Bundesministerium
Digitalisierung und
Wirtschaftsstandort

Christian Doppler
Forschungsgesellschaft

Sicherheit in allen Fällen

Hinter der elektronischen Steuerung moderner Anlagen stehen komplexe Systeme aus Hard- und Software, in denen Daten je nach Anforderung dezentral oder zentral verarbeitet werden. Effiziente und zuverlässige Testmethoden tragen zur Sicherheit dieser Systeme bei, beschleunigen die Entwicklungsprozesse und vereinfachen Zulassungsverfahren.

JR-Zentrum für Verifikation von eingebetteten Computersystemen

Leitung
Prof.(FH) DI Dr. Martin Horauer; Fachhochschule Technikum Wien

Laufzeit
01.05.2013 – 30.04.2018

Unternehmenspartner
Infineon Technologies Austria AG, Kapsch TrafficCom AG, LOYTEC electronics GmbH, Oregano Systems – Design & Consulting GmbH, Siemens AG Österreich; Bluetechnix R&D GmbH

Worum es geht

Ob U-Bahn, Kraftwerk, Zugsicherungssystem oder intelligentes Stromnetz: eingebettete Systeme realisieren Bremsassistenten, Fahrstände oder steuern Kraftwerksturbinen und verarbeiten Daten, die dann konsolidiert an einen zentralen Steuercontroller weitergeleitet werden. Dadurch entsteht eine sehr komplexe Landschaft aus Hard- und Software, die das effiziente Funktionieren der Anlagen ermöglicht und die für jede Anwendung individuell entwickelt werden muss. Sicherheit ist dabei ein großes Thema, denn jeder kleine Fehler hat potentiell große und oft lebensbedrohliche Konsequenzen.

Was auch immer passiert, welches Teilsystem auch ausfällt, das Gesamtsystem muss schnell in den nächsten sicheren Zustand übergehen können: Der ICE bleibt vor dem Tunnel stehen, das Kraftwerk reagiert richtig auf ein Erdbeben, das Stromnetz bleibt trotz Ausfällen stabil.

Drei Fragen an ...

DI Harald Loos
Leiter der zentralen Forschungseinheit bei Siemens Österreich

Warum ist (Grundlagen-) Forschung für Innovation so wichtig?
Ohne (Grundlagen-)Forschung gibt es keine neuen Technologien und keine neuen Geschäftsmöglichkeiten und -modelle, die die Basis für Wertschöpfung und Bildung am Standort bilden.

Was sind die großen Herausforderungen in der Zusammenarbeit mit Universitäten und Fachhochschulen?
Persönlich empfinde ich gar keine so großen Herausforderungen in der Zusammenarbeit, wenn die Finanzierung der Projekte geklärt und gesichert ist.

Was schätzen Sie besonders am Fördermodell der CDG?
Das Besondere am CDG-Modell ist, dass es eine Dreiecksbeziehung zwischen Grundlagenforschung, angewandter Forschung und Industrie ermöglicht. Die Stabilität dieser Dreiecksbeziehung basiert auf der sehr kompetenten Evaluierung UND Betreuung der einzelnen Labors und Zentren durch ExpertInnen aus Wissenschaft und Industrie. Dieses Modell ist für mich ein absolutes Vorzeigemodell für Forschungsförderung.

Die Forschungsfrage

Die eingebetteten Systeme kann man sich als kleine Computer vorstellen, die direkt mit Sensoren (Bausteinen, die Umgebungswerte messen) und Aktuatoren (z. B. Motoren, Turbinen) verbaut sind. Die dafür nötige Elektronik (Hardware) ist maßgeschneidert und direkt mit dem Gerät verbunden. Oft werden für diese Computer FPGAs (Field Programmable Gate Arrays) verwendet. In FGPAs sind eine große Menge digitaler Basiskomponenten (Prozessoren, Speicher, Gatter, etc.) vorhanden, die auf verschiedenste Arten miteinander verschaltet werden können und dadurch neue Funktionen ausführen können, also für wechselnde Anforderungen immer wieder neu konfigurierbar sind. Dies erfolgt in der Regel mit einer Hardwarebeschreibungssprache, aus der die neue Hardware synthetisiert wird.

