BGIA
Institut für Arbeitsschutz der
Deutschen Gesetzlichen Unfallversicherung

Praxisgerechte Validierung von Sicherheitsapplikationen

Dr. Michael Huelke, FB Unfallverhütung – Produktsicherheit, BGIA – Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung, Sankt Augustin

Die Norm EN 954-1 „Sicherheitsbezogene Teile von Steuerungen“ wurde an moderne Technologien angepasst. In deren neuen Fassung EN ISO 13849-1:2006 sind erstmals Anforderungen an die Software in diesen Steuerungen formuliert worden. Sowohl die EN 62061 als auch die EN ISO 13849-1 sind harmonisiert und beschreiben Anforderungen speziell für Applikations-Software in Maschinen. Obwohl die EN 954-1 in der Übergangsfrist bis November 2009 angewendet werden kann, beschreibt diese Norm aber bezüglich Software nicht den Stand der Technik. Die Softwareanforderungen in 62061 und 13849-1 sind damit faktisch heute schon zu berücksichtigen.

Dieser Beitrag behandelt speziell die Phase „Validierung“ im Entwicklungsprozess für Applikations-Software. Diese Validierung wird sowohl in der 62061 als auch in einem frühen Entwurf der derzeit überarbeiteten EN ISO 13849 Teil 2 beschrieben. Abbildung 1 zeigt, wie der Entwicklungsprozess für sicherheitsbezogene Applikations-Software prinzipiell abläuft.

