## FUNKTIONALE SICHERHEIT

# Functional Safety Management nach IEC 61508-1

*Artikelserie Functional Safety, Teil 8*

**Mit diesem letzten, dem achten Artikel zum Thema *Funktionale Sicherheit für KMU*, beschließen wir die Serie mit einem Resümee. Die folgende kurze Zusammenfassung von Inhalten der aufeinander aufbauenden Artikel zeigt noch einmal die jeweiligen Kernaussagen.**

## Licht im Normendschungel

*Teil 1 der Artikelserie beleuchtete die Normenwelt, beschrieb die einzelnen Normen, deren Zusammenhänge und die von der Norm geforderten formalen Notwendigkeiten.*

Die Normen der funktionalen Sicherheit – die sich über die Zeit in verschiedene Sektor-/produktspezifische Varianten ausdifferenziert haben – dienen primär dazu, Schäden an Menschen und Sachwerten zu vermeiden. Der Effekt wird statistisch sichtbar, im Optimum durch drastisch reduzierte Werte.

Allerdings ergeben sich dabei Ungereimtheiten: So gibt es für den Maschinebau mit der IEC 62061 und ISO 13849 zwei gleichberechtigte Normen. Der Systemintegrator kann sich für eine der beiden Normen entscheiden. Für den Komponentenhersteller werden jedoch beide Normen aus Vermarktungsgründen quasi zur Pflicht.

Aus der ISO 13849 ergeben sich einige zusätzliche Anforderungen an die Produktentwicklung. Am augenfälligsten ist, dass die ISO 13849 anstatt des SIL einen sogenannten Performance Level (PL a bis e) definiert.

Die grundlegendste Antriebssicherheitsfunktion *Safe Torque Off* (STO) kann prinzipiell rein hardwarebasiert umgesetzt werden. Die EN 61800-5-2 gibt dazu gute Hilfestellung. Interessant hingegen wird es, wenn komplexere Antriebssicherheitsfunktionen gefordert sind. In der Praxis werden derartige Funktionen in Software realisiert. Für Software verweist die Antriebsnorm auf die IEC 61508-3.

