TU Clausthal

Bachelor-, Master- und Doktorandenseminar
des Instituts für Informatik

Adaptation of Systems Theoretic Process Analysis (STPA) for SCADE-based Designs

Naghmeh Fannipour, B.Sc., TU Clausthal

Systems Theoretic Process Analysis (STPA), ist eine moderne Sicherheitsanalysemethode, die im Gegensatz zu herkömmlichen Methoden nicht auf Zuverlässigkeitstheorie basiert, sondern auf einem systemtheoretischen Modell von Unfällen. Durch die Anwendung dieses Verfahrens in einer frühen Phase des Entwurfsprozesses können Fehler und gefährliche Situationen in komplexen sicherheitskritischen Systemen kontrolliert und eliminiert werden. Das Ziel der Arbeit ist es, anhand einer Fallstudie zu bestimmen wie sich die STPA-Methode zur Prüfung von Systemmodell Designs verwenden lässt, um Gefährdungen eines Systems zu bestimmen und Sicherheitsanforderungen zu definieren. Wir wenden die STPA-Methode auf die patientenkontrollierte Analgesie Pumpe (PCA) an. Für die Automatisierung und Verwaltung der STPA Schritte verwenden wir A-STPA, ein Open Source Tool basierend auf der Eclipse Plattform. Das Tool ermöglicht es, die Sicherheitsanforderungen während des Konstruktionsprozesses eines Systems vollständig und konsistent zu erstellen. Für die Erstellung der Architektur und Verhaltensmodelle der PCA Pumpe als Block Definitions Diagramme und als interne Blockdiagramme (BDD, IBD) nutzen wir SCADE-System, ein modellbasiertes Entwicklungswerkzeug. Die Notwendigkeit präziser Modelle von Systemarchitekturen, Verhaltensweisen und Ausfallarten zwingt Sicherheitsanalysten viel Zeit aufzuwenden, um undokumentierte Informationen in Sicherheits Artefakten zu suchen. Deshalb ist eine modellbasierte Sicherheitsanalyse sinnvoll. Dazu entwickeln wir ein von Thomas vorgeschlagenes Verfahren für „multiple-controller systems“ weiter und wenden es auf die PCA Pumpe an, um potentielle Konflikte zu identifizieren. Die anschließende Überprüfung mit dem Design Verifier Tool von SCADE Suite bestätigt die Richtigkeit der entworfenen Modelle. Zusammenfassend kann gesagt werden, dass der auf STPA basierende Ansatz zur Sicherheitsnanalyse in den SCADE-gestützten Entwurfsprozess integriert werden kann. In der betrachteten Fallstudie konnte die Qualität der Analyse verbessert und in Teilen automatisiert werden.

Donnerstag, den 17.09.2015
10 Uhr s.t. in Raum 210, IfI, Am Regenbogen 15

Technische Universität Clausthal • Institut für Informatik • Julius-Albert-Straße 4 • 38678 Clausthal-Zellerfeld
Tel +49.(0)5323.72.7100 • Fax +49.(0)5323.72.7139 • http://www.in.tu-clausthal.de • info@in.tu-clausthal.de