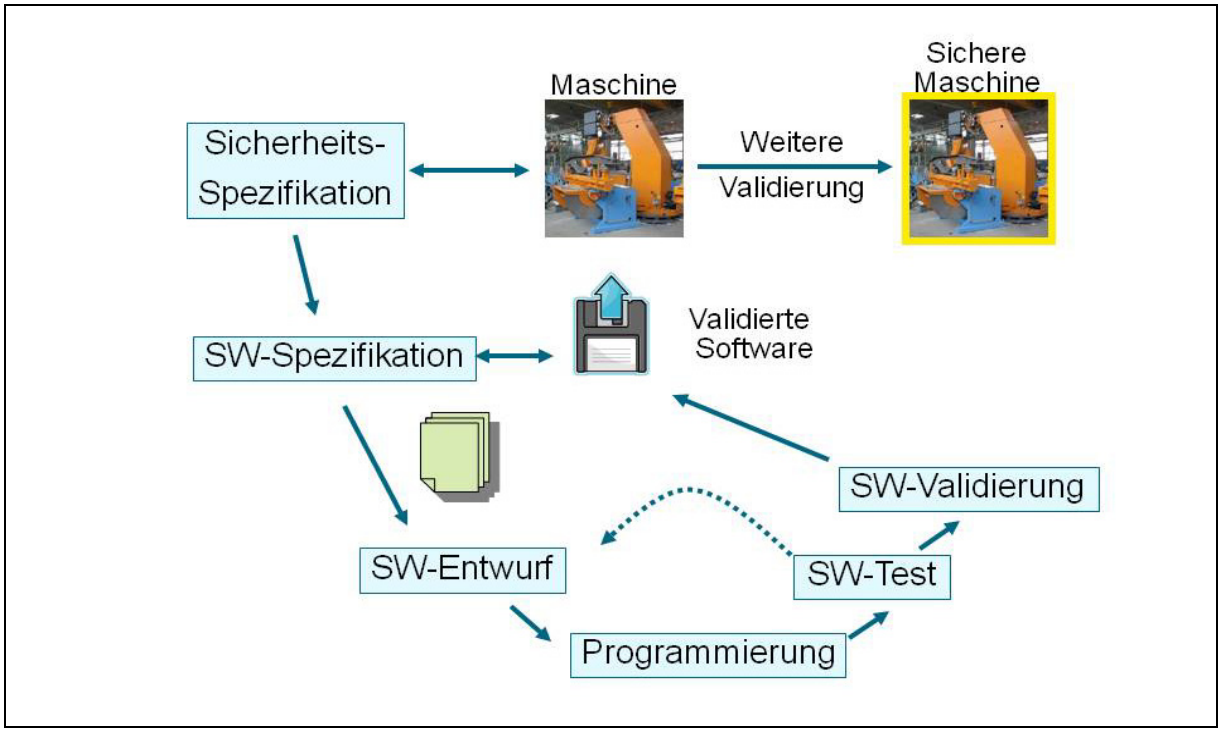

Abbildung 1: Entwicklungsprozess für sicherheitsbezogene Applikations-Software

Für das gesamte Sicherheitskonzept einer Maschine bzw. Maschinenanlage existiert zunächst eine Spezifikation mit den Sicherheitsanforderungen. Dort sind auch die technischen Schutzmaßnahmen beschrieben, deren Funktion z.B. von programmierbaren Steuerungen abhängt. Von diesen Anforderungen ausgehend wird die Software-Spezifikation erstellt, die als Lastenheft für die Applikations-Software dient. Sie beschreibt, welcher Beitrag zur Sicherheitsfunktion von der Applikations-Software zu leisten ist sowie welche Maßnahmen zur Fehlervermeidung bei der Entwicklung getroffen werden sollen. Die Programme werden unter Verwendung von bereits validierten bzw. zertifizierten Softwarebausteinen entworfen und die Aufbau- bzw. Ablaufstruktur des Programms im SW-Entwurf festgelegt. Neue, bisher noch nicht entwickelte Softwareteile sind ebenfalls zu spezifizieren. Unter Beachtung der vorher festgelegten Programmierrichtlinien werden die neu programmierten Softwarebausteine mit den vorhandenen Bausteinen logisch verknüpft und parametriert. Die Ein- und Ausgangssignale der Steuerung werden konfiguriert. Mit dem oben genannten Softwareentwurf als Maßstab werden die einzelnen Bausteine bzw. das Gesamtprogramm dem Softwaretest unterworfen. Dazu gehört auch der Integrationstest der Software mit der später an der Maschine verwendeten Steuerungshardware.

Bis hierhin ist dies ein typischer Softwareentwicklungsprozess. Zur Erhöhung der Qualität der Software im Sinne der Maschinensicherheit wird zusätzlich und entwicklungsbegleitend die Software-Validierung durchgeführt. Dazu werden die Applikations-Software und deren Entwicklungsablauf analysiert sowie auf der Steuerung geprüft, um nachzuweisen, dass alle Anforderungen der anfangs erstellten Softwarespezifikation erfüllt wurden. Details zu dieser Validierung werden in den folgenden Abschnitten vorgestellt.

Die Software-Validierung führt zu einer Bestätigung in Form eines Berichtes oder Protokolls, dass die betrachtete Applikations-Software der Spezifikation der Sicherheitsanforderungen entspricht. Für diese Untersuchung müssen vorrangig die Spezifikation und die Software vorhanden sein. Die Software muss auf der Steuerung ausgeführt werden können, um die Sicherheitsfunktionen der Maschine testen zu können. Zur Analyse des Entwicklungsprozesses und der Umsetzung der fehlervermeidenen Maßnahmen sind weitere Dokumente oder Nachweise zu betrachten: die Entwurfsunterlagen wie z.B. der SW-Entwurf, Protokolle zu durchgeführten Reviews oder Walkthroughs, Testberichte, Programmierrichtlinien usw. - selbstverständlich auch ein gut dokumentiertes Softwarelisting.

Wer validiert nun welche Steuerungsteile? Bei einem programmierten Steuerungssystem sind zunächst die Komponentenhersteller in der Verantwortung, die Hardware sowie deren Firmware zu validieren. Diese Hersteller können natürlich nicht wissen und vorab prüfen, in welcher Kombination bzw. Verschaltung von Komponenten welche Sicherheitsfunktionen mit einer maschinenspezifischen Applikations-Software realisiert werden. Für diese Software ist also der Maschinen- und Anlagenbauer zuständig.

Die Abbildung 2 stellt den Ablauf der Software-Validierung prinzipiell dar.

