https://runtimeverification.com

RV-ECU: Certifiable Runtime Verification for Automobiles

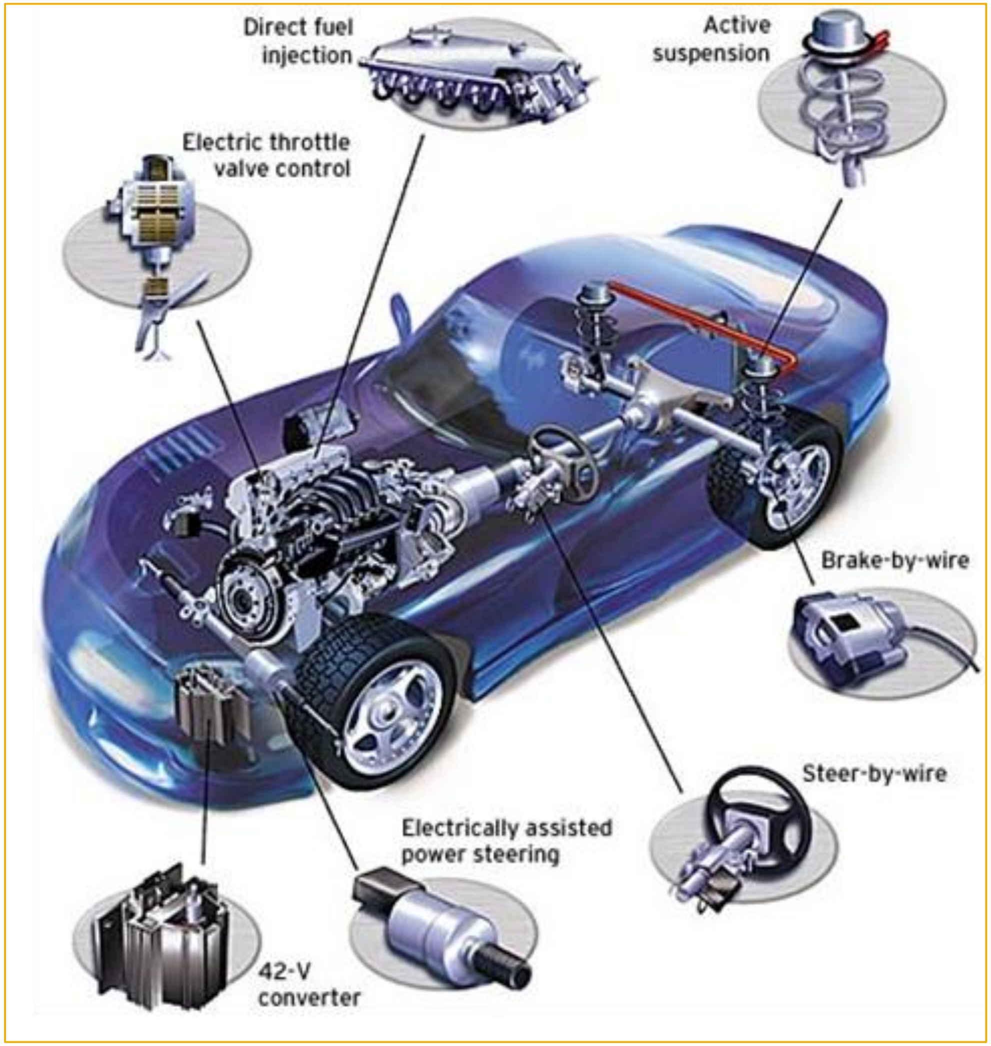
Grigore Rosu
President and CEO at Runtime Verification, Inc.
Professor of Computer Science at the University of Illinois at Urbana-Champaign

