20 IEC/EN 61508

Weltweit gibt es eine Vielzahl unterschiedlicher Gremien, die sich die Spezifikation von Normen und Standards bezüglich der Vorgehensweise bei der Entwicklung, der Verifikation und dem Einsatz sicherheitskritischer Systeme zur Aufgabe gemacht haben. Beim Einsatz von hochkritischen Systemen ist die Notwendigkeit der Zertifizierung der Systeme nach den für deren Einsatz gültigen Normen und Richtlinien durch eine Aufsichtsbehörde als Standard beim Betrieb solcher Anlagen vorgesehen.

Die Anwendung von sicherheitsgerichteten Computersystemen in verschiedenen Industriebereichen hat zu einer Fülle an Erfahrungen und Wissen in diesem Bereich geführt. Dieses Wissen liegt meist in kompakter Art in Form von Standards und Richtlinien vor, die dem Entwicklungsingenieur helfen sollen, bei den zukünftig zu entwickelnden Systemen ein einheitlich hohes Niveau an Qualität und Sicherheit zu erreichen. Sicherheitsgerichtete Systeme müssen für ihren Einsatzzweck bestimmte Standards erfüllen, die die Entwicklungsmethoden und die Systemanforderungen festlegen. Die Zertifizierung des endgültigen Gesamtprozesses und des diesen Prozess steuernden Sicherheitssystems hängt vom Einhalten dieser Standards und den Kriterien, die sie definieren, ab. Nicht in allen Industriebereichen ist die Einhaltung von Standards so strikt geregelt wie beim Einsatz in der sicherheitsgerichteten MSR[188]- und ESD[189]-Technik. Neben den formellen Standards existieren zusätzlich verschiedene Richtlinien, aus denen sich Notwendigkeiten bei der Systementwicklung ableiten lassen.

Industriespezifische Standards und Richtlinien, wie in der chemischen-, petrochemischen, Luftfahrt-, Atom- sowie Bergbauindustrie, beschreiben jeweils die Hauptgefahren dieser Industrien. Die verbleibenden Risiken, die mit den Anforderungen an die Zuverlässigkeit und die Verfügbarkeit letztlich einhergehen, werden durch Überlegungen der Aufsichtsbehörden und der Industrie selbst definiert und geregelt. Hieraus ergeben sich dann die Standards für Sicherheitsanforderungen an Systeme des spezifischen Industriesektors. Generellere Standards und Richtlinien beziehen sich dagegen auf alle Industriebereiche.[190, 191]

Die IEC[192] entwickelt und verwaltet Normen in Zusammenarbeit mit nationalen Komitees. Dazu werden Arbeitsgruppen eingesetzt, die sich jeweils mit einem Schwerpunktthema auseinandersetzen. Beispielhaft sei hier das „Technical Committee 65“ genannt, das für „Messen und Regeln in industriellen Prozessen“ verantwortlich ist. Von ihm stammt das im Folgenden näher beschriebene Dokument „IEC 61508: Functional Safety: Safety related Systems“. Die IEC 61508, die auch als Sicherheitsgrundnorm bezeichnet wird, beschreibt

---

[188] MSR-Technik: Mess-, Steuer- und Regelungstechnik
[189] ESD-Technik: Electronic-Shut-Down-Technik
[190] [HSE-87] HSE, *Programmable Electronic Systems in Safety-Related Applications*; *An Introductory Guide*. Health and Safety Executive. London: Her Majesty’s Stationery Office
[191] [IECa02] IEC 61508, Functional Safety; Safety-Related Systems.
[192] International Electrotechnical Commission

den grundsätzlichen, kompletten Lebenszyklus von sicherheitsgerichteten Systemen. Sie ist in sieben Teile unterteilt, wobei die Teile 1, 2, 3 und 4 auch als Sicherheits-Grundnorm verwendet und durch technische Komitees bei der Erstellung von Normen nach IEC Guide 104 und ISO/IEC Guide 51 herangezogen werden.

Neben der IEC 61508 wird im nächsten Kapitel auch die IEC 61511 beschrieben. Der Gruppentitel dieser Norm lautet: „Functional safety: Safety Instrumented Systems for the process industry sector“,[193] auf deutsch: „Funktionale Sicherheit: Sicherheitstechnische Systeme für die Prozessindustrie“.[194] Diese internationale Norm behandelt die Anwendung sicherheitstechnischer Systeme in der Prozessindustrie. Sie ist die Anwendung der IEC 61508 für die Verfahrenstechnik und fordert die Durchführung einer Gefährdungs- und Risikoanalyse. Aus dieser Analyse kann dann eine Spezifikation für sicherheitstechnische Systeme erstellt werden.

