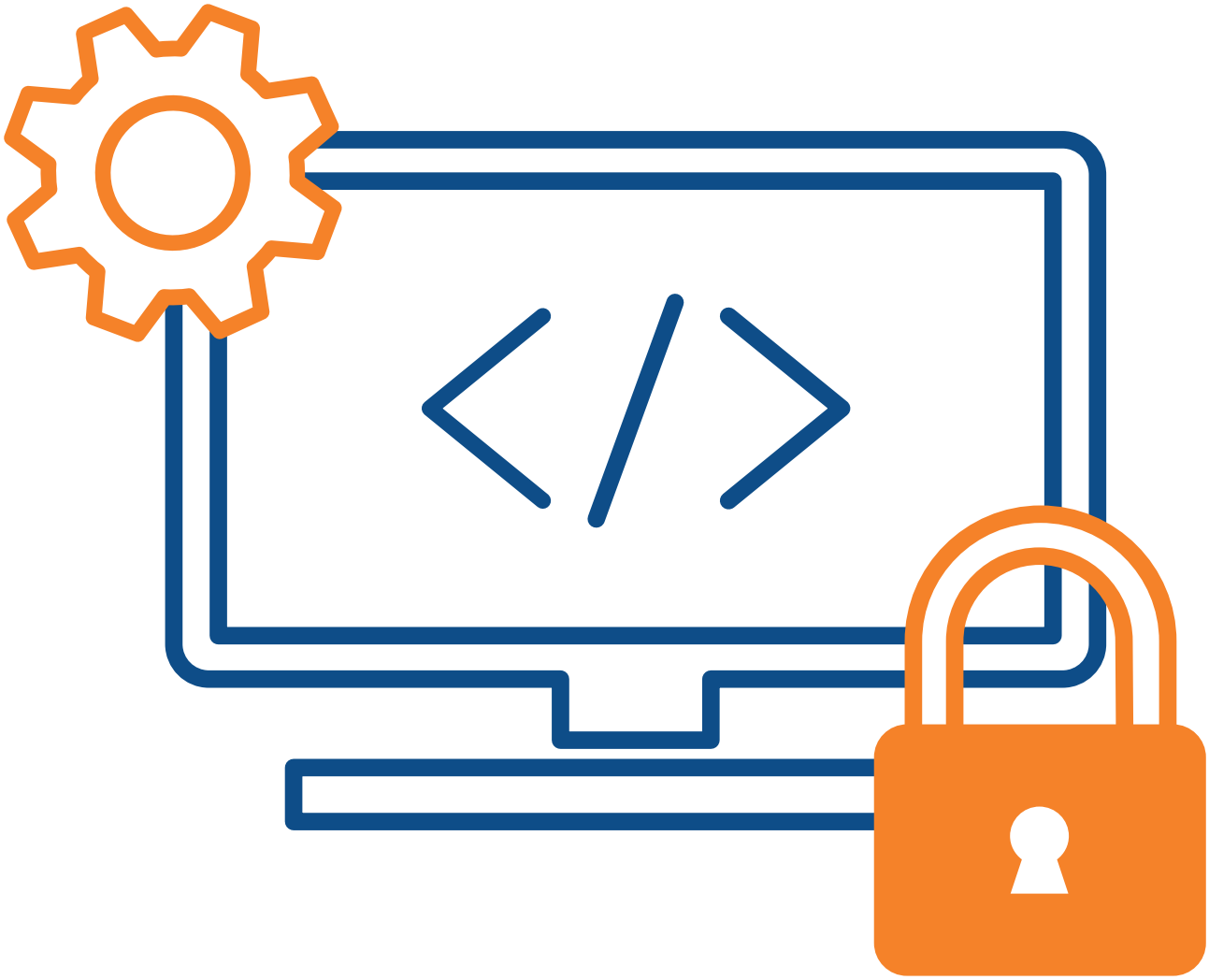
Sichere Software in der Maschinenverordnung EU 2023/1230

Frankfurt am Main, Oktober 2024



Verband der Elektro- und Digitalindustrie

zvei
electrifying ideas

Inhaltsverzeichnis

1. Einleitung 3
2. Software in der sicherheitsbezogenen Automation 6
3. Begriffe 7
4. Abkürzungen 10
5. Grundlagen 11
6. Funktionalitäten der Sicherheits-Teilfunktionen 15
7. Wer erstellt Software und wie ist Software rechtlich einzuordnen? 29
8. Software in der Maschinenrichtlinie und der Maschinenverordnung 30
9. Zusammenfassung und Ausblick 39
10. Anhang 40
11. Autorinnen und Autoren 46

Abbildungsverzeichnis

Abbildung 1 – Das Schichtenmodell 11
Abbildung 2 – Beispiel für die Realisierung eines schwarzen Kanals 14
Abbildung 3 – Risikominderung 15
Abbildung 4 – Funktionalität und Konfigurierbarkeit 16
Abbildung 5 – Diskret aufgebaute Sicherheitsschaltung 17
Abbildung 6 – Sicherheitsschaltgerät 18
Abbildung 7 – Frequenzumrichter mit STO 18
Abbildung 8 – FU mit Eingängen 19
Abbildung 9 – FU mit Wahlschalter 19
Abbildung 10 – Schaltgerät mit Display 20
Abbildung 11 – Parametrierung Sicherheitslaserscanner 21
Abbildung 12 – Verteiltes System – Logische Darstellung 22
Abbildung 13 – Verteiltes System – Physikalische Darstellung 22
Abbildung 14 – Struktur – Logik–Typ 4 – Variante 1 23
Abbildung 15 – Physikalische Darstellung Logik–Typ 4 – Variante 1 23
Abbildung 16 – Struktur – Logik–Typ 4 – Variante 2 24
Abbildung 17 – Physikalische Darstellung Logik–Typ 4 – Variante 2 24
Abbildung 18 – Struktur – Logik–Typ 4 – Variante 3 25
Abbildung 19 – Struktur – Logik–Typ 4 – Variante 4 26
Abbildung 20 – Beziehung zwischen Lieferant und Anwender 32

Tabellenverzeichnis

Tabelle 1 – Verantwortung für die Konformitätsbewertung 33
Tabelle 2 – Verantwortung für die Konformitätsbewertung 38
Tabelle 3 – Verantwortung für die Konformitätsbewertung 39

1. Einleitung

1.1 Motivation

Die Maschinenrichtlinie (MRL) ist eine der wichtigsten Rechtsvorschriften zur Harmonisierung der grundlegenden Sicherheitsanforderungen für Maschinen im europäischen Wirtschaftsraum. Sie beschreibt einheitliche Anforderungen an die Sicherheit und den Gesundheitsschutz bei der Interaktion von Mensch und Maschine. Die Richtlinie fördert den freien Warenverkehr von Maschinen im Binnenmarkt und garantiert ein hohes Schutzniveau für Arbeitnehmer und Bürger der EU.

Der offizielle Titel der Maschinenrichtlinie lautet: Richtlinie 2006/42/EG des Europäischen Parlaments und des Rates vom 17. Mai 2006 über Maschinen und zur Änderung der Richtlinie 95/16/EG (Neufassung). Sie gilt seit dem 29.12.2009. Unabhängig von Herstellungsort und -datum unterliegen alle Maschinen, die erstmals ab dem 01.01.1995 im europäischen Wirtschaftsraum eingesetzt werden, der EU-Maschinenrichtlinie und müssen somit konformitätsbewertet sein.

Die EU-Kommission hat die Maschinenrichtlinie zur Maschinenverordnung (MVO) weiterentwickelt, um den erweiterten technologischen Entwicklungen Rechnung zu tragen. Unter anderem werden Anforderungen hinsichtlich des Schutzes gegen Beeinflussung (Protection against Corruption) definiert und Aspekte aus der Anwendung künstlicher Intelligenz (maschinelles Lernen) berücksichtigt.

Offizieller Titel der Maschinenverordnung: Verordnung (EU) 2023/1230 des Europäischen Parlaments und des Rates über Maschinen. Sie ist ab dem 20. 01. 2027 für das Inverkehrbringen von Maschinen anzuwenden. Dieser Termin und weitere Termine sind der Berichtigung der Verordnung (EU) 2023/1230 vom 04.07.2023 zu entnehmen.

Die Maschinenverordnung hat die Bewertung von Software weiter fokussiert. Besonders von Bedeutung: Die Begriffsbestimmung der Sicherheitsbauteile erfasst jetzt neben Bauteilen physischer Art oder digitaler und/oder gemischter Art, auch die Software. Der Begriff „Software“ wird in der Maschinenverordnung 24-mal verwendet.

Der Begriff Software ist weder in der Maschinenverordnung noch im Normenkontext eineindeutig definiert.

Die „Nicht erschöpfende Liste der Sicherheitsbauteile“ im ANHANG II führt unter Punkt 18: „Software, die Sicherheitsfunktionen wahrnimmt“ auf. Software als Sicherheitsbauteil impliziert bestimmte Vorgehensweisen mit Rechten und Pflichten, deren Kenntnis für den Bereich Software häufig neu und von weitreichender Bedeutung ist.

Der Schlüssel hierzu ist das Konformitätsbewertungsverfahren, in dem der Hersteller nachweist, dass er die in der Verordnung enthaltenen grundlegenden Sicherheitsanforderungen eingehalten hat.

Das Konformitätsbewertungsverfahren muss vom Hersteller für jedes Produkt vor dem erstmaligen Inverkehrbringen durchgeführt werden. Am Ende des Konformitätsbewertungsverfahrens stellt der Hersteller eine EU-Konformitätserklärung für sein Produkt aus, in der er bestätigt, dass das Produkt zu den Anforderungen der anzuwendenden Richtlinie(n) konform ist.

Die Vielzahl an „Aggregierungen“ von Software (von Runtime, Betriebssystem, Tool, über das Anwenderprogramm) sowie die möglichen Darreichungsformen (Bspw.: Selbst erstellt, Kauf, Miete, Leasing, Nutzung) bzw. die Vorgehensweisen im Laufe des Lebenszyklus einer Software, exemplarisch seien hier die Erstlieferung, Update und Upgrade hervorgehoben, zusammen mit den Rollen (Bspw.: Hersteller, Nutzer) ergeben ein eher unübersichtliches Terrain.

Ein Schlüssel hierbei ist: „In Verkehr bringen“. Wer hat dabei welche Rechte und auch Pflichten? Und wie sich hierbei sicher und rechtssicher verhalten?

Deshalb wurde die mit diesem Dokument vorliegende Empfehlung zum Thema im ZVEI Technischen Ausschuss Sicherheitssysteme in der Automation (TASi) erarbeitet. Als Schnelleinstieg sei hier auf die Tabelle 1 auf Seite 34 mit dem Titel „Verantwortung für die Konformitätsbewertung“ verwiesen. Sie ermöglicht eine entsprechend den Rollen kompakte Navigation.

Ihr Studium ist allen Verantwortlichen nahe zu legen, um ggf. ihre Prozesse und Vorgehensweisen entsprechend auszurichten bzw. zu überprüfen. Darüber hinaus gehende Handreichungen und Orientierung bieten dabei die am Dokument mitarbeitenden Firmen.

Ihr Feedback ist unbedingt erwünscht.

Gutes Gelingen

Für das ZVEI TASi AG Software Team

1.2 Software in der Maschinensicherheit

Software in sicherheitsbezogenen Applikationen ist schon über mehrere Jahrzehnte im Einsatz. Die Entwicklung und Nutzung der ersten speicherprogrammierbaren Steuerungen mit der Eignung für Maschinensicherheits-Applikationen liegt bereits in den 80er Jahren des vergangenen Jahrhunderts.

Die ersten normativen Grundlagen, die sich neben der Hardware auch mit den Anforderungen an Software beschäftigt haben, waren in den 80er- und 90er-Jahren des letzten Jahrhunderts die DIN V VDE 19250 „Messen, Steuern, Regeln; Grundlegende Sicherheitsbetrachtungen für MSR-Schutzeinrichtungen" und die DIN V VDE 0801 „Grundsätze für Rechner in Systemen mit Sicherheitsaufgaben".Beide entstanden also in einer Zeit, als der Einsatz von Mikrocontrollern und Software in Applikationen der Maschinensicherheit noch quasi „verboten" war. Basierend auf diesen Standards wurde international die Entwicklung der EN 61508 „Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme" vorangetrieben, die erstmals den Sicherheits-Lebenszyklus von solchen Systemen umfänglich beschreibt.

1.3 Aktuelle Normensituation

Grundlage für die Betrachtung von Software-Sicherheitsaspekten im Sinne dieses Dokuments sind die folgenden Normen. Die datierten Normenverweise befinden sich im Anhang in Kapitel 10.2:

- EN 61508, die aus insgesamt acht Teilen besteht:
  - Teil 0: Funktionale Sicherheit und die EN 61508
  - Teil 1: Allgemeine Anforderungen (EN 61508-1)
  - Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/ programmierbare elektronische Systeme (EN 61508-2)
  - Teil 3: Anforderungen an Software (EN 61508-3)
  - Teil 4: Begriffe und Abkürzungen (EN 61508-4)
  - Teil 5: Beispiele zur Ermittlung der Stufe der Sicherheitsintegrität (Safety Integrity Level) (EN 61508-5)
  - Teil 6: Anwendungsrichtlinie für EN 61508-2 und EN 61508-3 (EN 61508-6)
  - Teil 7: Anwendungshinweise über Verfahren und Maßnahmen (EN 61508-7)

  Relevant aus Sicht dieses Dokuments ist insbesondere der Teil 3 dieser Normenreihe.

- EN 62061 „Sicherheit von Maschinen – Funktionale Sicherheit sicherheits bezogener elektrischer, elektronischer und programmierbarer elektronischer Steuerungssysteme"

- EN ISO 13849-1 „Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen - Teil 1: Allgemeine Gestaltungsleitsätze"

Alle verfügbaren Normen decken bestimmte Themenbereiche ab, jedoch jeweils mit unterschiedlichem Schwerpunkt. Dies lässt eigentlich vermuten, dass alle Facetten beim Thema Software beleuchtet wurden. Die Praxis zeigt, dass sowohl Begriffe zum Thema Software nicht eindeutig definiert sind, als auch die Anforderungen an Software in Bezug auf europäische Richtlinien und Normen nicht immer klar sind.

Die Einhaltung des anzuwendenden Rechtsrahmens ist im europäischen Wirtschaftsraum verpflichtend. Dazu zählen relevante Europäische Richtlinien, Verordnungen und delegierte Rechtsakte. Für das jeweilige Produkt einschlägige, im Europäischen Amtsblatt gelistete harmonisierte Normen können, in Abhängigkeit des in der jeweiligen Verordnung vorgeschriebenen Konformitätsbewertungsmoduls, herangezogen werden, die jeweiligen technischen Anforderungen zu belegen. Unabhängig von der Normenlage empfiehlt es sich grundsätzlich, den aktuellen Stand der Wissenschaft und Technik bei der Entwicklung, Realisierung und Verifikation/Validierung berücksichtigen.

2. Software in der sicherheitsbezogenen Automation

Die Industrie erlebt einen stetigen Wandel, wobei gegenwärtig zwischen vier Phasen der industriellen Revolution unterschieden wird. Als industrielle Revolution werden tiefgreifende Veränderungen im technologischen Fortschritt bezeichnet, die Auswirkungen auf einzelne Menschen und ganze Gesellschaftsgruppen haben. Nach der Mechanisierung um 1800, der Massenproduktion durch Elektrizität um 1900 und der Automatisierung durch Computertechnologien in den 1970er Jahren befinden wir uns derzeit im digitalen Zeitalter. Die Politik kam auf die Idee, die vierte Revolution der industriellen Entwicklung in Kurzform Industrie 4.0 zu nennen.

