Zum einen sind in diesen Bereichen viele Flächen die von unten bearbeitet werden müssen, was mit dem HTC nicht möglich ist und zum anderen werden die Radien, der zu verlegenden Schienen auf denen sich beide Maschinen bewegen, für den HTC zu klein.

Abbildung 21 zeigt den STEP im ausgefahrenen Zustand. Der Teleskopturm des STEPs erreicht eine Höhe von 24 m, inklusive Unterwagen ergibt das eine Höhe von 25 m vom Boden bis zur Turmspitze. Aufgrund von Umgebungsbedingungen in den Werften wurde der Teleskopturm im Vergleich zum Prototypen kürzer. Dafür ist es möglich ein zusätzliches Turmsegment mit einer Länge von bis zu sechs Metern an den Teleskopturm anzuflantschen und so die Bearbeitungshöhe noch zu vergrößern. Die beiden Schubarme, die an den Brücken befestigt sind, lassen sich bis auf acht Meter teleskopieren.

Abbildung 21: Unterwagen mit ausgefahrenem Turm und angeflanschter Turmverlängerung, Quelle: Eigene Darstellung

Wenn in den folgenden Kapiteln von rechts beziehungsweise links gesprochen wird, so ist per Definition die Blickrichtung immer in Richtung des zu bearbeitenden Schiffs.

7.1 Allgemeine Beschreibung zum STEP

In diesem Kapitel werden die einzelnen Baugruppen beschrieben. Des Weiteren werden die Funktionen der Baugruppen behandelt. In Tabelle 8 ist die Produktbeschreibung tabellarisch zusammengefasst.

Projektbeschreibung, Projektdaten			
Produkt:	Produktname / Bezeichnung:		Ship Treatment and Elevating Platform
	Typ:		Prototyp
	Handelsbezeichnung:		STEP
Hersteller:	Name:		Hubert Palfinger Technologies GmbH
	Adresse:		Weng 4
			8911 Admont
			Stmk., Österreich
Art und Beschreibung der Maschine:	Hydraulisch betriebene Hebe- und Fahrvorrichtung für maximal 4 Personen und Werkzeug zur Bearbeitung von Schiffsaussenhüllen in Trocken- und Schwimmdocks. Sämtliche Bewegungen erfolgen durch Bedienerinnen und Bediener anhand von Bedienelementen am Unterwagen und in den Arbeitskörben.		
Produktspezifikation nach Maschinenrichtlinie:	Maschinen-gattung:		Nahrungsmittelmaschine, Maschine für kosmetische bzw. pharmazeutische Erzeugnisse
			Handgehaltene und/oder handgeführte tragbare Maschine
			Maschine zur Bearbeitung von Holz und von Werkstoffen mit ähnlichen physikalischen Eigenschaften
		X	Gefährdungen die von der Beweglichkeit der Maschine ausgehen
		X	Durch Hebevorgänge bedingte Gefährdungen
			Maschine, die zum Einsatz unter Tage bestimmt ist
		X	Gefährdungen durch das Heben von Personen
			Keine dieser Spezifikationen zutreffend
	Vollständige / Unvollständige:	X	Vollständige Maschine
			Unvollständige Maschine

Tabelle 8: Produktbeschreibung des STEPs

7.1.1 Unterwagen, Fahrwerk, Abstützvorrichtung, Stützrolle

Der Unterwagen bildet das Untergestell des STEPs und besteht im Wesentlichen aus vier Komponenten. Dem Grundrahmen, zwei schienengebundenen Fahrwerken, sowie zwei ausfahrbaren Abstützvorrichtungen mit jeweils einer Stützrolle. Siehe dazu Abbildung 22.

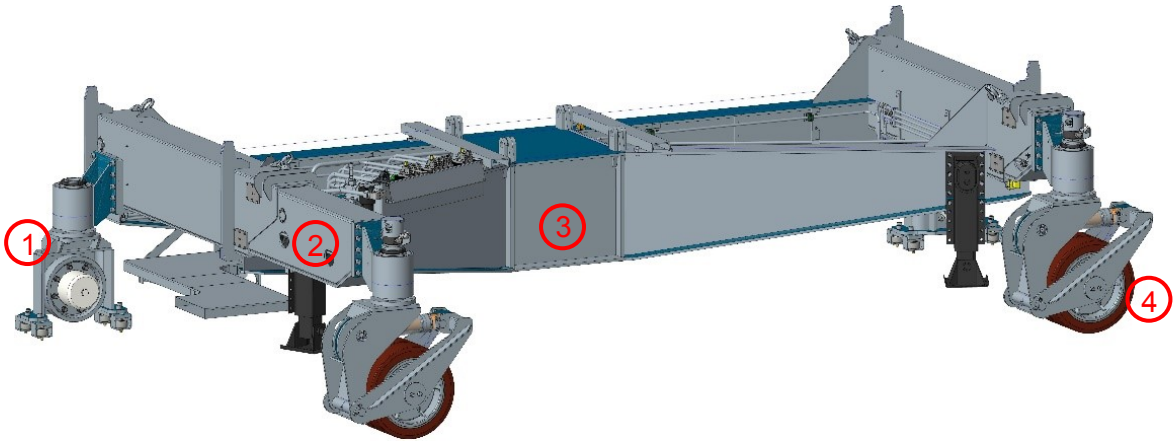


Abbildung 22: Unterwagen samt Abstützvorrichtung und Stützrollen. 1: Fahrwerk, 2: Ausleger, 3: Grundgerüst, 4: Stützrolle, Quelle: Eigene Darstellung

Der STEP besitzt zwei schienengebundene Fahrwerke, siehe Abbildung 23. Angetrieben wird das Fahrwerk am Unterwagen des STEPs von einem Hydraulikmotor je Fahrwerk. Die beiden schienengebundenen Fahrwerke an der Rückseite des Grundrahmens tragen die Hauptlast des STEP und sind für den Vortrieb entlang der Führungsschiene verantwortlich. Dies erfolgt über tragende Reduktionsgetriebe sowie direkt angeflanschte Hydraulikmotoren.

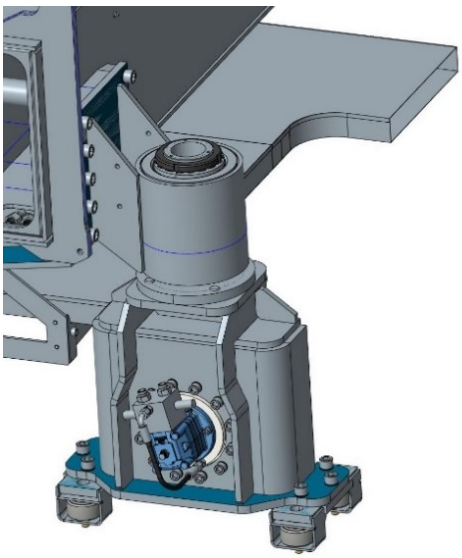


Abbildung 23: Hydraulisches, schienengebundenes Fahrwerk am Unterwagen des STEP, Quelle: Eigene Darstellung

Drei unterschiedliche Geschwindigkeiten wurden für die Längsfahrt des STEPs definiert. Diese sind in Tabelle 9 mit den vorausgesetzten Bedingungen aufgelistet.

Betriebszustand	**Bedingung**	**Geschwindigkeit**
Längsfahrt - Eilgang	• Der STEP muss sich in Grundstellung befinden • Die Arbeitskörbe dürfen nicht besetzt sein • Die Abstützvorrichtungen müssen ausgefahren sein	18 m/min

Längsfahrt - Arbeitsmodus im Trockendock	• Die Neigung des Unterwagens darf den vom Hersteller angegebenen Wert ± 0,5° nicht überschreiten • Passagiere im Arbeitskorb müssen einer Längsfahrt per Knopfdruck zustimmen • Die Abstützvorrichtungen müssen ausgefahren sein	6 m/min
Längsfahrt - Arbeitsmodus im Schwimmdock	• Die Neigung des Unterwagens darf den vom Hersteller angegebenen Wert ± 0,5° nicht überschreiten • Passagiere im Arbeitskorb müssen einer Längsfahrt per Knopfdruck zustimmen • Die Abstützvorrichtungen müssen ausgefahren sein	3 m/min

Tabelle 9: Festgelegte Geschwindigkeiten für die Längsfahrt des STEP, Quelle: Hubert Palfinger Technologies GmbH (Hrsg.) (2017)

Die Abstützvorrichtung ist eines der sicherheitsrelevantesten Elemente des STEPs. Sie verhindert ein Umfallen der Maschine und hält den Unterwagen in der Waage, auch während der Längsfahrt. Sie sorgt für einen stabilen, ebenen Zustand des Grundgerätes im stationären Betrieb und gleicht im Fahrbetrieb anfallende Unebenheiten des Untergrundes aus. Die Abstützeinheit besteht aus einem hydraulisch ausfahrbaren Ausleger und der angeflanschten Stützrolle. Siehe Abbildung 24. Die Stützrolle ist 360° drehbar und wird nicht aktiv angesteuert. Der an der Stützrolle angebrachte Hydraulikzylinder sorgt für die Nivellierung des Unterwagens. Der Hydraulikzylinder hat einen Hub von 250 mm und ist mit einem Wegmesssensor ausgestattet. Des Weiteren wird ein analoger Druckmessumformer den Druck am Zylinder messen. Unterschreitet der Druck am Zylinder ein definiertes Minimum, stoppt die Maschine, denn die Standsicherheit der Maschine ist sodann akut gefährdet.

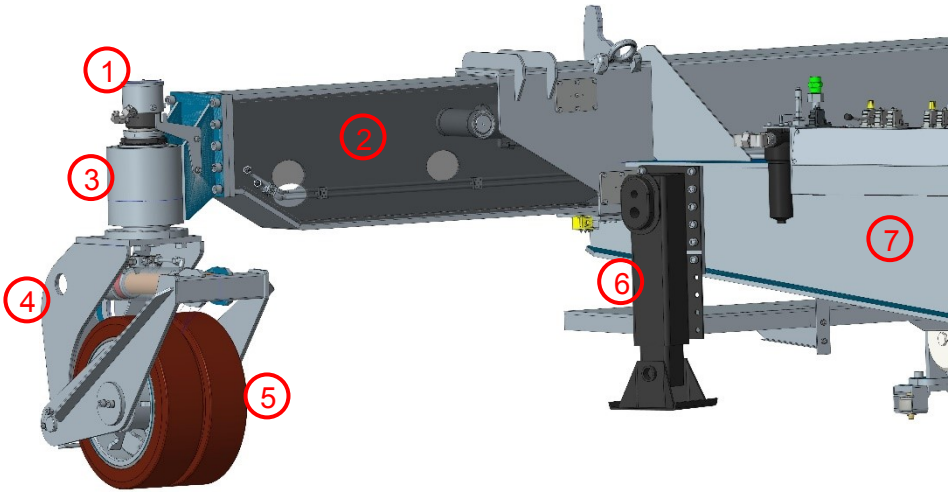


Abbildung 24: Ausleger mit Stützrolle, 1: Schleifring, 2: Ausleger, 3: Hydraulischer Drehverteiler, 4: Stützrolle, 5: Vulkollanrollen, 6: Stützwinde für den Fall, dass die Maschine über längeren Zeitraum nicht benutzt wird, 7: Grundgerüst des Unterwagens, Quelle: Eigene Darstellung

Der Unterwagen des STEPs darf eine Neigung von 0,2° nicht unterschreiten und 0,8° nicht überschreiten. Überwacht wird dies von zwei Neigungssensoren am Unterwagen, die links und rechts des Turmes angebracht sind. Ist die Neigung kleiner 0,2° beziehungsweise größer als 0,8°, werden sämtliche Maschinenbewegungen sofort gestoppt und somit die Maschine in einen sicheren Zustand gebracht. Damit

die Neigung, unabhängig vom Untergrund, innerhalb dieser Toleranz bleibt, wird der Unterwagen über die Abstützvorrichtung automatisch nivelliert. Die Nivellierregelung wird über den Druck der Nivellierzylinder und die Neigung des Unterwagens realisiert. Die Nivellierregelung steuert die beiden Nivellierzylinder individuell in Abhängigkeit der vorhandenen Druckdifferenz und damit indirekt der jeweiligen Abstützkraft, zwischen den beiden Zylindern sowie übergeordnet entsprechend der Neigung des Gesamtgerätes an.

Abbildung 25 zeigt den gesamten Unterwagen mit den oben beschriebenen Komponenten und den aufgebauten Containern. In den Containern befinden sich Ultrahochdruck Pumpen (UHP Pumpe – Ultra High Pressure Pumpe), die zur Bearbeitung der Schiffe benötigt werden. Sie erfüllen außerdem den Zweck der Ballastierung. Sollte der STEP nur zu Inspektion oder zum Beschichten eines Schiffes verwendet werden, kann das Abtragswerkzeug abgebaut werden. Werden die Container der UHP Pumpen ebenfalls abgebaut, müssen stattdessen Gewichte zur Ballastierung aufgebaut werden.

Über den Containern der UHP Pumpen befinden sich auf der linken Seite ein Dieselaggregat zur Stromerzeugung sowie ein Hydraulikaggregat auf der anderen Seite.

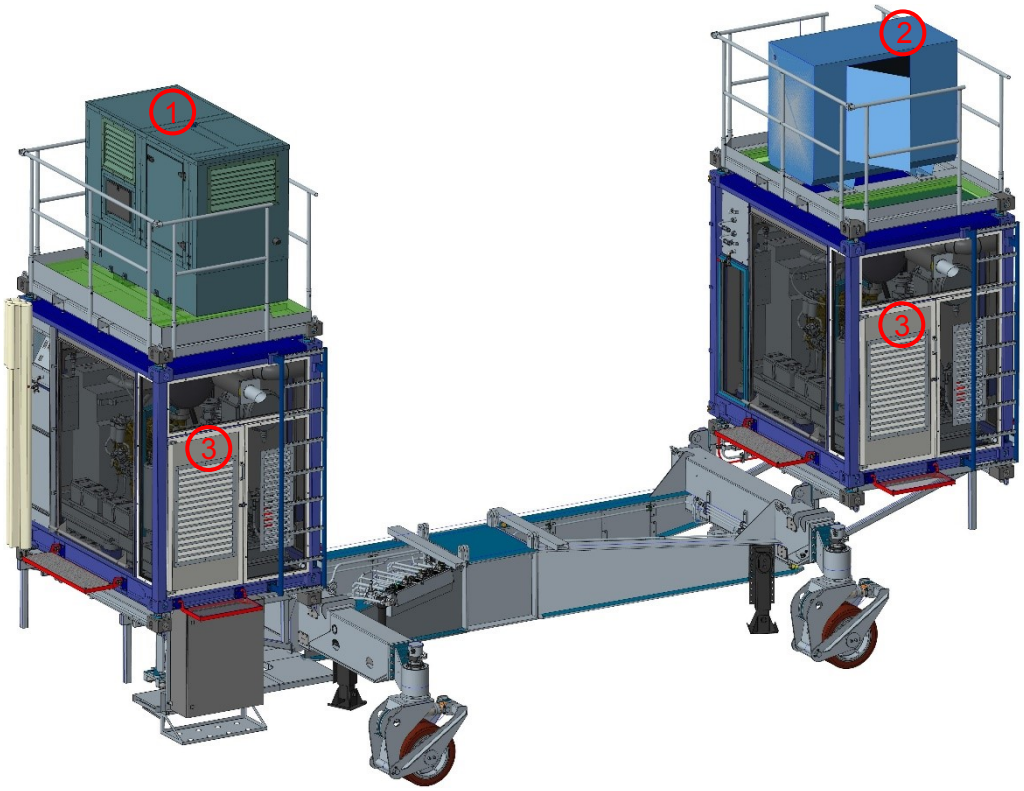


Abbildung 25: Unterwagen samt Containeraufbau. 1: Hydraulikaggregat, 2: Stromaggregat, 3: UHP Pumpe, Quelle: Eigene Darstellung

7.1.2 Teleskopturm

Zentrales Element des STEP stellt sein ausfahrbarer Turm dar. Dieser besteht aus drei in Fachwerkbauweise gefertigten Einzelsegmenten, die, jeweils über Rollen gelagert, ausgeschoben werden. Entgegen der allgemein bekannten Bauweise stellt beim STEP das innerste, kleinste Turmsegment das stationäre Element dar, welches fest mit dem Unterwagen verbunden ist. Diese außergewöhnliche Bauweise ermöglicht, dass an entsprechenden Führungen, entlang des äußersten Turmelements, die beiden Brücken eigenständig und individuell über die gesamte Höhe des besagten Turmelementes

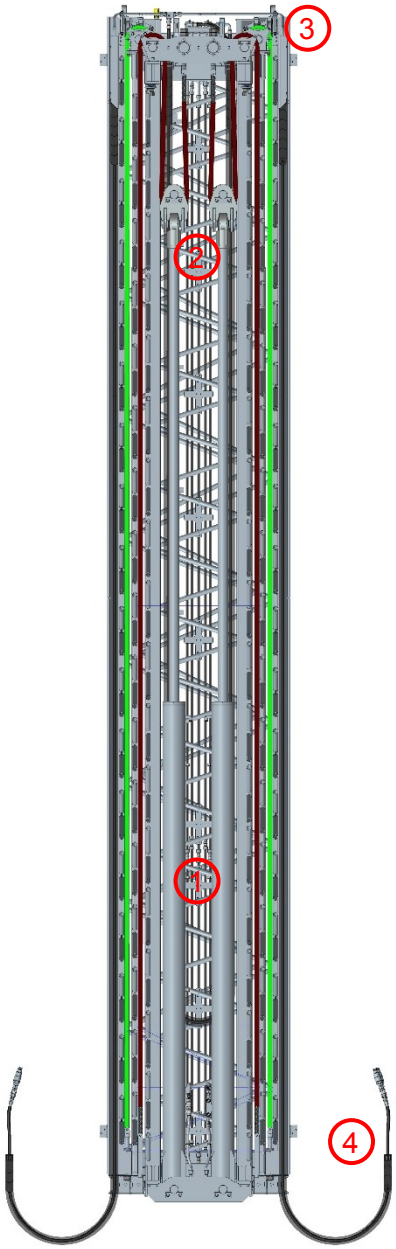


Abbildung 26: Schnitt durch den Teleskopturm. 1: Hydraulikzylinder, 2: Umlenkrollen Zylinder, 3: Umlenkrollen Turm, 4: Energiekette, Quelle: Eigene Darstellung

operieren können. Dies bewirkt eine höhere Flexibilität der einzelnen Korbeinheiten sowie ihrer Abtragwerkzeuge, was wiederum zu einer höheren Effizienz im Betrieb führt.

Abbildung 26 stellt einen Schnitt durch die Turmeinheit des STEP dar. Neben dem allgemeinen Aufbau des Turmes ist das für die Teleskopierung nötige Kettenlaufwerk ersichtlich. Dieses besteht aus insgesamt 2 redundanten Einheiten, welche symmetrisch innerhalb der Turmsegmente verlaufen.

Der Außenturm wird von zwei Flyerketten (Modell BL1266 - 90 kN Traglast) gehoben. In Abbildung 26 grün dargestellt. Diese Ketten beginnen am unteren, inneren Ende des Außenturmes, umlaufen am oberen Ende des Mittelturmes eine Umlenkrolle und enden am oberen Ende des Innenturmes. Aus dem Heben des Mittelturmes resultiert das Anheben des Außenturmes mit doppelter Geschwindigkeit des Mittelturmes.

Die beiden Kettenlaufwerke des Mittelturmes bestehen aufgrund der höheren Belastung aus jeweils zwei Flyerketten. Sie sind am inneren, unteren Ende des Mittelturmes befestigt, werden am oberen Ende des Innenturmes nach unten sowie an der Zylinderanbindung wieder nach oben umgelenkt und enden schlussendlich zentral an der Befestigungskonsole am oberen Ende des Innenturmes. In Abbildung 26 rot dargestellt. Dies ermöglicht einen doppelten Hubweg des Mittelturmes relativ zu den Bewegungen der Hubzylinder. Hierbei ist zu beachten, dass bei eingefahrenem Turm die Zylinder voll ausgefahren sind – und vice versa.

Die Überwachung der äußeren Kettenlaufwerke übernehmen Kettenbruch- bzw. Schlaffkettenüberwachungen. Die einwandfreie Funktionalität der inneren Kettenlaufwerke wird indirekt, durch Überwachung der Druckdifferenz zwischen den beiden Hubzylindern, überwacht.

Der Hub der Zylinder beträgt 3600 mm, wodurch sich Verfahrwege der einzelnen Turmsegmente um je 7200 mm ergeben und sich zu einem Gesamthub des Teleskopturmes von 14400 mm addieren. Im regulären Betrieb werden die Zylinder gleichmäßig mit je 205 kN Zugkraft (126 bar) beansprucht, diese Werte verdoppeln sich im nicht-redundantem Betrieb (Ausfall eines Kettenstranges) auf 410kN und 252 bar. Bei Eintritt dieses Falles kann aufgrund des gegenüber dem Systemdruck gestiegenen Zylinderdruckes keine Hebebewegung des Turmes mehr durchgeführt werden. Senkbewegungen sind jedoch immer möglich, bzw. können auch ohne vorhandenen Systemdruck im manuellen Betrieb durchgeführt werden.

Neben den Zylindern befindet sich im Innenturm auch die Energiekette, welche die oberen Enden von Innen- und Außenturm verbindet. Sie beinhaltet die gesamte hydraulische und elektrische Versorgung der beiden Brücken sowie daran angeschlossene Systeme.

7.1.3 Brücke, Schubarm

Die Brücke klettert auf einer Zahnstange entlang des äußersten Turmsegmentes auf und ab. Zwei Ritzel werden dabei von je einem Hydraulikmotor angetrieben. Zwei Hydraulikmotoren wurden aus Gründen der Redundanz aufgebaut. Somit kann auf eine Fangvorrichtung verzichtet werden. Sollte es zu einem Defekt in einem der beiden Motoren kommen, ist der zweite Motor in der Lage das gesamte Gewicht zu tragen beziehungsweise die Brücke sicher nach unten zu bewegen. Überwacht wird der Druck in der Arbeitsleitung der beiden Hydraulikmotoren durch zwei Druckschalter. Überschreitet der Druck einen definierten Grenzwert, wird die Kletterbewegung sofort gestoppt.

Nach Anwendungsbereich der EN 1495, siehe Kapitel 6.2, ist die Brücke durch ihre Antriebsart der harmonisierten Norm der Mastgeführten Kletterbühnen zuzuordnen. Abbildung 27 zeigt die gesamte Brücke mit eingefahrenem Schubarm.

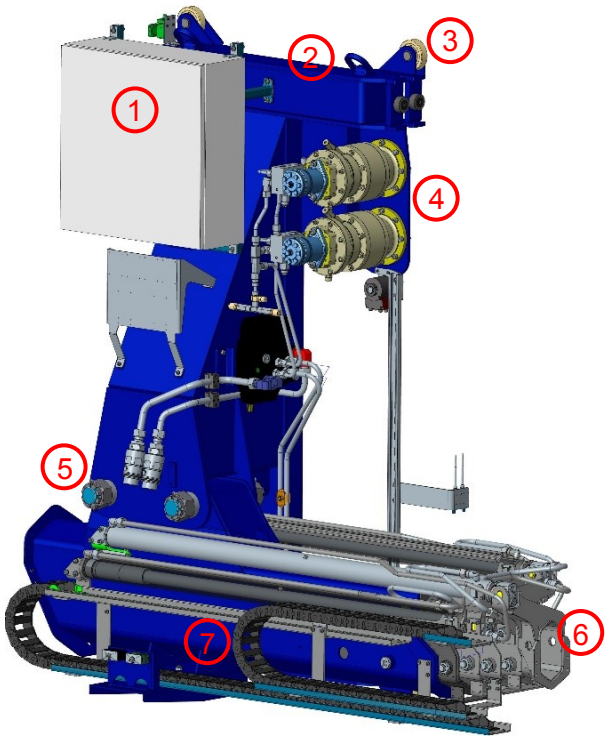


Abbildung 27: Brücke mit Schubarm, 1: Schaltschrank, 2: Brückenrahmen, 3: Führungsrollen, 4: Hydraulikmotoren, 5: Befestigung des Schubarms, 6: Schubarm mit Sechskant-Profil, 7: Energieketten, Quelle: Eigene Darstellung

In Abbildung 28 ist die Brücke mit ausgefahrenem Schubarm dargestellt. Der Schubarm ist bis auf sechs Meter teleskopierbar. Der Schubarm hat ein sechseckiges Profil und wird in dieser Form auch im Kranbau eingesetzt. Die Kabelführung für das Werkzeug am Arbeitskorb erfolgt in den Energieketten, die seitlich am Schubarm angebracht sind.

Hydraulisch ist der Schubarm ohne Folgesteuerung ausgeführt. Das Schubarmelement mit dem geringsten Widerstand wird als erstes bewegt.

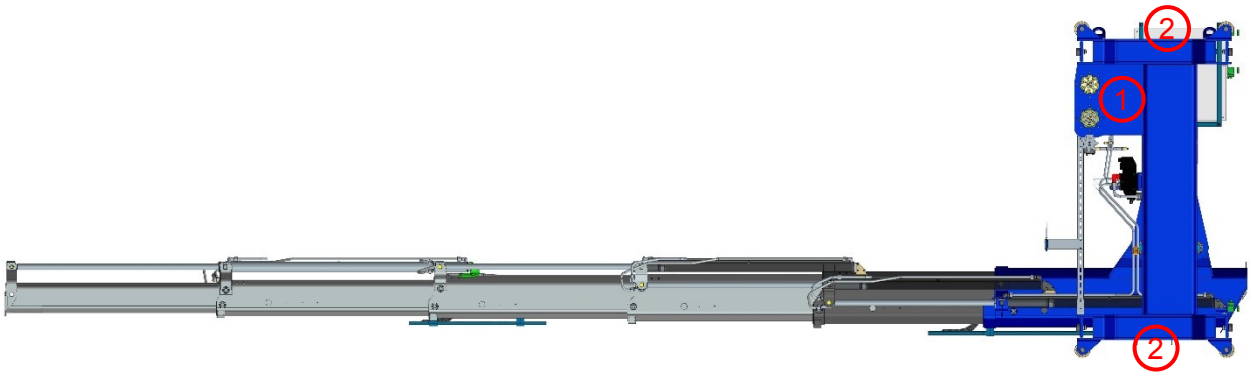


Abbildung 28: Brücke mit ausgefahrenem Schubarm, 1: Ritzel für die Brückenbewegung, 2: Führungsrollen oben und unten, Quelle: Eigene Darstellung

7.1.4 Arbeitskorb mit Werkzeug

Der Arbeitskorb ist über eine Drehkonsole mit dem Schubarm verbunden. Der Arbeitskorb kann 12° nach links und rechts geschwenkt werden. Um beim Einfahren des Schubarmes eine Kollision mit dem Teleskopturm zu verhindern, wird eine etwaige Schrägstellung des Arbeitskorbes überwacht. Kommt der Arbeitskorb in den Kollisionsbereich, wird die Bewegung des Schubarmes gestoppt und dem/der BedienerIn eine Warnung angezeigt.

Für den Kunden wird der STEP in zwei verschiedenen Ausführungen erhältlich sein. Einmal als Inspektions- und Beschichtungsplattform ohne Abtragswerkzeug und einmal mit der Zusatzfunktion Beschichtung am Schiff abtragen zu können. Dazu werden zwei Abtragswerkzeuge des Typen RJT05 (Rotor Jet Tool) an einer Führungseinheit angebracht - siehe Abbildung 29.

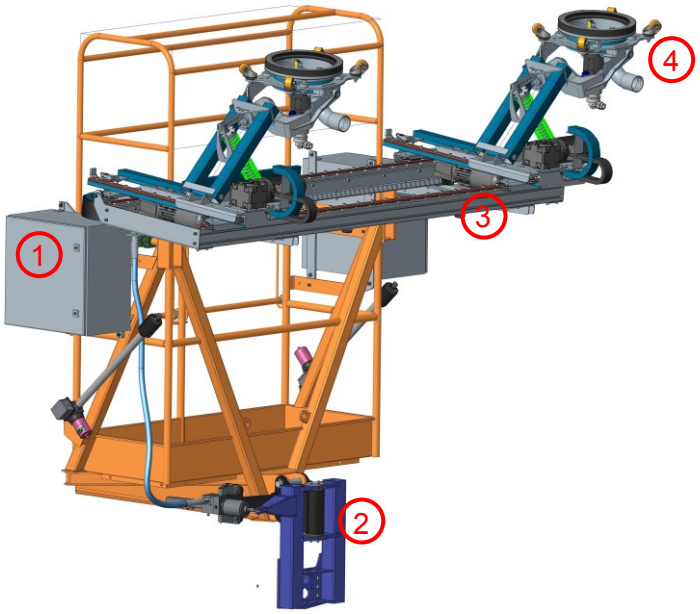


Abbildung 29: Arbeitskorb mit Rotor-Jet-Einheit, 1: Schaltschrank für Rotor-Jet-Einheit, 2: Drehkonsole, 3: Führungseinheit für X- und Y- Bewegungen, 4: Abtragswerkzeug, Quelle: Eigene Darstellung

Auf der Führungseinheit werden die Abtragswerkzeuge über insgesamt vier Drehstrommotoren in X- und Y-Richtung bewegt. Zusätzlich kann die ganze Führungseinheit 90° nach oben geschwenkt werden. Dies erfolgt über zwei Linearmotoren. Somit kann auch über Kopf abgetragen werden.