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

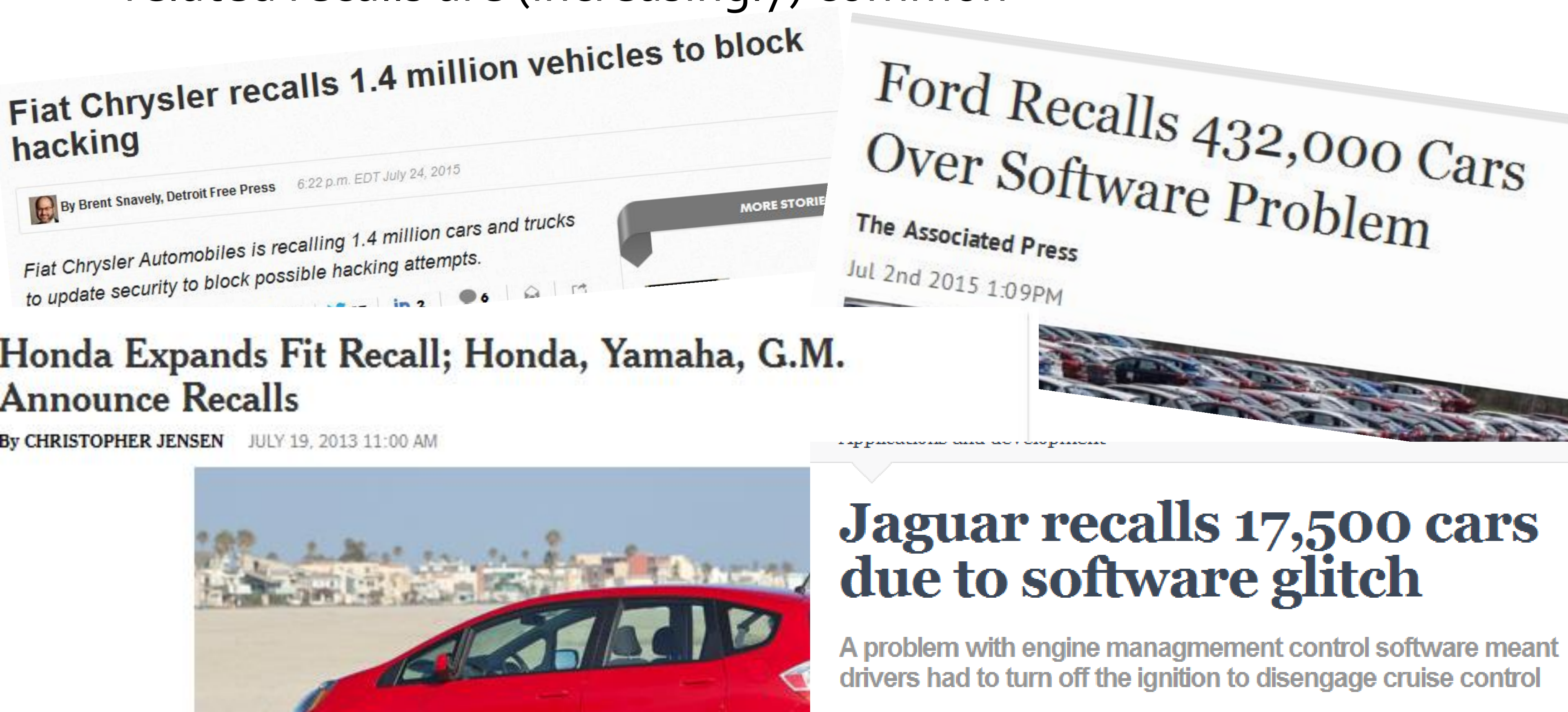
Background

Modern automobiles highly computerized, including dozens of Electronic Control Units (ECUs) communicating over the CAN bus



The Importance of Recall

- Recall is the most important unsolved problem in automotive
- Recalls are costly ($2B+) and bad for business, and software related recalls are (increasingly) common



Fiat Chrysler recalls 1.4 million vehicles to block hacking

By Brent Snavely, Detroit Free Press 6:22 p.m. EDT July 24, 2015

MORE STORIES

Fiat Chrysler Automobiles is recalling 1.4 million cars and trucks to update security to block possible hacking attempts.

