WHITEPAPER

PRODUCT-LIFECYCLE-MANAGEMENT

… von Komponenten Funktionaler Sicherheit in der Industrieautomation

Funktionale Sicherheit spielt in der industriellen Automation eine immer stärkere Rolle. Komponentenhersteller, die bisher den hohen Aufwand für die Einführung von Safety-Produkten gescheut hatten, sind nun mit dem steigenden Marktdruck konfrontiert und müssen ihre Produktportfolios um Funktional-sichere Produktvarianten ergänzen. Dabei sind schon die Herausforderungen für Standardprodukte groß, und es kommen bei FS-Produkten zusätzliche Aufgaben hinzu.

Dieses Whitepaper beleuchtet zum einen den Einstieg in dieses vielschichtige Thema und bietet zum anderen neue Perspektiven. Der nachfolgende Text teilt den Lebenszyklus eines Produkts in die Phasen *Marktvorbau, Produktdefinition, Produktentwicklung, Markteinführung* und *Serien-geschäft* ein und beschreibt anhand dieser Gliederung typische Herausforderungen, Aufgaben und mögliche Lösungsansätze.

Vor der Betrachtung der einzelnen Phasen, steht jedoch die Frage, warum sich viele Unternehmen mit der Funktionalen Sicherheit schwer tun. Ansatzpunkt ist die *Mutternorm* IEC 61508. Genau genommen ist sie eine ganze Normenreihe mit sieben Einzelpapieren (IEC 61508-1 bis IEC 61508-7) und insgesamt fast 700 Seiten. Die IEC 61508 beschreibt einen allgemeinen Lösungsweg für alle Tätigkeiten im Lebenszyklus eines sicherheitsgerichteten Systems. Da sie nicht auf eine bestimmte Branche, Marktsegment oder Produktgruppe ausgerichtet ist, passt die Bezeichnung *allgemeiner Lösungsweg* gut. So geht sie zum Beispiel auf industrie- bzw. produktspezifische Sachverhalte nicht ein und überlässt dies der Auslegung durch den Verwender.

