

Informatik aktuell

Herausgegeben
im Auftrag der Gesellschaft für Informatik (GI)

Herwig Unger (Hrsg.)

Echtzeit und Sicherheit

Echtzeit 2018

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, 15. und 16. November 2018

GESELLSCHAFT FÜR INFORMATIK E.V.



VDE

VDI/VDE-Gesellschaft
Mess- und Automatisierungstechnik

ITG

INFORMATIONSTECHNISCHE
GESELLSCHAFT IM VDE



Springer Vieweg

Herausgeber

Herwig Unger
Lehrstuhl für Kommunikationsnetze
FernUniversität in Hagen
Hagen, Deutschland

Programmkomitee

R. Baran	Hamburg
J. Bartels	Krefeld
M. Baunach	Graz
B. Beenen	Lüneburg
J. Benra	Wilhelmshaven
V. Cseke	Wedemark
R. Gumzej	Maribor
W. A. Halang	Hagen
H. H. Heitmann	Hamburg
M.M. Kubek	Hagen
R. Müller	Furtwangen
M. Schaible	München
G. Schiedermeier	Landshut
U. Schneider	Mittweida
H. Unger	Hagen
D. Zöbel	Koblenz

Netzstandort des Fachausschusses Echtzeitsysteme: www.real-time.de

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

ISSN 1431-472X

ISBN 978-3-662-58095-0 ISBN 978-3-662-58096-7 (eBook)

<https://doi.org/10.1007/978-3-662-58096-7>

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

© Springer-Verlag GmbH Deutschland, ein Teil von Springer Nature 2018

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsgesetz zugelassen ist, bedarf der vorherigen Zustimmung des Verlags. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.

Der Verlag, die Autoren und die Herausgeber gehen davon aus, dass die Angaben und Informationen in diesem Werk zum Zeitpunkt der Veröffentlichung vollständig und korrekt sind. Weder der Verlag noch die Autoren oder die Herausgeber übernehmen, ausdrücklich oder implizit, Gewähr für den Inhalt des Werkes, etwaige Fehler oder Äußerungen. Der Verlag bleibt im Hinblick auf geografische Zuordnungen und Gebietsbezeichnungen in veröffentlichten Karten und Institutionsadressen neutral.

Springer Vieweg ist ein Imprint der eingetragenen Gesellschaft Springer-Verlag GmbH, DE und ist ein Teil von Springer Nature

Die Anschrift der Gesellschaft ist: Heidelberger Platz 3, 14197 Berlin, Germany

Vorwort

Kontrolle des Eigenheims aus der Ferne, Überweisungen und andere Finanztransaktionen in Echtzeit, Videogespräche über das Internet mit Partnern am anderen Ende der Welt: längst ist eine Reihe von Anwendungen mit Echtzeitcharakter oder -anforderungen an Verarbeitungs- und/oder Übertragungsgeschwindigkeit bequeme Selbstverständlichkeit für jedermann geworden. Weitaus länger und genauso intensiv nutzt die Industrie über das Internet zugängliche oder beeinflussbare Steuerungen und Kommunikationseinrichtungen. Andererseits sind mittlerweile selbst die Nachrichten in den Medien voll mit Meldungen über ungewollte Störungen Dritter, private oder staatlich gewollte oder kontrollierte Angriffe.

Der Wurm Stuxnet, der gezielt kerntechnische Anlagen befiel und empfindlich hätte stören können, war nur ein erster, massiver Fall, der in die Öffentlichkeit durchdrang und damit der Allgemeinheit die Gefährdungslage unmissverständlich vor Augen führte. Die wirklichen Gefahren, die durch Cyberattacken oder gar einen Cyberkrieg heraufbeschworen werden, konnte der gewillte Bürger von diesem Zeitpunkt an leicht selbst einschätzen, insbesondere wenn er die Abhängigkeit der Industrie und des öffentlichen Lebens vom Internet in vollem Umfang begreift. Es wird klar, dass es hierbei nicht mehr nur um finanzielle Verluste, sondern um reale Gefahren für Leib und Leben der Bevölkerung geht.

Vergessen wird in den Betrachtungen gerne, dass immanente Gefährdungen jedoch vor allem von der Komplexität der zu steuernden und der steuernden Systeme selber ausgehen. Genaue und tiefgehende Durchdringungen aller Anwendungsfälle und Tests aller möglichen Kombinationen von Eingabedaten sind i. A. aber vor allem durch viel zu kurze Zeitvorgaben bei den Entwicklungsterminen nicht zu realisieren: ökonomische Zwänge dominieren Sicherheitsbedenken. So sind selbst bei einem optimal verlaufenden Systementwurf (systematische) Fehler in den Quellcodes in keiner Weise völlig auszuschließen und heute eher die im Prototyp zu erwartende Regel. Ungewollte und unberücksichtigte Veränderungen in den Systemumgebungen, insbesondere durch Wechselwirkungen mit anderen (fremdentwickelten) Systemen, tragen während der Nutzungsdauer ein weiteres, besonderes Risiko in sich, sind aber gerade im Zeitalter mehr und mehr automatischer und sich selbst organisierender Produktion typische Situationen.

