Willi Huber
ift Rosenheim

Funktionale Sicherheit bei Tür und Tor

EN ISO 13849-1-2: Sicherheit beginnt bei der Produktdefinition

1 Einführung

Wer denkt bei Produktinnovationen und zu Beginn eines Entwicklungsprojekts für eine neue Produktgeneration schon gleichzeitig gerne an Vorgaben durch Normen. Hoch motivierte Entwickler und Konstrukteure möchten ihre Ideen umsetzen und möglichst technische Höchstleistungen erreichen. Den Ideen soll dabei größtmöglicher Freiraum gegeben werden, um die Entwicklungsmotivation auf hohem Niveau zu halten und bestehende technologische Konzepte bestenfalls noch zu übertreffen.

Andererseits werden in Normen neben den reinen Produktanforderungen vermehrt auch Nachweise für einen strukturierten Produktspezifikations- und Entwicklungsprozess gefordert. Die Normenreihe EN ISO 13849-1 und -2 aus dem Bereich der funktionalen Sicherheit für sicherheitsbezogene Teile von Steuerungen ist ein Beispiel sehr detaillierter Vorgaben für die Spezifikationen und den Entwicklungsprozess. Aus Sicht der Produktverarbeiter und Endanwender ist die unmittelbare Einbeziehung von Sicherheitsaspekten bereits im Entwicklungsprozess nur zu begrüßen. Dies stellt eine hohe Produktsicherheit von Beginn an sicher und kann rechtzeitig Wechselwirkungen in der Anwendung berücksichtigen.

Innerhalb eines gut geplanten Prozesses ist es möglich, aber auch nötig, normative Vorgaben an den Produktdefinitions- und Entwicklungsprozess mit der Entwicklungsdynamik engagierter Entwickler zu verbinden. Normeninhalte sollten nicht primär als Hindernis, sondern als Navigator betrachtet werden, um die Produktentwicklung rechtlich und wirtschaftlich abzusichern.

2 Produktentwicklung nach der Anforderungsnorm EN ISO 13849-1

Bei den „klassischen“ Prüfungen werden Bauprodukte am ift Rosenheim auf ihr Verhalten unter Extrembedingungen getestet. Diese „Extrembedingungen“ können Umgebungseinwirkungen sein wie z.B. Temperaturbelastung, Belastung durch Feuchtigkeit/Wasser oder Wind. Andere Beispiele sind die Dauerfunktion bis zur maximalen Anzahl an Nutzungs-

zyklen oder auch die Belastung beim Einbruchversuch. Geprüft wird, ob die gewünschten Eigenschaften eines Produkts die spezifizierten Anforderungen erfüllen.

Sicherheitsfunktionen von elektrischen Steuerungen werden zunächst auf ähnliche Weise auf Ihre Funktionsfähigkeit getestet. Mit dem absichtlichen Auslösen einer Sicherheitseinrichtung wird überprüft, ob die Steuerung die vorgesehenen Sicherheitsmechanismen durchführt. Um auch hier für eine entsprechende Sicherheit des Produkts zu sorgen, erfolgen die Tests bis an die Grenzen der spezifizierten Umgebungsbedingungen – also unter Extrembelastung. Bei der funktionalen Sicherheit geht es nicht nur darum, die Funktionsfähigkeit von Sicherheitsfunktionen im Normalbetrieb einer Steuerung zu überprüfen, sondern auch um die weitere Aufrechterhaltung der Sicherheit speziell im Fehlerfall einzelner Bauteile auf einer Steuereinrichtung.

Dieser Ansatz wirkt sich ganz erheblich auf die Konzeption, Entwicklung und Prüfung von Produkten aus. Neben der Betrachtung des Normalbetriebs sind Produktverantwortliche und Entwickler gefordert, die Sicherheitsfunktionen mit dem zusätzlichen Szenario eines Fehlerfalls zu berücksichtigen. Aufgrund dieser zusätzlichen Komplexität ist es nachvollziehbar, dass normative Vorgaben für Sicherheitsfunktionen schon sehr früh bei der Produktdefinition und dem nachfolgenden Entwicklungsprozess ansetzen.