20.1 IEC/EN 61508-1

20.1.1 Übersicht und Anwendungsbereich

Für einen Anlageninhaber ist es unabdingbar, ein ausreichendes Sicherheitsmanagement einzurichten. Falls im Falle eines Unfalls das sicherheitsbezogene System nicht mit dem vorgegebenen Standard übereinstimmt, könnte die Firma für die Vernachlässigung der passenden Sicherheitsrichtlinien haftbar gemacht werden. Dementsprechend ist eine angemessene Sicherheitstechnik, die mit dem internationalen Standard übereinstimmt, für spätere Wartungen und firmenfremde Unternehmen erforderlich. Die IEC 61508 ist eine internationale Norm, welche von der Internationale Elektrotechnische Kommission (IEC) 1999 herausgegeben wurde. Sie bezieht sich auf alle Aspekte, die mit der Nutzung von E/E/PES (elektrischen / elektronischen / programmierbaren elektronischen Systemen) für sicherheitsrelevante Funktionen und Anwendungen zusammenhängen. Sie ist grundlegend anwendbar auf alle sicherheitsbezogenen E/E/PES, insbesondere wenn für ein Anwendungsgebiet keine spezielle Sicherheitsnorm existiert. Die Norm IEC 61508 umfasst die folgenden sieben Teile (61508-1 bis 61508-7) (siehe auch Bild 20.1):

- Teil 1: Allgemeine Anforderungen;
- Teil 2: Anforderung an sicherheitsbezogene elektrische/elektronische/programmierbar elektronische Systeme;
- Teil3: Anforderungen an Software;
- Teil 4: Begriffe und Abkürzungen;
- Teil 5: Beispiele zur Ermittlung der Stufe der Sicherheitsintegrität;
- Teil 6: Anwendungsrichtlinie für IEC 61508-2 und IEC 61508-3;
- Teil 7: Anwendungshinweise über Verfahren und Maßnahmen.

[193] [IEC-02] IEC 65A/324/FDIS 2002, *Functional safety: Safety Instrumented Systems for the process Industry sector*

[194] [DIN-03] DIN IEC 61511, Teil 1 bis 3, (VDE 0810 Teil 1), *Funktionale Sicherheit: Sicherheitstechnische Systeme für die Prozessindustrie*

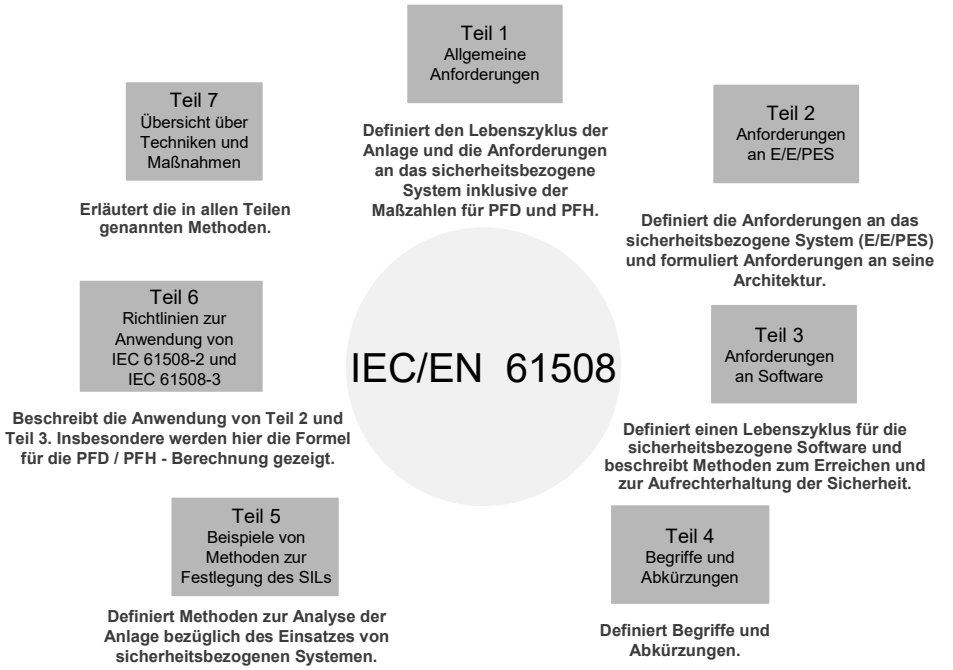

Bild 20.1: Überblick über die Teile der IEC/EN 61508

Diese Norm ermöglicht eine systematische, risikobasierte Herangehensweise an sicherheitsrelevante Probleme. Teil 1 dieser Norm spezifiziert die allgemeinen Anforderungen, die auf sämtliche anderen Teile anwendbar sind. Teil 2 und 3 definieren zusätzliche Anforderungen an die Hard- und Software der Systeme. Teil 4 erklärt die in dieser Norm benutzten Definitionen und Abkürzungen. Teil 5 liefert Richtlinien für die Anwendung von Teil 1, Teil 6 solche für Teil 2 und 3. Teil 7 schließlich enthält einen Überblick über Vorgehensweisen und Maßnahmen.