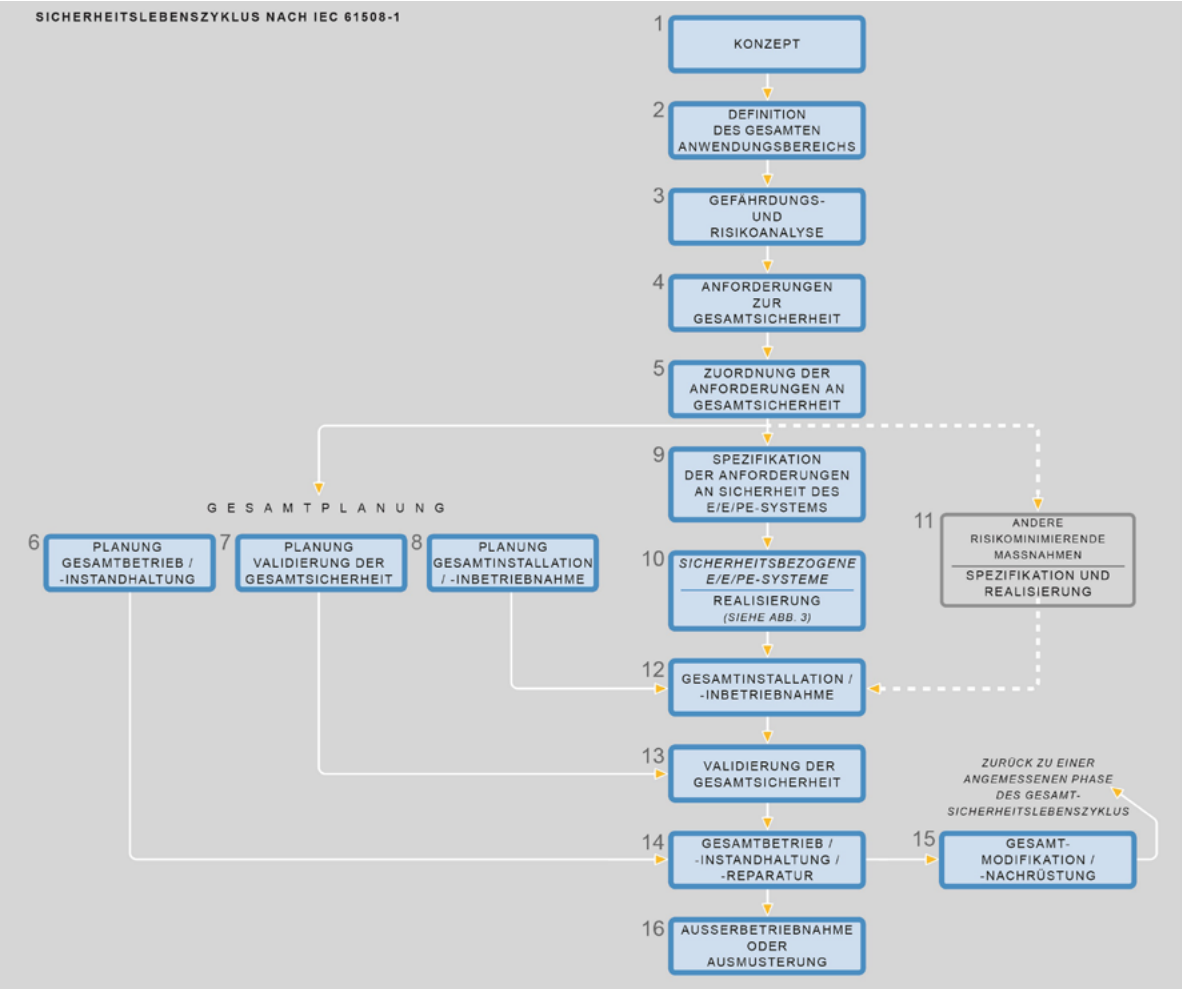


Abbildung 1
Sicherheits-lebenszyklus nach IEC 61508-1

Probleme für Komponentenhersteller

Die Norm macht keine explizite Unterscheidung zwischen den industrietypischen Beteiligten, wie Anlagenbetreiber, Maschinenbauer, Systemintegrator, Komponentenhersteller und den Bauteilelieferanten. Auch in der Praxis dürfte es kaum ein Unternehmen geben, für das alle Teile der Norm von Relevanz sind. Jeder Akteur muss zunächst die für ihn relevanten Inhalte herausarbeiten.

Mit dem Sicherheitslebenszyklus aus der IEC 61508-1 kann das verdeutlicht werden (siehe Abb. 1). Die Norm suggeriert einen Ablauf der sich, vereinfacht, folgendermaßen darstellt:

- *Phase 1 – 3:* Anlage, die auf von ihr ausgehende Gefährdungen untersucht wird
- *Phase 4 – 9:* die notwendige Sicherheitsfunktion wird definiert
- *Phase 10, Teil 1:* ein geeignetes elektronisches Sicherheitssystem (zur Ausführung der definierten Sicherheitsfunktion) wird entwickelt
- *Phase 10, Teil 2:* das elektronische Sicherheitssystem wird getestet
- *Phase 12:* das Sicherheitssystem wird in die Anlage eingebaut
- *Phase 13:* die Anlage wird auf Tauglichkeit hin untersucht

Gerade für Einsteiger sind manche Fragen schwer zu beantworten. *Etwa*: Wie hängen Gefährdung, Sicherheitsfunktion, das sicherheitsgerichtete System und die einzelnen Komponenten zusammen? *Oder auch*: Welche zeitlichen Abhängigkeiten werden von der Norm gefordert?

Folgende Betrachtungen schaffen dafür Transparenz:
Von einer realen Maschine oder Anlage geht eine konkrete Gefährdung aus, der mit einer Gegenmaßnahme begegnet werden soll. Die Maßnahme kann konstruktiver oder organisatorischer Natur sein, aber eben auch eine Sicherheitsfunktion. Die Sicherheitsfunktion wird vom sicherheitsgerichteten System ausgeführt. In der Automation setzt sich das in der Regel aus Einzelkomponenten wie Sensoren, Steuerungen und Aktoren zusammen. So wird auch klar, dass eine einzelne Komponente nicht mit der Sicherheitsfunktion gleichzusetzen ist. Die Komponente liefert einen Beitrag zur Realisierung der Sicherheitsfunktion.

Häufig wird die Norm auch dahingehend (fehl)interpretiert, dass die einzelnen Phasen streng sequentiell zu durchlaufen sind. Dies würde bedeuten, dass der Komponentenhersteller erst dann mit seiner Produktdefinition beginnen würde, wenn er den konkreten Bedarf einer Applikation kennt. In der Praxis darf und wird natürlich der Komponentenhersteller in *Vorleistung* treten und Produkte entwickeln, die dann später für den Systemintegrator bereits als Serienprodukte zur Verfügung stehen. **Der Komponentenhersteller darf also Annahmen zur späteren Verwendung treffen, ohne hier die Norm zu verletzen.**

Ebenfalls macht die Norm keinen Unterschied zwischen der einmaligen Komponentenentwicklung und der zyklischen Serienproduktion. Das wirft die Frage auf, ob die geforderten ausführlichen Tests während der Produktentwicklung auch für jedes einzelne (serien)produziertes Exemplar anzuwenden sind.