Ford Recalls 432,000 Cars Over Software Problem

The Associated Press

Jul 2nd 2015 1:09PM

Honda Expands Fit Recall; Honda, Yamaha, G.M. Announce Recalls

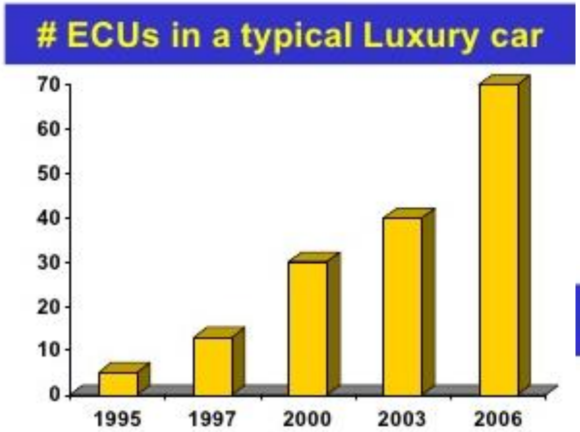
By CHRISTOPHER JENSEN JULY 19, 2013 11:00 AM

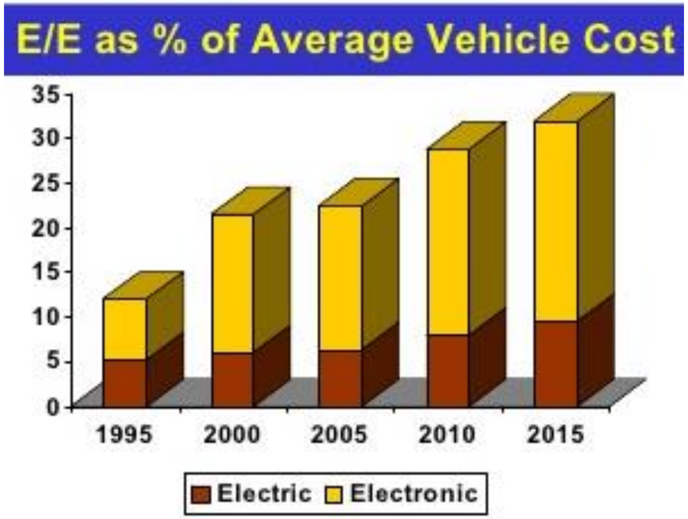
Jaguar recalls 17,500 cars due to software glitch

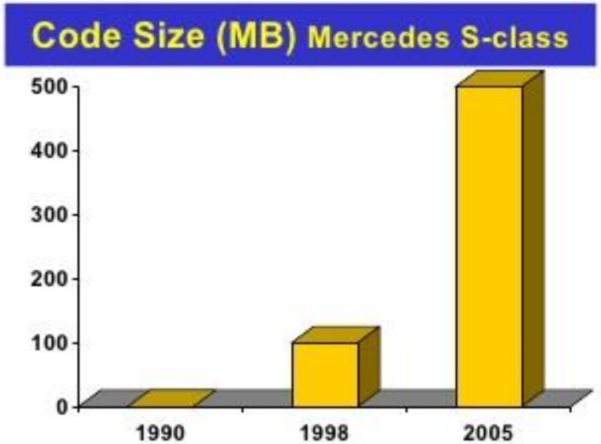
A problem with engine managmement control software meant drivers had to turn off the ignition to disengage cruise control

