RV-ECU: Certifiable Runtime Verification for Automobiles

Grigore Rosu
President and CEO at Runtime Verification, Inc.
Professor of Computer Science at the University of Illinois at Urbana-Champaign
Why Bother?

- NSF (Phase I) and NASA (Phase II) SBIR grants
  - Want to be sure technology is useful before developing it
- What you can get from it
  - Reduce or avoid car recalls
    - Safety requirements not violated, dynamically updatable
      - Even if car is hacked (no distinction between hacked or malfunctioning ECU)
  - Easier compliance to ISO 26262 for safety
    - Safety monitors generated automatically (provably correct)
  - Enhanced communication between OEMs and suppliers
    - Formal safety specifications will be required and shared
  - Easier, better, faster testing
    - Separation of major concerns: safety versus functionality
Modern automobiles highly computerized, including dozens of Electronic Control Units (ECUs) communicating over the CAN bus.
Recall is the most important unsolved problem in automotive. Recalls are costly ($2B+) and bad for business, and software related recalls are (increasingly) common.
More ECUs, more money on electronics, more features, more code

Source: "Automotive Embedded Software Verification and Validation Strategies", Shankar Akella, Emmeskay Advanced Technology Solutions
ISO 26262 Reshapes Safety

- ISO 26262 changing the face of automotive: first functional safety standard, in response to growing software complexity trends

- Both OEMs and suppliers scrambling for compliance
Current state-of-the-art not ideal

- Formal safety requirements not available
  - OEMs blame suppliers, suppliers blame OEMs
- ECUs developed by suppliers; code not available
- Poor CAN bus architecture
  - Any ECU can send messages to any other ECU
  - ECU sent messages cannot be stopped
Proposal

- RV-ECU: in charge of monitoring global safety
  - Provably correct (both monitoring and recovery code)
- ECUs locally monitored
  - Their critical CAN bus messages “approved” by local monitors
  - Local monitors communicate with RV-ECU
  - Local monitors achieved by instrumentation or API
All monitoring code (red) generated automatically from safety requirements; recovery code verified
- Certifiably correct (checkable proofs also generated)
- Local monitors added through instrumentation (automatically) or provided API, and can
  - Prevent ECU from sending wrong messages
  - Consult with RV-ECU to assure global safety
  - Add authentication
**Example**

**Informal requirements**

**Safe door lock**
Doors should always open only if they were unlocked in the past and not locked since then; at violation, close door.

...(hundreds of these)

**Formal requirements**

\[ \forall d : \text{always} \ (\text{Open}(d) \implies \neg \text{Lock since UnLock}) \]

@violation : \text{Close}(d)

Formalize requirements (by domain experts, using various formalisms; here an interval logic)

Automatically generated

**Monitor for each d**

// One such monitor instance
// in RV-ECU for each door d

State: one bit, b

\[ b = \text{UnLock} \ || \ \neg \text{Lock} \&\& b \]

if (Open \&\& \neg b) then send(Close)
Current RV-ECU Progress

- Prototype RV-ECU on an STM ECU board \textit{STM3210C-EVAL}
  - Working on a real car (model omitted)
    - controlling wipers, windows, doors
    - soon engine and brakes
- For the time being, local monitors intended to be as simple as just requesting acknowledgements for messages to be sent on the bus from RV-ECU
  - So RV-ECU does all monitoring, but local monitors ensure that safety violating messages are not sent
Certifiable runtime monitoring code generation

- Technology developed at the University of Illinois over a period of more than 12 years, funded with more than $6M by NSF, NASA, DARPA, NSA, Boeing
- Product for increasing safety in cars to be developed in our small company with SBIR funding from NSF, NASA, and research collaborations with automotive companies
  - Main insight: separate safety from functionality and take no chances with safety (use highest assurance known for it!)

Practical impact sought:

- Looking for collaboration, partnership, leverage, matching funding (for our NASA and NSF grants)