

Anforderungen an die Entwicklung und Zertifizierung sicherheitsgerichteter Betriebssysteme für Embedded Systems

Rainer Faller

TÜV Product Service GmbH, München

Betriebssysteme erlauben eine wesentlich effizientere Entwicklung von komplexer Software in Embedded Systems. Bis heute können die Entwickler sicherheitsgerichteter Computersysteme die Vorteile von käuflichen (off the shelf) Betriebssystemen und Libraries jedoch nur begrenzt nutzen. Die Hersteller von Betriebssystemen hatten bisher wenig Möglichkeit und Veranlassung die Anforderungen der Funktionalen Sicherheit zu verstehen.

Diese Situation hat sich mittlerweile vielfältig geändert. Nachdem die ersten zertifizierten Betriebssysteme für sicherheitsgerichtete Embedded Systems für Avionik-Systeme und große Automatisierungssysteme verfügbar sind, wird der Wunsch nach Anwendung von Betriebssystemen auch für andere sicherheitsgerichtete Embedded Systems in KFZ-Anwendungen, Maschinensteuerungen und in der Bahntechnik immer dominanter. Parallel dazu wurde nach langen Jahren der Diskussion unter Experten mit der internationalen Norm IEC 61508-3 und der anwendungsorientierten Norm DO178B weltweit anerkannte Grundlagen für die Entwicklung sowie Verification & Validation von sicherheitsgerichteter Software verabschiedet.

Der Vortrag wird die sicherheitstechnischen Anforderungen an Software insbesondere Betriebssysteme und deren Entwicklung sowie das Zertifizierungsverfahren beschreiben. Es werden die Betriebssystemeigenschaften erläutert auf die die Entwickler sicherheitsgerichteter Softwaresysteme aufbauen können.