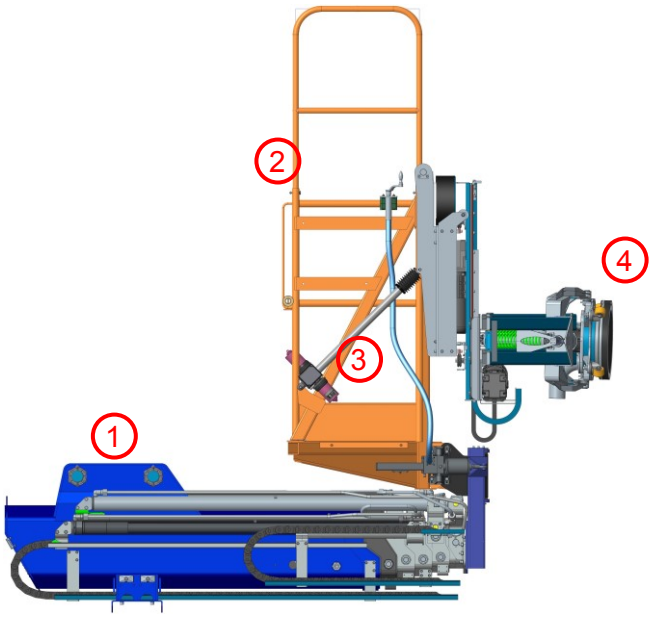


Abbildung 30: Schubarm mit angeflantschtem Arbeitskorb mit Rotor-Jet-Einheit, 1: teleskopierbarer Schubarm, 2: Arbeitskorb, 3: Linearmotor, 4: Abtragswerkzeug, Quelle: Eigene Darstellung

Für die Werkzeuge ergibt sich in X-Richtung eine Bearbeitungslänge von 2150 mm und in Y-Richtung eine Bearbeitungshöhe von 800 mm.

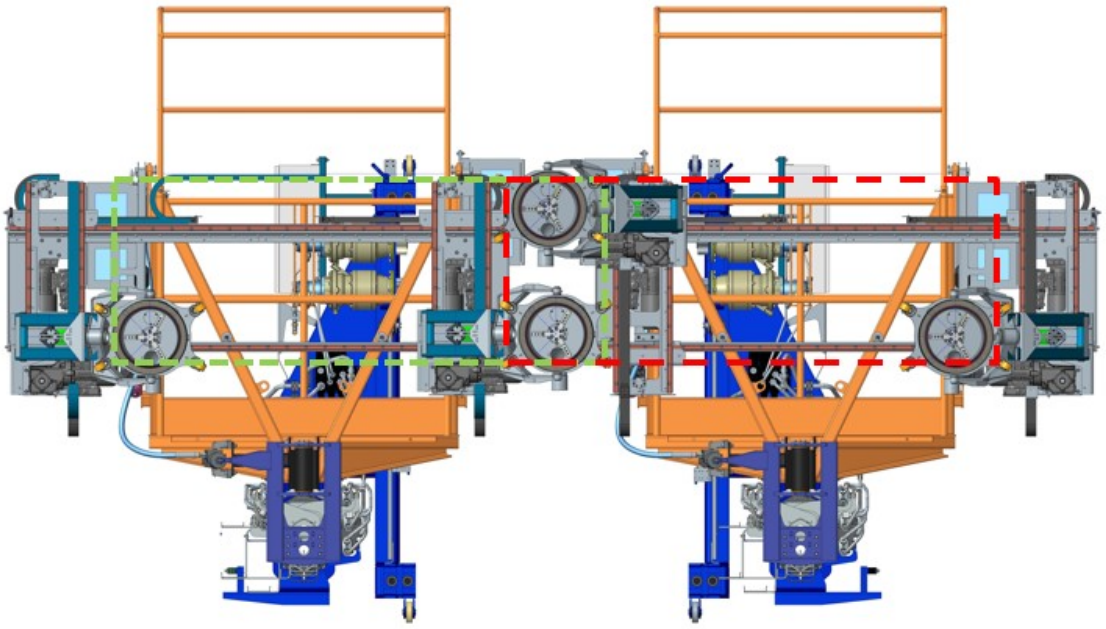


Abbildung 31: Arbeitskörbe inklusive der Abtragswerkzeuge, Quelle: Eigene Darstellung

7.2 Zusatzmaschinen – Hydraulikaggregat, Stromaggregat, Ultrahochdruck-Pumpe

Der STEP kommt ohne externe Energiezuführung aus. Dazu ist die Maschine mit einem Dieselaggregat zur Stromversorgung und einem Hydraulikaggregat ausgestattet. Keines der beiden Aggregate wird in die Steuerung des STEPs eingebunden. Sowohl das Dieselaggregat als auch das Hydraulikaggregat sind mit eigenen Steuerungen der Hersteller ausgestattet.

Beim Abtragen der Beschichtung der Schiffe wird mit einem Hochdruckwasserstrahl bis 3000 bar gearbeitet. Der Druck wird von der UHP Pumpe erzeugt. Aufgrund des Wasserstrahles und des rotierenden Düsensterns ergibt sich im Bereich der Abtragswerkzeuge eine potentielle Gefahrenquelle. Da das Starten des Hohlwellenmotors, welcher den Düsenstern antreibt beziehungsweise der Druckaufbau nur im angedockten Zustand möglich ist, kann die Gefahr für das Bedienpersonal möglichst klein gehalten werden.

8 RISIKOBEURTEILUNG STEP

Wie in Abbildung 5 gezeigt, ist für die Konformitätserklärung beim STEP eine Baumusterprüfung nötig. Für die Baumusterprüfung ist einer benannten Stelle die gesamte technische Dokumentation der Maschine zu übermitteln. Die Risikobeurteilung, wie sie in der MRL gefordert wird, ist Teil dieser technischen Dokumentation. In diesem Kapitel werden wesentliche Teile der Risikobeurteilung aufgegriffen, die für die spätere Analyse der Sicherheitsfunktion von Relevanz sind.

Unter anderem kommen folgende, zur Maschinenrichtlinie harmonisierte Normen, beim STEP zur Anwendung:

Typ-A-Norm:

- EN ISO 12100:2010 Sicherheit von Maschinen — Allgemeine Gestaltungsleitsätze — Risikobeurteilung und Risikominderung

Typ-B-Norm:

- EN 1037:1995+A1:2008 Sicherheit von Maschinen — Vermeidung von unerwartetem Anlauf
- EN ISO 4413:2010 Fluidtechnik — Allgemeine Regeln und sicherheitstechnische Anforderungen an Hydraulikanlagen und deren Bauteile
- EN ISO 13849-1:2015: Sicherheit von Maschinen — Sicherheitsbezogene Teile von Steuerungen — Teil 1: Allgemeine Gestaltungsleitsätze
- EN ISO 13849-2:2012: Sicherheit von Maschinen — Sicherheitsbezogene Teile von Steuerungen — Teil 2: Validierung
- EN ISO 13850:2015: Sicherheit von Maschinen — Not-Halt-Funktion — Gestaltungsleitsätze
- EN ISO 14119:2013: Sicherheit von Maschinen — Verriegelungseinrichtungen in Verbindung mit trennenden Schutzeinrichtungen — Leitsätze für Gestaltung und Auswahl
- EN ISO 14120:2015: Sicherheit von Maschinen — Trennende Schutzeinrichtungen — Allgemeine Anforderungen an Gestaltung und Bau von feststehenden und beweglichen trennenden Schutzeinrichtungen
- EN 60204-1:2006: Sicherheit von Maschinen — Elektrische Ausrüstung von Maschinen — Teil 1: Allgemeine Anforderungen
- EN 62061:2005: Sicherheit von Maschinen — Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronischer Steuerungssysteme

Typ-C-Norm:

- EN 280:2013+A1:2015 Fahrbare Hubarbeitsbühnen - Berechnung - Standsicherheit - Bau - Sicherheit – Prüfungen
- EN 1495:1997+A2:2009 Hebebühnen - Mastgeführte Kletterbühnen

8.1 Festlegen der Grenzen des STEPs

Wie im Prozess zur Risikobeurteilung in Abbildung 9 festgelegt werden als erster Schritt die Grenzen der Maschine definiert.

8.1.1 Verwendungsgrenzen

Der STEP dient in erster Linie als Hilfsmittel für Reinigungs-, Abtrags- und Beschichtungsarbeiten an Außenhüllen von Schiffen jeglicher Bauform im Onshore Bereich. Der STEP wird mithilfe eines Kranes, der in der Nähe des Docks montiert ist, in das Trocken- oder Schwimmdock gehoben und anschließend in Betrieb genommen. Die Bedienung des STEPs erfolgt direkt am Unterwagen beziehungsweise in den beiden Arbeitskörben. Für die Bedienung sind 3 Betriebsarten vorgesehen. Dazu gehören der Einrichtbetrieb, um die Maschine vor der Inbetriebnahme zu justieren, der Normalbetrieb während der ordnungsgemäßen Verwendung der Maschine und der Notbetrieb, um im Fehlerfall ein sicheres Absenken der Arbeitskörbe zu gewährleisten. Die Maschine darf nur von unterwiesenen Fachkräften, die die jeweils gültigen Sicherheitsbestimmungen und Errichtungsvorschriften beherrschen, transportiert, aufgestellt, angeschlossen, in Betrieb genommen, und gewartet werden. Bedienen darf den STEP nur geschultes Personal. Durch den Einsatz der Maschine in zutrittsbeschränkten Werftbetrieben mit unterwiesenem Personal besteht keine weitere spezifische Gefährdung.

Das Besteigen des Arbeitskorbs ist nur möglich, wenn sich die Maschine in der Grundstellung befindet. Die maximale Personenanzahl des Arbeitskorbes ist mit 2 Personen beschränkt. Das Fahren der Maschine entlang des Schiffes erfolgt schienengebunden und nur durch Zustimmung des gesamten Bedienpersonals. Die Maschine darf nur ihrer Funktion entsprechend genutzt werden. Die Einhaltung der Betriebsanleitung und aller Dokumente auf die in der Betriebsanleitung verwiesen werden, inklusive der darin enthaltenen Sicherheitsanweisungen sind verpflichtend einzuhalten. Jede Nutzung, die über die beschriebenen Einsatzmöglichkeiten hinausgeht, ist strengstens verboten.

8.1.2 Räumliche Grenzen

Die Maschine ist für die Verwendung im Freien in Schwimmdocks und Trockendocks in Industrieumgebung vorgesehen. Ebenso die Verwendung in Salzwasserumgebung.

Für die Bewegung der Maschine ist eine Schiene notwendig. Diese muss vor der Verwendung des STEP am Dockboden ausgelegt werden.

Für etwaige Wartungen am Teleskopturm sind abnehmbare Wartungspodeste mit entsprechenden Schutzgeländern vorgesehen.

Bedienkonsolen im Arbeitskorb sind mit dem Geländer verbunden. Für die Bedienkonsole am Unterwagen ist eine Halterung neben dem Bedienbildschirm am Schaltschrank angebracht. Während der Verwendung kann sie von der Bedienerin oder vom Bediener umgehängt werden. Sämtliche Bedienelemente sind mit einem Not-Aus-Schalter versehen.

Der Einsatz in explosionsgefährdeten Bereichen ist für den STEP nicht vorgesehen.

Die Maschine ist dafür vorgesehen an eine elektrische Stromversorgung von 400 V, drei Phasen, Neutralleiter und Schutzleiter angeschlossen zu werden. Die Vorsicherung muss mit einer gG (Ganzbereichsschutz für allgemeine Anwendung) 32 A Sicherung ausgeführt sein. Ob die Einspeisung über das örtlichen Energienetz oder das vorgesehene Stromaggregat erfolgt, ist dabei nicht von Relevanz.

8.1.3 Zeitliche Grenzen

Die Lebensdauer der Maschine hängt von den einzelnen Bauteilen und Maschinenteilen unter Berücksichtigung der bestimmungsgemäßen Verwendung und der vernünftigerweise vorhersehbaren Fehlanwendung ab. Bei Einhaltung der empfohlenen Wartungsintervalle einzelner Komponenten wurde seitens HPT eine Lebensdauer von 10 Jahren und 30.000 Betriebsstunden definiert. Das entspricht circa 180 Arbeitstagen zu je zwei Schichten mit acht Stunden.

8.1.4 Weitere Grenzen

Die Maschine befindet sich auf einem abgesperrten Betriebsgelände. Zutritt zu diesem Gelände gibt es nur für unterwiesene Personen.

Maximale Außentemperatur für den Betrieb + 50°C

Minimale Außentemperatur für den Betrieb - 10°C

Maximale Windgeschwindigkeiten: 40 km/h

Max. Zuladung im Korb: 250 kg

Max. Reichweite horizontal: 6.000 mm

Max. Reichweite vertikal: 30.000 mm

8.1.5 Vernünftigerweise vorhersehbare Fehlanwendungen

Folgende „vernünftigerweise vorhersehbare Fehlanwendungen“ werden für den STEP festgelegt:

- Transport von mehr als 2 Personen im Personenkorb bzw. einer maximal zulässigen Zuladung von mehr als 250 kg
- Beförderungen von Menschen außerhalb des Bedienstandes
- Das Befördern von Gütern, Gegenständen, Tieren, etc. ist strengstens verboten
- Einsatz der Maschine in explosionsfähiger Atmosphäre
- Nichteinhalten der Sicherheitshinweise speziell bei Wartungs- und Reparaturarbeiten
- Schweißarbeiten an tragenden Teilen sind verboten
- Es ist verboten, die Schaltschränke und Klemmkästen während des Betriebes zu öffnen
- Ein anderer als der definierte Einsatz der Maschine
- Überfüllung, Überlastungen, Überbeanspruchungen aller Art
- Umgehen von Sicherheitsvorkehrungen (Sicherheitsendschalter,…)
- Demontage von Schutzgittern, Schutzblechen, etc.
- Alle eigenständig durchgeführten Änderungen der Maschine ohne schriftliche Zustimmung des Herstellers
- Verwendung anderer als die vorgesehenen Ersatzteile, Schmiermittel, etc.
- Unzureichende Wartung
- Nicht geschultes und/oder nicht befugtes Bedienpersonal
- Betrieb der Maschine ohne Lesen von Betriebs- und Wartungsanleitung

8.2 Identifizierung der Gefährdungen

Um den Prozess aus Kapitel 5.4 zu folgen ist der nächste Schritt der Risikobeurteilung die Identifizierung der Gefährdungen. Um den Rahmen dieser Arbeit nicht zu sprengen werden nur jene Gefährdungen betrachtet, die nicht durch konstruktive Maßnahmen gelöst werden können beziehungsweise für diese Arbeit relevant sind.

Folgende Gefährdungen am STEP wurden im Zuge der Risikobeurteilung identifiziert:

- Stürzen von BedienerInnen aus dem Arbeitskorb beziehungsweise der gesamten Maschine. Der Ursprung dieser mechanischen Gefährdung ist dem Verlust der Standfestigkeit der Maschine geschuldet. Der Verlust der Standfestigkeit kann durch mehrere Ereignisse ausgelöst werden:
    - Über- beziehungsweise Unterschreiten der maximalen Neigungsgrenzen
    - Abstützeinrichtung ist nicht in der für den Betrieb vorgesehenen Endlage
    - Beschaffenheit des Untergrundes im Dock
- Überfahren von Bodenpersonal beziehungsweise Stürzen von Bedienpersonal im Arbeitskorb. Ursprung dieser Gefährdung ist eine zu hohe Geschwindigkeit während der Längsfahrt der Maschine. Der Aufenthalt des Bodenpersonals im Gefahrenbereich der Maschine ist einerseits durch die Bedienung und anderseits durch die Kontrolle des Fahrweges notwendig.
- Stürzen, Stoßen des Personals im Arbeitskorb. Die mechanische Gefährdung hat ihren Ursprung in der Schlaffung der Flyerkette. Aufgrund dieser Situation können ruckartige Bewegungen beim Anfahren passieren.
- Abstürzen des Bedienpersonals im Arbeitskorb, Erschlagen des Bodenpersonals durch herabfallende Gegenstände. Der Ursprung dieser mechanischen Gefährdung ergibt sich durch die Beweglichkeit der Maschine. Der Aufenthalt im Gefahrenbereich ergibt sich durch die Bedienung der Maschine.

8.3 Risikoeinschätzung

Im Folgenden wird die Einschätzung des Risikos für die aus Kapitel 8.2 identifizierte Gefährdung des Verlustes der Standsicherheit durch Überschreiten der maximalen Neigungsgrenzen durchgeführt. Die Einschätzung erfolgt anhand des Risikographs aus dem TR 14121-2:2012 siehe Abbildung 8. Alle anderen identifizierten Gefährdungen werden in dieser Arbeit nicht weiter betrachtet.

Schadensausmaß (S):

Kippt die Maschine, ist von schweren Verletzungen mit Todesfolge auszugehen. Deswegen ist dieser Gefährdung S2 zuzuordnen.

Exposition (F):

Die Gefahr des Verlusts der Standfestigkeit durch Über- beziehungsweise Unterschreiten der maximalen Neigungsgrenzen ist ständig gegeben. In diesem Fall muss der Gefährdung F2 zugeordnet werden.

Eintrittswahrscheinlichkeit eines Gefährdungsereignisses (O):

Die Maschine darf nur von gut ausgebildeten und unterwiesenen Personen bedient werden. Eine Erfahrung von mehr als sechs Monaten ist aber unrealistisch, deswegen muss die Gefährdung mit O3, also hoher Eintrittswahrscheinlichkeit, eingeschätzt werden.

Vermeidungsmöglichkeit (A):

Eine Vermeidung ist unmöglich, daher muss der Gefährdung A2 zugeordnet werden.

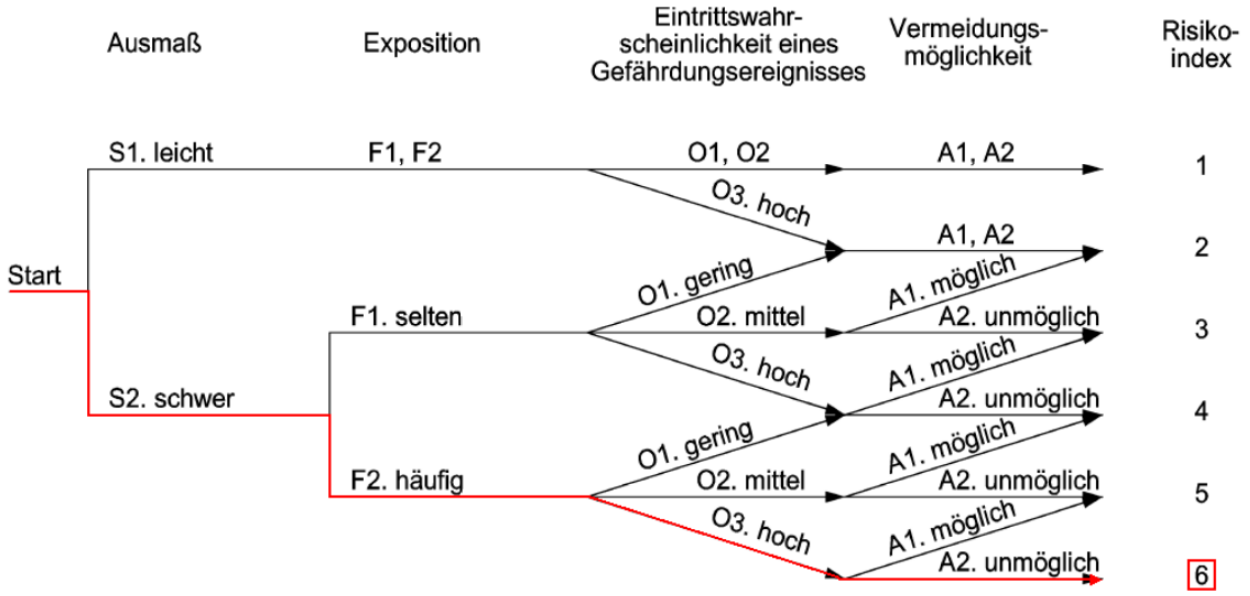


Abbildung 32: Risikograph aus dem TR 14121-2:2012 zur Einschätzung des Risikos durch Verlust der Standfestigkeit ohne Risikominderung, Quelle: ISO/TR 14121-2:2012 (2013), S. 19 (leicht modifiziert)

Die Einschätzung des Risikos ergibt also einen Risikoindex von „6“, welcher der höchsten Stufe entspricht.

8.4 Risikobewertung

In der Risikobewertung soll bewertet werden, ob die Einschätzung der Gefährdung aus Kapitel 8.3 einer Risikominderung bedarf oder nicht. Der aus der Risikoeinschätzung hervorgehende Risikoindex von „6“ für die Gefährdung des Verlustes der Standsicherheit bedarf natürlich einer Risikominderung. Daher wird im anschließenden Kapitel eine Risikominderung der Gefährdung durch Umsetzung von Schutzmaßnahmen in Übereinstimmung mit der EN ISO 12100:2010 durchgeführt.

8.5 Risikominderung

Das wirkungsvollste Verfahren zur Beseitigung von Gefährdungen sind konstruktive Maßnahmen. Die in der Norm EN ISO 12100:2010 unter Punkt 6.2.6 angeführten Punkte zur Vorkehrung der Standsicherheit wurden während der Konstruktion berücksichtigt. Außerdem wurden in der Konstruktion der Maschine mechanische Reserven berücksichtigt, die das Erreichen der Neigungsgrenzen erschweren. Zusätzlich werden in der Abstützvorrichtung Hydraulikzylinder eingesetzt, die der Neigung im positiven Sinn entgegen wirken. Diese Umstände sprechen zwar für eine niedrige Eintrittswahrscheinlichkeit, trotzdem führen diese Maßnahmen nicht zur gewünschten Minderung des Risikos. Das zeigt die Einschätzung des Risikos nach der Umsetzung der konstruktiven Maßnahmen in Abbildung 33.

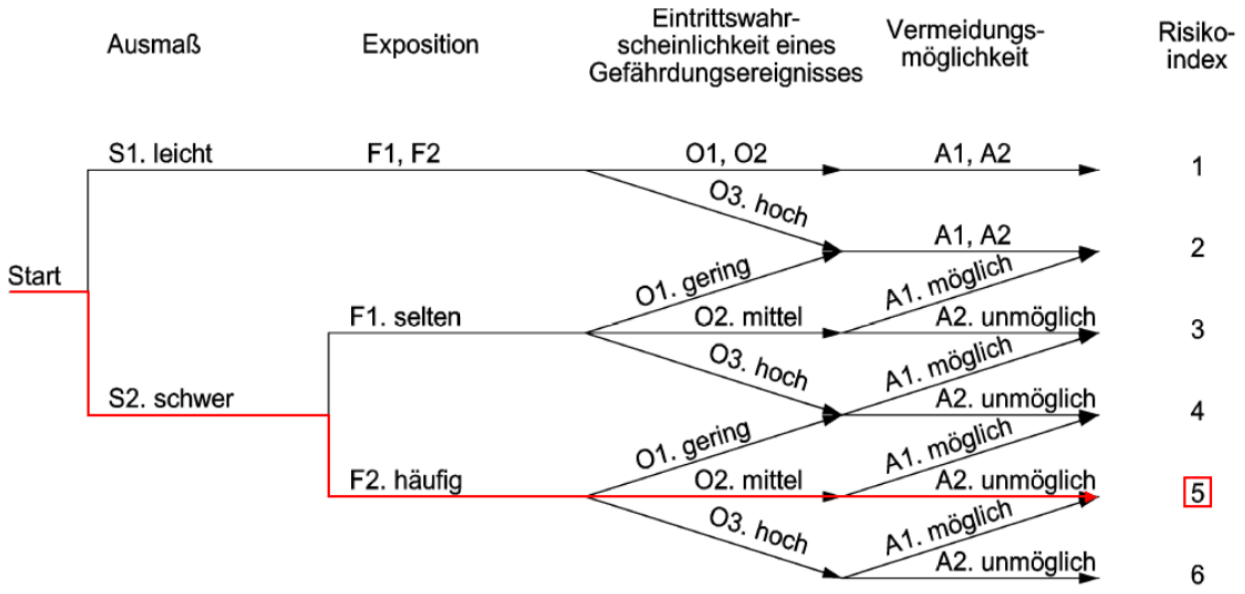


Abbildung 33: Einschätzung des Risikos durch Verlust der Standfestigkeit nach der Umsetzung konstruktiver Maßnahmen, Quelle: ISO/TR 14121-2:2012 (2013), S. 19 (leicht modifiziert)

Aus diesem Grund müssen weitere, technische Schutzmaßnahmen zur Risikominderung umgesetzt werden.

Das Risiko kann durch Überwachung der Neigungsgrenzen, das bei Über- oder Unterschreitung dieser Grenzen zum Abschalten von gefahrbringenden Bewegungen führt, hinreichend minimiert werden. Die Umsetzung dieser technische Maßnahme wird im nächsten Kapitel erläutert.

9 SICHERHEITSFUNKTION NEIGUNGSGRENZEN

Nur durch konstruktive Maßnahmen kann die Maschine nicht ausreichend standsicher konstruiert werden. Deswegen muss zusätzlich eine technische Schutzmaßnahme getroffen werden, um das Risiko angemessen zu minimieren. Die Sicherheitsfunktion zur Überwachung der Neigungsgrenzen wird in diesem Kapitel beschrieben.

9.1 Grundlegende Definition der Sicherheitsfunktion

Im folgenden Kapitel werden die Grenzen der Sicherheitsfunktion festgelegt. Außerdem werden die grundlegenden Bestandteile der Sicherheitsfunktion, die Häufigkeit der Anforderung sowie der erforderliche Performance Level bestimmt.

9.1.1 Grenzen der Sicherheitsfunktion

Am Beginn der Risikobeurteilung steht die Festlegung der Grenzen der Maschine. Analog zu diesem Prozess müssen auch für die Sicherheitsfunktion die Grenzen betrachtet und definiert werden.

9.1.1.1 Verwendungsgrenzen

Die Sicherheitsfunktion zur Überwachung der maximalen Neigungsgrenzen um das Kippen der Maschine zu verhindern, ist nur im Normalbetrieb der Maschine aktiv. Ausnahmslos in diesem Betrieb ist es gestattet Personen in den Arbeitskörben der Maschine an alle erreichbaren Plätze zu befördern. Daraus ergibt sich im Normalbetrieb auch die Möglichkeit, die für die Standfestigkeit der Maschine ungünstigsten Positionen anzufahren.

9.1.1.2 Räumliche Grenzen

Für die Sicherheitsfunktion werden keine räumlichen Grenzen definiert, da die Gefahrenstelle nicht räumlich begrenzt werden kann. Das Bedienpersonal in den Arbeitskörben und am Boden ist gleichermaßen gefährdet.

9.1.1.3 Zeitliche Grenzen

Die Gebrauchsdauer des STEPs beläuft sich auf 10 Jahre beziehungsweise 30.000 Betriebsstunden, siehe zeitlichen Grenzen der Maschine – Kapitel 8.1.3.

Die Sicherheitsfunktion ist nur im Normalbetrieb aktiv. Bei der Annahme, dass ein Viertel der 180 Arbeitstage für Montage, Demontage und Wartung benötigt wird, bleiben 135 Arbeitstage, die die Maschine im Normalbetrieb betrieben wird. 135 Arbeitstage pro Jahr im Zweischichtbetrieb zu je 8 Stunden pro Schicht, ergibt 16 Stunden pro Arbeitstag.

9.1.1.4 Maßnahmen zur vernünftigerweise vorhersehbaren Fehlanwendung

Eine Manipulation durch das Bedienpersonal oder durch nicht berechtigtes Personal an den Neigungssensoren der Maschine ist eine vernünftigerweise vorhersehbare Fehlanwendung. Zur Vermeidung dieser Fehlanwendung wurden die Neigungssensoren an einer schwer einsehbaren und zugänglichen Stelle der Maschine platziert. Außerdem werden die Eingangssignale der beiden Neigungssensoren in der Sicherheitssteuerung der Maschine überwacht. Kommt es zu einer Abweichung

zwischen den beiden Signalen der Neigungssensoren, ist von einer Manipulation der Neigungssensoren auszugehen.

9.1.2 Grundlegende Bestandteile der Sicherheitsfunktion

Mit der Festlegung der Grenzen der Sicherheitsfunktion im vorhergehenden Kapitel, können nun das auslösende Ereignis, die sicherheitsgerichtete Reaktion, sowie das gefahrbringende Maschinenteil näher spezifiziert werden.

