Fortschritt-Berichte VDI

VDI

Reihe 10

Informatik/
Kommunikation

Stefan Widmann, M.Sc.,
Freudenberg

Nr. 856

Eine Datenspezifikations-architektur

FernUniversität in Hagen
Schriften zur Informations- und Kommunikationstechnik

Fortschritt-Berichte VDI

Reihe 10

Informatik/
Kommunikation

Stefan Widmann, M.Sc.,
Freudenberg

Nr. 856

Eine Datenspezifikations-architektur

FernUniversität in Hagen
Schriften zur Informations- und Kommunikationstechnik

Widmann, Stefan
Eine Datenspezifikationsarchitektur
Fortschr.-Ber. VDI Reihe 10 Nr. 856. Düsseldorf: VDI Verlag 2017.
328 Seiten, 91 Bilder, 42 Tabellen.
ISBN 978-3-18-385610-7, ISSN 0178-9627,
€ 104,00/VDI-Mitgliederpreis € 93,60.

Für die Dokumentation: Echtzeitsysteme – funktionale Sicherheit – sicherheitsgerichtete Echtzeitsysteme – IEC 61508 – Mikroprozessorarchitekturen – Prozessorarchitekturen – Datentyparchitekturen – Befähigungsarchitekturen – Datenfluss – Datenflussüberwachung

Die vorliegende Arbeit richtet sich an Ingenieure und Wissenschaftler in den Bereichen Mikroprozessorarchitektur und sicherheitsgerichtete Echtzeitsysteme. Sie beginnt mit der Identifikation von 20 datenflussbezogenen Fehler- und Angriffsarten und evaluiert anhand dieser den Stand von Wissenschaft und Technik. Anschließend wird eine neue Prozessorarchitektur, die Datenspezifikationsarchitektur, vorgestellt, welche die in Vergessenheit geratenen Merkmale von Datentyparchitekturen stark erweitert und alle Dateneigenschaften in Form zusätzlicher Kennungen untrennbar mit dem Datenwert verknüpft, überträgt, speichert und verarbeitet. Dies ermöglicht es der neuen Architektur, alle 20 Fehler- und Angriffsarten zu erkennen. Die schlussendliche Gegenüberstellung des Stands von Wissenschaft und Technik und der Datenspezifikationsarchitektur zeigt die Überlegenheit der neuen Architektur und deren hervorragende Eignung für die Realisierung sicherheitsgerichteter Anwendungen.

Bibliographische Information der Deutschen Bibliothek
Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliographie; detaillierte bibliographische Daten sind im Internet unter http://dnb.ddb.de abrufbar.

Bibliographic information published by the Deutsche Bibliothek
(German National Library)
The Deutsche Bibliothek lists this publication in the Deutsche Nationalbibliographie (German National Bibliography); detailed bibliographic data is available via Internet at http://dnb.ddb.de.

Schriften zur Informations- und Kommunikationstechnik
Herausgeber:
Wolfgang A. Halang, Lehrstuhl für Informationstechnik
Herwig Unger, Lehrstuhl für Kommunikationstechnik
FernUniversität in Hagen

Als Manuskript gedruckt. Printed in Germany.
ISSN 0178-9627
ISBN 978-3-18-385610-7

Vorwort

Der Bedarf an sicherheitsgerichteten, programmgesteuerten (eingebetteten) Systemen aller Art ist hoch und steigt durch die zunehmende Automatisierung von Prozessen kontinuierlich weiter an. Im Einklang damit wächst auch das gesellschaftliche Sicherheitsbewusstsein. Weil die auf dem Markt vorherrschenden Prozessorarchitekturen kaum Schutz gegen typische Programmierfehler und Malware-Attacken bieten, hatte der Autor des vorliegenden Buches sich zur Aufgabe gemacht, aufbauend auf den allgemeinen Sicherheitsanforderungen gemäß der Norm IEC 61508 auf Maschinenebene eine völlig neue, von Grund auf auf Sicherheit hin ausgelegte Rechnerarchitektur zu entwerfen, die eine Fülle von Programmierfehlern ohne Software-Hilfe erkennen kann und daraufhin die Programmausführung abbricht.

