WHITEPAPER

IN SIEBEN SCHRITTEN ZUM SICHEREN PRODUKT

Einstieg in die Funktionale Sicherheit

Der Bedarf an funktional-sicheren Produkten für die Fabrik- und Fertigungsautomation wächst exponentiell. In demselben Masse steigen auch die Anforderungen für Komponentenhersteller. Dabei fordern die einzuhaltenden Normen gerade Einsteiger heraus. So etwa die IEC 61508, die relevanten Sektor-Normen IEC 62061, IEC 61511 und ISO 13849 oder die produktspezifischen Normen EN 61800-5-2, EN 61496. Diese Normen beeinflussen die technischen Anforderungen ans Produkt ebenso, wie den Entwicklungsprozess und das Qualitätsmanagementsystem des Unternehmens.

Das überlagerte Ziel der Funktionalen Sicherheit ist die Vermeidung von negativen Auswirkungen auf Leib und Leben. Jedoch können alle technischen Systeme versagen. Eine 100% Sicherheit ist nicht zu erreichen. In den Normen wird die Ausfallwahrscheinlichkeiten daher abgestuft. Bestimmte Grenzwerte dürfen nicht überschritten werden – dem tatsächlichen Risiko von Gefährdungen entsprechend.

Viele Feldausfälle lassen sich auf Fehler in den Spezifikationen zurückführen. Aus den Normen ergeben sich daher umfangreiche Massnahmen zur Vermeidung systematischer Fehler, die in den verschiedenen Phasen des Produktlebenszyklus angewendet werden – also von der Produktdefinition, über die Produktentwicklung bis zur Ausserbetriebnahme.

Sieben Schritte zur Produktsicherheit

Das stringente Einhalten der normativen Anforderungen, einschliesslich der zugehörigen Dokumentation, sind Voraussetzung für das abschliessende Assessment der Funktionalen Sicherheit und ein Mittel zur Minimierung von haftungsrechtlichen Risiken im Schadensfall.

Für Einsteiger bieten sich folgende Schritte an:

1. Der Kickoff-Workshop
2. Die Grundlagenschulung
3. Safety Plan, V&V-Plan und SRS
4. Die Konzeptfreigabe
5. Design & Integration
6. Tests
7. Zertifizierung / Assessment

Schritt 1: Der Kickoff-Workshop
Basierend auf den Produktanforderungen lassen sich schon mit Projektstart mögliche Lösungen auf der Architekturebene erarbeiten. Sofern die Produktanforderungen noch nicht ausreichend formuliert sind, können alternativ auch aus der Zielapplikation Schlüsselanforderungen abgeleitet werden.

Dabei empfiehlt es sich, bereits zu diesem frühen Zeitpunkt ein Auge auf die Prozesse zu werfen. Einige Anforderungen sind bereits durch die Standardprozesse der Unternehmen abgedeckt. Eventuelle Prozesslücken können jetzt identifiziert werden, um spätere Verzögerungen im Umsetzungsprozess zu vermeiden.

TIPP: Wird für das Produkt eine Zertifizierung durch einen Notified Body angestrebt, binden Sie ihn bereits früh mit ein. Die Praxis zeigt nämlich, dass die Auslegungen der Normen durchaus Raum für Interpretationen lässt.

Schritt 2: Die Grundlagenschulung
Sofern im Unternehmen noch keine oder nur geringe Kompetenzen vorhanden sind, empfiehlt sich eine Grundlagenschulung. Es ist sinnvoll, wenn am ersten Tag Teilnehmer aus allen relevanten Unternehmensbereichen vertreten sind. Für die R&D-Mitarbeiter bietet es sich an, eine zwei- bis dreitägige Spezialschulung anzuschliessen.

Schritt 3: Safety Plan, V&V-Plan, SRS
Der *Safety Plan* ist das zentrale Planungsdokument des Projektvorhabens. Er legt die anzuwendenden Prozesse fest, beschreibt die erforderliche Qualifikation und benennt die

zuständigen Personen im Projekt. Als Daumenregel gilt, dass der Safety Plan umso schlanker ausfallen kann, desto besser die Unternehmensprozesse ausformuliert sind.

Im *V&V-Plan* werden die im Entwicklungsprozess vorgesehenen Verifikations- und Validierungstätigkeiten sowie die jeweils dafür zuständigen Personen festgelegt. Es soll damit gewährleistet werden, dass später die erforderlichen Prüfungen mit der notwendigen Sorgfalt getätigt werden.

