Informatik aktuell

W. A. Halang (Hrsg.)

Funktionale Sicherheit

Echtzeit 2013

Springer Vieweg

Informatik aktuell

Herausgeber: W. Brauer
im Auftrag der Gesellschaft für Informatik (GI)

Wolfgang A. Halang (Hrsg.)

Funktionale Sicherheit

Echtzeit 2013

Fachtagung des gemeinsamen Fachausschusses
Echtzeitsysteme von
Gesellschaft für Informatik e.V. (GI),
VDI/VDE-Gesellschaft für Mess- und Automatisierungstechnik (GMA) und
Informationstechnischer Gesellschaft im VDE (ITG)
Boppard, 21. und 22. November 2013

GESELLSCHAFT FÜR INFORMATIK E.V.

VDI VDE VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik

ITG INFORMATIONSTECHNISCHE GESELLSCHAFT IM VDE

Springer Vieweg

CR Subject Classification (2001): C3, D.4.7

ISSN 1431-472X

ISBN 978-3-642-41308-7 e-ISBN 978-3-642-41309-4 (eBook)
DOI 10.1007/978-3-642-41309-4

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Springer Vieweg

Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier

Springer Vieweg ist eine Marke von Springer DE.

Springer DE ist Teil der Fachverlagsgruppe Springer Science+Business Media

www.springer-vieweg.de

Vorwort

Programmierbare elektronische Systeme werden in einer Fülle sicherheitsgerichteter Anwendungen eingesetzt. Sie übernehmen Aufgaben zur Überwachung oder Steuerung medizinischer Geräte, chemischer Anlagen, von Anti-Blockier-Systemen, Luft- oder Weltraumfahrzeugen, Fertigungsmaschinen sowie in Kraftwerken und der Energieverteilung. Weil falsch erstellte Systeme oder schlicht Fehler darin zum Versagen der Systemfunktionen führen können, was schwere Schäden verursachen oder gar Menschenleben gefährden kann, müssen solche eingebetteten Systeme hohe Sicherheitsanforderungen erfüllen. Der industrielle Bedarf an sicherheitsgerichteten, programmgesteuerten Systemen ist hoch und steigt durch die zunehmende Automatisierung von Prozessen kontinuierlich weiter an. Im Einklang damit wächst auch das gesellschaftliche Sicherheitsbewusstsein.

Dies sind die Gründe, warum die Fachtagung Echtzeit in diesem Jahr das Leitthema funktionale Sicherheit aufgreift, aber auch, weshalb der GI/GMA/ITG-Fachausschuss Echtzeitsysteme damit begonnen hat, die Echtzeitprogrammiersprache PEARL so weiterzuentwickeln, dass sowohl die funktionale Sicherheit in ihr geschriebener Programme erhöht als auch der Zustand erreicht werden, dass sich rechnergestützte, ggf. verteilte Systeme mit einem Grad an Vertrauen in ihre Verlässlichkeit erstellen lassen, der ihre Zulassung für sicherheitskritische Steuer- und Regelaufgaben durch die Aufsichtsbehörden auf der Basis formeller Abnahmen erlaubt. Diese Weiterentwicklung soll bis zur Formulierung einer neuen DIN-Norm vorangetrieben werden, um die bisherigen PEARL-Normen DIN 66253-2 und DIN 66253 Teil 3 abzulösen. Die zukünftige Norm wird jeweils geeignete, inhärent sichere Sprachteilmengen zur Erstellung von Anwendungen definieren, die den Sicherheitsintegritätsstufen SIL 1 bis SIL 4 nach IEC 61508 genügen müssen. So wird die weltweit einzige, im Hinblick auf funktionale Sicherheit konzipierte Programmiersprache entstehen. Aber davon wird an anderer Stelle zu berichten sein. Möglicherweise wird der Tagungsband des nächsten Jahres die ersten Ergebnisse enthalten.

