Entwicklung von Echtzeitsystemen

Hubert B. Keller

Entwicklung von Echtzeitsystemen

Einführung in die Entwicklung zuverlässiger softwarebasierter Funktionen unter Echtzeitbedingungen

Springer Vieweg

Hubert B. Keller
Institut für Automation und angewandte Informatik (IAI)
Karlsruher Institut für Technologie (KIT)
Karlsruhe, Deutschland

ISBN 978-3-658-26640-0 ISBN 978-3-658-26641-7 (eBook)
https://doi.org/10.1007/978-3-658-26641-7

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 Vieweg ist ein Imprint der eingetragenen Gesellschaft Springer Fachmedien Wiesbaden GmbH und ist ein Teil von Springer Nature.
Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

Vorwort

Die Automatisierung technischer Systeme ist das Rückgrat unserer modernen Gesellschaft. Softwarebasierte Funktionen realisieren dabei in allen Bereichen wesentliche Innovationen auf Basis zuverlässiger Technologien der Informationsverarbeitung unter Echtzeitbedingungen.

Die Anwendungen reichen dabei von verfahrenstechnischen Anlagen, verteilten kritischen Infrastrukturen wie Energieverteilungssystemen, der Wasserversorgung und Verkehrsleitanlagen über Home-Automation-Systeme, intelligente Staubsauger und Fuzzy-Control-gesteuerte Waschmaschinen, autonome Transportsysteme, mechatronische Systeme wie ABS- und ESP-Systeme sowie bildbasierte und interpretative Kollisions- und Fußgängererkennung im Automobil, Herzschrittmacher, Infusionspumpen und Röntgengeräte bis zu den zukünftigen vollständig autonomen mobilen Systemen aller Art.

Der Grad an Automatisierung in unserer Gesellschaft lässt sich daran bemessen, dass weit über 90 % aller Rechner in eingebetteten Anwendungen eingesetzt sind (mittlerweile wird von 98 % aller Rechner als eingebettet ausgegangen [Aca2011]). Alle Disziplinen vertrauen auf softwarebasierte Funktionen unter Echtzeitbedingungen. Der durch Software realisierte Anteil beträgt mittlerweile fast die Hälfte an der Wertschöpfung in den technischen Bereichen. Nach Isermann [Ise2008], Seite V, sind die Entwicklungen bei mechatronischen Systemen durch eine intensive Informationsverarbeitung charakterisiert: „Die funktionelle Integration wird jedoch entscheidend durch die Informationsverarbeitung und damit durch die Gestaltung der Software geprägt."

Die Herstellung von Software ist im Allgemeinen und insbesondere bei Echtzeitsoftware, wie sie in der Automatisierung zur Anwendung kommt, noch immer fehlerbehaftet und mit hohen Kosten verbunden. Ein echter Mehrwert durch Software kann dann erreicht werden, wenn die Funktionen zuverlässig, fehlerbeherrschbar und bei offenen und vernetzten Systemen informationstechnisch sicher sind. Die zeitlichen Eigenschaften sind beweisbar zu erbringen und die Herstellung muss ökonomisch vertretbar sein. Eine erhebliche Anzahl an Fehlern wird in frühen Phasen der Entwicklung injiziert und mit hohen Kosten erst in späteren Phasen erkannt und behoben. Hier muss die Analyse als Teil des gesamten Entwicklungsprozesses konkreter angegangen werden. Dazu bedarf es entspre-

chender analyse- und teamorientierter Beschreibungsverfahren. Der Rational Unified Process (RUP) als iterativer, inkrementeller, objektorientierter und architekturzentrierter Prozess liefert mit der Unified Modeling Language (UML) eine entsprechende grafische Methode. Die UML bietet als teamorientierter Zugang ein wertvolles Hilfsmittel. Ausgehend von Anwendungsfällen (Use Cases) können für nebenläufige Strukturen, wie sie in der Automatisierung grundsätzlich auftreten, notwendige Analysen und Beschreibungen erstellt werden. Auch die Optimierung von Entwicklungsprozessen ist nach den Vorgaben des Capability Maturity Model Integrated (CMMI) nachhaltig möglich, wie Ergebnisse abgeschlossener Projekte zeigen.