Die dritte industrielle Revolution wird auch digitale Revolution genannt und begann in den 1970er Jahren. Die Digitaltechnik wurde das bevorzugte Mittel zur Automatisierung. Im Gegensatz zur vorherigen Reihenfertigung in den Fabriken, wurde menschliche Arbeit vermehrt von Maschinen übernommen. Neuerungen in der Elektronik, insbesondere die Entwicklung von Transistoren, führten zur drastischen Verkleinerung elektrischer Schaltungen. Mit den Abmessungen sank der Aufwand für die Anwendung von Schaltalgebra. Die Entwicklung von integrierten Schaltkreisen führte schließlich dazu, dass Geräte ohne großen Aufwand mit Logik ausgestattet werden konnten. Fortschrittliche Feldgeräte (Sensoren und Aktoren) kommunizieren mit der Steuerung bzw. Regelung und stellen eine gleichbleibende Qualität der Produkte auch bei Schwankungen im Prozess sicher.

Speicherprogrammierbare Steuerungen (SPS) haben die „festverdrahtete" verbindungsprogrammierten Steuerungen (VPS) zur Steuerung oder Regelung einer Maschine oder Anlage in den meisten Bereichen abgelöst. Eine SPS besteht in der Regel aus Eingängen, Ausgängen, einer Systemsoftware (ESW) und einer Schnittstelle über die ein Anwendungsprogramm (ASW) geladen werden kann. Das Anwendungsprogramm legt fest, wie die Ausgänge in Abhängigkeit von den Eingängen geschaltet werden.

Eine SPS kann in sehr verschiedener Weise realisiert sein, beispielsweise als Einzelgerät („Baugruppe"), als PC-Einsteckkarte oder als Softwareemulation auf einem PC. Durch das softwaregesteuerte Arbeitsprinzip kann eine sonst starre Hardware individuell arbeiten. Obwohl dem Begriff , Software' teilweise Attribute wie Flexibilität, Individualität, Leistungsfähigkeit etc. zugeschrieben werden, wird alles, was eine Steuerung , tatsächlich tut', nicht von der Software, sondern ausschließlich durch die Hardware ausgeführt. Software , beschreibt' lediglich, was getan werden soll und in welcher Form das geschieht.

„Software ist die Gesamtheit von Informationen, die man der Hardware hinzufügen muss, damit das so entstandene Computersystem für ein definiertes Aufgabenspektrum nutzbar wird. Software besteht aus Computerprogrammen in jeder Erscheinungsform. Das reicht vom Quelltext (der Programmniederschrift in einer Programmiersprache) bis zum Maschinencode, der in einem Computer gespeichert ist. Dabei sind Computerprogramme nicht nur als Beschreibungen der auszuführenden Funktionen zu verstehen. Erst in Einheit mit Vereinbarungen zur Nutzung und Wartung benötigten Dokumentationsinhalten ist Software komplett." [Rothhardt]

3. Begriffe

3.1 Betreiber

In diesem Dokument ist der Betreiber einer Maschine/Anlage eine natürliche oder juristische Person, die als Vertragspartei des Beschäftigungsverhältnisses mit dem Arbeitnehmer die Verantwortung für das Unternehmen bzw. den Betrieb trägt [Arbeitsschutzrahmenrichtlinie 89/391/EWG].

3.2 Funktionsbaustein (sicherheitsbezogen oder nicht sicherheitsbezogen)

Ein Funktionsbaustein (FB) ist eine funktionale Einheit eines Anwendungsprogramms. Ein Anwendungsprogramm kann einen oder mehrere Funktionsbausteine enthalten.

3.3 Funktionseinheit

Eine Funktionseinheit ist eine Einheit aus Hardware oder einer Kombination aus Hardware und Software. Sie ist geeignet, eine definierte Funktion auszuführen. [ISO/IEC 2382, 01-01-40 mod.]

Anmerkung: Funktionseinheiten können z. B. Logikeinheiten, Sensoren und Leistungsantriebe sein.

3.4 Hersteller

Ein Hersteller ist jede natürliche oder juristische Person, die ein Produkt herstellt bzw. entwickeln oder herstellen lässt und dieses Produkt unter ihrem eigenen Namen oder ihrer eigenen Marke entgeltlich oder unentgeltlich in Verkehr bringt [Leitfaden für die Umsetzung der Produktvorschriften der EU 2022 („Blue Guide")].

3.5 Konfiguration

In technischen Zusammenhängen bedeutet Konfiguration das Auswählen, Gruppieren, Zusammenfügen von Hardware- und/oder Softwarekomponenten zu einem System, das eine bestimmte Funktion realisieren soll. Siehe auch IEV 351-43-20: ein System oder Gerät unter Ausnutzung seiner vorhandenen Funktionsvielfalt für eine bestimmte Aufgabe einrichten.

3.6 Logik-Typ

Der Logik-Typ beschreibt eine standardisierte Struktur von sicherheitsbezogenen Funktionseinheiten zur Verknüpfung von Ein- und Ausgängen.

3.7 Parametrierung

Zuweisung von Werten zu Parametern, Realisierung aufgabenspezifischer Einstellwerte und Verhaltensoptionen bei Geräten, Anpassung von Software an spezielle Aufgabenstellungen über eine Schnittstelle.
Siehe auch IEV 351-43-21

3.8 Parametrisierung

Zuweisung von einstellbaren Attributen zu einem Objekt. Das Ergebnis einer Parametrisierung ist ein parametrisiertes Objekt mit einstellbaren Größen. Diesen Größen können dann im Rahmen einer Parametrierung konkrete Werte zugewiesen werden, z. B. um eine bestimmte funktionale Ausprägung des Objekts zu erhalten.

3.9 Programmierung (im allgemeinen Sinn)[1]

[1] Quelle: Wikipedia

Programmierung bezeichnet die Tätigkeit, Software zu erstellen. Programme werden mit Hilfe einer allgemeinen Programmiersprache (z. B. höhere Programmiersprachen wie C oder C++) formuliert („codiert"). Der Programmierer „übersetzt" dabei die vorgegebenen Anforderungen (z. B. im Pflichtenheft) und Algorithmen in die Programmiersprache.

Programmieren in erweitertem Sinn umfasst neben der Codeerstellung zahlreiche weitere Tätigkeiten, zum Beispiel das Testen (Unittest) des Programms oder das Erstellen der Dokumentation. Abgrenzen vom Begriff des Programmierens lassen sich andere Tätigkeiten zur Softwareentwicklung, wie beispielsweise zum Projektmanagement, zur Anforderungsanalyse oder zur Datenmodellierung.

Abhängig vom Typ und der Einsatzumgebung von Software (z. B. für Systemsoftware, Spielesoftware, Standardsoftware, Grafiksoftware. usw.) können zur Entwicklung unterschiedliche Verfahren und/oder Werkzeuge (wie Programmiersprachen, Testverfahren etc.) zum Einsatz kommen.

„Quellcode" bezeichnet die derzeit installierte Version der Software eines in den Anwendungsbereich dieser Verordnung fallenden Produkts, die in einer Programmiersprache so geschrieben ist, dass sie für den Menschen eindeutig und verständlich ist.

3.10 Sicherheitsfunktion (SF)

Definition der Sicherheitsfunktion in der Maschinenverordnung:

„Sicherheitsfunktion" bezeichnet eine Funktion, die als Schutzmaßnahme zur Beseitigung oder, falls dies nicht möglich ist, zur Reduzierung eines Risikos fungiert, wobei ein Ausfall dieser Funktion zu einer Erhöhung dieses Risikos führen könnte.

Definition der Sicherheitsfunktion in der EN ISO 12100:

Funktion einer Maschine, wobei ein Ausfall dieser Funktion zur unmittelbaren Erhöhung des Risikos (der Risiken) führen kann

In diesem Dokument:

Eine Sicherheitsfunktion reduziert ein vorhandenes Risiko einer Maschinenfunktion auf ein akzeptiertes Maß (siehe EN ISO 12100).

Eine Sicherheitsfunktion beginnt üblicherweise mit der Erkennung und Bewertung eines „einleitenden Ereignisses" durch z. B. einen Sensor und endet mit einer Aktivität, die zu einer Reaktion eines leistungssteuernden Elements (z. B. Schütz) führt.

3.11 Sicherheits-Teilfunktion (SSF) (engl: Safety Sub Function)

Eine Sicherheits-Teilfunktion ist ein Teil einer Sicherheitsfunktion, deren Versagen zu einem Ausfall der Sicherheitsfunktion führen kann.

3.12 Software

Software (SW) ist ein geistiges Produkt, das aus Programmen, Verfahren, Daten, Regeln und allen dazugehörigen Beschreibungen besteht, die zur Arbeit mit einem Datenverarbeitungssystem gehören.

Software ist sicherheitsbezogen, wenn sie angewendet wird, um sicherheitsbezogene Funktionen in Funktionseinheiten bereitzustellen. Software (SW) kann in jeder Funktionseinheit enthalten sein.

Software ist unabhängig vom Medium, auf dem sie gespeichert ist.

3.13 Softwarearten

3.13.1 Anwendungsprogramm (ASW) (engl.: Application Software)

Programm für eine bestimmte Benutzer-Anwendung. Im Allgemeinen enthält sie Ablaufketten, Bedingungen, Grenzwerte und Ausdrücke, die die entsprechenden Eingänge, Ausgänge, Berechnungen und Entscheidungen beeinflussen, um die Anforderungen der Sicherheitsfunktionen zu befriedigen

3.13.2 Systemsoftware (ESW) (eng.: Embedded Software)

Systemprogramme werden als Bestandteil des Systems mitgeliefert und sind nicht dafür vorgesehen, durch den Anwender eines Gerätes verändert zu werden. Systemprogramme werden auch als Embedded-Software oder Firmware bezeichnet.

Die Hardware-Abstraktions-Schicht (HAL) zählt ebenfalls zu den Systemprogrammen. Sie umfasst insbesondere Treiber, die den direkten Zugriff auf die Hardware des Systems realisieren und stellt einheitliche Schnittstellen zur Verfügung.

3.13.3 Hilfsprogramme

Dies sind Software-Werkzeuge, die beispielsweise für die Erstellung, Pflege und Dokumentation von Software verwendet werden. Die Hilfsprogramme sind für den Betrieb des Systems nicht erforderlich und dürfen das sicherheitsbezogene System zur Laufzeit nicht beeinflussen.

4. Abkürzungen

Abkürzung	Beschreibung
E/E/PE	**electrical/electronic/programmable electronic** Geräte oder Systeme, basierend auf elektrischer (E) und/oder elektronischer (E) und/oder programmierbarer elektronischer (PE) Technologie
FSCP	**Functional Safety Communication Profile** Funktional sicheres Kommunikationsprofil
FU	**Frequenzumrichter** Stromrichter, der aus der speisenden Wechselspannung eine andere Wechselspannung erzeugt. Im Dokument verwendet für PDS.
NLF	**New Legislative Framework** Neues Konzept, das als Basis und Rahmen für die Erstellung europäischer Richtlinien und Verordnungen dient.
PDS(SR)	**Power Drive Systems (Safety Related)** Elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl, die Sicherheits-Teilfunktionen zur Verfügung stellen.
ProdSV	**Produkt-Sicherheitsverordnung** Umsetzung der Anforderungen aus dem Produkt-Sicherheitsgesetz durch eine Verordnung.
SF	**Safety Function** Funktion einer Maschine, wobei ein Ausfall der Funktion zur unmittelbaren Erhöhung des Risikos führen kann.
SLS	**Safely limited Speed** Der Antrieb überwacht, dass eine Maximalgeschwindigkeit nicht überschritten wird.
SRP/CS	**Safety-Related Part of a Control System** Sicherheitsbezogener Teil einer Steuerung
SSF	**Safety Subfunction** Teilfunktion einer Sicherheitsfunktion
SS1	**Safe Stop 1** Der Antrieb wird geregelt zum Stillstand gebracht, anschließend wird die Sicherheitsfunktion STO aktiviert.
STO	**Safe Torque Off** Sicher abgeschaltetes Drehmoment

5. Grundlagen

5.1 Software ist nicht gleich Software - Das Schichtenmodell

Mit dem Schichtenmodell wurde eine Softwarearchitektur eingeführt, die eine hardwareunabhängige Softwareentwicklung ermöglicht. Dadurch wird die Wiederverwendung von Software erleichtert, was z. B. auch durch EN 61508 („Verwendung bewährter/verifizierter Softwareelemente“) favorisiert wird.

Jede Plattform bzw. Funktionseinheit besteht meist[2] aus verschiedenen Schichten bzw. Softwareteilen. Die folgende Abbildung zeigt ein typisches SW-Schichtenmodell und die zugehörigen vertikalen und horizontalen Abhängigkeiten einer Plattform. Eine Plattform besteht typischerweise aus den folgenden Schichten:

[2] Diese Darstellung bezieht sich auf komplexe Software. Bei sehr einfach strukturierten Systemen können auf Grund dieser Einfachheit einzelne Schichten entfallen.

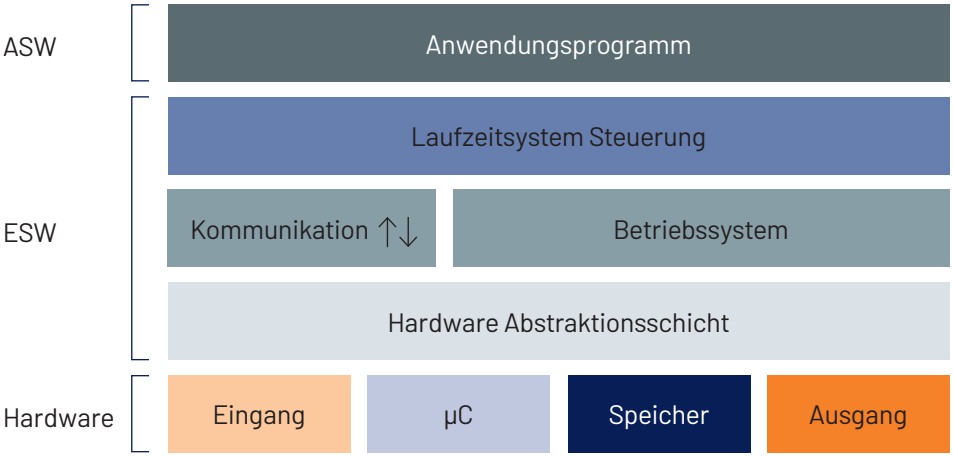


Abbildung 1 – Das Schichtenmodell

Beschreibung der Schichten:

- Hardware:

  Elektrisch/elektronisch/programmierbare elektronische Hardware (E/E/PE HW),
  Beispiele hierfür sind Sensoren, Teile der Logik (Steuerung), Aktoren oder andere Funktionseinheiten.

- Systemsoftware (ESW):

  - Laufzeitsystem Steuerung (Programmflusskontrolle)
  - Betriebssystem
  - Kommunikation (stellt Services zu anderen E/E/PE bereit)
  - Hardware-Abstraktionsschicht (beinhaltet standardisierte Schnittstellen zum Betriebssystem und der Peripherie)

- Anwendungsprogramm (ASW):

  Das Anwendungsprogramm besteht aus
  - Konfiguration von parametrierbaren Funktionseinheiten
  - einem oder mehreren verknüpften Funktionsbausteinen (FBs), die die Funktionalität realisieren, oder
  - einer frei programmierten Logik, die in einer Programmiersprache mit eingeschränktem oder vollem Sprachumfang erstellt wurde.

Die gesamte Software (ASW und ESW) besteht in der Regel aus mehreren Teilen. Diese können zugekauft, selbstentwickelt oder wiederverwendet werden und sich je nach Plattform unterschiedlich verhalten (z. B. Timings, Priorisierung, etc.). Deswegen ist die Integration und Bewertung der Software in die Hardwareplattform ein entscheidender Bestandteil des Software-Lebenszyklus.

Bei der klassischen Softwareentwicklung wurde eine Software (SW) immer speziell für eine bestimmte Hardware bzw. Aufgabe entwickelt. Durch den heutigen
Systemansatz und die Einführung innovativer neuer Technologien/Produkte (z. B. KI, Internet der Dinge, I4.0) ist das nicht mehr ausreichend, weil Software zunehmend abstrakt und plattformunabhängig entwickelt wird.

