Stiefmütterlich behandelt

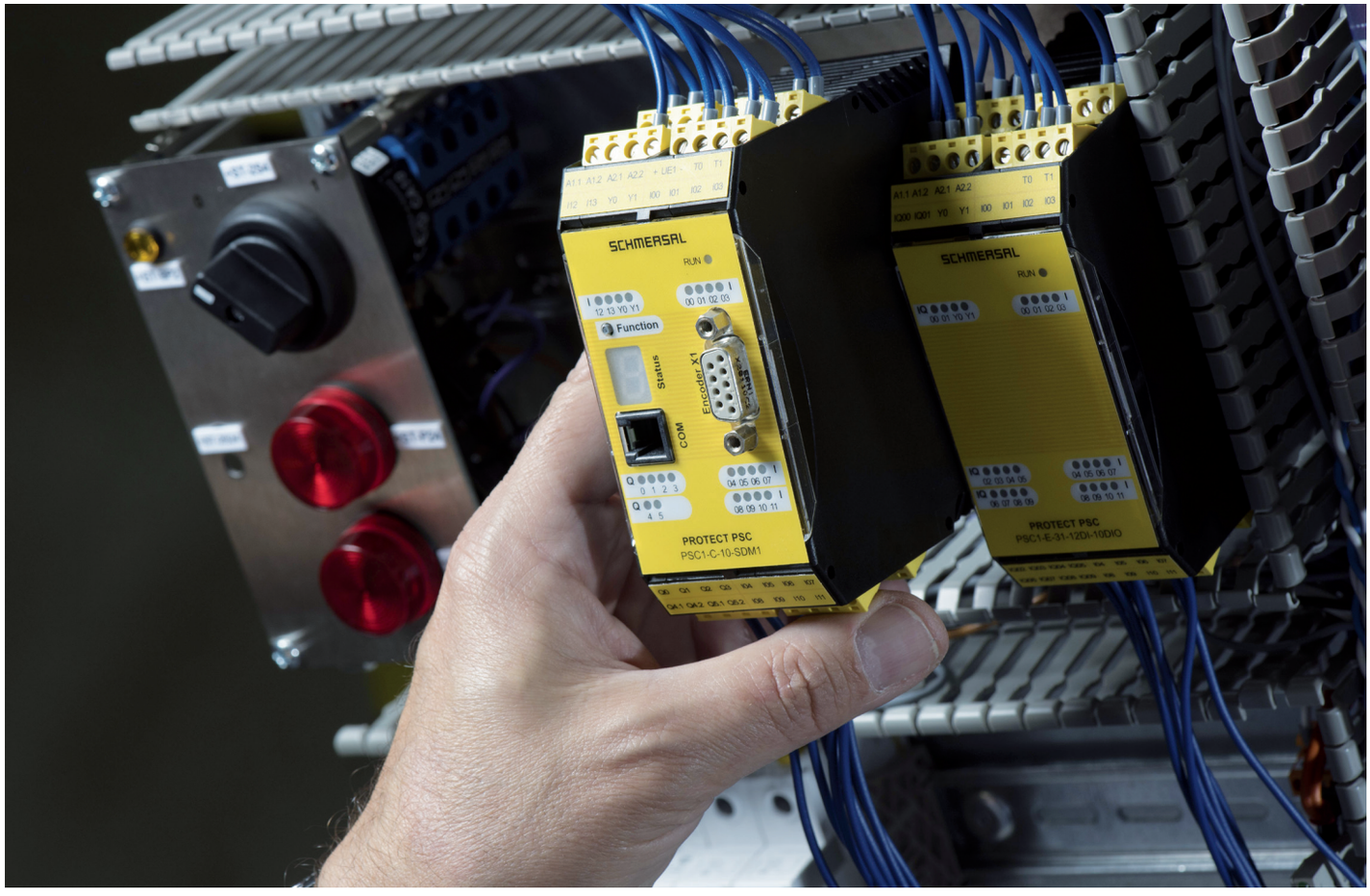
Bei der Einbindung sicherheitsgerichteter Steuerungsfunktionen in Maschinen ist die EN ISO 13849 maßgeblich. Dabei wird allerdings der die Validierung betreffende Teil der Norm in der Praxis oftmals vernachlässigt – ein großes Manko.