9.1.2.1 Auslösendes Ereignis

Als auslösendes Ereignis dieser Sicherheitsfunktion gilt das Über- oder Unterschreiten der maximal zulässigen Neigungsgrenzen. Um den unerwarteten Verlust der Standsicherheit zu vermeiden, muss sich das Niveau des Unterwagens in einem Bereich von +0,2° und +0,8° bewegen. Werden diese Maximalwerte unter- oder überschritten, führt dies zum sofortigen Stillsetzen sämtlicher Maschinenbewegungen. Überwacht wird die Neigung mithilfe von zwei Neigungssensoren, die am Unterwagen des STEPs platziert sind.

Auslöser für das Über- oder Unterschreiten der maximal zulässigen Neigungsgrenzen können Witterungsbedingungen sein, wie zum Beispiel Wind. Aber auch Bedienfehler wie zum Beispiel das Fahren gegen Hindernisse mit dem Arbeitskorb können das Über- oder Unterschreiten der Neigungsgrenzen zur Folge haben.

9.1.2.2 Sicherheitsgerichtete Reaktion

Durch die sicherheitsgerichtete Reaktion wird ein sicherer Zustand hergestellt. Im Fall der Über- oder Unterschreitung der maximalen Neigungsgrenze wird ein sicherer Zustand durch ungesteuertes Stillsetzen (STO – safety torque off, sicher abgeschaltetes Moment) sämtlicher Maschinenbewegungen hergestellt. Dies wird durch Abschalten redundanter Hydraulikventile sichergestellt.

9.1.2.3 Ausfall der Energieversorgung

Die Sicherheitsfunktion zur Überwachung der Standfestigkeit ist bei vorhandener Energieversorgung, elektrisch wie hydraulisch, aktiv. Der energielose Zustand der Maschine ist dem sicheren Zustand der Maschine gleichzusetzen. Hydraulikventile werden durch Federrückstellung in Sperr-Mittelstellung gebracht, Zylinder schwerkraftbelasteter Maschinenteile sind mit Lasthalteventilen versehen und Hydraulikmotoren sind mit hydraulisch gelüfteten Bremsen ausgestattet. Somit sind keine gefahrbringenden Maschinenbewegungen mehr möglich.

Der Ausfall der Energieversorgung ist einem ungesteuerten Stillsetzen der Maschine gleichzusetzen.

9.1.2.4 Gefahrbringendes Maschinenteil

Bei der Sicherheitsfunktion der Über- oder Unterschreitung der maximal zulässigen Neigungsgrenzen ist die gesamte Maschine als gefahrbringendes Maschinenteil anzusehen. Kippt die Maschine um, sind Personen in den Arbeitskörben und Bedienpersonal am Boden beziehungsweise Werftpersonal gleichermaßen gefährdet.

9.1.3 Betriebsarten

Das Stillsetzen sämtlicher Maschinenbewegungen bei Über- oder Unterschreiten der maximalen Neigungsgrenzen, ist nur im Normalbetrieb sinnvoll – siehe Verwendungsgrenzen der Sicherheitsfunktion in Kapitel 9.1.1.1.

Der Einrichtbetrieb dient in erster Linie zum Einrichten des Unterwagens während des Montageprozesses. Während des Montageprozesses befindet sich die Maschine in Grundstellung und darf auch nicht in Längsrichtung bewegt werden. Die Gefahr des Verlustes der Standfestigkeit ist somit nicht gegeben. Das Befördern von Personen im Arbeitskorb im Einrichtbetrieb ist verboten.

Der Notbetrieb dient ausschließlich dazu, in Not geratene BedienerInnen in den Arbeitskörben, die nicht mehr in der Lage sind die Maschine zu steuern, vom Bedienstand zum Boden abzulassen. Des Weiteren ist es im Notbetrieb möglich, bei technischen Gebrechen sämtliche Maschinenteile vom Bedienpersonal am Boden in Grundstellung zu bringen, um Personen aus den Arbeitskörben zu befreien. Da im Notbetrieb keine Fahrt in Längsrichtung zulässig ist und Bewegungen nur nach unten gefahren werden dürfen, was zu keiner Verschlechterung der Neigung führt, ist die Gefahr des Kippens der Maschine nicht gegeben.

9.1.4 Häufigkeit der Anforderung

Die Sicherheitsfunktion ist während der Verwendung der Maschine nur im Normalbetrieb notwendig. In den zeitlichen Grenzen der Sicherheitsfunktion wird angenommen, dass die Maschine im Jahr 135 Tage im Normalbetrieb eingesetzt wird. Die mittlere Betriebszeit der Sicherheitsfunktion in Tagen pro Jahr (d_{op}) ist also 135 Tage pro Jahr. Bei zwei Schichten pro Tag ergibt das eine mittlere Betriebszeit der Sicherheitsfunktion (h_{op}) von 16 Stunden pro Tag. Abhängig von den Bedingungen im Dock wird angenommen, dass einmal pro Woche die maximal zulässigen Neigungsgrenzen über- oder unterschritten werden. Somit ergibt die mittlere Betriebszeit zwischen dem Beginn zweier aufeinander folgender Zyklen (t_{Zyklus}) 403.200 Sekunden je Zyklus.

d_{op}…mittlere Betriebszeit der Sicherheitsfunktion in Tagen pro Jahr

h_{op}…mittlere Betriebszeit der Sicherheitsfunktion in Stunden pro Tag

t_{Zyklus}…mittlere Betriebszeit zwischen dem Beginn zweier aufeinander folgender Zyklen der Sicherheitsfunktion in Sekunden je Zyklus

$$n_{op} = \frac{d_{op} * h_{op} * 3600}{t_{Zyklus}} = \frac{135\,Tage/Jahr * 16\,h/Tag * 3600\ s/h}{403.200\,s/Zylus} = \underline{\underline{19{,}29 \sim 20\,Zyklen/Jahr}}$$

Formel 1: Berechnung der mittleren Anzahl an Betätigungen pro Jahr

Mit den oben getroffenen Annahmen beziehungsweise Erfahrungswerten ergibt das eine mittlere Anzahl an Betätigungen von gerundet 20 Zyklen pro Jahr. Die Aktivierung der Sicherheitsfunktion erfolgt durch Auswahl der Betriebsart „Normalbetrieb“, die Anforderung erfolgt bei Über- oder Unterschreitung der maximal zulässigen Neigungsgrenzen.

9.1.5 Priorisierung bei gleichzeitig auftretenden Sicherheitsfunktionen

Die Sicherheitsfunktion Neigungsgrenzen ist bezüglich der Priorisierung, bei gleichzeitig auftretenden Sicherheitsfunktionen, nur der Sicherheitsfunktion „Not-Halt“ untergeordnet. Die Betätigung eines Not-Halt-Gerätes beim STEP hat die höchste Priorität, gefolgt von der Sicherheitsfunktion Neigungsgrenzen. Beide Sicherheitsfunktionen bewirken einen sicheren Zustand der Maschine.

9.1.6 Erforderlicher Performance Level – PL_r

Die Typ-C-Norm, EN 280:2013 für fahrbare Hubarbeitsbühnen, legt in Tabelle 5 Performance Leveln für Sicherheitseinrichtungen fest. Für die Überschreitung der Neigungsgrenzen wird mindestens ein PL_r von „c“ gefordert.

Im Zuge der Risikobeurteilung wurde zusätzlich eine Einschätzung über den Zusammenhang zwischen der betrachteten Gefährdung und dem Risiko durchgeführt. Wie in der Norm EN ISO 13849-1:2015 vorgeschlagen, wurde dazu der Riskograph verwendet – siehe Abbildung 11. Über die Einschätzung der zu erwartenden Verletzungsschwere, der Häufigkeit beziehungsweise Dauer der Gefährdungsexposition sowie der Möglichkeit zur Gefährdungsvermeidung kann somit der erforderlichen Performance Level PL_r der Sicherheitsfunktion ermittelt werden. Bei strenger Auslegung des Risikographs ergibt das einen PL_r von „e“.

Die EN IS0 13849-1:2015 beschreibt die Möglichkeit den PL_r um einen Level zu verringern, wenn die Eintrittswahrscheinlichkeit mit niedrig eingestuft werden kann. Durch die in Kapitel 8.5 erwähnten konstruktiven Maßnahmen wird die Maschine nur sehr selten an die Grenzen der maximal zulässigen Neigung kommen. Das spiegelt sich auch in der Häufigkeit der Anforderung in Kapitel 9.1.4 wieder. Aus diesem Grund kann der PL_r von „e“ auf „d“ verringert werden, siehe Abbildung 34.

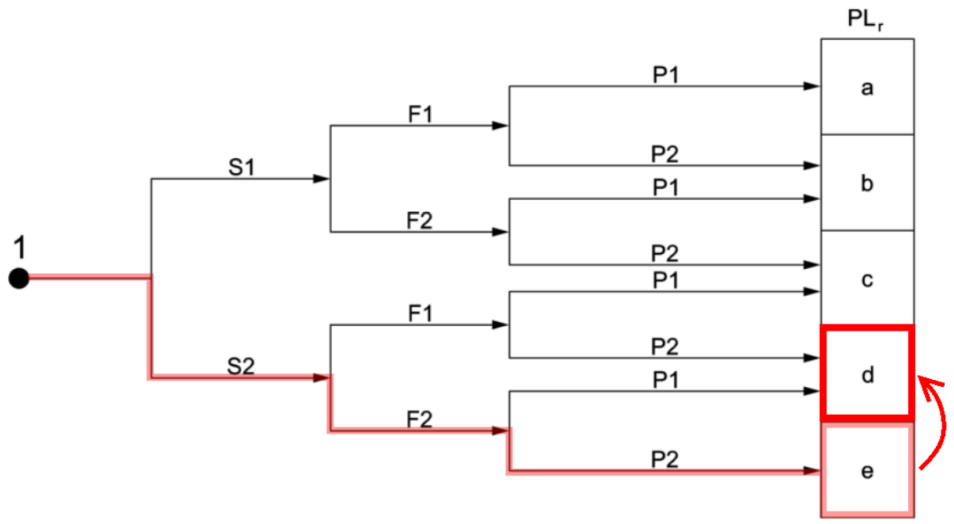


Abbildung 34: Bestimmung des erforderlichen Performance Level - PL_r der Sicherheitsfunktion mithilfe des Risikographes aus der Norm EN ISO 13849-1:2015, Quelle: EN ISO 13849-1:2015 (2015), S. 61 (leicht modifiziert)

9.2 Realisierung der Sicherheitsfunktion

Nach der Definition der Sicherheitsfunktion und der Festlegung des erforderlichen Performance Levels PL_r in den vorhergehenden Kapiteln kann nun die Sicherheitsfunktion nach diesen Kriterien entworfen werden.

9.2.1 Entwurf der Sicherheitsfunktion

Für die spätere Berechnung der Ausfallswahrscheinlichkeit der Sicherheitsfunktion ist es notwendig zu wissen, welche Bauteile in der Sicherheitsfunktion verwendet werden. Zur besseren Übersicht sind deshalb in Abbildung 35 alle sicherheitsbezogenen Teile der Sicherheitsfunktion dargestellt. Der Quittiertaster (S1), der der Wiederanlaufsperre dient, sowie der Schlüsselschalter (S2) zur Auswahl der Betriebsart sind ebenfalls im Prinzipschaltbild angedeutet. Sowohl die Wiederanlaufsperre, als auch die Auswahl der Betriebsart sind in einer eigenen Sicherheitsfunktion bewertet. Auf die Sicherheitsfunktion Neigungsgrenzen haben sie keinen direkten Einfluss, ergeben aber Anforderungen an die Software der Sicherheitsfunktion Neigungsgrenzen, weshalb die beiden Bauteile im Prinzipschaltbild eingezeichnet sind. Aus Übersichtsgründen wurde der hydraulische Teil vorerst weggelassen.

Das auslösende Ereignis, nämlich die Über- oder Unterschreitung der maximal zulässigen Neigungsgrenzen, wird über zwei Neigungssensoren (F1 und F2) sichergestellt. Die Neigungssensoren bestimmen die Neigung über ein verschleißbares Halbleitersensorelement und liefern über zwei 8-polige elektrische Leitungen ein analoges Stromsignal von 4 bis 20 mA an die fehlersichere Stromeingangskarte der Logik. Die Signale werden auf Plausibilität und Diskrepanz überprüft und im Sicherheitsprogramm der Steuerung (K1) verarbeitet. Über fehlersichere Digital-Ausgangkarten werden vier Koppelrelais (K2, K3, K4 und K5) angesteuert. Wird die Spule der Koppelrelais vom Strom durchflossen, schließen auch die zwangsgeführten Kontakte die der Fehlerdiagnose dienen. Sind beide Schließerkontakte geschlossen, wird die Spule der Magnetventile ebenfalls vom Strom durchflossen und die Hydraulikventile ändern ihre Stellung. Die Stellung der Hydraulikventile wird durch eine direkte Stellungsüberwachung überprüft.

In Abbildung 35 ist das elektrische Prinzipschaltbild dargestellt. Die markierten Bereiche zeigen Eingang, Logik und Ausgang der Sicherheitsfunktion.

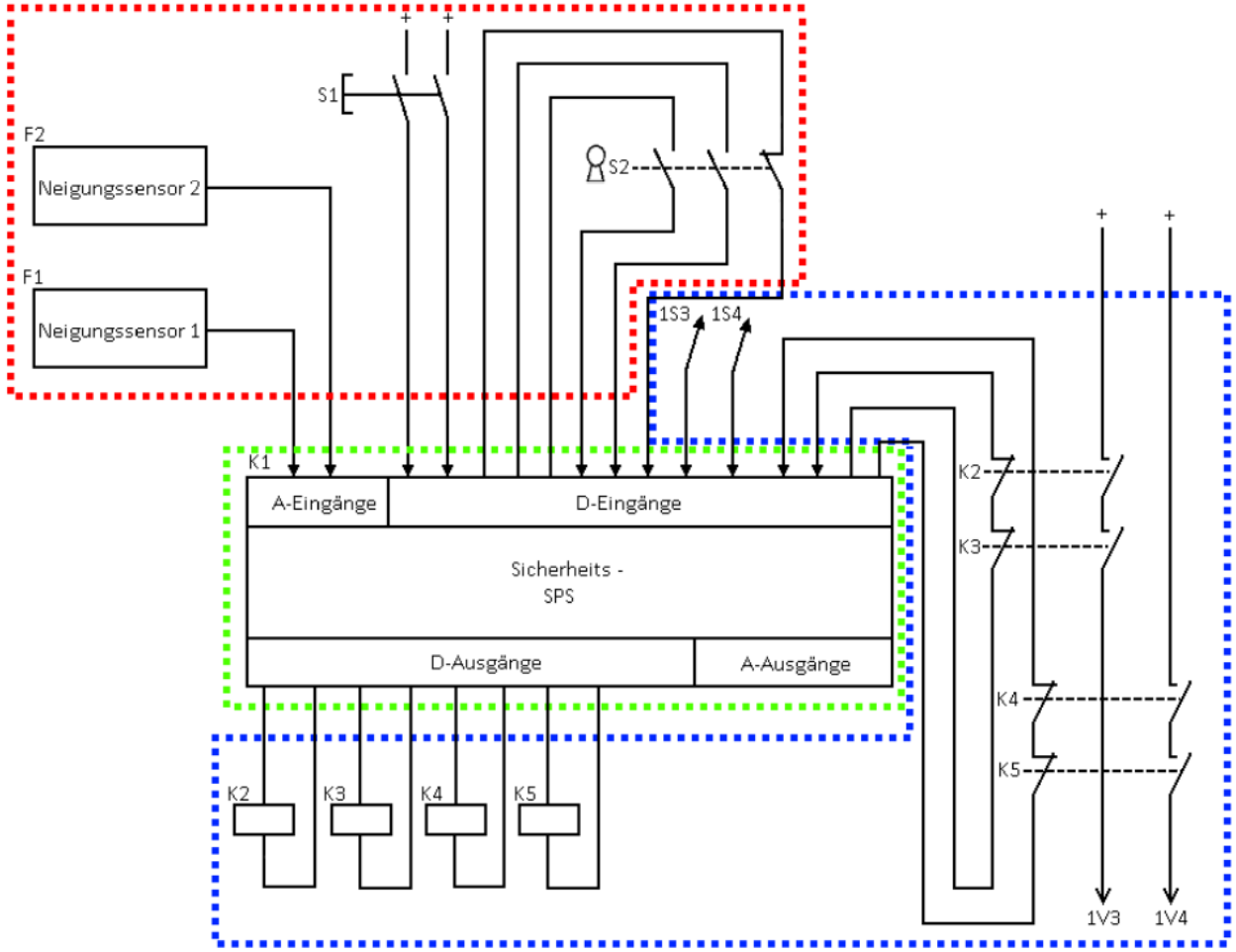


Abbildung 35: Elektrisches Prinzipschaltbild der Sicherheitsfunktion Neigungsgrenzen. Der rot markierte Bereich zeigt den „Eingang“, der grün markierte Bereich die „Logik“ und der blau markierte Bereich symbolisiert den „Ausgang“ der Sicherheitsfunktion. Quelle: Eigene Darstellung

9.2.2 Sicherheitsbezogene Bauteile der Sicherheitsfunktion

Im folgenden Abschnitt sind sämtliche sicherheitsbezogenen Bauteile der Sicherheitsfunktion aufgezählt und beschrieben.

9.2.2.1 Neigungssensoren F1 und F2

Zur Erfassung des Neigungswinkels werden Neigungssensoren am Unterwagen des STEPs montiert. Als Referenz für die Messung des Neigungswinkels werden die am Ort wirkende Gravitation beziehungsweise die Erdbeschleunigung genutzt. Die Neigungssensoren basieren auf einem mikro-elektro-mechanischen System (MEMS). Dabei wird ein kapazitives Sensorelement benutzt, bestehend aus zwei nebeneinander liegenden Plattenkondensatoren. Ein mikromechanisches Pendel bildet die gemeinsame mittlere Platte der beiden Kondensatoren. Ändert sich die Lage, verschiebt sich das mikromechanische Pendel und somit das Kapazitätsverhältnis der beiden Kondensatoren. Zur Ermittlung des Neigungswinkels wird die Änderung der elektrischen Kapazität genau gemessen.[66]

[66] Vgl. Hans Turck GmbH & Co. KG; Turck (Hrsg.) (2012), S. 481.

Bei den Neigungssensoren handelt es sich um Standard-Bauteile. Eine Sicherheitsbewertung der sicherheitsbezogenen Embedded-Software (SRESW), wie es die EN ISO 13849-1:2015 in Absatz 4.6.2 fordert, gibt es daher nicht. Seitens des Herstellers gibt es lediglich eine Angabe zum $MTTF_D$-Wert im Datenblatt des Neigungssensors, dieser beträgt 203 Jahre.[67]

Gemäß EN ISO 13849-1:2015, dürfen mehrere Bauteile für zwei Kanäle in Kategorie 2 oder 3 verwendet werden, um PL „c“ oder „d“ zu erreichen. Voraussetzung ist, dass die Bauteile der beiden Kanäle diversitäre Technologien verwenden.[68]

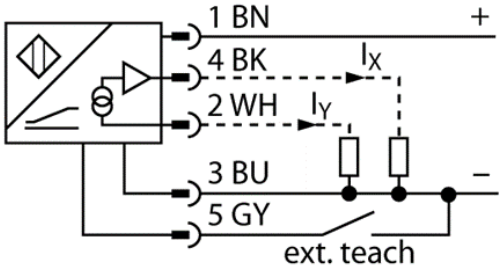


Abbildung 36: Anschlussbild des Turck Neigungssensors, Quelle: Hans Turck GmbH & Co KG, Turck (Hrsg.) (2016)

Der Neigungssensor F1 ist von der Firma Turck. Der Sensor hat einen Messbereich von ± 10° und liefert am Ausgang zwei analoge Stromsignale mit 4 bis 20 mA. Eine Nullpunktjustierung von ± 5° ist über einen Hardwarekontakt möglich. Siehe dazu das Anschlussbild in Abbildung 36. Beim Neigungssensor F2 handelt es sich um den baugleichen Sensor der Firma Kübler.

Mit der Verwendung unterschiedlicher Hersteller ist dem Punkt der Diversität genüge getan. Diversität im Zusammenhang mit CCF im Sinne der EN ISO 13849-1:2015 bedeutet:[69]

- Unterschiedliche Technologie oder physikalische Prinzipien werden verwendet, und /oder
- digitale und analoge Messung von Variablen, und/oder
- Bauteile von unterschiedlichen Herstellern

Der Punkt der unterschiedlichen Technologie kann im Fall der Neigungssensoren nicht erfüllt werden, weil die derzeit am Markt erhältlichen Sensoren alle auf MEMS Technologie basieren. Analoge Spannungswerte lassen sich in der Logik nicht fehlersicher erfassen, weswegen auch Punkt zwei nicht umsetzbar ist. Aus diesem Grund bleibt nur die Möglichkeit der unterschiedlichen Hersteller.

9.2.2.2 Fehlersichere Stromeingangskarte – K1

Die fehlersichere Stromeingangskarte von Siemens verfügt über sechs Analogeingänge mit Potentialtrennung zwischen den Kanälen und den Rückwandbus. Der Eingangsbereich des Bauteils reicht von 0 beziehungsweise 4 bis 20 mA. Die Stromeingangskarte ist im Sicherheitsbetrieb einsetzbar und erreiche einen PL von „e“ und Kategorie 4. Die Diagnose der Eingangssignale ist parametrierbar.

Zwei der sechs Eingänge werden für die Signale der Neigungssensoren benötigt.

Abbildung 37: Fehlersichere Stromeingangskarte von Siemens, Quelle: mall.industry.siemens.com

[67] Vgl. Hans Turck GmbH & Co KG, Turck (Hrsg.) (2016), S. 1.

[68] Vgl. EN ISO 13849-1:2015 (2015), S. 33 f.

[69] Vgl. 13849-1, S. 81

9.2.2.3 Central Processing Unit – CPU – K1

Abbildung 38: CPU von Siemens, Quelle: mall.industry.siemens.com

Die CPU 1512SP F-1 PN wurde für Standard- und fehlersichere Applikationen mit mittleren Anforderungen an die Verarbeitungsleistung und die Reaktionsgeschwindigkeit entwickelt. Der integrierte 3-Port-Switch ermöglicht eine Linienstruktur über Port 1 und 2. An Port 3 kann das HMI, welches am Hauptschaltschrank des STEPs angebracht ist, angeschlossen werden. Die CPU arbeitet völlig unabhängig von der zentralen Steuerung mit dem Vorteil, dass die CPU bei Ausfall der Steuerung weiter arbeitet. Daneben bietet die CPU umfangreiche Regelungsfunktionalitäten über einfach konfigurierbare Bausteine an, diese kommen zum Beispiel bei der Nivellierregelung zum Einsatz. Weiters besteht die Möglichkeit Antriebe über standardisierte PLC-open-Bausteine anzubinden. Die CPU kommuniziert mit den Unterbaugruppen über das PROFIsafe Protokoll.[70]

9.2.2.4 Fehlersichere Digitalausgabemodul – K1

Das fehlersichere Digitalausgabemodul besitzt 4 Ausgänge in PL „e“ und Kategorie 4. Jeder Ausgang liefert einen Ausgangsstrom von 2 A. Die Diagnose-Funktion erkennt neben Kurzschluss und Drahtbruch auch eine fehlende Lastspannung.

Angesteuert werden von dem Ausgangsmodul die Koppelrelais K2, K3, K4 und K5. Zusätzlich wird die Spule des Koppelrelais unter anderem auf Kurzschluss und Querschluss überwacht, indem der Ausgang der Spule wieder ins Ausgabemodul zurückgeführt wird.

Abbildung 39: Fehlersichere Digital-Ausgangskarte von Siemens, Quelle: mall.industry.siemens.com

9.2.2.5 Koppelrelais – K2, K3, K4, K5

Die Koppelrelais sind das Bindeglied zwischen der Steuerung und den Aktoren. Das eingesetzte Koppelrelais von Phoenix Contact ist ein Universal-Sicherheitsrelais mit zwangsgeführten Kontakten. Für die sicherheitsrelevante Betrachtung sind als Fehler nur Öffnungsversagen und Isolationsversagen von Bedeutung.

Das Relais besitzt einen Öffner und einen Schließer mit Zwangsführung, also eine mechanische Vorrichtung, die verhindert, dass Öffner und Schließer zur gleichen Zeit den gleichen Schaltzustand haben. Der Öffner wird dabei als Rückmeldekontakt verwendet. Kommt es beim antivalenten Kontakt zu einem Öffnungsversagen, kann der Rückführkreis nicht geschlossen werden und somit ein Fehler detektiert

[70] Vgl. Siemens AG (2016), Online-Quelle [3.12.2017]

werden. Abbildung 41 zeigt das Anschlussbild des Koppelrelais. Eine korrekte Funktionsweise ist nur bei Verwendung eines Öffners und eines Schließers gegeben. Der maximale Einschaltstrom beträgt 6 A[71].

Abbildung 40: Koppelrelais von Phoenix Contact, Quelle: www.phoenixcontact.com

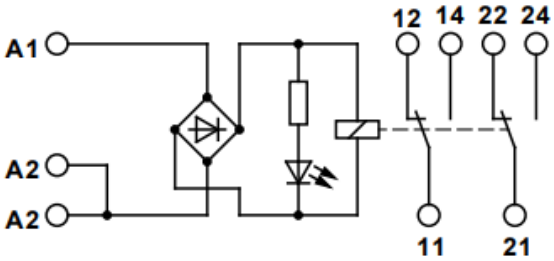


Abbildung 41: Anschlussplan des Koppelrelais von Phoenix mit zwangsgeführten Kontakten, Quelle: Phoenix Contact; Phoenix Contact (Hrsg.) (2004), S. 2.

9.2.2.6 Hydraulikventile 1V3 und 1V4

Bei den Hydraulikventilen werden elektrisch betätigte Ventile der Firma Danfoss verwendet. Danfoss-Ventilblöcke können je nach Anwendungsfall individuell zusammengestellt werden. Bei der Auswahl der Komponenten kommt ein interner Palfinger-Standard aus dem Kranbau zum Tragen. Die Ventile haben aus diesem Grund mehr Stellungen als für die Funktion notwendig.

Abbildung 42: Ventilblock der Firma Danfoss, Quelle: powersolutions.danfoss.at

Das Hauptfreigabeventil 1V3 ist als 5/3 Wegeventil mit Sperr-Mittelstellung ausgeführt. Die Rückstellung erfolgt mittels Federn. Somit wird auch im energielosen Zustand eine Rückstellung in Sperr-Mittelstellung gewährleistet.

Das Freigabeventil für einzelne Baugruppen ist als 3/3 Wegeventil ausgeführt. Das Ventil ist ebenfalls mit Sperr-Mittelstellung und Federrückstellung ausgeführt.

Beide Ventile werden elektrisch betätigt. Die maximale Stromaufnahme bei 24 V Versorgungsspannung gibt der Hersteller mit 420 mA an.[72]

9.2.3 Funktionsbeschreibung der Sicherheitsfunktion

Die beiden Neigungssensoren F1 und F2, die am Unterwagen des STEPs angebracht sind, überwachen während des Betriebes die Neigung des Unterwagens. Aufgrund unterschiedlicher Einflüsse, wie zum Beispiel Bewegungen der Schubarme oder äußere Einflüsse, wie zum Beispiel Wind, ändert sich die Neigung des Unterwagens ständig. Die maximalen Neigungsgrenzen von +0,2° und +0,8° dürfen nicht unter- beziehungsweise überschritten werden. Die analogen Ausgangssignale der beiden Neigungssensoren werden in die Sicherheits-SPS K1 eingelesen. K1 steuert, über redundant ausgeführte

[71] Vgl. Phoenix Contact; Phoenix Contact (Hrsg.) (2004), S. 2.

[72] Vgl. Danfoss Power Solutions GmbH & Co. OHG (2014), S. 35.

Koppelrelais mit zwangsgeführten Kontakten (K2, K3, K4 und K5), den hydraulischen Steuerungsteil und somit die Freigabe sämtlicher Bewegungen der Maschine – siehe Abbildung 43.

Der hydraulische Steuerungsteil ist zweikanalig aufgebaut. Der erste Kanal besteht aus einem 5/3 Wegeventil 1V3, das in Sperr-Mittelstellung sämtliche Bewegungen der Maschine unterbindet. Der zweite Kanal besteht aus einem 3/3 Wegeventil 1V4, das ebenfalls eine Sperr-Mittelstellung besitzt und somit keine Bewegungen der nachfolgenden Zylinder zulässt – siehe Abbildung 44.

Der alleinige Ausfall eines der genannten Ventile führt nicht zum Verlust der Sicherheitsfunktion.

Die Ventile 1V3 und 1V4 werden bei Überschreiten der maximalen Neigungsgrenzen, was der Anforderung der Sicherheitsfunktion entspricht, angesteuert, zusätzlich wenn ein Not-Halt-Gerät gedrückt wird, jedoch mindestens einmal pro Schicht, wenn die Maschine gestartet wird.

Als Maßnahme zur Fehlererkennung ist an 1V3 und 1V4 eine direkte Stellungsüberwachung 1S3 und 1S4 vorgesehen, die in der Sicherheits-SPS K1 ausgewertet wird. Die Anhäufung unentdeckter Fehler kann zum Verlust der Sicherheitsfunktion führen.