Normen sind für die funktionale Sicherheit von besonderer Bedeutung. Es könnte wohl keinen Geeigneteren als den Referenten des eingeladenen Vortrages geben, der innerhalb der zuständigen Organisation, der Deutschen Kommission Elektrotechnik Elektronik Informationstechnik, seit rund zwei Jahrzehnten die einschlägigen Gemeinschaftskomitees „Grundsätze für Rechner in Systemen mit Sicherheitsaufgaben“ und „Funktionale Sicherheit elektrischer, elektronischer und programmierbarer elektronischer Systeme zum Schutz von Personen und Umwelt“ betreut, Einblick in die Denkweise der Sicherheitstechnik sowie die Normungsarbeit zu geben. Wegen ihrer inhärenten Fehleranfälligkeit muss insbesondere sicherheitsgerichtete Software auf Normenkonformität hin geprüft werden. Um dieses schwierige und zeitraubende Unterfangen zu systematisieren und bei der Prüfung nichts auszulassen, bietet sich deren Unterstützung mit Werkzeugen an, so wie sie beispielhaft im zweiten Beitrag vorgestellt wird.

Die Problematik der funktionalen Sicherheit programmierbarer elektronischer Systeme tritt seit einigen Jahren in großem Umfang in der Automobilindustrie auf, weil dort zunehmend Funktionen, die früher mechanisch, elektromechanisch oder hydraulisch realisiert wurden oder die es früher noch gar nicht gab, durch eingebettete Systeme implementiert werden. Als Themen aus diesem Bereich werden deshalb in der zweiten Sitzung ein optisches Sensorsystem für die Einknickwinkel zwischen Zugfahrzeug und Zweiachsanhänger ebenso behandelt wie die Anforderungen an Betriebssysteme, die gemeinschaftlich in komplexen, am Fahrer angebrachten Multimediasystemen arbeiten sollen.

Seit Langem liegt dem Fachausschuss die Förderung des Nachwuchses besonders am Herzen, weshalb er Studierende aufruft, ihre Abschlussarbeiten zu einem jährlichen Graduiertenwettbewerb einzureichen. Die Sieger erhalten nicht nur Preise, sondern auch Gelegenheit, sich und ihre Arbeiten auf der Tagung zu präsentieren. Die drei prämierten Arbeiten dieses Jahres beschäftigen sich mit dem Einfluss von Betriebssystemeigenschaften auf die Qualität von Lastgeneratoren, hybriden Betriebssystemen zur Verringerung von Echtzeitanforderungen sowie Interprozesskommunikation auf Mehrkernrechnern.

Die vierte Sitzung ist der Entwicklung sicherer Systeme gewidmet. Nach einem Konzept zum Aufbau fehlertoleranter verteilter Echtzeitsysteme aus standardisierten, mit mehreren Schnittstellen zu verschiedenen Bussystemen ausgestatteten Einplatinenrechnern werden Verfahren zur empirischen Bestimmung von Programmausführungszeiten auf Mehrkernprozessoren sowie zur statistischen Synthese von Modellparametern zur Sicherheitsanalyse hybrider Systeme vorgestellt.

Vor ihrem Einsatz gilt es, sicherheitsgerichtete Systeme zu verifizieren und zu validieren. Damit beschäftigt sich die abschließende Sitzung. Im Rahmen der Integration vernetzter elektronischer Systeme müssen die Aktivitäten der einzelnen Teilnehmer simuliert werden. Sicherheitsgerichtete Anwendungen speicherprogrammierbarer Steuerungen aus verifizierten Bibliotheken entnommenen Funktionsblöcken zusammenzusetzen, ist ein aufwandsreduzierender Ansatz. Die resultierenden Funktionspläne werden zur Verifikation in formale Modelle transformiert. Schließlich werden programmgesteuerte Systeme zur qualitativen Analyse ihrer funktionalen Sicherheit durch eine Kombination von Zustandsdiagrammen und fehlerbaumtypischen Gattern modelliert: erstere für die zeitlichen Beziehungen und letztere für die kausalen Zusammenhänge.

Den Autoren sei gedankt, ihre Beiträge meistens pünktlich und in vorgegebener Form abgeliefert zu haben. Auf die redaktionelle Feinarbeit an diesem Band sowie Fehlerkorrektur hat Frau Dipl.-Ing. Jutta Düring wieder viel Mühe verwendet, wofür ich ihr besonders herzlich danken möchte. Für die auch in diesem Jahr gewährte finanzielle Unterstützung der Fachtagung in Boppard ist der Fachausschuss den langjährigen industriellen Sponsoren zu großem Dank verpflichtet.

