Einsteiger: Keine Angst vor SIL – IEC61508 - Projektbeispiel

Der Bedarf an sicheren Maschinenkomponenten in der Automatisierungstechnik und der Prozesstechnik wächst. Damit kommen auf Komponentenhersteller viele Anforderungen zu, bevor sie eine SIL-Komponente verkaufen dürfen. Für die Entwicklung nach IEC61508, DIN EN 62061, DIN IEC 61511 stehen Ingenieure und Entscheider vor dem Problem der Abschätzung von Risiken, Kosten und dem Einfluss auf ihre Organisation.

Die IEC61508 beschreibt Methoden und Anforderungen zur Minimierung des Risikos für Gesundheit und Kapital, das von einer Anlage ausgeht. Betroffen und daher verantwortlich ist jeder, der am Produktlebenszyklus in irgendeiner Form mitwirkt.

Wer als Unerfahrener erstmals ein Produkt mit SIL am Markt vertreiben möchte, muss dieses nicht nur funktional sicher entwickeln, sondern auch das Functional Safety Management in seiner Organisation etablieren und nachweisbar leben, damit er die Beweislastumkehr im Schadensfall vor Gericht anwenden kann.

Es gibt viele Fallstricke und zu klärende Fragen bezüglich der Firmenprozesse und der Produktentwicklung. Folgende Bereiche müssen u. a. untersucht werden:

Firmenprozesse, Entwicklungsprozesse, Qualitätsprozesse sowie Personalstruktur mit Know-how und Verantwortungen. Entlang des Produktlebenszyklusses müssen nach der Phase Entwicklung auch Anforderungen an Fertigung, Inbetriebnahme, Wartung/Reparatur und Außerbetriebnahme erfüllt werden.

Funktionale Sicherheit verlangt Erfahrung und geplantes Vorgehen. Schulungsmaßnahmen allein reichen nicht aus. Dieser Artikel beschreibt, wie man auch als Einsteiger mit wenig Erfahrung ein SIL-Produkt entwickeln kann.

Ein Projektbeispiel mit 6 Schritten:

Mögliche Schritte einer Entwicklung für eine funktional sichere Komponente:

Schritt 1a:	Safety Workshop (technisch)
Schritt 1b:	Functional Safety Grundlagenseminar (Management mit ins Boot nehmen) *(Bild 1)*
Schritt 1c:	Safety Requirements, Safety Plan, V&V-Plan
Schritt 2:	Concept Approval
Schritt 3-5:	Safety Hardware und Software Entwicklung (Design, Integration, Test) *(Bild 2)*
Schritt 6:	Zertifizierung

Schritt 1a: Safety Workshop

In einem Safety Workshop können die übergeordneten Anforderungen des Produktmanagements gesammelt und eine erste Grob-Architektur in Form einer System-FMEA auf Blockebene erstellt werden. Die sichere Funktion und der sichere Zustand des Produktes werden beschrieben.

Bei komplexen Projekten ist es ratsam, bereits zu diesem Zeitpunkt einen externen Assessor (TÜV, BGIA, etc.) für eine Vorkonzeptbesprechung einzubeziehen, um effizienter zur Konzeptfreigabe zu gelangen.

Tipp: Ein externer Assessor hilft während der gesamten Entwicklung beim Aufbau und der Bewertung der benötigten Prozesse. Er sollte wenigstens in einer anderen Abteilung, besser in einer anderen Organisation, angestellt sein.

Schritt 1b: Grundlage auch für Management

Häufig findet man in Organisationen die Problemstellung des Tunnelblicks. Der Produktmanager sieht nur sein Produkt, die Entwickler sehen nur die ihnen zugewiesenen Aufgaben und das Management ist sich der Implikationen der funktionalen

Sicherheit auf die gesamte Firma mit ihren Prozessen und Abläufen nicht bewusst.

Hilfreich ist ein Grundlagenseminar, wie es vom TÜV angeboten wird. Hier wird entlang des zukünftigen Produktes das Thema Funktionale Sicherheit für alle Ebenen erklärt. Als mögliche Folge werden nun Prozesse dokumentiert.