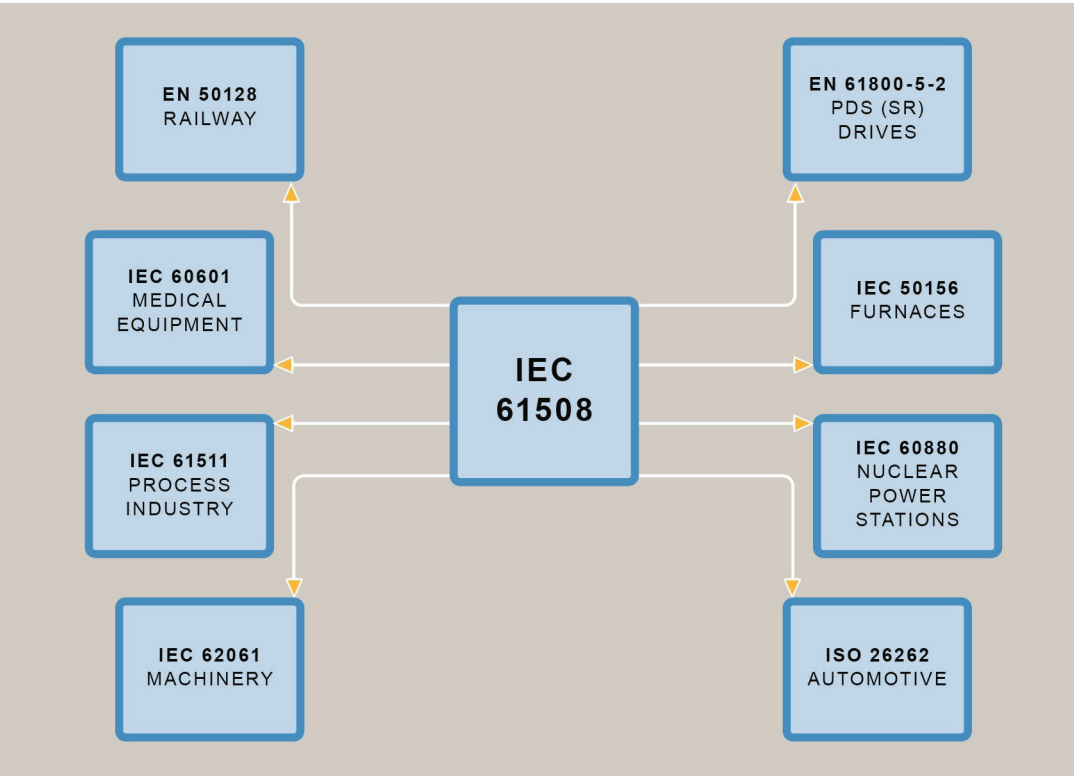


*Abbildung 1: Normen der Funktionalen Sicherheit*

MESCO Engineering GmbH | Berner Weg 7 | 79539 Lörrach | Deutschland | Tel. +49 7621 1575 0 | Fax +49 7621 1575 175 | info@mesco.de | www.mesco.de

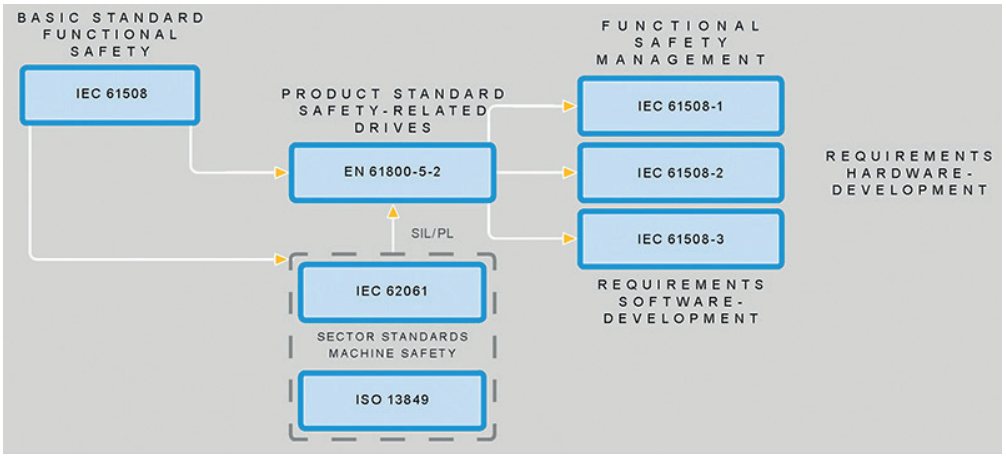


*Abbildung 2: Zusammenhang der Normen in der Industrieautomation*