Die Konstruktion von Maschinen, Anlagen oder auch Gebäuden ist häufig ein langwieriger Prozess – der nicht immer zu einem zufriedenstellenden Ergebnis führt. Gelegentlich liegt dies an mangelnder Präzision bei der Planung. Manchmal liegt es aber auch daran, dass die Akteure des Entwicklungsprozesses die tatsächlichen Bedingungen aus dem Auge verlieren, in denen das Produkt zum Einsatz kommen soll. Aus diesem Grund ist es wichtig, schon im Konstruktionsprozess die Funktionsfähigkeit und Tauglichkeit eines Produktes systematisch zu überprüfen, um gegebenenfalls erforderliche Anpassungen möglichst frühzeitig vornehmen zu können. Dies ist umso mehr von Bedeutung, wenn es sich um Produkte aus dem Bereich der Maschinensicherheit handelt, die den Schutz der Gesundheit – oder sogar des Lebens – der Beschäftigten gewährleisten sollen.

Im Maschinenbau ist es häufig notwendig, Maschinen durch die Einbindung sicherheitsgerichteter Steuerungsfunktionen abzusichern. Für die konstruktive Gestaltung der „sicherheitsbezogenen Teile von Steuerungen“ ist die EN ISO 13849 Teil 1 eine zentrale und weit verbreitete Norm. Teil 2 dieser Norm aber – in dem die Vorgehensweise für eine zielgerichtete Validierung von Sicherheitsfunktionen festgelegt ist – findet immer noch zu wenig Beachtung. Doch dieser Teil der Norm ist von mindestens ebenso großer Relevanz und Brisanz, schließlich wird erst mit der Validierung der Nachweis der Eignung – bezogen auf den realen Einsatzzweck – erbracht. Ergo nimmt die Validierung gemäß EN ISO 13849 Teil 2 im Gesamtprozess des CE-Konformitätsbewertungsverfahrens einen hohen Stellenwert ein.

Rechtlicher Rahmen

Die europäische Maschinenrichtlinie bildet den rechtlichen Rahmen für die EN ISO 13849. Seit 1995 ist jeder Hersteller von Maschinen dafür verantwortlich, dass



Bilder: K.A. Schmersal

die Anforderungen der europäischen Maschinenrichtlinie bezüglich Sicherheit und Gesundheitsschutz eingehalten werden. Unterstützt wird er hierbei durch Normen. Erfüllt ein Produkt die Anforderungen einer harmonisierten Norm, wird angenommen, dass das Produkt mit den grundlegenden Sicherheitsanforderungen aus Anhang 1 der Maschinenrichtlinie übereinstimmt. Die Rede ist in diesem Zusammenhang auch von der sogenannten ‚Vermutungswirkung' mit der damit einhergehenden Beweislastumkehr.

Die EN ISO 13849 Teil 2 legt das Validierungsverfahren für die in der Maschine enthaltenen Sicherheitsfunktionen fest. Gesprochen wird in diesem Zusammenhang auch von SRP/CS (Safety related parts of a control system). Die Validierung muss aufzeigen, dass die Gestaltung der SRP/CS die Sicherheitsanforderungen der EN ISO 13849-1 erfüllt, insbesondere im Hinblick auf die im Konstruktionsprozess festgelegten Eigenschaften der Sicherheitsfunktionen. Der ermittelte erforderliche Performance Level (PLr) steht hier besonders im Fokus. Damit Fehler oder Abweichungen von den Spezifikationen frühzeitig erkannt und korrigiert werden können, ist es ratsam, möglichst in einem frühen Stadium der Entwicklung beziehungsweise Konstruktion mit diesem Prozess zu beginnen.

Validierung und Verifikation

Die Validierung setzt sich aus verschiedenen Schritten zusammen, wobei grundsätzlich zwischen Verifikation und Validierung zu unterscheiden ist: Die Verifikation umfasst die Analysen und Prüfungen für SRP/CS beziehungsweise deren Teilaspekte. Dabei wird festgestellt, ob die erzielten Resultate einer Entwicklungsphase respektive eines Konstruktionsabschnittes den Vorgaben für diese Phase entsprechen, ob also zum Beispiel das Schaltungslayout dem Schaltungsentwurf entspricht. Bei der Verifikation steht die Frage im Vordergrund, ob der erreichte Performance Level (PL) dem erforderlichen Performance Level (PL r) mindestens entspricht (oder größer ist). Ist dies nicht der Fall, müssen konstruktive Anpassungen vorgenommen werden.

Demgegenüber bezeichnet Validierung den Nachweis der Eignung – bezogen auf den realen Einsatzzweck –, der während des Entwicklungsprozesses oder an seinem Ende erfolgt. Überprüft wird, ob die spezifizierten Sicherheitsanforderungen an den sicherheitsrelevanten Teilen der Maschinensteuerung erfüllt wurden.

