„Safety Assessment Formal Modelling

For Critical Embedded Automotive Sensor Systems”

Jan de Meer, www.smartspacelab.de - deMeer@acm.org

Eingeladener Vortrag bei der Fachgruppe “SW Testing” des ASQF e.V. Am Borsigturm 40, Berlin-Tegel, 6. 12. 2006, 18:00 – 20:00 Uhr.

Zusammenfassung des Vortrags:
Im Vortrag werden zuerst Prinzipien und Architekturen von Aircraft-On-Board-Systemen, am Beispiel von Integrated Modular Avionics Communications (IMAC), Resource Reservation Architecture (RRA) for Passenger Cabin Domain etc. vorgestellt. Anschließend erfolgt eine Einführung in das sog. „Airborne Safety Assessment“ der Federal Aviation Administration (FAA). Intensiv wird dabei auf die Problematik einer bedeutungsvollen Hazard Analyse eingegangen. Dafür werden Lösungsvorschläge erarbeitet, die einerseits das allgemeine Vorgehensmodell (V®-Modell) an eine spezifische Avionics-Problematik anpassen und andererseits semantische Probleme, welche man beim „Assessment“, d.h. Testen von Avionics Safety Requirements u. U. hat, mit Hilfe formaler Modelle zu überwinden hilft. In Ergänzung dazu werden die Modelle von UML (für Requirements-Analyse), TTCN3 (für Formal Testing), TLA (für die Darstellung der Temporalen Logik von Aktionen), Z (für eine mathematische (Set-Theoretical) Betrachtungen von Systemen mit Zustandsautomaten) konzeptionell vorgestellt. Abschließend erfolgt eine Betrachtung, wie ein Beitrag geleistet werden kann, zu aktuellen relevanten Forschungsthemen, wie Embedded Systems, Autonome Verteilte Sensorsysteme oder die Erprobung formaler Methoden für sicherheitskritische, eingebettete Systeme.