Michael Kieviet (innotec GmbH):

# IEC 61508 – Umfassende Sicherheit für Maschinen und Anlagen

## Sichere Produkte – Sichere Organisation

Jeder, der sich mit elektrischer oder elektronischer Maschinen- oder Anlagensicherheit beschäftigt, stößt zwangsläufig auf die internationale Norm IEC 61508, auch als DIN EN 61508 sowie VDE 0803 bekannt. Dieser Standard regelt applikationsunabhängig die einheitliche Vorgehensweise bei der Entwicklung von sogenannten elektrisch / elektronisch / programmierbaren Systemen. Hervorgegangen aus dem mittlerweile zurückgezogenen nationalen Standard DIN-V-VDE 0801, etabliert sich diese Norm weltweit als Marktanforderung für die Sicherheitstechnik.

Neben dem vordergründigen Anspruch, Schutz für Leben und Gesundheit des Menschen zu bieten, findet dieses Regelwerk auch Anklang im Bereich Umweltschutz und bei der Gefahrenabwehr von wirtschaftlichen Schäden. Durch seine klar strukturierten Vorgehensweisen, gerade im Bereich der Softwareentwicklung, nutzen viele Branchen auszugsweise die IEC 61508 - auch im nicht sicherheitsrelevanten Bereich - um die Verfügbarkeit ihrer Produkte zu erhöhen.

In den zahlreichen Artikeln einschlägiger Fachzeitschriften zeichnet sich ein eindeutiger Trend zu immer sichereren Produkten ab. Dieser Bedarf ist auch auf Kundenseite klar zu erkennen.

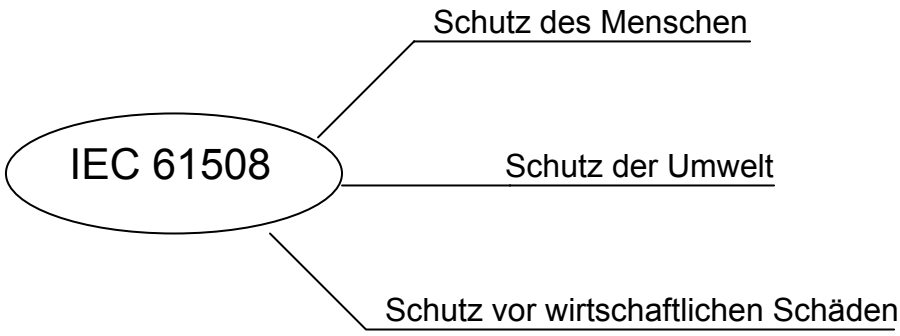


**Abb. 1: Einsatzmöglichkeit der IEC 61508**

## Normen-Dschungel

Mit der Idee, Sicherheitstechnik nach dem neuesten Stand der Technik zu entwickeln, stellt sich für viele das Problem: Wie setze ich diese Norm überhaupt ein?

Erfahrungsgemäß tun sich Umsteiger (also Firmen, die lange Jahre Erfahrung im Bereich der Sicherheitstechnik mitbringen) dabei genau so schwer wie Neulinge. Dies liegt vor allem an der neuartigen Philosophie, die hinter den aktuellen Sicherheitsstandards steht.

Natürlich gibt es auch viele Mutmaßungen, wie z.B.:

- dass Entwickler nicht mehr in der Lage wären, eine Schaltung zu designen, weil sie mehr Sicherheitsmängel zu sehen glaubten, als tatsächlich vorhanden wären.
- dass es Firmen gebe, die seit der Einführung der neuen Normen keine Produkte mehr auf den Markt gebracht hätten, da sie nur noch mit der Dokumentation und dem Ausfüllen der Checklisten beschäftigt seien.

Die Hauptschwierigkeit liegt oftmals nicht in der Realisierung der Technik, sondern vielmehr im Bereich des Sicherheitsmanagements.