Schritt 1c: Safety Plan, Safety Requirements / Concept

Der Safety Plan legt dar, auf welcher Grundlage das Produkt sicher sein wird, beschreibt Prozesse und Verantwortungen sowie organisatorische Dinge. Er ist ein zentrales Dokument und steht am Anfang jeder Entwicklung. Im Verification & Validation Plan (V&V-Plan) kann gelesen werden, wie, wann, von wem, was verifiziert und am Ende validiert wird. Entlang jeder Lebenszyklusphase werden so Verantwortungen, Qualitätsmanagement, Konfigurationsmanagement, Änderungsmanagement, Tooling und Maßnahmen zur Fehlervermeidung dokumentiert. Safety Requirements und Safety Integrity Requirements müssen systematisch (bei mittleren und großen Projekten mit einem datenbankbasierten Werkzeug) erfasst werden. Die Dokumente werden nach einer Review mit dem Ziel der Vollständigkeit und Verständlichkeit zur Konzeptprüfung eingereicht.

Schritt 2: Die Konzeptprüfung

Beurteilt werden neben dem Safety Plan die Safety Requirements und der V&V-Plan. Inhalte sind u. a.

- Safety Policy des Unternehmens
- Organisationsstruktur der Firma
- Personal, Verantwortungen, Erfahrung
- Prozessbeschreibungen
- Standards und Vorlagen

Das Ergebnis ist ein Statusbericht mit einer entsprechenden Mängelliste. Die Mängel müssen gemäß Änderungsprozess behoben werden. Betroffen sein kann die Geschäftsführung, der Vertrieb, die Entwicklung, etc.. Dann kann die eigentliche Entwicklung nach V-Modell beginnen.

Parallel zu allen Phasen läuft nun der Assessment Prozess mit geplanten Reviews und Berichten an. Während aller Entwicklungsphasen muss das Vier-Augen-Prinzip gelten (geplante, protokollierte Reviews mit Freigabe durch benannte Personen). Dabei darf ein Autor nicht selbst sein Werk testen. Eigenschaften und Änderungen müssen nachvollziehbar sein (Traceability), im einfachsten Fall mit einer Traceabilitymatrix.

Schritt 3: Design

Beim Firmware Design kann ein CASE-Tool mit möglicher Anbindung an die Requirementsdatenbank hilfreich verwendet werden. Hierdurch werden weitere Fehler vermieden und eine Nachvollziehbarkeit (Traceability) sichergestellt. Das fertige Firmware Design wird einer Software Kritikalitätsanalyse (FMECA oder SWCA) unterzogen. Hierbei werden alle Operationen klassifiziert in Bezug auf ihren Einfluss auf sicherheitskritische Funktionalität. Kontroll- und Datenfluss für jede Operation werden analysiert. Das Ergebnis sind Maßnahmen zur Fehlervermeidung oder -beherrschung, die im Design umzusetzen sind.

Auch im Hardware Design kommen Tools für Berechnungen und Simulation zum Einsatz. Nach Erstellung der Hardware Schemas wird eine FMEDA auf Bauteilebene durchgeführt, um die erreichte PFH für jede Sicherheitsfunktion zu bestimmen. Das Design ist nun abgeschlossen.

Testfälle werden spezifiziert mit Bezug auf die betroffenen Requirements, d.h. jeder Testfall zeigt, welche Requirements damit getestet werden. In der Regel wird man zuerst Black-box Tests definieren, um die Gerätefunktionalität sicherzustellen. Dann werden Requirements übrig bleiben, die weitere Testfälle erfordern. Werden alle Tests ebenfalls datenbankbasiert spezifiziert, kann die Testabdeckung automatisiert gewährleistet werden.

Den Abschluss bildet eine Design Review durch eine qualifizierte Person mit dem Ziel der Erfüllung aller Requirements.

Schritt 4: Design Integration

Hier wird das Layout erstellt (Luft- und Kriechstrecken beachten!), Boards werden bestückt und vorab in Betrieb genommen.

In der Firmware wird gemäß dem Firmware Design implementiert. Zur Qualitätssicherung sind statische Codeanalysen mit Softwaremetriken, Unit Testing und Code Coverage Tests unerlässlich. Defensive Programmierung sollte angestrebt werden. Ein Codierstandard wie MISRA-C 2004 hilft ebenso bei der Fehlervermeidung.