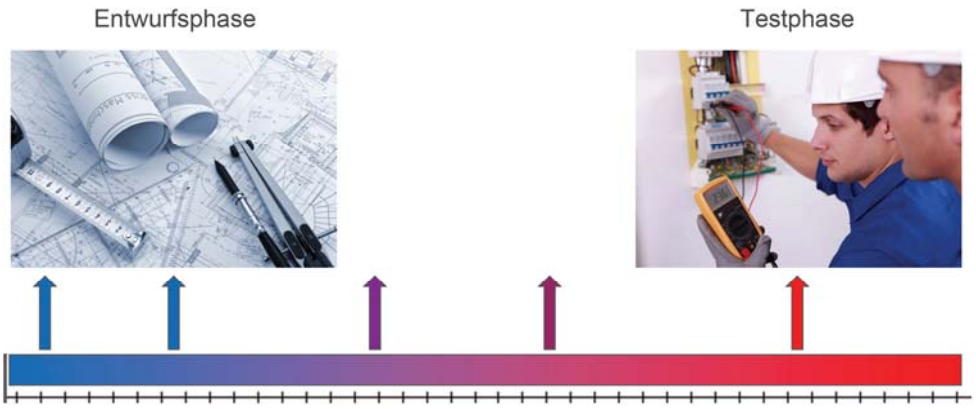

Bild 1 Verlauf Entwicklungsprozess

Die EN ISO 13849-1 als Basisnorm für die Sicherheit von Steuerungen beschreibt allgemeine Gestaltungsleitsätze für sicherheitsbezogene Teile von Steuerungen; sie setzt dabei die Anwendung strukturierter Sicherheitsfunktionen voraus. Die Norm fordert im Wesentlichen eine durchgängige Spezifikation der Sicherheitsfunktionen. Nachzuweisen sind:

– die Festlegung der Sicherheitsfunktionen für eine Steuerung,
– die Definition der Leistungsparameter jeder Sicherheitsfunktion,
– die Definition der erlaubten Umgebungsbedingungen für eine einwandfreie Funktion der Sicherheitsfunktionen,
– eine detaillierte Beschreibung der Funktionsweise jeder Sicherheitsfunktion,
– eine Beschreibung der Umsetzung jeder Sicherheitsfunktion auf Seiten der Hardware und Software,
– Beschreibung des Verhaltens der Sicherheitsfunktion im Fehlerfall,
– die Definition und Umsetzung einer adäquaten Test- und Freigabeprozedur der Sicherheitsfunktionen.

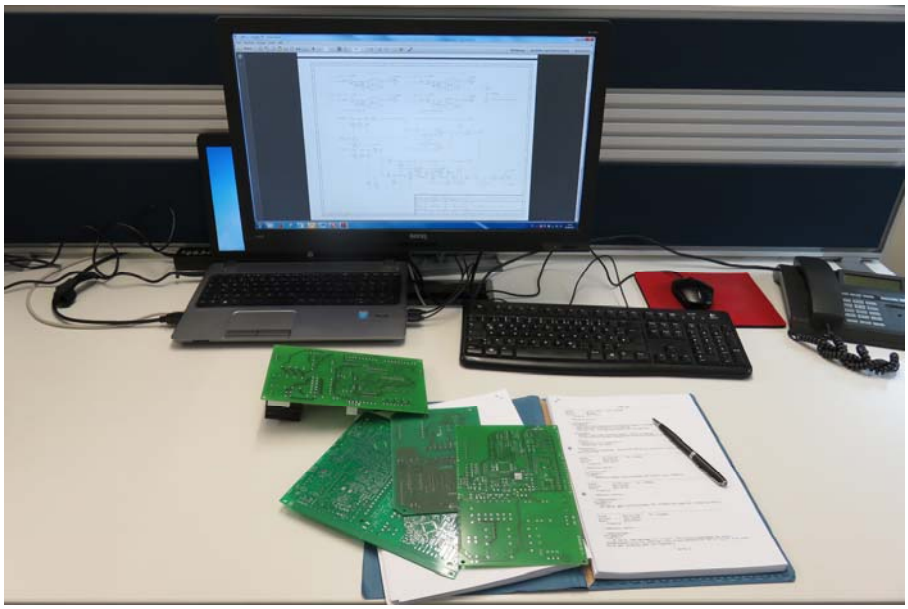

Bild 2 Prüfung der funktionalen Sicherheit durch Analyse

Dabei ist die Bearbeitungsreihenfolge der Einzelschritte streng geregelt. Vor dem eigentlichen Entwicklungsstart müssen alle die Sicherheitsfunktionen betreffenden Vorgaben inklusive des Test- und Qualifizierungsprozesses verfügbar, dokumentiert, im Vier-Augen-Prinzip geprüft und zur weiteren Bearbeitung freigegeben sein. Den Sicherheitsfunktionen und deren Gestaltung muss nach den Kriterien der funktionalen Sicherheit von Anfang an die gleiche Aufmerksamkeit entgegengebracht werden wie den eigentlichen Betriebsfunktionen einer Steuerung. Liegt dem Entwicklungsteam die vollständige Produktspezifikation vor, sind in der Entwurfsphase die Sicherheitsfunktionen nach Vorgabe mit zu erarbeiten; die Realisierung ist im Konzept im Bereich Hardware/Software nachzuweisen.