9.2.3.1 Elektrisches Prinzipschaltbild

Zur Übersicht sind in Abbildung 43 alle sicherheitsbezogenen Teile der Sicherheitsfunktion Neigungsgrenzen dargestellt, vom Eingang, über die Logik bis zum Ausgang. Aus Übersichtsgründen ist der hydraulische Teil in Abbildung 44 separat dargestellt.

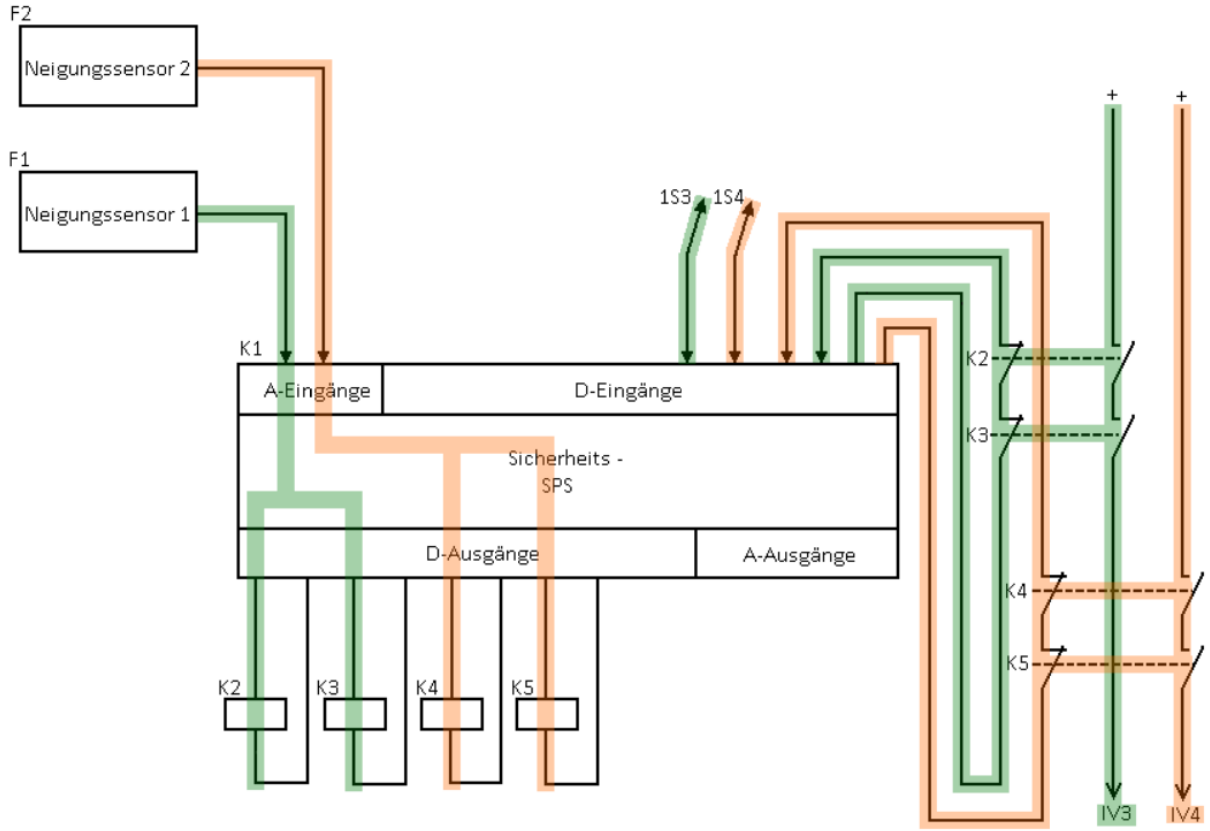


Abbildung 43: Elektrisches Prinzipschaltbild. Der grün markierte Pfad zeigt den Funktionskanal 1, der orange markierte Pfad Funktionskanal 2. Quelle: Eigene Darstellung

Das elektrische Prinzipschaltbild zeigt außerdem die redundanten Funktionskanäle der Sicherheitsfunktion. Im Wesentlichen bestehen die beiden Kanäle aus den gleichen Komponenten. In Abbildung 43 ist der erste Funktionskanal grün markiert, der zweite Funktionskanal ist in oranger Farbe gekennzeichnet.

9.2.3.2 Hydraulisches Prinzipschaltbild

Abbildung 44 zeigt neben den wesentlichen hydraulischen Bauteilen der Sicherheitsfunktion auch die für die Einhaltung der grundlegenden und bewährten Sicherheitsprinzipien relevanten Komponenten.

Zu den sicherheitsbezogenen Teilen der Sicherheitsfunktion zählen das elektrisch betätigte 5/3 Wegeventil 1V3 und das elektrisch betätigte 3/3 Wegeventil 1V4. Beide Ventile werden durch eine Feder in Mittelstellung zurückgestellt und besitzen eine Sperr-Mittelstellung. Das bedeutet, im energielosen Zustand sind keine Bewegungen der Maschine möglich. Wird die Maschine durch Über- oder Unterschreitung der Neigungsgrenzen in den sicheren Zustand gebracht, befinden sich die Ventile ebenfalls in Sperr-Mittelstellung.

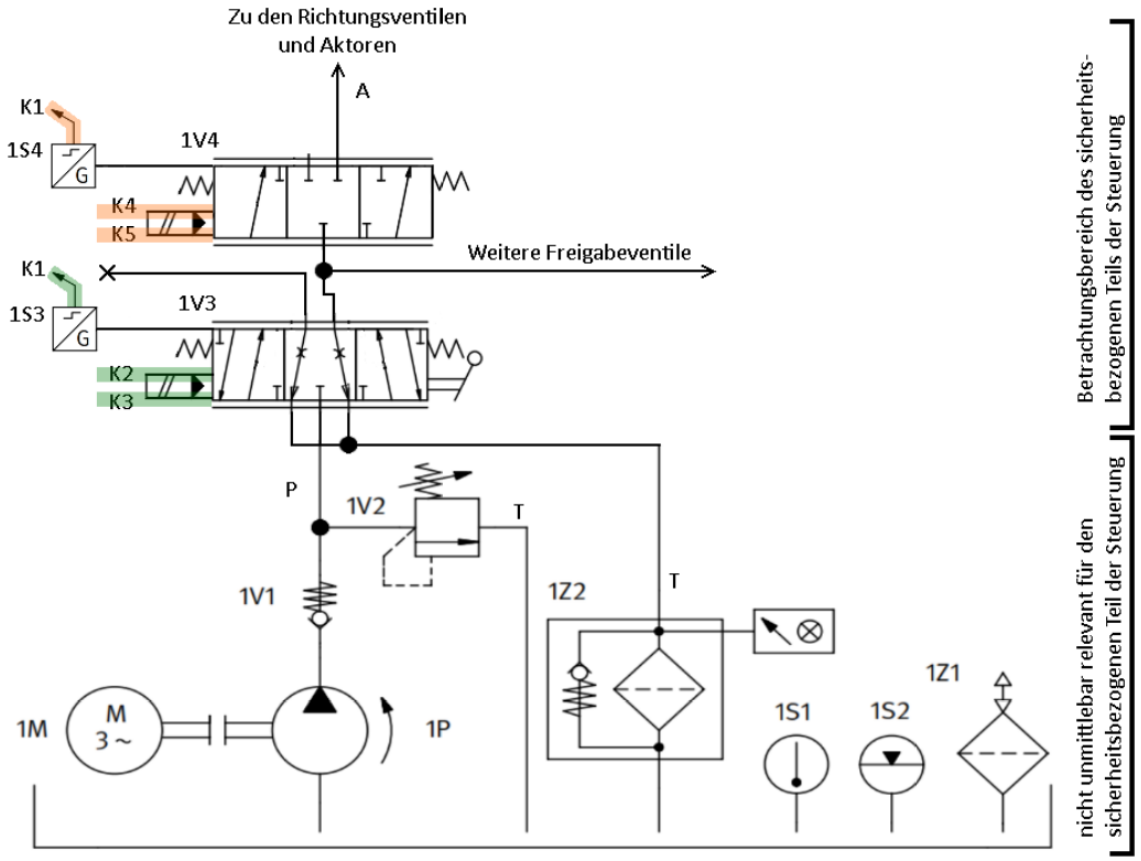


Abbildung 44: Vereinfachtes hydraulisches Prinzipschaltbild, die markierten Bereiche zeigen die Schnittstellen zum elektrischen Prinzipschaltbild in Abbildung 43. Die Spulen der Magnetventile werden über die Koppelrelais von der Steuerung K1 gesteuert. 1S3 und 1S4 symbolisieren eine direkte Stellungsüberwachung der Hydraulikventile. Quelle: Eigene Darstellung

9.2.4 Konstruktive Merkmale der Sicherheitsfunktion

Die grundlegenden und bewährten Sicherheitsprinzipien für hydraulische und elektrische Systeme, wie in der Norm EN ISO 13849-2:2012, in Anhang C und Anhang D angeführt, wurden eingehalten. Ebenso wurden die Anforderungen der Kategorie B, wie in Kapitel 5.7.1 aufgezählt, eingehalten.

Fehler in den Anschlussleitungen von F1, F2 und K1 dürfen sich nicht gefährlich auswirken. Hierzu werden auftretende Fehler in K1 erkannt und der sichere Zustand der Maschine eingeleitet.

Bei der Sicherheits-SPS K1 handelt es sich um ein geprüftes Sicherheitsbauteil für den Einsatz in PL „e“, das der Kategorie 4 und den jeweiligen Produktnormen entspricht.

Die Wegeventile 1V3 und 1V4 haben eine Sperr-Mittelstellung mit ausreichend positiver Überdeckung und Federzentrierung. 1V3 und 1V4 sind mit elektrischer Stellungsüberwachung ausgeführt, da keines der Ventile zyklisch geschaltet wird.

Die Programmierung der Sicherheits-Software erfolgt entsprechend den Anforderungen für PL „d“. Anforderungen der Sicherheitsfunktion an die Software sind in Kapitel 9.2.5 angeführt.

9.2.5 Anforderungen an die Software der Sicherheitsfunktion

Neben der Hardware ist auch die Software ein essentieller Teil bei der Gestaltung von sicherheitsbezogenen Teilen von Steuerungen. Fehler in der Software können ebenfalls zum Ausfall der Sicherheitsfunktion führen. Aus diesem Grund werden auch an die sicherheitsbezogene Embedded- beziehungsweise Anwendungssoftware von Steuerungen, sowie deren Entwicklung Anforderungen gestellt. Diese sind in der EN ISO 13849-1:2015 festgelegt. Das Hauptziel der Anforderungen ist es, lesbare, verständliche, testbare und wartbare Software zu erhalten.[73]

Der Unterschied zwischen Software- und Hardwarefehler ist, dass Softwarefehler nicht durch defekte Bauteile entstehen, sondern systematische Ursachen haben. Bei der Entwicklung von sicherheitsbezogener Software werden deswegen bereits validierte Funktionsblöcke eingesetzt. Die Entwicklung der sicherheitsbezogenen Anwendungssoftware ist nicht Teil dieser Arbeit. Deswegen wird auch nicht näher an die Anforderungen der Software nach EN ISO 13849-1:2015 eingegangen.

9.2.6 Strukturanalyse der Sicherheitsfunktion

In der Strukturanalyse werden die Bauteile aus den elektrischen und hydraulischen Prinzipschaltbilder in ein sicherheitsbezogenes Blockdiagramm übertragen und somit die Kategorie anhand der Merkmale Redundanz, Testung und Verwendung bewährter Bauteile bestimmt. Vorgegangen wird dabei nach dem vereinfachten Verfahren zur Abschätzung der quantifizierbaren Aspekte des PL aus der EN ISO 13849-1:2015, Abschnitt 4.5.4.

- **Bauteile des Funktionskanals aneinanderreihen**
  Alle Bauteile eines Kanals aus dem elektrischen und hydraulischen Prinzipschaltbildern (Abbildung 43 und Abbildung 44) werden aneinandergereiht, beginnend mit dem Funktionskanal, der die geringste Anzahl an Bauteilen hat. Im Fall dieser Sicherheitsfunktion haben beide Funktionskanäle die gleiche Anzahl an Bauteilen. Abbildung 45 zeigt alle Bauteile des ersten Funktionskanals: Neigungssensor (F1), Logik (K1), Koppelrelais (K2 und K3) und das Hydraulikventil mit Stellungsüberwachung (1V3 mit 1S3)

[73] Vgl. EN ISO 13849-1:2015 (2015), S. 32.

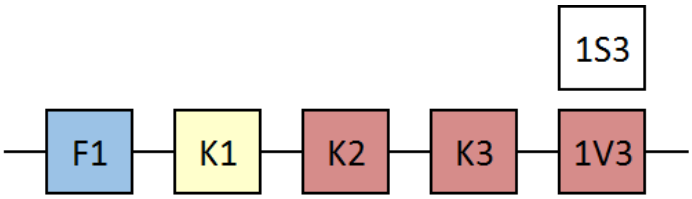


Abbildung 45: Sämtliche Bauteile aus Funktionskanal 1 vom Sensor bis zum Aktor, Quelle: Eigene Darstellung

- **Jeden Block betrachten**

  Anhand der charakteristischen Merkmale der Kategorien wird für jeden Block eine Zuordnung in Subsysteme der zutreffenden Kategorie vorgenommen.

  - Nennt der Bauteilhersteller einen PL oder gibt er einen PFH_D-Wert und eine Kategorie an, wird von einem gekapselten Subsystem gesprochen. Eine weitere Zerlegung ist dann nicht mehr notwendig. Befindet sich ein gekapseltes Subsystem in beiden Funktionskanälen, laufen beide Funktionskanäle über dieses Subsystem. Im Fall STEP ist die Logik ein gekapseltes Subsystem, das in beiden Funktionskanälen vorkommt.
  - Werden kein PL oder PFH_D-Wert angegeben, müssen für die Blöcke nacheinander alle anzunehmenden Fehler betrachtet werden. Bleibt die sicherheitstechnisch beabsichtigte Funktion erhalten, wird von einem ungefährlichen Ausfall ausgegangen, bei Ausfall der Sicherheitsfunktion von einem gefährlichen Ausfall. Können alle Bauteilfehler ausgeschlossen werden, ist der Block ein gekapseltes Subsystem mit Fehlerausschluss.

- **Auswirkungen durch Bauteilfehler**

  Durch den redundanten Funktionskanal bleibt bei Ausfall eines Bauteils die Sicherheitsfunktion erhalten. Ein redundanter Funktionskanal ist beim STEP vorhanden, also wird mindestens Kategorie 3 oder Kategorie 4 erreicht. Bleibt die Sicherheitsfunktion auch bei Anhäufung unerkannter Fehler erhalten, wären die Kriterien für Kategorie 4 erfüllt. Dies ist beim STEP nicht der Fall.

Wurden alle Blöcke betrachtet, können Blöcke gleicher Kategorie zusammengefasst werden.

Die Strukturanalyse der Sicherheitsfunktion ergibt eine zweikanalige Struktur. Die Anhäufung unerkannter Fehler kann zum Ausfall der Sicherheitsfunktion führen. Die Einfehlersicherheit ist jedoch gegeben, somit wird mit dieser Struktur Kategorie 3 erreicht. Abbildung 46 zeigt das Blockschaltbild der Sicherheitsfunktion Neigungsgrenzen.

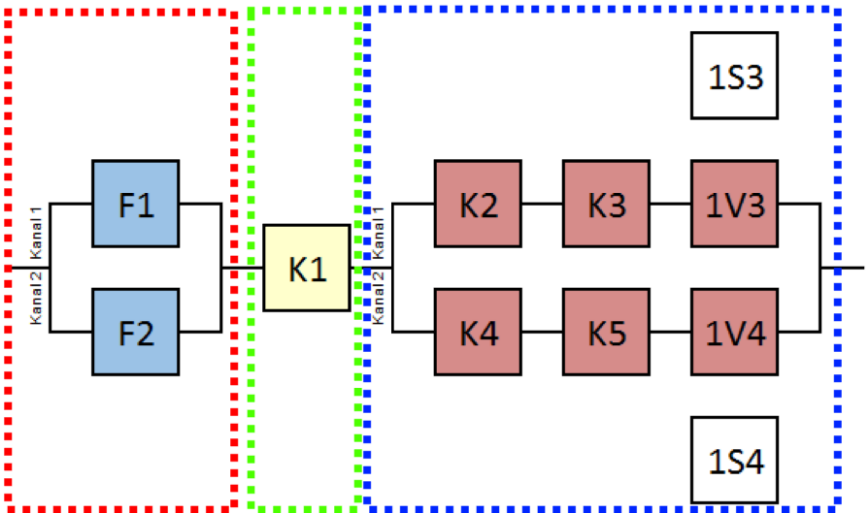


Abbildung 46: Blockschaltbild der Sicherheitsfunktion. Der rot markierte Bereich stellt den Eingang der Sicherheitsfunktion dar, grün die Logik und der blau markierte Bereich zeigt den Ausgang der Sicherheitsfunktion, Quelle: Eigene Darstellung

Um eine besser Übersicht für die Berechnung der Sicherheitsfunktion zu bekommen, können gekapselte Subsysteme, wie in Abbildung 47 der Block für die Logik (K1), nach vorne gezogen werden. Der gegebene PFH_D-Wert des gekapselten Subsystems wird am Ende zu den berechneten PFH_D-Werten der Funktionskanäle addiert.

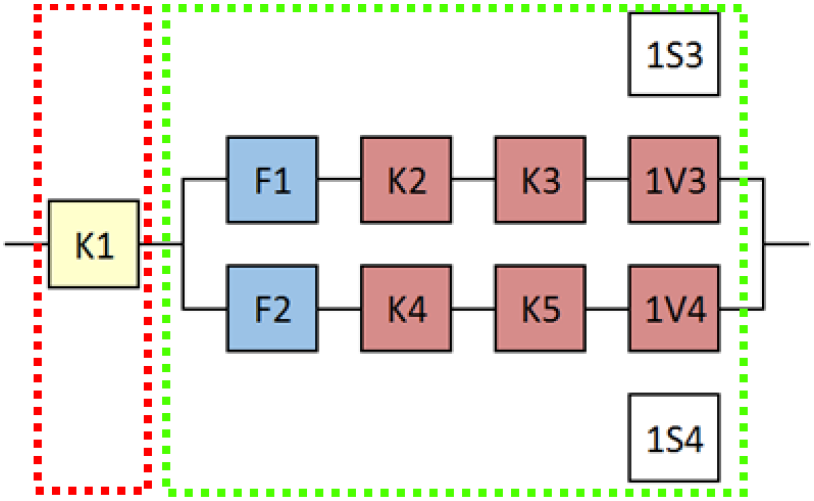


Abbildung 47: Blöcke gleicher Kategorie wurden zusammengefasst. Das gekapselte Subsystem der Logik wurde nach vorne gezogen. Die rote Markierung zeigt das Subsystem 1 (SB1), der grüne Bereich die Subsystem 2 (SB2). Quelle: Eigene Darstellung

9.2.7 Berechnung des erreichten Performance Level der Sicherheitsfunktion

Nach der Definition der Sicherheitsfunktion im vorhergehenden Kapitel, wird in diesem Kapitel der Nachweis über das Erreichen des erforderlichen Performance Level PL_r erbracht. Anhand des PL kann eine Aussage über die Zuverlässigkeit und die Ausfallswahrscheinlichkeit der Sicherheitsfunktion getroffen werden. Der Nachweis über die Kategorie wurde durch die Strukturanalyse bereits erbracht. In einem ersten Schritt werden für jeden Block der $MTTF_D$-Wert und der DC, sowie Maßnahmen gegen Ausfälle gemeinsamer Ursache, CCF ermittelt. In einem weiteren Schritt werden diese Parameter für den gesamten

Funktionskanal bestimmt. Für die Bestimmung der $MTTF_D$-Werte eines Kanals wird das „Parts-Count"-Verfahren nach EN ISO 13849-1:2015, Anhang D angewandt.

9.2.7.1 Berechnung der Parameter - Funktionskanal 1

Nachstehend werden die Parameter des Funktionskanals 1 berechnet. Für den Neigungssensor (F1) und das Hydraulikventil mit Stellungsüberwachung (1V3, 1S3) werden vom Hersteller $MTTF_D$-Werte angegeben. Für die Koppelrelais (K2, K3) werden vom Hersteller B_{10D}-Werte zur Verfügung gestellt.

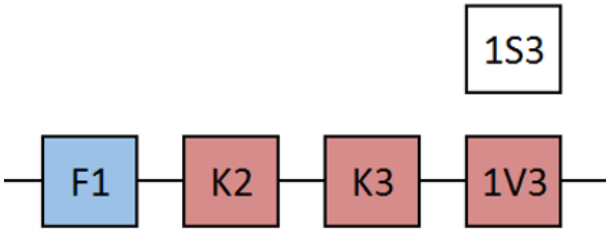


Abbildung 48: Funktionskanal 1, Quelle: Eigene Darstellung

Für die Koppelrelais muss die mittlere Anzahl der Betätigungen berechnet beziehungsweise abgeschätzt werden. Bei jedem Start der Maschine werden die Koppelrelais angesteuert. Bei einem Start pro Arbeitstag ergibt das im Jahr:

$$n_{op\ Ein/Aus} = \frac{d_{op} * h_{op} * 3600}{t_{Zyklus}} = \frac{135\,Tage/Jahr * 16\,h/Tag * 3600\ s/h}{57.600\,s/Zylus} = \underline{135\,Zyklen/Jahr}$$

Formel 2: Mittlere Anzahl an Betätigungen für den Ein- und Ausschalt-Vorgang

Weiters werden die Koppelrelais bei der Betätigung des Not-Halt-Gerätes angesteuert. Es wird angenommen, dass jeden zweiten Tag der Not-Halt betätigt wird.

$$n_{op\ Not-Halt} = \frac{d_{op} * h_{op} * 3600}{t_{Zyklus}} = \frac{135\,Tage/Jahr * 16\,h/Tag * 3600\ s/h}{115.200\,s/Zylus} = \underline{67{,}5 \sim 68\,Zyklen/Jahr}$$

Formel 3: Mittlere Anzahl an Betätigungen für die Sicherheitsfunktion Not-Halt

Zur Berechnung der Zyklen, die pro Jahr auf die Koppelrelais zukommen, werden nun die Zyklen für den Einschaltvorgang, die Zyklen bedingt durch das Betätigen des Not-Halt-Gerätes und die Zyklen die durch das Über- oder Unterschreiten der Neigungsgrenzen verursacht werden (Kapitel 9.1.4), addiert.

$$n_{op\ Gesamt} = n_{op\ Ein/Aus} + n_{op\ Not-Halt} + n_{op\ Neigung} = (135 + 68 + 20)\,Zyklen/Jahr =$$

$$n_{op\ Gesamt} = \underline{223\,Zyklen/Jahr}$$

Die folgenden Berechnungen für die Koppelrelais werden mit 250 Zyklen pro Jahr durchgeführt. Das großzügige Aufrunden dient als zusätzliche Reserve.

Zur Abschätzung des DC wird ein vereinfachter Ansatz aus Tabelle E der EN ISO 13849-1:2015, Anhang E, herangezogen. Die Begründung für die jeweilige Auswahl des DC ist dem Wert angefügt.

- Neigungssensor – F1

Der Hersteller der Neigungssensoren gibt einen $MTTF_D$-Wert für den Neigungssensor von 203 Jahren[74] an.

$$MTTF_{D\,F1} = \underline{203\,Jahre}$$

$$DC_{F1} = \underline{99\,\%}$$

Begründung für den DC der Neigungssensoren: In der Logik (K1) wird ein Kreuzvergleich von Eingangssignalen mit unmittelbarem und Zwischenergebnissen von F1 und F2 durchgeführt und zeitlich und logische Programmlaufüberwachung und Erkennung statischer Ausfälle und Kurzschlüsse gemacht.[75] Das ergibt laut EN ISO 13849-1:2015 einen DC von 99 %.

- Koppelrelais – K2

Der Hersteller des Koppelrelais stellt für das Bauteil einen B_{10D}-Wert von 180.000 Zyklen[76] zur Verfügung.

$$B_{10D} = 180.000\,Zyklen$$

$$MTTF_{D\,K2} = \frac{B_{10D}}{0{,}1 \cdot n_{op}} = \frac{180.000\,Zyklen}{0{,}1 \cdot 250} = \underline{7.200\,Jahre}$$

Formel 4: Berechnung des $MTTF_D$ Wert des Sicherheitsrelais

$$DC_{K2} = \underline{99\,\%}$$

Begründung: Indirekte Überwachung von K2 in K1 durch die Zwangsführung der elektromechanischen Einheiten.

- Koppelrelais – K3

$$MTTF_{D\,K3} = \frac{B_{10D}}{0{,}1 \cdot n_{op}} = \frac{180.000\,Zyklen}{0{,}1 \cdot 250} = \underline{7.200\,Jahre}$$

$$DC_{K3} = \underline{99\,\%}$$

Begründung: Direkte Überwachung von K3 in K1 durch die Zwangsführung der elektromechanischen Einheiten.

- Hydraulikventil – 1V3

Der Hersteller der Hydraulikventile stellt für das Ventil einen $MTTF_D$-Wert von 150 beziehungsweise 50 Jahren[77] zur Verfügung. Ein $MTTF_D$-Wert von 150 Jahren darf dann eingesetzt werden, wenn das Ventil in Sperr-Mittelstellung spannungslos ist. Wird die Sperr-Mittelstellung über eine Steuerspannung gehalten, dürfen lediglich 50 Jahre eingesetzt werden. Beim STEP wird das Ventil über die beiden Öffner der

[74] Vgl. Hans Turck GmbH & Co KG, Turck (Hrsg.) (2016), S. 1.

[75] Vgl. EN ISO 13849-1:2015 (2015), S. 76.

[76] Vgl. PHOENIX CONTACT GmbH & Co. KG;Phoenix Contact (Hrsg.) (2016), S. 8.

[77] Vgl. Danfoss Power Solutions GmbH & Co. OHG (2014), S. 5.

Koppelrelais K2 und K3 spannungslos geschalten, somit darf der $MTTF_D$-Wert mit 150 Jahren angenommen werden.

$$MTTF_{D\,1V3} = \underline{150\,Jahre}$$

$$DC_{1V3} = \underline{99\,\%}$$

Begründung: Direkte Überwachung von 1V3 in K1 durch die Stellungsüberwachung 1S3 des Hydraulikventils.

- $MTTF_D$ für Funktionskanal 1

$$\frac{1}{MTTF_D} = \sum_{i=1}^{N} \frac{1}{MTTF_{Di}}$$

Formel 5: Formel für die Berechnung zur Symmetrisierung des $MTTF_D$-Wertes für einen Kanal

$$MTTF_{D\,Kanal1} = \frac{1}{\frac{1}{203} + \frac{1}{7.200} + \frac{1}{7.200} + \frac{1}{150}} = \underline{84{,}24\,Jahre}$$

9.2.7.2 Berechnung der Parameter - Funktionskanal 2

Beim Funktionskanal 2 handelt es sich, ausgenommen vom Neigungssensor F2, um die gleichen Bauteile wie im Funktionskanal 1. Der Neigungssensor F2 ist baugleich dem Sensor F1 mit demselben $MTTF_D$-Wert, nur von einem anderen Hersteller. Die Begründung für die Wahl des DC des jeweiligen Bauteils kann in Kapitel 9.2.7.1 nachgeschlagen werden.

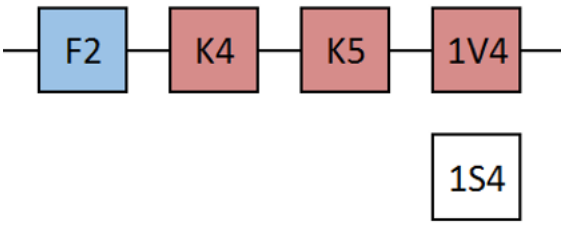


Abbildung 49: Funktionskanal 2, Quelle: Eigene Darstellung

- Neigungssensor – F2

$$MTTF_{D\,F2} = \underline{203\,Jahre}^{78}$$

$$DC_{F2} = 99\,\%$$

- Koppelrelais – K4

$$MTTF_{D\,K4} = \frac{B_{10D}}{0{,}1 \cdot n_{op}} = \frac{180.000\,Zyklen}{0{,}1 \cdot 250} = \underline{7.200\,Jahre}$$

$$DC_{K4} = \underline{99\,\%}$$

[78] Vgl. Kübler GmbH;Kübler GmbH (Hrsg.) (2016), S. 2.