Hagen, im August 2013 Wolfgang A. Halang

Inhaltsverzeichnis

Funktionale Sicherheit und ihre Normen

Automobiltechnische Anwendungen

Graduiertenwettbewerb

Systementwicklung

Verifikation

Funktionale Sicherheit programmierbarer elektronischer Systeme

Ingo Rolle

DKE Deutsche Kommission
Elektrotechnik Elektronik Informationstechnik
im DIN und VDE, Frankfurt/Main
ingo.rolle@vde.com

Zusammenfassung. Die Deutsche Kommission Elektrotechnik Elektronik Informationstechnik (DKE) im DIN und VDE ist die nationale Organisation für die Erarbeitung von Normen und Sicherheitsbestimmungen in ihrem Bereich sowie deutsches Mitglied in der Internationalen Elektrotechnischen Kommission (IEC) und im Europäischen Komitee für elektrotechnische Normung (CENELEC). Aus Sicht dieser Organisation werden die Bedeutung funktionaler Sicherheit programmierbarer elektronischer Systeme erläutert und Aspekte ihrer Normung beleuchtet.

1 Einleitung

In unsere technisierte Umgebung halten immer mehr mikrorechnerbasierte Systeme Einzug – und sie übernehmen dabei auch Sicherheitsfunktionen. Sie wachen über den richtigen Druck im Reaktionskessel von Anlagen der chemischen Industrie, sie sorgen dafür, dass Eisenbahnzüge auf dem richtigen Gleis mit der richtigen Geschwindigkeit fahren, sie kontrollieren die Kräfte im Bremssystem in unserem Automobil, lösen bei Bedarf den Airbag aus und sie verhindern Unfälle im Umgang mit Maschinen. Wir sprechen von eingebetteten Systemen, wobei die erwähnten Sicherheitsfunktionen eine Teilmenge ihrer Aufgaben bilden.

Die Menschen möchten auf diese Helfer in ihrer Umgebung vertrauen können und erwarten hierfür eine entsprechend befähigte Technik. Funktionale Sicherheit ist das Werkzeug des Automatisierungsingenieurs, um hinreichend sicher zu sein, dass die Sicherheitsfunktionen auch richtig ausgeführt werden.

2 Was ist funktionale Sicherheit?

Funktionale Sicherheit bedeutet hierbei die Fähigkeit, die festgelegten Sicherheitsfunktionen zuverlässig und spezifikationsgemäß auszuführen. Die Auslegungsgrundsätze für Systeme, die diese Fähigkeit aufweisen sollen, sind Gegenstand der siebenteiligen Internationalen Sicherheitsgrundnorm IEC 61508, die in das deutsche Normenwerk als DIN EN 61508 (VDE 0803) übernommen wurde. Diese Norm baut auf Modellvorstellungen auf, die der Wissenschaft entnommen wurden. Aus diesen Modellvorstellungen werden Anforderungen hergeleitet. Sie

W. A. Halang (Hrsg.), *Funktionale Sicherheit,* Informatik aktuell,
DOI 10.1007/978-3-642-41309-4_1,

teilen den Markt für Produkte der Automatisierungstechnik in solche, mit denen man die Norm erfüllen kann, und solche, mit denen man dies eben nicht kann. Einige unserer Unternehmen haben sich hier sehr gut behauptet und können normgerechte Produkte anbieten. Im Folgenden werden wir beleuchten, woran das liegt und welche Rolle die Norm dabei spielt.

2.1 Warum ist funktionale Sicherheit wichtig für die Industrie?

In vielen Bereichen bietet die Automatisierungstechnik heute besondere Möglichkeiten der Produktgestaltung. In einem Markt mit ansonsten vergleichbaren Produkten können diese mittels Automatisierungstechnik besondere Merkmale bekommen, die sie vom Wettbewerb abheben. Das ist im Maschinenbau so oder auch in der Automobiltechnik, wie die vielen Assistenzsysteme eindrucksvoll zeigen, die man heute in Automobilen vorfindet. In der Automatisierungstechnik wird aber mehr und mehr die „Sicherheitstechnik“ zum entscheidenden Faktor, also die Fähigkeit, funktionale Sicherheit zu implementieren.

2.2 Wie wird funktionale Sicherheit genormt?

Dazu schauen wir uns einmal an, wie die IEC 61508, sozusagen die Mutter aller Normen zur funktionalen Sicherheit, vorgeht. Zunächst wird eine klare Vorstellung vom Versagen risikoreduzierender Maßnahmen entwickelt. Folgende Ausfallmodelle sind vertreten:

- Zufällige Ausfälle von Bauteilen.
- Ausfälle, die auf eine bestimmte Ursache zurückgeführt werden können, also systematische Ausfälle. Meistens entstehen sie durch die Begrenztheit des menschlichen Geistes, bspw. in Form von Entwurfsfehlern.

