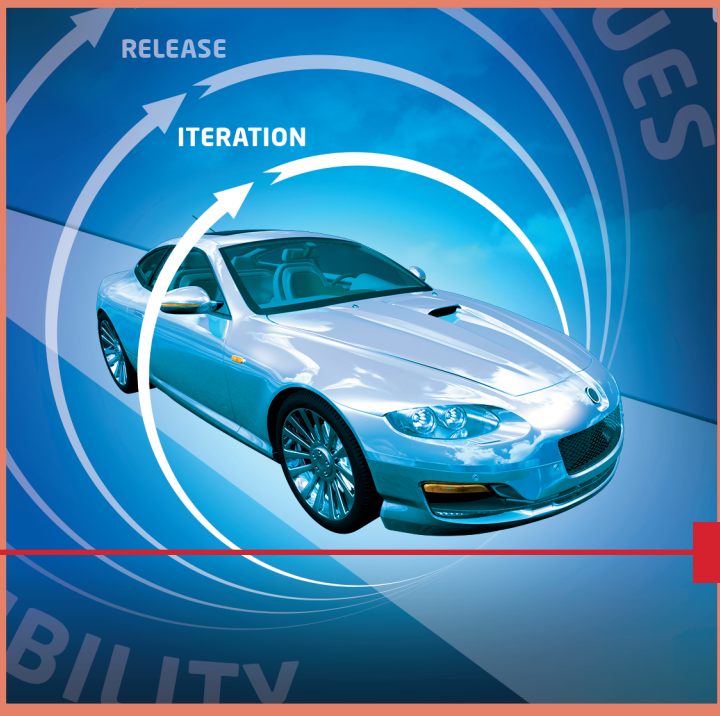
Hans-Leo Ross

Funktionale Sicherheit im Automobil

ISO 26262, Systemengineering auf Basis eines Sicherheitslebenszyklus und bewährten Managementsystemen



HANSER

Hans-Leo Ross

Funktionale Sicherheit im Automobil

Hans-Leo Ross

Funktionale Sicherheit im Automobil

ISO 26262, Systemengineering auf Basis eines Sicherheitslebenszyklus und bewährten Managementsystemen

HANSER

MIX
Papier aus verantwortungsvollen Quellen
FSC® C013736
FSC www.fsc.org

Bibliografische Information der Deutschen Nationalbibliothek:
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.ddb.de> abrufbar.

ISBN 978-3-446-43632-9
E-Book ISBN 978-3-446-43840-8

www.hanser-fachbuch.de
Lektorat: Dipl.-Ing.Volker Herzberg
Seitenlayout und Herstellung: Der Buch*macher*, Arthur Lenner, München
Coverconcept: Marc Müller-Bremer, Rebranding, München, Germany
Titelillustration: Frank Wohlgemuth, Hamburg
Coverrealisierung: Stephan Rönigk
Druck und Bindung: Kösel, Krugzell
Printed in Germany

Vorwort vom Autor

Das vorliegende Buch ist ein Auszug aus mehr als 20 Jahren Berufserfahrung mit dem Thema Funktionssicherheit. Als ich mich 1992 als Diplom-Ingenieur ins Berufsleben stürzte, war der Anlagenbau von verschiedenen Katastrophen wie Bhopal und Seveso geprägt. Das erste Regelwerk, das sich mit dem Thema Sicherheit beschäftigte, war die VDI/VDE-Richtlinie 2180 „Sicherung von Anlagen der Verfahrenstechnik“ aus dem Jahr 1966, in der es nur um die reine Anlagensicherung ging. Im Jahr 1984 wurde die Richtlinie erweitert; man machte nun einen Unterschied zwischen Betriebs- und Sicherungseinrichtungen sowie Überwachungs- und Schutzeinrichtungen. Danach erschien auch die DIN VDE 31000 „Allgemeine Leitsätze für das sicherheitsgerichtete Gestalten technischer Erzeugnisse“. Hier wurden die Zusammenhänge zwischen Risiko, Sicherheit und Gefahr beschrieben und das Grenzrisiko wurde eingeführt. Zu dieser Zeit waren noch Maschinenstandards gültig, die die Nutzung von Mikrocontrollern für Sicherheitsaufgaben verboten. Es gab jedoch bereits einen akzeptierten Markt für Sicherheitssteuerungen. Verschiedene Normen und Standards definierten die Grundlage für die Prüfung, Zertifizierung und Auslegung dieser Sicherheitssteuerungen. Sie wurden in Anforderungsklassen (AK 1-8) gemäß der DIN V 19250 klassifiziert. Diese Norm war anwendungs- und technologieunabhängig und beschrieb anhand eines Risikographen ein qualitatives Verfahren zur Risikoabschätzung. 1990 erschien die DIN V VDE 0801 „Grundsätze für Rechner in Systemen mit Sicherheitsaufgaben“. In der Revision von 1994 wurden Begriffe wie „betriebsbewährt“ und der Einsatz einer „Betrachtungseinheit“ eingeführt. Als Antwort auf die unterschiedlichen Risiko- oder Anforderungsklassen kannte man aber weitgehend nur Redundanz. In der Mess- und Regelungstechnik wurden jedoch auch schon diversitäre Messprinzipien genutzt, um Gefahrenszenarien frühzeitig zu entdecken. Die technischen Regeln für Dampf oder Richtlinien für Druckbehälter schrieben schon die redundante Messung von Druck und Temperatur aus Sicherheitsgründen vor. Selbst das Wasserhaushaltsgesetz kannte die Begrenzung der Füllmenge von Behältern durch Vorschrift oder Regelung sowie die unabhängige Überfüllsicherung als Sicherheitsmaßnahme. Viele dieser Sicherheitsprinzipien waren in den Sicherheitsstandards der Anlagenbetreiber entstanden und dienten sogar als

