

EMV und Funktionale Sicherheit

Zwei Querschnittsdisziplinen treffen sich

A.02

Funktionale Sicherheit ist die Sicherheit vor Gefährdungen, die aus der (fehlerhaften) Funktion einer Einrichtung resultieren. Gestützt auf die IEC 61000-1-2 [1] und IEC 61508 [2] werden Methoden zur Sicherstellung der Funktionalen Sicherheit unter Berücksichtigung elektromagnetischer Phänomene behandelt.

Zur Festlegung und Auswahl angemessener EMV-Anforderungen an sicherheitsrelevante Einrichtungen bedarf es eines intensiven Dialoges zwischen den beiden Disziplinen; zwei unterschiedliche Denkweisen und -ansätze müssen respektiert, verstanden und zu einem gemeinsamen Verständnis zusammengeführt werden.

Grundprinzipien der funktionalen Sicherheit nach IEC 61508

Sicherheit ist aus Sicht des zu schützenden Gutes unteilbar und erfordert den umfassenden Schutz vor Gefährdung verschiedener Ursachen. Technische Maßnahmen zum Erzielen der Sicherheit können, je nach Ursache der möglichen Gefährdung, sehr unterschiedlich sein, deshalb unterscheidet man neuerdings verschiedene Arten von Sicherheit. So spricht man z. B. von ‚elektrischer Sicherheit‘, wenn der Schutz vor der Gefährdung durch Elektrizität zum Ausdruck gebracht werden soll, oder von ‚funktionaler Sicherheit‘, wenn die Sicherheit von der korrekten Funktion einer Einrichtung abhängt. Wichtig ist hier der Fokus auf die korrekte Funktion, d. h. die mögliche Gefährdung resultiert aus dem Versagen oder

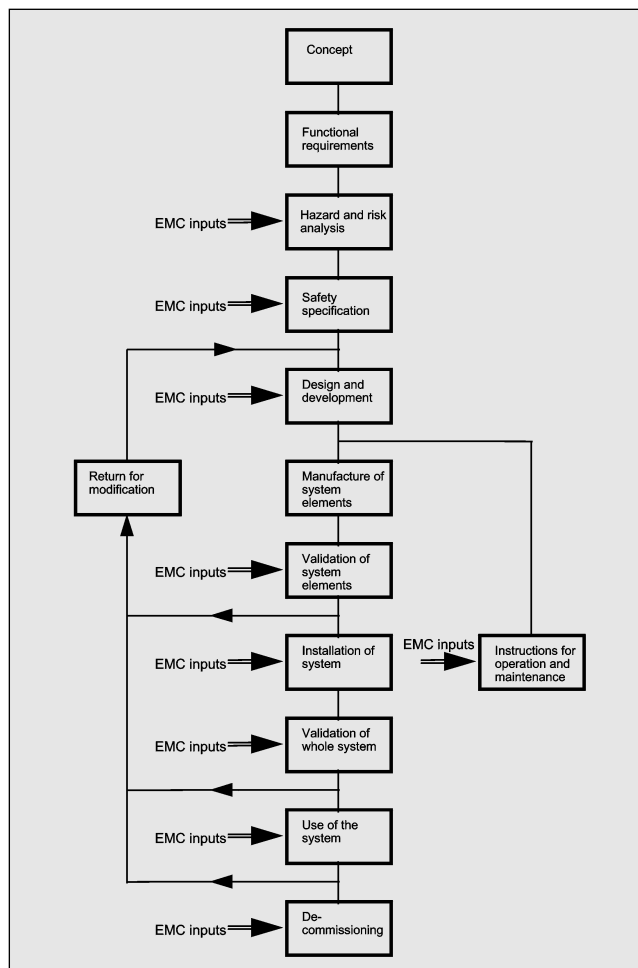


Abb. 1:
Ablaufdiagramm aus IEC 61000-1-2 für die Berücksichtigung der EMV von sicherheitsrelevanten Systemen

dem Fehler einer Funktion. Ein Risiko besteht immer dann, wenn eine Funktion sicherheitsrelevant ist und das Versagen der Funktion zu einer Gefährdung führen kann.