Ebenfalls gibt es eine klare Vorstellung davon, welche Maßnahmen gegen diese Arten von Ausfällen zu treffen sind:

- Maßnahmen gegen zufällige Ausfälle von Bauteilen sehen vor, die Anzahl der Ausfälle zu begrenzen, da man Zufälle nicht gänzlich verhindern kann. Dabei wird von jeder Art von Bauteil das Ausfallverhalten beobachtet. Die Ergebnisse dieser Beobachtungen werden in Form von Statistiken zusammengefasst. Auf der Grundlage dieser Statistiken und mit Hilfe bestimmter Rechenverfahren wird das zukünftige Verhalten in Bezug auf zufällige Ausfälle vorhergesagt. Ein System muss nun so ausgelegt werden, dass dieser Vorhersagewert unter einer vorgegebenen Grenze liegt.
- Systematische Ausfälle sollen durch ein Managementsystem vermieden werden, genannt „Sicherheitslebenszyklus“. Ferner werden bestimmte Techniken zur Vermeidung systematischer Fehler vorgeschrieben, wie z.B. umfangreiche Prüfungen oder das Verbot bestimmter Programmierarten.
- Falls während des Einsatzes eines Systems trotz dieser Maßnahmen dennoch zufällige oder systematische Ausfälle auftreten, muss das System hiergegen eine gewisse Toleranz aufweisen, für die ebenfalls bestimmte Techniken vorgeschrieben sind. Auch Forderungen nach Redundanz seien hier genannt.

Nun wollen wir uns ansehen, wie diese Grundsätze in der Norm umgesetzt werden und gleichzeitig, wo diese auf Opposition stoßen, was bei marktrelevante Normen meistens der Fall ist.

Tabelle 1 zeigt einen Auszug aus den normativen Anhängen des Teils 3 der IEC 61508, der sich auf Software bezieht. Dort werden bestimmte Verfahrensweisen angegeben, deren Anwendung das Entstehen systematischer Fehler vermeiden soll, also in diesem Falle Entwurfsfehler. Beispielsweise wird verlangt, dass alle Programmierer gemeinsamen Richtlinien folgen und somit ihre eigene Kreativität einschränken. An anderer Stelle geht es um die eingeschränkte Verwendung von Unterbrechungen und von Objekten, die erst zur Laufzeit mit Code hinterlegt werden. All dies wird abhängig von Sicherheitsintegritätsniveaus vorgeschrieben, d.h. je mehr das mit dem Einsatz eines Systems verbundene Risiko reduziert werden soll, umso stärkere Forderungen gelten. Es wird also nicht nur das Vorhandensein eines Qualitätssicherungssystems oder die Einhaltung des V-Modells vorgeschrieben. Alle Maßnahmen müssen dokumentiert werden, was insbesondere den Einsatz zugekaufter Software schwierig macht. Diese Anforderungen schließen bspw. die Verwendung komplexer proprietärer Betriebssysteme mehr oder weniger aus. Somit ist nachvollziehbar, dass eine Norm wie die IEC 61508 bei Produktmanagern nicht unbedingt auf Begeisterung stößt. Sie stellt zwar in vielen Fällen keinen gesetzlichen Zwang dar, entfaltet aber oft die Kraft des Faktischen. Falls ein Markt sie verlangt, heißt das meistens Neuentwicklung der Produkte.

Tabelle 1. Beispiel: DIN EN 61508-3 (VDE 0803-3): 2011, Tabelle B.1.
In der zweiten Spalte wird zu DIN EN 61508-7 (VDE 0803-7) verwiesen.
++ = besonders empfohlen, + = empfohlen, − − − = neutral

Verfahren/Maßnahme		siehe	SIL1	SIL2	SIL3	SIL4
	Verwendung von Programmierrichtlinien	C.2.6.2	++	++	++	++
	keine dynamischen Objekte	C.2.6.3	+	++	++	++
	keine dynamischen Variablen	C.2.6.3	− − −	+	++	++
	Online-Test der Erzeugung dynamischer Variablen	C.2.6.4	− − −	+	+	++
	eingeschränkte Verwendung von Unterbrechungen	C.2.6.5	+	+	++	++
	eingeschränkte Verwendung von Zeigern	C.2.6.6	− − −	+	++	++
	eingeschränkte Verwendung von Rekursionen	C.2.6.7	− − −	+	++	++
	keine unbedingten Sprünge in hochsprachlichen Programmen	C.2.6.2	+	++	++	++