Mit steigendem *Sicherheitsintegritätslevel* (SIL) werden sehr hohe Anforderungen an die Softwareentwicklung gestellt – wie etwa die verwendeten Methoden und die durchzuführenden Verifikationen, einschließlich der verwendeten Werkzeuge. Das bedingen eine Dokumentation, wie sie die Abbildung 3 rechts darstellt.

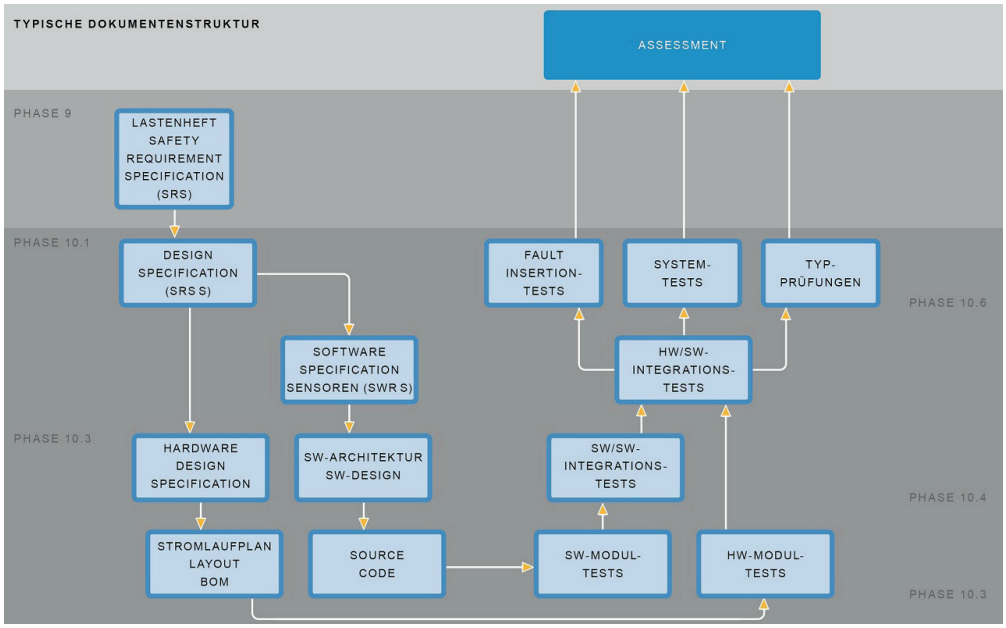


*Abbildung 3: Typische Dokumentenstruktur bei der Entwicklung eines Safety-Produkts*