**Lebenszyklusmodell**

Die IEC 61508 beruft sich bei einem Produkt auf das Lebenszyklusmodell: Die Lebensphasen, angefangen vom ersten Brainstorming bis zu dem Zeitpunkt, an dem das Produkt außer Betrieb genommen und entsorgt wird, geraten nun in den Fokus. Betrachtet man die einzelnen Schritte eines Produktlebenszyklus, kristallisiert sich sehr schnell heraus, dass die gesamte Organisation einer Firma von der Norm betroffen ist. Die Richtlinien der Norm erstrecken sich nun vom Produktmarketing über die Entwicklung, den Einkauf, die Qualitätssicherung, den Vertrieb und Support bis hin zum Kunden. Da alle Abteilungen auch koordiniert und beauftragt werden müssen, versteht sich von selbst, dass übergeordnete Hierarchien mit einbezogen sind.

Es ist vor allem wichtig, klar zu definieren: Wer ist wofür und wann zuständig?

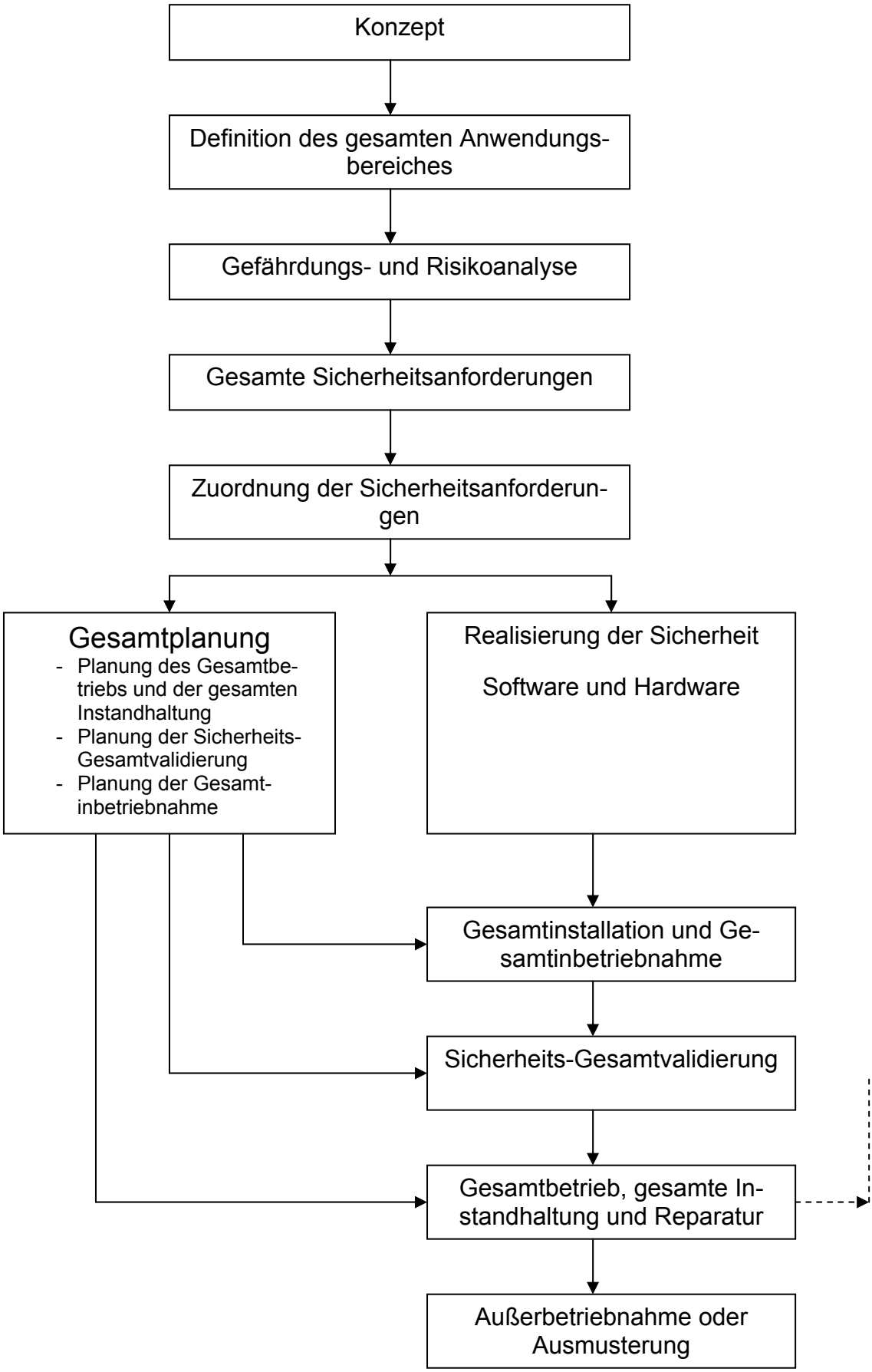


**Abb. 2: Produkt-Lebenszyklusmodell**

Abweichend von dem dargestellten Lebenszyklus fordern Kunden von Komponentenherstellern einen entsprechenden Sicherheitslevel (Safety Integrity Level = SIL), so dass eine Risikobetrachtung der Applikation häufig verlagert wird. Sollte diese nicht bereits feststehen, sei hier auf den Teil 5 der IEC 61508 verwiesen.

Für den Komponentenhersteller (wobei hier der gesamte Bereich von Sensor-, Steuerungs-, und Antriebsherstellern gemeint ist) stellt sich dann „nur" noch die Frage, wie er sein Produkt in eine entsprechende Sicherheitskategorie bringen kann. Allerdings sei gleich dazu gesagt, dass es ganz ohne das Wissen um die zukünftigen Applikationen nicht geht. Der häufige Wunsch, eine einzige Steuerung für jeden Einsatzbereich zu entwickeln, kann nie realisiert werden.

Deshalb muss sich jeder Hersteller zunächst einmal Gedanken über den typischen Einsatzort und die typische Anwendung machen. Mit dieser Überlegung treten gleichzeitig eine ganze Anzahl von Forderungen an die Umweltbedingungen auf, wie Temperaturbereiche, EMV, Schwingungen, Gehäuse etc. Hier ist größte Sorgfalt geboten, da häufig schon zu klein gewählte Gehäuse oder falsch gewählte Temperaturbereiche enorme Aufwendungen in fortgeschrittenen Entwicklungsphasen verursacht haben. Man kann beispielsweise davon ausgehen, dass ein Layout für eine Platine 60% bis 70% größer ausfällt als das einer Standardentwicklung.

