19 Anwendungsbeispiele

19.1 Praktische Implementierung des IEC 61508 Sicherheitsstandards

Die IEC 61508[186] ist eine internationale Norm, welche von der internationalen elektrotechnischen Kommission (IEC) 1999 herausgegeben wurde. Dieser internationale Standard ist der erste seiner Art, indem die funktionale Sicherheit von elektrisch/elektronisch/ programmierbaren sicherheitsbezogenen Systemen eine zentrale Rolle spielen.

Für einen Anlageninhaber ist es unabdingbar, ein ausreichendes Sicherheitsmanagement einzurichten. Wenn im Falle eines Unfalls das sicherheitsbezogene System nicht mit dem vorgegebenen Standard übereinstimmt, könnte die Firma für die Vernachlässigung der passenden Sicherheitsrichtlinien beschuldigt und haftbar gemacht werden. Dementsprechend sind eine ausreichende Abschalteinrichtung und eine angemessene Technik, die mit dem internationalen Standard übereinstimmt, für spätere Wartungen und für firmenfremde Unternehmen notwendig und wahrlich erforderlich.

Der Begriff des Safety Instrumented System (SIS) wurde in die Sicherheitsnormen eingeführt. Darin enthalten sind alle Ausrüstungen, von den Sensoren über Logikauslöser bis hin zu den abschließenden Aktuatoren. Diese Durchführung der Risikoreduzierung ist für den reibungslosen und sicheren Betrieb der Anlage erforderlich.

Die IEC 61508 Sicherheitsnorm beginnt mit der Ermittlung der Prozessgefahren und deren Analyse mit einer anschließenden Risikobeurteilung. Alle erforderlichen Sicherheitsfunktionen müssen in einer sogenannten „Safety Requirement Specification“ aufgeführt und dokumentiert werden, darin eingeschlossen sind alle Sensoren- und Ventilkonfigurationen. Der Anbieter des Sicherheitssystems beginnt mit dem Design des SIS, basierend auf die zuvor ermittelte Spezifikation.

Ebenfalls werden mit der Norm alle Sicherheitsvalidierungen nach der Installation und Beauftragte oder periodische manuelle Beweistests sowie unvermeidliche Änderungen während des Betriebs abgedeckt. Erforderlich ist dabei, alle Entscheidungen, Tätigkeiten und Resultate zu notieren, um eine prüffähige Spur zu hinterlassen. Diese TI (Technical Information) stellt die praktischen, aufeinanderfolgenden Schritte und Maßnahmen vor, die vom Benutzer ergriffen und gleichermaßen von Lieferanten bzw. Fremdfirmen eingehalten werden müssen, um dem Standard nachzukommen. Die Auswahl und die Tragweite der Eingangssensoren sowie die Art des Logikauslösers und der Sicherheitsventile werden ebenfalls erwähnt.

---

[186] [IECa] IEC 61508, *International Standard 61508 Functional Safety: Safety-Related System*

19.1.1 IEC 61508 Norm

Der IEC 61508 stellt eine systematische Methode dar, um alle in Verbindung stehenden Prozessgefahren und deren Definitionen aufzustellen und Maßnahmen zu ergreifen. Dabei erhält eine außerordentliche Gewichtung das Design und die Gültigkeitserklärung des sicherheitsbezogenen Systems. Die Norm stellt ein Lebenszykluskonzept einschließlich einer Methode vor, um das erforderliche Sicherheitsintegritätslevel (SIL) für die Art des Betriebes herzustellen. Im Mittelpunkt steht im Allgemeinen die eingebaute Sicherheit und eine Herangehensweise eines Risikomanagements, zudem wird die Anforderung an die SIS als letzte Schicht für eine Beherrschung einer gefährlichen Situation gesehen.

Dieser neue Ansatz bedarf eines hervorragenden Fachwissens, das in einer Ausbildung oder während eines Trainingprogramms vermittelt werden muss. Durch Kontakte mit der Industrie zeigte sich das steigende Interesse für eine Beratung bzw. Unterstützung mit der Umsetzung des Standards IEC 61508 und IEC 61511.