## Der sichere Weg

*Teil 2 gab Hilfestellung für frühe SRS-Projektphasen und befasste sich mit der Entstehung und den richtigen Inhalten einer Safety Requirement Specification (SRS).*

Eine wesentliche Phase jeder Entwicklung im Bereich funktionaler Sicherheit ist das Requirement Engineering, also die Phase der Erstellung der Anforderungen. Die Planung erfolgt in der Regel im überlagerten *Functional Safety Management Plan* und im *Verifikation- und Validierungs-Plan* (V&V-Plan).

Abbildung 4 rechts zeigt das V-Modell. Im Projekt entstehen schrittweise, entlang des linken Astes, die typischen Dokumente SRS, SDRS, Design Spezifikationen für die Hardware und Software und erst am Ende die klassischen technischen Unterlagen, wie Stromlaufpläne und Quellcode.

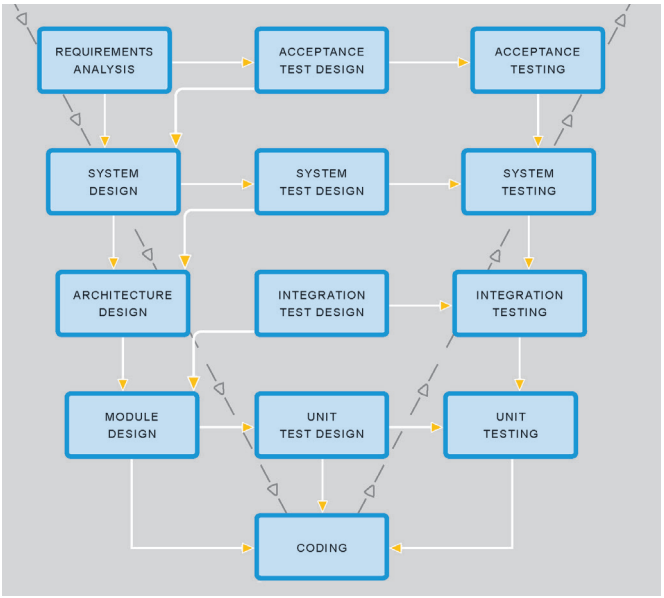


*Abbildung 4: V-Modell*

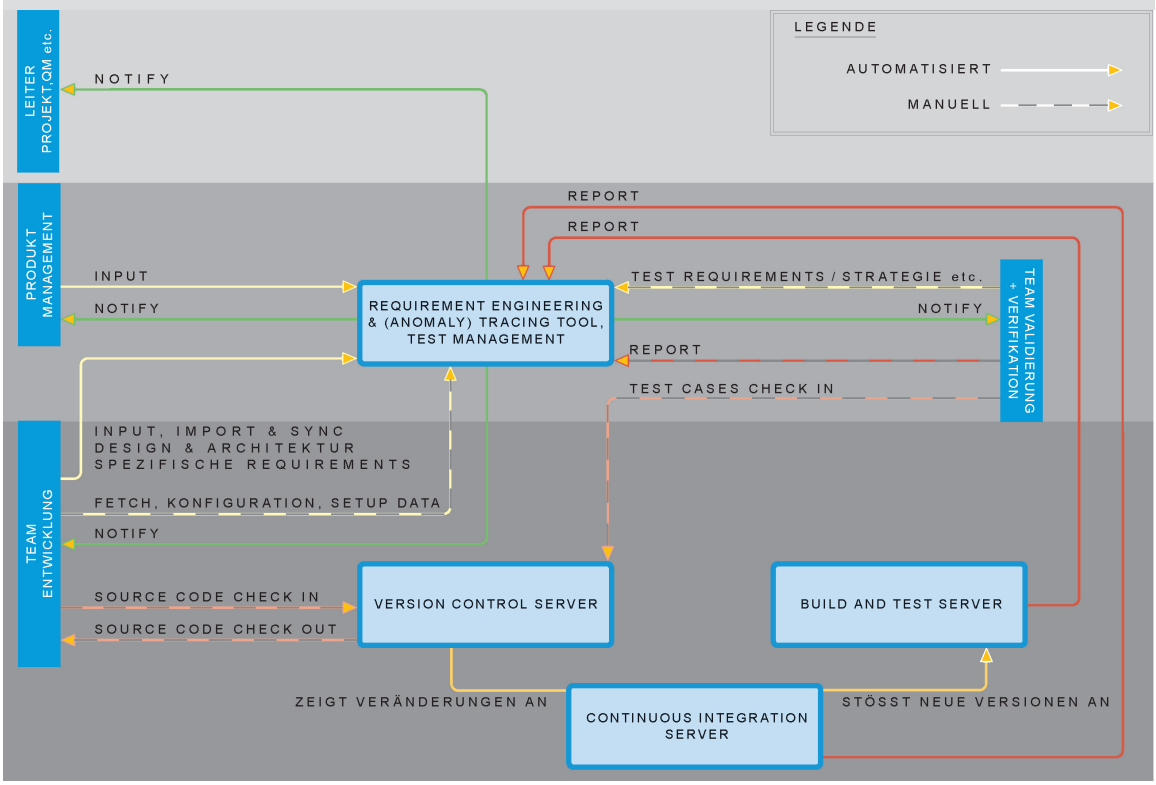


*Abbildung 5 : Gesamtüberblick der Software Entwicklungs-Toolchain*

## Toolchain – vom Requirement zum Test Case

*Teil 3 der Serie diskutierte den (Software-) Entwicklungsprozess und die Product Lifecycle Managementumgebung, die Dokumentations- und Entwicklungsumgebung, in der, nachvollziehbar und auditierbar, aus Requirements ein nach Regeln der IEC 61508 zertifizierbares Produkt entstehen soll.*

Die Nachvollziehbarkeit von der Anforderung bis zum durchgeführten Test und die überprüfbaren statistischen Aussagen ergeben sich durch die Integration der Tools, also der Werkzeuge. Die Toolchain ist eine Kombination der Prozesse mit diesen Werkzeugen. Allein die Prozesse können den Nachweis und Rückverfolgbarkeit nur schwerlich und mit erheblichem Aufwand generieren. Auch die ToolChain – ohne Integration und definierte Prozesse – kann das nicht leisten. Eine intelligente Integration der einzelnen Werkzeuge kombiniert mit intelligenten Prozessen, die jeweils auf den benötigten Safety Integrity Level adaptiert werden (von Standard Entwicklung ohne SIL Anforderung bis zur SIL 3 Anforderung), ist das Mittel der Wahl. Die Abbildung 5 oben veranschaulicht das.

