

VirtuOS macht Software funktions- und angriffssicher

Wissenschaft und Industrie kooperieren für mehr Sicherheit im Auto

Berlin, 11. August 2010. Zuverlässigkeit im Sinne von Funktionssicherheit (Safety) und Sicherheit im Sinne von Angriffsschutz (Security) sind die zwei Kriterien, die bei der Entwicklung von automotive Software darüber entscheiden, ob ein System marktfähig ist oder nicht. „Vor dem Hintergrund, dass die elektronikbasierten Funktionen im Automobil weiter drastisch ansteigen, werden sichere und zuverlässige softwarebasierte, eingebettete Systeme zur Grundvoraussetzung für die Entwicklung moderner Kraftfahrzeuge,“ betont Frank-Peter Böhm, Chief Executive Officer der OpenSynergy GmbH. Das Softwareunternehmen ist Partner in dem Forschungsprojekt VirtuOS (Virtuelle Architekturen in Automotiven Softwaresystemen), das mit Mitteln des Europäischen Fonds für Regionalentwicklung (EFRE) und des Zukunftsfonds Berlin gefördert wird. Weitere Projektpartner sind die Technische Universität Berlin, Fachgebiet Softwaretechnik (SWT) am Institut für Softwaretechnik und Theoretische Informatik, und das Fraunhofer-Institut für Rechnerarchitektur und Softwaretechnik FIRST. Gemeinsam entwickeln die Experten aus Wissenschaft und Wirtschaft Prozesse, Werkzeuge und Methoden, damit die Softwarefunktionen im Auto diesem Qualitätsanspruch voll genügen können.

Zukünftig werden in Fahrzeugen mehrere Funktionen auf weniger, aber dafür leistungsfähigeren Steuergeräten integriert, um Kosten zu sparen und das Gewicht der Fahrzeuge zu reduzieren. Dabei können Applikationen auf einem Steuergerät laufen, die sehr unterschiedlich sind, wie z. B. Infotainment-Applikationen und Fahrerassistenzsysteme (Park-Distance Control, Spurhalteassistentz oder Verkehrsschilderkennung). Darüber hinaus können verschiedene Funktionen, die auf dem neuen Entwicklungsstandard für Software in Autos, AUTOSAR, basieren und von unterschiedlichen Zulieferern stammen, auf einer Hardware zusammengeführt werden. Voraussetzung dafür ist, dass schon die Plattform, auf der implementiert werden soll, sicherstellt, dass es zu keinen gegenseitigen Beeinflussungen der Funktionen kommt und die Funktionssicherheit gewährleistet bleibt.

PRESS RELEASE

Eine weitere Veränderung in den Fahrzeugen betrifft die Infotainment-Applikationen. Da diese sich potenziell mit anderen mobilen Endgeräten verbinden oder über Internet Informationen von einem Server abrufen, können sie ein Einfallstor für die Manipulation der gesamten Fahrzeugelektronik sein. Da elektronische Systeme in Fahrzeugen bisher geschlossen waren („Security by obscurity“), gibt es zurzeit noch keine allgemeingültigen oder gar standardisierten Technologien, um die Angriffssicherheit zu gewährleisten. Partitionierung und virtuelle Maschinen helfen hier, das System sicherer zu machen.

Um sich diesen Herausforderungen zu stellen, werden in Zukunft sicherheitskritische Funktionen auf der Basis der AUTOSAR Software-Architektur realisiert. In diesem Standard existieren schon vielversprechende Ansätze zur Integration verschiedener Softwarekomponenten. Diese müssen aber in Hinblick auf die unterschiedlichen Sicherheitsanforderungen der Einzelkomponenten neu bewertet und bei Bedarf erweitert werden. Auch vorhandene Ansätze zur Angriffssicherheit müssen unter Berücksichtigung neuer Bedrohungsszenarien, die durch die Integration verschiedener funktionssicherer Software entstehen können, überprüft werden.

Vor diesem Hintergrund sind neue Prozesse, Werkzeuge und Methoden erforderlich, die im Rahmen des Projekts VirtuOS entwickelt werden.

Die Ergebnisse der Forschungs- und Entwicklungsarbeit werden zunächst dazu beitragen, Sicherheitsanforderungen an moderne automotive Software zu definieren. Weiter werden die Projektpartner Methoden erarbeiten und Regeln formulieren, nach denen sichere Systeme entwickelt werden können. Dabei wird vor allem das Zusammenspiel der einzelnen sicheren Software-Komponenten in einer sicheren Architektur definiert.

Am Beispiel eines Demonstrators soll gezeigt werden, dass nach den Vorgaben von VirtuOS entwickelte Software den Safety- und Security-Ansprüchen genügt, die relevante Normen wie AUTOSAR, Automotive SPICE, ISO 26262 oder Common Criteria vorschreiben. Am Beispiel des automobilen Software-Frameworks COQOS von OpenSynergy soll nachgewiesen werden, dass durch die Methodik Sicherheits- und Funktionsanforderungen erfüllt werden können.