Liegt die entwickelte Hardware auf dem Tisch, wird sie mit einer Test-Firmware in Betrieb genommen, um Schnittstellentests durchzuführen. Die Integration ist beendet, wenn die Hardware beweisbar funktioniert. Erst jetzt wird die Hauptfirmware auf der neuen Hardware integriert.

Schritt 5: Test

Black-Box Tests auf Systemebene werden durchgeführt für alle Systemfunktionen, die sich auf externe Schnittstellen auswirken. Dazu gehören Funktionstests unter Normalbedingungen, Temperaturtests wie auch EMV-Tests und Umwelttests gemäß den anzuwendenden Normen. White-Box Tests im Bereich Hardware sind die Charakterisierung an einem Muster (Signalpegel, -form, Ströme, Wärme) oder Firmware Verifikation (Timings, Interrupts, Belastung, Teil-Funktionalität). Fault Insertion Tests in Hard- und Software werden angewendet, um zu beweisen, dass Fehler auch wirklich funktional sicher beherrscht werden. Tests werden in separaten Berichten (nicht in der Testspezifikation) so dokumentiert, dass jeder Test reproduzierbar ist. Daraus folgt, dass automatisierte Tests in jedem Fall zu bevorzugen sind. Alle Berichte sind aufzubewahren. Mängel sind gemäß dem definierten Änderungsprozess zu bewerten und zu beseitigen.

Funktioniert das Produkt nach allen Spezifikationen korrekt, so kann das Produkt zur Zertifizierung eingereicht werden.

Schritt 6: Zertifizierung

Während der Zertifizierung wird die gesamte Entwicklungsdokumentation begutachtet. Es wird nachvollzogen, inwieweit die Anforderungen der IEC61508 eingehalten wurden. Stichprobenartig wird vom Assessor von der Organisation über Reviewberichte bis auf Einzelbauteilebene (Hardware) und Codezeile (Software) nach Konformität geprüft.

Nach Schließen aller offenen Punkte wird das Zertifikat erteilt.

Bei der Produktentwicklung sind die ersten Schritte entscheidend: MESCO unterstützt Sie auf dem Weg von der IEC Norm über das Sicherheitskonzept und dessen Umsetzung bis zum serienreifen Produkt. Unsere „TÜV certified Functional Safety Engineers“ setzen Ihre Ideen in die notwendige Hardware und Firmware um.

Zum Lieferumfang gehört sämtliche projektrelevante Dokumentation, so dass die Produktwartung und -weiterentwicklung beim Hersteller verbleiben kann.

Durch enge Kooperation mit dem TÜV profitieren Sie von etablierter Zusammenarbeit, gemeinsam abgestimmten Prozessen und schließlich durch ein SIL Zertifikat für Ihr Produkt.

Dipl.-Ing. Andreas Keller ist TÜV zertifizierter “Functional Safety Engineer” und Projektleiter für sicherheitskritische Entwicklungen bei MESCO Engineering GmbH, Lörrach.

info@mesco-engineering.com
www.mesco-engineering.com

Buchtipps:
Steve McConnell:
Code Complete
Microsoft Press

Christof Ebert:
Systematisches Requirements Engineering und Management
dpunkt.verlag

