Funktional sichere Komponenten effizient entwickeln

Anlagen und Maschinen können durch ihre Funktion Menschen und Umwelt gefährden. Funktionale Sicherheit hat zum Ziel, diese Gefahren auf ein von der Gesellschaft toleriertes Maß zu reduzieren.

ANDREAS KELLER *

Ein Sicherheitskonzept gemäß IEC 61508 ermöglicht die durchgängige Berücksichtigung der funktionalen Sicherheit in allen Entwicklungsphasen – vom Lastenheft bis zur Abnahme durch den Zertifizierer. Wer funktional sichere Anlagen- und Maschinenkomponenten gemäß der Maschinenrichtlinie (2006/42/EG) anbietet, muss sich an den Normen für Maschinensicherheit (IEC 62061 oder ISO 13849) sowie an der Basisnorm für Funktionale Sicherheit (IEC 61508) orientieren. Die Sicherheitsanforderungen für das Produkt müssen von den Endanwendungen abgeleitet werden.

*** Andreas Keller**
... ist Diplom-Ingenieur und leitet bei MESCO Engineering in Lörrach die Technologiegruppe Funktionale Sicherheit.

Die Basis: Lastenheft mit System Safety Requirements

Um die Anforderungen der IEC 61508 erfüllen zu können, benötigen Entwickler zuerst Informationen von den Endanwendern (z. B. Anlagenintegratoren, Maschinenbetreibern) zu Applikationen und Erwartungen bezüglich der geforderten Sicherheitsfunktionen. Andererseits müssen Informationen an die Endanwender fließen, damit diese ihre Aufgaben gemäß den Anforderungen der funktionalen Sicherheit ausführen können. Ziel ist die Durchgängigkeit im ganzen Sicherheitslebenszyklus, vom ersten Konzept bis zur Demontage der Anlage.

Noch vor Erstellung eines detaillierten Sicherheitskonzeptes sollte der Produktsteckbrief fixiert werden. Wesentliche Aspekte sind die Beschreibung von Zielapplikationen, in denen das Produkt eingesetzt werden soll, sowie typische Gefahren für die Umgebung (Beispiel: Die zu entwickelnde Komponente minimiert das Risiko, dass eine Maschine einen Servicemitarbeiter im laufenden Betrieb tötet oder verletzt).

Die Produkteigenschaften inklusive der Sicherheitsfunktionen müssen beschrieben sein, entweder im Lastenheft selbst oder als separates Dokument (System Safety Requirements Specification, SSRS). Sehr wichtig ist dabei der klare, von der Norm geforderte Bezug zu den Zielapplikationen. Wenn diese nicht sämtlich bekannt sind, sollten die Einsatzmöglichkeiten der zu entwickelnden Komponente möglichst genau beschrieben werden. Eine Beschreibung der Sicherheitsfunktion muss zumindest folgende Parameter enthalten: Reaktionszeit, Fehlerreaktionszeit, Sicherheitsintegritätsstufe (SIL), Betriebsmodus, maximale Ausfallwahrscheinlichkeit sowie Umgebungsbedingungen.

Bild: MESCO Engineering

Letztes Mittel: *Ein Not-Aus-Schalter ist bei vielen Maschinen unentbehrlich. Er darf jedoch keineswegs das einzige Element der Sicherheitsarchitektur darstellen.*

Produktsicherheitsplan: Fehler durch Planung minimieren

Spätestens nach Fertigstellung des Lastenhefts sollte die gesamte Planung des Sicherheitslebenszyklus für die Komponente und die Organisation in einem Produktsicherheitsplan dargelegt werden. Dazu gehören insbesondere die folgenden Inhalte:

Organisationsebene:

- Informationen zum QM-System,
- Mitarbeiterqualifikation,
- Projektsetup,

- Audits,
- Assessment der Funktionalen Sicherheit.