Bei Verwendung einer Plattform kann eine Sicherheitsfunktion in mehrere SSF aufgeteilt sein. Somit ist für die Bewertung des gesamten Systems die E/E/PE-Hardware und die gesamte Software (Systemsoftware, Anwendungsprogramm und Hilfsprogramme) zu betrachten, um belastbare und zuverlässige Ergebnisse zu erhalten. In der Sicherheitstechnik bedeutet das, dass einzelne Funktionseinheiten (z. B. Sicherheitslaserscanner oder sicherheitsbezogene Steuerungen) nur Sicherheits-Teilfunktionen ausführen. Erst das Gesamtsystem führt Sicherheitsfunktionen aus.

Beispiel:

Ein FB soll für verschiedene Steuerungen einsetzbar sein. Aufgrund des unterschiedlichen Verhaltens der jeweiligen Plattform muss zuerst geprüft werden, ob der FB für den Einsatz auf dieser Plattform geeignet ist. Der Grund hierfür ist, dass das Ausführen des FBs auf einer nicht geeigneten Plattform zum Versagen der Sicherheitsfunktion führen kann. Solche Ausfälle können entstehen, wenn Reaktionszeiten nicht eingehalten werden oder z. B. die Struktur der Hardware nicht für den erforderlichen Performance Level (PL) oder Safety Integrity Level (SIL) entwickelt wurde.

Fazit:

Ob die Funktionseinheit (Sensor, Steuerung, etc.) für ein sicherheitsbezogenes E/E/PE-System eingesetzt werden kann oder nicht, hängt von der systematischen Eignung der Plattform ab. Deswegen haben die Verifizierung und Validierung der sicherheitsbezogenen Eigenschaften und die Konformitätsbewertung des Produkts eine entscheidende Bedeutung.

5.2 Sicherheitsaspekte

Wie das Schichtenmodell darstellt, benötigt jede Plattform auch eine Hardware als Basis. Deswegen unterscheidet man grundsätzlich zwischen generellen Hardware-Anforderungen aus Normen zur Funktionalen Sicherheit (z. B. EN 61508), spezifischen Hardware-Anforderungen aus Sicht der Software und Anforderungen an die Software selbst. Die Anwendung von Normen ist generell rechtlich nicht bindend aber in der Betrachtung der Zusammenhänge in den Systemen äußerst hilfreich. Die weiteren Aussagen im Dokument basieren auf Anforderungen und Beschreibungen aus einzelnen internationalen Normen.

5.2.1 Generelle Anforderungen an sicherheitsbezogene Hardware

Grundsätzlich unterscheidet man zwischen zuvor bewerteter und nicht bewerteter sicherheitsbezogener Hardware (z. B. nach EN 61508).

Bewertete Hardware wurde basierend auf den Anforderungen aus einer relevanten Norm zur funktionalen Sicherheit bewertet bzw. qualifiziert und ist deshalb für ein bestimmtes Sicherheitslevel (PL oder SIL) geeignet. Bei nicht bewerteter sicherheitsbezogener Hardware muss der Integrator dafür sorgen, dass die systematische Sicherheitsintegrität der Hardware gegeben ist. Er muss Maßnahmen zur Beherrschung zufälliger Hardwarefehler treffen.

Die generellen Hardware-Anforderungen für die Ausführung einer Software sind wesentlich – aber nicht ausschließlich – von dem Diagnosedeckungsgrad (DC) und der Hardware-Fehlertoleranz (HFT) bzw. der Kategorie abhängig, die sich maßgeblich vom SIL/PL ableiten.

Mit einem höheren SIL bzw. PL steigen die Anforderungen an:

- den Diagnosedeckungsgrad und/oder
- die Anforderungen an die Struktur (z. B. Redundanz)
- Verifikation und Validierung

5.2.2 Anforderungen an die Hardware aus Sicht der Software

Ob die Software für die geplante Ausführung der Sicherheitsfunktion und für die ausgewählte Hardware wirklich geeignet ist, hängt neben der eigentlichen Funktionalität von der systematischen Eignung (en: systematic capability) der Software ab. Normativ werden je nach Sicherheitsniveau unterschiedliche Maßnahmen und Techniken für den Entwurf der Software empfohlen. Diese Maßnahmen haben einen entscheidenden Einfluss auf den SIL/PL des Gesamtsystems inclusive der Hardware, weil der zu erreichende SIL/PL durch die systematische Eignung der Software begrenzt ist.

Für die plattform- bzw. hardwareunabhängige Softwareentwicklung kann die EN 61508 angewendet werden. Das „Sicherheitshandbuch für konforme Objekte[3]“ dient als Grundlage für den Integrator und für die Beurteilung/Qualifikation der Hardware. Es enthält eine vollständige Beschreibung der Voraussetzungen, Funktionen und Einschränkungen.

[3] Wenn Elemente erworben und verwendet werden, deren Hersteller die Konformität zur IEC 61508 bestätigen, so muss der jeweilige Hersteller ein „Sicherheitshandbuch für konforme Objekte“ nach IEC 61508 Teil 2 Anhang D mitliefern.

Falls die Software SSFs verschiedener Sicherheits-Integritätslevel beinhaltet oder Teile nicht sicherheitsrelevanter Software, muss die Unabhängigkeit nachgewiesen werden.

5.2.3 Anforderungen an die Software

Die folgenden Quellen enthalten Hinweise zu allgemeinen Anforderungen an Software:

- für Embedded Software (ESW): EN 61508-3
- für die Programmierung von Embedded Software (ESW): IFA-Report 2020/1
- für das Anwendungsprogramm (ASW): EN ISO 13849-1 und EN 62061
- für die Nutzung modularer Software in verteilten Systemen: EN 61499
- für die Entwicklung von ASW (Matrixmethode): IFA-Report 2016/2

5.3 Anforderungen an die Kommunikation

Aktuelle sicherheitsbezogene Geräte und Systeme bieten vielfältige Kommunikationsschnittstellen. Alle sicheren Bussysteme, wie z. B. Profisafe, Safety over Ethercat oder AS-i Safety, ermöglichen die sichere Kommunikation zwischen den Busteilnehmern und/oder den Busteilnehmern mit der übergeordneten Steuerung. Für die Realisierung einer sicherheitsbezogenen Datenkommunikation gibt es grundsätzlich zwei mögliche Lösungsansätze:

- Der gesamte Kommunikationskanal (inklusive der benötigten Hardware) wird gemäß einem Regelwerk (Norm, Standard) zur funktionalen Sicherheit (z. B. EN 61508 und EN 61784-3) entworfen, implementiert und validiert. In diesem Fall spricht man von einem „weißen Kanal". Dies trifft beispielsweise auf proprietäre, also herstellerspezifische Kommunikationsschnittstellen zu. Beispiel hierfür ist die Kommunikation auf dem Rückwandbus einer sicherheitsbezogenen Steuerung.

- Teile des Kommunikationskanals sind nicht gemäß einem Regelwerk (Norm, Standard) zur funktionalen Sicherheit (z. B. EN 61508 und EN 61784-3) entworfen oder validiert. Dies ist ein sogenannter „schwarzer Kanal". Bei diesem Prinzip wird die Kommunikation über eine „sichere Schicht" (FSCP) realisiert, die auch bei der Qualifikation des sicherheitsrelevanten E/E/PE-Teilsystemen oder Elementen betrachtet wird. In diesem Fall müssen die Maßnahmen zur Beherrschung der Übertragungsfehler, um eine sicherheitsrelevante Übertragung zu realisieren, von der „sicheren Schicht" gewährleistet werden. Das Prinzip eines „schwarzen Kanals" ist in der Sicherheitstechnik weit verbreitet und wird auch für höhere SILs/PLs, wie z. B. bei Ethernet oder IO-Link Safety, verwendet. Das folgende Bild zeigt eine prinzipielle Darstellung, wie sich sowohl die Sicherheitsapplikation als auch die Standardapplikation den Kommunikationskanal teilen.

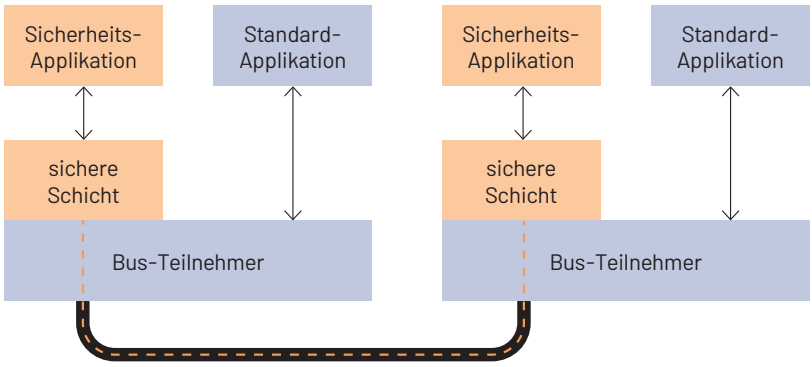


Abbildung 2 - Beispiel für die Realisierung eines schwarzen Kanals

5.4 Validierung

Zur Validierung der realisierten Sicherheitsfunktion(en) zählen die Aktivitäten, welche die vollständige Übereinstimmung mit den in der Sicherheitsanforderungsspezifikation festgelegten funktionalen Anforderungen nachweisen.

Zu diesen Aktivitäten gehören z. B.:

- die Prüfung, ob die spezifizierte Sicherheitsfunktion korrekt ausgeführt wird (Funktionstest, Black Box Test)
- der Nachweis, dass die vorgesehene Reaktionszeit erreicht wird (Leistungstest)
- die Prüfung der korrekten Reaktion auf fehlerhafte Eingangssignale oder inkorrekte Bedienereingaben (Fehlerinjektionstests)

Bei ESW wird die Validierung durch den Hersteller des sicherheitsbezogenen Geräts durchgeführt.

Die Validierung von ASW wird durch den Hersteller der Maschine unter realen Einsatzbedingungen durchgeführt.

Weiterführende Informationen zur Validierung von Software befinden sich im Literaturverzeichnis.

6. Funktionalitäten der Sicherheits-Teilfunktionen

6.1 Einleitende Bemerkungen

Technische Schutzmaßnahmen zur Risikominderung werden durch eine oder mehrere Sicherheitsfunktionen realisiert. Eine Sicherheitsfunktion setzt sich üblicherweise aus mehreren Sicherheits-Teilfunktionen zusammen.

Das erforderliche Niveau der Sicherheitsfunktionen (PL, SIL) ergibt sich aus dem jeweils zu erbringenden Beitrag zur Risikominderung.

Für die sichere Verwendung einer Funktionseinheit durch den Anwender muss deutlich erkennbar sein, welche Anforderungen der Hersteller der Funktionseinheit bereits erfüllt hat und welche noch vom Anwender zu erfüllen sind:

- Welche Funktionsbausteine sind (im Gerät) vorhanden und geprüft und welche müssen vom Anwender geprüft werden?
- Welche HW- und SW-Fehler werden vom Gerät erkannt und welche müssen erst durch ASW aufgedeckt werden?
- Welche Fehlerreaktionen erfolgen unmittelbar durch das Gerät selbst und welche Fehlerreaktionen müssen noch vom Anwender programmiert werden?

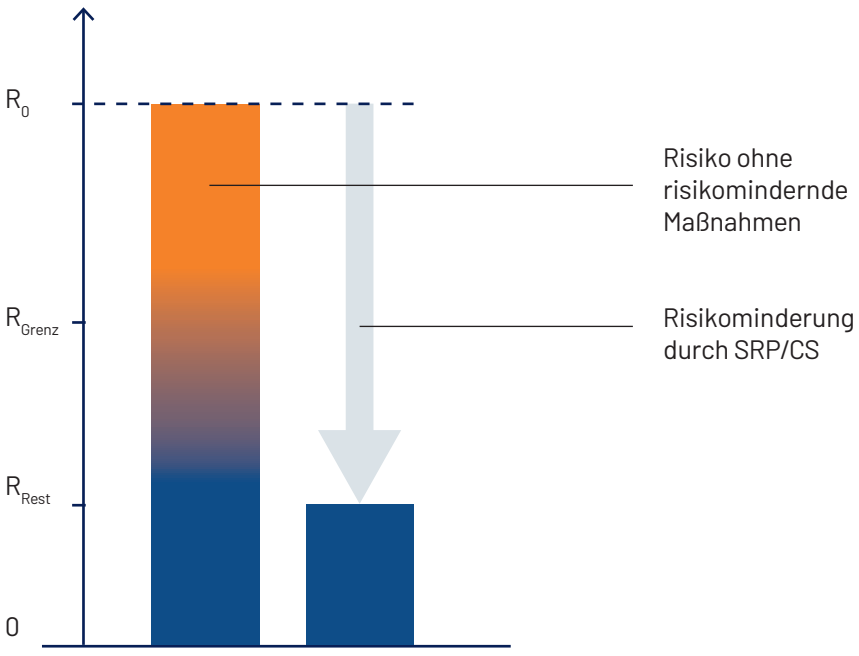


Abbildung 3 – Risikominderung

6.2 Eigenschaften von ASW

Der anwendungsspezifische Teil der Software (ASW) kann unter Verwendung einer Vielzahl von Programmierwerkzeugen und Programmiersprachen entwickelt werden. Diese Sprachen und Werkzeuge beeinflussen den Umfang der Funktionalität des Anwendungsprogramms, der in weiten Bereichen variieren kann.

		Funktionalität		
		fest vorgegeben	eingeschränkt	vollständig
Konfigurierbarkeit	vollständig	nicht zutreffend	nicht zutreffend	Programmierung (bei Logik-Typ 5)
	eingeschränkt	Parametrierung (bei Logik-Typ 3)	Konfiguration (bei Logik-Typ 4)	nicht zutreffend

Abbildung 4 – Funktionalität und Konfigurierbarkeit

- Parametrierung
  Das Softwarewerkzeug zur Parametrierung erlaubt es dem Anwender nicht, die Funktion des Systems zu ändern. Es ermöglicht die Auswahl von Eigenschaften aus einem vorgegebenen Vorrat von Funktionalitäten durch die Belegung von Parametern in vorgegebenen Wertebereichen.

  Softwarewerkzeuge zur Parametrierung können nach Norm klassifiziert sein (EN 61508-3). Es ist jedoch auch der Einsatz eines Standard-PCs oder eines Mobiltelefons zur Parametrierung, unter Verwendung zusätzlicher Maßnahmen, möglich.

- Konfiguration
  Softwarewerkzeuge für konfigurierbare Steuerungen haben häufig eine grafische Oberfläche. In einem grafischen Editor können Funktionsbausteine mit fest vorgegebenem Funktionsumfang platziert und untereinander bzw. mit Ein- und Ausgängen verbunden werden. Abschließend sind die Funktionsbausteine zu parametrieren.

  Softwarewerkzeuge zur Konfiguration können nach Norm klassifiziert sein (EN 61508-3). Es ist jedoch auch der Einsatz eines Standard-PCs oder eines mobilen Bediengerätes zur Konfiguration unter Verwendung zusätzlicher Maßnahmen, möglich.

- Programmierung
  Die freie Gestaltung des Anwendungsprogramms basiert auf allgemeinen Programmiersprachen. Typischerweise wird die Logik in Verbindung mit einem rechnergestützten System verwendet, ausgestattet mit einem Betriebssystem, das die Zuordnung der System-Ressourcen durchführt und eine echtzeitfähige Umgebung für einen Mehrprogrammbetrieb liefert.

  Softwarewerkzeuge zur Programmierung sind nach Norm klassifiziert (EN 61508-3).

6.3 Logik-Typen

Kennzeichnende Merkmale der hier beschriebenen Funktionalitäten von sicherheitsbezogenen Funktionseinheiten sind sogenannte Logik-Typen.

6.3.1 Logik-Typ „E“ – Sicherheits-Teilfunktion durch Verschaltung von Hardware

Der Anwender realisiert eine Sicherheits-Teilfunktion durch Verschaltung von Bauteilen, wie etwa drei Relais.