Werfen wir jetzt einen Blick auf die hardwaretechnische Systemauslegung einer sicherheitsgerichteten Steuerung einschließlich ihrer Aktorik und Sensorik. Hier wird die Forderung nach einer bestimmten Probabilistik direkt mit dem Ergebnis der Risikoanalyse verknüpft. Je höher die geforderte Risikoreduzierung, also das Sicherheitsintegritätsniveau (SIL), desto geringer muss die Ausfallwahrscheinlichkeit des Systems sein. Die der Norm IEC 61508-1 bzw. DIN EN 61508-1 entnommenen Tabellen 2 und 3 zeigen dies für Systeme in niedriger Anforderungsrate bzw. für Systeme mit hoher oder kontinuierlicher Anforderungsrate. Mit dieser Forderung sehen sich viele Unternehmen überfordert. Die daraus entspringende Opposition gegen die IEC 61508 äußert sich in branchenspezifischen Normen, die keine probabilistischen Betrachtungen fordern oder sie stark reduzieren. Dabei wird übersehen, dass auch in Bereichen wie der chemischen Industrie, die die IEC 61508 übernommen haben, mit der branchenspezifischen Norm IEC 61511 letztlich auch nur „mit Wasser gekocht wird“. Das heißt, hier werden für die zu erwartende Ausfallwahrscheinlichkeit pauschale Rechnungen durchgeführt, die auf der sicheren Seite liegen, und zu sog. „Typicals“ führen. Die Gegner dieser Tabelle wünschen sich ausschließlich Architekturanforderungen, also Redundanz gemäß Tabelle 4. Da die Normung sehr dezentral organisiert ist und es keine zentrale, kontrollierende Instanz gibt, jedenfalls keine, die wirklich funktionieren würde, ist es meistens möglich, branchenspezifische Normen zur Verabschiedung zu führen. Das Problem dabei ist, dass in manchen Teilen der Welt sehr großer Wert auf Probabilistik gelegt und diese als Beleg für Hardwarequalität angesehen wird. Diese Märkte verunsichert man durch derartige Seitwärtsbewegungen in der Normung.

Tabelle 2. Ausfallgrenzwerte für eine Sicherheitsfunktion, die in einer Betriebsart mit niedriger Anforderungsrate betrieben wird

Sicherheits-integritätsniveau	mittlere Wahrscheinlichkeit eines gefahrbringenden Ausfalls bei Anforderung der Sicherheitsfunktion
4	$\geq 10^{-5}$ bis $< 10^{-4}$
3	$\geq 10^{-4}$ bis $< 10^{-3}$
2	$\geq 10^{-3}$ bis $< 10^{-2}$
1	$\geq 10^{-2}$ bis $< 10^{-1}$
Siehe nachfolgende Anmerkungen 2 bis 6 für Einzelheiten zur Interpretation dieser Tabelle.	

Sichere Ausfälle sind solche, die ein System in einen sicheren Zustand versetzen, also z.B. eine Maschine stillsetzen. Wenn in einem redundanten System eine Diagnoseeinrichtung in einem Kanal einen Fehler erkennt und auf die fehlerfreien Kanäle umschaltet, so ist das auch ein sicherer Ausfall. Fehlertoleranz der Hardware von 1 bedeutet einfache Redundanz, d.h. bei Ausfall eines Kanals kann die Sicherheitsfunktion noch aufrecht erhalten werden.

Tabelle 3. Ausfallgrenzwerte für eine Sicherheitsfunktion, die in einer Betriebsart mit hoher Anforderungsrate oder mit kontinuierlicher Anforderung betrieben wird

Sicherheits-integritätsniveau	Rate gefahrbringender Ausfälle der Sicherheitsfunktion (h^{-1})
4	$\geq 10^{-9}$ bis $< 10^{-8}$
3	$\geq 10^{-8}$ bis $< 10^{-7}$
2	$\geq 10^{-7}$ bis $< 10^{-6}$
1	$\geq 10^{-6}$ bis $< 10^{-5}$
Siehe nachfolgende Anmerkungen 2 bis 6 für Einzelheiten zur Interpretation dieser Tabelle.	