Software Complexity Trends

- More ECUs, more money on electronics, more features, more code



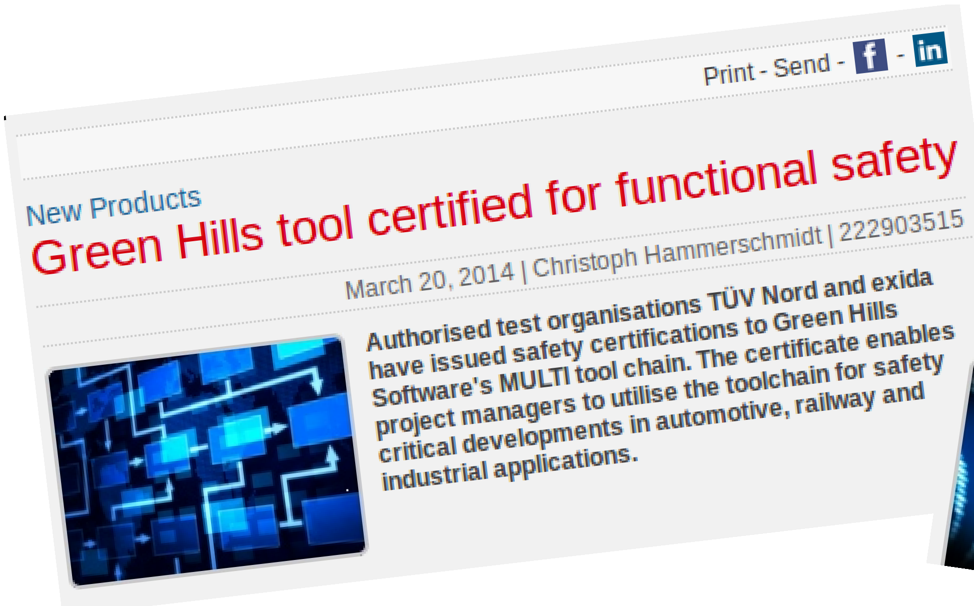




Source: "Automotive Embedded Software Verification and Validation Strategies", Shankar Akella, Emmeskay Advanced Technology Solutions

ISO 26262 Reshapes Safety

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



Print - Send - f - in

New Products

Green Hills tool certified for functional safety

March 20, 2014 | Christoph Hammerschmidt | 222903515

Authorised test organisations TÜV Nord and exida have issued safety certifications to Green Hills Software's MULTI tool chain. The certificate enables project managers to utilise the toolchain for safety critical developments in automotive, railway and industrial applications.

Home » News » Full News

New Products

Print - Send - f

Static code analysis tools gain ISO26262, IEC61508, EN50128 certification

July 04, 2014 | Graham Prophet | 222903708

GrammaTech, Inc., has announced that CodeSonar, the company's static analysis product, has been certified for use in the development of safety-critical software according to several international standards: ISO 26262, IEC 61508, and EN 50128 for automotive systems, medical devices, and railway applications, respectively.

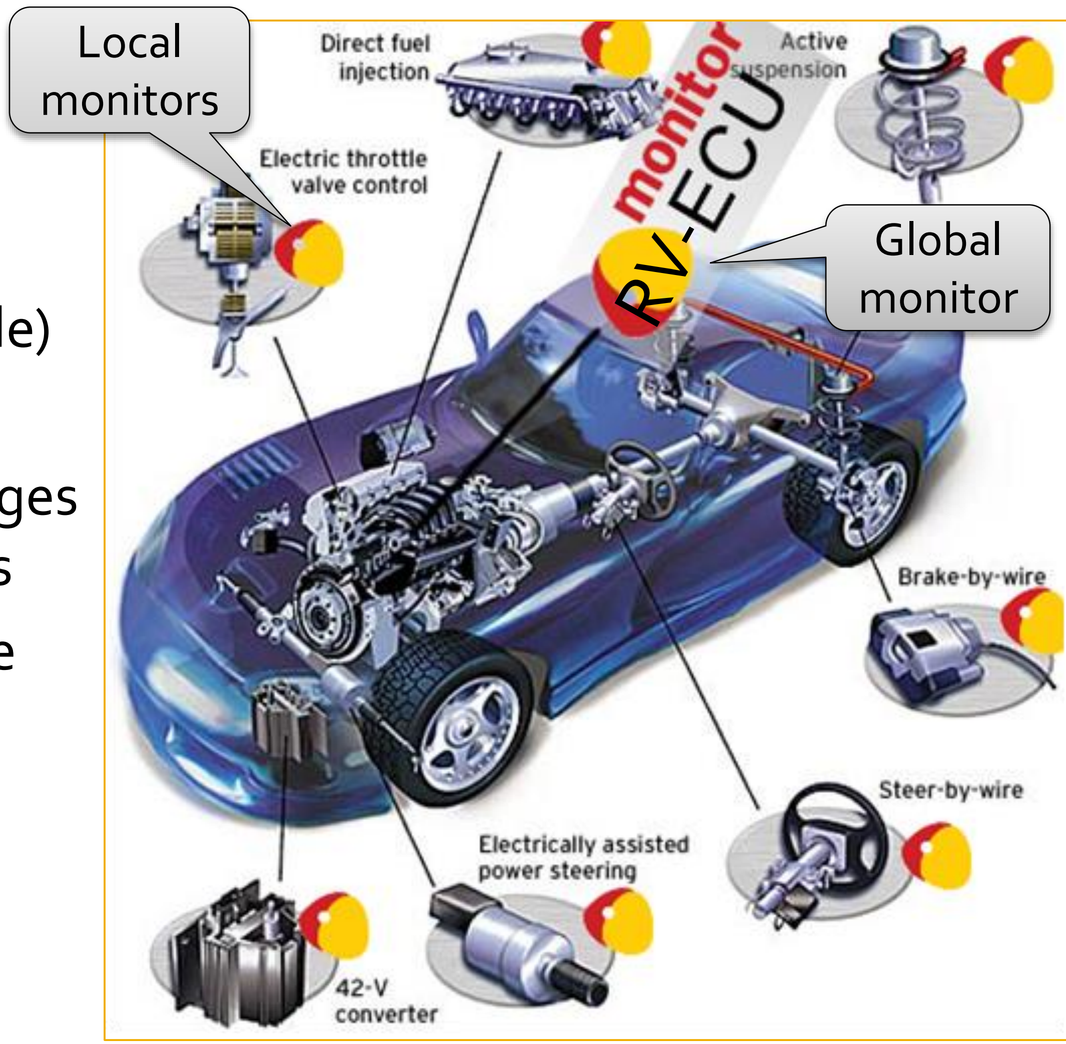
- Both OEMs and suppliers scrambling for compliance

