Software Verification for Autonomy: A Tour of Projects and Experiences

Roderick Chapman
Altran UK
Contents

• Early autonomous systems…
• What’s changed?
• Some more recent examples…
An early Autonomous System
Properties

• “Pilot Aids” are highly critical, but…

• Small number of systems actually deployed (hundreds, not millions…)

• Pilot is at risk, but is highly trained, and getting paid to be there…

• Developers have obligation to produce convincing evidence of fitness for purpose before deployment.
  • “Ship a patch” mentality doesn’t work.
  • Software verification emphasis on static analysis.
  • Thankfully, software is running in a known, controlled and largely benign environment…
What’s changed?

• Exposure of third parties and “innocents” to autonomous systems…
What’s changed?

• Complexity…

• Staggering rise in volume and complexity of software…

• Complexity is like entropy – it’s really hard to maintain order and discipline as systems grow and evolve.

• System Integrators have an “emergent behaviour” problem… but whose problem is it???

• See “Bookout vs Toyota” for an example…
  • (Google for “bookout toyota barr” for a fun read…)
What’s changed?

- **Connectivity** of … everything?

- Risks?
  - Opportunities?
    - Both?

- Environment can be blatantly malicious…
  - “Programming Satan’s Computer” requires almost divine care and attention…
Risk?

Fiat Chrysler recalls 8,000 more Jeeps over wireless hacking

Latest recall designed to protect connected vehicles from remote manipulation, says automobile company

Source: www.theguardian.com (7th September 2015)
Risk?

BLOG: INTERNET OF THINGS
Hacking the Mitsubishi Outlander PHEV hybrid

David Lodge
05 Jun 2016

The Mitsubishi Outlander plug-in hybrid electric vehicle (PHEV) is a big-selling family hybrid SUV. It has an electric range of up to 30 miles or so plus petrol range of another 250ish miles. We noticed that the mobile app had an unusual method of connecting to the vehicle so we bought one to investigate.

Source: www.pentestpartners.com
Opportunity?

“Over-The-Air Software Updates
Over-the-air software updates add functionality, enhance performance, and improve the driving experience of Tesla vehicles. Similarly to how you receive updates to your smartphone, Model S owners receive updates to their car remotely without visiting a service center. The ability to receive these updates is free for the life of the vehicle. Software update 7.0 included Autopilot capabilities.”

Source: www.teslamotors.com
Opportunity?

DATA DRIVER

Tesla has 780 million miles of driving data, and adds another million every 10 hours

Source: www.qz.com
Observations

• Successful systems have safety and security designed in at the architectural level.
  • Redundancy.
  • Isolation of critical from non-critical.
  • Make the critical bit as small as possible.

• Recent Altran Projects:
  • NATS iFACTS – “Driver Assistance” for UK Air Traffic Controllers…
  • VueForge for ADAS
Observations

• Example: QF32 (Airbus A380) *still worked* following an uncontained engine failure and substantial damage.

Source: www.atsb.gov.au
NATS iFACTS
ADAS and autonomous driving require fusion of all sensor data to ensure a consistent view on the traffic situation at all times.

Sensor fusion is challenging to verify: huge amount of data to record, to process, to test, to store, to manage.

Users expect cost savings from changing verification methodology (single vs. system).

Currently no COTS solution exists to address the whole process and to manage the amount of data.
Questions…

• How “good” do autonomous systems have to be?
  • “Perfect”?  
  • “Better than nothing”? (e.g. dialysis machine…)  
  • “Better than human system that it replaces”?

• How do you define “Good enough” anyway?

• How do you know when you can ship the product?
A Final Challenge…

• Imagine you’re building a great new connected autonomous system that will ship by the million and be a great success…

• Should you…
  • Ship the software with a warranty?
  • Get insurance?
  • Both…
  • Neither…

• Please come back next year and tell us what happened…
Altran UK Limited
22 St Lawrence Street
SouthGate
Bath BA1 1AN

Tel: +44 1225 466991
Fax: +44 1225 469006
Website: intelligent-systems.altran.com

Email: rod.chapman@altran.com