- Koppelrelais – K5

$$MTTF_{D\,K5} = \frac{B_{10D}}{0{,}1 \cdot n_{op}} = \frac{180.000\ Zyklen}{0{,}1 \cdot 250} = \underline{7.200\ Jahre}$$

$$DC_{K5} = \underline{99\ \%}$$

- Hydraulikventil – 1V4

$$MTTF_{D\,1V4} = \underline{150\ Jahre}$$

$$DC_{1V4} = \underline{99\ \%}$$

- $MTTF_D$ für Funktionskanal 2

$$MTTF_{D\,Kanal2} = \frac{1}{\frac{1}{203} + \frac{1}{7.200} + \frac{1}{7.200} + \frac{1}{150}} = \underline{\underline{84{,}24\ Jahre}}$$

9.2.7.3 Symmetrisierung der $MTTF_D$-Werte für jeden Kanal

$$MTTF_D = \frac{2}{3}\left[MTTF_{D\,Kanal1} + MTTF_{D\,Kanal2} - \frac{1}{\frac{1}{MTTF_{D\,Kanal1}} + \frac{1}{MTTF_{D\,Kanal2}}}\right]$$

Formel 6: Formel zur Symmetrisierung der beiden Funktionskanäle

$$= \frac{2}{3}\left[84{,}24 + 84{,}24 - \frac{1}{\frac{1}{84{,}24} + \frac{1}{84{,}24}}\right] = 84{,}24\ Jahre$$

$$MTTF_{D\,FK1\,FK2} = \underline{\underline{84{,}24\ Jahre\ (hoch)}}$$

9.2.7.4 Durchschnittlicher Diagnosedeckungsgrad

$$DC_{avg} = MTTF_{D\,gesamt} * \sum_{i=1}^{N} \frac{DC_i}{MTTF_{Di}}$$

Formel 7: Formel für die Berechnung des durchschnittlichen Diagnosedeckungsgrad

$$MTTF_{D\,gesamt} = \frac{1}{\frac{1}{203} + \frac{1}{7200} + \frac{1}{7200} + \frac{1}{150} + \frac{1}{203} + \frac{1}{7200} + \frac{1}{7200} + \frac{1}{150}} =$$

$$MTTF_{D\,gesamt} \sim \underline{42{,}12\ Jahre}$$

$$DC_{avg} = MTTF_{D\,gesamt} \cdot \left(\frac{99}{203} + \frac{99}{7.200} + \frac{99}{7.200} + \frac{99}{150} + \frac{99}{203} + \frac{99}{7.200} + \frac{99}{7.200} + \frac{99}{150}\right) =$$

$$DC_{avg} = 42{,}12\ Jahre \cdot\ 2{,}350 \sim 99\ \%$$

$$DC_{avg} = \underline{\underline{99\ \%\ (hoch)}}$$

	Durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde, PFH_D (1/h) und der zugehörige Performance Level (PL)															
$MTTF_D$ für jeden Kanal Jahre	Kat. B DC_{avg} = kein	PL	Kat. 1 DC_{avg} = kein	PL	Kat. 2 DC_{avg} = niedrig	PL	Kat. 2 DC_{avg} = mittel	PL	Kat. 3 DC_{avg} = niedrig	PL	Kat. 3 DC_{avg} = mittel	PL	Kat. 4 DC_{avg} = hoch	PL
11	$1{,}04 \times 10^{-5}$	a			$6{,}44 \times 10^{-6}$	b	$4{,}53 \times 10^{-6}$	b	$2{,}81 \times 10^{-6}$	c	$1{,}18 \times 10^{-6}$	c		
12	$9{,}51 \times 10^{-6}$	b			$5{,}84 \times 10^{-6}$	b	$4{,}04 \times 10^{-6}$	b	$2{,}49 \times 10^{-6}$	c	$1{,}04 \times 10^{-6}$	c		
13	$8{,}78 \times 10^{-6}$	b			$5{,}33 \times 10^{-6}$	b	$3{,}64 \times 10^{-6}$	b	$2{,}23 \times 10^{-6}$	c	$9{,}21 \times 10^{-7}$	d		
15	$7{,}61 \times 10^{-6}$	b			$4{,}53 \times 10^{-6}$	b	$3{,}01 \times 10^{-6}$	b	$1{,}82 \times 10^{-6}$	c	$7{,}44 \times 10^{-7}$	d		
16	$7{,}13 \times 10^{-6}$	b			$4{,}21 \times 10^{-6}$	b	$2{,}77 \times 10^{-6}$	c	$1{,}67 \times 10^{-6}$	c	$6{,}76 \times 10^{-7}$	d		
18	$6{,}34 \times 10^{-6}$	b			$3{,}68 \times 10^{-6}$	b	$2{,}37 \times 10^{-6}$	c	$1{,}41 \times 10^{-6}$	c	$5{,}67 \times 10^{-7}$	d		
20	$5{,}71 \times 10^{-6}$	b			$3{,}26 \times 10^{-6}$	b	$2{,}06 \times 10^{-6}$	c	$1{,}22 \times 10^{-6}$	c	$4{,}85 \times 10^{-7}$	d		
22	$5{,}19 \times 10^{-6}$	b			$2{,}93 \times 10^{-6}$	c	$1{,}82 \times 10^{-6}$	c	$1{,}07 \times 10^{-6}$	c	$4{,}21 \times 10^{-7}$	d		
24	$4{,}76 \times 10^{-6}$	b			$2{,}65 \times 10^{-6}$	c	$1{,}62 \times 10^{-6}$	c	$9{,}47 \times 10^{-7}$	d	$3{,}70 \times 10^{-7}$	d		
27	$4{,}23 \times 10^{-6}$	b			$2{,}32 \times 10^{-6}$	c	$1{,}39 \times 10^{-6}$	c	$8{,}04 \times 10^{-7}$	d	$3{,}10 \times 10^{-7}$	d		
30			$3{,}80 \times 10^{-6}$	b	$2{,}06 \times 10^{-6}$	c	$1{,}21 \times 10^{-6}$	c	$6{,}94 \times 10^{-7}$	d	$2{,}65 \times 10^{-7}$	d	$9{,}54 \times 10^{-8}$	e
33			$3{,}46 \times 10^{-6}$	b	$1{,}85 \times 10^{-6}$	c	$1{,}06 \times 10^{-6}$	c	$5{,}94 \times 10^{-7}$	d	$2{,}30 \times 10^{-7}$	d	$8{,}57 \times 10^{-8}$	e
36			$3{,}17 \times 10^{-6}$	b	$1{,}67 \times 10^{-6}$	c	$9{,}39 \times 10^{-7}$	d	$5{,}16 \times 10^{-7}$	d	$2{,}01 \times 10^{-7}$	d	$7{,}77 \times 10^{-8}$	e
39			$2{,}93 \times 10^{-6}$	c	$1{,}53 \times 10^{-6}$	c	$8{,}40 \times 10^{-7}$	d	$4{,}53 \times 10^{-7}$	d	$1{,}78 \times 10^{-7}$	d	$7{,}11 \times 10^{-8}$	e
43			$2{,}65 \times 10^{-6}$	c	$1{,}37 \times 10^{-6}$	c	$7{,}34 \times 10^{-7}$	d	$3{,}87 \times 10^{-7}$	d	$1{,}54 \times 10^{-7}$	d	$6{,}37 \times 10^{-8}$	e
47			$2{,}43 \times 10^{-6}$	c	$1{,}24 \times 10^{-6}$	c	$6{,}49 \times 10^{-7}$	d	$3{,}35 \times 10^{-7}$	d	$1{,}34 \times 10^{-7}$	d	$5{,}76 \times 10^{-8}$	e
51			$2{,}24 \times 10^{-6}$	c	$1{,}13 \times 10^{-6}$	c	$5{,}80 \times 10^{-7}$	d	$2{,}93 \times 10^{-7}$	d	$1{,}19 \times 10^{-7}$	d	$5{,}26 \times 10^{-8}$	e
56			$2{,}04 \times 10^{-6}$	c	$1{,}02 \times 10^{-6}$	c	$5{,}10 \times 10^{-7}$	d	$2{,}52 \times 10^{-7}$	d	$1{,}03 \times 10^{-7}$	d	$4{,}73 \times 10^{-8}$	e
62			$1{,}84 \times 10^{-6}$	c	$9{,}06 \times 10^{-7}$	d	$4{,}43 \times 10^{-7}$	d	$2{,}13 \times 10^{-7}$	d	$8{,}84 \times 10^{-8}$	e	$4{,}22 \times 10^{-8}$	e
68			$1{,}68 \times 10^{-6}$	c	$8{,}17 \times 10^{-7}$	d	$3{,}90 \times 10^{-7}$	d	$1{,}84 \times 10^{-7}$	d	$7{,}68 \times 10^{-8}$	e	$3{,}80 \times 10^{-8}$	e
75			$1{,}52 \times 10^{-6}$	c	$7{,}31 \times 10^{-7}$	d	$3{,}40 \times 10^{-7}$	d	$1{,}57 \times 10^{-7}$	d	$6{,}62 \times 10^{-8}$	e	$3{,}41 \times 10^{-8}$	e
82			$1{,}39 \times 10^{-6}$	c	$6{,}61 \times 10^{-7}$	d	$3{,}01 \times 10^{-7}$	d	$1{,}35 \times 10^{-7}$	d	$5{,}79 \times 10^{-8}$	e	$3{,}08 \times 10^{-8}$	e
91			$1{,}25 \times 10^{-6}$	c	$5{,}88 \times 10^{-7}$	d	$2{,}61 \times 10^{-7}$	d	$1{,}14 \times 10^{-7}$	d	$4{,}94 \times 10^{-8}$	e	$2{,}74 \times 10^{-8}$	e
100			$1{,}14 \times 10^{-6}$	c	$5{,}28 \times 10^{-7}$	d	$2{,}29 \times 10^{-7}$	d	$1{,}01 \times 10^{-7}$	d	$4{,}29 \times 10^{-8}$	e	$2{,}47 \times 10^{-8}$	e

Tabelle 10: Auszug aus der Tabelle zur Bestimmung des PFH_D Wertes und des PL, Quelle: EN ISO 13849-1:2015 (2015), S. 102. (leicht modifiziert)

$$PFH_{D\,FK1\,FK2} = \underline{\underline{3{,}08 * 10^{-8} \frac{1}{h}}}$$

9.2.7.5 Parameter der gesamten Logik

Für die gesamte Logik Baugruppe gibt es bereits vom Hersteller Angaben zur mittleren Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde - PFH_D. Die Angaben wurden den Hersteller-Datenblättern beziehungsweise der VDMA Bibliothek des Herstellers entnommen. Sämtliche Logik Bauteile mit der Angabe des PFH_D Wertes sind nachfolgend aufgezählt. Es handelt sich dabei ausschließlich um gekapselte Subsysteme:

- **Fehlersichere Stromeingangskarte**

  Kategorie 4 und ein PFH_D Wert von $1 * 10^{-9} \frac{1}{h}$
- **CPU**

  Kategorie 4 und ein PFH_D Wert von $2 * 10^{-9} \frac{1}{h}$
- **Fehlersichere Digital-Ausgangskarte**

  Kategorie 4 und ein PFH_D Wert von $1 * 10^{-9} \frac{1}{h}$
- **Profisafe Protokoll zur Übermittlung des Safety Telegramms innerhalb der Logik Bauteile**

  PFH_D Wert von $1 * 10^{-9} \frac{1}{h}$

Einzelheiten zu den Logik Baugruppen befinden sich im Kapitel 9.2.2.

- Gesamt PFH_D für die Logik

  Zur Berechnung des PFH_D-Wert für die gesamte Logik Baugruppe werden die Werte für die einzelnen Komponenten addiert.

$$PFH_{D-Logik} = PFH_{D-AI} + PFH_{D-CPU} + PFH_{D-DO} + PFH_{D-PROFIsafe}$$

$$PFH_{D-Logik} = 1 * 10^{-9}\,\frac{1}{h} + 2 * 10^{-9}\,\frac{1}{h} + 1 * 10^{-9}\,\frac{1}{h} + 1 * 10^{-9}\,\frac{1}{h}$$

$$PFH_{D-Logik} = \underline{\underline{5 * 10^{-9}\,\frac{1}{h}}}$$

9.2.7.6 CCF der Sicherheitsfunktion

Um Fehler gemeinsamer Ursache (CCF – Common Cause Failure), wie zum Beispiel der Ausfall beider Kanäle, zu vermeiden, müssen Maßnahmen getroffen werden. Dazu sind in der EN ISO 13849-1:2015 im Anhang F Gegenmaßnahmen aufgelistet. Jede dieser Gegenmaßnahmen ist mit einer bestimmten Punkteanzahl bewertet. Für sicherheitsbezogene Teile von Steuerungen, für die Kategorie 2, 3 oder 4 zutreffend ist, müssen Gegenmaßnahmen im Ausmaß von 65 Punkten erreicht werden. In der nachfolgenden Tabelle sind die Maßnahmen gegen Fehler gemeinsamer Ursache der Sicherheitsfunktion Neigungsgrenzen aufgelistet.

Maßnahme gegen CCF	**Punktzahl**
Trennung/Abtrennung	
Erkennen von Kurzschlüssen und Unterbrechungen in Kabeln durch dynamische Prüfung	15
Diversität	
Bauteile unterschiedlicher Hersteller	20
Gestaltung/Anwendung/Erfahrung	
Schutz gegen Überspannung, Überstrom, Überdruck	15
Kompetenz/Ausbildung	
Ausbildung der Konstrukteure, um die Gründe und Auswirkungen von Ausfällen infolge gemeinsamer Ursache zu verstehen	5
Umgebung	
Für elektrische/elektronische Systeme, Verhindern von Verunreinigungen und elektromagnetischen Störungen (EMV) zum Schutz vor Ausfällen infolge gemeinsamer Ursache entsprechend den einschlägigen Normen (z. B. IEC 61326-3-1) Fluidische Systeme: Filtrierung des Druckmediums, Verhinderung von Schmutzeintrag, Entwässerung von Druckluft, z. B. in Übereinstimmung mit den Anforderungen des Herstellers für die Reinheit des Druckmediums ANMERKUNG Bei kombinierten fluidischen und elektrischen Systemen sollten beide Aspekte berücksichtigt werden.	25
Summe	80

Tabelle 11: Zutreffende Maßnahmen gegen Ausfälle gemeinsamer Ursache, Quelle: EN ISO 13849-1:2015 (2015), S. 81.

Beschreibung der umgesetzten Maßnahmen gegen Ausfälle gemeinsamer Ursachen:

- **Trennung/Abtrennung**

Die Signalpfade der Neigungssensoren werden im Eingangsmodul der Logik auf Plausibilität und Diskrepanzfehler überwacht. Weiters überwacht das Eingangsmodul die Pfade auf Kurzschluss, Querschluss und Kabelbruch.

- **Diversität**

Die Diversität ist durch Verwendung unterschiedlicher Hersteller bei den Neigungssensoren gegeben.

- **Gestaltung/Anwendung/Erfahrung**

Sowohl die Firma HPT, als auch die Lieferanten der Schaltschränke haben sich bei der Gestaltung der Maschine an die IEC 60204-1 gehalten. Durch die Einhaltung dieser Norm ist der Schutz sämtlicher Komponenten vor Überspannung und Überstrom gegeben. Hydraulische Systeme sind gegen Überdruck gesichert. Als Beispiel sei an dieser Stelle der Filter des Druckmediums in Abbildung 44 erwähnt.

- **Kompetenz/Ausbildung**

Die Konstrukteure der HPT sind durch entsprechende Schulungen und Weiterbildungen in der Lage Gründe und Auswirkungen von Ausfällen infolge gemeinsamer Ursache zu erkennen.

- **Umgebung**

Durch Einhaltung der IEC 60204-1 werden die Maßnahmen in elektrischen, elektronischen und in programmierbar elektronischen Systemen umgesetzt.

Für das hydraulische System werden die Maßnahmen unter anderem durch das Einsetzen von Filtern und Temperaturüberwachung umgesetzt. Siehe Abbildung 44.

9.2.7.7 Berechnung Gesamt PFH_D für die Sicherheitsfunktion Neigungsgrenzen

Im letzten Schritt der Berechnung werden die PFH_D-Werte der beiden Funktionskanäle und der Logik addiert.

$$PFH_{D\,Gesamt} = PFH_{D\,FK1\,FK2} + PFH_{D-Logik} = 3{,}08 * 10^{-8}\frac{1}{h} + 5 * 10^{-9}\frac{1}{h}$$

$$PFH_{D\,Gesamt} = \underline{\underline{3{,}58 * 10^{-8}\frac{1}{h}}}$$

Die durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls der Sicherheitsfunktion je Stunde liegt bei $3{,}58 * 10^{-8}\frac{1}{h}$. Der errechnete Wert entspricht einem PL von „e“, siehe Tabelle 12.

Performance Level (PL)	Durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde (PFH_D) 1/h
a	$\geq 10^{-5}$ bis $< 10^{-4}$
b	$\geq 3 \times 10^{-6}$ bis $< 10^{-5}$
c	$\geq 10^{-6}$ bis $< 3 \times 10^{-6}$
d	$\geq 10^{-7}$ bis $< 10^{-6}$
e	$\geq 10^{-8}$ bis $< 10^{-7}$

Tabelle 12: Zusammenhang des Performance Level und PFH_D, Quelle: EN ISO 13849-1:2015 (2015), S. 21 (leicht modifiziert).

9.2.7.8 Ergebnis der Sicherheitsfunktion

- Subsystem 1
  - $MTTF_D$ = 84,24 Jahre (hoch)
  - DC_{avg} = 99 % (hoch)
  - CCF = 80 Punkt (erfüllt)
  - $PFH_D = 3{,}08 * 10^{-8} \frac{1}{h}$
  - PL = e
- Subsystem 2
  - $PFH_D = 5 * 10^{-9} \frac{1}{h}$
  - PL = e
- Sicherheitsfunktion
  - $PFH_D = 3{,}58 * 10^{-8} \frac{1}{h}$
  - Kategorie 3, PL e
    - Anforderungen
      - Grundlegende Sicherheitsprinzipien ✓
      - Bewährte Sicherheitsprinzipien ✓
      - Ein-Fehlertoleranz ✓
      - Anhäufung von Fehlern ×
      - $MTTF_D$ hoch ✓
      - DC_{avg} hoch ✓
      - CCF mindestens 65 Punkte ✓

Berechnungen zufolge ergibt sich ein PL von „e“. Auf Grund der Tatsache, dass die Neigungssensoren die Anforderungen an sicherheitsbezogene Embedded-Software nicht erfüllen, kann maximal PL „d“ erreicht werden, siehe Kapitel 9.2.2.1.

Analog zu den Berechnungen in Kapitel 9.2.7 wurden die Berechnungen auch mit Hilfe von SISTEMA durchgeführt. Das vom Institut für Arbeitsschutz (IFA) der Deutschen Gesetzlichen Unfallversicherung (DGUV) kostenfrei zur Verfügung gestellte Windows-Tool, bietet eine Hilfestellung bei der Entwicklung, Prüfung und Dokumentation von sicherheitsbezogenen Maschinensteuerungen. Eine detaillierte Zusammenfassung der Berechnung mit SISTEMA ist dem Anhang 2 dieser Masterarbeit angefügt.

Zusätzlich wurden bei der SISTEMA-Berechnung die Optimierungsvorschläge aus Kapitel 11.1 berücksichtigt und die beiden Ergebnisse gegenübergestellt.

9.2.7.9 Verifikation der Sicherheitsfunktion

Die Sicherheitsfunktion Neigungsgrenzen erfordert, wie in Kapitel 9.1.6 beschrieben, einen PL_r von „d“. Mit der Berechnung des erreichten PL wurde der Nachweis erbracht, dass der PL_r von „d“ erreicht wurde.

$$PL \geq PL_r$$

Somit braucht der iterative Prozess zur Gestaltung von sicherheitsbezogenen Teilen von Steuerungen nicht wiederholt werden.

10 VALIDIERUNG DER SICHERHEITSFUNKTION

Im folgenden Kapitel wird die Validierung von Fehlerverhalten und Mitteln zur Diagnose der Sicherheitsfunktion nach EN ISO 13849-2:2012 durchgeführt. Diese muss zeigen, dass die Anforderungen der EN ISO 13849-1:2015 durch die Kombination von sicherheitsbezogenen Teilen der Steuerung erfüllt werden. Die Validierung wird durch eine Ausfallsanalyse und ergänzende Fehlereingabeprüfungen durchgeführt.

FMEA und Abschätzung des DC-Wertes für die Bauteile der Sicherheitsfunktion

Mit einer Fehlermode- und Ausfallanalyse (FMEA) werden die DC-Werte, die jeder überwachten Einheit jedes sicherheitsbezogenen Teiles der Steuerung zugewiesen wurden, sowie das Fehlverhalten des Systems überprüft.

Da die Sicherheitsfunktion Neigungsgrenzen sowohl das sicherheitsbezogene Abschalten, als auch die nachfolgende Verhinderung eines unerwarteten Wiederanlaufes ausführen muss, wird die Ausfallanalyse für jedes zur Sicherheitsfunktion zugehörige Bauteil in einer gesonderten Zeile für jede dieser Anforderungen betrachtet.

Für die Analyse wurden die entsprechenden Fehlerlisten in den Anhängen C und D der EN ISO 13849-2:2012 verwendet.

	Bauteil/ Einheit	**Möglicher Ausfall**	**Fehlererkennung**	**Wirkung/ Reaktion**	**Prüfung zur Bestätigung**
F1	Neigungs-sensor F1	Fehler in allen Teilen der Funktion oder in einem Teil der Funktion einschließlich Software-Fehler	Ein Fehler von F1 wird in der Logik (K1) durch Kreuzvergleich mit F2 erkannt.	K1 stellt über die Ausgabeeinheit einen sicheren Zustand der Maschine her, wenn es zu einer Abweichung der beiden Eingangssignale kommt. Der Wiederanlauf wird verhindert.	Im sicheren Zustand sind die elektrischen Steuersignale von 1S3 und 1S4 auf High-Level
F2		Kurzschluss zwischen zwei beliebigen Anschlüssen	Kurzschlüsse werden durch das Eingangsmodul der Logik (K1) erkannt	K1 stellt über die Ausgabeeinheit einen sicheren Zustand der Maschine her, wenn es zu einem Kurzschluss zweier beliebiger Anschlüsse in F1 kommt. Der Wiederanlauf wird verhindert.	Im sicheren Zustand sind die elektrischen Steuersignale von 1S3 und 1S4 auf High-Level

F3	Neigungs-sensor F2	Fehler in allen Teilen der Funktion oder in einem Teil der Funktion einschließlich Software-Fehler	Ein Fehler von F2 wird in der Logik (K1) durch Kreuzvergleich mit F1 erkannt.	K1 stellt über die Ausgabeeinheit einen sicheren Zustand der Maschine her, wenn es zu einer Abweichung der beiden Eingangssignale kommt. Der Wiederanlauf wird verhindert.	Im sicheren Zustand sind die elektrischen Steuersignale von 1S3 und 1S4 auf High-Level
F4		Kurzschluss zwischen zwei beliebigen Anschlüssen	Kurzschlüsse werden durch das Eingangsmodul der Logik (K1) erkannt	K1 stellt über die Ausgabeeinheit einen sicheren Zustand der Maschine her, wenn es zu einem Kurzschluss zweier beliebiger Anschlüsse in F2 kommt. Der Wiederanlauf wird verhindert.	Im sicheren Zustand sind die elektrischen Steuersignale von 1S3 und 1S4 auf High-Level
Durch Kreuzvergleiche zwischen F1 und F2 mit unmittelbaren und Zwischenergebnissen in der Logik (K1) und zeitlich und logische Programmlaufüberwachung und Erkennung statischer Ausfälle und Kurzschlüsse kann für F1 und F2 ein DC von 99 % angenommen werden.					
F5	Koppel-relais K2	Der Kontakt öffnet sich nicht, wenn die maximalen Neigungsgrenzen über- oder unterschritten werden (elektrischer Fehler, z.B. verschweißte Kontakte).	Ein Fehler wird durch die Logik (K1), Überwachung des zwangsgeführten K2 – Rückmeldekontakts erkannt, wenn die Sicherheitsfunktion angefordert wird.	Sämtliche Bewegungen der Maschine werden sofort über K3 abgeschaltet, wenn die maximalen Neigungsgrenzen über- oder unterschritten werden. Der Wiederanlauf wird verhindert.	Der K2 – Rückmeldekontakt wird in der geschlossenen Schaltstellung gehalten, wenn die Maschine im sicheren Zustand ist.
F6		gleichzeitiges Geschlossensein üblicherweise offener und üblicherweise geschlossener Kontakte ANMERKUNG Dieser Fehler kann ausgeschlossen werden, durch die Verwendung von zwangsläufig betätigte Kontakte	/	/	/

F7		gleichzeitiger Kurzschluss zwischen den drei Klemmen eines Wechselkontaktes ANMERKUNG Gleichzeitiger Kurzschluss kann ausgeschlossen werden – durch Einhaltung von IEC 60664-1	/	/	/
F8	Koppel-relais K3	Der Kontakt öffnet sich nicht, wenn die maximalen Neigungsgrenzen über- oder unterschritten werden (elektrischer Fehler, z.B. verschweißte Kontakte).	Ein Fehler wird durch die Logik (K1), Überwachung des zwangsgeführten K3 – Rückmeldekontakts erkannt, wenn die Sicherheitsfunktion angefordert wird.	Sämtliche Bewegungen der Maschine werden sofort über K2 abgeschaltet, wenn die maximalen Neigungsgrenzen über- oder unterschritten werden. Der Wiederanlauf wird verhindert.	Der K3 – Rückmeldekontakt wird in der geschlossenen Schaltstellung gehalten, wenn die Maschine im sicheren Zustand ist.
F9		gleichzeitiges Geschlossensein üblicherweise offener und üblicherweise geschlossener Kontakte ANMERKUNG Dieser Fehler kann ausgeschlossen werden, durch die Verwendung von zwangsläufig betätigten Kontakte	/	/	/
F10		gleichzeitiger Kurzschluss zwischen den drei Klemmen eines Wechselkontaktes ANMERKUNG Gleichzeitiger Kurzschluss kann ausgeschlossen werden – durch Einhaltung von IEC 60664-1	/	/	/
Die Überwachung der Koppelrelais K2, K3, K4 und K5 durch die Logik K1 über die Stellung der zwangsgeführten Rückmeldekontakte ergibt einen DC von 99 % für K2, K3, K4 und K5.					
Anmerkung: Auf die Betrachtung von K4 und K5 wurde verzichtet, da es analog zu K2 und K3 zu sehen ist. Kabel, Leitungen, Klemmstellen und mehrpolige Steckverbindungen wurden in der FMEA nicht berücksichtigt.					

Tabelle 13: Durchführung einer FMEA der sicherheitsbezogenen elektrischen-Teile der Steuerung zur Überprüfung der angenommen DC-Werte.

F11	Elektro-magne-tisches Wege-ventil 1V3	Nicht-Schalten (Hängenbleiben in der geschalteten Stellung) oder nicht vollständiges Zurückschalten (Hängenbleiben in einer beliebigen Zwischenstellung)	Ein Fehler wird in der Logik (K1) durch die direkte Überwachung der Schieberstange erkannt.	Sämtliche Bewegungen werden über das Ventil 1V4 von K1 abgeschaltet. Ein Wiederanlauf wird bis zum Tausch	Im sicheren Zustand sind die elektrischen Steuersignale von 1S3 auf High-Level

				des Hydraulikventils verhindert.	
F12		selbsttätige Veränderung der Ausgangs-Schaltstellung (ohne Eingangssignal), während des sicheren Zustandes der Maschine ANMERKUNG Dieser Fehler kann ausgeschlossen werden, da in 1V3 bewährte Federn verwendet und übliche Einbau- und Betriebsbedingungen angewendet werden.	/	/	/
F13		Bersten des Ventilgehäuses oder Bruch des/der bewegten Bauteils/Bauteile sowie Bruch der Befestigungs- oder Gehäuseschrauben ANMERKUNG Fehlerausschluss, wenn Konstruktion, Dimensionierung und Einbau bewährten technischen Erfahrungen entsprechen.	/	/	/
F14	Elektro-magne-tisches Wege-ventil 1V4	Nicht-Schalten (Hängenbleiben in der geschalteten Stellung) oder nicht vollständiges Zurückschalten (Hängenbleiben in einer beliebigen Zwischenstellung)	Ein Fehler wird in der Logik (K1) durch die direkte Überwachung der Schieberstange erkannt.	Sämtliche Bewegungen werden über das Ventil 1V3 von K1 abgeschaltet. Ein Wiederanlauf wird bis zum Tausch des Hydraulikventils verhindert.	Im sicheren Zustand sind die elektrischen Steuersignale von 1S4 auf High-Level
F15		selbsttätige Veränderung der Ausgangs-Schaltstellung (ohne Eingangssignal), während des sicheren Zustandes der Maschine ANMERKUNG Dieser Fehler kann ausgeschlossen werden, da in 1V3 bewährte Federn verwendet und übliche Einbau- und Betriebsbedingungen angewendet werden.	/	/	/
F16		Bersten des Ventilgehäuses oder Bruch des/der bewegten Bauteils/Bauteile sowie Bruch der Befestigungs- oder Gehäuseschrauben ANMERKUNG Fehlerausschluss, wenn Konstruktion,	/	/	/

		Dimensionierung und Einbau bewährten technischen Erfahrungen entsprechen.			
Infolge der direkten Überwachung von 1V3 und 1V4 durch K1 über die Stellungsüberwachung 1S3 und 1S4 kann angenommen werden, dass 1V3 und 1V4 einen DC-Wert von 99% aufweisen.					
Anmerkung: Rohrleitungen, Schlauchleitungen, Verbindungselemente und Filter wurden in der FMEA nicht berücksichtigt.					