Damit ist es nur konsequent, dass das Leitthema unserer nun zum 39. Mal stattfindenden Tagung „Echtzeit“ mit der Unterthematik Systemsicherheit wieder einmal die aktuelle Entwicklung aufgreift und sich (wiederholt) der Frage stellt, welche Veränderungen hier in den letzten Jahren eingetreten sind.

Mit der nun DIN-normierten Echtzeitsprache SafePEARL hat der entsprechende Arbeitskreis unseres Fachausschusses unzweifelhaft einen einzigartigen Beitrag für sichere Systeme geleistet: eine Arbeit, die auf eine inzwischen fast fünfzigjährige Entwicklung von den ersten Anfängen an zurückblicken kann. Diesem Erfolg widmen wir in diesem Jahr einen speziellen Eröffnungsvortrag, der nach allen Einzelbeiträgen der Vorjahre das Gesamtwerk ausführlich würdigt.

Neben weiteren Beiträgen zur Vermeidung von Störungen der Arbeit datenverarbeitender Systeme und von Kommunikation durch Dritte ist Fehlervermeidung und -toleranz die zweite Seite der Medaille. Funktionale Sicherheit stellt daher das Thema einer weiteren Sitzung unseres Treffens dar, das sowohl in industriellen Normen als auch in der Lehre seine Widerspiegelung findet. Aktuelle Anwendungen im Rahmen von Industrie 4.0, wie z. B. flexible Transportsysteme und insbesondere Autonomes Fahren, bieten hier eine Vielzahl von Themen zur Diskussion. Eine Reihe weiterer Beiträge aus Hardware- und Betriebssystemsicht und insbesondere in Bezug auf Schnittstellen komplettiert die Perspektive des Fachausschusses auf die Probleme.

Offen bleibt trotz aller wissenschaftlichen und technischen Leistungen dennoch eine Reihe von Fragen. Ihr Kern lässt sich in einer Frage zusammenfassen, und zwar warum die Industrie auf alle bislang präsentierten und z. T. sogar sehr einfachen Hardwarelösungen (wie z. B. den Übergang zur Harvard-Architektur) verzichtet und stattdessen ausschließlich auf immer wieder korrumpierbare Softwarelösungen setzt.

Alle Organisatoren der Tagung hoffen, dass das Hotel „Ebertor“ in Boppard mit der unvergleichlichen Natur des mittleren Rheintals erneut ein inspirierender und für den Fachausschuss fast heimischer Ort für eine Reihe innovativer Vorträge und fruchtbringender Diskussionen sein wird. Nicht zuletzt sei wiederum Frau Düring für ihre Arbeit bei der Organisation der Tagung und der technischen Erstellung des vorliegenden Tagungsbandes gedankt.

Hagen, im August 2018

Herwig Unger

Inhaltsverzeichnis

Eröffnungsvortrag

Von Algol 68 zu SafePEARL	1
<i>Wolfgang A. Halang, Marcel Schaible</i>	

Funktionale Sicherheit

Funktionale Sicherheit von autonomen Transportsystemen in flexiblen I4.0 Fertigungsumgebungen	11
<i>Philip Kleen, Janis Albrecht, Jürgen Jasperneite, Detlev Richter</i>	

Secure Real-time Communication	21
<i>Dimitrios Savvidis, Dietmar Tutsch</i>	

Entwicklungsvorschläge für ISO 26262 konforme MCUs in sicherheitskritischer Avionik	29
<i>Georg Seifert, Sebastian Hiergeist, Andreas Schwierz</i>	

Lehre

Autonomes Fahren in der Lehre	39
<i>Andreas Werner, Robert Kaiser</i>	

Automatische Evaluierung von Anforderungen bezüglich der Informationssicherheit für das zukünftige industrielle Netzwerkmanagement	49
<i>Marco Ehrlich, Henning Trsek, Jürgen Jasperneite</i>	

SWAN: Systemweite statische Laufzeitanalyse echtzeitfähiger Betriebssysteme	59
<i>Simon Schuster</i>	

Applikationen von Echtzeitsystemen

Spezifikation projektspezifischer Software	69
<i>Jens Lehmann</i>	

Timekeeper - Zeiterfassung mittels RFID und Raspberry Pi	79
<i>Denise Papaioannou, Mario Kubek</i>	

Schutz automatisierungstechnischer Programme vor Umkehrentwicklung .	89
<i>Sergej Gertje</i>	

Sicherheitsgerichtete Echtzeitsysteme

Latenzen von POSIX Betriebssystemen im Kontext von Hypervisoren in Real-Time Systemen	99
<i>Ludwig Thomeczek, Andreas Attenberger, Václav Matoušek, Jürgen Mottok</i>	
fastAN(BD) – eine Methode zur schnellen Dekodierung und Integritätsprüfung ANBD-kodierter Daten	109
<i>Stefan Widmann</i>	
Parametrierbare Übergabeschnittstellen im Entwurfsprozess für sicherheitsgerichtete Systeme	119
<i>Daniel Koß</i>	