ESW	„Funktion der Relais“
Bemerkung	–
ASW	„Verschaltung aller Bauteile“
Verifikation ASW	Prüfen des Schaltplanes gegen die geplante SSF und der Schaltung gegen den Schaltplan.

Beispiel: diskret aufgebaute Sicherheitsschaltung

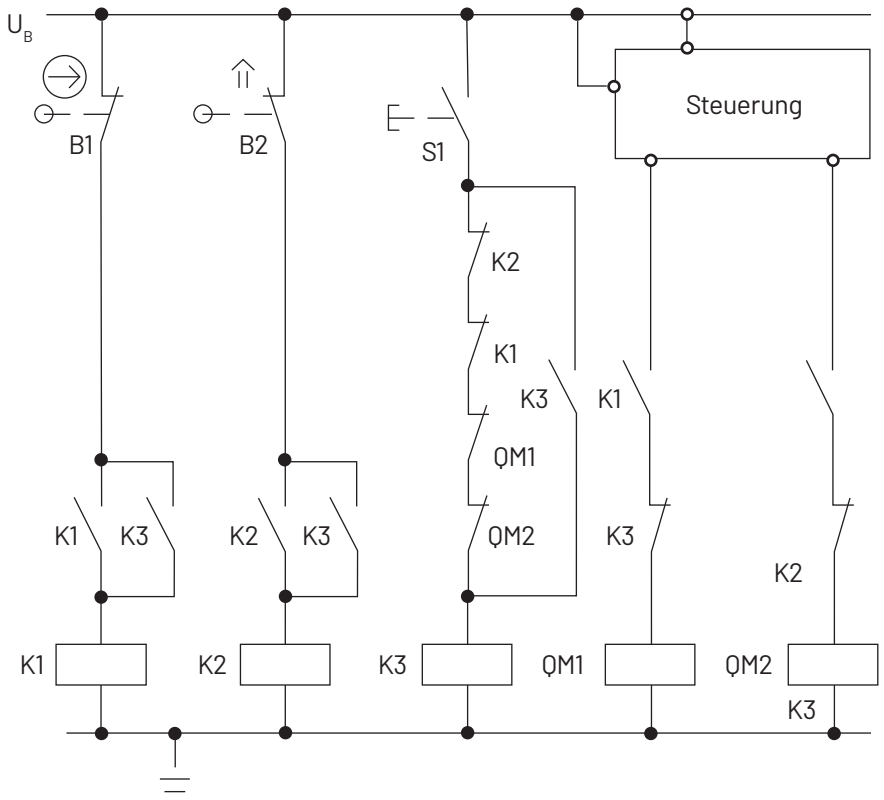


Abbildung 5 – Diskret aufgebaute Sicherheitsschaltung

6.3.2 Logik-Typ „1“ – Eine feste Sicherheits-Teilfunktion in Geräten

Sicherheitsschaltgerät, sicherheitsbezogener Sensor (z. B. Näherungsschalter, Sicherheitslichtvorhang) oder leistungssteuerndes Element (z. B. Frequenzumrichter (FU) mit STO); interner Aufbau fix, ohne Möglichkeiten zur Veränderung der SSF.

ESW	eine Sicherheitsteilfunktion (SSF)
Bemerkung	incl. Fehlererkennung und Fehlerreaktion
ASW	keine (die Verschaltung der Bauteile ist fix im Gerät)
Verifikation ASW	keine

Beispiel: Sicherheitsschaltgerät

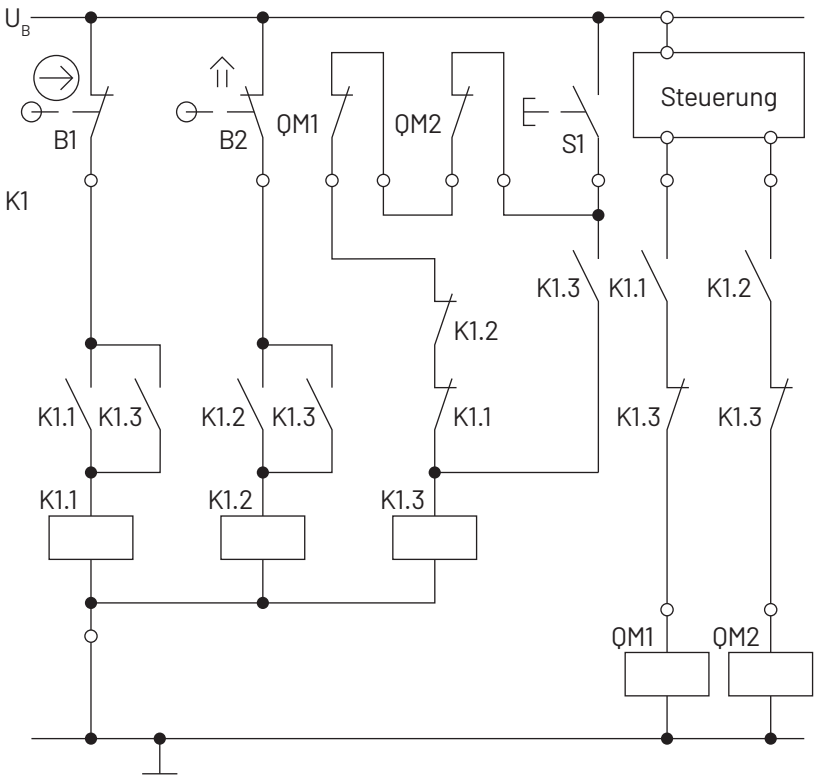


Abbildung 6 - Sicherheitsschaltgerät

Beispiel: Frequenzumrichter mit STO

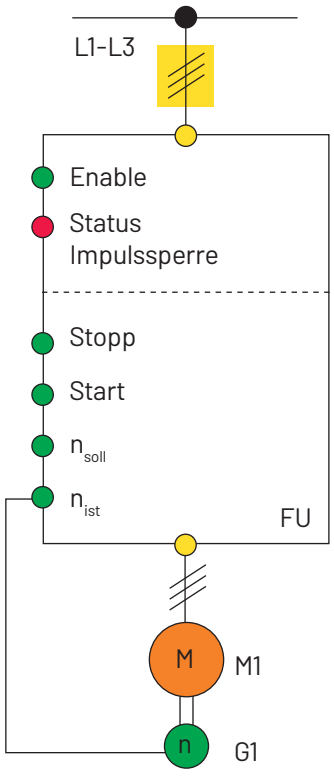


Abbildung 7 – Frequenzumrichter mit STO

6.3.3 Logik-Typ „2“ – Auswählbare Sicherheits-Teilfunktion(en) in Geräten

Funktionseinheit mit mehreren SSF, von denen eine durch Schalter vor der Inbetriebnahme ausgewählt werden muss oder die Auswahl mittels Codierung durch Verdrahtung erfolgt (z. B. SSF an Frequenzumrichtern (z. B. Binärcode an speziellen Eingängen zur Auswahl von STO, SS1 oder SLS)).

ESW	mehrere SSF
Bemerkung	incl. Fehlererkennung und Fehlerreaktion, auswählbar durch (elektrische) Signale
ASW	Auswahl der SSF, also die Schalterstellung oder die Binärcodierung an den Eingängen
Verifikation ASW	Prüfen der Auswahl gemäß der Betriebsanleitung

Beispiel: Frequenzumrichter mit Eingängen zur Auswahl der SSF

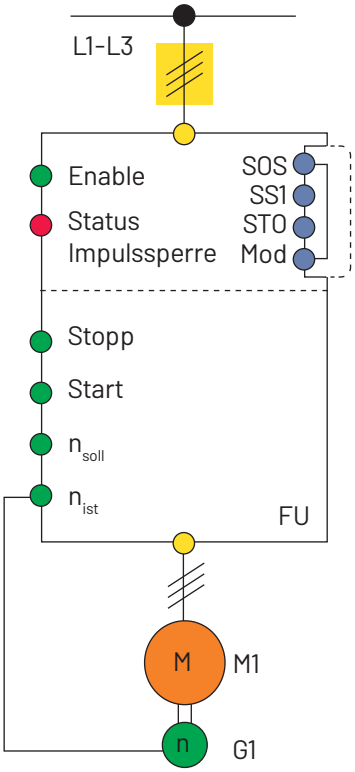


Abbildung 8 – FU mit Eingängen

Beispiel: Frequenzumrichter mit Wahlschalter zur Auswahl der SSF

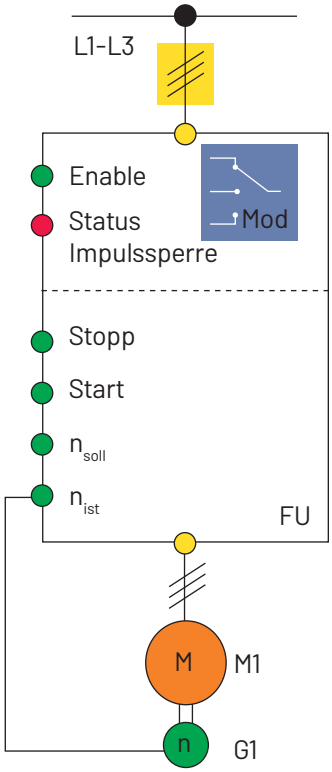


Abbildung 9 – FU mit Wahlschalter

6.3.4 Logik-Typ „3“ – Auswählbare/parametrierbare Sicherheits-Teilfunktion(en) in Geräten

Variante 1: Auswahl der Sicherheitsteilfunktion

Funktionseinheit mit mehreren SSF, von denen eine mittels (externem) „Programmiergerät“ vor der Inbetriebnahme ausgewählt und zum Schaltgerät übertragen werden muss.

ESW	mehrere SSF
Bemerkung	incl. Fehlererkennung und Fehlerreaktion, auswählbar durch (elektrische) Signale
ASW	Auswahl der SSF, also die Schalterstellung oder die Binärcodierung an den Eingängen
Verifikation ASW	Prüfen der Auswahl gemäß der Betriebsanleitung

Beispiel: Schaltgerät mit integriertem Display/Drehschalter z. B. für Verzögerungszeit, Schaltschwellen.

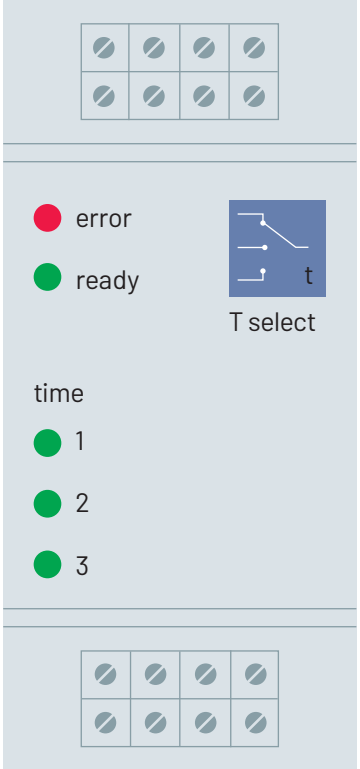


Abbildung 10 - Schaltgerät mit Display

Variante 2: Auswahl der Parameter

Funktionseinheit mit einer oder mehreren SSF, die mittels (externem) „Programmiergerät“ vor der Inbetriebnahme parametriert und die Parameter zum Schaltgerät übertragen werden müssen (z. B. Schutzfeld beim Sicherheits-Laserscanner; max. Drehzahl beim Frequenzumrichter mit SLS).

ESW	eine SSF
Bemerkung	incl. Fehlererkennung und Fehlerreaktion, parametrierbar
ASW	gewählte(r) Parameter
Verifikation ASW	Prüfen der Auswahl, also der auf dem Schaltgerät gespeicherten Parameter (gemäß Betriebsanleitung)

Beispiel: Schaltgerät mit integriertem Display/Drehschalter z. B. für Verzögerungszeit, Schaltschwellen.

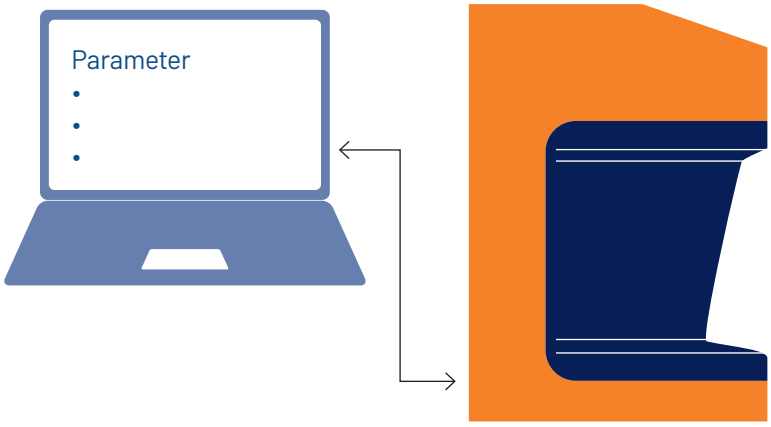


Abbildung 11 – Parametrierung Sicherheitslaserscanner

6.3.5 Logik-Typ „4“ – Konfigurierbare Sicherheits-Teilfunktion(en) in Geräten mit Kommunikation zwischen Geräten

Die SSF wird in Funktionsbausteinen mit eingebauter Fehlererkennung und Fehlerbehandlung realisiert.
Die *Abbildung 13 - Verteiltes System - Logische Darstellung* zeigt die logische Sicht, die folgende *Abbildung 14 - Verteiltes System - Physikalische Darstellung* die physikalische Sicht auf ein verteiltes System

