FUNKTIONALE SICHERHEIT

FSM nach IEC 61508-1 – FSM als Teil des QM

Artikelserie Functional Safety, Teil 7

Einleitung

Im letzten Artikel haben wir die System-FMEA im Kontext einer funktional-sicheren Produktentwicklung als Methode zur Identifikation von Diagnosemassnahmen zur Erkennung und Beherrschung von Fehlern während des Betriebs vorgestellt. Adressiert hierdurch werden primär die zufälligen Ausfälle der Hardware.
Betrachtet man nun reale Feldausfälle stellt man fest, dass diese häufig auf systematische Fehlerursachen zurückzuführen sind. Folgerichtig definiert die IEC 61508 in Teil 1 ausführlich das Management der Funktionalen Sicherheit (FSM) – als Erweiterung eines ISO 9001-Qualitätsmanagement-Systems.

Auch dieser Artikel der Serie fokussiert sich auf die Sichtweise des Herstellers einer sicheren Komponente. Hierdurch begrenzt sich der zu betrachtende Teil des Sicherheitslebenszyklus vor allem auf die Phasen 9 und 10.

Wie bereits betont: Die Norm ist generisch und soll für unterschiedlichste Marktsegmente anwendbar sein. Das erschwert die Lesbarkeit, und eine sinnvolle Interpretation für das jeweilige Anwendungsgebiet muss daher erfolgen.

Themenfelder

Zu Beginn stellt sich die Frage, welche Themen beziehungsweise Forderungen sich überhaupt aus der IEC 61508-1 für den Komponentenhersteller ergeben.

Eine Auswahl der wichtigsten Bereiche:

- Benennung der verantwortlichen Personen für das Management der funktionalen Sicherheit
- Definition der Tätigkeiten, die von diesen Personen auszuführen sind
- Festlegung der notwendigen Informationen zur Ausführung (relevanter) Phasen des Sicherheitslebenszyklus
- Festlegung der Information, die zwischen den relevanten Parteien mitzuteilen sind

Weitere geforderte Prozesse / Verfahren:

- Beurteilung der funktionalen Sicherheit
- Verifikations- und Validierungstätigkeiten
- Konfigurationsmanagement
- Durchführung regelmässiger Audits
- Durchführung von Modifikationen
- Sicherstellung einer angemessenen Qualifikation der beteiligten Personen