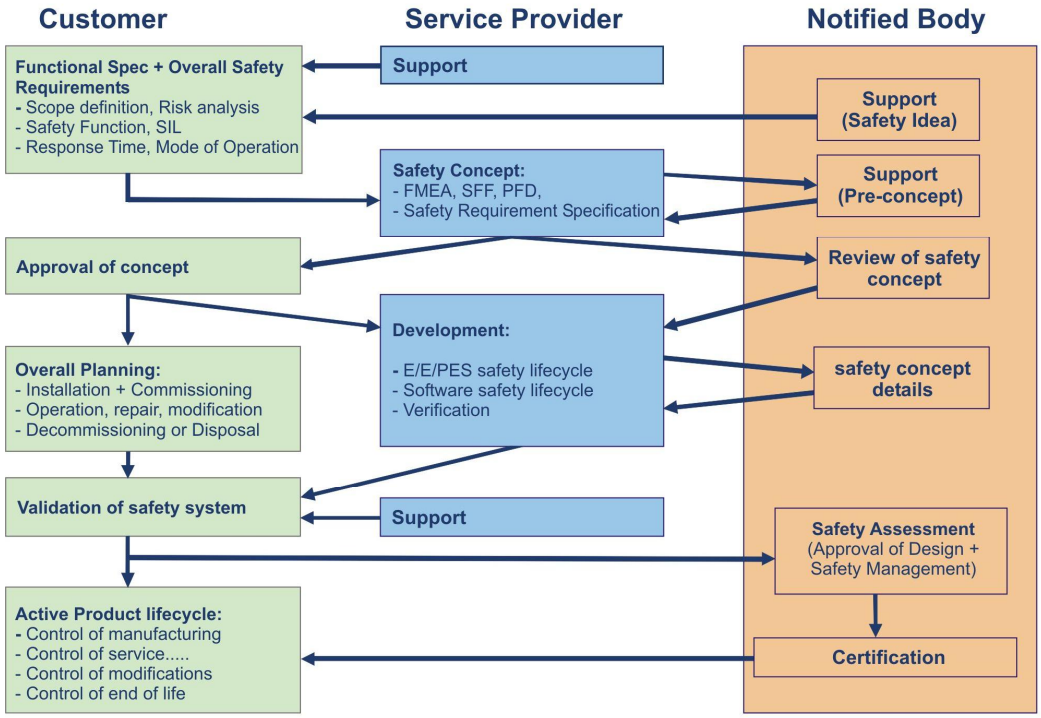

Bild 1: Zusammenarbeit Kunde – MESCO - Tüv

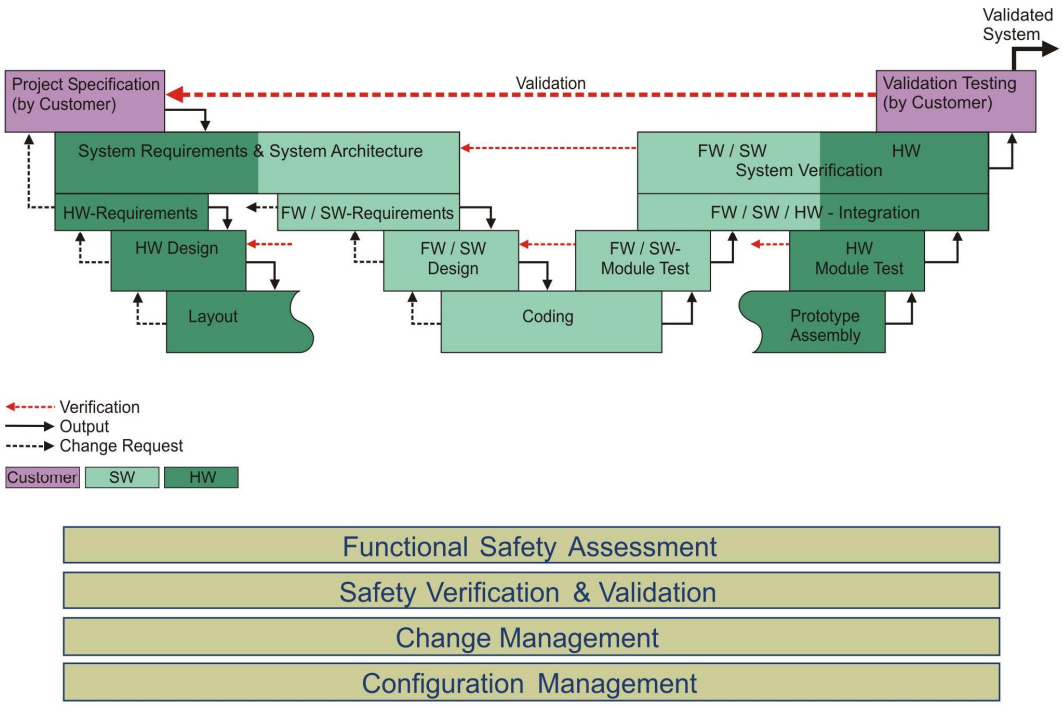

Bild 2: Entwicklung und V-Modell