Produktebene:

- Produktvarianten,
- Vertriebskanäle (Direktvertrieb, OEM),
- Entwicklungsplanung,
- Planung der Wartung/Reparatur,
- Organisation der Fertigung,
- Einbindung von Zulieferern.

Der Produktsicherheitsplan bildet sozusagen das Management der Funktionalen Sicherheit ab und hilft, mögliche Entwicklungsfehler frühzeitig erkennen und vermeiden. Er ist das Einstiegsdokument für das Entwicklungsteam und zugleich das Bindeglied zwischen QM-System und Produkt, um die Anforderungen aus der IEC 61508-1, Kapitel 6 erfüllen zu können. Für die Entwicklungsplanung (Reviews, Rückverfolgbarkeit der Anforderungen, Projektmanagement etc.) bietet die IEC 61508 in den Teilen 2 und 3 sehr klare Vorgaben für jede SIL.

Der Produktsicherheitsplan sieht ferner die Erstellung eines Sicherheitshandbuchs vor. Es muss sämtliche Informationen enthalten, die der Anwender benötigt, um das Produkt im Rahmen seines Anlagen-/Maschinenlebenszyklus einzusetzen. Dazu können im Sicherheitskonzept bereits die Anhänge D der IEC 61508 (Teile 2 und 3) beantwortet werden. Die Erstellung des Sicherheitshandbuchs erfolgt parallel zur Elektronikentwicklung.

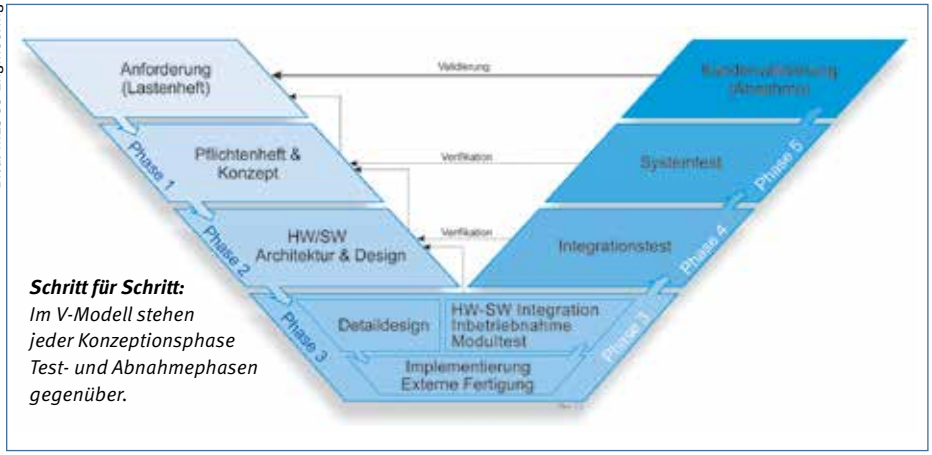
Systemdesign und Software Requirements als Leitlinien

Aus dem Lastenheft und/oder der SSRS wird die technische Lösung (Hardware) in der System Design Requirements Specification (SDRS) für die Entwicklung spezifiziert. Die Sicherheitsfunktionen des Produkts sind dabei so auszulegen, dass die Endanwender ihre Sicherheitsfunktionen an der Anlage/Maschine ausführen können. Die SDRS können als Teil des Pflichtenheftes oder als separates Dokument erstellt werden; häufig wird diese Aufgabe von einem externen, auf das Thema funktionale Sicherheit spezialisierten Dienstleister übernommen.

Entwickler denken oft in Bildern – deshalb dient meist ein Blockschaltbild der angestrebten Elektronikarchitektur als Einstieg in das Entwicklungsvorhaben. Darin werden die wesentlichen technischen Funktionen abgebildet (z.B. alle komplexen Bauteile, Schnittstellen, Rückwirkungsfreiheit). Diese Darstellungsweise ist auch nützlich, um grundsätzliche Projektinhalte mit dem Prüfer des Zertifizierers zu diskutieren.

