DSN Automotive Panel; June 24 2003, San Francisco

DSN Panel: Technological Readiness for Safety-Critical Automotive Applications

John Rushby

Computer Science Laboratory
SRI International
Menlo Park, California, USA

. . . So I'll Focus on Software

The Scale of Automotive Software

- Amount of software in an individual car is quite large
- But it's the huge numbers of variants that raises concern
  - E.g., One manufacturer releases variant powertrain control software every two days

  How to perform qualification for safety-critical applications at that rate?

Development Practices in Automotive Software

- Much of it is model-based design—they are far ahead of avionics in this regard
  - Matlab, Simulink, Stateflow
  - Statecharts

  How to qualify software developed by these means?

- And quite a lot of it is developed by suppliers
  - OK when it's a self-contained function
  - May get unintended emergent behavior when subsystems (or their plants) interact

  How to qualify integrated systems composed of such subsystems?

Safety-Critical Applications

- Need fault detection/tolerance
- So add fault monitoring, redundancy and replica management to all the above
- How to qualify such complex systems?
  - Based on no prior experience

Some Answers

- Individual software modules
  - Highly automated test case generation and evaluation
  - Again, far ahead of avionics
  - E.g., Motorola's VeriState, RSI Reactis
  - Much more is possible
- Individual controllers
  - Automated analysis for hybrid systems
  - E.g., Verification Toolbox, HybridSAL
  - This area is taking off
- Integrated and fault tolerant systems
  - Frameworks that provide partitioning and compositionality
  - E.g., TTA
  - Appreciation of higher-level services is growing

And Outstanding Challenges

- Compositional analysis and certification is the big challenge
- Establish properties of components
- And then deduce properties of the whole from these plus some algebra of composition
- RTCA SC200/Eurocae ED60 are working on certification guidelines for this kind of approach in avionics
- I suggest the automobile industry should similarly have open discussion about these and other technical issues in assurance and safety