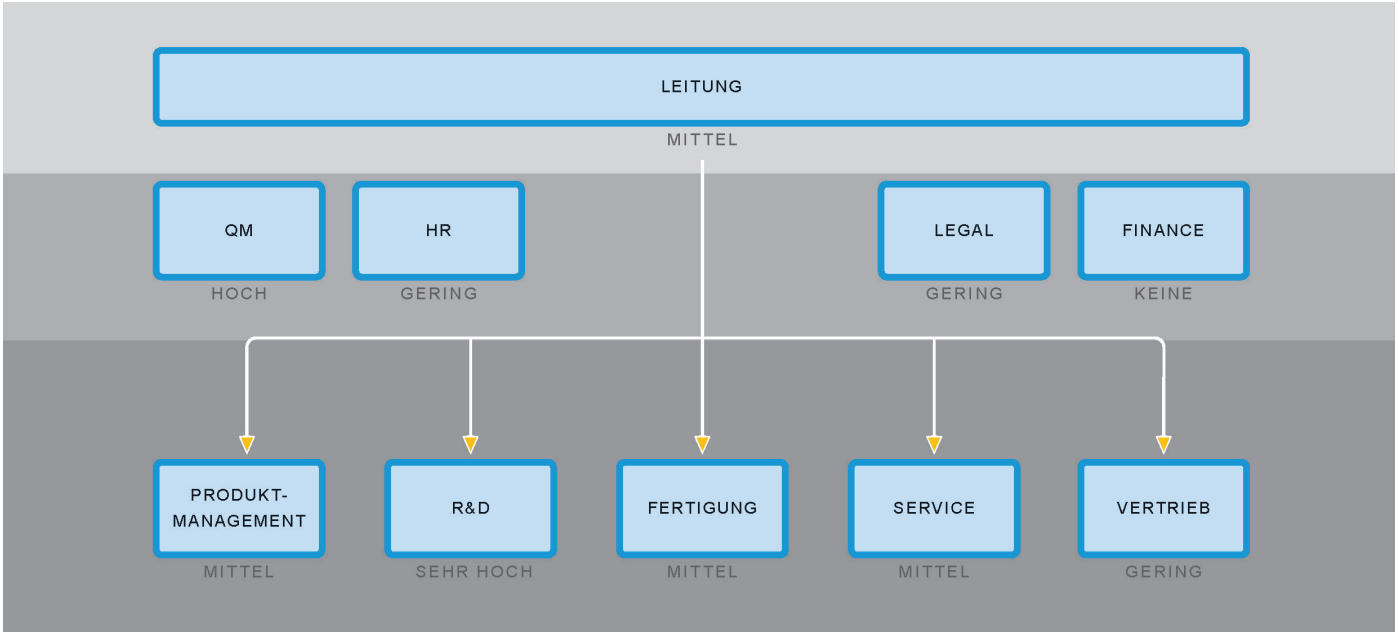

Abbildung 1: Betroffene Unternehmensbereiche

Anhand des ersten Punkts wird bereits deutlich, dass Funktionale Sicherheit ohne Unterstützung des Top-Managements nicht funktioniert. Bei der IEC 61508 handelt es sich nicht nur um eine weitere Norm, die von der Entwicklungsabteilung einzuhalten ist. Sie betrifft das ganze Unternehmen. Wie breit die Einflüsse der Funktionalen Sicherheit sind, kann überraschen. Das folgende Schaubild zeigt eine Übersicht der beeinflussten typischen Unternehmensbereiche.

Im Folgenden beleuchten wir einige der einzelnen Themen näher und zeigen mögliche Interpretationen der oft abstrakten Normanforderungen sowie Wege zur Umsetzung beim Komponentenhersteller auf.

Verantwortliche Personen

Die obige Aufzählung zeigt den engen Bezug zum Qualitätsmanagement und wer die Verantwortung für Aufbau und Pflege des FS-Management trägt. Üblicherweise wird die Gesamtverantwortung für das Management der funktionalen Sicherheit dem Leiter des Qualitätsmanagements zugeordnet und oft die neue Rolle des Functional Safety Managers eingeführt, eventuell in Personalunion des QM-Leiters.

In grösseren Organisationen mit vielen parallel verlaufenden Safety-Entwicklungsprojekten oder Safety-Projekten in aktiven Vermarktungsphasen, kann das Delegieren von Teilverantwortung sinnvoll sein, zum Beispiel die für die operative FS-Betreuung einer Produktfamilie. In der Praxis wird hierfür häufig der Rollenbegriff Functional Safety Coordinator (FSC) verwendet.

Die Position(en) können verschiedene Personen bekleiden, etwa Mitarbeiter aus der Q-Abteilung, der verantwortliche Produktmanager oder ein Fertigungsbetreuer. Aus Sicht der Norm ist jedoch weniger entscheidend, wo die Verantwortung verankert ist, als dass sie im Vorfeld klar geregelt wird.

Um Missverständnissen vorzubeugen: Vor allem im Vorfeld und während der Produktentwicklungsphase sollten weitere Personen Teilverantwortung übernehmen, da die Umsetzung der technischen Anforderungen der IEC 61508-2 und IEC 61508-3 üblicherweise nur von R&D-Mitarbeitern ausführbar ist. Es wäre möglich, den Projektleiter zusammen mit dem Teilprojektleiter HW (für die IEC 61508-2) und dem Teilprojektleiter SW (für die IEC 61508-3) einzusetzen.

Unüblich ist, explizit neue Rollen im Unternehmen zu definieren. Stattdessen können zusätzliche Anforderungen an die Qualifikation der Entwicklungsingenieure definiert werden, die im Safety-Projekt mitarbeiten. Die Benennung der relevanten Personen erfolgt meist im (projekt-)spezifischen Safety-Plan.

Festlegung der notwendigen Information

Die Normforderung zielt darauf ab, bereits im Vorfeld des Entwicklungsprojekts festzulegen, welche (zusätzlichen) Aktivitäten im Safety-Projekt auszuführen und zu dokumentieren sind, um für jedes Projekt/Produkt das obligatorische abschliessende Assessment der funktionalen Sicherheit durchführen zu können.