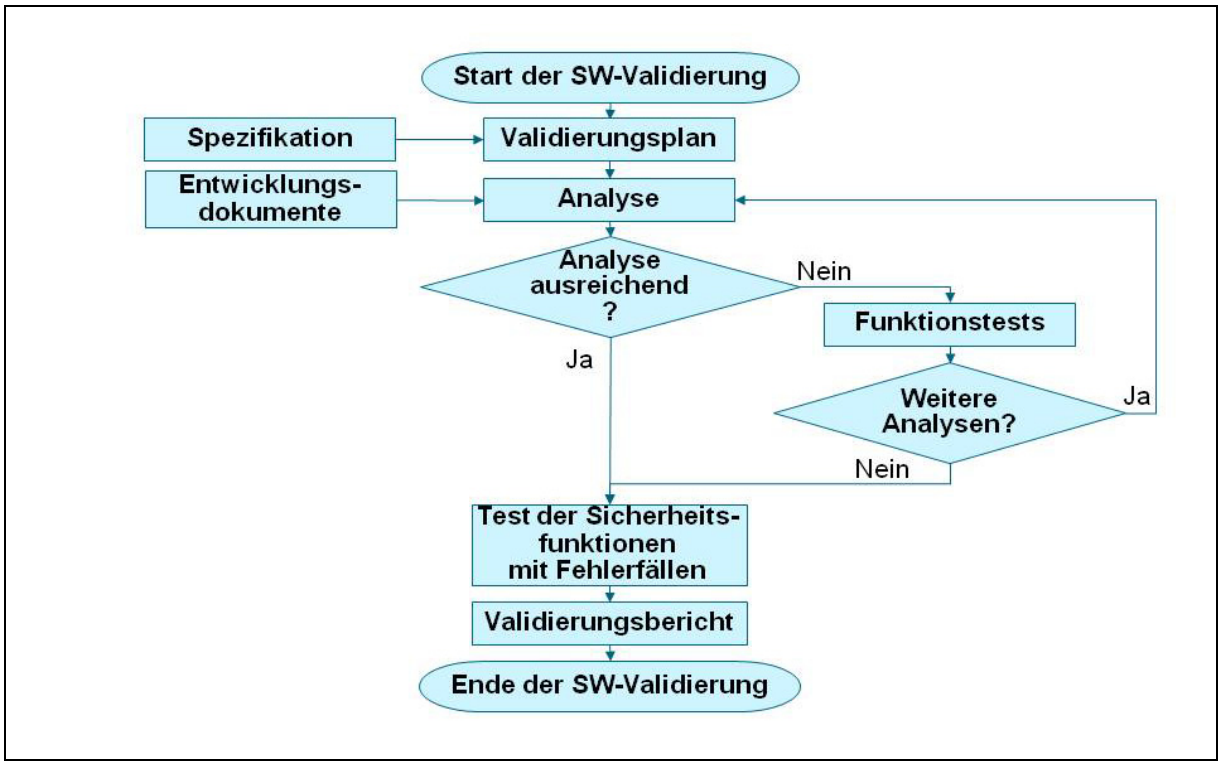

Abbildung 2: Ablauf der Software-Validierung

Der Aufwand und das Vorgehen hängen von dem zu erreichenden Sicherheitslevel (Performance Level PL oder Safety Integrity Level SIL) ab. Eventuell kann die Analyse von Entwicklungsdokumenten ausreichen, um dann mit einem praktischen Test der Sicherheitsfunktionen die Übereinstimmung von Applikations-Software und deren Spezifikation nachzuweisen. Bei komplexeren Steuerungen müssen zusätzliche Funktionstests mit seltenen oder nicht definierten Signalen bzw. provozierten Fehlern erfolgen. Ein praktischer Test der Sicherheitsfunktionen mit Fehlerfällen ist in jedem Fall erforderlich.

Die Validierung soll nicht der Projekteur bzw. Programmierer selber durchführen. Auch hier gilt das Vier-Augen-Prinzip. Diese Aufgabe können andere Personen, andere Abteilungen oder andere Stellen übernehmen, die der Konstruktionsabteilung hierarchisch nicht unterstehen. Der Grad der Unabhängigkeit sollte dabei dem Risiko, also dem erforderlichen PL oder SIL angemessen sein. Alle Analyse- und Prüfaktivitäten müssen vorher geplant werden – am besten schon im Rahmen der Spezifikation – und inklusive ihrer Ergebnisse dokumentiert werden.