Grundlage für behördliche Genehmigungen. Als ich 1998 mit dem Vertrieb von Sicherheitssteuerungen begann, wurden besonders in England, den Niederlanden und Norwegen die Entwürfe der IEC 61508 diskutiert. Man kannte die skalierbare Redundanz und es wurde zwischen Redundanz für Sicherheit und Verfügbarkeit unterschieden. Mikrocontroller wurden auch im Lockstep-Prinzip gekoppelt und konnten im laufenden Betrieb der Anlage den Programmablauf oder die Steuerungslogik ändern. Es waren Programmierprogramme verfügbar, die Sicherheitslogik zwischen einer definierten Laufzeitumgebung konfigurieren konnten.

Mit der Veröffentlichung der IEC 61508 wurde ein Lebenszyklusansatz für Sicherheitssysteme vorgestellt. Weiter wurde die Prozessbetrachtung der Produktentwicklung und der Bezug zu den Qualitätsmanagementsystemen formuliert. Während meines Masterstudiums am Wirtschaftswissenschaftlichen Institut der Universität Basel durfte ich auch die Vorlesung von Professor Dr. Walter Masing genießen, der die Qualitätsmanagementsysteme in Deutschland sehr geprägt hat. Die Einführung der Diagnose zur Sicherung der Funktion bzw. der elektrischen Trägersysteme der Funktion erweiterte den Gedanken der Sicherheitsarchitektur. 1998 durfte ich in Birmingham das erste passive elektronische System vorstellen, welches bis SIL 4 gemäß IEC 61508 zertifiziert war. Nach der Vorgängerveranstaltung der safetronic im Jahre 1999, die in den Räumlichkeiten des TÜV-Süd stattfand, war ich bei der Unterschrift des ersten Zertifikats für ein einkanaliges vollständig gemäß IEC 61508 entwickeltes Steuerungssystem dabei. Auf einer VDMA-Veranstaltung berichtete ich über die Erfahrung mit der IEC 61508 im Anlagenbau und deren Einfluss auf die Entwicklung von sicherheitsgerichteten Steuerungssystemen. Die Maschinenbauindustrie war damals noch sehr stark von Relaistechnik geprägt. Dass die software-basierende Sicherheitstechnik diese Branche so schnell mit neuen Lösungen und Systemen verändern würde, wollte damals kaum jemand glauben. Als ich 2001 die Leitung des Produktmanagements übernahm, galt es neue Anwendungen für neue Sicherheitssysteme zu finden. Ein weiterer Themenschwerpunkt wurde die vernetzte Sicherheitstechnik, die bis dahin auf seriellen Datenbussen beruhte. Jetzt mussten verteilte und dezentrale Sicherheit sowie dynamische, situations- oder zustandsabhängige Sicherheitssysteme realisiert werden. Als Lösung kam nur noch Ethernet in Frage. Wichtig war hier, die vorhandene Datentechnik für die Sicherheitstechnik handhabbar zu machen. Im Rahmen von Diplomarbeiten wurden Sicherheitssteuerungen in ganz Norwegen verteilt, die auf dem Datennetz der norwegischen Mineralölgesellschaft „Statoil“ sicherheitsrelevante Daten austauschten. Die Erfahrungen mit Datenübertragung über Satelliten zwischen Ölplattformen und Landanlagen oder zwischen Norwegen und Deutschland und verschiedenen Lösungen zur Pipelineüberwachung über Funksysteme zeigte, dass sicherheitstechnische Datensysteme auch auf Basis von Ethernet realisierbar sind.