Ein wesentlicher Parameter zur Qualifizierung eines Risikos ist neben der Größe des Schadens die Wahrscheinlichkeit für das Eintreten des gefährlichen Ereignisses. Aus dieser Betrachtung leitet sich das Risiko-orientierte, probabilistische Prinzip von IEC 61508 ab. Durch sicherheitsrelevante Steuer- oder Überwachungsfunktionen wird die Wahrscheinlichkeit für das Eintreten eines gefährlichen Ereignisses um die Versagenswahrscheinlichkeit dieser Funktion verhindert. Die Norm verwendet für dieses Maß den Begriff ‚Safety Integrity‘ und definiert dazu 4 konkrete Stufen, ‚Safety Integrity Level‘ genannt (Tabellen 2 und 3).

Fehlerarten

Bei der Betrachtung möglicher Ursachen für die inkorrekte Ausführung einer Funktion durch Steuerungssysteme oder deren Versorgungsanlagen unterscheidet man verschiedene Ausfall- bzw. Fehlerarten. Dabei wird bzgl. der möglichen Auswirkungen zwischen ‚safe failure‘ und ‚dangerous failure‘ (siehe Tabelle 3) und im Bezug auf die Ausfallursache zwischen ‚systematic failure‘ und ‚random hardware failure‘ unterschieden. Jede Fehlerart kann natürlich jede der genannten Ursachen haben. In Bezug auf Sicherheit ist nur die Wahrscheinlichkeit gefährlicher Fehler bzw. Ausfälle (failures) von Bedeutung, unabhängig von ihrer Ursache.

Für die Bestimmung der Ausfallwahrscheinlichkeit ist jedoch die Fehlerursache wichtig. Im Zusammenhang mit ‚random hardware failures‘ können Ausfallwahrschein-

Autoren

HARTMUT VON KROSIGK ist tätig in der Abteilung A&D ATS 4; Gleiwitzer Straße 555, D-90475 Nürnberg
Fon: 09 11/895-2845, Fax: 09 11/895-4903
E-Mail: hartmut.krosigk@nbgm.siemens.de

ANTON KOHLING ist tätig in der Abteilung A&D ATS SR bei Siemens A&D; Paul-Gossen-Str. 100, D-91050 Erlangen
Fon: 091 31/7-3 1453, Fax: 091 31/7-2 5007
E-Mail: anton.kohling@erl6.siemens.de

Tabelle 1: In IEC 61000-2-5 aufgeführte Elektromagnetische Phänomene

Niederfrequente Phänomene auf Leitungen	<ul style="list-style-type: none"> • Oberschwingungen, Zwischenharmonische • Signalspannungen • Spannungsschwankungen, Spannungseinbrüche, Kurzzeitunterbrechungen • Spannungsunsymmetrie • Frequenzvariation • Gleichanteile in Wechselstromnetzen
Niederfrequente Felder	<ul style="list-style-type: none"> • Netzfrequente Magnetfelder • Impulsförmiges Magnetfeld • Gedämpft schwingendes Magnetfeld
Hochfrequente Phänomene auf Leitungen	<ul style="list-style-type: none"> • 100/1300 ms Stoßspannung/-strom • Blitz 1,2/50 us- 8/20 us; Stoßspannung/-strom • Blitz 10/700 us (Telekom.) • Burst n x 5/50 nsec • Ring waves 0,5 us/100 kHz • gedämpfte Welle 0,1 und 1 MHz • hochfrequente induzierte Spannung
Hochfrequente Strahlung	<ul style="list-style-type: none"> • Elektromagnetisches Feld • Magnet-Feld • Elektrisches Feld
Entladung statischer Elektrizität	<ul style="list-style-type: none"> • ESD • HEMP Elektromagnetischer Impulse

lichkeiten berechnet werden, da die verursachenden Fehler zufällig auftreten. Bei systematischen Fehlern ist dies kaum möglich. Sie sind permanent im System vorhanden und werden abhängig von bestimmten Ereignissen (z.B. Funktionsabläufen oder Umgebungsbedingungen) wirksam. Deshalb kann eine Wahrscheinlichkeit für ihr Auftreten im Allgemeinen nicht bestimmt werden. IEC 61508 wendet folglich im Zusammenhang mit systematischen Fehlern die probabilistische Betrachtung nicht an, sondern verlangt angemessene Maßnahmen zu ihrer Vermeidung oder Beherrschung.