Kern der Norm ist die Vermeidung und Beherrschung von Fehlern, die dazu führen könnten, dass die Sicherheitsfunktion versagt. Sie fordert daher die Anwendung von umfangreichen Schritten und Methoden. Aufgrund der verschiedenen Fehlerarten – wie *zufällige Fehler*, *systematische Fehler* oder *Fehler mit gemeinsamer Ursache* – sind sie sehr unterschiedlich und umfassen technische, organisatorische sowie qualitätssichernde Maßnahmen.
Auch sind ein lineares Lesen und die anschließende Anwendung der Norm durch ihren didaktischen Aufbau praktisch nicht möglich.

Bei aller Kritik muss man der Norm zu Gute halten, dass sie explizit als **Basis für die Erstellung von produkt- und anwendungsspezifischen Normen** gedacht ist. Im Standard für sicherheitsgerichtete Antriebe (EN 61800-5-2) sind etwa viele allgemein dargestellte Sachverhalte der IEC 61508 produktspezifisch formuliert und damit deutlich besser verständlich. Die Antriebsnorm für das Management der Funktionalen Sicherheit und für sicherheitsgerichtete Software verweist jedoch direkt auf die jeweiligen Teile der IEC 61508.

Die Auswirkungen auf den Produktlebenszyklus

Der Aufbau des Whitepapers sowie die Abbildungen orientieren sich an dem industrieüblichen Produktlebenszyklus, wie er für Komponentenhersteller in der industriellen Automation gängig ist, mit den für FS-Produkte typischen Durchlaufzeiten der Phasen. Die Zeiten können natürlich individuell schwanken. Deutlich werden soll jedoch, wie lange der Zeitraum sein kann, über den sich der Produktlebenszyklus einer (sicherheitsgerichteten) Komponente erstreckt.

Grundsätzlich lassen sich die (Prozess-)Anforderungen der IEC 61508 gut in die existierenden Prozesse integrieren. Ein häufiges Missverständnis ist, dass die IEC 61508 den ganzen Prozess, samt Dokumenten und Begrifflichkeiten, streng vorgibt. Tatsächlich liegt die Kunst in der richtigen Interpretation des Standards für die Zwecke und den individuellen Gegebenheiten des Unternehmens.

Die Vorfeldphase

Sofern in einem Unternehmen noch keine oder nur geringe Erfahrungen mit Funktionaler Sicherheit vorhanden sind, empfiehlt es sich, mit einer eintägigen Grundlagenschulung

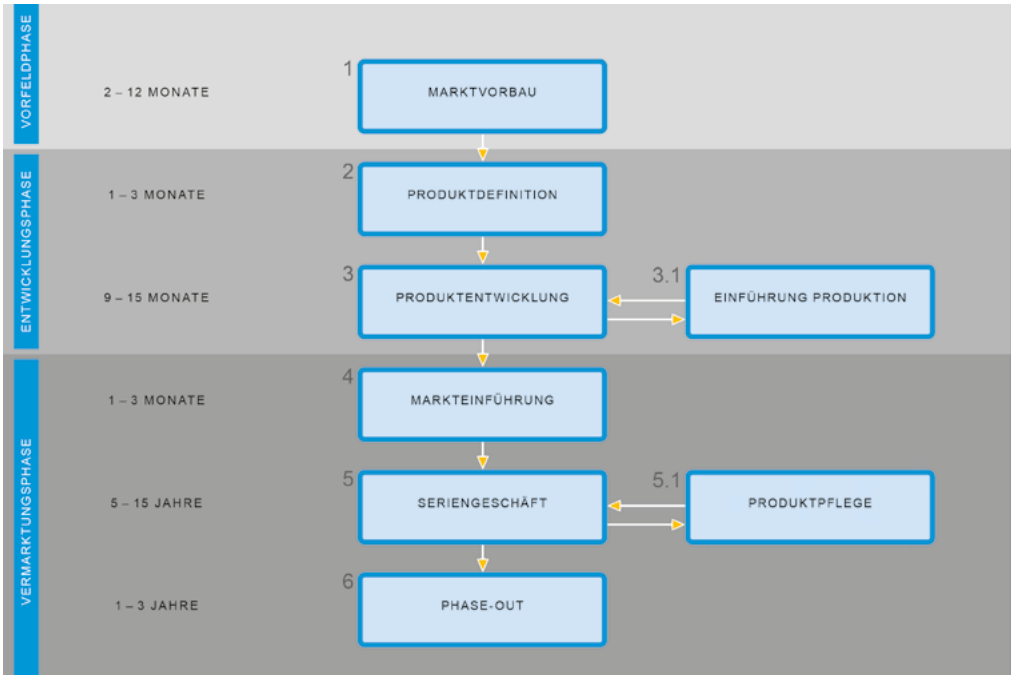


Abbildung 2
Beispiel einer typischen Lebenszyklusphase einer Komponente

zu beginnen, in der die Grundzüge der Funktionalen Sicherheit und die Auswirkungen auf die verschiedenen Bereiche des Unternehmens in kompakter Form dargelegt werden. Diese Schulung dient primär zur Sensibilisierung aller Beteiligten, bis hin zum oberen Management, da ohne dessen Unterstützung *Safety* nicht umsetzbar ist.