Problem

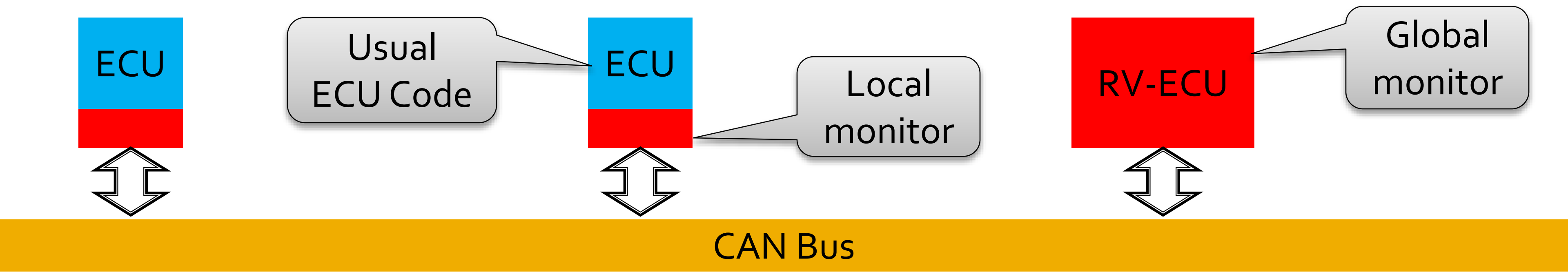
- Current state-of-the-art not ideal
  - Formal safety requirements not available
    - OEMs blame suppliers, suppliers blame OEMs
  - ECUs developed by suppliers; code not available
  - Poor CAN bus architecture
    - Any ECU can send messages to any other ECU
    - ECU sent messages cannot be stopped

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



Local vs. Global (RV-ECU) Monitor



- 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)

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

Formal requirements

∀ d : always (Open(d) implies not Lock since UnLock)
@violation : Close(d)

Automatically generated

Monitor for each d

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

State: one bit, b

b = UnLock || !Lock && b
if (Open && !b)
then send(Close)
```

Provably correct

Current RV-ECU Progress

- Prototype RV-ECU on an STM ECU board 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

Wrap Up

- 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)