Schritt für Schritt zur sicheren Maschine mit Sensor-Technik Wiedemann. Foto: STW

SCHRITT FÜR SCHRITT

SPEZIAL ANTRIEBS- UND STEUERUNGSTECHNIK

von Philipp Luger: Maschinensicherheit nach EN ISO 13849 zu gewährleisten ist eine komplexe Aufgabe. Die Herausforderung besteht darin, das richtige Maß an Aufwand zu finden, um die Anforderungen der Sicherheitsnorm umzusetzen. Allerdings gibt die EN ISO 13849 für die Planung und Überwachung der funktionalen Sicherheit im Gegensatz zur Grundnorm IEC 61508 kaum eine Hilfestellung. Ein Sicherheitsmanagementprozess kann dabei helfen, die Normkonformität effizient zu erreichen.

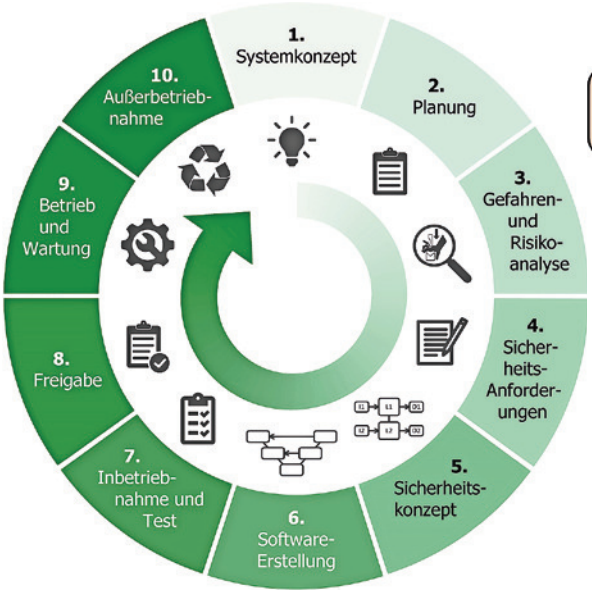
Um die funktionale Sicherheit bei der Umsetzung der Sicherheitsnormen zu gewährleisten, muss der Hersteller einer Maschine den gesamten Produktlebenszyklus betrachten. Im Bereich der Maschinensicherheit bedeutet dies, dass ab Erstellen des Konzeptes für die Maschine bis zur dauerhaften Außerbetriebnahme und Entsorgung der Maschine die funktionale Sicherheit berücksichtigt werden muss.

Produktlebenszyklus einer Maschine

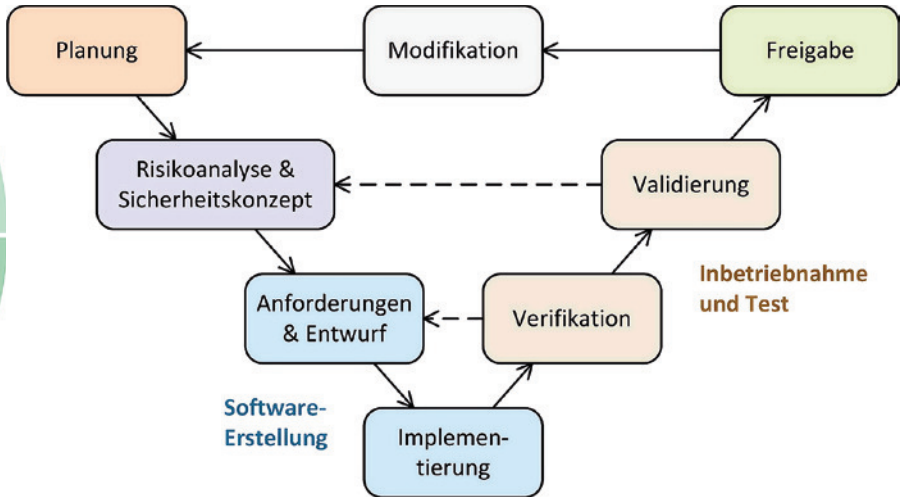
Je nach Lebenszyklusphase ist der Aufwand für die funktionale Sicherheit unterschiedlich hoch. Der größte Aufwand entsteht nach der Planung, wenn die Gefahren und Risiken ermittelt und die Sicherheitsanforderungen zu deren Reduzierung abgeleitet wurden. Im Sicherheitskonzept und der Software-Erstellung müssen diese Anforderungen, die den Sicherheitslevel und somit den Grad der Zuverlässigkeit festlegen, durch fehlervermeidende und fehlerbeherrschende Maßnahmen umgesetzt werden. Zudem werden weiterführende Anforderungen spezifiziert, die bei der Inbetriebnahme, im Betrieb, bei der Wartung und bei der Außerbetriebnahme beachtet werden müssen.
Der Sicherheitslebenszyklus umfasst dabei bestimmte Tätigkeiten im gesamten Produktlebenszyklus. Das Sicherheitsmanagement ist nur im Entwicklungslebenszyklus, sprich von der Planung bis zur Freigabe, aktiv tätig. Dies schließt Modifikationen an der Maschine mit ein.