Diese Internationale Norm betrachtet alle relevanten sicherheitsbezogenen Phasen des Gesamtkonzepts der E/E/PES und des Software-Sicherheits-Lebenszyklus vom Konzept, über Entwurf, Durchführung, Betrieb und Instandhaltung bis zur Außerbetriebnahme. Sie ermöglicht die Erstellung anwendungsspezifischer internationaler Normen, die sich mit sicherheitsbezogenen E/E/PES befassen. Des Weiteren liefert sie eine Methode für die Entwicklung der Spezifikation der Sicherheitsanforderungen, die notwendig sind, um die geforderte funktionale Sicherheit des sicherheitsbezogenen E/E/PE-Systems zu erreichen. Sie verwendet das Sicherheits-Integritätslevel für die Spezifikation der Zielvorgabe der Sicherheitsintegrität der Sicherheitsfunktionen. Für die Festlegung der Anforderungen der Sicherheits-Integritätslevel verwendet sie einen auf dem Risiko basierenden Lösungsansatz. Für die sicherheitsbezogenen Systeme wird eine numerische Ausfallgrenze gesetzt.

Die Norm ist allgemeingültig und auf alle sicherheitsbezogenen Systeme anwendbar.

Bild 20.2 zeigt die Zuordnung der Teile der Norm zu den Anforderungen bezüglich des Sicherheitslebenszyklus. Die Anforderungen unterscheiden zwischen technischen und anderen Anforderungen (z. B. Dokumentation, Management of Functional Safety).

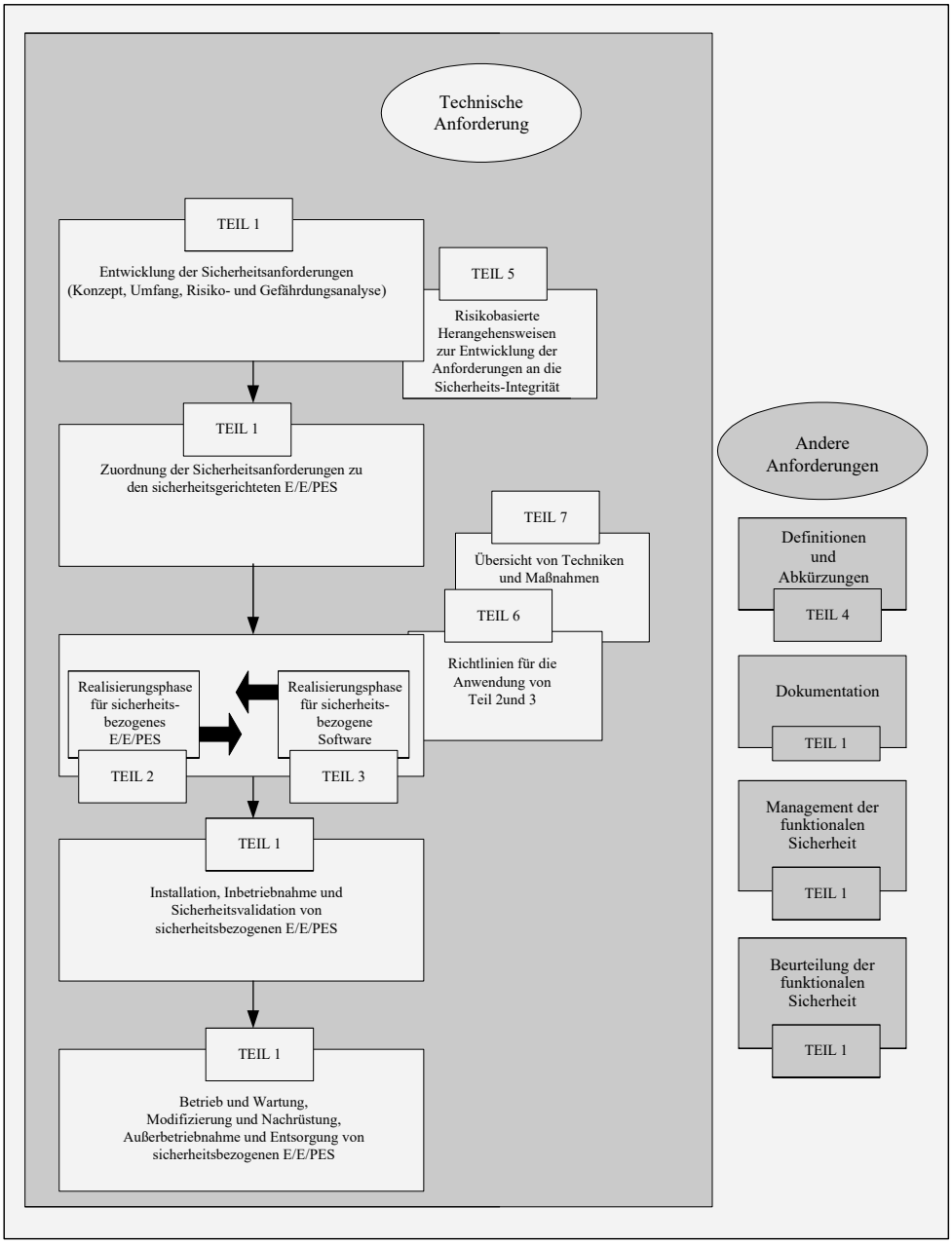

Bild 20.2: Gesamtstruktur der IEC/EN 61508