Durch die Veröffentlichung der IEC 61508 als DIN EN 61508 (VDE 0803) „Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme“ im Jahre 2001 wurde die deutsche Automobilindustrie auf das Thema aufmerksam. Öffentlicher Schriftverkehr zwischen dem VDA und den VDTÜVs führte zur Gründung des AK16 im FAKRA (Facharbeitskreis Automobil). Durch meinen Wechsel zu Continental Teves wurde ich 2004 Mitglied in diesem Arbeitskreis. Noch im selben Jahr wurden die ersten Strukturen für die spätere ISO 26262 entworfen und man nahm Kontakt zu weiteren Automobilnormungsgremien in anderen Ländern auf. Insbesondere mit Frankreich wurden konkrete Rahmenbedingungen für die Norm ausgearbeitet. Die erste Sitzung der ISO/TC22/SC03/WG16 fand vom 31.10. bis 02.11.2005 in Berlin statt. Die Arbeitsgruppen aus Frankreich und Deutschland bildeten die größten Fraktionen neben anderen Ländervertretungen aus Japan, USA, Schweden, Großbritannien u.s.w.. Bis zu diesem Zeitpunkt kursierte die ISO 26262 unter dem Namen „FAKRA-Norm“. Die safetronic 2005 adressierte bereits die ersten Ideen der zukünftigen Automobilnorm und es wurden Vorträge zu „Best Practices“ und Methoden präsentiert. Die safetronic begleitete die Entwicklung der ISO 26262 bis zum heutigen Tag. Im November 2011 wurde die ISO 26262 als „Internationaler Standard“ veröffentlicht. Das Buch ist der Versuch all die Hintergrundinformationen, die in den ganzen Jahren gesammelt und hart erfahren wurden, zusammenzutragen. Weiter will das Buch die Idee der Sicherheitsarchitektur als Grundlage für die Entwicklung von sicherheitsrelevanten Produkten näherbringen.

Dankwort des Autors

Die vielen Diskussionen mit den Experten der internationalen Normierung, den Kollegen, in den Arbeitskreisen, mit Hochschulen, bei Vorträgen sowie die Erkenntnisse aus Diplomarbeiten und Förderprojekten haben zu diesem Buch beigetragen. All den beteiligten Menschen möchte ich danken für die Leidenschaft, mit der sie das Thema Funktionssicherheit mit mir betrachtet haben. Neben all den Experten gilt der besondere Dank meiner Frau. Sie brachte viel Verständnis auf und gab mir den Freiraum dieses Buch zu schreiben.

Inhalt

Der Autor

Hans-Leo Ross absolvierte sein Ingenieurstudium an der Uni-GH-Paderborn. Für die Preussag-Noell-LGA Gastechnik plante und realisierte er sicherheitsrelevante Anlagen und Systeme für die Öl- und Gasindustrie sowie für Offshore- und Chemieanlagen. Für HIMA Paul Hildebrandt war er für den Vertrieb von sicherheitsgerichteten Steuerungen in Großbritannien sowie Nord- und Osteuropa zuständig, bevor er die Leitung des Produktmanagements übernahm.

Seit 2004 ist der Autor bei Continental Automotive tätig. Dort ist er für die Einführung der Funktionalen Sicherheit bei Continental verantwortlich und koordiniert alle geschäftsbereichsübergreifenden Sicherheitsaktivitäten.

Er ist seit 2004 auch Mitglied im VDA AK 16 und leitet seit 2009 das deutsche Spiegelgremium zur ISO 26262, die heutige VDA-Arbeitsgruppe AK 26-01 (Grundlagen der Funktionssicherheit für Straßenfahrzeuge). Weiter war er Gründungsmitglied der WG 16 (ISO Gremium für die ISO 26262) und ist seitdem einer der deutschen Experten dieser internationalen Arbeitsgruppe. In den beiden Gremien wurden die wesentlichen Grundlagen für die Funktionale Sicherheit im Automobil erarbeitet.