Tabelle 4. Aus Architekturanforderungen abgeleitete Eingruppierung in Sicherheitsintegritätsniveaus

	Fehlertoleranzen der Hardware (siehe Anmerkung 2)		
Anteil sicherer Ausfälle	0	1	2
< 60 %	nicht erlaubt	SIL1	SIL2
60 % < 90 %	SIL1	SIL2	SIL3
90 % < 99 %	SIL2	SIL3	SIL4
> 99 %	SIL3	SIL4	SIL4
Hardware-Fehlertoleranz von N bedeutet, dass N + 1 Fehler zu einem Verlust der Sicherheitsfunktion führen können.			

Der Umgang mit Diagnoseeinrichtungen und Mehrheitsentscheidern muss jedoch geübt sein; dazu reichen die Fähigkeiten vieler Entwicklungsabteilungen oft nicht aus. Deshalb bewirkt gerade die Orientierung an Tabelle 4 eine Trennung des Marktes in solche Anbieter, die Sicherheitsprodukte entwickeln können, und solche, die es nicht können.

Für die Fortschreibung der IEC 61508 ist der internationale Normenausschuss IEC SC 65A MT 61508 zuständig, in den die Mitgliedsländer der IEC Experten entsenden. Die deutschen Experten kommen aus Betreiberunternehmen der chemischen Industrie, Herstellerfirmen von Automatisierungsprodukten und Prüfhäusern. Eine starke Fraktion innerhalb des Ausschusses, die nicht aus Deutschland kommt, kämpft seit vielen Jahren dafür, Tabelle 4 abzuschaffen bzw. eine Umgehung dafür in die Norm einzubauen. Ziel dieser Gruppe ist es, auch einkanalige Systeme bis hin zu SIL 4 zuzulassen, sofern hinreichende statistische Belege für ihre Zuverlässigkeit vorliegen. Statistiken sind mitunter schwierig überprüfbar und die deutschen Prüfhäuser sind strikt dagegen, weil sie befürchten, dass dieses Vorgehen zu unsicheren Anlagen führt. Außerdem wäre es natürlich eine große Gefahr für diejenigen Hersteller, die in die Entwicklung von anspruchsvoller Sicherheitstechnik investiert haben. Die Trennung des Mark-

tes in Sicherheitsprodukte und andere wäre aufgehoben. Ein Hersteller sagte im persönlichen Gespräch:

> „Wenn das kommt, brauchen wir nur noch einen guten Mathematiker und eine billige Fertigung."

Der Kampf ging erst einmal so aus, dass in die jüngst erschienene zweite Ausgabe der IEC 61508-2 eine solche Umgehung zwar eingebaut ist, jedoch mit so hohen statistischen Hürden, dass sie für die allermeisten Hersteller kaum in Frage kommen dürfte.

3 Fazit

Es ist sicher nicht übertrieben, funktionale Sicherheit als eine Schlüsseltechnologie für viele Industrien zu bezeichnen. Bis jetzt sind wir auf einem guten Wege, diese international zu vertreten und weiter zu entwickeln – trotz einiger „Seitwärtsbewegungen". Die DKE unterstützt die deutsche Industrie nach besten Kräften dabei, die internationale Normung als entscheidende Plattform zu nutzen. Eine Norm mit klarem Modell als Ausgang und einem nachvollziehbaren Gang des Nachweises hilft hierbei. Damit das so bleibt, sollten wir weiterhin in vorderster Linie in der internationalen Normung mitarbeiten, unseren internationalen Partnern dabei zuhören und versuchen, sie zu verstehen. Aufweichungsversuche wären dabei schädlich und würden das öffentliche Vertrauen in die Automatisierungstechnik zerstören. Wir sollten den Mut haben, ihnen entgegenzutreten. Der Erfolg zeigt sich in der weltweiten Akzeptanz der Produkte der Hersteller und den Referenzprojekten der Anlagenbauer.

Literaturverzeichnis

1. DIN EN 61508-1 (VDE 0803-1): Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 1: Allgemeine Anforderungen (IEC 61508-1:2010); Deutsche Fassung EN 61508-1:2010
2. DIN EN 61508-2 (VDE 0803-2): Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme (IEC 61508-2:2010); Deutsche Fassung EN 61508-2:2010
3. DIN EN 61508-3 (VDE 0803-3): Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 3: Anforderungen an Software (IEC 61508-3:2010); Deutsche Fassung EN 61508-3:2010