Ein zeitnah an die Grundlagenschulung anschließender ein- bis zweitägiger Workshop empfiehlt sich. Darin erfolgt eine Bestandsaufnahme der Ziele, der Rahmenparameter und des Reifegrades des Projektvorhabens. Neben ersten technischen Betrachtungen und der Abschätzung von Kosten- und Zeitaufwänden sollten nun mögliche passende Projektkonstellationen und mögliche Vorgehensweisen diskutiert werden.

Modellhafte Projektkonstellationen können sein:
- Eigenentwicklung
- Eigenentwicklung mit entwicklungsbegleitender Beratung
- Eigenentwicklung mit Rückgriff auf vorentwickelte Module
- Externe Entwicklung (als Teil- oder gesamtes Projekt)
- Fremdbezug / Brandlabel eines existierenden Produkts

In der Praxis wiederum sind auch Kombinationen möglich, etwa wenn Teilprojekte sinnvoll abgespaltet werden können.

Im Nachgang zum Workshop ist eine ausführliche Bewertung in Form eines schriftlichen Berichts wichtig, in dem auch die empfohlenen Maßnahmen festgehalten sind.

Falls ein Functional Safety Management System (FSM) noch nicht vorhanden ist, hat sich zum Aufbau und zur Einführung der erforderlichen Prozesse eine möglichst frühe und detaillierte Gap-Analyse bewährt. Dabei wird der Bestandsprozess mit den relevanten Anforderungen der IEC 61508 verglichen und mögliche Anpassungen bereits evaluiert.

Auch die strategischen und operativen Ziele des Unternehmens sind zu berücksichtigen. Etwa:
- Soll ein vollumfängliches Functional-Safety-Management-Systems intern aufgebaut werden oder sollen ggf. Teile im (Safety)-Lifecycle durch externe Organisationen erbracht werden?
- Bleiben FS-Produkte eher Exoten im Portfolio oder wird eine dominierende Stellung erwartet?
- Welche Produktstrategie wird verfolgt: Kostenführerschaft, Innovationsführerschaft, ein reines Me-Too-Produkt oder Brand Labelling?

Ein eingeführtes und gelebtes QM-System nach ISO 9001 stellt erfahrungsgemäß eine sehr gute Basis dar und deckt auch Anforderungen der IEC 61508 bezüglich Dokumentation und Umgang mit Modifikationen gut ab. Die Erfahrung zeigt auch, dass es praktisch immer Lücken gibt, die zu schließen sind.

Verantwortlichkeiten und Aufgaben für das Management der funktionalen Sicherheit, sowie die Formulierung der Qualifikationsanforderungen, sind möglicherweise noch nicht im Unternehmensprozess verankert. Die erforderliche Anpassung kann aber, bis zu einem gewissen Grad, zeitlich überlappend mit dem Entwicklungsvorhaben erfolgen. So können zum Beispiel die Prozesse, die die Vermarktungsphase betreffen, noch während der Entwicklungsphase entworfen und gezielt geschult werden. Erfahrungsgemäß erstreckt sich diese Prozessanpassung über einen Zeitraum von mehreren Monaten.

Will das Unternehmen die Entwicklung größtenteils mit eigenen Entwicklungsressourcen durchführen, empfiehlt sich eine tiefergehende Schulung für die beteiligten R&D-Mitarbeiter im Projekt. Solche Schulungen gehen fundiert auf die Anforderungen der IEC 61508-2 (Systementwicklung / Hardwareentwicklung einschließlich ASIC & programmierbare Logik) und der IEC 61508-3 (SW-/FW-Entwicklung) ein und zeigen, wie diese praxisorientiert umgesetzt werden. Für beide Teile sind jeweils zwei Tage einzukalkulieren.

Häufig bieten derartige Schulungen eine Prüfung inklusive Zertifikat optional an. Das kann den Nachweis der erforderlichen Qualifikation erleichtern, ist aber normativ nicht zwingend erforderlich.