Der Autor des 2014 unter dem Titel „Verfahren zur Kontrollflussüberwachung in sicherheitsgerichteten Rechensystemen“ in dieser Buchreihe mit der Nummer 832 erschienenen Bandes hatte sich bereits sehr eingehend mit der Sicherung des Kontrollflusses in sicherheitsgerichteten Echtzeitsystemen beschäftigt und beeindruckende Ergebnisse vorgelegt. Allerdings stellen Kontrollflussfehler nur einen geringen Anteil aller Programmfehler dar. Der weitaus größere Teil aller Fehler, die in programmgesteuerten Digitalrechnern auftreten, sind Datenflussfehler, deren Überwachung und Verhinderung sich deshalb Herr Widmann an dieser Stelle annimmt.

Datenflussfehler sind in höchstem Maße gefährlich, da sie insbesondere in der von Neumann-Architektur, die die völlig beliebige Interpretation jedes Bitmusters erlaubt, eine Vielzahl der technisch möglichen Reaktionen solcher Rechner auszulösen vermögen. Durch während des Entwurfs eines Programms gemachte oder zur Laufzeit auftretende Datenflussfehler kann sich auch der Kontrollfluss in unerwarteter Weise verändern, so dass Befehle in unvorhergesehener und falscher Reihenfolge, aber auch Daten, in denen keine Befehle codiert sind, als Befehle interpretiert und ausgeführt werden. Durch Fehler in der Gerätetechnik, transiente Störungen, intermittierende Fehler oder permanente Ausfälle kann es dazu kommen, dass die Bitmuster von Daten verändert werden. Sehr oft reicht eine einzige fehlerhafte Bitposition aus, um eine völlig verschiedene Aktion auszuführen.

Die von Herrn Widmann verfolgte Zielstellung ergibt sich unmittelbar aus dem unzureichenden Stand der Technik, und zwar gerätetechnische Fehlervermeidungs- und -erkennungsmöglichkeiten zu schaffen, um damit datenflussbezogene Fehler und Angriffe erkennen und die Einhaltung von Echtzeitbedingungen überwachen zu können. Die vorgestellten Ergebnisse sind in allen Bereichen der elektronischen Datenverarbeitung anwendbar und dort wegen deren geringer Zuverlässigkeit auch dringend erforderlich. Trotzdem ist das Werk aus Sicht der Automatisierungstechnik geschrieben, weil Digitalrechner trotz der Unmöglichkeit, wirklich vertrauenswürdige Sicherheitsnachweise für programmgesteuerte Systeme zu führen, mehr und mehr auch für sicherheitsgerichtete Anwendungen eingesetzt werden und dabei bewährte, oft inhärent sichere gerätetechnische Lösungen ersetzen. Weiterhin sind im Anwendungsgebiet sicherheitskritischer Echtzeitsysteme weder nicht zeitdeterministisch arbeitende Verfahren hinnehmbar, noch dürfen Fehler erst nachträglich korrigiert werden.

Bemerkenswert an Herrn Widmanns wissenschaftlich-technischen Beiträgen ist eine Reihe von Aspekten. In ganzheitlicher Betrachtung von Hardware und Software verfolgt er konzeptionell ein neuartiges Entwurfsparadigma, dass nämlich alle Deskriptoren eines Datenspeicherelementes in untrennbarer Verknüpfung mit diesem gespeichert, verarbeitet und übertragen sowie gerätetechnisch überprüfbar dargestellt werden sollen. Mit Hilfe solcher selbstbeschreibenden Daten können dann in Hardware implementierte Überprüfungen die meisten datenflussbezogenen Fehler in der Datenverarbeitung auch über Grenzen zwischen Systemkomponenten hinweg aufdecken. Er liefert theoretische Beiträge, indem er die datenflussbezogenen Fehler- und Angriffsarten analysiert und identifiziert, die Eigenschaften in sicherheitsgerichteten Echtzeitsystemen gehaltener Daten zusammenstellt und darauf aufbauend seine Datenspezifikationsarchitektur entwirft, die die Dateneigenschaften mit bisher unerreichter Aussagekraft abbildet. Und schließlich arbeitet er konstruktiv-ingenieurmäßig, indem er für jedes angegebene Verfahren geeignete Implementierungsmöglichkeiten vorschlägt und ihre jeweiligen Vor- und Nachteile diskutiert.

Der Preis, den Herr Widmann für die Sicherung des Datenflusses in Digitalrechnern bezahlt, ist erheblich erhöhter Speicherbedarf und dementsprechend größerer Übertragungsaufwand, wohingegen der Umfang zusätzlicher Hardware für die Verarbeitung der Datenkennungen gering ist. In Zeiten enormer Speicherkapazitäten ist deutlich erhöhte Sicherheit diesen Preis jedoch unbestreitbar wert.

Hagen, im August 2017 Wolfgang A. Halang

Inhaltsverzeichnis