Projektphasen im Entwicklungslebenszyklus

Unterstützt wird das Sicherheitsmanagement durch das Projekt-, Anforderungs-, Test-, Qualitäts-, Konfigurations- und Änderungsmanagement. Diese Prozesse stellen eine Basis dar, auf die das Sicherheitsmanagement zurückgreift. Im Folgenden werden für jeden Schritt im Produktlebenszyklus die wichtigsten Tätigkeiten mit Bezug auf die funktionale Sicherheit beschrieben.
1. Systemkonzept: Anhand eines Systemlastenheftes soll den Konstrukteuren ein Gesamtüberblick gegeben werden, damit diese die Maschine für ihre bestimmungsgemäße Verwendung entwickeln können. Das Systemkonzept definiert den Produkteinsatz, d.h. die Anwendungsfälle und die Grenzen der Maschine, eine grobe Architektur, die relevanten Richtlinien und Normen, die Umweltanforderungen sowie den Lieferumfang. Diese Informationen werden auch für die Gefahren und Risikoanalyse benötigt.
2. Planung: Die Planung der funktionalen Sicherheit beginnt bereits sehr früh. Das liegt daran, dass für die Tätigkeiten im Sicherheitslebenszyklus ausreichend qualifizierte Mitarbeiter ausgewählt werden müssen. Um deren Tätigkeit überwachen zu können, werden Projektphasen zu Sicherheitsmeilensteinen zusammengefasst, zu denen jeweils ein Audit durch den Sicherheitsverantwortlichen stattfindet. Die Sicherheitsplanung legt zudem fest, welche Dokumente erzeugt, welche Software-Werkzeuge verwendet und welche Kommunikationswege eingehalten werden müssen. Im Verifikations- und Validierungsplan werden die durchzuführenden Tests definiert. Hierzu zählen die Modul-, Integrations- und Systemtests sowie die Reviews. Der Projektmanagementplan legt den Projektumfang fest, besetzt die Projektrollen und definiert die Rahmenbedin-



Produktlebenszyklus Grafik: STW



Projektphasen im Entwicklungslebenszyklus Grafik: STW

gungen, wie zum Beispiel Eskalationsstufen. Die Planungsphase kann erst abgeschlossen werden, wenn die Sicherheitsfunktionen identifiziert wurden, da deren Anforderungen Einfluss auf die Sicherheitsplanung haben, wie zum Beispiel die Festlegung von Methoden zur Ermittlung der geforderten Sicherheitskennzahlen.

3. Gefahren- und Risikoanalyse: Auf Basis des Systemlastenheftes und eines ersten Entwurfes der Maschine werden die Gefährdungen identifiziert und das Risiko eingeschätzt. Dies geschieht typischerweise auf Basis der EN ISO 12100. Wenn eine Steuerung als Schutzmaßnahme eingesetzt werden soll, wird der Grad der benötigten Risikoreduzierung anhand des Risikographen der EN ISO 13849-1 ermittelt.

4. Sicherheitsanforderungen: Die in der Risikoanalyse ermittelten Sicherheitsfunktionen auf Basis eines Steuerungssystems werden in den Sicherheitsanforderungen spezifiziert. Zu jeder Sicherheitsfunktion muss der geforderte Performance Level sowie die Prozesssicherheitszeit (maximal zulässige Zeit, um nach einem gefährlichen Ausfall den sicheren Zustand zu erreichen) festgelegt werden. Die Spezifikation der Sicherheitsanforderungen kann Bestandteil der Dokumentation des Sicherheitskonzeptes sein.

5. Sicherheitskonzept: Für jede Sicherheitsfunktion muss ein Konzept zur technischen Umsetzung erstellt werden. Hierzu wird eine Sicherheitsarchitektur ausgewählt, die einer der durch die EN ISO 13849 vorgegebenen Kategorien B, 1, 2, 3 oder 4 entsprechen muss. Je nach gefordertem Performance Level muss dann ein bestimmter mittlerer Diagnosedeckungsgrad (DCavg) sowie eine mittlere Zeit bis zum gefahrbringenden Ausfall (MTTFD) erreicht werden und ggf. Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (CCF) ergriffen werden. Je nach Komplexität der Funktion

Philipp Luger Foto: STW

macht es Sinn, diese in mehrere Sub-Systeme zu unterteilen, für die jeweils eine geeignete Sicherheitsarchitektur gewählt wird, die dann wieder sinnvoll kombiniert werden können. Die benötigten Werte für die Berechnung der Kennzahlen kommen entweder vom Hersteller einer Komponente oder können einer Normentabelle entnommen werden. Als weiteres Ergebnis des Sicherheitskonzeptes werden zum einen Anforderungen an die Hardware und vor allem an die Software bezüglich benötigter Diagnosemaßnahmen spezifiziert, zum anderen die Verfahren zum Ausgeben einer Warnung beziehungsweise zum Erreichen des sicheren Zustandes festgelegt.