In diesen hochkomplexen Systemen aus Hard- und Software kann nicht jede Verbindung und Schnittstelle einzeln geprüft und jede mögliche Kombination von Fehlern einzeln vorweggenommen werden. Viele Anwendungen, die damit realisiert werden, müssen jedoch unter allen Umständen sicher und fehlertolerant sein. Durch verifizierte Test- und Verifikationslösungen sollen Probleme schon im Entwurfsprozess erkannt werden – und auch bei der Zulassung einer Neuentwicklung ist der Nachweis validierter Testverfahren äußerst relevant.

Die Kooperation im JR-Zentrum

Um effiziente und umfassende Tests für eingebettete Systeme entwickeln zu können, braucht es Expertise an der Schnittstelle von Hard- und Software, an der mit eigenen Methoden und Sprachen gearbeitet wird. Siemens hat diese Expertise bei Prof. Horauer an der FH Technikum Wien und seinem Team gefunden. Testsysteme für die Sicherheit der eingebetteten Systeme sind ein klar definiertes Arbeitspaket und eignen sich daher sehr gut für die Zusammenarbeit in einem Josef Ressel Zentrum.

Ergebnisse

Durch die Zusammenarbeit im JR-Zentrum konnten einige Benchmarks dafür entwickelt werden, wie die Sicherheit eines Systems definiert werden kann. Ein relevantes Ergebnis ist FIJI, das „Fault Injection Tool“. Mit diesem im JR-Zentrum entwickelten Open Source Tool können verschiedenste Fehler in unterschiedliche FPGA basierte Lösungen eingeschleust werden. Auf diese Weise kann überprüft werden, dass eingebaute Sicherheitsmaßnahmen im System diesen Fehlern gewachsen sind. Das Tool wurde von der FH publiziert und wird von der Forschungscommunity gepflegt und aktualisiert. Siemens profitiert damit von einem Gesamtfortschritt der Branche und gleichzeitig vom Wissensvorsprung durch die Kooperation im JR-Zentrum.

Wissenschaftliche Herausforderung

Wie kann man schon bei der Entwicklung sicherheitskritischer Systeme möglichst rasch und kostengünstig alle nur erdenklichen Fehler simulieren und austesten, ob diese Systeme in jedem Fall richtig reagieren? Wie müssen adaptive Hardware und systemnahe Software konzipiert und umgesetzt werden, um möglichst robuste Systeme zu erhalten? Diese Fragen der Elektrotechnik und der Technischen Informatik sind bei eingebetteten Systemen besonders relevant. Um solche Systeme verstehen und kontrollieren zu können sowie den zahlreichen Regularien und Zertifizierungsprozessen gerecht zu werden, sind fundiertes Wissen und ein extremes Maß an Sorgfalt notwendig. Das im JR-Zentrum entwickelte Fehlertestsystem FIJI leistet einen wichtigen Beitrag für die Weiterentwicklung des Forschungsgebietes und kann systemunabhängig für alle sicherheitskritischen FPGA basierten elektronischen Systeme verwendet werden.

Mehrwert für das Unternehmen

Das im JR-Zentrum entwickelte Open Source Tool FIJI wird von Siemens im Entwicklungsprozess verwendet, um mögliche Sicherheitslücken frühzeitig zu erkennen (correct by construction).
Durch die Entwicklung eines Demonstrators für Anschauungs- und Lehrzwecke wurde diese Technologie auch für die Ausbildung aufbereitet.
Siemens profitiert von der Weiterentwicklung der Branche und gleichzeitig vom Wissensvorsprung durch die Kooperation.

Christian Doppler Forschungsgesellschaft (CDG)
Boltzmanngasse 20/1/3, 1090 Wien, Österreich, Tel.: +43 1 5042205, e-Mail: office@cdg.ac.at
CD-Labors und JR-Zentren sind Förderprogramme des Bundesministeriums für Digitalisierung und Wirtschaftsstandort.