Die Safety Requirements Specification (SRS) ist am besten mit dem Lastenheft vergleichbar. Bei einem Safety-Produkt sind jedoch weitere Parameter zu spezifizieren, wie etwa der zu erreichende SIL, die Reaktionszeiten oder die maximale Ausfallrate.

TIPP: Schreiben Sie Lösungsansätze in dieser Phase nieder und unterziehen Sie sie einer Konzeptprüfung, zusammen mit den anderen erstellten Dokumenten. Vor allem bei neuartigen und komplexen Entwicklungsprojekten! Die Ausformulierung des technischen Konzepts ist zwar normativ nicht gefordert, jedoch ist sie sehr hilfreich, um Projektrisiken zu umgehen (siehe auch Konzeptfreigabe).

Schritt 4: Die Konzeptfreigabe

Der Grundgedanke der Konzeptfreigabe ist, ein stabiles tragfähiges Fundament als Voraussetzung für den späteren Projekterfolg zu schaffen. Gerade aufgrund der mannigfaltigen Anforderungen beinhalten FS-Projekte nicht zu unterschätzende Projektrisiken, die zu längeren Laufzeiten, Kostenüberschreitungen oder gar zum Projektabbruch führen können.

Nach der Konzeptfreigabe kann die Umsetzung in Angriff genommen werden.

TIPP: Binden Sie möglichst viele erfahrene Mitarbeiter in die Konzeptfreigabe ein, um die Risiken zu minimieren.

Schritt 5: Design und Integration

In diesem Schritt kommt ein weiterer Kerngedanke der Funktionalen Sicherheit zum Tragen. Wie geschildert, müssen Massnahmen gegen systematische Fehler ergriffen werden. Eine typische Quelle für systematische Fehler ist zu grosse Komplexität. Die Norm fordert daher eine schrittweises Verfeinerung der Produkt-Requirements / SRS, auf für den HW-/SW-Entwickler immer handhabbarer werdende Anforderungen.

Anschliessend an die SRS bilden folgende Stufen eine typische Kette im Software-Pfad:

- (System) Design Requirements Specification (SDRS), mit Geräte-Architektur
- Software Safety Requirements (SWRS)
- Software Architektur
- Software Design
- Codierung

Eine Vorwärts- und Rückwärtsverfolgbarkeit der Requirements zwischen den einzelnen Stufen muss nachgewiesen werden. Dedizierte Requirements-Tracking-Tools machen die Komplexität heutiger Produktentwicklung aber handhabbar. Für die Verifikation des Source-Codes eignen sich Code-Reviews – auch mit Verwendung von statischer Codeanalyse, bei der gegen die festgelegten Codier-Richtlinien geprüft wird.

Der Hardware-Pfad ist meist etwas grobkörniger. Auf die SDRS, als gemeinsames Dachdokument für die SW und HW-Entwicklung, folgt die Erstellung einer sogenannten Hardware Design Specification (HWDS). In dieser werden die einzelnen Blöcke der Produktarchitektur genau spezifiziert, zum Beispiel die Stromversorgung. Auch die technische Umsetzung wird formuliert. Erst im Anschluss daran wird die technische Umsetzung im Stromlaufplan und Layout vorgenommen.

