Die Anforderungen an die Funktionalität autonomer Steuerungen wachsen weiter. Dadurch steigt die Systemkomplexität und damit das Risiko für die fehlerhafte Ausführung einer eigentlich korrekten Software. Zur Kompensation sind zusätzliche Investitionen in die Systemsicherheit nötig. Die SIListra Lösung verzichtet auf zusätzliche Hardware, reduziert dadurch die Komplexität und hilft Kosten zu senken, ohne auf Sicherheit verzichten zu müssen. Ziel ist die Vermarktung der SIListra Lösung ab 2012.

TECHNISCHE UNIVERSITÄT DRESDEN

Kontakt:
Technische Universität Dresden
Fakultät Informatik
Institut für Systemarchitektur
Lehrstuhl für Systems Engineering
01062 Dresden
Prof. Dr. Christof Fetzer
Michael Heuschkel
Tel.: +49-351-463-39613
Fax: +49-351-463-39710
E-Mail: michael.heuschkel@tu-dresden.de
www.silistra-systems.de

Neue Lösung für sicherheitskritische Systeme

Kostengünstige Sicherheit mit SIListra

Auch in sicherheitskritischen Systemen nimmt die Computerisierung zu. In solchen Systemen werden strenge Anforderungen an die sichere Erkennung und Behandlung von Ausführungsfehlern gestellt. Ein Ausführungsfehler tritt immer dann auf, wenn die Software zwar korrekt ist, jedoch nicht korrekt ausgeführt wird. Häufigstes Beispiel für Ausführungsfehler sind Hardwarefehler, bei denen das System zwar nicht abstürzt, aber die aktuelle Berechnung verfälscht wird. Tritt, beispielsweise bei einem ABS-System, das nicht anderweitig geschützt ist, ein solcher Hardwarefehler auf, kann es passieren, dass aufgrund der falsch berechneten Bremskraft die Bremsen gar nicht anziehen oder blockieren.

Die derzeitig am häufigsten genutzte Möglichkeit zur Erkennung von Ausführungsfehlern ist Redundanz: Es werden zwei Systeme parallel geschaltet. Die Berechnung wird jeweils auf beiden Systemen getrennt von einander durchgeführt. Am Ende werden die Ergebnisse verglichen. Damit können Ausführungsfehler erkannt werden, die genau eines der Systeme betroffen haben. Der Preis dafür ist eine hohe Komplexität.

Ziel der SIListra-Lösung ist die Verringerung der Komplexität. Erreicht wird das dadurch, dass auf ein zweites paralleles System zur Erkennung von Ausführungsfehlern verzichtet werden kann. Ein mit der SIListra-Lösung geschütztes Programm erzeugt neben seinen Ausgaben noch sogenannte „Prüfsummen“. Diese Prüfsummen hängen nur von der korrekten Ausführung des Programmes ab und nicht von den Programmeingaben. Tritt ein Ausführungsfehler auf, dann ändern sich die ausgegebenen Prüfsummen. Weiterhin erlaubt es die SIListra-Lösung, die Prüfsummen für den Fall, das kein Ausführungsfehler auftritt, vorab zu berechnen. Damit wird die Fehlererkennung einfach: Stimmen die ausgegebenen Prüfsummen mit den vorausberechneten Prüfsummen nicht überein, ist ein Ausführungsfehler aufgetreten. Diese Überprüfung kann beispielsweise von einem einfachen Überwachungschip vorgenommen werden. Ein weiterer Vorteil der SIListra-Lösung ist die Automatisierung: Der SIListra-Transformer fügt automatisch zu einem existierenden C-Programm die Berechnung der Prüfsummen hinzu und sorgt auch für die Vorausberechnung.

Das SIListra-Projekt ist ein EXIST-Forschungstranferprojekt der TU Dresden. Es wird mit Mitteln des BMWi gefördert. Kern des Projektes ist die Vermarktung und Weiterentwicklung der SIListra-Lösung. Zielmärkte sind der Automobilbau, die Automatisierungstechnik, Luft- und Raumfahrtechnik sowie Medizintechnik. Besonderes Augenmerk liegt auf dem Automobilmarkt. Hier empfiehlt ein neuer Sicherheitsstandard die der SIListra-Lösung zu Grunde liegende Technologie. Nach derzeitigem Stand beginnt die Vermarktung nach der Firmengründung Anfang 2012.

Features der SIListra-Lösung im Überblick.
(Quelle: SIListra Projekt)

eXIST Existenzgründungen aus der Wissenschaft
Gefördert durch:
Bundesministerium für Wirtschaft und Technologie
aufgrund eines Beschlusses des Deutschen Bundestages
COOL SILICON