Ist der Sicherheitsintegritätslevel bekannt, so muss noch in Erfahrung gebracht werden, welche Art der Anforderungsrate an die Sicherheit gestellt wird. Die Norm unterscheidet hier zwischen einem „Low-Demand" und einem „High-Demand" (also einer niedrigen Anforderungsrate oder einer hohen Anforderungsrate). Leider tauchen in diesem Zusammenhang schon die ersten Probleme auf: Wann benötige ich was? Die Norm gibt hierzu zwar eine Erklärung, diese sorgt aber nicht für endgültige Klarheit. Prinzipiell kann man sagen, dass Systeme, die nur sehr selten eine Sicherheitsauslösung erfahren, zu den Low-Demand Systemen gehören. Hier ist das beste Beispiel der Notaus-Taster. Der Notaus-Taster dient nur dazu, in einer Gefahrensituation betätigt zu werden, um dann auch garantiert den sichereren Zustand einzuleiten. Natürlich darf hierzu nicht der Notaus-Taster isoliert betrachtet werden, sondern es muss immer die gesamte Notaus-Kette von Sensor bis zum Aktor beachtet werden.
„High-Demand" wird immer dort gefordert, wo sicherheitsrelevante Aktionen ständig erfolgen, wie z.B. beim Laserscanner oder einer sicheren Regelung im Roboterbereich.
Die Unterschiede machen sich auch sehr stark bei der mathematischen Betrachtung der Sicherheit bemerkbar. Die quantitative Einordnung erfolgt über die Ausfallwahrscheinlichkeit der Sicherheitsfunktion. Beim „Low-Demand" wird eine bestimmte Ausfallwahrscheinlichkeit pro Sicherheitsanforderung gefordert. Bei der „High-Demand"-Forderung hingegen, wird die Ausfallwahrscheinlichkeit pro Stunde betrachtet.

| SIL | Betriebsart mit niedriger Anforderungsrate „Low-Demand" |
|---|---|
| 4 | $\geq 10^{-5}$ bis $<10^{-4}$ |
| 3 | $\geq 10^{-4}$ bis $<10^{-3}$ |
| 2 | $\geq 10^{-3}$ bis $<10^{-2}$ |
| 1 | $\geq 10^{-2}$ bis $<10^{-1}$ |

