Sicherheitstechnik – Notwendigkeit zum Schutz von Personen und zum Erhalt von Ressourcen

Sicherheitsanspruch

Sicherheit ist ein Grundbedürfnis des Menschen. Unser Leben ist in allen Handlung von der Vorstellung geprägt, dass die Dinge in der Zukunft so ablaufen, wie wir uns das vorstellen. Doch wie können wir sicher sein, dass nicht unerwartete Ereignisse zu einem fatalen Sicherheitsrisiko werden? Kleinigkeiten vermögen einen vermeintlich sicheren Vorgang mit einer Katastrophe zu beenden. Ein defekter O-Ring kann die Explosion einer Trägerrakete bewirken, das Versagen einer elektronischen Schaltung verhindert das Bremsen unseres Autos vor einer Absperrung oder wir begeben uns deshalb in Gefahr, weil ein übermüdeter Busfahrer fahrtechnisch eine Kurve nicht beherrscht?
Wenn man sich die Frage nach den Ursachen fataler und damit nicht zu erwartender Ausgänge stellt, so fällt die Antwort nicht schwer. Ein nicht sicherer Ablauf ist stets durch einen Fehler begründet, der entweder in unserer Planung nicht berücksichtigt wurde oder der später völlig unerwartet aufgetreten ist. Also scheint es einen überaus einfachen Weg zu geben, eine hohe Sicherheit zu erreichen: Man muss einfach alle Fehler eliminieren!
So simpel diese Aussage zu sein scheint, sie ist doch schwer realisierbar. Es gibt unzählige Fehler, die wir überhaupt nicht vorher einkalkulieren. Zudem ereignen sich spontane Ausfälle, die sich vollkommen zufällig ereignen und damit kaum zu berücksichtigen sind. Jeder hat im Laufe seines Lebens die Erfahrung gemacht, dass man niemals alle Fehler ausräumen kann und dass man mit eventuellen Fehlern zu leben hat. Trotzdem sollte die Sicherheit möglichst erhalten bleiben und Abläufe sollten kalkulierbar sein.

IEC 61508 – Regelwerk zur Sicherheitstechnik

Die Erfahrungen der letzten Jahrzehnte haben gezeigt, dass die alleinige Konzentration auf einzelne Produkte und Komponenten innerhalb von Maschinen und Anlagen nicht ausreicht. Vielmehr muss der gesamte Prozess der Verarbeitung oder Herstellung in Augenschein genommen und sicher gemacht werden. Dieser Grundgedanke bildet die Basis der Sicherheitsnorm IEC 61508. 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. So bezieht sich die IEC 61508 nicht nur auf den Schutz des Menschen, sondern auch auf die Erhaltung von Umwelt und technische Ressourcen (Bild 1).

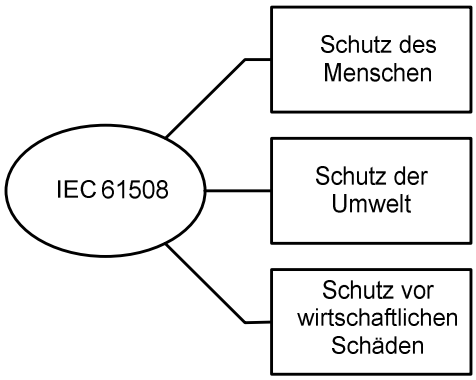

Bild 1: Anwendungsbereich der IEC 61508

Lebenszyklusmodell innerhalb der Norm

Die IEC 61508 beruft sich bei einem Produkt auf das Lebenszyklusmodell. Darunter versteht man die Lebensphasen, angefangen vom ersten Brainstorming bis zu dem Zeitpunkt, an dem das Produkt außer Betrieb genommen und entsorgt wird. 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.