Die IEC 61508 Norm umfasst sieben Teile:

- die allgemeinen Anforderungen,
- Anforderung für das E/E/PES Sicherheitsbezogene System,
- Software-Anforderung,
- Definitionen und Abkürzungen,
- Methoden für die Ermittlung der Richtlinien für die SIL,
- Richtlinien über die Anwendung von Teil 2 und 3,
- Überblick über die Techniken und Maßnahmen.

Die Teile 1, 2, 3 und 4 sind normativ, die Teile 5, 6 und 7 dienen nur zur Information.

Grundlegend in der IEC 61508 ist der sogenannte „Safety Lifecycle“, dieser Lebenszyklus wie er in Bild 19.1 dargestellt wird, zeigt eine Abdeckung nicht nur über die Entwicklung eines Systems, sondern über alle Hauptphasen seines Bestehens. Die Vorangehensweise an den Gesamt-Sicherheitslebenszyklus verlangt eine nochmalige Betrachtung der Sicherheit der Messgeräte durch alle beteiligten Unternehmen, wie Auftragnehmer, Lieferanten, Integratoren und Benutzern.

Der Schwerpunkt der Norm liegt auf vier Hauptaspekten:

- Gesamt-Lebenszyklus,
- Management der funktionalen Sicherheit,
- Einschätzung der quantitativen Sicherheit,
- Pipe-to-Pipe-Ansatz.

Jeder dieser Aspekte wird kurz in den folgenden Abschnitten besprochen.