Mittlere Ausfallwahrscheinlichkeit der entworfenen Funktion bei Anforderung

| SIL | Betriebsart mit hoher Anforderungsrate „High-Demand" |
|---|---|
| 4 | $\geq 10^{-9}$ bis $<10^{-8}$ |
| 3 | $\geq 10^{-8}$ bis $<10^{-7}$ |
| 2 | $\geq 10^{-7}$ bis $<10^{-6}$ |
| 1 | $\geq 10^{-6}$ bis $<10^{-5}$ |

Wahrscheinlichkeit eines Gefahr bringenden Ausfalls pro Stunde

Ein Vergleich beider Tabellen lässt nicht automatisch den Schluss zu: „High-Demand“ ist besser als „Low-Demand“. Um dieses zu beurteilen, müsste bei einem „Low-Demand“-System bekannt sein, wie groß die mittlere Anforderungswahrscheinlichkeit der Sicherheitsfunktion ist. Kann man beispielsweise definieren, dass der NOT-AUS einmal im Jahr zur Sicherheitsabschaltung verwendet wird, ist die Umrechnung in Ausfallwahrscheinlichkeit pro Stunde möglich und somit auch der Vergleich der beiden Tabellen.
Im Zweifelsfall sollte die Einordnung des Systems mit der jeweiligen Zertifizierungsstelle vorab geklärt werden.

**Harmonisierung mit EN 954-1**

Neben der Forderung, einen entsprechenden Safety Integrity Level (SIL) zu erreichen, kommt es vor allem im Maschinenbau vor, dass eine bestimmte Kategorie nach EN 954 gefordert ist. Diese Norm misst die Sicherheit hauptsächlich über die Fehlerbetrachtung der Funktion. Dies muss bei der Entwicklung berücksichtigt werden. Es ist relativ einfach, beide Standards in der Entwicklung des Systems zu realisieren. Denn auch die IEC 61508 hat eine Fehlerbetrachtungsweise definiert, die in der Norm mit „Hardware-Fehler-Toleranz“ (HFT) bezeichnet ist. Laut Norm ist es zwar möglich, fast jeden SIL mit beliebiger HFT zu erreichen, doch in der Praxis gestaltet sich dieses teilweise als unmöglich.

| Anteil ungefährlicher Ausfälle Safe Failure Fraction SFF | Hardware-Fehler-Toleranz (HFT) | | |
|---|---|---|---|
| | 0 | 1 | 2 |
| <60 % | Nicht erlaubt | SIL 1 | SIL 2 |
| 60% - < 90% | SIL 1 | SIL 2 | SIL 3 |
| 90% - < 99% | SIL 2 | SIL 3 | SIL 4 |
| ≥ 99% | SIL 3 | SIL 4 | SIL 4 |
| Eine Fehlertoleranz der Hardware von N bedeutet, dass N+1 Fehler zu einem Verlust der Sicherheitsfunktion führen können. | | | |

Abhängigkeit zwischen der HFT und dem SIL bei entsprechender SFF*

Wenn man sich vor Augen führt, dass in einen Mikrocontroller eine Vielzahl von Funktionen implementiert sind, bei denen auch eine Vielzahl von Fehlern auftreten kann, ist es bei komplexen Technologien extrem schwer nachzuweisen, dass der Anteil ungefährlicher Ausfälle bei ≥99% liegt. Daher verwendet man oftmals niedrigere Werte für die SFF (Safe Failure Fraction) und legt anhand der Kenntnis der HFT (Hardware-Fehler-Toleranz) das Konzept und die Architektur des Systems fest.

Das geplante Konzept sollte auch als Basis für eine Konzeptbeurteilung der Zertifizierungsstelle herangezogen werden. Die IEC 61508 sieht vor, dass die Prüforganisation entwicklungsbegleitend agiert, um so einen Einblick in die Qualität der Entwicklung zu bekommen. Gravierende Fehler können so auch in einem frühen Entwicklungsstadium erkannt und behoben werden.