Der Einfluss elektromagnetischer Phänomene wird unter dem Gesichtspunkt systematischer Fehler behandelt, dabei sind auch ‚common cause failure‘ zu beachten. Die EMV ist durch entsprechendes Design sicherzustellen und mittels Prüfung nachzuweisen.

Safety Requirements Specification (SRS)

Ausgangsbasis für die Entwicklung eines sicherheitsrelevanten Systems ist eine ‚Safety Requirements Specification‘, in der alle Funktionen mit ihren Sicherheitseigenschaften sowie die zugehörigen Umgebungsbedingungen festgelegt sind. Diese Festlegungen resultieren aus einer anwendungsbezogenen Gefährdungs- und Risiko-Analyse mit deren Hilfe die sicherheitsrelevanten Funktionen bestimmt werden, der jeweils notwendige SIL gewählt wird und die Umgebungsbedingungen einschließlich der EMV-Anforderungen

festgeschrieben werden. Analyse und Spezifikation sind im Aufgabenbereich der für die Anlage verantwortlichen Planer. Der Steuerungshersteller muss die Spezifikation erfüllen und mit entsprechenden Methoden an seinen Produkten nachweisen. Bezüglich der Auswahl der relevanten EM-Phänomene und zugeordneten Prüfpegel verweist ICE 61508-2 [3] in Kapitel 7.2.3.2 auf IEC 61000-2-5 [5]. Hier ist EMV-Fachwissen gefragt.

Elektromagnetische Phänomene

Der Verweis und IEC 61000-2-5 erfordert für die Spezifikation der sicherheitsrelevanten Einrichtung und den Nachweis der Anforderungen die Berücksichtigung der dort beschriebenen EM-Phänomene und der umgebungsspezifischen Verträglichkeitspegel. Tabelle 1 gibt einen Überblick über die behandelten EM-Phänomene. Diese sind in [5] in 13 Tabellen detailliert beschrieben, in dem bis zu 6 verschiedene Pegel begründet werden. Die Auswertung dieser Tabellen führt zu mehr als 30 unterschiedlichen EM-Phänomenen. Im Anhang A von IEC 61000-2-5 sind die Verträglichkeitspegel für 8 typische

Umgebungen in Tabellenform dargestellt. Die Verträglichkeitspegel für die industrielle Umgebung sind in Tabelle 5 von IEC 61000-2-5 beschrieben. Vergleicht man diese Tabelle mit den Anforderungen in den Fachgrundnormen, so sind in der EN 61000-6-2 [6] lediglich 7 der über 30 in IEC 61000-2-5 [5] aufgeführten EM-Phänomene spezifiziert.

Eine vergleichende Gegenüberstellung zeigt, einige der in [6] spezifizierten Störfestigkeitspegel liegen unterhalb der in [5] angegebenen Verträglichkeitspegel. Dies ist nicht verwunderlich, den die Fachgrundnormen basieren auf einer gesunden Mischung aus technischen und wirtschaftlichen Überlegungen für den ungehinderten Marktzugang der Produkte im Binnenmarkt. Was ist zu tun, wer wählt die sicherheitsrelevanten EM-Phänomene und die angemessenen Prüfpegel mit welcher Begründung aus? Helfen sollen die in IEC 61000-1-2 angegebenen Methoden. Aber ist dem auch so? Die Auswahl der Phänomene und die Festlegung von ‚safety margins‘ ist ohne Begründung angegeben.

Ein Blick auf die Ablaufdiagramme (Abb. 1) in IEC 61000-1-2 zeigt: Auswahl und Festlegung muss einsetz- und aufgabenspezifisch erfolgen. Welch ein dauerhaftes Arbeitsbeschaffungsprogramm! Zur Reduzierung des zu wiederholenden Aufwandes sind die Betroffenen gut beraten, für typische Einsatzbedingungen und Anwendungen, Richtlinien zu erstellen bei deren Berücksichtigung die funktionale Sicherheit in Übereinstimmung mit den ‚Safety Requirements Specification‘ ohne überzogene EMV-Anforderungen erfüllt wird.