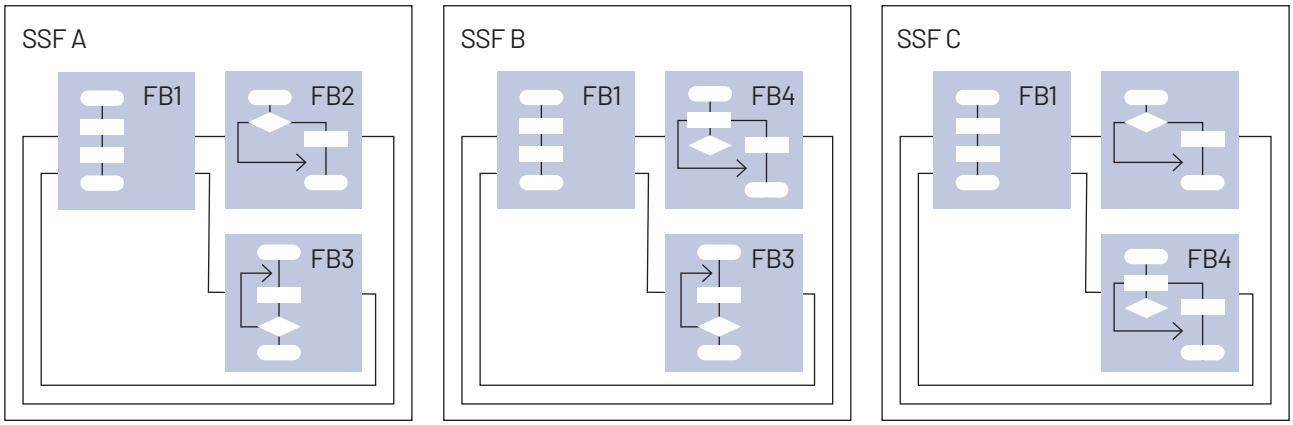


Abbildung 12 - Verteiltes System - Logische Darstellung

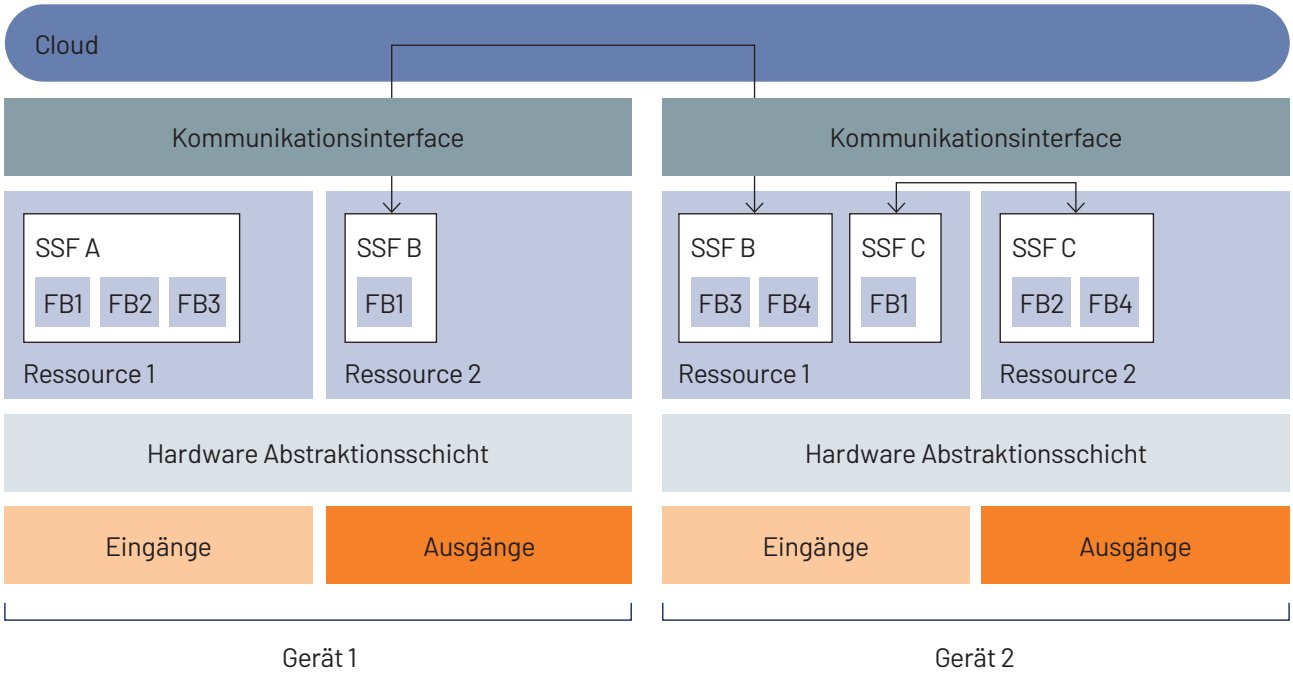


Abbildung 13 - Verteiltes System - Physikalische Darstellung

Variante 1: Auswahl von SSF bei Verwendung eines Logikmoduls

Funktionseinheit bestehend aus mehreren kommunizierenden Komponenten, z. B. Logikmodul mit Eingangs- und Ausgangsmodulen, Sicherheitsschaltgerät mit mehreren SSF, die mittels (externem) „Programmiergerät" (auch mehrfach) ausgewählt, E/A-konfiguriert (Software-Verdrahtung), parametriert werden müssen und die Konfiguration zum Schaltgerät übertragen werden muss.

ESW	mehrere SSF = komplexe Funktionsbausteine (z. B. Baustein „Schutztürüberwachung"
Bemerkung	instanzierbar, parametrierbar, E/A konfigurierbar incl. Fehlererkennung von Bauteilefehlern, Busfehlern, ungültigen Parametern sowie E/A-Tests, Plausibilisierung etc. Diese Funktionalitäten werden durch die ESW automatisch durchgeführt und Fehlerreaktionen eingeleitet (=Abschalten der Ausgänge). Dies geschieht unabhängig von der verwendeten Programmiersprache oder der Programmierumgebung.
ASW	Auswahl mehrerer SSF, jeweils mit E/A-Konfiguration und Parametern
Verifikation ASW	Prüfen der im Schaltgerät gespeicherten Konfiguration (gemäß Betriebsanleitung)

Beispiel: Logikmodul mit angeschlossenen Modulen für Eingänge und Ausgänge

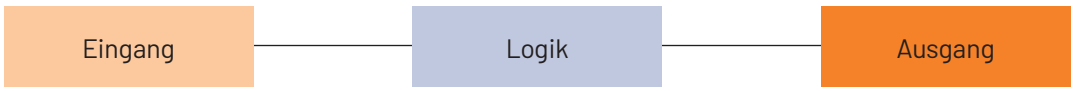


Abbildung 14 – Struktur – Logik-Typ 4 – Variante 1

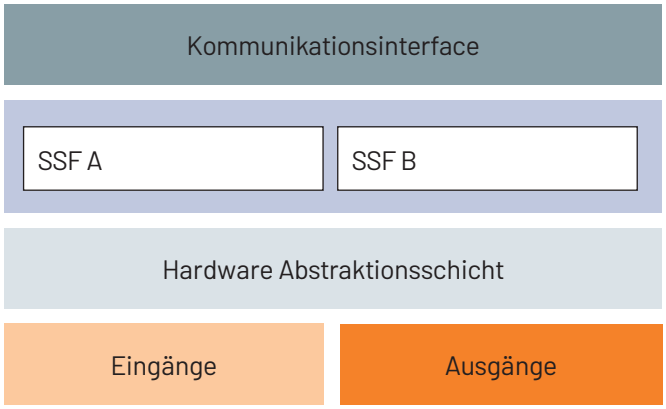


Abbildung 15 - Physikalische Darstellung Logik-Typ 4 - Variante 1

Variante 2: Auswahl von SSF bei Verwendung mehrerer Logikmodule

wie Logik-Typ 4 Variante 1, jedoch mehrere vernetzte Logikmodule

ESW	mehrere SSF = komplexe Funktionsbausteine (z. B. Baustein „Schutztürüberwachung“)
Bemerkung	instanzierbar, parametrierbar, E/A konfigurierbar incl. Fehlererkennung von Bauteilefehlern, Busfehlern, ungültigen Parametern sowie E/A-Tests, Plausibilisierung etc. Diese Funktionalitäten werden durch die ESW automatisch durchgeführt und Fehlerreaktionen eingeleitet (=Abschalten der Ausgänge). Dies geschieht unabhängig von der verwendeten Programmiersprache oder der Programmierumgebung.
ASW	Auswahl mehrerer SSF, jeweils mit E/A-Konfiguration und Parametern
Verifikation ASW	Prüfen der im Schaltgerät gespeicherten Konfiguration (gemäß Betriebsanleitung) für jedes einzelne Logikmodul

Beispiel: System mit zwei vernetzten Logikmodulen

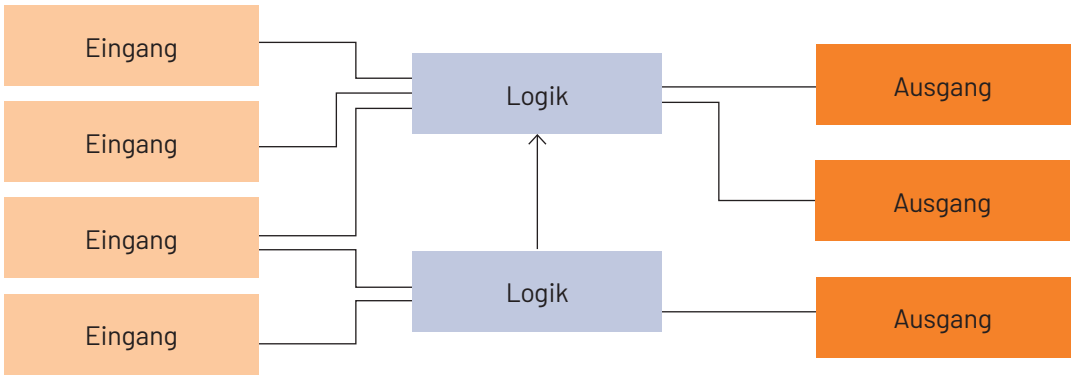


Abbildung 16 – Struktur – Logik-Typ 4 – Variante 1

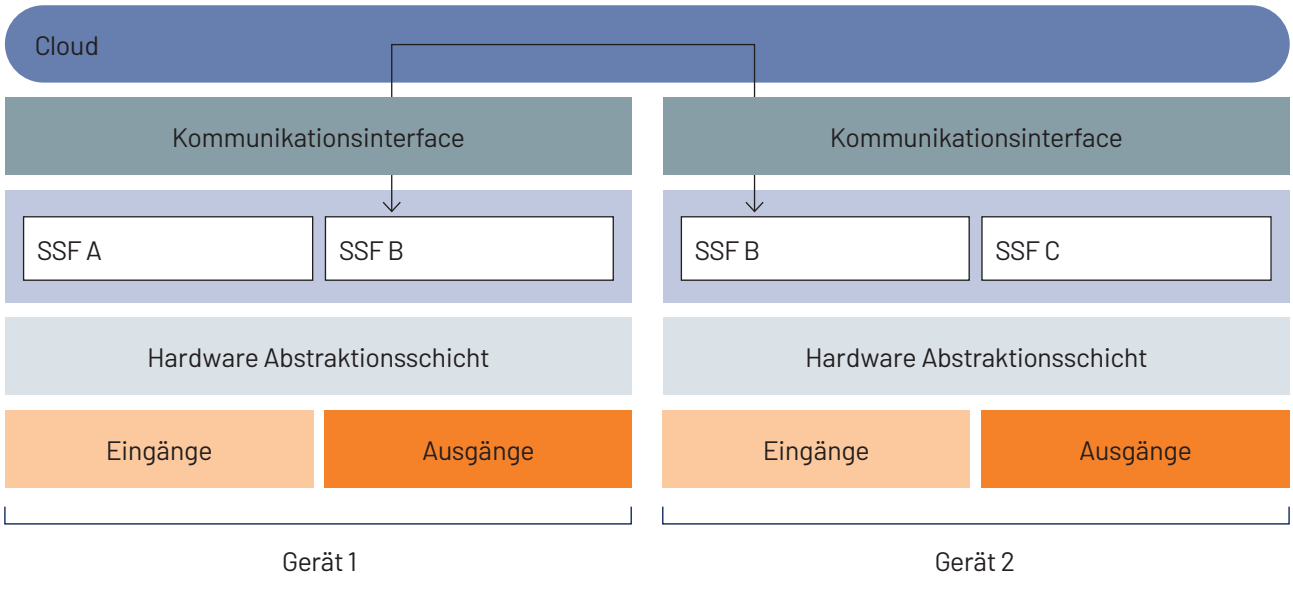


Abbildung 17 - Physikalische Darstellung Logik-Typ 4 - Variante 2

Variante 3: Auswahl und Kombination von Funktionsbausteinen

wie Logik-Typ 4 Variante 1 oder Variante 2, jedoch bestehen SSF aus miteinander verknüpften Funktionsbausteinen (z.B. 2 x Baustein „Schutztürüberwachung“ und Baustein „AND“)

ESW	mehrere SSF = komplexe Funktionsbausteine (z. B. Baustein „Schutztürüberwachung“)
Bemerkung	instanzierbar, parametrierbar, E/A konfigurierbar incl. Fehlererkennung von Bauteilefehlern, Busfehlern, ungültigen Parametern sowie E/A-Tests, Plausibilisierung etc. Diese Funktionalitäten werden durch die ESW automatisch durchgeführt und Fehlerreaktionen eingeleitet (=Abschalten der Ausgänge). Dies geschieht unabhängig von der verwendeten Programmiersprache oder der Programmierumgebung
ASW	Auswahl mehrerer SSF, jeweils mit E/A-Konfiguration und Parametern
Verifikation ASW	Prüfen der im Schaltgerät gespeicherten Konfiguration (gemäß Betriebsanleitung) für jedes einzelne Logikmodul, für jeden Funktionsbaustein und die (logische) Verknüpfung daraus.

Beispiel: Logikmodul mit angeschlossenen Modulen für Eingänge und Ausgänge

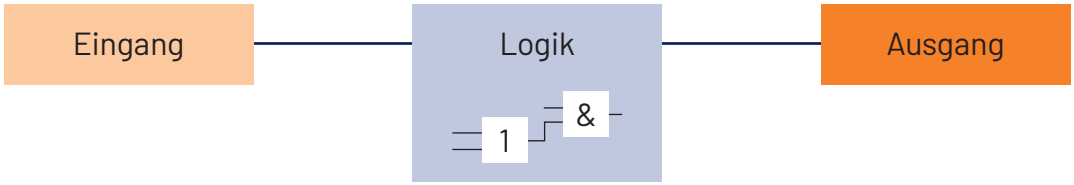


Abbildung 18 – Struktur – Logik-Typ 4 – Variante 3

Variante 4:

wie Logik-Typ 4-Variante 1 oder Variante 2 oder Variante 3, jedoch können vom Anwender eigene, wiederverwendbare Funktionsbausteine aus den auf einem Logikmodul vorhandenen Funktionsbausteinen durch Verknüpfung und Parametrierung geschaffen werden.

ESW	mehrere SSF = komplexe Funktionsbausteine (z. B. Baustein „Schutztürüberwachung“)
Bemerkung	instanzierbar, parametrierbar, E/A konfigurierbar incl. Fehlererkennung von Bauteilefehlern, Busfehlern, ungültigen Parametern sowie E/A-Tests, Plausibilisierung etc. Diese Funktionalitäten werden durch die ESW automatisch durchgeführt und Fehlerreaktionen eingeleitet (=Abschalten der Ausgänge). Dies geschieht unabhängig von der verwendeten Programmiersprache oder der Programmierumgebung.
ASW	Auswahl mehrerer SSF, jeweils mit E/A-Konfiguration und Parametern
Verifikation ASW	Prüfen der im Schaltgerät gespeicherten Konfiguration (gemäß Betriebsanleitung) für jedes einzelne Logikmodul, für jeden Funktionsbaustein und die (logische) Verknüpfung daraus und für jeden derart erstellten Funktionsbaustein. Wiederverwendbare Funktionsbausteine bedürfen vor ihrer Verwendung einer eigenständigen Validierung.

Beispiel: Logikmodul mit angeschlossenen Modulen für Eingänge und Ausgänge

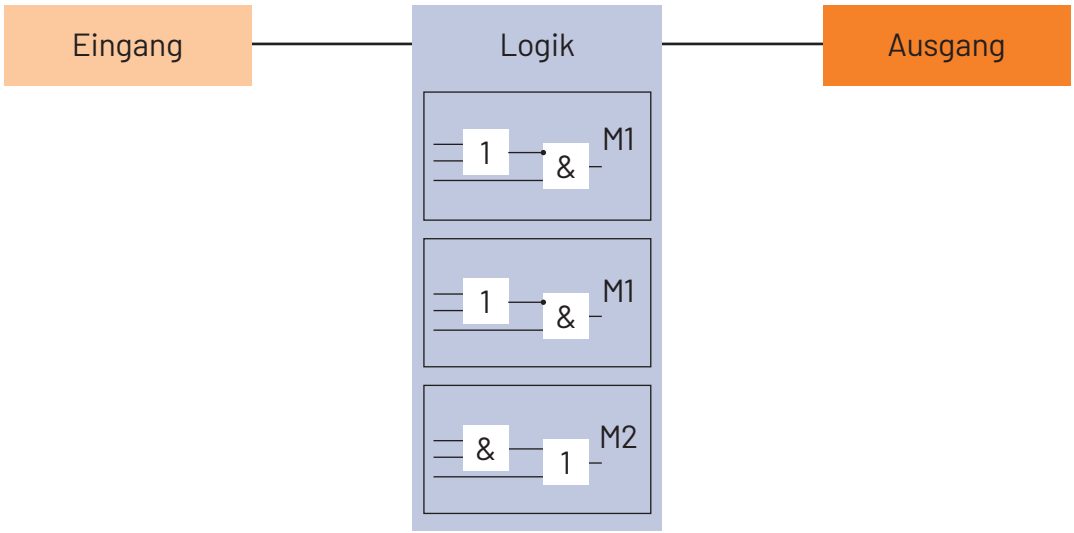


Abbildung 19 – Struktur – Logik-Typ 4 – Variante 4

6.3.6 Logik-Typ „5“ – Programmierbare Steuerung mit eingeschränktem oder vollem Sprachumfang

Steuerung bestehend aus mehreren mittels Bussystem kommunizierenden Komponenten, z. B. Logikmodul mit Eingangs- und Ausgangsmodulen.