6. Software-Erstellung: Die im Rahmen des Sicherheitskonzeptes spezifizierten Software-Anforderungen werden abgeleitet und verfeinert. Auf Basis dieser detaillierten Anforderungen wird ein Software-Entwurf erstellt, in dem das Software-System in Komponenten und Module zerlegt wird. Der Software-Entwurf liefert verschiedene Sichten auf die Software bezüglich Struktur, Informationsfluss und zeitlichem Ablauf. Für diesen Zweck wird eine einheitliche Modellierungssprache (UML) verwendet, mit der beispielsweise Zustands- oder Sequenzdiagramme erstellt werden. Hieraus lässt sich eine Beschreibung der benötigten Softwaremodule ableiten. Diese Modulspezifikation definiert die Schnittstellen und die Funktionalität der Software-Module. Unter Verwendung einer geeigneten Programmiersprache und entsprechenden Programmier-Richtlinien wird dann die eigentliche Software implementiert.

7. Inbetriebnahme und Test: Die Inbetriebnahme erfolgt in mehreren Schritten entlang der einzelnen Teststufen. Der Modultest entspricht einem Test der kleinsten, sinnvoll vom Rest der Applikation isoliert testbaren Einheiten. Es wird zwischen statischem und dynamischem Modultests unterschieden. Die einzeln getesteten Module werden im Software/Software-Integrationstest zu einer oder mehreren Komponente zusammengeführt, um das korrek-

te Zusammenspiel zu verifizieren. Im Hardware/Software-Integrationstest wird das komplette Software-System auf die Hardware integriert und validiert. Mit Hilfe von Fehlerinjektionstests wird geprüft, ob die gefährlichen Ausfälle erkannt werden und der sichere Zustand eingenommen wird und ob der geforderte Diagnosedeckungsgrad praktisch erreicht wird. Zuletzt wird durch die EMV-, Umwelt- und Abnahmetests nachgewiesen, dass die Maschine für den bestimmungsgemäßen Gebrauch geeignet ist und auch alle gesetzlichen Anforderungen erfüllt.

8. Freigabe: Nach Abschluss der Entwicklungs- und Testtätigkeiten erfolgt die Sicherheitsbeurteilung auf Basis des Sicherheitsnachweises. Dieser entspricht der Summe aller Dokumente, die gemäß Sicherheitsplan für die Beurteilung der funktionalen Sicherheit benötigt werden, und dient auch als Konformitätsnachweis zur Maschinenrichtlinie. Die Sicherheitsbeurteilung muss durch eine ausreichend unabhängige Stelle erfolgen und führt bei erfolgreicher Prüfung zur Sicherheitsfreigabe, zum Beispiel in Form einer EG-Konformitätserklärung.

9. Betrieb und Wartung: Die für den Betrieb und die Wartung relevanten Informationen zur Gewährleistung der funktionalen Sicherheit der Maschine müssen dem Benutzer bzw. Instandhalter in geeigneter Form zur Verfügung gestellt werden. In der Regel geschieht dies durch die Betriebsanleitung, die alle risikomindernden Maßnahmen beinhalten muss, die nicht konstruktiv oder durch Schutzeinrichtungen abgedeckt werden konnten.

10. Außerbetriebnahme: in einigen Fällen kann es notwendig sein, für die Außerbetriebnahme gesonderte Sicherheitsanforderungen zu spezifizieren, wenn die Risikoanalyse dies ergeben hat. Typischerweise werden diese auch durch Benutzerinformation in der Betriebsanleitung umgesetzt. Wurde die Maschine erfolgreich stillgelegt, ist ihr Lebenszyklus zu Ende und die funktionale Sicherheit muss nicht weiter berücksichtigt werden.

Lifecycle Support

Wie man sieht, kann der Weg zur sicheren Maschine durch eine strukturierte Arbeitsweise erleichtert werden. STW hat ein Schulungsprogramm zusammengestellt, mit dem das Know-how vermittelt wird, um das Sicherheitsmanagement in die eigenen Unternehmensprozesse zu integrieren und die Anforderungen der funktionalen Sicherheit in der Produktentwicklung zielorientiert umzusetzen. Unterstützt wird das Ganze durch Dokumentenvorlagen und Review-Protokollvorlagen, in denen die Norminhalte strukturiert aufbereitet wurden. Die Schulung orientiert sich am Produktlebenszyklus einer Maschine. STW hat ein Poster entworfen, das diesen übersichtlich darstellt und einen Überblick über die wichtigsten Inhalte gibt. Das Poster kann auf der Firmenhomepage kostenlos heruntergeladen werden. ■

www.stw-mm.com