„Das besondere an diesem Projekt ist“, so Professor Stefan Jähnichen, Leiter von Fraunhofer FIRST, „dass es Wissenschaftler des Fraunhofer FIRST und der Technischen Universität Berlin mit Experten aus der Industrie und dem automotiven Umfeld von OpenSynergy zusammenführt. Die Wissenschaft steht hier in ständigem Dialog mit Automobilherstellern und Lieferanten, sodass die Forschungsergebnisse punktgenau bei der Automobilindustrie landen. Deshalb wird VirtuOS signifikant dazu beitragen, Autos sicherer zu machen.“

PRESS RELEASE

Kurzporträts der Projektpartner

Opensynergy GmbH

Das in Berlin ansässige Unternehmen OpenSynergy entwickelt und vermarktet Softwareprodukte für die Automobilindustrie. Der Software-Baukasten COQOS erlaubt das sichere Ausführen von Infotainment- oder/und AUTOSAR-Applikationen auf nur einer Hardware mittels Virtualisierungstechnologie. Durch den modularen Ansatz von COQOS kann dieses in Head-Units, Kombiinstrumenten sowie Body Control Modulen eingesetzt werden. Zusätzlich bietet OpenSynergy Consulting- und Engineering-Leistungen für Software-Entwicklung und Software-Architekturen in den Feldern Infotainment, Connectivity und AUTOSAR an.

Fraunhofer-Institut für Rechnerarchitektur und Softwaretechnik FIRST

Das Fraunhoferinstitut FIRST entwickelt „State-of-the-art“-Softwaretechnologie, um seine Kunden und Partner bei der optimalen Gestaltung von IT-basierten Prozessen zu unterstützen. Im Sinne eines Human Centric Computing sorgt FIRST dafür, dass sich Prozesse und Werkzeuge an die Bedürfnisse des Menschen anpassen und angemessen zur jeweiligen Situation, zur richtigen Zeit und am richtigen Ort zu Verfügung stehen.

FIRST sorgt für eine klare Architektur eingebetteter Systeme. Das Institut berät seine Kunden und Partner bei der Gestaltung des Softwareentwicklungsprozesses, bietet ihnen geeignete Methoden und Werkzeuge und übernimmt die Qualitätssicherung. Schwerpunkte liegen in den Bereichen Medizin, Automotive, Luft- und Raumfahrt sowie Bahn- und Automatisierungstechnik.

Technische Universität Berlin, Institut für Softwaretechnik und Theoretische Informatik (SWT)

Die Forschungsschwerpunkte des Fachgebietes Softwaretechnik liegen in den Bereichen Methoden und Werkzeuge zur Softwareentwicklung, Qualitätssicherungstechniken und -maßnahmen und Softwaretechnische Realisierung von IT-Sicherheitsanforderungen. Für die TU Berlin stehen Aspekte neuer Themen in der Ausbildung zukünftiger Software-Ingenieure auf der Basis der erforschten Methoden im Vordergrund. Neben der Grundausbildung zum Thema Informatik bietet das Institut weiterführende Lehrveranstaltungen an zu Softwaretechnik im Allgemeinen und zu weiteren speziellen Themen, wie z.B. Objektorientierung, Aspektorientierung und neue Softwareentwicklungsparadigmen, modellgetriebene Softwareentwicklung, formale Techniken zur Modellierung und Analyse softwarebasierter Systeme, Qualitätssicherung, Testen, Softwareentwicklungsprozessen und IT Sicherheit.

PRESS RELEASE

Kontaktadressen:

Ansprechpartner OpenSynergy GmbH

Frank-Peter Böhm
Chief Executive Officer

Rotherstr. 9
D-10245 Berlin
Tel.: +49 (0)30 20181835-11
Email: info@opensynergy.com

Fraunhofer-Institut für Rechnerarchitektur und Softwaretechnik FIRST

Friedrich Schön
Abteilungsleiter Eingebettete Systeme EST

Kekuléstraße 7
12489 Berlin
Tel.: +49 (0) 30 / 63 92 – 18 38
Fax: +49 (0) 30 / 63 92 – 18 05
E-Mail: friedrich.schoen@first.fraunhofer.de

Technische Universität Berlin, Fachgebiet Softwaretechnik (SWT) am Institut für Softwaretechnik und Theoretische Informatik

Prof. Dr. Stefan Jähnichen
Fakultät IV
Softwaretechnik

Ernst-Reuter-Platz 7
10587 Berlin

Tel.: +49 30 314-73174
Fax: +49 30 314-73488
E-Mail: stefan.jaehnichen@tu-berlin.de

PRESS RELEASE