Tabelle 14: Durchführung einer FMEA der sicherheitsbezogenen Hydraulik-Teile der Steuerung zur Überprüfung der angenommen DC-Werte.

Anhand der Analyse in Tabelle 14 kann geschlossen werden, dass alle Einzelfehler in den sicherheitsbezogenen Teilen der Steuerung entweder sofort oder bei der nächsten Anforderung der Sicherheitsfunktion erkannt werden. Wenn ein Einzelfehler auftritt, wird die Sicherheitsfunktion immer ausgeführt und ein Wiederanlauf verhindert. Dies entspricht den Eigenschaften einer Kategorie 3, die bei der Gestaltung der Sicherheitsfunktion ausgewählt wurde.

11 ZUSAMMENFASSUNG UND AUSBLICK

In der vorliegenden Masterarbeit wurde unter Berücksichtigung aktueller Gesetze, Richtlinien und Normen eine Sicherheitsfunktion des Sicherheitskonzeptes für eine Schiffsbearbeitungs- und Inspektionsplattform analysiert. Dabei wurde die Gefahr des Kippens der Maschine identifiziert und eine technische Schutzmaßnahme erarbeitet, die in einem weiteren Schritt validiert wurde. Das Ergebnis ist eine optimierte Sicherheitsfunktion, die auch bei anderen Maschinen der HPT angewandt werden kann.

Bei der Überarbeitung von Maschinen der HPT, aber auch bei der Neuentwicklung kann jederzeit auf die optimierte Sicherheitsfunktion dieser Masterarbeit zurückgegriffen werden. Gewonnene Erkenntnisse aus dem Werftbetrieb können rasch und effektiv in die bestehende Sicherheitsfunktion eingearbeitet werden und so die Sicherheit aller Maschinen der HPT erhöhen.

11.1 Optimierungen der Sicherheitsfunktion

In diesem Kapitel werden die Optimierungsmaßnahmen an der Sicherheitsfunktion erläutert.

Ursprünglich wurden zwei idente Neigungssensoren von Turck verbaut. Da die Neigungssensoren aber die Anforderungen für sicherheitsbezogene Embedded-Software, wie es die EN ISO 13849-1:2015 in Absatz 4.6.2 fordert, nicht erfüllen, kann maximal PL „b“ erreicht werden. Da die Sicherheitsfunktion Neigungsgrenzen aber einen PL_r von „d“ fordert, müssen zumindest zwei Sensoren verbaut werden. Um einen PL von „c“ oder „d“ zu erreichen, müssen die Sensoren diversitäre Technologien verwenden. Diversität nach EN ISO 13849-1:2015 bedeutet zumindest unterschiedliche Hersteller. Wird ein Neigungssensor von Turck gegen einen baugleichen Neigungssensor von Kübler ersetzt, wird ein PL von „d“ erreicht.

Je Funktionskanal werden zwei Koppelrelais mit zwangsgeführten Kontakten verwendet. Die beiden Koppelrelais könnten gegen fehlersichere Relais-Module der SPS ersetzt werden, das folgenden Vorteil mit sich bringen würde:

- Der PFH_D-Wert der gesamten Sicherheitsfunktion würde sich verbessern, wie die Gegenüberstellung der beiden Ergebnisse der SISTEMA-Berechnung zeigt, siehe Abbildung 51 und Abbildung 50.

Neigungsgrenzen	
PLr	e
PL	e
PFHD [1/h]	3,5E-8

Abbildung 51: Das Ergebnis der SISTEMA Berechnung mit den Komponenten, wie in Kapitel 9.2.2 beschrieben. Quelle: Eigene Darstellung

Neigungsgrenzen (optimiert)	
PLr	e
PL	e
PFHD [1/h]	4,5E-8

Abbildung 50: Das Ergebnis der SISTEMA Berechnung mit den berücksichtigten Optimierungen. Quelle: Eigene Darstellung

11.2 Anwendung der Sicherheitsfunktion beim RFMT

Die validierte und optimierte Sicherheitsfunktion könnte auch bei anderen Maschinen der HPT eingesetzt werden. Konkret kann die Sicherheitsfunktion Neigungsgrenzen beim Rail Floor Multi Tool (RFMT) Anwendung finden. Beim RFMT bewegen sich, ähnlich wie beim STEP zwei Brücken entlang eines Turms,

der an einem Unterwagen montiert ist. Wie beim STEP kann das Über- oder Unterschreiten der Neigungsgrenzen des Unterwagens auch beim RFMT zum Kippen der Maschine führen. Beim RFMT ist es eine fehlerhafte Anwendung durch die Bedienerin oder den Bediener, die die Maschine an die Neigungsgrenzen bringen kann.

Der RFMT (Abbildung 52) dient ebenso wie der STEP als Inspektionsplattform in Schiffswerften. Der RFMT ist nur in seiner Grundstellung und mit unbesetzten Arbeitskörben entlang des Schiffes bewegbar. Aus diesem Grund kann er nicht so flexibel eingesetzt werden wie der STEP. Außerdem kann der Arbeitskorb des RFMT nur mit einem Abtragswerkzeug bestückt werden und ist dem STEP auch bezüglich der Abtragsleistung unterlegen.

Abbildung 52: RFMT – Ähnlich wie beim STEP bewegen sich beim RFMT zwei Brücken entlang eines Turmes, der an einem Unterwagen verbolzt ist, Quelle: Hubert Palfinger Technologies GmbH

11.3 Fazit

Mit dieser Masterarbeit konnte in der HPT großes Bewusstsein für das Thema Maschinensicherheit geschaffen werden. Das Thema der funktionalen Sicherheit ist für Unternehmen nicht nur durch den steigenden Automatisierungsgrad von höchster Bedeutung, sondern es steckt auch ein hohes Einsparungspotential dahinter. Des Weiteren ist die Sicherheit von Maschinen nicht das Thema einer/eines Einzelnen im Unternehmen sondern jede Abteilung hat das Seine dazu beizutragen. Je sensibilisierter und vertrauter MitarbeiterInnen mit der Maschinensicherheit sind, desto schneller lassen sich zum Beispiel Zertifizierungsverfahren durchziehen, seien es die Zertifikate von Bauteilen, die während des Beschaffungsprozesses mitangefordert und abgelegt werden müssen, oder die gesammelten Notizen eines/einer KonstrukteurIn, die bei der Risikoanalyse hilfreich sind.

LITERATURVERZEICHNIS

Gedruckte Werke (20)

Hubert Palfinger Technologies GmbH (Hrsg.) (2017): *Lastenheft STEP*, 1. Auflage, ohne Verlagsangaben, Admont, Stmk.

Hans Turck GmbH & Co KG, Turck (Hrsg.) (2016): *Datenblatt Neigungssensor - B2N10H-Q20L60-2LI2-H1151*, Mülheim an der Ruhr

HYDAC Electronic GmBH; HYDAC Electronic GmBH (Hrsg.) (2013): *Datenblatt - Elektronischer Druckmessumformer HDA 4700*, Saarbrücken

Phoenix Contact; Phoenix Contact (Hrsg.) (2004): *PSR – Phoenix Sicherheits-Relais PSR-URM/2X21*, Tagelswangen

Pilz GmbH & Co. KG;Pilz GmbH & Co. KG (Hrsg.) (2008): *Datenblatt - PSENcs1.1p*, Ostfildern

Siemens AG; Siemens AG (Hrsg.) (2017): *Datenblatt - 6ES7336-4GE00-0AB0*, München

Siemens AG; Siemens AG (Hrsg.) (2017): *Datenblatt - 6ES7135-6HD00-0BA1*, München

Siemens AG; AG, Siemens (Hrsg.) (2017): *Datenblatt - 6ES7136-6BA00-0CA0*, München

Siemens AG; AG, Siemens (Hrsg.) (2017): *Datenblatt - 6ES7136-6DB00-0CA0*, München

TR Electronic GmbH;TR Electronic GmbH (Hrsg.) (2014): *Datenblatt - CDH75M*8192/32768 EPN 20H7NT +FS*, 10 Auflage, Trossingen

Hans Turck GmbH & Co. KG; Turck (Hrsg.) (2012): *Industrielle Automation - Sensortechnik*, 1 Auflage, Mülheim an der Ruhr

PHOENIX CONTACT GmbH & Co. KG;Phoenix Contact (Hrsg.) (2016): *Functional Safety Characteristic*, Blomberg

Danfoss Power Solutions GmbH & Co. OHG;Danfoss (Hrsg.) (2014): *Datenblatt - EMD Speed Sensor*, Neumünster

Kübler GmbH;Kübler GmbH (Hrsg.) (2016): *Datenblatt Neigungssensor - IS40*, Villingen-Schwenningen

Blasge, Franz (2016): *Lehrveranstaltung Funktionale Sicherheit Teil 1*, ohne Verlagsangaben, Graz

Danfoss Power Solutions GmbH & Co. OHG (2014): *Reliability Data (MTTF) for PVG32 Proportional valve*, Offenbach/Main

Danfoss Power Solutions GmbH & Co. OHG (2014): *Installation Guid - Electrical Actuating Module*, Offenbach/Main

Fraser, Ian; u.a. (2010): *Leitfaden für die Anwendung der Maschinenrichtline 2006/42/EG*, 2. Auflage, ohne Verlagsangaben, Brüssel

Hauke, Michael; u.a. (2017): *IFA Report 2/2017 Funktionale Sicherheit von Maschinen*, 3 Auflage, Berlin

Kirchberg, Siegfried (2006): *Erläuterung zum Anwendungsbereich der Maschinenrichtlinie*, Bundesanstalt für Arbeitsschutz und Arbeitsmedizin, Dortmund

Online-Quellen (17)

Hubert Palfinger Technologies GmbH (2017): *Company*
https://www.hpalfingertech.com/page/detail/9/ [Stand: 12.09.2017]

Siemens AG (2014): *Der Weg zur sicheren Maschine*
https://www.siemens.de/Digital-Factory/download/EventDocs/00017/Der%20Weg%20zur%20sicheren%20Maschine.pdf [Stand: 08.08.2017]

Wirtschaftskammer Österreich (2017): *CE-Kennezichnung und Normen*
https://www.wko.at/service/innovation-technologie-digitalisierung/ce-kennzeichnung-normen.html [Stand: 21.08.2017]

Wirtschaftskammer Österreich (2017): *EU-Richtlinie betreffend die Allgemeine Produktsicherheit*
https://www.wko.at/service/innovation-technologie-digitalisierung/EU-Richtlinie_betreffend_die_Allgemeine_Produktsicherheit_.html [Stand: 22.08.2017]

European Commission (2017): *Growth: Sectors: Mechanical Engineering*
https://ec.europa.eu/growth/sectors/mechanical-engineering_en [Stand: 13.11.2017]

KEYENCE Deutschland GmbH (2015): *Grundgedanke des Performance Level: PL-Parameter*
http://www.keyence.de/ss/products/safetyknowledge/performance/parameter/ [Stand: 14.09.2017]

Deutsche Gesetzliche Unfallversicherung e.V. (2015): *Praxishilfen Maschinenschutz: Software SISTEMA*
http://www.dguv.de/ifa/praxishilfen/praxishilfen-maschinenschutz/software-sistema/index.jsp [Stand: 15.09.2017]

Ingenieurbüro Vogt (2017): *RV - Risiken vermeiden*
http://www.rv-risikenvermeiden.de/index.php/normen-und-richtlinien/23-menuepunkt-grundkagen/normeninfo/46-typ-a-typ-b-und-typ-c-normen [Stand: 20.08.2017]

Siemens AG (2016): *Steuerungen: Fehlersichere CPUs*
https://mall.industry.siemens.com/mall/de/WW/Catalog/Products/10255635 [Stand: 3.12.2017]

Conrad Electronic Österreich; (2018):
https://www.conrad.at/de/sicherheitsrelais-10-st-psr-scf-24ucurm2x21-phoenix-contact-betriebsspannung-24-vdc-24-vac-2-wechsler-b-x-h-x-t-704192.html?insert=U3&WT.srch=1&WT.mc_id=sea_9_Shopping&gclid=EAIaIQobChMIsOTI0afn2AIVBGYbCh0wTQdhEAQYBCABEgL_kfD_BwE [Stand: 20.01.2018]

Agerer, Markus (2016): *Risikobeurteilung*
http://www.maschinen-sicherheit.net/07-seiten/0300-risikobeurteilung.php [Stand: 31.08.2017]

Agerer, Markus (2016): *Risikobewertung*
http://www.maschinen-sicherheit.net/07-seiten/0460-risikobewertung.php [Stand: 02.09.2017]

Kramer, Burkhard (2016): *CE-Richtlinien*
http://ce-richtlinien.eu/ce-richtlinien/ [Stand: 24.08.2017]

Kringf (2014): *News: 25 Jahre jung oder ein Vierteljahrhundert alt: Die europäische Maschinenrichtlinie*
http://www.maschinenrichtlinie-2006-42-eg.de/25-jahre-jung-oder-ein-vierteljahrhundert-alt-die-europ%C3%A4ische-maschinenrichtlinie [Stand: 25.08.2017]

Kurrus; u.a. (2016): *Leitfaden Sichere Maschinen*
https://www.sick.com/media/docs/7/77/677/Special_information_Guide_for_Safe_Machinery_de_IM0014677.PDF [Stand: 08.08.2017]

Unbekannt (2017): *CE-Kennzeichnung*
https://de.wikipedia.org/wiki/CE-Kennzeichnung [Stand: 21.08.2017]

Walther, Peter (2015): *Gesetze und Normen: Die Maschinenrichtlinie 2006/42/EG: Warum ist sie so wichtig? Wie setze ich sie effektiv um?*
https://www.hein.eu/hein-blog-industrieschilder-und-mehr/maschinenrichtlinie-2006-42-eg--blog.html [Stand: 26.08.2017]

Normen (10)

DIN Deutsches Institut für Normung e.V. (Hrsg.) (2014): *DIN ISO/TR 23849:2014-12; DIN SPEC 33883:2014-12: Leitfaden zur Anwendung von ISO 13849-1 und IEC 62061 bei der Gestaltung von sicherheitsbezogenen Steuerungen für Maschinen*

Austrian Standards Institute (Hrsg.) (2009): *EN 1495:1997+A2:2009: Hebebühnen - Mastgeführte Kletterbühnen*

Austrian Standards Institute (Hrsg.) (2015): *EN 280:2013+A1:2015: Fahrbare Hubarbeitsbühnen - Berechnung - Standsicherheit - Bau - Sicherheit - Prüfungen*

Austrian Standards Institute (Hrsg.) (2010): *EN ISO 12100:2010: Sicherheit von Maschinen - Allgemeine Gestaltungsleitsätze - Risikobeurteilung und Risikominderung*

Austrian Standards Institute (Hrsg.) (2015): *EN ISO 13849-1:2015: Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen, Teil 1: Allgemeine Gestaltungsleitsätze*

Austrian Standards Institute (Hrsg.) (2012): *EN ISO 13849-2:2012: Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen, Teil 2: Validierung*

Austrian Standards Institute (Hrsg.) (2010): *IEC 61508-4:2010: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme - Teil 4: Begriffe und Abkürzungen*

DIN Deutsches Institut für Normung e.V. (Hrsg.) (2013): *ISO/TR 14121-2:2012: Sicherheit von Maschinen – Risikobeurteilung – Teil 2: Praktischer Leitfaden und Verfahrensbeispiele*

Europäisches Parlament, Europäischer Rat (Hrsg.) (2006): *Maschinenrichtlinie: Maschinenrichtlinie MRL 2006/42/EG*

Bundesministers für Wirtschaft und Arbeit (Hrsg.) (2008): *Maschinensicherheitsverordnung: Maschinen-Sicherheitsverordnung 2010 – MSV 2010*

ABBILDUNGSVERZEICHNIS

TABELLENVERZEICHNIS

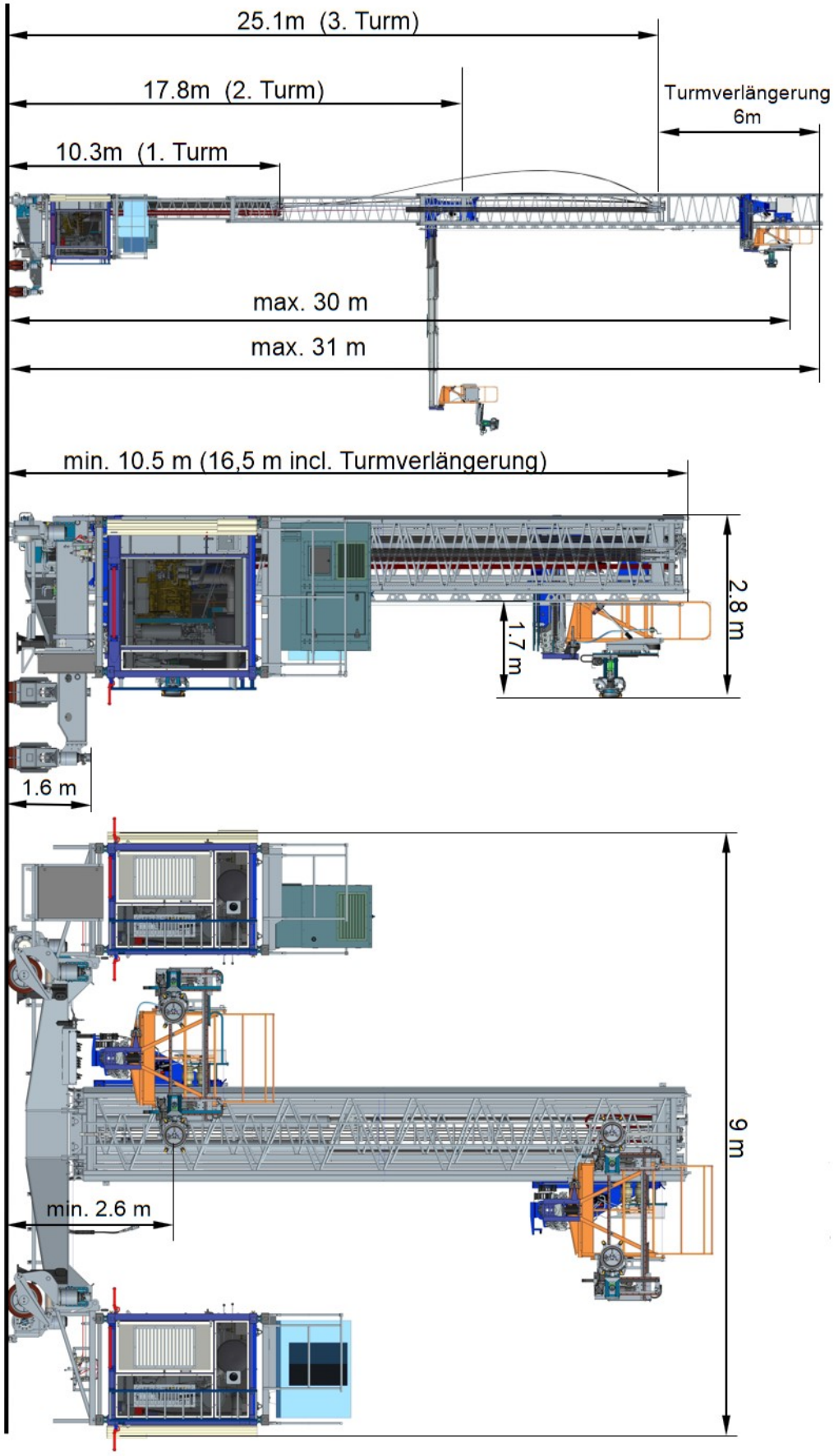
FORMELVERZEICHNIS

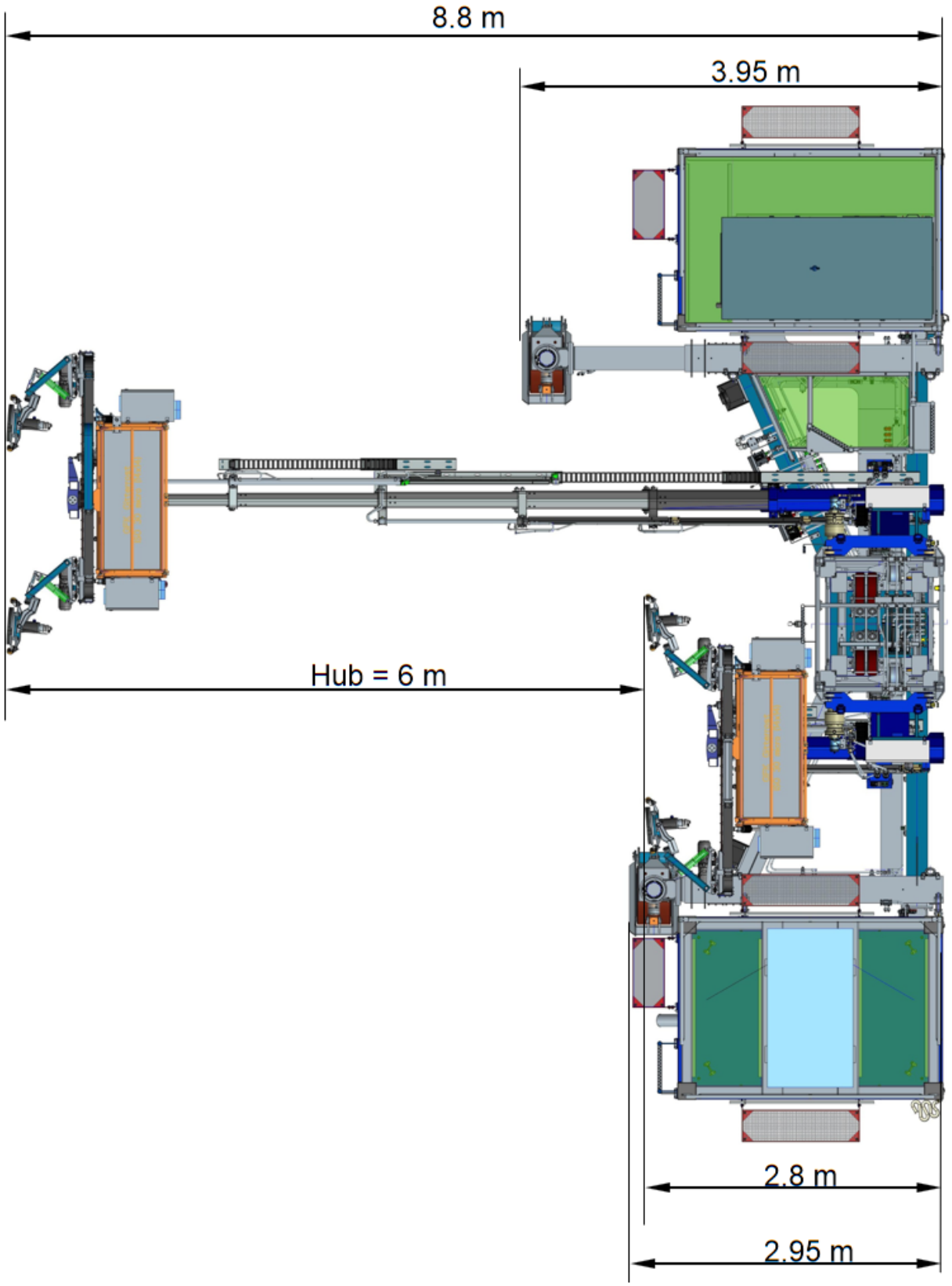
ABKÜRZUNGSVERZEICHNIS

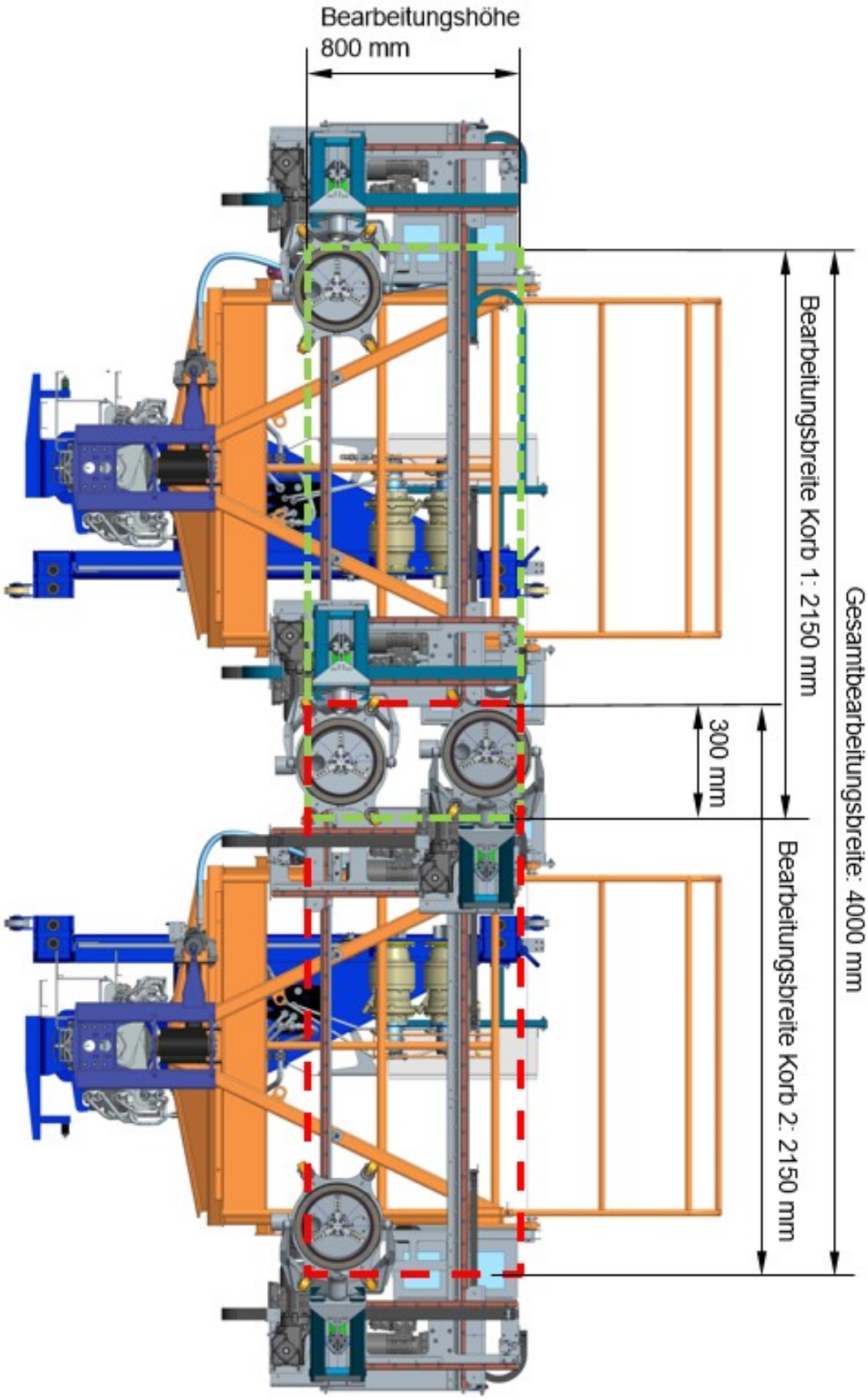
CCF	Common Cause Failure
CEN	Europäisches Komitee für Normen
Cenelec	Europäisches Komitee für Elektrotechnische Normung
CPU	Central Processing Unit
DC	Diagnosedeckungsgrad (Diagnostic Coverage)
DGUV	Deutsche Gesetzliche Unfallversicherung e.V.
EMV	Elektromagnetische Verträglichkeit
ETSI	Europäisches Institut für Telekommunikationsnormen
EUC	Equipment under control
EWR	Europäischer Wirtschaftsraum
FHAB	Fahrbare Hubarbeitsbühne
FMEA	Fehlermode- und Ausfallanalyse
gG	Ganzbereichsschutz für allgemeine Anwendung
GU	Generalunternehmer
HPT	Hubert Palfinger Technologies
HTC	Hull Treatment Carrier
IFA	Institut für Arbeitsschutz
ITP	Internal Tank Platform
MEMS	Mikro-elektro-mechanischem System
MKB	Mastgeführte Kletterbühne
MRL	Maschinenrichtlinie
MSV	Maschinensicherheitsverordnung
$MTTF_D$	Mean Time to Dangerous Failure
PFH_D	durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde
PL	Performance Level
RFMT	Rail Floor Multi Tool
RJT	Rotor Jet Tool
SB	Subsysteme
SIL	Safety Integrity Level
SRESW	Sicherheitsbezogenen Embedded-Software

STEP	Ship Treatment Elevating Platform
STO	Safety torque off, sicher abgeschaltetes Moment
UHP Pumpe	Ultrahochdruck-Pumpe

ANHANG 1: GRUNDABMESSUNGEN DES STEPS




8.8 m
3.95 m
Hub = 6 m
2.8 m
2.95 m


Bearbeitungshöhe
800 mm
Bearbeitungsbreite Korb 1: 2150 mm
300 mm
Bearbeitungsbreite Korb 2: 2150 mm
Gesamtbearbeitungsbreite: 4000 mm

ANHANG 2: SISTEMA – DETAILLIERTE ZUSAMMENFASSUNG

SISTEMA - Sicherheit von Steuerungen an Maschinen

Projektname: Masterarbeit - STEP

Dateidatum: 28.01.2018 10:37:49 Reportdatum: 28.01.2018 Prüfsumme: deede0e33e596d4803c9de10adaa75bb

PR **Projektname: Masterarbeit - STEP**

Name der Projektdatei:	G:\01_Masterarbeit\04_Working\SISTEMA\Masterarbeit.ssm
Erstellungsdatum:	02.12.2017 21:15:47
Projektstatus:	Erledigt
Projektnummer:	
Projektversion:	1
Autoren:	Thomas Moßhammer
Projektleitende:	Thomas Moßhammer
Prüfende:	
Gefahrenstelle / Maschine:	STEP
Dokumentation:	
Dokument:	
Version der Software:	2.0.7 build 2
Version der Norm:	ISO 13849-1:2015, ISO 13849-2:2012
Prüfsumme:	deede0e33e596d4803c9de10adaa75bb
Optionen:	☑ DC-Zwischenstufen zur Berechnung der PFHD verwenden (genauer) ☐ MTTFD-Kappung für Kategorie 4 von 2500 auf 100 Jahre absenken
Status:	grün
Anmerkung:	Für das Projekt (bzw. seine untergeordneten Grundelemente) liegen keine Meldungen vor.