Da ein FS-Entwicklungsprojekt üblicherweise in einem Entwicklungsprozess nach V-Modell abgefahren wird, hilft der gedankliche Durchlauf des V, um systematisch die zusätzlichen Aktivitäten zu identifizieren. Auch die Detailanforderungen an die Phase 10 aus der IEC 61508-2 und -3 sollte nun beachtet werden.

Der Umfang zusätzlicher Aktivitäten hängt naturgemäss stark vom Prozessreifegrad der Organisation ab. Sind zum Beispiel im Unternehmen für den rechten Ast des V-Modells die dedizierten Testebenen – Modultest – Validierungstest definiert, sind die normativen Anforderungen bereits abgedeckt. In diesem Fall blieben die Fault-Insertion-Tests zum Nachweis der Wirksamkeit der Diagnosemassnahmen als zusätzlich festzulegende Aktivität.

Hinzu kommen Safety-typische Aktivitäten – v. a. für die linke V-Seite – wie Safety Plan, V&V-Plan, FMEA / FMEDA, Derating Analyse, (SW)-Tool-Chain-Validierung und Forward-/Backward-Traceability.

Im Safety Plan könnten prinzipiell alle zusätzlichen Massnahmen festgeschrieben werden. Das ist vor allem dann sinnvoll, wenn es sich um eine einmalige Safety-Entwicklung handelt und der Aufwand für direkte Prozesserweiterungen vermieden werden soll.

In der Praxis ist meist eine Kombination von Anpassungen an mehreren Stellen angebracht:

- Einführung von zusätzlichen Prozessen
- Anpassung von Meilenstein-Checklisten
- Anpassung bzw. Neuerstellung von Templates
- Einführung und Beschreibung neuer Methoden (z.B. zur Durchführung einer FMEDA)
- Durchführung von Modifikationen
- Sicherstellung einer angemessenen Qualifikation der beteiligten Personen

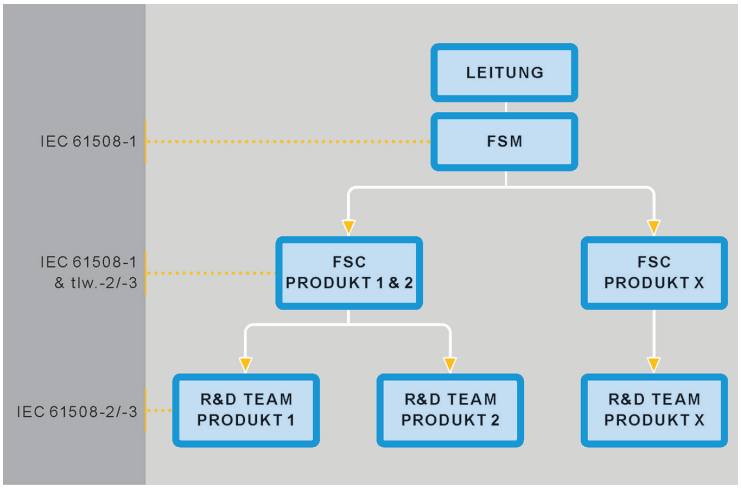

Abbildung 2: Organisation FSM

Fahrplan zur Einführung eines FSM-Systems

Die obige Schilderung zeigt, dass die Einführung eines FSM-Systems durchaus zeitaufwändig ist und am besten selbst als Projekt angegangen wird.

Die Motivation dazu ist häufig eine zunehmende Nachfrage nach Safety-Produkten und die Gefahr, ohne Safety-Produkte im Portfolio gegenüber dem Wettbewerb zurückzufallen, da Kunden den Kauf aus einer Hand bevorzugen. Idealerweise hat die Unternehmensleitung bereits Basiskenntnisse der Funktionalen Sicherheit und beauftragt den passendsten Unternehmensbereich mit der Aufgabe.

Die Länge der Vorlaufzeit eines Entwicklungsprojekts hängt stark vom Unternehmen, den Bestandprozessen und den verfügbaren Ressourcen ab. Als Richtwert gelten hierfür drei bis sechs Monate.

