

W. Hohmann: „Testen ist nicht genug“

■ Es stellt keine Besonderheit dar, in modernen Automobilen mehr als 30 Steuerungsgeräte oder ECUs vorzufinden. Software sorgt nicht nur für das Wohlbefinden der Insassen; sie bestimmt in zunehmender Masse auch die grundsätzlichen Parameter und Eigenschaften des Fahrzeugs. Ohne massiven Softwareeinsatz bliebe die Effizienz der heutigen Antriebsaggregate ebenso ein Traum wie auch die aktive und

passive Sicherheit, die selbst in kleineren Bauweisen zum Standard gehört. Wer würde noch einen Neuwagen ohne Airbag, ABS und ESP akzeptieren. Und tatsächlich scheint dieser Trend ungebrochen. Man spricht von einer Vervierfachung der Softwarekomplexität alle 18 Monate. Die Abhängigkeit von Software stellt die Qualitätssicherungsabteilungen vor neue Herausforderungen, insbesondere dann, wenn ein



Versagen der Software nicht nur ärgerlich ist, sondern Menschenleben kostet. Wir müssen uns folglich die Frage stellen: „tun wir genug, um das fehlerfreie Funktionieren sicherheitsrelevanter Software zu garantieren?“.

Der Stand der Technik im Bereich Softwarequalitätssicherung ist von systematischen Tests geprägt; langsam setzt sich auch die Messung der Testabdeckung durch. In der Luftfahrtindustrie ist allerdings seit einigen Jahren ein weiteres Werkzeug im Einsatz, dass in jüngster Zeit auch in der Automobilindustrie vermehrt Aufmerksamkeit erregt: die formale Verifikation, die eng mit modellbasierter Softwareentwicklung verknüpft ist.

Während ein Test Fehler sucht, beweist die formale Verifikation deren Abwesenheit. Zu diesem Zweck werden fatale Fehlerzustände einer ECU beschrieben; ein Vorgang, der sich aus der wohlbeherrschten FMEA-Praxis ergibt. Diese so gefundenen Fehlersituationen werden nun modelliert und mit dem zu untersuchenden Softwaremodell verbunden. Eine spezielle ‚Proofengine‘ führt nun einen Theorembeweis durch, um entweder die Unmöglichkeit des Fehlerfalles zu beweisen oder aber Situationen zu finden, in denen das fatale Systemverhalten auftreten kann. Die Toolsuite ‚SCADE Drive‘ von Esterel



WOLFRAM HOHMANN
ist Worldwide Industry
Marketing Manager Automotive
bei Esterel Technologies

Technologies ist in der Lage derartige Theorembeweise sowohl für finite Automaten als auch für datenflussgetriebene Systeme durchzuführen. Man kann erwarten, dass diese Vorgehensweise sehr bald zum Arsenal der Qualitätssicherer gehören wird. Es bleibt uns allen zu wünschen, dass im Sinne der Sicherheit auf den Strassen bei der Sicherstellung der Softwarequalität die selbe Sorgfalt zur Anwendung kommt, die das Fliegen bereits seit Jahrzehnten sicherer macht. ■

Beitrag als PDF auf www.duv24.net

more @ click

TG0409