Aus Sicht der IEC 61508 ist der Marktvorbau keine formal geforderte Phase. Wie bereits beschrieben, werden in der Industriepraxis sowohl die erforderlichen sicherheitsgerichteten Komponenten, als auch die Standardkomponenten nicht erst dann entwickelt, wenn ein Systemintegrator sie benötigt. Sie sind in der Regel zum Zeitpunkt der Auswahl bereits als Serienprodukte verfügbar. Der Komponentenhersteller muss daher die Anforderungen des Marktes *vorweg* nehmen. Eine Aufgabe, die in größeren Unternehmen oft im Produktmanagement verankert ist. Da hierzu die *Zukunft antizipiert* werden muss, tun sich viele Unternehmen damit schwer. In dieser Phase wird jedoch der Grundstein für den Markterfolg gelegt. Die relevanten Informationsquellen sind in den meisten Unternehmen vorhanden bzw. leicht zu erreichen und könnten so auch systematisch ausgewertet werden.

Es lohnt sich sehr, zu Beginn der Vorfeldphase Informationen zu sammeln. Dazu gehören fundierte Markt-/Wettbewerbsanalysen. Zudem sind Kunden und eigene Mitarbeiter mit Kundenkontakt – wie Vertrieb, Applikation oder Service – Quellen für relevante Infos. Auch das weitere Marktumfeld und technologische Trends bergen Hinweise. Ein solcher Marktvorbau generiert zudem oft weitere Produktideen, die ebenfalls in einen strukturierten Entscheidungsprozess einfließen können.

Nach der Festlegung des favorisierten Produkts rückt die Erstellung des Lastenhefts mit dem richtigen *Requirement-Bündel* für das Produkt in den Fokus des Produktmanagements.

Die Entwicklungsphase

Die Erstellung des Lastenhefts bildet den Übergang zur Entwicklungsphase. Sie entspricht nahezu vollständig der *Phase 9* des Sicherheitslebenszyklus der IEC 61508-1. Streng genommen fordert die Norm nur die Formulierung der sicherheitsrelevanten Anforderungen. In der Praxis werden diese meistens aber nicht in einem separaten Dokument, sondern als Bestandteil des Lastenhefts erfasst. Sie werden explizit als *sicherheitsrelevant* gekennzeichnet und oft mit dem Begriff *Safety Requirements Specification* (SRS) benannt.

Typische zusätzliche Kriterien für ein FS-Produkt sind:
Der SI-Level (SIL); die Ausfallraten; die *Anforderungsrate*; der Beitrag zur *Sicherheitsfunktion*; der sichere Zustand und die *maximale Fehlerreaktionszeit* bzw. zu *unterschreitende Prozesssicherheitszeit*.

Wie beschrieben, trifft der Komponentenhersteller Annahmen über die spätere Verwendung seines Produkts. Es empfiehlt sich, das im Lastenheft zu skizzieren, ohne dabei die Verwendung zu stark einzuschränken. Die *Verwendungshinweise* werden über die Betriebsanleitung (IEC 61508: Sicherheitshanbuch / Safety Manual) vom Komponentenhersteller zum Systemintegrator weitergegeben.

Je präziser dieses Lastenheft ausgearbeitet ist, umso vorteilhafter ist es. Besondere Aufmerksamkeit gilt hier den formalen Aspekten, wie eindeutige Aussagen, Vollständigkeit, präzise Formulierungen, Testbarkeit der Anforderungen und Durchführung einer Verifikation (typ. protokolliertes Review). Darin unterscheidet es sich in der Regel von einem gängigen Lastenheft.

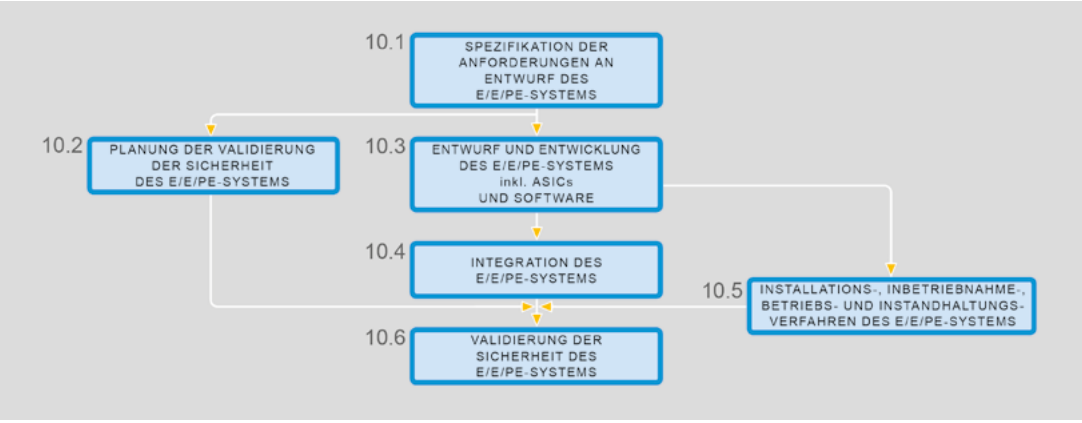


Abbildung 3
Sicherheitslebenszyklus des E/E/PE-Systems (in der Realisierungsphase)