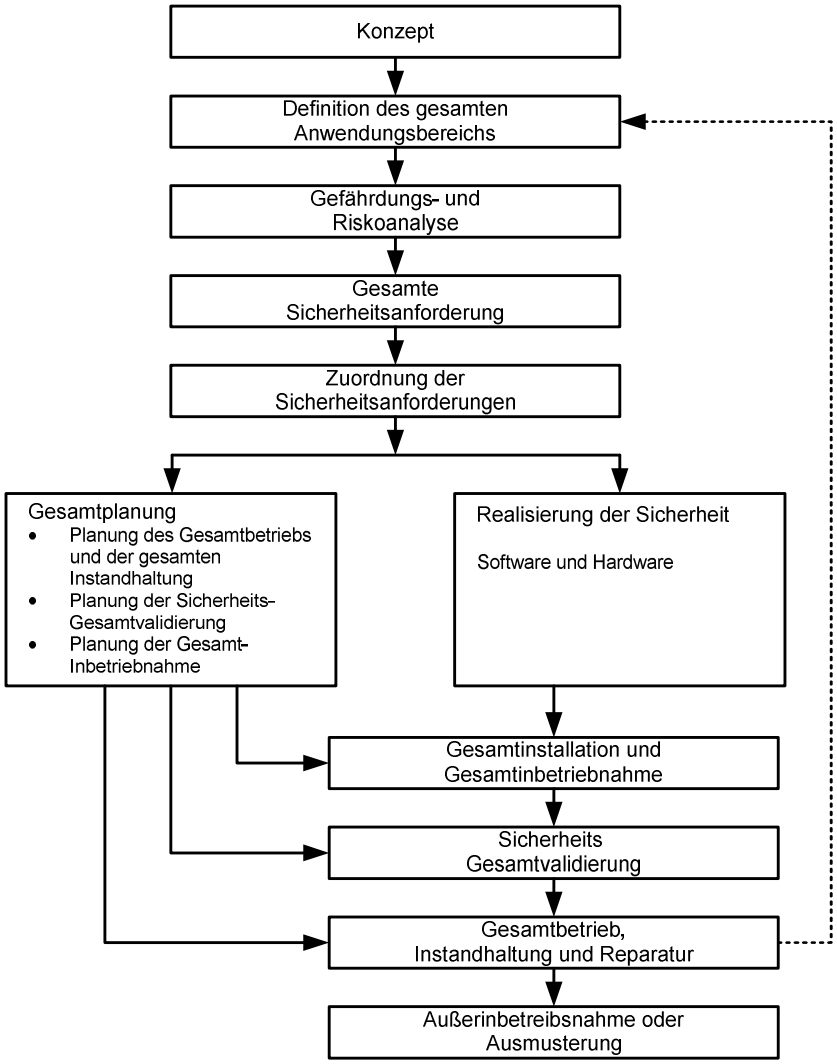

Bild 2: Produkt-Lebenszyklusmodell (nach IEC 61508)

Das Bild 2 stellt das in der Norm vorgestellte Lebenszyklusmodell dar. Dieses Modell ist aber nur beispielhaft zu verstehen, so dass jede Firma oder jeder Dienstleister sein bereits bestehendes Ablaufschema direkt verwenden oder leicht abändern kann.

Als fundamentale Neuerung hat die Norm IEC 61508 eine Einstufung in Sicherheitskategorien gebracht, die mit SIL abgekürzt werden (SIL = Safety Integrity Level). 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.

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	PFH (pro Stunde)	PFD (pro Anforderung)
4	10^{-9} bis < 10^{-8}	10^{-5} bis < 10^{-4}
3	10^{-8} bis < 10^{-7}	10^{-4} bis < 10^{-3}
2	10^{-7} bis < 10^{-6}	10^{-3} bis < 10^{-2}
1	10^{-6} bis < 10^{-5}	10^{-2} bis < 10^{-1}

Werte für die maximale tolerierbare Wahrscheinlichkeit für einen Ausfall pro Stunden (High Demand) und für die Ausfallswahrscheinlichkeit pro Anforderung (Low Deamand)

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 die Notaus-Funktion 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 der Norm EN 954-1 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-Fehlertoleranz“ (HFT) bezeichnet ist. Wenn der Wert für HFT 0 ist, so kann jeder Fehler in einem System zum Verlust der Sicherheit führen. Bei Werten für HFT, die größer oder gleich 1 sind, nimmt das System bei einem beliebigen Ausfall stets noch den sichern Zustand an. Diese zuletzt genannte Eigenschaft ist normalerweise nur mit mehrkanaligen Strukturen realisierbar. Laut Norm ist es zwar möglich, fast jede SIL-Stufe mit beliebiger HFT zu erreichen, doch in der Praxis gestaltet sich dieses teilweise als unmöglich.

Anteil der sicheren Ausfälle (SFF)	Hardwarefehlertoleranz		
	0	1	2
< 60%	Nicht erlaubt	SIL 1	SIL 2
60% bis 90%	SIL 1	SIL 2	SIL 3
90% bis 99%	SIL 2	SIL 3	SIL 4
> 99%	SIL 3	SIL 4	SIL 4

Abhängigkeit zwischen der HFT und dem SIL bei entsprechender SFF

Wie die Tabelle darstellt, wird der HFT-Wert mit dem SFF-Wert verknüpft. SFF ist eine Abkürzung für „Safe Failure Fraction“. Gemeint sind hiermit die Ausfälle eines Systems, die in den sicheren Zustand führen. Je höher diese Anzahl ist, desto wahrscheinlicher ist es, dass man bei Ausfällen oder bei einem Versagen die Sicherheit nicht verliert. Der Wert für SFF lässt sich auch noch deutlich erhöhen, wenn man das System mehrfach testet, da auch erkannte Fehler in der Regel zu keinem Sicherheitsverlust führen.

FMEA und Qualitätssicherung

Wie schon anfangs erwähnt, gehören auch organisatorische Maßnahmen zur Einhaltung der Sicherheit. Eine bereits vielfach bewährte Methode zur Fehlervermeidung ist die Erarbeitung einer FMEA (Failure Mode and Effect Analysis). Hierbei nimmt man gewisse Fehlerfälle an und überlegt sich das zu erwartende Ausfallsszenario. 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

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.

Autor des Betrags ist Dr. Peter Wratil, Geschäftsführer der Firma innotec GmbH

innotec verfügt über jahrelange Erfahrung bei der Anwendung der Sicherheitstechnik im Maschinen- und Anlagenbau. Neben der Beratung bietet innotec auch Schulung und Zertifizierungsunterstützung an.

innotec Gmbh
Heinrich-Wildung-Weg 3
D-21224 Rosengarten (Hamburg)
Tel.: +49+4105+1559182
www.innotecsafety.de