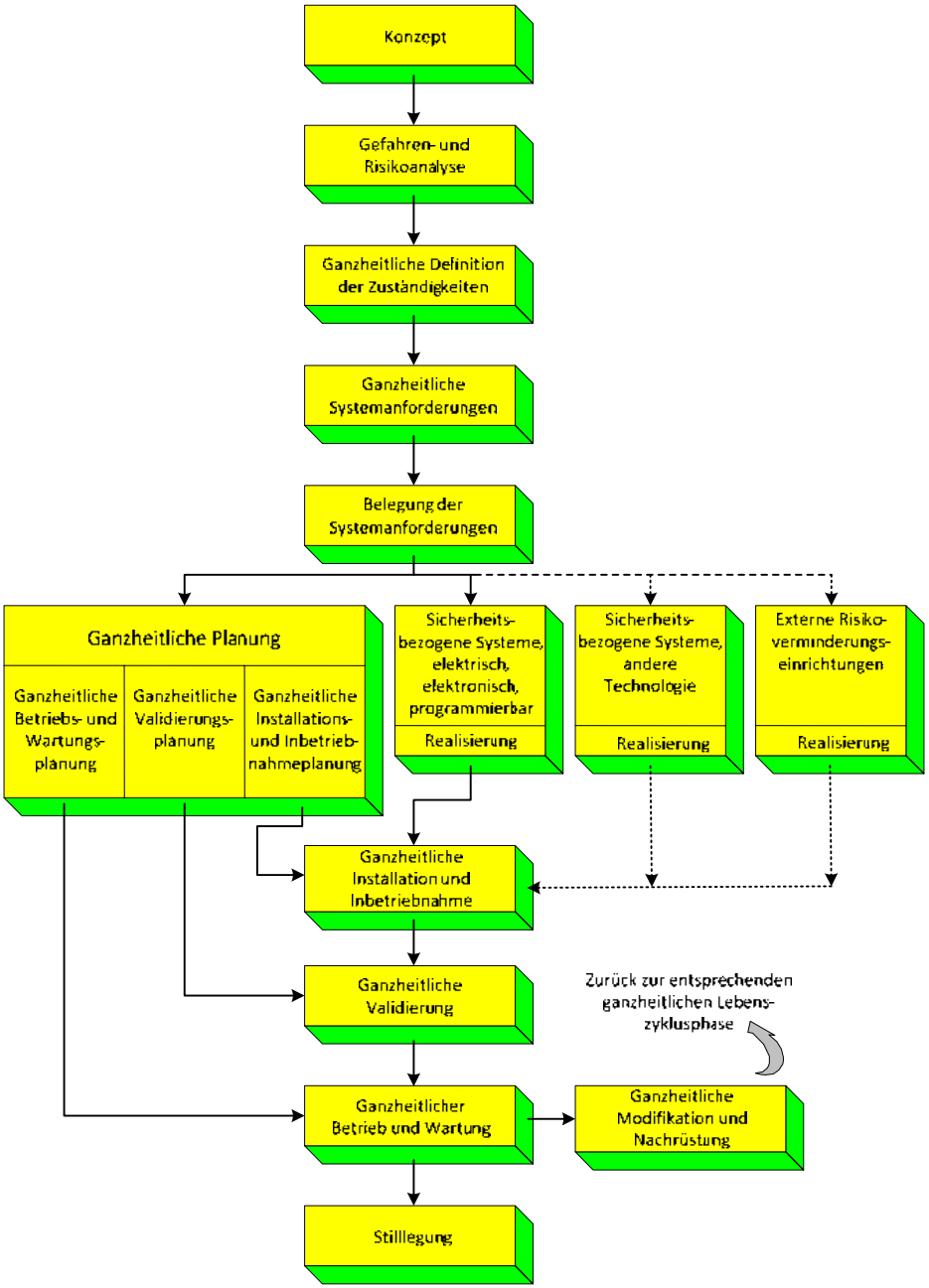

Bild 19.1: *Sicherheitslebenszyklus*[187]

[187] [IECa99] IEC 61508-1, Bild 2

Es gilt zu betonen, dass im Sicherheitsmanagement großer Wert darauf gelegt wird, dass jeder Schritt im Lebenszyklus vollständig dokumentiert wird. Darin eingeschlossen ist ebenfalls die Kompetenz der Organisationen und der beteiligten Leute, die in diesem Lebenszyklus mit einbezogen werden.

In einigen Firmen ist ein bestimmtes Managementsystem für die funktionale Sicherheit bereits eingebaut. Diese stimmen größtenteils mit den IEC-Anforderungen überein, jedoch nicht immer wird dem erwähnten Lebenszyklus diese bedeutsame Aufmerksamkeit beigemessen.

Das folgende Kapitel beschreibt alle Schritte der Gesamtlebensdauer. Bild 19.2 zeigt die praktisch aufeinanderfolgenden Schritte einschließlich jener, um die Sicherheitsfunktionen festzustellen. Zudem wird das Entwerfen und Anbringen von Sicherheitsschleifen gezeigt.

19.1.1.1 Funktionales Sicherheitsmanagement

Dies kann der schwerste und am meisten unterschätzte Teil der Norm sein. Alle Unternehmen, die mit jedem möglichen Schritt im Lebenszyklus teilhaben werden, müssen im Funktionalen Sicherheitsmanagementsystem (FSM) untergebracht werden. Es sollte die gesamte Handhabung und die technischen Tätigkeiten spezifiziert werden, die notwendig sind, um die erforderliche funktionale Sicherheit zu erzielen. Zudem werden alle im Lebenszyklus verwendeten Verfahren, die Kompetenzen der verantwortlichen Personen, Abteilungen und Organisationen und die Art und Weise wie die Überprüfung und die Gültigkeitserklärung gehandhabt wird, gezeigt. Sämtliche Ereignisse erfordern eine genaue Durchführung, so dass die Prüffähigkeit besteht und alle Entscheidungen genau nachvollziehbar sind.

Dokumentation

Die normativen Maßnahmen bei Dokumentationen in der neuen Sicherheitsnorm sind sehr streng und umfangreich. Es gibt die Anforderung, alle Schritte, die im Lebenszyklus unternommen werden, zu dokumentieren (in schriftlicher oder in digitaler Form). Das gesamte Design und technische Entscheidungen und deren Rechtfertigung müssen sorgfältig dokumentiert werden. Eine vornehmliche Spur aller Tätigkeiten und Resultate müssen sorgfältig organisiert werden.

Kompetenz

Alle Organisationen, die in die Lebensdauer mit einbezogen werden, müssen nachweisen können, dass sie für die Aufgaben kompetent sind, für die sie verantwortlich sind. Alle Manager, Projektleiter und Ingenieure, die in die Design, Technik- und Integrationsphase miteinbezogen werden, müssen ausreichende Erfahrung und Kompetenz vorweisen. Betriebsnormen für Ausbildung und Training müssen aufgestellt werden, und regelmäßiges Training ist ebenfalls festzulegen.