Die Automatisierung von Anlagen und Maschinen sowie kritischen Infrastrukturen etc. bedeutet das Ausführen von softwarebasierten Funktionen unter Echtzeitbedingungen. Die Ausführung hat deterministisch und beweisbar zu erfolgen. Sicherheitskritische Anwendungen müssen die entsprechenden Zielfunktionen verlässlich und rechtzeitig erbringen. Hierzu sind verschiedene Arten der rechtzeitigen und gleichzeitigen Behandlung von realen Ereignissen möglich. Das prozessorientierte Konzept mit virtuellen Recheneinheiten (CPU – Central Processing Unit) und der prioritätenbasierten Abbildung auf reale CPUs mit preemptivem Scheduling (verdrängende Ausführung) erlaubt die Trennung der Ausführung und der Verwaltung von Funktionen bzw. Prozessen. Die Trennung von Ausführung und Verwaltung mit der gegenseitigen Isolierung der Prozessausführung ist ein zentraler Aspekt für die konstruktive Sicherstellung der Zuverlässigkeit von Echtzeitsoftware.

Sowohl bei Model Driven Architecture (MDA) zur automatischen Codegenerierung als auch bei der manuellen Programmierung steht eine Programmiersprache als Ziel den Modellbeschreibungen gegenüber. Die Programmiersprache muss adäquate Sprachelemente zur Abbildung nebenläufiger Prozesse und alle weiteren Modellierungsaspekte, wie typstrenge Datenstrukturen, Module mit „information hiding“ (Verbergen der Implementierung) als Architekturbausteine sowie sichere Kontrollstrukturen besitzen. Zusätzlich ist eine Laufzeitumgebung notwendig, die Fehler im Ablauf erkennt und es erlaubt, sinnvoll darauf zu reagieren. Die Programmiersprache Ada erfüllt hierzu alle wesentlichen Anforderungen.

Safety-Anforderungen sind bei offenen und vernetzten Systemen und Anlagen des Maschinenbaus untrennbar mit Security-Anforderungen verknüpft. Hierzu müssen Architekturen und Konzepte definiert werden, um sicherheitskritische Risiken zu beherrschen. Sender und Empfänger von Daten sind zu identifizieren, Transportwege zu sichern und auch systemfremde Software beherrschbar einzubinden. Viele Probleme aus dem Bereich der Informationssicherheit (Cyber-Angriffe) können in der Implementierung durch eine Sprache wie Ada vermieden werden. Dies ist durch den Vergleich der Indizierungskonzepte von C/C++ und Ada ersichtlich. Die Manipulation und Veränderung von Daten in Programmanweisungen durch Überschreiten von Indexgrenzen oder beim Aufrufkontext („call frame“) von Prozeduren wird durch das Typkonzept von Ada und die Prüfung zur Laufzeit verhindert. Hier ist ein Umdenken in der Ausbildung im Bereich der Programmierung und des Softwareengineerings erforderlich, damit „Buffer Overflow“

oder „handcrafted commands and parameter“ als Angriffsvektoren im Cyber Security nicht mehr existent sind.

Automatisierung ist umfassend zu verstehen. Die Entwicklung softwarebasierter Funktionen unter Echtzeitbedingungen in der Automatisierung wird hier auf eine systematische Basis gestellt. Es werden die notwendigen Anforderungen sowie deren Erfüllbarkeit analysiert und eine integrative Darstellung und Bewertung der notwendigen Randbedingungen und Methoden zur Realisierung von zuverlässigen softwarebasierten Funktionen unter Echtzeitbedingungen zur Automatisierung vorgenommen.

Arbeiten des VDI (Verein Deutscher Ingenieure e.V.) Präsidiumsarbeitskreises „Technische Sicherheit“, in denen der Autor maßgeblich involviert war, haben gezeigt, dass der Begriff und das Konzept der „funktionalen Sicherheit“ (Safety) in den verschiedenen Anwendungsbereichen sehr unterschiedlich ausgelegt und umgesetzt wird. Der Arbeitskreis hat über viele Jahre das große Gemeinsame herausgearbeitet und eine disziplinübergreifende Sichtweise, Systematik und Methodik abgeleitet und definiert. Das Ergebnis ist mittlerweile als englischsprachiges Buch im Springer-Verlag publiziert.

Auch eine integrative Sicht auf Security-Anforderungen in der Automatisierung wurde unter Mitwirkung des Autors im Rahmen des Lenkungskreises Security des ZVEI erarbeitet. Das Ergebnis wurde als Namur-Empfehlung NE 153 publiziert (Namur – Interessengemeinschaft Automatisierungstechnik der Prozessindustrie) und deckt von der Anforderungsanalyse bis zur Wartung im Betrieb alle Aspekte von Security in der Automatisierung ab.