Im Rahmen einer Gap-Analyse werden die Bestandsprozesse mit den (relevanten) Anforderungen der IEC 61508 verglichen. Es macht dabei Sinn, drei Blickwinkel einzunehmen: die Sicht der Bestandsprozesse, die der Unternehmensbereiche und die der IEC 61508, die sozusagen als Checkliste herangezogen wird. Das stellt sicher, dass bei der späteren Umsetzung der notwendigen Anpassungen nichts übersehen wird.

Beim Durcharbeiten der Norm kann auf bereits existente Prozesse oder mögliche Lücken verwiesen werden. Das ist auch beim späteren Assessment hilfreich, da der Assessor bei der Bewertung von der Norm ausgeht.

Die Bestandsprozesse und Unternehmensbereiche werden zunächst in *relevant* und *nicht relevant* eingeteilt. Beispielsweise sind sowohl der Produktentwicklungsprozess als auch die Entwicklungsabteilung eindeutig safety-relevant, Bereiche wie Finance und IT normalerweise jedoch nicht.

Der nächste Schritt gilt der Überprüfung von relevanten Prozessen auf Konformität mit der Norm. Bei einem bereits eingeführten ISO 9001-System ist es realistisch, dass einige Bestandsprozesse bereits den Normanforderungen genügen (z. B. Dokumentenmanagement, Konfigurationsmanagement, Versionsverwaltung), andere zu ergänzen (z. B. Entwicklungsprozesse) oder neue Prozesse zu definieren sind (z. B. Audits und Assessment der funktionalen Sicherheit).

Bei zu ergänzenden oder neu zu erstellenden Prozessen werden Änderungen skizziert und der Aufwand für die Einführung grob geschätzt. Spätestens hier sind sowohl die Einbindung betroffener Prozesseigner als auch die Festlegung einer Reihenfolge für die Umsetzung empfehlenswert.

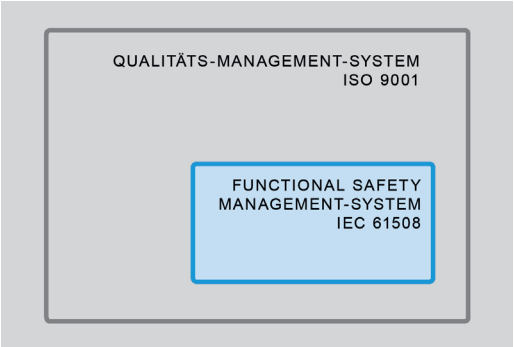

Abbildung 3: Zusammenhang QM / FSM

Die Gap-Analyse schliesst somit mit einem konkreten Fahrplan für die Umsetzung der erforderlichen Massnahmen ab. Richtwert für den Zeitaufwand der ganzen Analyse ist ein bis 1,5 Monate.

Die Umsetzung erfolgt in mehreren Stufen. Der Fokus sollte zunächst auf der Schaffung grundlegender Strukturen liegen, wie etwa der Weiterbildung beteiligter Mitarbeiter. Danach kann es sinnvoll sein, sich auf die Anpassung der Entwicklungsprozesse zu konzentrieren, um daraufhin mit der im Allgemeinen relativ langen Produktentwicklungsphase zu beginnen. Parallel dazu können die fertigungsrelevanten Prozesse und final die Prozesse für Vertrieb und Vermarktung angepasst werden.

Zusammenfassung

Das Management der Funktionalen Sicherheit hat viele Überlappungen mit dem Qualitätsmanagement. Somit ist eine Trennung der Disziplinen nicht sinnvoll. Bewährt hat es sich, das FSM als Teilmenge des QM aufzufassen. Lebt die ISO 9001 im Unternehmen und existiert ein reifes Prozessmanagement (in Richtung CMMI Level3) ist bereits eine stabile Basis für die Einführung eines Functional Safety Managements gelegt. Wird jedoch stark auf Zuruf gearbeitet zieht es gravierendere Veränderungen der Prozesswelt im Unternehmen nach sich.

Autor: Dr. Johann Pohany
Managing Director
Medidtcine Consultants
www.medidtcine.com

Autor: Armin Götzmann
Geschäftsführer
MESCO Systems GmbH
www.mesco.de