Analyse und Prüfung

Verifikation und Validierung können ausschließlich durch eine Analyse oder alternativ durch eine Kombination aus Analyse und Prüfung erfolgen. Im Rahmen der Analyse werden beispielsweise Unterlagen gesichtet und, wo nötig, Analysewerkzeuge eingesetzt – beispielsweise Schaltungssimulatoren, Tools zur statischen und dynamischen Software-Analyse oder FMEA-Tools.

Ist die Analyse nicht ausreichend, um zu zeigen, dass die Anforderungen erfüllt werden, müssen Prüfungen die Validierung vervollständigen. Um das Ausfallverhalten der Sicherheitsfunktionen zu testen, werden hier unter anderem Fehler simuliert, deren Auftreten nicht zum Verlust der Sicherheitsfunktion führen darf.

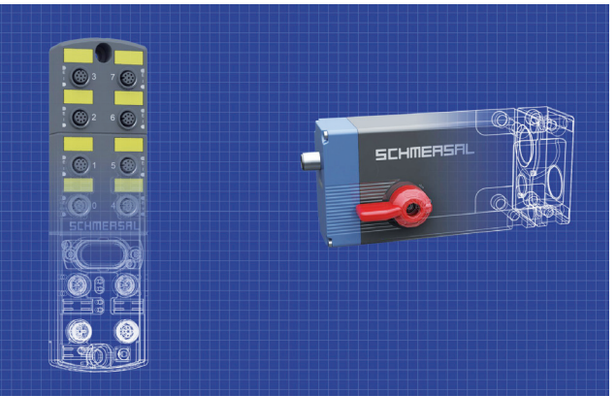
Generell gilt, dass das gesamte Validierungsverfahren von ‚anderen' oder ‚unabhängigen' Personen durchgeführt werden sollte, also von Personen, die nicht in Gestaltung und Konstruktion der SRP/CS einbezogen waren. Dies bedeutet allerdings nicht unbedingt, dass eine Prüfung durch Dritte erforderlich ist.

Das Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA) gibt hierzu Empfehlungen nach dem Grundsatz, dass der Grad der Unabhängigkeit dem Risiko – also dem erforderlichen Performance Level PL r – angemessen sein sollte. Bei PL a könnte dies beispielsweise eine ‚andere Person' sein (etwa der Vorgesetzte), bei PL e wäre dies nicht ausreichend, sondern ein höherer Unabhängigkeitsgrad nötig.

Prozessschritte der Validierung

Das Validierungsverfahren nach EN ISO 13849-2 schreibt die Erstellung eines Validierungsplans vor, der die Anforderungen und Ziele aller durchzuführenden Tätigkeiten beschreibt. Zudem werden in ihm die Mittel bestimmt, um die festgelegten Sicherheitsfunktionen, Kategorien und Performance Level zu validieren. Dazu zählen:

- Produktidentifikationen der zu prüfenden SRP/CS,
- Identifikation der Sicherheitsfunktionen mit Zuordnung der beteiligten SRP/CS,



Schon im Konstruktionsprozess ist es wichtig, die Funktionsfähigkeit und Tauglichkeit eines Produktes systematisch zu überprüfen.

- Dokumentenliste,
- Spezifikationen der Sicherheitsfunktionen,
- Betriebs- und Umgebungsbedingungen der Prüfung,
- die anzuwendenden Analysen und Prüfungen inklusive Kriterien I.O./N.I.O.,
- anzuwendende Fehlerlisten,
- Verweise auf anzuwendende Prüfnormen sowie
- Liste der verantwortlichen Personen oder Parteien.

Zur Vorbereitung des Validierungsverfahrens ist es unerlässlich, umfangreiche Dokumente zusammenzustellen – beispielsweise eine Beschreibung der Eigenschaften jeder einzelnen Sicherheitsfunktion, Zeichnungen und Festlegungen zur Sicherheitsfunktion, Prinzip- und Blockdiagramme, Schaltpläne, Fehlerlisten, die Begründung aller Fehlerausschlüsse sowie Benutzerinformationen.

Nach dem Erstellen des Validierungsplans und der Zusammenstellung der notwendigen Dokumente kann mit der Analyse begonnen werden. Hierzu gehört unter anderem die Überprüfung der einzelnen Kategorien sowie der Parameter Mean Time to Dangerous Failure (MTTFD), Diagnostic Coverage – beziehungsweise Diagnosedeckungsgrad (DCavg) sowie Common Cause Failure(CCF).

Kategorien klassifizieren die SRP/CS in Bezug auf ihre Widerstandsfähigkeit gegen Fehler und ihr Verhalten im Fehlerfall. Darüber hinaus sind sie der Ausgangspunkt für die Bestimmung der Ausfallwahrscheinlichkeit und des PL. Ziel der Kategorie-Validierung ist die Bestätigung aller gestellten Anforderungen an die durch die SRP/CS realisierte Kategorie.

