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

Funktionale Sicherheit programmierbarer elektronischer Systeme 1
Ingo Rolle

Werkzeugunterstützung der Prüfung sicherheitsgerichteter Software auf Normenkonformität 7
Günter Glöe, Detlev Volkwarth

Automobiltechnische Anwendungen

Reaktive optische Einknickwinkelvermessung bei Gliederfahrzeugen 19
Simon Eggert, Christian Fuchs, Frank Bohdanowicz, Dieter Zöbel

IT-Sicherheits-Eigenschaften für eng gekoppelte, asynchrone Multi-Betriebssysteme im automotiven Umfeld 29
Pierre Schnarz, Joachim Wietzke

Graduiertenwettbewerb

Leistungs- und Präzisionssteigerung des Lastgenerierungsprozesses von UniLoG unter Verwendung echtzeitfördernder Maßnahmen durch das Betriebssystem 39
Alexander Beifuß

Slothful Linux: Ein effizientes, hybrides Echtzeitbetriebssystem durch Hardware-basierte Task-Einlastung 49
Rainer Müller

Entwurf und Implementierung einer Prozessinterkommunikation für Multi-Core CPUs 59
Manuel Strobel

Systementwicklung

Fehlertolerante verteilte Systeme aus Standardkomponenten 69
Peter F. Elzer

Framework für die empirische Bestimmung der Ausführungszeit auf Mehrkernprozessoren 77
Julian Godesa, Robert Hilbrich

Statistische Parametersynthese für hybride Systeme 87
Christian Schwarz

Verifikation

Simulation von Teilnehmern verteilter Systeme zur Verifikation und Systemintegration 97
Silvije Jovalekic, Michael Wiescholek, Bernd Rist

Verifikation und Validierung sicherheitsgerichteter SPS-Programme 107
Doaa Soliman, Georg Frey

Qualitative Analyse der funktionalen Sicherheit software-intensiver Systeme mittels Zustands/Ereignis-Fehlerbäumen 117
Michael Roth, Peter Liggesmeyer

http://www.springer.com/978-3-642-41308-7

Funktionale Sicherheit
Echtzeit 2013
(Ed.)W.A. Halang
2013, VIII, 126 S. 50 Abb., Softcover
ISBN: 978-3-642-41308-7