**Dokumentation**

Die Dokumentation ist eines der wichtigsten Instrumentarien, die eine strukturierte Entwicklung gewährleisten. Die Dokumente können später auch als Nachweis im Falle eines Unfalls dienen. Sollte es wirklich einmal zu einem Haftungsproblem mit dem Produkt kommen, kann die Dokumentation Aufschlüsse über eventuelle Fehler geben. Auch der Nachweis, dass das Produkt dem Stand der Technik entspricht, kann über die Dokumentation bewiesen werden.

* Diese Tabelle ist für ein Typ B Teilesystem

Dokumente sollten immer verständlich formuliert sein. Es ist darauf zu achten, dass auch außen stehende Personen diese Dokumente verstehen müssen. Damit erspart man sich häufig eine Vielzahl von Rückfragen und kann Zertifizierungszeiten erheblich reduzieren. Die eigentliche Form der Dokumente kann bei den meisten Firmen, die bereits über ein bewährtes Qualitätsmanagement verfügen, bestehen bleiben.
Es gilt immer, dass die Dokumente mit einer Versionsnummer und dem Datum zu versehen sind. Namens- und Historienverzeichnis sind ebenfalls von Vorteil. Einige Anregungen dazu kann der Teil 1 der IEC 61508 liefern.

Erforderliche Dokumente für eine Zertifizierung sind z.B.:

- Produktlastenheft und Produktpflichtenheft
- Sicherheitsspezifikation (Safety Requirement Specification)
- Entwicklungsplan
- V&V Plan
- Hardwareentwicklungsdokumente
- Softwareentwicklungsdokumente
- Konstruktionspläne
- Hardware Verifikations- und Testplan
- Hardware Testergebnisse
- Software Verifikations- und Testplan
- Software Testergebnisse
- FMEA
- Quantitative Nachweise der Sicherheit
- Technische Kundendokumentation (Installationsplan und Benutzerhandbuch)

Inhaltlich können die Dokumente stark variieren, aber prinzipiell sollten alle aufgeführten Punkte sich irgendwo niedergeschrieben wiederfinden.

**Spezifikation**

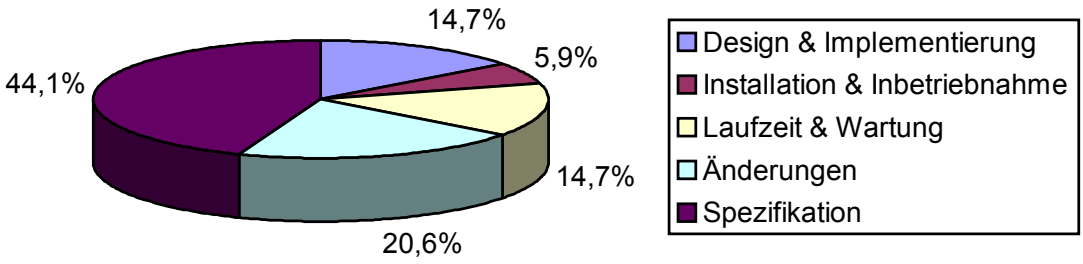


**Abb. 3: Fehlerentstehungsorte bei 34 untersuchten fehlerhaften Steuerungssystemen***

Die Spezifikation muss eine allgemeine Beschreibung des gesamten Systems enthalten sowie alle geforderten Funktionalitäten und Eigenschaften, Schnittstellen, Steckverbinder, HMI-Beschreibungen, Zeitkriterien, Interaktionen mit anderen Geräten oder Maschinen.
Für das Sicherheitsverständnis ist zu erkären, welche Normen und Standards eingesetzt werden, welcher SIL erreicht und welche Sicherheitsstruktur verwendet wird. Des Weiteren muss auch ersichtlich sein, welche Umweltbedingungen für das System gelten. Dazu zählen

* Quelle: STSARCES Report

Umgebungs-, Arbeits-, Lager- und Transporttemperatur, Spannungsbereiche, mechanische Belastung und elektromagnetische Verträglichkeit usw.