Der Autor war in der Entwicklung von Prozessrechnersystemen mit redundanter Funktionalität für hoch sicherheitskritische Anwendungen bei der Siemens AG tätig. Danach entwickelte er am Kernforschungszentrum Karlsruhe umfangreiche verteilte Echtzeitsysteme mit der Sprache Ada. Diese war nach softwaretechnischen Kriterien ausgewählt worden. Die Verwendung von Tasks mit entsprechenden Kommunikationsschnittstellen in Ada ist eine Methode, um die Komplexität im Ablaufverhalten zu beherrschen. Weitere Systeme zur Automatisierung komplexer industrieller Prozesse haben auch sprachfremde Software eingebunden. Hier hat sich dann die Eigenschaft des Ada-Laufzeitsystems gezeigt, Fehler synchron zur Programmausführung grundsätzlich zu erkennen, zu melden und eine Reaktion darauf zu ermöglichen. Der weitere Weg war der Einsatz von Model-Driven-Architecture-Ansätzen für hochzuverlässige und gleichzeitig zu 70 % automatisch generierte Systeme. Dabei erfolgte die Integration von Sicherheitsprotokollen für die Kommunikation verteilter Systemkomponenten. Im Rahmen von Kooperationen mit der Industrie ist z. B. das INSPECT-pro-control-System mit sehr hoher Zuverlässigkeit, geringsten Fehlerraten und erheblich geringerem Budget als vergleichbare Entwicklungen realisiert worden. Das INSPECT-pro-control-System ist ein generisches Werkzeug, das mittlerweile weltweit und nahezu fehlerfrei in Anlagen der Industrie unter Echtzeitbedingungen eingesetzt wird. Anwendungsbereiche sind z. B. thermische Abfallbehandlung, Zinkrecycling, Zementindustrie, verteilte Sensorsysteme und Sonderabfallbehandlung.

Die vielfältigen Anforderungen der wissenschaftlichen Tätigkeit im Bereich der hochinterdisziplinären Technologieentwicklung am Karlsruher Institut für Technologie

(KIT) und dessen Vorläufer (Kernforschunsgzentrum und später Forschunsgzentrum) und einer gleichzeitigen erfolgreichen industriellen Umsetzung sowie die Vermittlung des gesamten Methodenspektrums in der Lehre waren und sind eine hochinteressante Herausforderung. Das angestrebte Ziel war immer, innovative, leistungsfähige und von der Industrie akzeptierte Systeme zur Automatisierung komplexer industrieller Prozesse unter Echtzeitbedingungen zu realisieren. Das ingenieurwissenschaftliche Vorgehen verbindet hierbei die Methoden des Ingenieurwesens und den hohen Zuverlässigkeitsgrad von Systemen mit den Methoden der Informatik. Mein Dank geht sowohl an meine Mitarbeiter für die fruchtbare und hervorragende Zusammenarbeit als auch an die übergeordneten Führungsebenen für die kreativen und konstruktiven Freiräume. Dadurch konnten schon früh wissenschaftlich innovative Entwicklungen der Ingenieurwissenschaften und der Informatik sich gegenseitig befruchtend prototypisch angegangen und nachfolgend industriell erfolgreich umgesetzt werden.

Diese vielfältigen und herausfordernden Forschungs- und Entwicklungsthemen haben dabei zeitlich durchweg auch in den privaten Bereich hineingewirkt. Daher danke ich ganz besonders meiner Familie für das Verständnis für die Arbeit eines immer intensiv beschäftigten Wissenschaftlers.

Karlsruhe, 2019 Hubert B. Keller

Literatur

[Aca2011] Cyber-Physical Systems. Acatech Position. Deutsche Akademie der Wissenschaften, Berlin (2011), Seite 5.

[Ise2008] Isermann, R.: Mechatronische Systeme – Grundlagen. Springer, Heidelberg (2008). ISBN: 978-3-540-32512-3

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Lizenz zum Wissen.

Sichern Sie sich umfassendes Technikwissen mit Sofortzugriff auf tausende Fachbücher und Fachzeitschriften aus den Bereichen: Automobiltechnik, Maschinenbau, Energie + Umwelt, E-Technik, Informatik + IT und Bauwesen.

Exklusiv für Leser von Springer-Fachbüchern: Testen Sie Springer für Professionals 30 Tage unverbindlich. Nutzen Sie dazu im Bestellverlauf Ihren persönlichen Aktionscode **C0005406** auf *www.springerprofessional.de/buchaktion/*

Jetzt 30 Tage testen!

Springer für Professionals.
Digitale Fachbibliothek. Themen-Scout. Knowledge-Manager.

- Zugriff auf tausende von Fachbüchern und Fachzeitschriften
- Selektion, Komprimierung und Verknüpfung relevanter Themen durch Fachredaktionen
- Tools zur persönlichen Wissensorganisation und Vernetzung

www.entschieden-intelligenter.de

Springer für Professionals

Springer