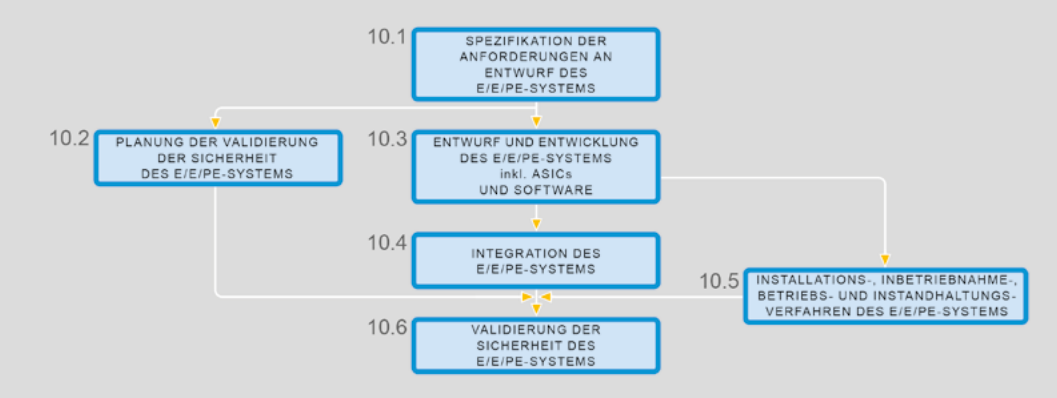


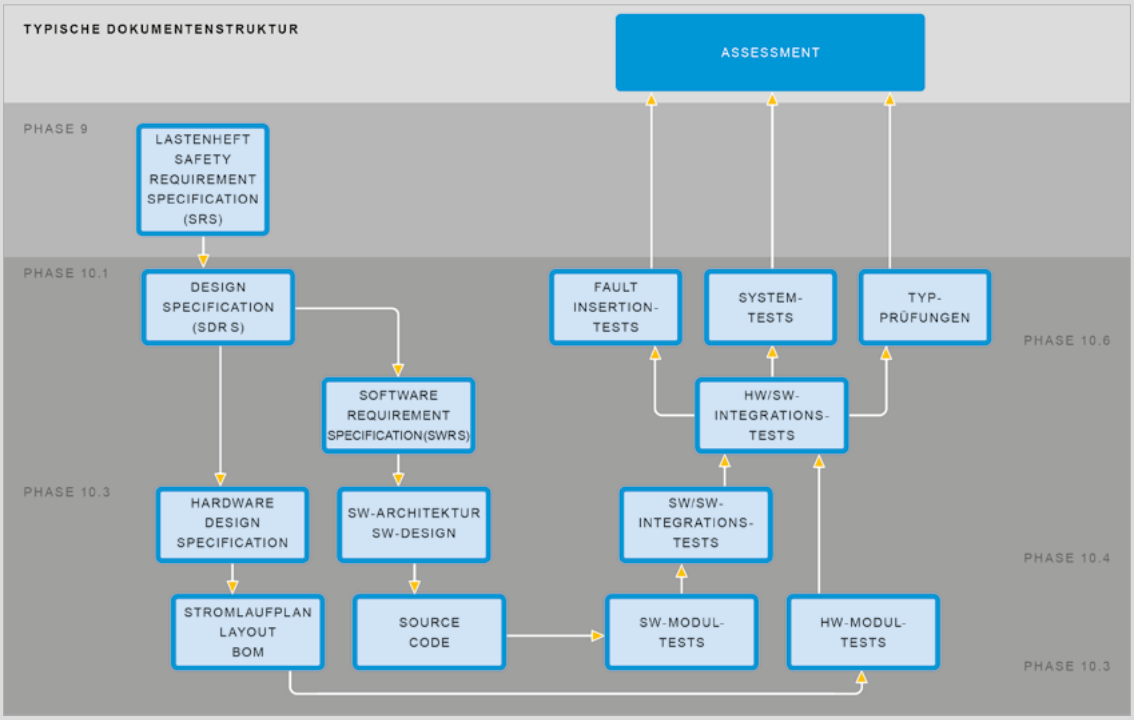
Abbildung 4
Software-Sicherheitslebenszyklus (in der Realisierungsphase)

Unabhängig von der FS empfiehlt es sich, die klassischen Anforderungen eines Lastenhefts zu beachten und das „Was“ (*Welche Eigenschaften soll das Produkt haben.*), aber nicht das „Wie“ (*Wie soll das technisch umgesetzt werden.*) zu beschreiben. Die Prüfbarkeit der Requirements spielt auch deswegen eine große Rolle, da die geforderte spätere Validierung gegen das Lastenheft durchgeführt wird.