Mit der Beschreibung von Entwicklungsreglementierungen können interne Entwicklungsanforderungen festgelegt werden.
Ausführlich muss auch das Sicherheitskonzept spezifiziert werden. Die Spezifikation spielt hierbei eine der bedeutendsten Rollen im gesamten Sicherheitslebenszyklus. Den Grund hierfür kann Abb. 3 veranschaulichen.
Für die Vermeidung der Fehler in Spezifikationen müssen die Strukturen detailliert beschrieben sein. Dienlich sind dazu Blockdiagramm, Ablaufdiagramme, Wahrheitstabellen, Petrinetze und dergleichen.
Mit weitläufigen Gedanken über die Test- und Verifizierungsmaßnahmen sowie eine „Failure Mode Effect Analyse“ (FMEA) auf Blockebene reduzieren sich die Fehler in der Spezifikation erheblich. Die FMEA kann als entwicklungsbegleitendes Dokument in den entsprechenden Abschnitten modifiziert und erweitert werden.

**FMEA**

Ein FMEA ist relativ leicht zu erstellen, wenn man sich ein gewisses Verständnis über die Art der möglichen Fehler angeeignet hat. Die entsprechenden Maßnahmen, den Fehler zu erkennen und zu bearbeiten, sind dann häufig eine logische Konsequenz. So ist es oftmals ausreichend, die FMEA mittels einer Tabelle zu erstellen, die folgende Gliederung aufweist (Beispiel für eine Hardware-Einheit):

- Bauteil
- Fehlerunterstellung (Fehlerursache)
- Fehlerauswirkung
- Maßnahme zur Fehlererkennung und Fehlervermeidung
- Technische Lösung
- Verbleibendes Restrisiko

**Qualität der Sicherheit**

Neben einer ausführlichen Liste von unterstellten Fehlern, bietet die IEC 61508 auch eine ausführliche Beschreibung von Maßnahmen, die diese Fehler erkennen können. Mit den Teilen 2, 3 und 7 ist es möglich, ein gesamtes System für den entsprechenden Sicherheitslevel technisch zu planen.

Für die Hardwarekomponenten ist es wichtig, die jeweiligen Ausfallwahrscheinlichkeiten der Bauteile zu berücksichtigen. Achtet man bei der Bauteilauswahl schon darauf, dass die Bauteile eine möglichst geringe Ausfallwahrscheinlichkeit haben, ist die PFH bzw. PFD mit der entsprechenden Struktur auch relativ leicht zu erreichen.

Neben der Hardware sollten auch die jeweiligen Sicherheitsalgorithmen für die Software definiert werden. Die Software unterliegt keinen statistischen Ausfällen. Alle auftretenden Fehler sind systematischer Natur. Diese Art von Fehler kann durch eine Vielzahl von Validierungs- und Verifizierungsmaßnahmen reduziert werden. Neben dem Bestreben, Fehler zu vermeiden, muss aber auch der gewählte Sicherheitsalgorithmus in seiner Qualität quantifiziert werden. Da die Sicherheitsalgorithmen hauptsächlich zur Entdeckung von Hardwarefehlern dienen, werden diese Algorithmen mit einem Diagnose-Deckungsgrad „Diagnostic Coverrage“ (DC) bereits in der Norm bewertet.

### Bestätigung von Sicherheitsmaßnahmen

Durch Verifikation kann überprüft werden, ob die Spezifikation in sich konsistent (frei von Widersprüchen) ist, ob bestimmte Eigenschaften (z.B. Sicherheitsanforderungen) garantiert werden können und ob die Anforderungen richtig entworfen und implementiert worden sind (theoretisch). Verifikation kann nur innerhalb und zwischen formal geschriebenen Dokumenten erfolgen. Dadurch können Spezifikationsfehler entdeckt werden. Aber ob die Spezifikation der Realität entspricht, kann nur durch Validierung gezeigt werden.

Beispiele von verifizierbaren Eigenschaften einer Spezifikation sind: Typ-Check, Vollständigkeitsanalyse, Totalität von Operationen, Konsistenz, Undeterminismus, Zeitconstraints, Deadlocks, Lebendigkeit (liveliness), Erreichbarkeit von Zuständen (z.B. verbotene oder gefährliche Zustände), Erfüllung der Sicherheitsanforderungen, das Einhalten von Randbedingungen und Restriktionen der Technik und Sprache. Die Analyse der Erreichbarkeit von Zuständen kann feststellen, ob das zu vermeidende Verhalten tatsächlich (im Entwurf) vermieden wird. Dazu muss das zu vermeidende Verhalten explizit modelliert werden.