Bei der Konzeptfreigabe sind neben allen anderen Kriterien wiederum die Umsetzung der Sicherheitsfunktionen (entsprechend der funktionalen Sicherheit) innerhalb der Entwurfs-

dokumentation nachzuweisen sowie freizugeben, und die Freigabe ist zu dokumentieren. Für die Produkt-Qualifizierungstests gelten dieselben Anforderungen. Mit der Spezifikation der Sicherheitsfunktionen ist durch den Hersteller bereits zu definieren, wie die Prüfung dieser Sicherheitsfunktionen später durchzuführen ist. Anhand des definierten Testplans erfolgen Prüfung, Freigabe und Dokumentation von Prüfergebnissen und Freigabe.

Bild 3 Schrittfolge von Produktspezifikation bis Produktfreigabe

Wie können diese Vorgaben nun gewertet werden, die zweifelsohne einen zeitlichen Aufwand für Produktverantwortliche und Entwickler zu Beginn einer Produktentwicklung bedeuten? Zunächst einmal sind die Vorgaben an Sicherheitsfunktionen von Steuereinrichtungen nach EN ISO 13849-1 klar definiert und müssen folglich am fertigen Produkt vorhanden bzw. nachgewiesen sein. Dieser Umstand setzt die Festlegung und Umsetzung der Funktionalität voraus. Darüber hinaus sind Sicherheitsfunktionen an sich schon ein obligatorischer „Produktbestandteil“ und müssen von Anfang an mit berücksichtigt werden. Schließlich benötigen sie in der Umsetzung z.B. im Fall elektrischer Steuerungen zusätzliche elektronische Bauteile, Leiterplattenfläche, Prozessorkapazitäten und separate Softwarestrukturen. Sicherheitsfunktionen nach den Kriterien der funktionalen Sicherheit erweitern Steuerungskonzepte um zusätzliche Kanäle, um z.B. redundante Architekturen (parallele Sicherheitskanäle) oder Testkanäle zu implementieren.

Müssen diese Schaltungsbestandteile auf einem nahezu fertig entwickelten Produkt „nachgezogen“ werden, kann ein schwer überschaubarer Zusatzaufwand mit teils erheblichen zeitlichen Verzögerungen im Projektplan entstehen. Insofern helfen die Vorgaben zum Produktdefinitions- und Entwicklungsprozess aus EN ISO 13849-1 dabei, aufwendige und kostspielige Nacharbeit zu verhindern. Der gleiche Effekt kann mit den Zweitprüfungen und Freigaben der einzelnen Teilschritte aus dem Produktentstehungsprozess erreicht werden. Eine Überprüfung nach dem Mehraugen-Prinzip stellt sicher, dass die Vorgaben aus dem aktuellen Bearbeitungsschritt umfänglich und korrekt umgesetzt wurden. Ein Rücksprung in einen vorherigen Bearbeitungsschritt und die Wiederholung geleisteter Aufgaben aufgrund fehlender Ergebnisse kann so leichter vermieden werden.

Zu guter Letzt kann noch eine Betrachtung der geforderten Dokumentation zu Produktdefinition und Produktentwicklung erfolgen. Eine korrekte Prüfung und Freigabe eines Bearbeitungsschrittes setzt das Vorhandensein der vollständigen Dokumentation voraus, an-

sonsten kann keine ordnungsgemäße Freigabe erfolgen. Insofern stellt die Forderung zum Nachweis der umfänglichen Projektdokumentation keine zusätzliche Anforderung dar, sondern definiert nur die Vorlage ohnehin bereits verfügbarer Dokumente.

3 Fazit

Im Zuge des Nachweises der funktionalen Sicherheit nach EN ISO 13849-1 legt das ift Rosenheim besonderen Wert auf die Prüfung der Prozesse für Produktdefinition und Produktentwicklung. Aus den Erfahrungen dieser Prüfungen hat sich gezeigt, dass eine zuverlässige Einhaltung dieser Vorgaben einen reibungslosen Prüf- und Zertifizierungsprozess enorm unterstützen kann. Die Anforderungen an Produktspezifikation, Produktentwicklung, Freigabeprozeduren und der Nachweis der Dokumentation stellen keinen zusätzlichen Aufwand in der Produktentwicklung dar, sondern beschreiben lediglich die Voraussetzungen für einen zuverlässigen Entwicklungsprozess von Sicherheitsfunktionen nach den Kriterien der funktionalen Sicherheit. Die Norm regelt den zeitlichen Ablauf der Bearbeitungsschritte ohnehin erforderlicher Aufgaben. Der Vorteil der Vorgaben besteht sicherlich darin, dass auf diese Weise wichtige Aspekte nicht übersehen werden. Somit kann das Risiko von häufig sehr aufwendigen und langwierigen Nacharbeiten oder Wiederholungen von Entwicklungsschritten vermieden werden, um die Produktentwicklung rechtlich und wirtschaftlich abzusichern.

Literatur

[1] EN ISO 13849-1:2015
Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen –
Teil 1: Allgemeine Gestaltungsleitsätze.
Beuth Verlag GmbH, Berlin