Druckoptionen

- ☑ Gerätedetails anzeigen
- ☑ Dokumentationen zu SF, SB, BL und EL anzeigen
- ☑ CCF- und DC-Maßnahmen detailliert anzeigen
- ☑ Anforderungen an PL und Kategorie anzeigen
- ☑ Kennwerte-Dokumentationen zu PLr, PL, Kategorie, CCF, MTTFD und DC anzeigen
- ☑ Meldungen anzeigen

Enthaltene Sicherheitsfunktionen

SF Name: Neigungsgrenzen

Gefordert: PLr e	Erreicht: PL e	PFHD [1/h]: 3,5E-8	Status: grün

SF Name: Neigungsgrenzen (optimiert)

Gefordert: PLr e	Erreicht: PL e	PFHD [1/h]: 4,5E-8	Status: grün

SISTEMA - Sicherheit von Steuerungen an Maschinen

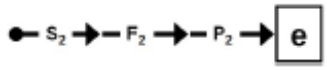
Projektname: **Masterarbeit - STEP**

Dateidatum: 28.01.2018 10:37:49 Reportdatum: 28.01.2018 Prüfsumme: deede0e33e596d4803c9de10adaa75bb

SF Sicherheitsfunktion: Neigungsgrenzen

Typ der Sicherheitsfunktion:	Sicherheitsbezogene Stoppfunktion, eingeleitet durch eine Schutzeinrichtung
Auslösendes Ereignis:	Überschreiten der max. zulässigen Neigung des Turmes +0,2° / +0,8°
Reaktion und Verhalten bei Energieausfall:	Stillsetzen der gefahrbringenden Bewegungen Abschaltung der Hydraulikventile
Sicherer Zustand:	Stillstand der gefahrbringenden Bewegungen!
Betriebsart:	Normalbetrieb
Häufigkeit der Anforderung:	~ 20 Zyklen/Jahr
Nachlaufzeit:	< 200 ms
Priorität:	Höchste Priorität nach Not-Halt
Dokumentation:	
Dokument:	

Erforderlicher Performance Level Sicherheitsfunktion

PLr (durch Risikograph):	e
Schwere der Verletzung (S): False	Schwere (üblicherweise irreversible) Verletzung, einschl. Tod
Häufigkeit / Dauer der Exposition (F):	Häufig bis dauernd / lange Dauer der Exposition
Möglichkeit der Vermeidung (P):	Kaum möglich
Risikograph:	
Dokumentation:	Die Eintrittswahrscheinlichkeit kann für diese Sicherheitsfunktion mit niedrig angegeben werden. Aus diesem Grund darf der PLr von "e" auf "d" geändert werden.
Dokument:	

Performance Level Sicherheitsfunktion

Erreichter PL: e PFHD [1/h]: 3,5E-8

Status / Meldungen Sicherheitsfunktion

Status: grün

Subsysteme (1 / 5)

SB Name: SIMATIC ET200M - fehlersichere Module | SM336 F-AI 6 | 6ES7336-4GE00-0AB0

Betriebsmittelkennzeichen: K1 Inventarnummer:

Gerätedetails Subsystem

Gerätehersteller:	SIEMENS AG
Geräteidentifikator:	SM336 F-AI 6_6ES7336-4GE00-0AB0_SIMATIC ET200M - fail-safe Modules
Gerätegruppe:	SIMATIC ET200M - fehlersichere Module

Artikelnummer: 6ES7336-4GE00-0AB0 Revisionsnummer:

SISTEMA - Sicherheit von Steuerungen an Maschinen

Projektname: **Masterarbeit - STEP**

Dateidatum: 28.01.2018 10:37:49 Reportdatum: 28.01.2018 Prüfsumme: deede0e33e596d4803c9de10adaa75bb

SF Sicherheitsfunktion: Neigungsgrenzen

Funktion:	☐ Eingabe ☐ Ausgabe	☑ Logik ☐ unbekannt
Anwendungsfall:	- | Zweikanalig | - | - | -	
Beschreibung des Anwendungsfalls:		

Dokumentation Subsystem

Dokumentation:	SIMATIC S7, ANALOGEINGABE SM336, 6 AE; 15 BIT; 20-POLIG, FEHLERSICHERE ANALOGEINGAENGE FUER SIMATIC S7F-SYSTEME MIT DIAGNOSEALARM
Dokument:	http://support.automation.siemens.com/WW/llisapi.dll/csfetch/19026151/s7300_failsafe_signal_modules_manual_de-DE_de-DE.pdf

Performance Level Subsystem

PL Bestimmung:	PL bzw. PFHD-Wert direkt angeben (Hersteller garantiert die Erfüllung der Kategorie- und PL-Anforderungen)
PL: e	Software geeignet bis PL: n.a.
Erreichter PL: e	PFHD [1/h]: 1E-9
Dokumentation:	
Gebrauchsdauer [a]: 20	Kleinste Gebrauchsdauer [a]: 20

Kategorie Subsystem

Kat.:	4
Kategorie-Anforderungen:	erfüllt
Anforderungen der Kategorie:	Da die Kategorie durch den Hersteller angegeben wird, verantwortet dieser auch die Erfüllung der Anforderungen.
Dokumentation:	
Quelle (z.B. Norm) Kategorie:	
Datei:	

Status / Meldungen Subsystem

Status:	grün

Subsysteme (2 / 5)

SB Name: SIMATIC S7 F-CPU | CPU 1512SPF-1PN | 6ES7512-1SK01-0AB0

Betriebsmittelkennzeichen: K1 Inventarnummer:

Gerätedetails Subsystem

Gerätehersteller:	SIEMENS AG
Geräteidentifikator:	CPU 1512SPF-1PN _6ES7512-1SK01-0AB0_SIMATIC S7 F-CPU
Gerätegruppe:	SIMATIC S7 F-CPU
Artikelnummer: 6ES7512-1SK01-0AB0	Revisionsnummer:

SISTEMA - Sicherheit von Steuerungen an Maschinen

Projektname: **Masterarbeit - STEP**

Dateidatum: 28.01.2018 10:37:49 Reportdatum: 28.01.2018 Prüfsumme: deede0e33e596d4803c9de10adaa75bb

SF Sicherheitsfunktion: Neigungsgrenzen

Funktion:	☐ Eingabe ☐ Ausgabe	☑ Logik ☐ unbekannt
Anwendungsfall:	Standard Anwendungsfall	
Beschreibung des Anwendungsfalls:		

Dokumentation Subsystem

Dokumentation:	SIMATIC S7-1500F, CPU 1512SP F-1 PN FUER ET 200SP, ZENTRALBAUGRUPPE MIT ARBEITSSPEICHER 300 KB FUER PROGRAMM UND 1 MB FUER DATEN, 1. SCHNITTSTELLE: PROFINET IRT MIT 3 PORT SWITCH, 48 NS BIT-PERFORMANCE, SIMATIC MEMORY CARD NOTWENDIG, BUSADAPTER NOTWENDIG FUER PORT 1 UND 2
Dokument:	https://support.industry.siemens.com/cs/attachments/107672531/et200sp_cpu1512sp_f_1_pn_manual_de-DE_de-DE.pdf

Performance Level Subsystem

PL Bestimmung:	PL bzw. PFHD-Wert direkt angeben (Hersteller garantiert die Erfüllung der Kategorie- und PL-Anforderungen)
PL: e	Software geeignet bis PL: n.a.
Erreichter PL: e	PFHD [1/h]: 2E-9
Dokumentation:	
Gebrauchsdauer [a]: 20	Kleinste Gebrauchsdauer [a]: 20

Kategorie Subsystem

Kat.:	4
Kategorie-Anforderungen:	erfüllt
Anforderungen der Kategorie:	Da die Kategorie durch den Hersteller angegeben wird, verantwortet dieser auch die Erfüllung der Anforderungen.
Dokumentation:	
Quelle (z.B. Norm) Kategorie:	
Datei:	

Status / Meldungen Subsystem

Status:	grün

Subsysteme (3 / 5)

SB Name: SIMATIC ET200SP - fehlersichere Module | EM136 4 F-DQ | 6ES7136-6DB00-0CA0

Betriebsmittelkennzeichen: K1 Inventarnummer:

Gerätedetails Subsystem

Gerätehersteller:	SIEMENS AG
Geräteidentifikator:	EM136 4 F-DQ_6ES7136-6DB00-0CA0_SIMATIC ET200SP - fail-safe -Modules

SISTEMA - Sicherheit von Steuerungen an Maschinen

Projektname: **Masterarbeit - STEP**

Dateidatum: 28.01.2018 10:37:49 Reportdatum: 28.01.2018 Prüfsumme: deede0e33e596d4803c9de10adaa75bb

SF Sicherheitsfunktion: Neigungsgrenzen

Gerätegruppe:	SIMATIC ET200SP - fehlersichere Module
Artikelnummer: 6ES7136-6DB00-0CA0	Revisionsnummer:
Funktion:	☐ Eingabe ☑ Logik ☐ Ausgabe ☐ unbekannt
Anwendungsfall:	Standard Anwendungsfall
Beschreibung des Anwendungsfalls:	

Dokumentation Subsystem

Dokumentation:	SIMATIC DP, ELEKTRONIKMODUL F. ET 200SP, 4 F-DQ PROFISAFE, DC 24V/2A, 15MM BAUBREITE BIS PL E (ISO13849) BIS SIL 3 (IEC 61508)
Dokument:	https://support.automation.siemens.com/WW/llisapi.dll/csfetch/78645789/et200sp_f_dq_4x24vdc_2a_pm_hf_manual_de-DE_de-DE.pdf

Performance Level Subsystem

PL Bestimmung:	PL bzw. PFHD-Wert direkt angeben (Hersteller garantiert die Erfüllung der Kategorie- und PL-Anforderungen)
PL: e	Software geeignet bis PL: n.a.
Erreichter PL: e	PFHD [1/h]: 1E-9
Dokumentation:	
Gebrauchsdauer [a]: 20	Kleinste Gebrauchsdauer [a]: 20

Kategorie Subsystem

Kat.:	4
Kategorie-Anforderungen:	erfüllt
Anforderungen der Kategorie:	Da die Kategorie durch den Hersteller angegeben wird, verantwortet dieser auch die Erfüllung der Anforderungen.
Dokumentation:	
Quelle (z.B. Norm) Kategorie:	
Datei:	

Status / Meldungen Subsystem

Status:	grün

Subsysteme (4 / 5)

SB Name: Profisafe Abschlag

Betriebsmittelkennzeichen:	Inventarnummer:

Gerätedetails Subsystem

Gerätehersteller:	
Geräteidentifikator:	

SISTEMA - Sicherheit von Steuerungen an Maschinen

Projektname: **Masterarbeit - STEP**

Dateidatum: 28.01.2018 10:37:49 Reportdatum: 28.01.2018 Prüfsumme: deede0e33e596d4803c9de10adaa75bb

SF Sicherheitsfunktion: Neigungsgrenzen

Gerätegruppe:		
Artikelnummer:		Revisionsnummer:
Funktion:	☐ Eingabe ☐ Ausgabe	☑ Logik ☑ unbekannt
Anwendungsfall:		
Beschreibung des Anwendungsfalls:		

Dokumentation Subsystem

Dokumentation:	
Dokument:	

Performance Level Subsystem

PL Bestimmung:	PL bzw. PFHD-Wert direkt angeben (Hersteller garantiert die Erfüllung der Kategorie- und PL-Anforderungen)
PL: e	Software geeignet bis PL: n.a.
Erreichter PL: e	PFHD [1/h]: 1E-9
Dokumentation:	
Gebrauchsdauer [a]: 20	Kleinste Gebrauchsdauer [a]: 20

Kategorie Subsystem

Kat.:	4
Kategorie-Anforderungen:	erfüllt
Anforderungen der Kategorie:	Da die Kategorie durch den Hersteller angegeben wird, verantwortet dieser auch die Erfüllung der Anforderungen.
Dokumentation:	
Quelle (z.B. Norm) Kategorie:	
Datei:	

Status / Meldungen Subsystem

Status:	grün

Subsysteme (5 / 5)

SB Name: Steuerstromkreis + Hydraulikventile

Betriebsmittelkennzeichen:	Inventarnummer:

Gerätedetails Subsystem

Gerätehersteller:	
Geräteidentifikator:	
Gerätegruppe:	
Artikelnummer:	Revisionsnummer:

SISTEMA - Sicherheit von Steuerungen an Maschinen

Projektname: **Masterarbeit - STEP**

Dateidatum: 28.01.2018 10:37:49 Reportdatum: 28.01.2018 Prüfsumme: deede0e33e596d4803c9de10adaa75bb

SF Sicherheitsfunktion: Neigungsgrenzen

Funktion:	☐ Eingabe ☐ Ausgabe	☐ Logik ☑ unbekannt
Anwendungsfall:		
Beschreibung des Anwendungsfalls:		

Dokumentation Subsystem

Dokumentation:	
Dokument:	

Performance Level Subsystem

PL Bestimmung:	PL bzw. PFHD-Wert aus Kategorie, MTTFD und DCavg ermitteln
Software geeignet bis PL:	n.a.
PL-Anforderungen:	erfüllt
Der PL wird durch Abschätzung folgender Aspekte bestimmt:	- Verhalten der Sicherheitsfunktion unter Fehlerbedingungen (siehe Abschnitt 6) [erfüllt] - sicherheitsbezogene Software nach Abschnitt 4.6 entwickelt bzw. keine Software vorhanden [erfüllt] - systematische Ausfälle (siehe Anhang G) [erfüllt] - Fähigkeit, die Sicherheitsfunktion unter vorhersehbaren Umgebungsbedingungen auszuführen [erfüllt]
Erreichter PL: e	PFHD [1/h]: 3E-8
Dokumentation:	

Kategorie Subsystem

Kat.:	3
Kategorie-Anforderungen:	erfüllt
Anforderungen der Kategorie:	- Übereinstimmung mit zutreffenden Normen, um zu erwartenden Einflüssen standzuhalten. [erfüllt] - Grundlegende Sicherheitsprinzipien werden angewendet. [erfüllt] - Bewährte Sicherheitsprinzipien werden angewendet. [erfüllt] - Eine Ein-Fehlertoleranz und angemessene Fehlererkennung sind gegeben. [erfüllt] - MTTFD ist mindestens Niedrig oder Mittel oder Hoch. [erfüllt] - DCavg ist mindestens Niedrig oder Mittel. [erfüllt] - Der erreichte Punktestand der CCF-Bewertung beträgt mindestens 65. [erfüllt]
Dokumentation:	
Quelle (z.B. Norm) Kategorie:	
Datei:	

MTTFD und Gebrauchsdauer Subsystem

MTTFD [a]:	84,2 (Hoch)
Gebrauchsdauer [a]: 20	Kleinste Gebrauchsdauer [a]: 20

SISTEMA - Sicherheit von Steuerungen an Maschinen

Projektname: **Masterarbeit - STEP**

Dateidatum: 28.01.2018 10:37:49 Reportdatum: 28.01.2018 Prüfsumme: deede0e33e596d4803c9de10adaa75bb

SF Sicherheitsfunktion: Neigungsgrenzen

Diagnosedeckungsgrad Subsystem

DCavg [%]:	99 (Hoch)

Fehler gemeinsamer Ursache Subsystem

CCF-Punkte:	80 (erfüllt)
CCF-Maßnahmen:	- Trennung / Abtrennung (15 Punkte) Physikalische Trennung zwischen den Signalpfaden, Trennung der Verdrahtung / Verrohrung, ausreichende Luft- und Kriechstrecken auf gedruckten Schaltungen. - Entwurf / Anwendung / Erfahrung (15 Punkte) Schutz gegen Überspannung, Überdruck, Überstrom, usw. - Entwurf / Anwendung / Erfahrung (5 Punkte) Verwendung bewährter Bauteile - Beurteilung / Analyse (5 Punkte) Sind die Ergebnisse einer Ausfallart und Effektanalyse berücksichtigt worden, um Ausfälle infolge gemeinsamer Ursache in der Entwicklung zu vermeiden? - Kompetenz / Ausbildung (5 Punkte) Sind Konstrukteure / Monteure geschult worden, um die Gründe und Auswirkungen von Ausfällen infolge gemeinsamer Ursache zu erkennen? - Umgebung (25 Punkte) Schutz vor Verunreinigung und elektromagnetischer Beeinflussung (EMC) gegen CCF in Übereinstimmung mit den angemessenen Normen. Fluidische Systeme: Filtrierung des Druckmediums, Verhinderung von Schmutzeintrag, Entwässerung von Druckluft, z. B. in Übereinstimmung mit den Anforderungen des Herstellers für die Reinheit des Druckmediums, Elektrische Systeme: Wurde das System hinsichtlich elektromagnetischer Immunität geprüft, z. B. wie in zutreffenden Normen gegen CCF festgelegt. Bei kombinierten fluidischen und elektrischen Systemen sollten beide Aspekte berücksichtigt werden. - Umgebung (10 Punkte) Andere Einflüsse. Wurden alle Anforderungen hinsichtlich Unempfindlichkeit gegenüber allen relevanten Umgebungsbedingungen wie Temperatur, Schock, Vibration, Feuchte (z. B. wie in den zutreffenden Normen festgelegt) berücksichtigt?
Dokumentation:	
Dokument:	

Status / Meldungen Subsystem

Status:	grün

Kanäle / Testkanal (1 / 2)

CH Name: Kanal 1

MTTFD [a]: 84,2

SISTEMA - Sicherheit von Steuerungen an Maschinen

Projektname: **Masterarbeit - STEP**

Dateidatum: 28.01.2018 10:37:49 Reportdatum: 28.01.2018 Prüfsumme: deede0e33e596d4803c9de10adaa75bb

SF Sicherheitsfunktion: Neigungsgrenzen

Blöcke (1 / 4)

BL Name: Neigungssensor

Betriebsmittelkennzeichen: F1 Inventarnummer:

Gerätedetails Block

Gerätehersteller:	Turck	
Geräteidentifikator:		
Gerätegruppe:		
Artikelnummer: B2N10H-Q20L60-2LI2-H1151	Revisionsnummer:	
Funktion:	☑ Eingabe ☐ Ausgabe	☐ Logik ☐ unbekannt
Technologie:	elektronisch	
Kategorie:	1	
Anwendungsfall:		
Beschreibung des Anwendungsfalls:		

Dokumentation Block

Dokumentation:	
Dokument:	

MTTFD und Gebrauchsdauer Block

MTTFD [a]: 203 (Hoch)	
Gebrauchsdauer [a]: 20	Kleinste Gebrauchsdauer [a]: 20
Rate gefahrbringender Ausfälle [FIT]: 562,3	
Dokumentation:	

Diagnosedeckungsgrad Block

DC [%]: 99 (Hoch)	
Maßnahme:	Kreuzvergleich von Eingangssignalen mit unmittelbarem und Zwischenergebnissen in der Logik (L) und zeitlich und logische Programmlaufüberwachung und Erkennung statischer Ausfälle und Kurzschlüsse (bei Mehrfach-Ein-/Eingängen) (Eingabeeinheit) (99 %)
Dokumentation:	

Status / Meldungen Block

Status:	grün

Blöcke (2 / 4)

BL Name: Koppelrelais

Betriebsmittelkennzeichen: K2 Inventarnummer:

SISTEMA - Sicherheit von Steuerungen an Maschinen

Projektname: **Masterarbeit - STEP**

Dateidatum: 28.01.2018 10:37:49 Reportdatum: 28.01.2018 Prüfsumme: deede0e33e596d4803c9de10adaa75bb

SF Sicherheitsfunktion: Neigungsgrenzen

Gerätedetails Block

Gerätehersteller:	Phoenix Contact
Geräteidentifikator:	
Gerätegruppe:	
Artikelnummer: PSR-URM-2X21	Revisionsnummer:
Funktion:	☐ Eingabe ☐ Logik ☑ Ausgabe ☐ unbekannt
Technologie:	elektromechanisch
Kategorie:	-
Anwendungsfall:	
Beschreibung des Anwendungsfalls:	

Dokumentation Block

Dokumentation:	
Dokument:	

MTTFD und Gebrauchsdauer Block

MTTFD [a]: 7200 (Hoch)	
Gebrauchsdauer [a]: 20	Kleinste Gebrauchsdauer [a]: 20
B10D [Zyklen]: 180000	nop [Zyklen/a]: 250
Dokumentation:	

Diagnosedeckungsgrad Block

DC [%]: 99 (Hoch)	
Maßnahme:	Direkte Überwachung (z. B. elektrische Überwachung der Steuerungsventile, Überwachung elektromechanischer Einheiten durch Zwangsführung) (Ausgabeeinheit) (99 %)
Dokumentation:	

Status / Meldungen Block

Status:	grün

Blöcke (3 / 4)

BL Name: Koppelrelais

Betriebsmittelkennzeichen: K3	Inventarnummer:

Gerätedetails Block

Gerätehersteller:	Phoenix Contact
Geräteidentifikator:	

SISTEMA - Sicherheit von Steuerungen an Maschinen

Projektname: **Masterarbeit - STEP**

Dateidatum: 28.01.2018 10:37:49 Reportdatum: 28.01.2018 Prüfsumme: deede0e33e596d4803c9de10adaa75bb

SF Sicherheitsfunktion: Neigungsgrenzen

Gerätegruppe:		
Artikelnummer: PSR-URM-2X21	Revisionsnummer:	
Funktion:	☐ Eingabe ☑ Ausgabe	☐ Logik ☐ unbekannt
Technologie:	elektromechanisch	
Kategorie:	-	
Anwendungsfall:		
Beschreibung des Anwendungsfalls:		

Dokumentation Block

Dokumentation:	
Dokument:	

MTTFD und Gebrauchsdauer Block

MTTFD [a]: 7200 (Hoch)	
Gebrauchsdauer [a]: 20	Kleinste Gebrauchsdauer [a]: 20
B10D [Zyklen]: 180000	nop [Zyklen/a]: 250
Dokumentation:	

Diagnosedeckungsgrad Block

DC [%]: 99 (Hoch)	
Maßnahme:	Direkte Überwachung (z. B. elektrische Überwachung der Steuerungsventile, Überwachung elektromechanischer Einheiten durch Zwangsführung) (Ausgabeeinheit) (99 %)
Dokumentation:	

Status / Meldungen Block

Status:	grün

Blöcke (4 / 4)

BL Name: Hauptfreigabeventil

Betriebsmittelkennzeichen: IV3	Inventarnummer:	

Gerätedetails Block

Gerätehersteller:	Danfoss	
Geräteidentifikator:		
Gerätegruppe:		
Artikelnummer: PVG32	Revisionsnummer:	
Funktion:	☐ Eingabe ☑ Ausgabe	☐ Logik ☐ unbekannt

SISTEMA - Sicherheit von Steuerungen an Maschinen

Projektname: **Masterarbeit - STEP**

Dateidatum: 28.01.2018 10:37:49 Reportdatum: 28.01.2018 Prüfsumme: deede0e33e596d4803c9de10adaa75bb

SF **Sicherheitsfunktion: Neigungsgrenzen**

Technologie:	hydraulisch
Kategorie:	-
Anwendungsfall:	
Beschreibung des Anwendungsfalls:	

Dokumentation Block

Dokumentation:	
Dokument:	

MTTFD und Gebrauchsdauer Block

MTTFD [a]: 150 (Hoch)

Gebrauchsdauer [a]: 20	Kleinste Gebrauchsdauer [a]: 20
Rate gefahrbringender Ausfälle [FIT]: 761	
Dokumentation:	

Diagnosedeckungsgrad Block

DC [%]: 99 (Hoch)

Maßnahme:	Direkte Überwachung (z. B. elektrische Überwachung der Steuerungsventile, Überwachung elektromechanischer Einheiten durch Zwangsführung) (Ausgabeeinheit) (99 %)
Dokumentation:	

Status / Meldungen Block

Status:	grün

Kanäle / Testkanal (2 / 2)

CH Name: Kanal 2

MTTFD [a]: 84,2

Blöcke (1 / 4)

BL Name: Neigungssensor

Betriebsmittelkennzeichen: F2	Inventarnummer:

Gerätedetails Block

Gerätehersteller:	Kübler
Geräteidentifikator:	
Gerätegruppe:	
Artikelnummer: 8.IS40.21121	Revisionsnummer:

Funktion: ☑ Eingabe ☐ Logik ☐ Ausgabe ☐ unbekannt

SISTEMA - Sicherheit von Steuerungen an Maschinen

Projektname: **Masterarbeit - STEP**

Dateidatum: 28.01.2018 10:37:49 Reportdatum: 28.01.2018 Prüfsumme: deede0e33e596d4803c9de10adaa75bb

SF Sicherheitsfunktion: Neigungsgrenzen

Technologie:	elektronisch
Kategorie:	1
Anwendungsfall:	
Beschreibung des Anwendungsfalls:	

Dokumentation Block

Dokumentation:	
Dokument:	

MTTFD und Gebrauchsdauer Block

MTTFD [a]: 203 (Hoch)	
Gebrauchsdauer [a]: 20	Kleinste Gebrauchsdauer [a]: 20
Rate gefahrbringender Ausfälle [FIT]: 562,3	
Dokumentation:	

Diagnosedeckungsgrad Block

DC [%]: 99 (Hoch)	
Maßnahme:	Kreuzvergleich von Eingangssignalen mit unmittelbarem und Zwischenergebnissen in der Logik (L) und zeitlich und logische Programmlaufüberwachung und Erkennung statischer Ausfälle und Kurzschlüsse (bei Mehrfach-Ein-/Eingängen) (Eingabeeinheit) (99 %)
Dokumentation:	

Status / Meldungen Block

Status:	grün

Blöcke (2 / 4)

BL Name: Koppelrelais

Betriebsmittelkennzeichen: K4	Inventarnummer:

Gerätedetails Block

Gerätehersteller:	Phoenix Contact
Geräteidentifikator:	
Gerätegruppe:	
Artikelnummer: PSR-URM-2X21	Revisionsnummer:
Funktion:	☐ Eingabe ☐ Logik ☑ Ausgabe ☐ unbekannt
Technologie:	elektromechanisch
Kategorie:	-
Anwendungsfall:	

SISTEMA - Sicherheit von Steuerungen an Maschinen

Projektname: **Masterarbeit - STEP**

Dateidatum: 28.01.2018 10:37:49 Reportdatum: 28.01.2018 Prüfsumme: deede0e33e596d4803c9de10adaa75bb

SF Sicherheitsfunktion: Neigungsgrenzen

Beschreibung des Anwendungsfalls:

Dokumentation Block

Dokumentation:

Dokument:

MTTFD und Gebrauchsdauer Block

MTTFD [a]: 7200 (Hoch)

Gebrauchsdauer [a]: 20	Kleinste Gebrauchsdauer [a]: 20
B10D [Zyklen]: 180000	nop [Zyklen/a]: 250

Dokumentation:

Diagnosedeckungsgrad Block

DC [%]: 99 (Hoch)

Maßnahme:	Direkte Überwachung (z. B. elektrische Überwachung der Steuerungsventile, Überwachung elektromechanischer Einheiten durch Zwangsführung) (Ausgabeeinheit) (99 %)

Dokumentation:

Status / Meldungen Block

Status:	grün

Blöcke (3 / 4)

BL Name: Koppelrelais

Betriebsmittelkennzeichen: K5	Inventarnummer:

Gerätedetails Block

Gerätehersteller:	Phoenix Contact
Geräteidentifikator:	
Gerätegruppe:	
Artikelnummer: PSR-URM-2X21	Revisionsnummer:

Funktion:	☐ Eingabe	☐ Logik
	☑ Ausgabe	☐ unbekannt
Technologie:	elektromechanisch	
Kategorie:	-	
Anwendungsfall:		
Beschreibung des Anwendungsfalls:		

Dokumentation Block

SISTEMA - Sicherheit von Steuerungen an Maschinen

Projektname: **Masterarbeit - STEP**

Dateidatum: 28.01.2018 10:37:49 Reportdatum: 28.01.2018 Prüfsumme: deede0e33e596d4803c9de10adaa75bb