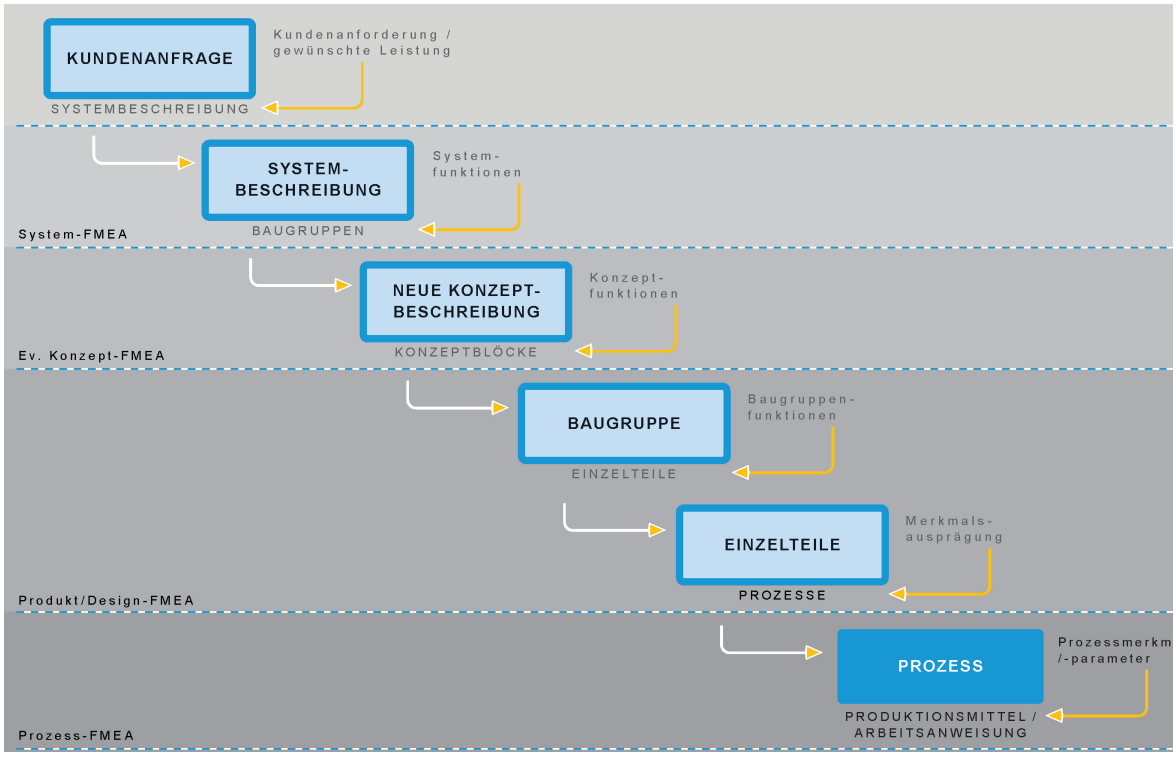


*Abbildung 6: Unterschiedliche FMEA im Produkt Entstehungs-Prozess*

## FMEA – Fehlermöglichkeit und Einflussanalyse

*Mit Qualitätsplanung und System-FMEA im Safety-Projekt haben wir uns in gleich zwei Artikeln beschäftigt (Teil 4 + 5). Deren Anwendung in der Praxis ist oft ein zeitaufwendiges Unterfangen mit einigen Stolpersteinen.*

Das Ziel der Untersuchung von *Fehlermöglichkeit und Einflussanalyse* (FMEA) ist zum einen das präventive Erkennen der Zusammenhänge von potentiellen Fehlern, Ursachen und Folgen sowie die Priorisierung der Ursachen-Wirkungs-Ketten bezüglich ihres Risikos. Zum anderen ist es die präventive Einleitung von Abstellmaßnahmen für Ursachen-Wirkungs-Ketten mit hohem Risiko. Die Abbildung 6 (vorhergehende Seite) zeigt unterschiedliche FMEA im Produkt Entstehungs-Prozess.

## Die System-FMEA im Safety-Projekt

*Teil 5 erörterte die Verwendung des Werkzeuges FMEA in der Entwicklung funktional-sicherer Komponenten. Er beschrieb den Schritt von den normativen Anforderungen zur praktischen Anwendung und zog die typischen Anforderungen der Fabrikautomation heran: SIL 3, Anforderungsrate High Demand.*

Abhängig vom zu erreichenden Sicherheitsintegritätslevel macht die Norm konkrete Vorgaben bezüglich der zu erreichenden *Hardwarefehlertoleranz* (HFT) sowie dem *Anteil sicherer Fehler* (SFF). Neben fehlersicheren Design-Prinzipien sind Diagnosemaßnahmen der Schlüssel zu einer hohen SFF. Die Tabelle in Abbildung 7 veranschaulicht diesen Zusammenhang.

Die Vielfalt und die gegenseitige Abhängigkeit der Einflussfaktoren erschweren gerade Neueinsteigern die Anwendung und führen bei falscher Anwendung oft zu sub-optimalen Ergebnissen. Typische negative Folgen in der

| | HARDWARE-FEHLERTOLERANZ FÜR SICHERHEITSBEZOGENE ELEMENTE | | | | | |
|---|---|---|---|---|---|---|
| | HFT=0 | | HFT=1 | | HFT=2 | |
| ANTEIL SFF | TYP A | TYP B | TYP A | TYP B | TYP A | TYP B |
| < 60% | SIL 1 | — | SIL 2 | SIL 1 | SIL 3 | SIL 2 |
| 60% – < 90% | SIL 2 | SIL 1 | SIL 3 | SIL 2 | SIL 4 | SIL 3 |
| 90% – < 99% | SIL 3 | SIL 2 | SIL 4 | SIL 3 | SIL 4 | SIL 4 |
| ≥ 99% | SIL 3 | SIL 3 | SIL 4 | SIL 4 | SIL 4 | SIL 4 |