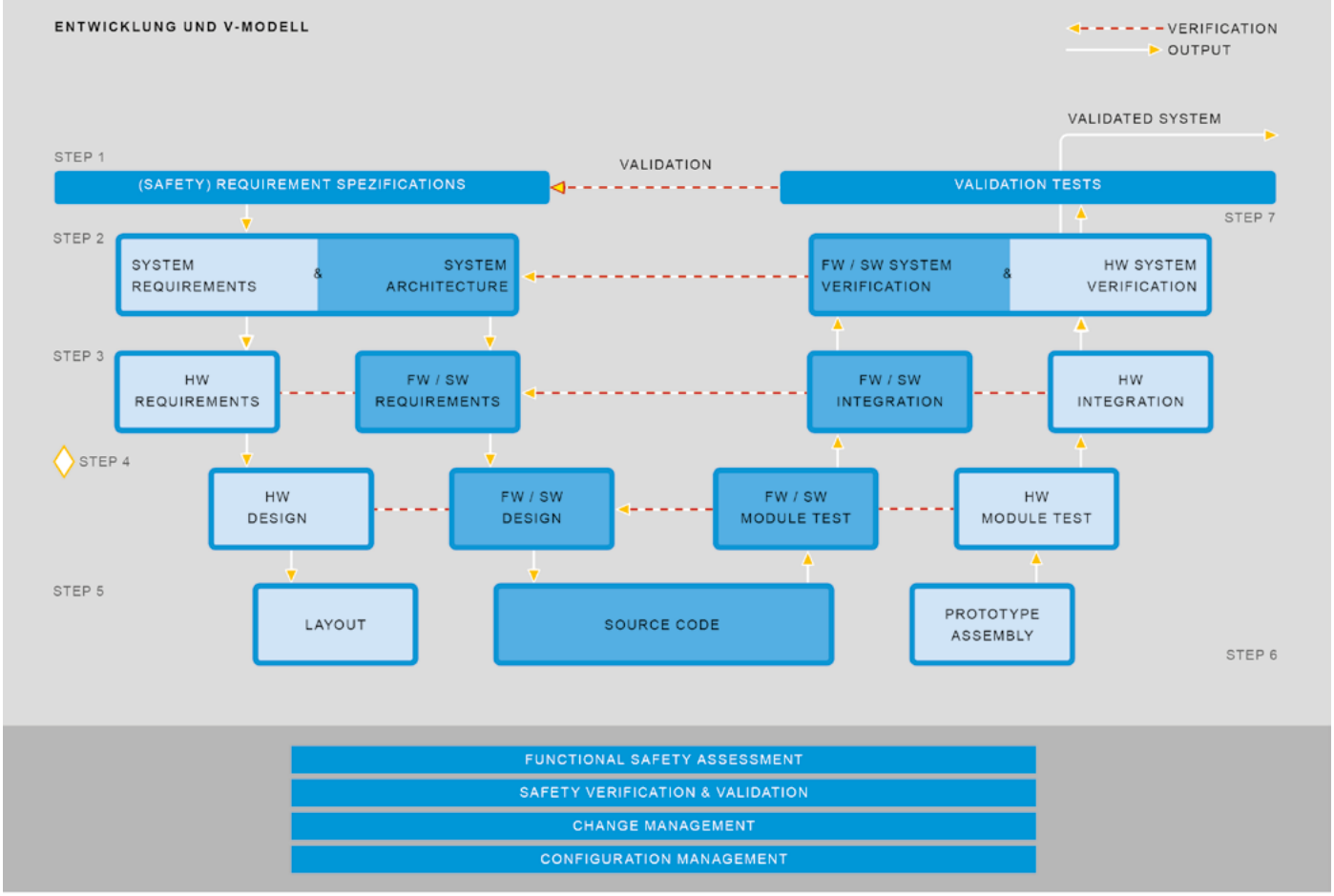
Der Stromlaufplan und die Bauteilestücklisten dienen nun als Input für die FMEDA, bei der die wichtigen Sicherheitsparameter PFH bzw. PFD berechnet werden.

Schritt 6: Tests

Die Tests stehen – bildlich gesprochen – auf der rechten Seite des V-Modells und werden von unten nach oben durchlaufen. Bei der Produktentwicklung in der Industrieautomation meist in drei Stufen: Modultests, Integrationstests und Validierungstests. Die Tests werden, zumindest in der Theorie, immer genau gegen das entsprechende Requirements- / bzw. Designdokument auf der linken Seite im V-Modell durchgeführt.

Es ergeben sich so typische Paare:

- Produkt Requirements / SRS – Validierungstest
- Architektur – Integrationstests
- Design – Modultests



Auf der Ebene der Modul-und Integrationstests wird zudem noch zwischen HW und FW/SW-Tests unterschieden.

Der Aufwand für die Tests ist hoch und daher nicht zu unterschätzen. Für die SW-Tests können erfahrungsgemäss 80 bis 100 Prozent des SW-Entwicklungsaufwands angesetzt werden. Daher ist es ökonomisch sehr sinnvoll, von Qualität wird hineingeprüft auf Qualiät wird eindesignt überzugehen.

Sind alle Tests bestanden und protokolliert, kann das Produkt zur Zertifizierung eingereicht werden.

Schritt 7: Zertifizierung / Assessment
Während der Zertifizierung wird die gesamte Entwicklungsdokumentation begutachtet und die Erfüllung der normativen Anforderungen nachvollzogen.

Der Assessor arbeitet meist anhand einer individuellen Checkliste und dokumentiert seine Ergebnisse. Teile des Assessments können aber bereits entwicklungsbegleitend erfolgt sein. Gerade bei zeitkritischen Projekten ist das eine interessante Option. In einer Präsenzveranstaltung, in der zum Teil sehr tief in Details eingestiegen wird, werden weitere Teile des Assessments durchgeführt.

In der Praxis lassen sich Abweichungen jedoch oft nicht vermeiden. Die einreichende Organisation bessert und reicht dann nach.

Nach Schliessen aller offenen Punkte wird das Zertifikat erteilt.

...und aus Ideen werden Erfolge!