SF Sicherheitsfunktion: Neigungsgrenzen

Dokumentation:

Dokument:

MTTFD und Gebrauchsdauer Block

MTTFD [a]: 7200 (Hoch)

Gebrauchsdauer [a]: 20	Kleinste Gebrauchsdauer [a]: 20
B10D [Zyklen]: 180000	nop [Zyklen/a]: 250

Dokumentation:

Diagnosedeckungsgrad Block

DC [%]: 99 (Hoch)

Maßnahme:	Direkte Überwachung (z. B. elektrische Überwachung der Steuerungsventile, Überwachung elektromechanischer Einheiten durch Zwangsführung) (Ausgabeeinheit) (99 %)

Dokumentation:

Status / Meldungen Block

Status:	grün

Blöcke (4 / 4)

BL Name: Hauptfreigabeventil

Betriebsmittelkennzeichen: IV4	Inventarnummer:

Gerätedetails Block

Gerätehersteller:	Danfoss
Geräteidentifikator:	
Gerätegruppe:	
Artikelnummer: PVG32	Revisionsnummer:
Funktion:	☐ Eingabe ☐ Logik ☑ Ausgabe ☐ unbekannt
Technologie:	unbekannt
Kategorie:	-
Anwendungsfall:	
Beschreibung des Anwendungsfalls:	

Dokumentation Block

Dokumentation:

Dokument:

MTTFD und Gebrauchsdauer Block

SISTEMA - Sicherheit von Steuerungen an Maschinen

Projektname: **Masterarbeit - STEP**

Dateidatum: 28.01.2018 10:37:49 Reportdatum: 28.01.2018 Prüfsumme: deede0e33e596d4803c9de10adaa75bb

SF Sicherheitsfunktion: Neigungsgrenzen

MTTFD [a]: 150 (Hoch)	
Gebrauchsdauer [a]: 20	Kleinste Gebrauchsdauer [a]: 20
Rate gefahrbringender Ausfälle [FIT]: 761	
Dokumentation:	

Diagnosedeckungsgrad Block

DC [%]: 99 (Hoch)	
Maßnahme:	Direkte Überwachung (z. B. elektrische Überwachung der Steuerungsventile, Überwachung elektromechanischer Einheiten durch Zwangsführung) (Ausgabeeinheit) (99 %)
Dokumentation:	

Status / Meldungen Block

Status:	grün

SISTEMA - Sicherheit von Steuerungen an Maschinen

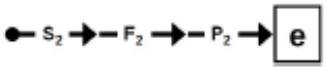
Projektname: **Masterarbeit - STEP**

Dateidatum: 28.01.2018 10:37:49 Reportdatum: 28.01.2018 Prüfsumme: deede0e33e596d4803c9de10adaa75bb

SF Sicherheitsfunktion: Neigungsgrenzen (optimiert)

Typ der Sicherheitsfunktion:	Sicherheitsbezogene Stoppfunktion, eingeleitet durch eine Schutzeinrichtung
Auslösendes Ereignis:	Überschreiten der max. zulässigen Neigung des Turmes +0,2° / +0,8°
Reaktion und Verhalten bei Energieausfall:	Stillsetzen der gefahrbringenden Bewegungen Abschaltung der Hydraulikventile
Sicherer Zustand:	Stillstand der gefahrbringenden Bewegungen!
Betriebsart:	Normalbetrieb
Häufigkeit der Anforderung:	~ 20 Zyklen/Jahr
Nachlaufzeit:	< 200 ms
Priorität:	Höchste Priorität nach Not-Halt
Dokumentation:	
Dokument:	

Erforderlicher Performance Level Sicherheitsfunktion

PLr (durch Risikograph):	e
Schwere der Verletzung (S): False	Schwere (üblicherweise irreversible) Verletzung, einschl. Tod
Häufigkeit / Dauer der Exposition (F):	Häufig bis dauernd / lange Dauer der Exposition
Möglichkeit der Vermeidung (P):	Kaum möglich
Risikograph:	
Dokumentation:	Die Eintrittswahrscheinlichkeit kann für diese Sicherheitsfunktion mit niedrig angegeben werden. Aus diesem Grund darf der PLr von "e" auf "d" geändert werden.
Dokument:	

Performance Level Sicherheitsfunktion

Erreichter PL: e PFHD [1/h]: 4,5E-8

Status / Meldungen Sicherheitsfunktion

Status: grün

Subsysteme (1 / 6)

SB Name: SIMATIC ET200M - fehlersichere Module | SM336 F-AI 6 | 6ES7336-4GE00-0AB0

Betriebsmittelkennzeichen: K1 Inventarnummer:

Gerätedetails Subsystem

Gerätehersteller:	SIEMENS AG
Geräteidentifikator:	SM336 F-AI 6_6ES7336-4GE00-0AB0_SIMATIC ET200M - fail-safe Modules
Gerätegruppe:	SIMATIC ET200M - fehlersichere Module

Artikelnummer: 6ES7336-4GE00-0AB0 Revisionsnummer:

SISTEMA - Sicherheit von Steuerungen an Maschinen

Projektname: **Masterarbeit - STEP**

Dateidatum: 28.01.2018 10:37:49 Reportdatum: 28.01.2018 Prüfsumme: deede0e33e596d4803c9de10adaa75bb

SF Sicherheitsfunktion: Neigungsgrenzen (optimiert)

Funktion:	☐ Eingabe ☐ Ausgabe	☑ Logik ☐ unbekannt
Anwendungsfall:	- | Zweikanalig | - | - | -	
Beschreibung des Anwendungsfalls:		

Dokumentation Subsystem

Dokumentation:	SIMATIC S7, ANALOGEINGABE SM336, 6 AE; 15 BIT; 20-POLIG, FEHLERSICHERE ANALOGEINGAENGE FUER SIMATIC S7F-SYSTEME MIT DIAGNOSEALARM
Dokument:	http://support.automation.siemens.com/WW/llisapi.dll/csfetch/19026151/s7300_failsafe_signal_modules_manual_de-DE_de-DE.pdf

Performance Level Subsystem

PL Bestimmung:	PL bzw. PFHD-Wert direkt angeben (Hersteller garantiert die Erfüllung der Kategorie- und PL-Anforderungen)
PL: e	Software geeignet bis PL: n.a.
Erreichter PL: e	PFHD [1/h]: 1E-9
Dokumentation:	
Gebrauchsdauer [a]: 20	Kleinste Gebrauchsdauer [a]: 20

Kategorie Subsystem

Kat.:	4
Kategorie-Anforderungen:	erfüllt
Anforderungen der Kategorie:	Da die Kategorie durch den Hersteller angegeben wird, verantwortet dieser auch die Erfüllung der Anforderungen.
Dokumentation:	
Quelle (z.B. Norm) Kategorie:	
Datei:	

Status / Meldungen Subsystem

Status:	grün

Subsysteme (2 / 6)

SB Name: SIMATIC S7 F-CPU | CPU 1512SPF-1PN | 6ES7512-1SK01-0AB0

Betriebsmittelkennzeichen: K1	Inventarnummer:

Gerätedetails Subsystem

Gerätehersteller:	SIEMENS AG
Geräteidentifikator:	CPU 1512SPF-1PN _6ES7512-1SK01-0AB0_SIMATIC S7 F-CPU
Gerätegruppe:	SIMATIC S7 F-CPU
Artikelnummer: 6ES7512-1SK01-0AB0	Revisionsnummer:

SISTEMA - Sicherheit von Steuerungen an Maschinen

Projektname: **Masterarbeit - STEP**

Dateidatum: 28.01.2018 10:37:49 Reportdatum: 28.01.2018 Prüfsumme: deede0e33e596d4803c9de10adaa75bb

SF Sicherheitsfunktion: Neigungsgrenzen (optimiert)

Funktion:	☐ Eingabe ☐ Ausgabe	☑ Logik ☐ unbekannt
Anwendungsfall:	Standard Anwendungsfall	
Beschreibung des Anwendungsfalls:		

Dokumentation Subsystem

Dokumentation:	SIMATIC S7-1500F, CPU 1512SP F-1 PN FUER ET 200SP, ZENTRALBAUGRUPPE MIT ARBEITSSPEICHER 300 KB FUER PROGRAMM UND 1 MB FUER DATEN, 1. SCHNITTSTELLE: PROFINET IRT MIT 3 PORT SWITCH, 48 NS BIT-PERFORMANCE, SIMATIC MEMORY CARD NOTWENDIG, BUSADAPTER NOTWENDIG FUER PORT 1 UND 2
Dokument:	https://support.industry.siemens.com/cs/attachments/107672531/et200sp_cpu1512sp_f_1_pn_manual_de-DE_de-DE.pdf

Performance Level Subsystem

PL Bestimmung:	PL bzw. PFHD-Wert direkt angeben (Hersteller garantiert die Erfüllung der Kategorie- und PL-Anforderungen)
PL: e	Software geeignet bis PL: n.a.
Erreichter PL: e	PFHD [1/h]: 2E-9
Dokumentation:	
Gebrauchsdauer [a]: 20	Kleinste Gebrauchsdauer [a]: 20

Kategorie Subsystem

Kat.:	4
Kategorie-Anforderungen:	erfüllt
Anforderungen der Kategorie:	Da die Kategorie durch den Hersteller angegeben wird, verantwortet dieser auch die Erfüllung der Anforderungen.
Dokumentation:	
Quelle (z.B. Norm) Kategorie:	
Datei:	

Status / Meldungen Subsystem

Status:	grün

Subsysteme (3 / 6)

SB Name: SIMATIC ET200SP - fehlersichere Module | EM136 1 F-RQ | 6ES7136-6RA00-0BF0

Betriebsmittelkennzeichen:	Inventarnummer:

Gerätedetails Subsystem

Gerätehersteller:	SIEMENS AG
Geräteidentifikator:	EM136 1 F-RQ_6ES7136-6RA00-0BF0_SIMATIC ET200SP - fail-safe -Modules

SISTEMA - Sicherheit von Steuerungen an Maschinen

Projektname: **Masterarbeit - STEP**

Dateidatum: 28.01.2018 10:37:49 Reportdatum: 28.01.2018 Prüfsumme: deede0e33e596d4803c9de10adaa75bb

SF Sicherheitsfunktion: Neigungsgrenzen (optimiert)

Gerätegruppe:	SIMATIC ET200SP - fehlersichere Module
Artikelnummer: 6ES7136-6RA00-0BF0	Revisionsnummer:
Funktion:	☐ Eingabe ☑ Logik ☑ Ausgabe ☐ unbekannt
Anwendungsfall:	- | Funktionstest einmal pro Monat | - | - | -
Beschreibung des Anwendungsfalls:	

Dokumentation Subsystem

Dokumentation:	
Dokument:	https://support.industry.siemens.com/cs/attachments/90181204/et200sp_f_rq_1x24vdc_24_230vac_5a_st_manual_de-DE_de-DE.pdf

Performance Level Subsystem

PL Bestimmung:	PL bzw. PFHD-Wert direkt angeben (Hersteller garantiert die Erfüllung der Kategorie- und PL-Anforderungen)
PL: e	Software geeignet bis PL: n.a.
Erreichter PL: e	PFHD [1/h]: 6E-9
Dokumentation:	
Gebrauchsdauer [a]: 20	Kleinste Gebrauchsdauer [a]: 20

Kategorie Subsystem

Kat.:	4
Kategorie-Anforderungen:	erfüllt
Anforderungen der Kategorie:	Da die Kategorie durch den Hersteller angegeben wird, verantwortet dieser auch die Erfüllung der Anforderungen.
Dokumentation:	
Quelle (z.B. Norm) Kategorie:	
Datei:	

Status / Meldungen Subsystem

Status:	grün

Subsysteme (4 / 6)

SB Name: SIMATIC ET200SP - fehlersichere Module | EM136 1 F-RQ | 6ES7136-6RA00-0BF0

Betriebsmittelkennzeichen:	Inventarnummer:

Gerätedetails Subsystem

Gerätehersteller:	SIEMENS AG
Geräteidentifikator:	EM136 1 F-RQ_6ES7136-6RA00-0BF0_SIMATIC ET200SP - fail-safe -Modules
Gerätegruppe:	SIMATIC ET200SP - fehlersichere Module

SISTEMA - Sicherheit von Steuerungen an Maschinen

Projektname: **Masterarbeit - STEP**

Dateidatum: 28.01.2018 10:37:49 Reportdatum: 28.01.2018 Prüfsumme: deede0e33e596d4803c9de10adaa75bb

SF Sicherheitsfunktion: Neigungsgrenzen (optimiert)

Artikelnummer: 6ES7136-6RA00-0BF0		Revisionsnummer:
Funktion:	☐ Eingabe ☑ Ausgabe	☑ Logik ☐ unbekannt
Anwendungsfall:	- | Funktionstest einmal pro Monat | - | - | -	
Beschreibung des Anwendungsfalls:		

Dokumentation Subsystem

Dokumentation:	
Dokument:	https://support.industry.siemens.com/cs/attachments/90181204/et200sp_f_rq_1x24vdc_24_230vac_5a_st_manual_de-DE_de-DE.pdf

Performance Level Subsystem

PL Bestimmung:	PL bzw. PFHD-Wert direkt angeben (Hersteller garantiert die Erfüllung der Kategorie- und PL-Anforderungen)

PL: e	Software geeignet bis PL: n.a.
Erreichter PL: e	PFHD [1/h]: 6E-9
Dokumentation:	
Gebrauchsdauer [a]: 20	Kleinste Gebrauchsdauer [a]: 20

Kategorie Subsystem

Kat.:	4
Kategorie-Anforderungen:	erfüllt
Anforderungen der Kategorie:	Da die Kategorie durch den Hersteller angegeben wird, verantwortet dieser auch die Erfüllung der Anforderungen.
Dokumentation:	
Quelle (z.B. Norm) Kategorie:	
Datei:	

Status / Meldungen Subsystem

Status:	grün

Subsysteme (5 / 6)

SB Name: Profisafe Abschlag

Betriebsmittelkennzeichen:	Inventarnummer:

Gerätedetails Subsystem

Gerätehersteller:	
Geräteidentifikator:	
Gerätegruppe:	
Artikelnummer:	Revisionsnummer:

SISTEMA - Sicherheit von Steuerungen an Maschinen

Projektname: **Masterarbeit - STEP**

Dateidatum: 28.01.2018 10:37:49 Reportdatum: 28.01.2018 Prüfsumme: deede0e33e596d4803c9de10adaa75bb

SF Sicherheitsfunktion: Neigungsgrenzen (optimiert)

Funktion:	☐ Eingabe ☐ Ausgabe	☑ Logik ☑ unbekannt
Anwendungsfall:		
Beschreibung des Anwendungsfalls:		

Dokumentation Subsystem

Dokumentation:	
Dokument:	

Performance Level Subsystem

PL Bestimmung:	PL bzw. PFHD-Wert direkt angeben (Hersteller garantiert die Erfüllung der Kategorie- und PL-Anforderungen)
PL: e	Software geeignet bis PL: n.a.
Erreichter PL: e	PFHD [1/h]: 1E-9
Dokumentation:	
Gebrauchsdauer [a]: 20	Kleinste Gebrauchsdauer [a]: 20

Kategorie Subsystem

Kat.:	4
Kategorie-Anforderungen:	erfüllt
Anforderungen der Kategorie:	Da die Kategorie durch den Hersteller angegeben wird, verantwortet dieser auch die Erfüllung der Anforderungen.
Dokumentation:	
Quelle (z.B. Norm) Kategorie:	
Datei:	

Status / Meldungen Subsystem

Status:	grün

Subsysteme (6 / 6)

SB Name: Steuerstromkreis + Hydraulikventile

Betriebsmittelkennzeichen:	Inventarnummer:

Gerätedetails Subsystem

Geräteherstellter:	
Geräteidentifikator:	
Gerätegruppe:	
Artikelnummer:	Revisionsnummer:

Funktion:	☐ Eingabe ☐ Ausgabe	☐ Logik ☑ unbekannt
Anwendungsfall:		

SISTEMA - Sicherheit von Steuerungen an Maschinen

Projektname: **Masterarbeit - STEP**

Dateidatum: 28.01.2018 10:37:49 Reportdatum: 28.01.2018 Prüfsumme: deede0e33e596d4803c9de10adaa75bb

SF Sicherheitsfunktion: Neigungsgrenzen (optimiert)

Beschreibung des Anwendungsfalls:	

Dokumentation Subsystem

Dokumentation:	
Dokument:	

Performance Level Subsystem

PL Bestimmung:	PL bzw. PFHD-Wert aus Kategorie, MTTFD und DCavg ermitteln
Software geeignet bis PL:	n.a.
PL-Anforderungen:	erfüllt
Der PL wird durch Abschätzung folgender Aspekte bestimmt:	- Verhalten der Sicherheitsfunktion unter Fehlerbedingungen (siehe Abschnitt 6) [erfüllt] - sicherheitsbezogene Software nach Abschnitt 4.6 entwickelt bzw. keine Software vorhanden [erfüllt] - systematische Ausfälle (siehe Anhang G) [erfüllt] - Fähigkeit, die Sicherheitsfunktion unter vorhersehbaren Umgebungsbedingungen auszuführen [erfüllt]

Erreichter PL: e	PFHD [1/h]: 2,9E-8
Dokumentation:	

Kategorie Subsystem

Kat.:	3
Kategorie-Anforderungen:	erfüllt
Anforderungen der Kategorie:	- Übereinstimmung mit zutreffenden Normen, um zu erwartenden Einflüssen standzuhalten. [erfüllt] - Grundlegende Sicherheitsprinzipien werden angewendet. [erfüllt] - Bewährte Sicherheitsprinzipien werden angewendet. [erfüllt] - Eine Ein-Fehlertoleranz und angemessene Fehlererkennung sind gegeben. [erfüllt] - MTTFD ist mindestens Niedrig oder Mittel oder Hoch. [erfüllt] - DCavg ist mindestens Niedrig oder Mittel. [erfüllt] - Der erreichte Punktestand der CCF-Bewertung beträgt mindestens 65. [erfüllt]
Dokumentation:	
Quelle (z.B. Norm) Kategorie:	
Datei:	

MTTFD und Gebrauchsdauer Subsystem

MTTFD [a]:	86,3 (Hoch)
Gebrauchsdauer [a]: 20	Kleinste Gebrauchsdauer [a]: 20

Diagnosedeckungsgrad Subsystem

DCavg [%]:	99 (Hoch)

SISTEMA - Sicherheit von Steuerungen an Maschinen

Projektname: **Masterarbeit - STEP**

Dateidatum: 28.01.2018 10:37:49 Reportdatum: 28.01.2018 Prüfsumme: deede0e33e596d4803c9de10adaa75bb

SF **Sicherheitsfunktion: Neigungsgrenzen (optimiert)**

Fehler gemeinsamer Ursache Subsystem

CCF-Punkte:	80 (erfüllt)
CCF-Maßnahmen:	- Trennung / Abtrennung (15 Punkte) Physikalische Trennung zwischen den Signalpfaden, Trennung der Verdrahtung / Verrohrung, ausreichende Luft- und Kriechstrecken auf gedruckten Schaltungen. - Entwurf / Anwendung / Erfahrung (15 Punkte) Schutz gegen Überspannung, Überdruck, Überstrom, usw. - Entwurf / Anwendung / Erfahrung (5 Punkte) Verwendung bewährter Bauteile - Beurteilung / Analyse (5 Punkte) Sind die Ergebnisse einer Ausfallart und Effektanalyse berücksichtigt worden, um Ausfälle infolge gemeinsamer Ursache in der Entwicklung zu vermeiden? - Kompetenz / Ausbildung (5 Punkte) Sind Konstrukteure / Monteure geschult worden, um die Gründe und Auswirkungen von Ausfällen infolge gemeinsamer Ursache zu erkennen? - Umgebung (25 Punkte) Schutz vor Verunreinigung und elektromagnetischer Beeinflussung (EMC) gegen CCF in Übereinstimmung mit den angemessenen Normen. Fluidische Systeme: Filtrierung des Druckmediums, Verhinderung von Schmutzeintrag, Entwässerung von Druckluft, z. B. in Übereinstimmung mit den Anforderungen des Herstellers für die Reinheit des Druckmediums, Elektrische Systeme: Wurde das System hinsichtlich elektromagnetischer Immunität geprüft, z. B. wie in zutreffenden Normen gegen CCF festgelegt. Bei kombinierten fluidischen und elektrischen Systemen sollten beide Aspekte berücksichtigt werden. - Umgebung (10 Punkte) Andere Einflüsse. Wurden alle Anforderungen hinsichtlich Unempfindlichkeit gegenüber allen relevanten Umgebungsbedingungen wie Temperatur, Schock, Vibration, Feuchte (z. B. wie in den zutreffenden Normen festgelegt) berücksichtigt?
Dokumentation:	
Dokument:	

Status / Meldungen Subsystem

Status:	grün

Kanäle / Testkanal (1 / 2)

CH Name: Kanal 1

MTTFD [a]: 86,3

Blöcke (1 / 2)

BL Name: Neigungssensor

SISTEMA - Sicherheit von Steuerungen an Maschinen

Projektname: **Masterarbeit - STEP**

Dateidatum: 28.01.2018 10:37:49 Reportdatum: 28.01.2018 Prüfsumme: deede0e33e596d4803c9de10adaa75bb

SF Sicherheitsfunktion: Neigungsgrenzen (optimiert)

Betriebsmittelkennzeichen: F1		Inventarnummer:

Gerätedetails Block

Gerätehersteller:	Turck	
Geräteidentifikator:		
Gerätegruppe:		
Artikelnummer: B2N10H-Q20L60-2LI2-H1151		Revisionsnummer:
Funktion:	☑ Eingabe ☐ Ausgabe	☐ Logik ☐ unbekannt
Technologie:	elektronisch	
Kategorie:	1	
Anwendungsfall:		
Beschreibung des Anwendungsfalls:		

Dokumentation Block

Dokumentation:	
Dokument:	

MTTFD und Gebrauchsdauer Block

MTTFD [a]: 203 (Hoch)		
Gebrauchsdauer [a]: 20		Kleinste Gebrauchsdauer [a]: 20
Rate gefahrbringender Ausfälle [FIT]: 562,3		
Dokumentation:		

Diagnosedeckungsgrad Block

DC [%]: 99 (Hoch)	
Maßnahme:	Kreuzvergleich von Eingangssignalen mit unmittelbarem und Zwischenergebnissen in der Logik (L) und zeitlich und logische Programmlaufüberwachung und Erkennung statischer Ausfälle und Kurzschlüsse (bei Mehrfach-Ein-/Eingängen) (Eingabeeinheit) (99 %)
Dokumentation:	

Status / Meldungen Block

Status:	grün

Blöcke (2 / 2)

BL Name: Hauptfreigabeventil

Betriebsmittelkennzeichen: IV3		Inventarnummer:

Gerätedetails Block

Gerätehersteller:	Danfoss

SISTEMA - Sicherheit von Steuerungen an Maschinen

Projektname: **Masterarbeit - STEP**

Dateidatum: 28.01.2018 10:37:49 Reportdatum: 28.01.2018 Prüfsumme: deede0e33e596d4803c9de10adaa75bb

SF **Sicherheitsfunktion: Neigungsgrenzen (optimiert)**

Geräteidentifikator:		
Gerätegruppe:		
Artikelnummer: PVG32	Revisionsnummer:	
Funktion:	☐ Eingabe ☑ Ausgabe	☐ Logik ☐ unbekannt
Technologie:	hydraulisch	
Kategorie:	-	
Anwendungsfall:		
Beschreibung des Anwendungsfalls:		

Dokumentation Block

Dokumentation:	
Dokument:	

MTTFD und Gebrauchsdauer Block

MTTFD [a]: 150 (Hoch)	
Gebrauchsdauer [a]: 20	Kleinste Gebrauchsdauer [a]: 20
Rate gefahrbringender Ausfälle [FIT]: 761	
Dokumentation:	

Diagnosedeckungsgrad Block

DC [%]: 99 (Hoch)	
Maßnahme:	Direkte Überwachung (z. B. elektrische Überwachung der Steuerungsventile, Überwachung elektromechanischer Einheiten durch Zwangsführung) (Ausgabeeinheit) (99 %)
Dokumentation:	

Status / Meldungen Block

Status:	grün

Kanäle / Testkanal (2 / 2)

CH Name: Kanal 2

MTTFD [a]: 86,3

Blöcke (1 / 2)

BL Name: Neigungssensor

Betriebsmittelkennzeichen: F2	Inventarnummer:

Gerätedetails Block

Gerätehersteller:	Kübler

SISTEMA - Sicherheit von Steuerungen an Maschinen

Projektname: **Masterarbeit - STEP**

Dateidatum: 28.01.2018 10:37:49 Reportdatum: 28.01.2018 Prüfsumme: deede0e33e596d4803c9de10adaa75bb

SF **Sicherheitsfunktion: Neigungsgrenzen (optimiert)**

Geräteidentifikator:		
Gerätegruppe:		
Artikelnummer: 8.IS40.21121	Revisionsnummer:	
Funktion:	☑ Eingabe ☐ Ausgabe	☐ Logik ☐ unbekannt
Technologie:	elektronisch	
Kategorie:	1	
Anwendungsfall:		
Beschreibung des Anwendungsfalls:		

Dokumentation Block

Dokumentation:	
Dokument:	

MTTFD und Gebrauchsdauer Block

MTTFD [a]: 203 (Hoch)	
Gebrauchsdauer [a]: 20	Kleinste Gebrauchsdauer [a]: 20
Rate gefahrbringender Ausfälle [FIT]: 562,3	
Dokumentation:	

Diagnosedeckungsgrad Block

DC [%]: 99 (Hoch)	
Maßnahme:	Kreuzvergleich von Eingangssignalen mit unmittelbarem und Zwischenergebnissen in der Logik (L) und zeitlich und logische Programmlaufüberwachung und Erkennung statischer Ausfälle und Kurzschlüsse (bei Mehrfach-Ein-/Eingängen) (Eingabeeinheit) (99 %)
Dokumentation:	

Status / Meldungen Block

Status:	grün

Blöcke (2 / 2)

BL Name: Hauptfreigabeventil

Betriebsmittelkennzeichen: IV4	Inventarnummer:

Gerätedetails Block

Gerätehersteller:	Danfoss
Geräteidentifikator:	
Gerätegruppe:	
Artikelnummer: PVG32	Revisionsnummer:

SISTEMA - Sicherheit von Steuerungen an Maschinen

Projektname: **Masterarbeit - STEP**

Dateidatum: 28.01.2018 10:37:49 Reportdatum: 28.01.2018 Prüfsumme: deede0e33e596d4803c9de10adaa75bb

SF Sicherheitsfunktion: Neigungsgrenzen (optimiert)

Funktion:	☐ Eingabe ☑ Ausgabe	☐ Logik ☐ unbekannt
Technologie:	unbekannt	
Kategorie:	-	
Anwendungsfall:		
Beschreibung des Anwendungsfalls:		

Dokumentation Block

Dokumentation:	
Dokument:	

MTTFD und Gebrauchsdauer Block

MTTFD [a]: 150 (Hoch)	
Gebrauchsdauer [a]: 20	Kleinste Gebrauchsdauer [a]: 20
Rate gefahrbringender Ausfälle [FIT]: 761	
Dokumentation:	

Diagnosedeckungsgrad Block

DC [%]: 99 (Hoch)	
Maßnahme:	Direkte Überwachung (z. B. elektrische Überwachung der Steuerungsventile, Überwachung elektromechanischer Einheiten durch Zwangsführung) (Ausgabeeinheit) (99 %)
Dokumentation:	

Status / Meldungen Block

Status:	grün

SISTEMA - Sicherheit von Steuerungen an Maschinen

IFA
Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung

Projektname: **Masterarbeit - STEP**

Dateidatum: 28.01.2018 10:37:49 Reportdatum: 28.01.2018 Prüfsumme: deede0e33e596d4803c9de10adaa75bb

HAFTUNGSAUSSCHLUSS

Die Software wurde gemäß dem Stand von Wissenschaft und Technik sorgfältig erstellt. Sie wird dem Nutzer unentgeltlich zur Verfügung gestellt.

Die Haftung des IFAs/ DGUV ist damit auf Vorsatz und grobe Fahrlässigkeit (§ 521 BGB) bzw. bei Sach- und Rechtsmängel auf arglistig verschwiegene Fehler beschränkt (523, 524 BGB).

Das IFA ist bemüht, seine Homepage virenfrei zu halten, gleichwohl kann keine Virenfreiheit der zur Verfügung gestellten Software und Informationen zugesichert werden. Nutzerinnen und Nutzern wird daher empfohlen, vor dem Herunterladen von Software, Dokumentationen oder Informationen selbst für angemessene Sicherheitsvorkehrungen und Virenscanner zu sorgen.

KONTAKT

Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA)
Fachbereich 5: Unfallverhütung - Produktsicherheit
Alte Heerstr. 111, 53757 Sankt Augustin
E-Mail: sistema@dguv.de
www.dguv.de/ifa (Webcode: d561582)

Datum, Unterschrift Autor

Datum, Unterschrift Prüfer