SSF müssen mittels (externem) „Programmiergerät“ durch Verknüpfung und Parametrierung von Befehlen programmiert und das Programm zur Steuerung übertragen werden.

ESW	Systemsoftware ohne Fehlererkennung und Fehlerreaktion
Bemerkung	–
ASW	SSF und zusätzlich die Fehlererkennung von Bauteilefehlern, Busfehlern, ungültigen Parametern sowie E/A-Tests, Plausibilisierung etc. Die entsprechenden Fehlerreaktionen müssen ebenfalls programmiert werden. Dies ist unabhängig von der verwendeten Programmiersprache oder der Programmierumgebung.
Verifikation ASW	Sicherheitstechnische Bewertung des Anwenderprogramms entsprechend der Anforderungen zur Verifikation (z. B. gemäß den relevanten Teilen aus der DIN EN 61508). Anschließende Prüfung der korrekten Übertragung auf die Steuerung, ggf. gemäß Betriebsanleitung.

6.4 Beispiele für die Nutzung der Logik-Typen

Im Folgenden werden mögliche Grundformen von Funktionseinheiten dargestellt.
Mischformen daraus sind möglich.

6.4.1 Sicherheitsschaltgeräte

Ein Sicherheitsschaltgerät besteht aus:

- einer Verarbeitungseinheit, Logik-Typ 1 oder Typ 2 mit einer aktiven und fixen SSF im Gerät
- einer Ein-/Ausgabeeinheit, integriert, nicht erweiterbar
- optional:manuelle Rücksetzfunktion, Überwachung externer Steuerungsteile (EDM).

6.4.2 Sicherheitssensoren und –antriebe

Sicherheitssensoren und –antriebe bestehen aus:

- einer Verarbeitungseinheit, Logik-Typ 3 mit einer aktiven und parametrierbaren SSF im Gerät
- einer Ein-/Ausgabeeinheit, integriert, nicht erweiterbar
- optional:manuelle Rücksetzfunktion, Überwachung externer Steuerungsteile (EDM).

6.4.3 Modulare Sicherheitssteuerungen

Eine modulare Sicherheitssteuerung besteht aus:

- einer Verarbeitungseinheit, Logik-Typ 4 mit mehreren aktiven und konfigurierbaren SSF, mit Kommunikation
- einer oder mehreren Ein-/Ausgabeeinheit(en), lokal (Kommunikation über Rückwandbus), und/oder extern (Kommunikation über Feldbus).

6.4.4 Steuerung mit eingeschränktem oder vollem Sprachumfang

Eine solche Steuerung besteht aus:

- einer Verarbeitungseinheit, Logik-Typ 5 mit mehreren aktiven und frei programmierbaren SSF, mit Kommunikation
- einer oder mehreren Ein-/Ausgabeeinheit(en), einer Kommunikationsschnittstelle für eine direkte Kommunikation zwischen der Verarbeitungseinheit, anderen Logikeinheiten und den Feldgeräten (Feldbus)

7. Wer erstellt Software und wie ist Software rechtlich einzuordnen?

7.1 Hersteller

Der in diesem Dokument benutzte Begriff „Hersteller“ entspricht dem Wirtschaftsakteur, der das Produkt herstellt oder in seinem Namen / unter seiner Verantwortung herstellen lässt.

In diesem Dokument sind demnach „Hersteller“ insbesondere:

- **„Komponentenhersteller“:** dies sind Hersteller von sicherheitsbezogenen Funktionseinheiten
- **„Softwarehersteller“:** dies sind Hersteller von ESW oder ASW
- **„Maschinenhersteller“:** dies sind Hersteller einer oder mehrerer Maschinen als vollständige oder unvollständige Maschine
- **„Integrator“:** dies sind Hersteller von Anlagen, bestehend aus mindestens einer Maschine und Infrastruktur, häufig auch „Systemhersteller“ genannt
- **„Generalunternehmer“:** dies sind natürliche oder juristische Personen, die in einem Projekt die Hauptverantwortung für die Ausführung der Gewerke (z. B. Maschine, Fördertechnik, Lager oder Arbeitsstationen) übernehmen und mit ihrer Ausführung weitere Firmen beauftragt. Rechtsbeziehungen entstehen grundsätzlich nur zwischen dem Generalunternehmer und seinem Auftraggeber einerseits und dem Generalunternehmer und den Subunternehmern andererseits.
- **„Betreiber“:** ein Betreiber wird dann zum Hersteller, wenn er
  - sich selbst eine Maschine aus eigenen oder zugekauften Komponenten herstellt, oder
  - eine vorhandene Maschine oder Anlage wesentlich verändert, oder
  - eine vorhandene Maschine oder Anlage in eigener Verantwortung wesentlich verändern lässt.

7.2 Ist Software ein Produkt?

Hersteller verantworten die Zuverlässigkeit und Sicherheit ihrer Produkte. Bei der Einhaltung der gesetzlichen Anforderungen an Systeme der Funktionalen Sicherheit mit Software bedarf es einer detaillierten Betrachtung. Der Anwender eines solchen Systems erwartet ein zuverlässig funktionierendes Produkt, das den Sicherheitsanforderungen ohne Funktionseinschränkungen genügt. Es gibt in Deutschland und in Europa gesetzliche Regelungen, die Anwendung finden, wenn die Anforderungen an die funktionale Sicherheit nicht eingehalten werden:

- in der deliktischen Produkthaftung
  - Produzentenhaftung nach § 823 Bürgerliches Gesetzbuch (BGB)
  - Produkthaftungsgesetz (ProdHaftG)

- im Kaufrecht/Werkvertragsrecht
  - Mängelhaftung nach §§ 434 ff, §§634 ff (BGB)

- im öffentlichen Produktsicherheitsrecht
  - Europäische Richtlinien
  - Produktsicherheitsgesetz (ProdSG) bzw.
  - Produktsicherheitsverordnung (2023/988)

- im Strafrecht
  - insbesondere §§ 222, 229 Strafgesetzbuch (StGB)

In diesem Zusammenhang lässt sich die Frage, ob Software (ESW und/oder ASW) ein Produkt sein kann, nicht pauschal beantworten.

8. Software in der Maschinenrichtlinie und der Maschinenverordnung

Die Maschinenrichtlinie (MRL) ist (war) eine der wichtigsten Rechtsvorschriften zur Harmonisierung der grundlegenden Sicherheits- und Gesundheitsschutzanforderungen für Maschinen im europäischen Wirtschaftsraum. Die EU-Kommission hat die Maschinenrichtlinie zur Maschinenverordnung (MVO) weiterentwickelt, um den technologischen Entwicklungen Rechnung zu tragen. Sie ist ab dem 20.01.2027 für das Inverkehrbringen von Maschinen anzuwenden und auch die Basis für die Beurteilung von Software mit Sicherheitsfunktion, die mit und für Maschinen in Verkehr gebracht wird. Die folgenden Kapitel beschreiben die Auswirkungen in Bezug auf Software für beide Rechtsvorschriften.

8.1 Software in der Maschinenrichtlinie

Die Maschinenrichtlinie (2006/42/EG) ist bis einschließlich 19.01.2027 anwendbar.
Die Einhaltung der sich aus der Maschinenrichtlinie ergebenden Pflichten obliegt dem Hersteller einer Maschine. Die von sicherheitsbezogenen Systemen mit Software zu erfüllenden Anforderungen werden in der Maschinenrichtlinie Anhang 1 Abschnitt 1.2 dargelegt. Sicherheitsbezogene Steuerungen und Befehlseinrichtungen sind u.a. so zu konzipieren und zu bauen, dass es nicht zu Gefährdungssituationen kommt, und insbesondere müssen diese so ausgelegt und beschaffen sein, dass ein Defekt der Hardware oder ein systematischer Fehler in der Software (ESW und ASW) nicht zu einer Gefährdungssituation führt.

Wird Software gemeinsam mit einer zugehörigen Hardware (wie z. B. in Sicherheitssteuerungen, sicherheitsbezogenen Sensoren) in Verkehr gebracht, dann ist sie Teil eines „Sicherheitsbauteils“. Die Konformitätserklärung bezieht sich dann auf die Hardware mit integrierter Software.

Systemsoftware oder Anwendersoftware für sich allein erfüllt nicht die Maschinendefinition bzw. die Definition für ein Sicherheitsbauteil des Art. 2 der Maschinenrichtlinie. Die Software (ESW und ASW) selbst kann keine Sicherheitsfunktion ausführen, sie ist ein Teil der Logikeinheit. Erst die Logikeinheit ermöglicht die Verknüpfung zwischen den Ein- und Ausgängen. Für einen Softwarehersteller ist es somit rechtlich nicht vorgesehen, die Konformität („CE-Zeichen“) zur Maschinenrichtlinie für sicherheitsbezogene Software unabhängig von einer Logikeinheit zu erklären.

Gesondert in den Verkehr gebrachte sicherheitsbezogene Anwendersoftware (ASW) wird nicht als Sicherheitsbauteil im Sinne der Maschinenrichtlinie betrachtet, da sie für sich alleine keine Sicherheitsfunktion ausführen kann. Sie benötigt hierzu immer eine Hardware (siehe §42 und §418 - Anmerkung 5, Leitfaden für die Anwendung der Maschinenrichtlinie 2006/42/EG; Ausgabe 2.2; Oktober 2019): „Sicherheitsbezogene Anwendungssoftware selbst wird nicht als Logikeinheit angesehen, weil sie kein Sicherheitsbauteil ist und in jedem Fall von einem physischen Bauteil abhängig ist, um ihre Sicherheitsfunktion ausführen zu können (siehe § 42 Sicherheitsbauteile).“. Die Realisierung, Verifizierung und Validierung dieser sicherheitsbezogenen Anwendersoftware (ASW) soll entsprechend des aktuellen Stands der Technik erfolgen (z. B. nach EN 61508).

Die korrekte Integration einer sicherheitsbezogenen Anwendungssoftware (ASW) in eine Maschine wird durch die Konformitätserklärung für diese Maschine bestätigt. Der Maschinenhersteller trägt die alleinige und unmittelbare Verantwortung für die Konformität seines Produkts mit den anzuwendenden Rechtsvorschriften (Leitfaden für die Umsetzung der Produktvorschriften der EU 2022 („Blue Guide“)).

8.2 Software in der Maschinenverordnung

Motivation der EU-Kommission

Technologische Entwicklungen haben die EU-Kommission motiviert, die bewährte Maschinenrichtlinie in die Maschinenverordnung unter der Berücksichtigung der Anforderungen aus dem New Legislative Framework (NLF) weiterzuentwickeln. Im Gegensatz zu einer Richtlinie gilt eine Verordnung ab dem festgesetzten Stichtag. Sie muss nicht mehr von den Einzelstaaten in nationales Recht umgesetzt werden.

In der Maschinenverordnung wird der Begriff „Software" an folgenden Stellen referenziert: Der vollständige Text hierzu ist im Anhang dieses Dokuments nachzulesen. Im Folgenden sind nur die jeweiligen Kernaussagen zitiert:

1) Erwägungsgrund 19
   *...Um der zunehmenden Verwendung von **Software** als Sicherheitsbauteil Rechnung zu tragen, sollte **Software**, die eine Sicherheitsfunktion erfüllt und separat in Verkehr gebracht wird, als Sicherheitsbauteil betrachtet werden.*

2) Erwägungsgrund 32
   Der Hersteller sollte ferner dafür sorgen, dass für das in den Anwendungsbereich dieser Verordnung fallende Produkt, das der Hersteller in Verkehr bringen oder in Betrieb nehmen will, eine Risikobeurteilung vorgenommen wird...

3) *... Bei der Risikobeurteilung sollten ferner künftige Aktualisierungen oder Entwicklungen einer in der Maschine oder dem dazugehörigen Produkt installierten **Software** berücksichtigt werden, die zum Zeitpunkt des Inverkehrbringens oder der Inbetriebnahme der Maschine oder des dazugehörigen Produkts vorgesehen sind...*

   Erwägungsgrund 55
   *Die Bestimmungen dieser Verordnung über die Konformitätsbewertung von **Software**, die Sicherheitsfunktionen gewährleistet, durch unabhängige Dritte sollten nur für Systeme mit vollständig oder teilweise selbstentwickelndem Verhalten unter Verwendung von Ansätzen des maschinellen Lernens, die Sicherheitsfunktionen gewährleisten, gelten...*

4) Artikel 3 – Begriffsbestimmungen – Abschnitt 1
   *... f) eine Gesamtheit im Sinne der Buchstaben a bis e, bei der lediglich das Aufspielen einer für die vom Hersteller vorgesehene bestimmte Anwendung vorgesehenen **Software** fehlt*

5) Begriffsbestimmung – Abschnitt 3
   *„Sicherheitsbauteil" bezeichnet ein physisches oder digitales Bauteil, einschließlich **Software**, eines in den Anwendungsbereich dieser Verordnung fallenden Produkts, die zur Gewährleistung einer Sicherheitsfunktion konstruiert oder bestimmt ist, gesondert in Verkehr gebracht wird und dessen Ausfall oder Fehlfunktion die Sicherheit von Personen gefährdet, die aber für das Funktionieren dieses Produkts nicht erforderlich ist oder durch normale Bauteile ersetzt werden kann, um den Betrieb dieser Produkte zu gewährleisten*

6) Anhang II Nicht erschöpfende Liste der Sicherheitsbauteile
   *... 18. **Software**, die Sicherheitsfunktionen wahrnimmt.*
   19. Sicherheitsbauteile mit vollständig oder teilweise selbstentwickelndem Verhalten unter Verwendung von Ansätzen des maschinellen Lernens, die Sicherheitsfunktionen gewährleisten.

7) Anhang I Teil A Kategorien von Maschinen
   5. Sicherheitsbauteile mit vollständig oder teilweise selbstentwickelndem Verhalten unter Verwendung von Ansätzen des maschinellen Lernens, die Sicherheitsfunktionen gewährleisten.

8) Anhang III Teil B 1.1.9 Schutz gegen Korrumpierung
   *... Ein Hardware-Bauteil, das Signale oder Daten überträgt, die für den Anschluss oder den Zugriff auf die **Software** relevant sind, die für die Übereinstimmung einer Maschine oder eines dazugehörigen Produkts mit den einschlägigen Sicherheits- und Gesundheitsschutzanforderungen von entscheidender Bedeutung ist, muss so konstruiert sein, dass es angemessen gegen unbeabsichtigte oder vorsätzliche Korrumpierung geschützt ist...*

9) Anhang III Teil B 1.2.1
*Steuerungen müssen so ausgelegt und beschaffen sein, dass ... b) ein Defekt der Hardware oder der **Software** der Steuerung nicht zu Gefährdungssituationen führt; c) Fehler in der Logik des Steuerkreises nicht zu Gefährdungssituationen führen; ...*

8.3 Inverkehrbringen von Software

Im Anwendungsbereich der Maschinenverordnung kann eine Konformitätsbewertung von Software erforderlich sein, wenn sie (Teil-)Sicherheitsfunktionen realisieren soll. Die nachfolgend beschriebenen Fälle betrachten hierzu jeweils das erstmalige Inverkehrbringen (Erstlieferung), die Fehlerbehebung (Update) und die Funktionserweiterung (Upgrade). Zur Laufzeit der Maschine nachladbare Softwaremodule (z. B. im Rahmen von I4.0) werden wie ein Upgrade betrachtet.