‚Safety margins‘ und Performance-Kriterien

Basierend auf individuellen oder auch beispielhaften Analysen wird die Definition von system- und anwendungsspezifischen ‚safety margins‘ für bestimmte EM-Phänomene notwendig werden. Diese ‚safety margins‘ sind aber nur auf die sicherheitsrelevante Funktion mit einem eigenen sicherheitsrelevanten Ausfallkriterium (Performance Kriterium) anzuwenden. Ein solches zusätzliches Performance-Kriterium könnte lauten:

Die Funktion eines Systems darf vorübergehend oder dauerhaft gestört werden, wenn das betreffende System in der Lage ist, auf diese Störung so zu reagieren, dass ein sicherer

Tabelle 2: Sicherheits-Integritätslevel (SIL; Safety Integrity Levels)

SIL 1	Nicht mehr als ein gefährlicher Ausfall der Sicherheitsfunktion in 10 Jahren
SIL 2	Nicht mehr als ein gefährlicher Ausfall der Sicherheitsfunktion in 100 Jahren
SIL 3	Nicht mehr als ein gefährlicher Ausfall der Sicherheitsfunktion in 1.000 Jahren
SIL 4	Nicht mehr als ein gefährlicher Ausfall der Sicherheitsfunktion in 10.000 Jahren

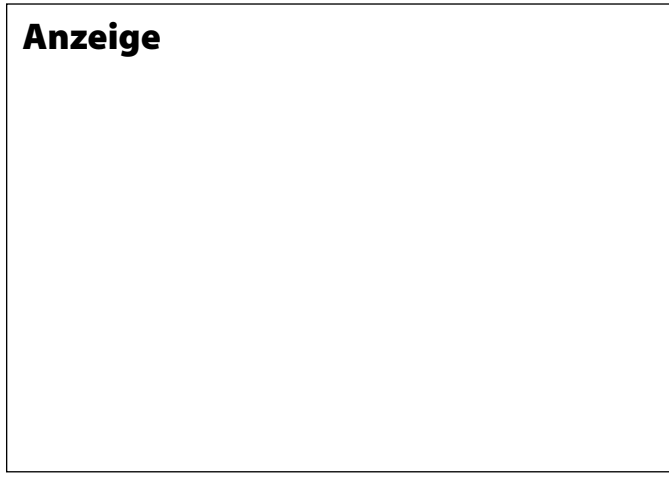
Zustand erreicht oder erhalten wird. Dieses Kriterium sollte für alle relevanten EM-Phänomene gelten und dabei nicht zwischen kontinuierlichen und transienten Störgrößen unterschieden werden.

Sicherheitsanforderungen in EG-Richtlinien für die CE-Kennzeichnung

Aufgabe der EG-Richtlinie ist der Abbau von Handelshemmnissen durch Harmonisierung der Regulierung in den Mitgliedstaaten.

In dem Neuen Konzept [7] ist folgendes grundlegende Prinzip festgelegt:

„Die Harmonisierung der Rechtsvorschriften beschränkt sich auf die Festlegung der grundlegenden Sicherheitsanforderungen (oder sonstigen Anforderungen im Interesse des Gemeinwohls) im Rahmen von Richtlinien nach Artikel 100 des EWG Vertrages, denen die in den Verkehr gebrachten Erzeugnisse genügen müssen ...“



Die EMV-Richtlinie beinhaltet keine Sicherheitsanforderungen. Sicherheitsaspekte sind umfassend in der Niederspannungsrichtlinie als horizontale Anforderung und in vertikalen Richtlinien wie z.B. der Maschinen-Richt-

linien, der Medizinprodukterichtlinie, der R&TTE-Richtlinie usw. reguliert.

Zusammenfassung

EMV und Sicherheit werden und wurden in den letzten Jahren oft kontrovers diskutiert und mit Zuverlässigkeits- und Verfügbarkeitsanforderungen vermischt. Die objektive Betrachtung dieser Verknüpfung bedarf eines fundierten Grundwissens beider Themenfelder. Es ist weiterhin mit normativen Festlegungen und gesetzlichen Anforderungen zu rechnen. Zur Formulierung ausgewogener und aufeinander abgestimmter Anforderungen ist eine Koordination innerhalb nationaler und internationaler Normungsgremien unerlässlich.