Die reine Entwicklungsphase, also die technische Umsetzung, ist komplex. Sie entspricht zwar zunächst direkt der *Phase 10* im Sicherheitslebenszyklus, in der IEC 61508-2 und IEC 61508-3* wird sie jedoch in weitere Phasen unterteilt (*sofern auch die SW sicherheitsrelevant ist).

V-Modell

Im linken Ast entstehen von oben nach unten die Requirements- und Design-Dokumente, sowie die jeweils zugehörigen Testspezifikationen. Der rechte Ast umfasst die Durchführung der Prüfungen und Erstellung der Testprotokolle. Er wird von unten nach oben durchlaufen. Zumindest in der Theorie steht eine Verifikations- bzw. Validierungsebene auf der rechten Seite genau einer Requirements bzw. Design-Ebene auf der linken Seite gegenüber. In der Praxis adressieren vor allem auf der *Validierungsebene 10.6* die Tests mehrere Ebenen der linken Seite. Wichtig ist, dass in Summe allen Anforderungen der linken Seite ein geeigneter (bestandener) Test auf der rechten Seite zugeordnet ist.
Bei einem Safety-Produkt stellt in der Regel das Assessment den Abschluss der Entwicklungsphase dar.



Die Anforderungen aus dem Lastenheft werden nun in feinere, konkrete Design-Requirements heruntergebrochen. Der Kerngedanke dabei ist, die Anforderungen handhabbar für die Entwickler zu machen und so die Wahrscheinlichkeit von Designfehlern bei der technischen Umsetzung in der Elektronik bzw. in der Software zu minimieren.

Ist auch die Software der Komponenten sicherheitsrelevant, ergibt sich ein eigener Software-Sicherheitslebenszyklus, der aber natürlich sehr eng mit dem System- bzw. Hardware-Lebenszyklus verbunden ist.

Bringt man die diversen entstehenden Dokumente, die auch für das abschließende Assessment zwingend erforderlich sind, in einen grafischen Zusammenhang, ergibt sich die typische V-Struktur. Das erklärt, warum meistens das V-Modell im Entwicklungsprozess sicherheitsgerichteter Produkte verwendet wird.

Die Vermarktungsphase

Der Zeitpunkt der nach außen gerichteten Vermarktungsaktivitäten liegt grundsätzlich im Ermessen jedes Unternehmens. In unserem Fall gehen wir modellhaft davon aus, dass die Produkte alle relevanten Zulassungen bestanden haben und als Serienprodukt bestellbar sind.

Neue Produkte verkaufen sich meist nicht von alleine. FS-Produkte machen da keine Ausnahme. Sie sind zudem stark erklärungsbedürftig. Die Vertriebsmitarbeiter stehen also vor großen Herausforderungen. Idealerweise werden daher in einer aktiven Markeinführungsphase Mitarbeiter im Kundenkontakt (Vertrieb, Applikation, Service) intensiv geschult. Im Mittelpunkt stehen hierbei natürlich die Verwendung des Produkts und sein Einsatz für (System-)Sicherheitsfunktionen. Berührungsängste können so aktiv abgebaut und den Vertriebsmitarbeitern im Vorfeld ein grundlegendes Verständnis für die Fragen der Endanwender mitgegeben werden.

Wie bei jedem Produkt, muss auf Basis des Produktsicherheitsgesetzes, eine aktive Marktbeobachtung erfolgen: Wie wird mein Produkt von den Kunden verwendet? Werden die Anweisungen im Handbuch beachtet? Treten Qualitätsprobleme auf? Stimmen die berechneten Ausfallraten mit den tatsächlich auftretenden Ausfällen überein? Wie entwickelt sich der Stand von Wissenschaft und Technik weiter?

Bei erkannten Problemen sollte die Organisation über, bereits im Vorfeld definierte Prozesse und Abläufe, geeignete Korrekturmaßnahmen einleiten.

Durch die oft lange Produktlebenszeit sind Produktpflegemaßnahmen – aufgrund von Bauteileabkündigungen oder Normänderungen – nach einigen Jahren, eher die Regel als die Ausnahme. Die Dokumentation von Safety-Produkten ist gegenüber Standardprodukten meist deutlich umfangreicher. Das wirkt sich nun positiv aus, vor allem, wenn die ursprünglichen Entwickler nicht mehr verfügbar sind.

Ist ein Safety-Produkt beim Endkunden erst einmal etabliert, möchte er es meistens bis zur nächsten Maschinengeneration weiter einsetzen. Sind die Stückzahlen noch hoch genug, bietet sich aufgrund neuer Bauteiltechnologien nach einigen Jahren möglicherweise auch ein Design-to-Cost-Projekt an. Hierbei werden die kundenrelevanten Eigenschaften des Produkts nicht verändert, jedoch könnten etwa durch höherintegrierte Bauteile die Produktkosten gesenkt und die Margen verbessert werden.