Um die Integrität der Sicherheitsfunktionen zu gewährleisten, müssen Sicherheitsintegritätsmaßnahmen ermittelt werden. Eine Konzept-FMEA (z.B. nach VDA Band 4) kann anhand der Grobarchitektur zur Findung der notwendigen Maßnahmen dienen. Diese Maßnahmen müssen als Anforderungen in die SDRS aufgenommen werden.

Bild: MESCO Engineering



Schritt für Schritt: *Im V-Modell stehen jeder Konzeptionsphase Test- und Abnahmephasen gegenüber.*

Viele Anforderungen der SDRS betreffen die technischen Konzepte für die Elektronik; deshalb empfiehlt es sich, die einzelnen Funktionsblöcke im nächsten Schritt genauer zu untersuchen. Dazu gehören vor allem

- die Auswahl der Schlüsselkomponenten,
- der grundsätzliche (geplante) Aufbau der Schaltungen,
- Betrachtungen zu Platz und Wärme,
- Strategien zur Diagnose und Überwachung,
- Begründungen für sicherheitsgerichtete Lösungen.

Analog wird bei der Konzepterstellung für die (embedded) Software vorgegangen. Hierzu gehören

- Ablaufdiagramme für den Start-up,
- der Umgang mit Interrupts und Tasks,
- das Echtzeitbetriebssystem,
- Anforderungen an den Mikrocontroller und dessen Eignung,
- Entwicklungswerkzeuge,
- die Umsetzung von Performanz- und Zeitanforderungen.

Die Software-Anforderungen (Software Requirements) sind aus der SDRS abzuleiten und aus Softwaresicht zu dokumentieren. Nach Abschluss der Konzeptarbeit sollten nun sämtliche Anforderungen an die Hard- und Software in schriftlicher Form vorliegen.

Testplanung und Abstimmung mit dem Zertifizierer

Zu einem vollständigen Sicherheitskonzept gehört schließlich noch eine detaillierte Testplanung mit folgenden Inhalten:

- Testorganisation (Rollen, Zeitpunkt, Testobjekt),
- Testsetups,
- Testreihenfolgen,
- Testvorgehen (Methodologie),
- Kriterien zur Bündelung von Testfällen,
- vorgesehene Testarten,
- Kriterien zur Bewertung von Testfällen und Tests,
- Abnahmekriterien.

Zum Abschluss dieser Phase ist die Einreichung aller zuvor genannten Dokumente/Inhalte beim Zertifizierer (in der IEC 61508 als „benannte Stelle“ bezeichnet) sinnvoll, um das gesamte Sicherheitskonzept in Bezug auf die Normerfüllung zu beurteilen und früh die richtigen Weichen zu stellen. Als Prüfergebnisse erhält der Entwickler beispielsweise Listen mit priorisierten Abweichungen und Empfehlungen oder bereits eine erste Version des begonnenen Prüfberichts – diese kann hilfreich sein, um das Systemverständnis des Prüfers zu synchronisieren.

Nach Beseitigung der Problempunkte mit hoher Priorität kann mit der eigentlichen Entwicklung begonnen werden (Architektur und Design, Umsetzung, Integrationstests, Systemtests). Dabei geben die Spezifikationen das erwartete Ergebnis vor und die Konzepte werden zum Design verfeinert.

Sämtliche in diesem Beitrag beschriebenen Entwicklungsschritte im Rahmen des Sicherheitskonzeptes können sowohl vom Komponentenentwickler selbst als auch von externen Dienstleistern übernommen werden. Deren Einbindung ist insbesondere dann zu empfehlen, wenn intern wenig Erfahrung im Bereich der funktionalen Sicherheit vorhanden ist. Ein spezialisierter Dienstleister kann hier wertvolle Erfahrungen einbringen, sodass möglicherweise kostspielige Fehler im Entwicklungsprozess vermieden werden. // **FG**

MESCO Engineering
+49 (0)7621 15750