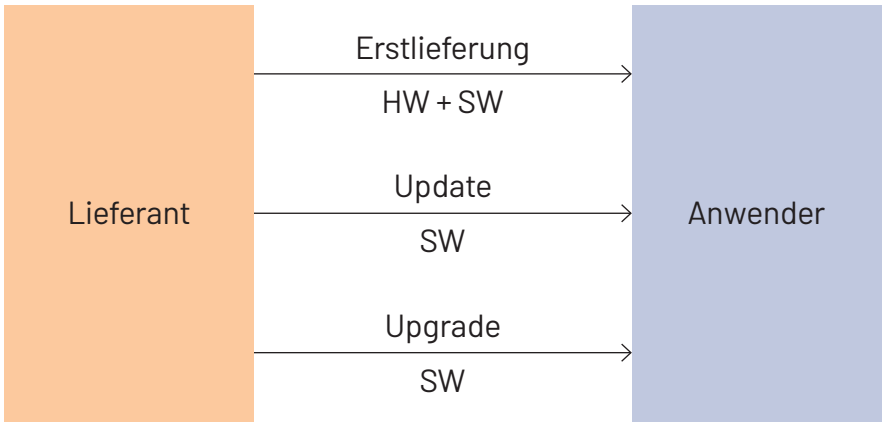


Abbildung 20 - Beziehung zwischen Lieferant und Anwender

Betrachtet wird immer eine sicherheitsbezogene Software, die maßgeschneidert auf eine bestimmte Funktionseinheit, Maschine oder Anwendung und deren spezifischen technischen, organisatorischen und funktionellen Anforderungen angepasst wird.

Werkzeuge (Tools) zur Programmierung oder Konfiguration sind keine Sicherheitsbauteile im Sinne der Maschinenverordnung. Diese Hilfsprogramme (siehe Definition in 3.13.3) sind für den Betrieb des Systems nicht erforderlich und beeinflussen das sicherheitsbezogene System zur Laufzeit nicht. Gegebenenfalls ist eine Qualifizierung z. B. nach IEC 61508 erforderlich.

8.4 Beschreibung der Auswirkungen auf die Marktteilnehmer

Die Fälle in der nachfolgenden Tabelle 1 dienen der Übersicht der typischen Beziehungen zwischen Lieferant und Anwender. Sie beschreiben die Verantwortung für die Konformitätsbewertung.

Nur in den Fällen 4b und 4c wird ASW oder ESW als Produkt eigenständig in Verkehr gebracht und benötigt daher eine Konformitätsbewertung durch den Softwarehersteller.

Verantwortung für die Konformitätsbewertung

Fall		Lieferant	Anwender	Lieferung	Konformitätsbewertung
1		Komponenten-hersteller	Maschinen-hersteller	ESW mit HW (FE)	Komponentenhersteller (für die Funktionseinheit)
2		Software-hersteller	Maschinen-hersteller	ASW (im Auftrag von MH)	Maschinenhersteller (für die Maschine)
3		Maschinen-hersteller	Betreiber	ASW mit HW (MA)	Maschinenhersteller (für die Maschine)
4	a	Software-hersteller	Betreiber	ASW (im Auftrag von BE)	Betreiber (für die Hardware bei wesentlicher Veränderung)
	b			ASW (im Namen von SH)	Softwarehersteller (für die Software)
	c			ESW (im Namen von SH)	Softwarehersteller (für die Software)
5	a	Betreiber		ASW (HW ohne ASW)	Betreiber (für die Maschine)
	b			Retrofit (FE)	Betreiber (für die Maschine bei wesentlicher Veränderung)
	c			Modifikation (ASW)	Betreiber (für die Hardware bei wesentlicher Veränderung)

Legende:

ASW	Anwendungsprogramm	KH	Komponentenhersteller
ESW	Systemsoftware	MH	Maschinenhersteller
FE	Funktionseinheit	SH	Softwarehersteller
MA	Maschine	BE	Betreiber

Tabelle 1 - Verantwortung für die Konformitätsbewertung

In den nachfolgenden Unterkapiteln werden die einzelnen Fälle im Detail betrachtet und beschrieben.

8.4.1 Fall 1: Komponentenhersteller liefert an einen Maschinenhersteller

Lieferung einer sicherheitsbezogenen Funktionseinheit (Maschinenprodukt) z. B.:

- Sicherheits-Laserscanner
- Sicherheits-Lichtvorhang
- Sicherheitsbezogene Steuerung
- Servoantrieb mit integrierten Sicherheitsteilfunktionen

Erstlieferung:

- ESW innerhalb einer Funktionseinheit inclusive Tools
- Konformitätsbewertung durch Komponentenhersteller für die Funktionseinheit (HW, ESW)

Update:

- Fehlerkorrektur ESW
- aktualisierte Konformitätsbewertung für die Funktionseinheit
- keine eigenständige Konformitätsbewertung für ESW
- Betrachtung als „Ersatzteil" möglich

Upgrade:

- Funktionserweiterung ESW (nicht durch bisherige Konformitätsbewertung abgedeckt)
- neue Konformitätsbewertung für die Funktionseinheit
- keine eigenständige Konformitätsbewertung für ESW
- Gleichstellung mit Erstlieferung

8.4.2 Fall 2: Softwarehersteller liefert an einen Maschinenhersteller

Die Realisierung von Sicherheitsfunktionen erfolgt im Auftrag des Maschinenherstellers durch den Softwarehersteller. Die bestimmungsgemäße Verwendung gibt der Maschinenhersteller vor.

Lieferung einer ASW für spezifizierte Funktionseinheiten (z. B. sicherheitsbezogener Teil der Steuerung). Betrachtung von ESW ist nicht möglich.

Erstlieferung:

- ASW wird nicht eigenständig in Verkehr gebracht
- Konformitätsbewertung erfolgt durch den Maschinenhersteller im Rahmen der Validierung der Maschine
- keine eigenständige Konformitätsbewertung für ASW

Update:

- Fehlerkorrektur ASW
- aktualisierte Konformitätsbewertung durch den Maschinenhersteller
- keine eigenständige Konformitätsbewertung für ASW
- Betrachtung als „Ersatzteil" möglich

Upgrade:

- Funktionserweiterung ASW
- bei nicht wesentlicher Veränderung: aktualisierte Konformitätsbewertung für die Maschine
- bei wesentlicher Veränderung: neue Konformitätsbewertung durch den Maschinenhersteller für die Maschine
- keine eigenständige Konformitätsbewertung für ASW
- Gleichstellung mit Erstlieferung

8.4.3 Fall 3: Maschinenhersteller liefert an einen Betreiber

Der Maschinenhersteller liefert eine Maschine mit integrierter ASW zur Realisierung von Sicherheitsfunktionen an den Betreiber.

Erstlieferung:

- Konformitätsbewertung für die Maschine
- keine eigenständige Konformitätsbewertung für die ASW

Update:

- Fehlerkorrektur ASW
- aktualisierte Konformitätsbewertung für die Maschine
- keine eigenständige Konformitätsbewertung für die ASW
- Betrachtung als „Ersatzteil" möglich

Upgrade:

- Funktionserweiterung ASW
- bei nicht wesentlicher Veränderung: aktualisierte Konformitätsbewertung für die Maschine
- bei wesentlicher Veränderung: neue Konformitätsbewertung durch den Maschinenhersteller für die Maschine (Gleichstellung mit Erstlieferung)

8.4.4 Fall 4: Softwarehersteller liefert an einen Betreiber

Fall 4a: Softwarehersteller ist verlängerte Werkbank für einen Betreiber

Die Realisierung von Sicherheitsfunktionen erfolgt im Auftrag des Betreibers durch den Softwarehersteller. Die bestimmungsgemäße Verwendung gibt der Betreiber vor.

Dieser Fall ist analog zu Fall 2 zu betrachten (ersetze „Maschinenhersteller" durch „Betreiber").

Fall 4b: Softwarehersteller bringt eigenständig entwickelte ASW für mehrere Betreiber in Verkehr

Die Realisierung von Sicherheitsfunktionen für eine bestimmte Maschine oder einen bestimmten Maschinentyp erfolgt durch den Softwarehersteller. Die bestimmungsgemäße Verwendung gibt der Softwarehersteller vor.

Erstlieferung:

- ASW wird durch den Softwarehersteller eigenständig in Verkehr gebracht
- Konformitätsbewertung für ASW durch den Softwarehersteller
- neue Konformitätsbewertung für die Maschine durch den Betreiber, da wesentliche Veränderung

Update:

- Fehlerkorrektur ASW
- aktualisierte Konformitätsbewertung für die Maschine durch den Betreiber
- aktualisierte Konformitätsbewertung für ASW durch den Softwarehersteller
- Betrachtung als „Ersatzteil" möglich

Upgrade:

- Funktionserweiterung ASW
- neue Konformitätsbewertung für ASW durch den Softwarehersteller
- bei nicht wesentlicher Veränderung: aktualisierte Konformitätsbewertung für die Maschine durch den Betreiber
- bei wesentlicher Veränderung: neue Konformitätsbewertung durch den Betreiber für seine Maschine

Fall 4c: Softwarehersteller entwickelt ESW für Komponenten als Teil eines SRP/CS

Erstellung von Funktionsbausteinen für sicherheitsbezogene Steuerungen, die durch den Betreiber nicht weiter verändert werden können. Die bestimmungsgemäße Verwendung gibt der Softwarehersteller vor. In diesem Fall ergibt sich die Verantwortung des Betreibers, wie im Fall 5b.

Erstlieferung:

- geschlossener Funktionsbaustein für sicherheitsbezogene Steuerung
- Konformitätsbewertung für die ESW durch den Softwarehersteller

Update:

- Fehlerkorrektur Funktionsbaustein
- aktualisierte Konformitätsbewertung für die ESW durch den Softwarehersteller
- bei nicht wesentlicher Veränderung: aktualisierte Konformitätsbewertung für die Maschine durch den Betreiber
- bei wesentlicher Veränderung: neue Konformitätsbewertung durch den Betreiber für seine Maschine

Upgrade:

- Funktionserweiterung Funktionsbausteine
- neue Konformitätsbewertung für die ESW durch den Softwarehersteller

8.4.5 Fall 5: Ein Betreiber wird selbst zum Maschinenhersteller (Modifikation)

Fall 5a: Integrieren von ASW in eine Maschine, die ohne ASW von einem Maschinenhersteller in Verkehr gebracht wurde

Dieser Fall ist in Fall 3 beschrieben.

Fall 5b: Austausch von sicherheitsbezogenen Funktionseinheiten mit ASW, wenn die Originalkomponente nicht mehr als Ersatzteil am Markt verfügbar ist. Hierbei bleibt die Funktionalität der ursprünglichen Komponente erhalten (Retrofit).

Erstlieferung:

- nicht relevant, da Modifikation

Update:

- 1:1 Austausch der ursprünglichen Funktionalität der ASW
- keine wesentliche Veränderung der Maschine
- keine neue Konformitätsbewertung für ASW und Maschine durch den Betreiber erforderlich

Upgrade:

- Erweiterung der ursprünglichen Funktionalität der ASW
- bei nicht wesentlicher Veränderung: keine neue Konformitätsbewertung für die Maschine erforderlich
- bei wesentlicher Veränderung: neue Konformitätsbewertung durch den Betreiber für seine Maschine
- keine eigenständige Konformitätsbewertung der ASW

Fall 5c: Veränderung der ursprünglich vom Maschinenhersteller gelieferten ASW an einer bestehenden Maschine

Erstlieferung:

- nicht relevant, da Veränderung

Update:

- Fehlerkorrektur ASW
- aktualisierte Konformitätsbewertung für die Maschine durch den Betreiber

Upgrade:

- Funktionserweiterung ASW
- bei nicht wesentlicher Veränderung: keine neue Konformitätsbewertung für die Maschine erforderlich
- bei wesentlicher Veränderung: neue Konformitätsbewertung durch den Betreiber für seine Maschine
- keine eigenständige Konformitätsbewertung der ASW

Verantwortung für die Konformitätsbewertung

gemäß MVO 2023/1230 vom 14. Juni 2023
(ZVEI, TA Si, AG Software, Stand: 22. 11. 2023)

Fall		Lieferant	Anwender	Lieferung	Erstlieferung				Update (Fehlerbehebung)				Upgrade (Funktionserweiterung)				
					ASW	ESW	FE	MA	ASW	ESW	FE	MA	ASW	ESW	FE	MA	MA VW
1		Komponenten-hersteller	Maschinen-hersteller	ESW mit HW (FE)	–	~~KH~~	KH	–	–	~~KH~~	KH	–	–	~~KH~~	KH	–	–
2		Software-hersteller	Maschinen-hersteller	ASW (im Auftrag von MH)	~~SH~~	–	–	MH	~~SH~~	–	–	MH	~~SH~~	–	–	(MH)	–
3		Maschinen-hersteller	Betreiber	ASW mit HW (MA)	~~MH~~	–	–	MH	~~MH~~	–	–	MH	~~MH~~	–	–	(MH)	–
4	a	Software-hersteller	Betreiber	ASW (im Auftrag von BE)	~~SH~~	–	–	BE		–	–	–	~~SH~~	–	–	~~BE~~	BE
	b			ASW (im Namen von SH)	SH	–	–	BE	SH	–	–	BE	SH	–	–	~~BE~~	BE
	c			ESW (im Namen von SH)	–	SH	–	BE	–	SH	–	–	–	SH	–	~~BE~~	BE
5	a	Betreiber		ASW (HW ohne ASW)	~~BE~~	–	–	BE	~~BE~~	–	–	BE	~~BE~~	–	–	~~BE~~	BE
	b			Retrofit (FE)	–				~~BE~~	1:1 Austausch		–	~~BE~~	–	–	~~BE~~	BE
	c			Modifikation (ASW)	–				~~BE~~	–	–	–	~~BE~~	–	–	~~BE~~	BE

Legende:

ASW	Anwendungsprogramm	MH	Maschinenhersteller	AA	Konformitätsbewertung
ESW	Systemsoftware	SH	Softwarehersteller	~~AA~~	keine Konformitätsbewertung
FE	Funktionseinheit	BE	Beschreibung der Akteure	AA	Aktualisierung der Konformitätsbewertung
MA	Maschine	KH	Komponentenhersteller	–	leeres Feld

Tabelle 2 - Verantwortung für die Konformitätsbewertung

9. Zusammenfassung und Ausblick

Für das Inverkehrbringen von sicherheitsbezogener Software ergeben sich folgende Punkte:

- Die Maschinenverordnung (EU) 2023/1230 ist ab dem 20.01.2027 verpflichtend anzuwenden.
- In Bezug auf die funktionale Sicherheit sind die Themen „Security“ und „Software als Sicherheitsbauteil“, DIE wichtigen Neuerungen.
- Der Begriff „Sicherheitsbauteile“ wurde dazu erweitert und umfasst nun auch Software, die eigenständig Sicherheits(teil)funktionen ausführt.
- Dies gilt es bei allen Abläufen von der Erstellung bis zu Update und Upgrade zu berücksichtigen. Das Entscheidungskriterium ist die „wesentliche Veränderung“.
- Die unterschiedlichen Verantwortungen für eine Konformitätsbewertung beim Inverkehrbringen von Software als Sicherheitsbauteil sind in Tabelle 2 beschrieben.
- Aus der Verknüpfung der Schutzziele von Security und Software, ist auf eine entsprechende Wartbarkeit und damit Versionierung und Dokumentation zu achten.
- Hersteller, die ihre Prozesse nach der aktuellen Maschinenrichtlinie 2006/42/EG gut organisiert haben, sind auch für die neuen Anforderungen gewappnet.
- Die unterschiedlichen Verantwortungen für eine Konformitätsbewertung beim Inverkehrbringen von Software als Sicherheitsbauteil sind in der folgenden Tabelle 3 (identisch Tabelle 1) beschrieben.