Irgendwann hat jedoch jedes Produkt das Ende seines Produktlebenszyklus erreicht. Der Bestandskunden wird es dankend zur Kenntnis nehmen, wenn er frühzeitig über die Abkündigung informiert wird und somit die Gelegenheit bekommt, sich noch resteinzudecken. Ideal ist natürlich auch, die Abkündigung frühzeitig in der eigenen Portfoliostrategie zu berücksichtigen, damit überlappend geeignete Ersatztypen verfügbar sind und Bestandskunden Migrationspfade aufgezeigt werden können.

Fazit

Der Einstieg ins Thema und die Anwendung der Funktionalen Sicherheit sind kein leichtes Unterfangen. Um langfristig Zeit und Geld zu sparen, ist es ratsam, durch externe Unterstützung die Lernkurve schneller zu durchlaufen und von den Erfahrungen anderer zu profitieren. Eine Kombination aus Grundlagenschulung, Workshops, Aufbauschulungen und einer, das Projekt begleitenden Beratung, ist dabei eine mögliche und bewährte Option.

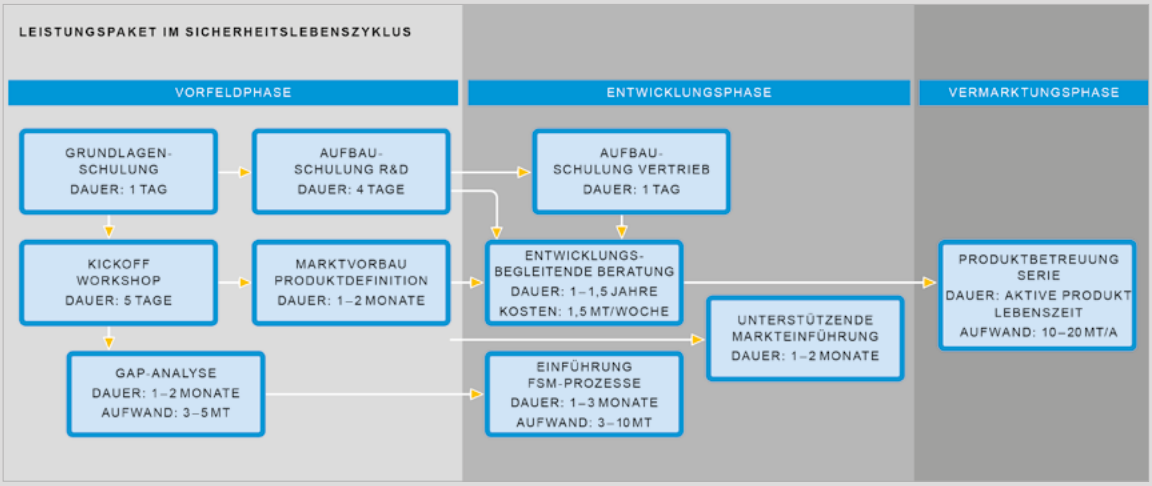
Für Unternehmen, die ihr Portfolio mit Safety-Produkte abrunden möchten, sich aber auf ihre Kernkompetenzen konzentrieren müssen, kann auch ein gesamtes Outsourcing attraktiv sein, indem eine externe Produktbetreuung während der Vermarktungsphase erfolgt.

... und aus Ideen werden Erfolge!

DEVELOPMENT CONSULTING

Möglichkeiten zur externen Unterstützung

Die folgende Grafik bietet einen Überblick über mögliche Leistungspakete, mit den typischen zeitlichen Aufwänden entlang des Produktlebenszyklus.



Das Beratungspaket von MESCO

Produktdefinition

- Gap-Analyse
- FS-Grundlagenschulung
- Support bei der Prozessanpassung
- Beratung zur Portfoliogestaltung
- Beratung zur Produktstrategie und Produktdefinition
- Erstellung (Safety) Requirements

Produktentwicklung

- Entwicklerschulung IEC 61508-2/-3 / Coaching während der Produktentwicklung
- Durchführung der Produktentwicklung
- Musterfertigung
- Erstellung der FS-Dokumentation
- Durchführung Verifikations-/Validierungstests
- Erstellung Safety Manual
- Betreuung der Produktzulassungen
- Serienführung

Markteinführung

- Schulungen der Vertriebs-/Marketing-Mitarbeiter
- Schulungen der Applikationsingenieure
- Unterstützung bei Gestaltung von Vertriebs-/Marketing-Maßnahmen (z. B. PR, Fachartikel)

Sprechen Sie uns an >

...und aus Ideen werden Erfolge!