Die zugelieferten Hardwarekomponenten und auch die Softwarebibliotheken für die Applikationsprogrammierung sind meist bereits zertifiziert und damit validiert worden. Diese einzelnen Teile sind nicht vom Verwender erneut zu validieren, wohl aber deren Kombinationen. Zur vollständigen Prüfung der Sicherheitsfunktionen an der kompletten Maschine gehört eine Reihe weiterer Aspekte wie z.B. die Bemessung von Nachläufen und Sicherheitsabständen.

Für die Validierung sind Dokumente erforderlich, die im Rahmen der Entwicklung entstanden sind:

- Spezifikation aller Anforderungen an die Sicherheitsfunktionen (Abbildung 1)
- vollständige Softwaredokumentation
- Identifikation der Werkzeuge und ihrer Konfiguration
- Übersicht über die benutzten zertifizierten (oder selber validierten) Softwarebausteine einschließlich ihrer Identifikation (Versionsnummer, Autor, Datum usw.)
- eingehaltene Qualitätssicherungsregeln für den Entwurf und die Realisierung wie z.B. Programmierrichtlinien
- Nachweise zu den durchführten Modul- und Integrationstests sowie statischen und dynamischen Codeanalysen
- Dokumentation der durchgeführten fehlervermeidenden Maßnahmen, Methoden und Tools

Da die Validierung durch unbeteiligte bzw. unabhängige Personen durchzuführen ist: Die Dokumente müssen vollständig, die Inhalte widerspruchsfrei, logisch aufgebaut, leicht verständlich und nachvollziehbar sein.

Zusammenfassung
Die neuen Normen zur funktionalen Sicherheit für den Maschinensektor, EN ISO 13849-1 und EN 62061, stellen erstmals sektorspezifische Anforderungen an Applikations-Software. Die Normen dokumentieren damit den Stand der Technik, während die bisherige EN 954-1 gar keine Softwareanforderungen beinhaltet. Trotz der Übergangsfrist bis November 2009 ist daher die 954-1 in diesem Aspekt faktisch abgelöst.

Die Validierung der Sicherheitsfunktionen und insbesondere der sicherheitsbezogenen Applikations-Software ist in allen relevanten Normen gefordert. Die Vorbereitung und Durchführung von Validierungsschritten ist kein technisches Problem, sondern eine Frage der richtigen und verantwortungsvollen Organisation. Validierung ist ein Schritt auf die sichere Seite (Produkthaftung). Voraussetzung für eine Validierung ist eine gute Sicherheits-Spezifikation, denn sie ist der Maßstab, an dem die realisierten Sicherheitsfunktionen mit der zugehörigen Applikations-Software überprüft werden.

Zur Entwicklung von qualitativ hochwertiger Applikations-Software werden gute, zertifizierte Tools angeboten. Diese Tools leisten heutzutage einen wesentlichen Beitrag zur Vermeidung von Fehlern während der Codierung, zur Einhaltung von Programmierstandards und –richtlinien sowie zum Test und zur Validierung. Die in Bibliotheken mitgelieferten zertifizierten Softwarebausteine sind bereits validiert und decken die meisten Sicherheitsfunktionen ab. Je mehr dieser Bausteine eingesetzt werden können, desto weniger die Wahrscheinlichkeit individueller Softwarefehler und desto geringer der Validierungsaufwand. Zukünftig könnten diese Tools den Applikationsprogrammierer auch bei der Spezifizierung und der Validierung unterstützen – die Vorarbeiten an entsprechenden Standards hat bereits begonnen (VDI/GMA Fachausschuss 1.50 „Methoden der Steuerungstechnik“).

Weitere Informationen zu den Normen finden sich auf den Internetseiten des BGIA:

- über die Portalseite zur Funktionalen Sicherheit **http://www.dguv.de/bgia/13849** und
- im kostenlosen **BGIA-Report 2/2008** „Funktionale Sicherheit von Maschinensteuerung“.