Der zur Bestimmung des PL herangezogene MTTFD-Wert wird im Rahmen der Analyse auf seine Plausibilität überprüft, zum Beispiel durch den Vergleich von Produktdatenblättern mit den Werten aus der EN ISO 13849-1, Anhang C. Die DC-Maßnahmen zur Erkennung und Beherrschung von Fehlern und Ausfällen müssen nachvollziehbar begründet sein und die entsprechenden Angaben auf Plausibilität überprüft werden.

Für die Validierung der ausgewählten Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (CCF) beschreibt die EN ISO 13849-2 ein spezielles Verfahren, das auf einem Punktesystem basiert. Eine entsprechende Tabelle findet sich im Anhang F, Tabelle F.1. der Norm. Auch hier sollten die Angaben nachvollziehbar begründet werden.

Systematische Ausfälle vermeiden

Ein weiterer Verfahrensschritt ist die Validierung von Maßnahmen zur Vermeidung systematischer Ausfälle, etwa durch eine gründliche Inspektion der Entwicklungsdokumente sowie durch Fehleranalysen – Failure Mode and Effects Analysis (FMEA) oder kurz ‚Auswirkungsanalyse'. Dabei werden auch Tests durch das Simulieren von Fehlern durchgeführt. Außerdem muss die Leistungsfähigkeit und Störfestigkeit der SRP/CS gegenüber Umgebungseinflüssen validiert werden – durch Analyse und nötigenfalls durch Prüfung. Zu den erwartbaren widrigen Bedingungen gehören unter anderem mechanische Beanspruchungen wie Schwingungen oder Verschmutzungen, Temperaturschwankungen, Luftfeuchte oder elektromagnetische Beeinflussung.

Validierung der Software

Die Validierung der sicherheitsbezogenen Software erfolgt mittels des sogenanntes V-Modells: Hier wird zum einen geprüft, ob die Anforderungen der sicherheitsbezogenen Softwarespezifikation an das funktionale Verhalten sowie die Leistungskriterien (zum Beispiel zeitbezogene Vorgaben) korrekt umgesetzt wurden. Zum anderen werden Tests durchgeführt, um die Fehlererkennung und -beherrschung durch die Software zu erproben. Um zu bestätigen, dass die Software der Spezifikation der Sicherheitsanforderungen entspricht, wird auch hier ein entsprechender Bericht erstellt, der Bestandteil des Validierungsberichts der Maschine oder Anlage wird.

Zum Ende der Analyse wird die korrekte Abschätzung des PL überprüft sowie eine Validierung hinsichtlich der Frage durchgeführt, ob eine Kombination sicherheitsbezogener Teile den bei der Gestaltung festgelegten Performance Level erreicht.

Abschließend und nach der Durchführung aller Verifikations- und Validierungsschritte geht es an die Erstellung des Validierungsberichts. Dieser enthält in nachvollziehbarer Form alle Angaben zu den durchgeführten Analysen und Prüfungen der Hard- und Software der SRP/CS.

Externe Dienstleister

Eine frühzeitige Einbindung der Validierung in den Konstruktionsprozess hilft dabei, kostenträchtige Konstruktionsfehler zu verhindern und ist damit für den Hersteller auch unter dem Aspekt der Wirtschaftlichkeit interessant. Zudem stellt eine sorgfältig durchgeführte und entsprechend dokumentierte Validierung eine nicht zu unterschätzende Entlastung bei der Umsetzung behördlich angeordneter Maßnahmen oder auch bei Gerichtsverfahren dar. Auch noch nach vielen Jahren kann eine nachvollziehbare Dokumentation ein entlastender Faktor für den Hersteller von Maschinen und Anlagen sein.

Dabei muss die Validierung nicht zwangsläufig durch Dritte durchgeführt werden, es kann aber durchaus hilfreich sein, externe Dienstleister hinzuzuziehen. So bietet beispielsweise das tec.nicum – die Dienstleistungssparte der Schmersal-Gruppe – sowohl Einzelleistungen an, die im Rahmen des Validierungsprozesses erforderlich sind, als auch eine Begleitung durch den gesamten Prozess. Bei Bedarf überprüfen die Experten unter anderem zielgerichtet Schaltpläne des elektrischen, pneumatischen und hydraulischen Systems, berechnen die Performance Level und erstellen alle Dokumente für eine lückenlose Dokumentation. *ik*

TOBIAS KELLER
ist Safety Consultant beim tec.nicum, dem Geschäftsbereich Dienstleistungen der Schmersal-Gruppe in Wuppertal.