Literatur

- [1] IEC 61000-1-2; Electromagnetic Compatibility (EMC) – Part 1: General – Section 2: Methodology for the achievement of the functional safety of electrical and electronic equipment
- [2] IEC 61508; Functional safety of electrical/electronic/programmable electronic safety-related systems
- [3] IEC 61508-2; Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems
- [4] IEC 61000-1-1; Electromagnetic compatibility (EMC) - Part 1: General; Section 1: Application and interpretation of fundamental definitions and terms
- [5] IEC 61000-2-5; Electromagnetic compatibility (EMC) - Part 2: Environment; Section 5: Classification of environments
- [6] IEC 61000-6-2; Electromagnetic compatibility (EMC) - Part 6-2: Generic standards - Immunity for industrial environments
- [7] COUNCIL RESOLUTION of 7 May 1985 on a new approach to technical harmonization and standards (85/C 136/01)

Tabelle 3: Ausgewählte Definitionen zur funktionalen Sicherheit	
<p>Funktionale Sicherheit</p> <p>Teil der Gesamtsicherheit, bezogen auf die EUC und die EUC-Betriebseinrichtung, die von der korrekten Funktion des E/E/PE-sicherheitsbezogenen Systems, Sicherheitssystemen anderer Technologie und externer Einrichtungen zur Risikominderung abhängt</p>	<p>Ungefährlicher Ausfall</p> <p>Ausfall ohne das Potential, das sicherheitsbezogene System in einen gefährlichen oder funktionsunfähigen Zustand zu setzen</p>
<p>Sicherheitsfunktion</p> <p>Funktion, die von einem E/E/PE-sicherheitsbezogenem System, einem sicherheitsbezogenem System anderer Technologie oder externer Einrichtungen zur Risikoreduzierung ausgeführt wird mit dem Ziel, unter Berücksichtigung eines festgelegten unerwünschten Ereignisses (siehe 3.4.1), einen sicheren Zustand für die EUC zu erreichen oder aufrechtzuerhalten</p>	<p>gefährlicher Ausfall</p> <p>Ausfall mit dem Potenzial, das sicherheitsbezogene System in einen gefährlichen oder funktionsunfähigen Zustand zu setzen</p>
<p>Sicherheitsintegrität</p> <p>Wahrscheinlichkeit, dass ein sicherheitsbezogenes System die geforderten Sicherheitsfunktionen unter allen festgelegten Bedingungen innerhalb eines festgelegten Zeitraumes anforderungsgemäß ausführt</p>	<p>Zufälliger Hardwareausfall</p> <p>Ausfall, der zu einem zufälligen Zeitpunkt auftritt und der aus einem oder mehreren möglichen Mechanismen in der Hardware resultiert, die zu einer Verschlechterung der Eigenschaften der Bauteile führen</p>
<p>Sicherheits-Integritätslevel (SIL)</p> <p>eine von vier diskreten Stufen zur Spezifizierung der Anforderung für die Sicherheitsintegrität der Sicherheitsfunktionen, die dem E/E/PE-sicherheitsbezogenen System zugeordnet werden, wobei der Sicherheits-Integritätslevel 4 die höchste Stufe der Sicherheitsintegrität und der Sicherheits-Integritätslevel 1 die niedrigste darstellt</p>	<p>Systematischer Ausfall</p> <p>Ausfall, bei dem eindeutig auf eine Ursache geschlossen werden kann, die nur durch eine Veränderung des Entwurfs oder des Fertigungsprozesses, der Art und Weise des Betriebes, der Bedienungsanleitung oder anderer Einflussfaktoren beseitigt werden kann.</p>
	<p>Ausfall infolge gemeinsamer Ursache</p> <p>Ausfall, der das Ergebnis eines oder mehrerer Ereignisse ist, die gleichzeitige Ausfälle von zwei oder mehreren getrennten Kanälen in einem mehrkanaligen System verursachen und zu einem Systemausfall führen</p>
	<p>Spezifikation der Sicherheitsanforderungen</p> <p>Spezifikation, die alle Anforderungen an die Sicherheitsfunktionen beinhaltet, die vom sicherheitsbezogenen System ausgeführt werden müssen</p>