TECHNISCHE FAKULTÄT

Department Elektrotechnik-Elektronik-Informationstechnik

# EEI-KOLLOQUIUM

## Entwicklung sicherheitskritischer Systeme

**Dr.-Ing. Werner Wolz**
ATS Applied Test Solutions GmbH, Neunkirchen

**Donnerstag, der 10.12.2009, $17^{15}$ Uhr**
Cauerstraße 7/9, Hörsaal H5

**Diskussionsleitung: Prof. Dr.-Ing. S. M. Sattler**

Sicherheitskritische Systeme sind so zu entwerfen, dass jeder Ausfall eines Bauteils, einer Software-Funktion oder eines Kommunikationskanals sofort erkannt wird. Hierzu müssen vom Entwickler Überwachungsmaßnahmen vorgesehen werden, die im Fehlerfall das System per Notbetrieb oder Notabschaltung in einen gefahrlosen Zustand bringen (Notfall-Abschaltung: failsafe; Notfall-Betrieb: fail operational). Da das System bei jedem kritischen Fehler in den sicheren Zustand wechseln muss, ist der Entwickler gezwungen, alle relevanten Fehler zu berücksichtigen. Die genaue Kenntnis möglicher Fehlerursachen ist Voraussetzung, um mittels Failure Mode Effect Analysis (FMEA) ein Bild des Systemverhaltens im Fehlerfall zu gewinnen. Der Umfang der erforderlichen Sicherheitsmaßnahmen richtet sich in der Regel nach dem Schadensausmaß und der Eintrittswahrscheinlichkeit eines Fehlers, so dass numerische Verfahren zur Ermittlung des Grenzrisikos verwendet werden. Um die Nomenklatur sicherheitskritischer Systeme verstehen zu können, werden am Beispiel der EN 61508 grundlegende Begriffe erläutert. Beispiele für Fehlerquellen in elektronischen Schaltungen werden dargestellt.