Fall		Lieferant	Anwender	Lieferung	Konformitätsbewertung
1		Komponenten-hersteller	Maschinen-hersteller	ESW mit HW (FE)	Komponentenhersteller (für die Funktionseinheit)
2		Software-hersteller	Maschinen-hersteller	ASW (im Auftrag von MH)	Maschinenhersteller (für die Maschine)
3		Maschinen-hersteller	Betreiber	ASW mit HW (MA)	Maschinenhersteller (für die Maschine)
4	a	Software-hersteller	Betreiber	ASW (im Auftrag von BE)	Betreiber (für die Hardware bei wesentlicher Veränderung)
	b			ASW (im Namen von SH)	Softwarehersteller (für die Software)
	c			ESW (im Namen von SH)	Softwarehersteller (für die Software)
5	a	Betreiber		ASW (HW ohne ASW)	Betreiber (für die Maschine)
	b			Retrofit (FE)	Betreiber (für die Maschine bei wesentlicher Veränderung)
	c			Modifikation (ASW)	Betreiber (für die Hardware bei wesentlicher Veränderung)

Tabelle 3 - Verantwortung für die Konformitätsbewertung

10. Anhang

Nachfolgende Übersicht relevanter Gesetze, Vorschriften, Normen und weiterer Literatur dient der Orientierung. Die Auflistung erhebt keinen Anspruch auf Vollständigkeit.

10.1 Dokumente der EU

Maschinenverordnung

Verordnung (EU) 2023/1230 des europäischen Parlaments und des Rates vom 14. Juni 2023 über Maschinen und zur Aufhebung der Richtlinie 2006/42/EG des Europäischen Parlaments und des Rates und der Richtlinie 73/361/EWG des Rates

Maschinenrichtlinie

Richtlinie 2006/42/EG (*) über Maschinen und zur Änderung der Richtlinie 95/16/EG (Neufassung)

Arbeitsschutzrahmenrichtlinie

Richtlinie 89/391/EWG des Rates vom 12. Juni 1989 über die Durchführung von Maßnahmen zur Verbesserung der Sicherheit und des Gesundheitsschutzes der Arbeitnehmer bei der Arbeit

Verordnung (EG)765/2008

Verordnung über die Vorschriften für die Akkreditierung und Marktüberwachung, im Zusammenhang mit der Vermarktung von Produkten

Blue Guide

Bekanntmachung der Kommission – Leitfaden für die Umsetzung der Produktvorschriften der EU 2022 („Blue Guide")

10.2 Normen

DIN EN ISO 12100

Sicherheit von Maschinen - Allgemeine Gestaltungsleitsätze - Risikobeurteilung und Risikominderung (ISO 12100:2010); Deutsche Fassung EN ISO 12100:2010

DIN EN 61508-1

Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme - Teil 1: Allgemeine Anforderungen (IEC 61508-1:2010); Deutsche Fassung EN 61508-1:2010

DIN EN 61508-2

Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/ programmierbarer elektronischer Systeme - Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme (IEC 61508-2:2010); Deutsche Fassung EN 61508-2:2010

DIN EN 61508-3

Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/ pro¬grammierbarer elektronischer Systeme - Teil 3: Anforderungen an Software (IEC 61508-3:2010); Deutsche Fassung EN 61508-3:2010

DIN EN 61508-4

Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme - Teil 4: Begriffe und Abkürzungen (IEC 61508-4:2010); Deutsche Fassung EN 61508-4:2010

DIN EN 61508-5

Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme - Teil 5: Beispiele zur Ermittlung der Stufe der Sicherheitsintegrität (safety integrity level) (IEC 61508-5:2010); Deutsche Fassung EN 61508-5:2010

DIN EN 61508-6

Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme - Teil 6: Anwendungsrichtlinie für IEC 61508-2 und IEC 61508-3 (IEC 61508-6:2010); Deutsche Fassung EN 61508-6:2010

DIN EN 61508-7

Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme - Teil 7: Überblick über Verfahren und Maßnahmen (IEC 61508-7:2010); Deutsche Fassung EN 61508-7:2010

DIN EN 61508-Beiblatt 1

Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme - Teil 0: Funktionale Sicherheit und die IEC 61508 (IEC/TR 61508-0:2005)

DIN EN ISO 13849-1 (2023)

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

DIN EN ISO 13849-2

Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen - Teil 2: Validierung (ISO 13849-2:2012); Deutsche Fassung EN ISO 13849-2:2012

DIN EN 61499-1

Funktionsbausteine für industrielle Leitsysteme - Teil 1: Architektur (IEC 61499-1:2012); Deutsche Fassung EN 61499-1:2013

DIN EN 61499-2

Funktionsbausteine für industrielle Leitsysteme - Teil 2: Anforderungen an Software-Werkzeuge (IEC 61499-2:2012); Deutsche Fassung EN 61499-2:2013

DIN EN 61499-4

Verteilte Funktionsbausteine für die Automatisierungstechnik - Teil 4: Regeln für normgerechte Profile (IEC 61499-4:2013); Deutsche Fassung EN 61499-4:2013

DIN EN 62061

Sicherheit von Maschinen - Funktionale Sicherheit sicherheitsbezogener Steuerungssysteme (IEC 62061:2021); Deutsche Fassung EN IEC 62061:2021

10.3 weitere Literatur/Informationsquellen

IFA-Report 2/2016

Sicherheitsbezogene Anwendungssoftware von Maschinen – Die Matrixmethode des IFA, Link: IFA-Report 2/2016

IFA-Report 2/2017

Funktionale Sicherheit von Maschinensteuerungen, Link: IFA-Report 2/2017

IFA-Report 1/2020

Praxisgerechte Umsetzung der Anforderungen für sicherheitsbezogene Embedded-Software nach DIN EN ISO 13849-1, Link: IFA-Report 1/2020

IEV

Internationales Elektrotechnisches Wörterbuch, Link: IEV-Wörterbuch

Rothhardt

Praxis der Softwareentwicklung, Günter Rothhardt, VEB Verlag Technik Berlin, 1987, ISBN: 3341002960

10.4 Sammlung: Erwägungsgründe der Kommission (Zitat entnommen aus der MVO)

1) Erwägungsgrund 19
   Die Entwicklung im Maschinensektor hat dazu geführt, dass zunehmend digitale Mittel eingesetzt werden und ***Software*** *eine immer wichtigere Rolle bei der Konstruktion von Maschinen spielt. Folglich sollte die Definition von Maschinen angepasst werden. In dieser Hinsicht sollten Maschinen, bei denen lediglich das Aufspielen einer* ***Software*** *fehlt, die für die bestimmte Anwendung der Maschine, wie sie vom Hersteller vorgesehen ist und die Gegenstand des Konformitätsbewertungsverfahren der Maschine ist, bestimmt ist, unter die Begriffsbestimmung für Maschinen und nicht unter die Begriffsbestimmungen für dazugehörige Produkte oder unvollständige Maschinen fallen. Darüber hinaus sollte die Begriffsbestimmung für Sicherheitsbauteile nicht nur physische, sondern auch digitale Komponentenumfassen. ...Um der zunehmenden Verwendung von* ***Software*** *als Sicherheitsbauteil Rechnung zu tragen, sollte* ***Software****, die eine Sicherheitsfunktion erfüllt und separat in Verkehr gebracht wird, als Sicherheitsbauteil betrachtet werden.*

2) Erwägungsgrund 32
   Der Hersteller sollte ferner dafür sorgen, dass für das in den Anwendungsbereich dieser Verordnung fallende Produkt, das der Hersteller in Verkehr bringen oder in Betrieb nehmen will, eine Risikobeurteilung vorgenommen wird. In diesem Zusammenhang sollte der Hersteller ermitteln, welche grundlegenden Sicherheits- und Gesundheitsschutzanforderungen auf das in den Anwendungsbereich dieser Verordnung fallende Produkt anwendbar sind und welche Maßnahmen ergriffen werden müssen, um die von dem Produkt möglicherweise ausgehenden Risiken zu beseitigen. Bei der Risikobeurteilung sollten ferner künftige Aktualisierungen oder Entwicklungen einer in der Maschine oder dem dazugehörigen Produkt installierten ***Software*** *berücksichtigt werden, die zum Zeitpunkt des Inverkehrbringens oder der Inbetriebnahme der Maschine oder des dazugehörigen Produkts vorgesehen sind. Die bei der Risikobeurteilung ermittelten Risiken sollten diejenigen Risiken einschließen, die während des Lebenszyklus des Produkts aufgrund einer geplanten Entwicklung seines Verhaltens im Hinblick auf einen Betrieb mit unterschiedlichen Autonomiegraden auftreten können.*

3) Erwägungsgrund 55
Die Bestimmungen dieser Verordnung über die Konformitätsbewertung von ***Software***, *die Sicherheitsfunktionen gewährleistet, durch unabhängige Dritte sollten nur für Systeme mit vollständig oder teilweise selbstentwickelndem Verhalten unter Verwendung von Ansätzen des maschinellen Lernens, die Sicherheitsfunktionen gewährleisten, gelten. Dagegen sollten diese Bestimmungen nicht für* ***Software*** *gelten, die weder lern- noch weiterentwicklungsfähig ist und nur für die Ausführung bestimmter automatisierter Funktionen von Maschinen oder dazugehörigen Produkten programmiert ist.*

4) Artikel 3 – Begriffsbestimmungen – Abschnitt 1
f) eine Gesamtheit im Sinne der Buchstaben a bis e, bei der lediglich das Aufspielen einer für die vom Hersteller vorgesehene bestimmte Anwendung vorgesehenen ***Software*** *fehlt*

5) Begriffsbestimmung – Abschnitt 3
„Sicherheitsbauteil" bezeichnet ein physisches oder digitales Bauteil, einschließlich ***Software****, eines in den Anwendungsbereich dieser Verordnung fallenden Produkts, die zur Gewährleistung einer Sicherheitsfunktion konstruiert oder bestimmt ist, gesondert in Verkehr gebracht wird und dessen Ausfall oder Fehlfunktion die Sicherheit von Personen gefährdet, die aber für das Funktionieren dieses Produkts nicht erforderlich ist oder durch normale Bauteile ersetzt werden kann, um den Betrieb dieser Produkte zu gewährleisten*

6) Anhang II Nicht erschöpfende Liste der Sicherheitsbauteile
18. ***Software****, die Sicherheitsfunktionen wahrnimmt. 19. Sicherheitsbauteile mit vollständig oder teilweise* ***selbstentwickelndem Verhalten*** *unter Verwendung von Ansätzen des* ***maschinellen Lernens,*** *die Sicherheitsfunktionen gewährleisten.*

7) Anhang I Teil A Kategorien von Maschinen
5. Sicherheitsbauteile mit vollständig oder teilweise ***selbstentwickelndem Verhalten*** *unter Verwendung von Ansätzen des* ***maschinellen Lernens,*** *die Sicherheitsfunktionen gewährleisten.*

8) Anhang III Teil B 1.1.9 Schutz gegen Korrumpierung
Die Maschine bzw. das dazugehörige Produkt muss so konstruiert und gebaut sein, dass der Anschluss von einer anderen Einrichtung an die Maschine oder das dazugehörige Produkt durch jede Funktion der angeschlossenen Einrichtung selbst oder über eine mit der Maschine bzw. dem dazugehörigen Produkt kommunizierende entfernte Fernzugriffseinrichtung nicht zu einer gefährlichen Situation führt.
Ein Hardware-Bauteil, das Signale oder Daten überträgt, die für den Anschluss oder den Zugriff auf die ***Software*** *relevant sind, die für die Übereinstimmung einer Maschine oder eines dazugehörigen Produkts mit den einschlägigen Sicherheits- und Gesundheitsschutzanforderungen von entscheidender Bedeutung ist, muss so konstruiert sein, dass es angemessen gegen unbeabsichtigte oder vorsätzliche Korrumpierung geschützt ist. Maschinen bzw. dazugehörige Produkte müssen Beweise für ein rechtmäßiges oder unrechtmäßiges Eingreifen in das genannte Hardware-Bauteil sammeln, soweit es für den Anschluss oder den Zugriff auf die* ***Software*** *relevant ist, die für die Konformität der Maschinen bzw. dazugehörigen Produkte von entscheidender Bedeutung ist.*

Software *und Daten, die für die Übereinstimmung der Maschine oder des dazugehörigen Produkts mit den einschlägigen Sicherheits- und Gesundheitsschutzanforderungen von entscheidender Bedeutung sind, sind als solche zu benennen und angemessen gegen unbeabsichtigte oder vorsätzliche Korrumpierung zu schützen.*

Die Maschine bzw. das dazugehörige Produkt muss die installierte ***Software****, die für den sicheren Betrieb erforderlich ist, kenntlich machen und diese Informationen jederzeit in leicht zugänglicher Form bereitstellen können.*

Maschinen bzw. dazugehörige Produkte müssen Nachweise für ein rechtmäßiges oder unrechtmäßiges Eingreifen in die ***Software*** *oder eine Veränderung der in Maschinen bzw. dazugehörigen Produkte installierten* ***Software*** *oder ihrer Konfiguration sammeln.*

9) Anhang III Teil B 1.2.1
*Steuerungen müssen so ausgelegt und beschaffen sein, dass b) ein Defekt der Hardware oder der **Software** der Steuerung nicht zu Gefährdungssituationen führt; c) Fehler in der Logik des Steuerkreises nicht zu Gefährdungssituationen führen; f) das Rückverfolgungsprotokoll der Daten, das im Zusammenhang mit einem Eingreifen generiert wurden, und der Versionen der **Sicherheitssoftware**, die nach dem Inverkehrbringen oder der Inbetriebnahme der Maschine oder des dazugehörigen Produkts hochgeladen wurden, bis zu fünf Jahre nach dem Hochladen ausschließlich für den Nachweis der Konformität der Maschine oder des dazugehörigen Produkts*

10) Anhang III Teil B – Allgemeine Grundsätze
*Die Risikobeurteilung und Risikominderung umfassen Gefährdungen, die im Laufe des Lebenszyklus der Maschinen oder dazugehörigen Produkte auftreten können und die zum Zeitpunkt ihres Inverkehrbringens vorhersehbar sind, da sie sich aus der bestimmungsgemäßen Veränderung ihres vollständig oder teilweise selbstentwickelnden Verhaltens oder ihrer vollständig oder teilweise **selbstentwickelnden Logik** infolge der Auslegung der Maschinen oder dazugehörigen Produkte für einen in wechselndem Maße autonomen Betrieb ergeben. Die Risikobeurteilung und Risikominderung umfassen auch Risiken, die sich aus Wechselwirkungen zwischen Maschinen ergeben, die, damit sie zusammenwirken, so angeordnet sind und betätigt werden, dass sie als Gesamtheit funktionieren und somit eine Maschine im Sinne von Artikel 3 Absatz 1 Buchstabe d bilden.*

11) Anhang IV Teil A
*m) den Quellcode oder die Programmierlogik der Schaltung der sicherheitsrelevanten **Software** zum Nachweis der Konformität der Maschine oder des dazugehörigen Produkts mit dieser Verordnung auf begründeten Antrag einer zuständigen nationalen Behörde, falls dies für die Überprüfung der Einhaltung der grundlegenden Sicherheits- und Gesundheitsschutzanforderungen nach Anhang III durch diese Behörden erforderlich ist*

11. Autorinnen und Autoren

Dieter Käßer ABB STOTZ-KONTAKT GmbH

Jürgen Leng Georg Schlegel GmbH & Co. KG

Manfred Strobel ifm electronic gmbh

Michael Niehaus Lenze SE

Frank Bauder Leuze electronic GmbH + Co. KG

Dipl.-Ing. Klaus Stark PILZ GmbH & Co. KG

Torsten Gast PHOENIX CONTACT ELECTRONICS GmbH

Carsten Gregorius PHOENIX CONTACT GmbH & Co. KG

Urs Dietrich SICK AG

Timo Loeffler SICK AG

Rolf Schumacher SICK AG

Dimitrios Petridis WAGO GmbH & Co. KG

Dr. Markus Winzenick ZVEI e. V.

Franziska Wirths ZVEI e. V.

Impressum

Sichere Software in der
Maschinenverordnung EU 2023/1230

Amelia-Mary-Earhart-Str. 12
60549 Frankfurt am Main

Fachverband Automation
Fachbereich Schaltgeräte, Schaltanlagen,
Industriesteuerungen

Ansprechpartner:
Dr. Markus Winzenick
+49 162 2664-938
markus.winzenick@zvei.org
www.zvei.org

Dezember 2024

zvei
electrifying ideas