Die Verifikation ist zurzeit noch äußerst aufwendig. Es gibt zwar einige Werkzeuge für ihre Unterstützung, wie z.B. Modellchecker und Theorembeweiser, aber sie können in der Regel nur mit großem Aufwand und nur von Spezialisten benutzt werden. Deswegen werden meistens nur kleine Teile des Systems punktartig verifiziert.

### Validierung

Die Validierung ist die Tätigkeit, die darlegt, dass das betrachtete sicherheitsbezogene System vor und nach der Installation in jeder Hinsicht der Spezifikation den Sicherheitsanforderungen des sicherheitsbezogenen Systems entspricht. Deshalb bedeutet Software-Validierung zum Beispiel die Bestätigung durch Untersuchung und Bereitstellung eines Nachweises, dass die Software die Spezifikation der Sicherheitsanforderungen der Software erfüllt.

Mit formalen Methoden kann das System durch Animation (Simulation) validiert werden, bevor es fertig gebaut ist. Dies ist oft, aber nicht immer der Fall. Nur wenige operationale Formalismen unterstützten eine Animation. Wenn der Detaillierungsgrad der Spezifikation zu abstrakt ist, ist eine Ausführung auch nicht möglich. Die Validierung ist eine prototypische Ausführung (z.B. durch Simulation) einer operationalen Spezifikation, um zu prüfen, ob das Spezifizierte den Erwartungen entspricht. Dies kann meistens nur der Auftraggeber beurteilen. Eine weitere verbreitete Methode, um das Gleiche zu erreichen, ist die Erstellung von Funktionsprototypen. Ein Funktionsprototyp wird benutzt, um die geplante Funktionalität mit den Erwartungen des Auftraggebers zu vergleichen. Die Validierung trägt dazu bei, Verständnisfehler schon in frühen Phasen der Entwicklung zu finden. Wenn diese Fehler erst während des Betriebs erkannt werden, ist ihre Korrektur extrem aufwändig. Die Ausführung hilft auch dem Entwickler, ein besseres Problemverständnis zu gewinnen. Auf diese Weise wird das so genannte „Rush to Code-Syndrom“ vermieden, nach dem Entwickler dazu tendieren, zu früh mit der Implementierung zu beginnen, um möglichst schnell die Ergebnisse ihrer Arbeit anhand eines lauffähigen Programms zu sehen und demonstrieren zu können.

Die Validierung arbeitet auf einer Seite mit formalen Dokumenten (Spezifikation, Prototyp) und auf der anderen Seite mit Gedanken und Gefühlen (z.B. die Meinung des Auftraggebers). Deswegen kann die Korrektheit des Systems nur anhand von Beispielen gezeigt, aber nicht bewiesen werden. Im Detail geht es darum, Dokumente der Entwicklung auf Inhalt, Konsistenz und Vollständigkeit zu prüfen. Zudem wird die Verantwortung für die Abschlüsse der notwendigen Meilensteine während des Entwicklungsablaufs geklärt.

**Ausblick**

Als allgemeingültige Norm für Sicherheit ist die IEC 61508 sehr umfangreich und oftmals recht schwierig für spezielle Applikationen einzusetzen. Die Norm orientiert sich an dem Lebenszyklusmodell und geht dort auf alle Belange des Produkts und der Organisation ein. Die moderne Sichtweise garantiert dabei ein Höchstmaß an Sicherheit für Mensch, Maschine und Umwelt. Zahlreiche Produktnormen haben bereits die Gedanken der IEC 61508 aufgegriffen und deren Inhalte produkt- und applikationsspezifisch integriert. Sicherheit ohne Rücksicht auf die Inhalte der IEC 61508 zu nehmen, ist nicht mehr möglich.

**Hinweis:**

Die Firma innotec GmbH berät Unternehmen, die Sicherheitsprodukte entwickeln und einsetzen und dort mit der IEC 61508 konfrontiert werden.
Der TÜV Rheinland/Brandenburg bietet eine CD mit dem Titel „SafeyFirst“ an, die speziell über Sicherheit im Zusammenhang mit der IEC 61508 informiert.