*Abbildung 7: Zusammenhang HFT und SFF*

Praxis sind die Notwendigkeit von Anpass-Entwicklungen, die erst spät im Entwicklungszyklus erkannt werden. Es ist aber auch Over-Engineering von Sicherheitsmaßnahmen, die zu Lasten der Verfügbarkeit des Produkts gehen und das Produkt unnötig verteuern. Design Packages für sichere Antriebstechnik auf Basis der EN 61800-2 minimieren solche Risiken.

Neben sehr produktspezifischen Blöcken, wie dem Leistungsteil und der Steuereinheit, eignen sich Funktionsblöcke wie Diagnostic Functions sowie Communication & IO-Block zur Standardisierung als generischer Funktionsblock, der letztlich Zeit, Aufwand und Personal schont und wiederverwendet werden kann. In Form von:

- Anforderungen
- abgenommener Dokumentation
- spezifischer FMEA
- spezifischem Testdesign und Testprotokollen

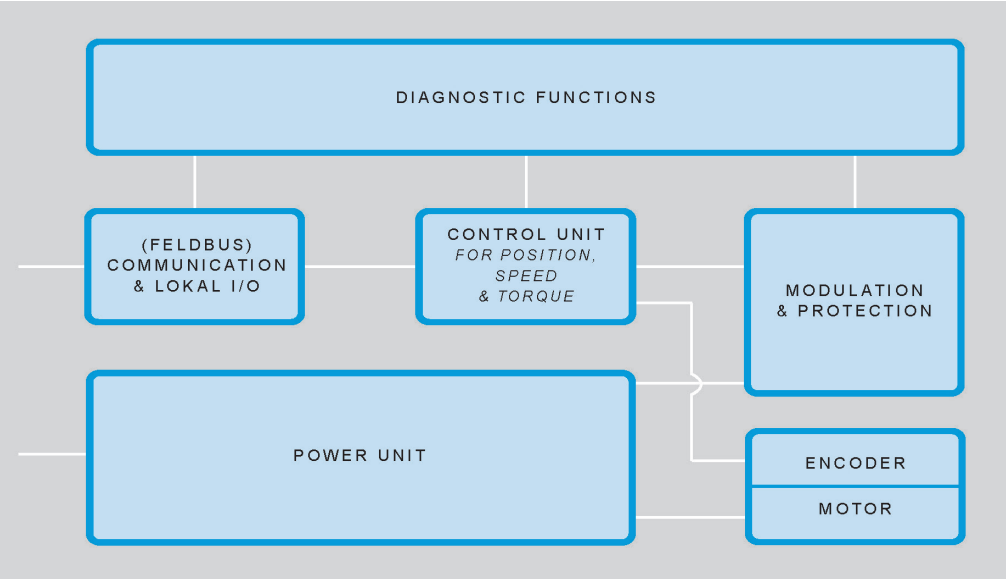


*Abbildung 8: Blockschaltbild sicherheitsgerichteter Antrieb - PDS(SR)*

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

*In Teil 6 haben wir uns mit der Frage beschäftigt, welche Themen bzw. Forderungen sich überhaupt aus der IEC 61508-1 für den Komponentenhersteller ergeben und welche Unternehmensbereiche dadurch beeinflusst werden.*

Funktionale Sicherheit funktioniert nicht ohne Unterstützung des Top-Managements. Bei der IEC 61508 handelt es sich nämlich nicht nur um eine weitere Norm, die von der Entwicklungsabteilung einzuhalten ist. Sie betrifft das ganze Unternehmen. Die IEC 61508 definiert ausführlich das Management der *Funktionalen Sicherheit* (FSM) als Erweiterung eines ISO 9001-Qualitätsmanagement-Systems.
In der Praxis ist meist eine Kombination von Anpassungen an mehreren Stellen angebracht:

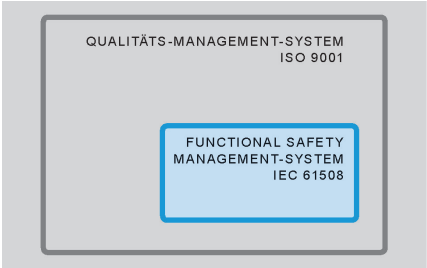


*Abbildung 9: Zusammenhang QM / FSM*

- Einführung von zusätzlichen Prozessen
- Einführung von zusätzlichen / neuen Werkzeugen
- Anpassung von Meilenstein-Checklisten
- Anpassung bzw. Neuerstellung von Templates
- Einführung und Beschreibung neuer Methoden (z.B. zur Durchführung einer FMEDA)

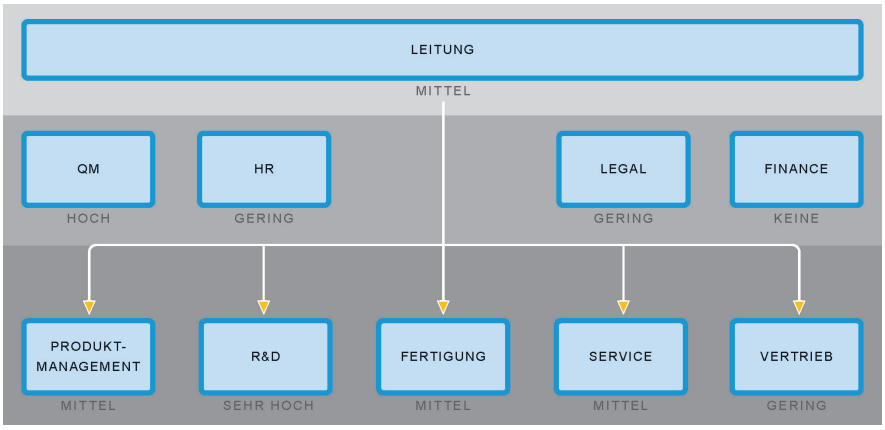


*Abbildung 10: Wie breit die Einflüsse der Funktionalen Sicherheit sind kann überraschen!* Übersicht der beeinflussten typischen Unternehmensbereiche

## Ein Resümee

Diese Informationen, Schaubilder und Schilderungen zeigen, warum die Einführung eines FSM-Systems und der Aufbau einer Functional Safety Entwicklung sinnvoll ist. Sie zeigen aber auch, dass das zeitaufwändig ist, weit über die Entwicklung hinausgeht, Fallstricke in jeglicher Hinsicht bereithält und am besten selbst als Projekt angegangen wird.

Die größte Motivation, sich dieser Herausforderung zu stellen, ist häufig die zunehmende Nachfrage nach Safety-Produkten und die Gefahr, ohne Safety-Produkte im Portfolio gegenüber dem Wettbewerb zurückzufallen. Kunden bevorzugen den Kauf aus einer Hand.

Für ein Vorprojekt zum Aufbau eines Functional Safety Management Systems sollten drei bis sechs Monaten veranschlagt werden. Die Länge der Vorlaufzeit eines Entwicklungsprojekts hängt jedoch stark vom Unternehmen, den Bestandprozessen und den verfügbaren Ressourcen ab.

Das Management der Funktionalen Sicherheit hat viele Überlappungen mit dem Qualitätsmanagement. Somit ist eine Trennung der Disziplinen nicht sinnvoll. Bewährt hat sich, das FSM als Teilmenge des QM aufzufassen. Lebt die ISO 9001 im Unternehmen und existiert ein reifes Prozessmanagement, ist bereits eine stabile Basis für die Einführung eines Functional Safety Managements gegeben.

Prozessorientierung bei der Produktentwicklung trägt maßgeblich dazu bei, Entwicklungsrisiken zu vermeiden, die Produktqualität zu verbessern, Product Life Cycle Costs zu reduzieren, externe Auditierungs- und Zertifizierungskriterien zu erfüllen und schlussendlich die Time-to-market zu verkürzen.

Es bedarf Erfahrung, Expertise und Pragmatismus, um die geforderten Strukturen aufzubauen (beziehungsweise anzupassen) und um eine typische Überauslegung der Anforderungen zu vermeiden.

Die Artikelserie hat gezeigt, dass Prozesse und Strukturen nicht behindern müssen, sondern gerade dazu dienen, geistige Freiräume zu schaffen, in denen wahre Innovationen entstehen.

**Autoren:**
Dr. Johann Pohany, Managing Director
Medidtcine Consultants / www.medidtcine.com

Armin Götzmann, Geschäftsführer
MESCO Systems GmbH / www.mesco.de