Certification for autonomous vehicles

James Martin
jamesml@cs.unc.edu

Micaiah Chrisholm
micaiah@cs.unc.edu

Namhoon Kim
namhoonk@cs.unc.edu

Dhruv Mittal
mittald@live.unc.edu

Introduction

Why certify?

- Maintain safety / protect consumers
- Create industry standards

What do current vehicle certifications look like?

- Federal Motor Vehicle Safety Standards
  - Fairly robust document detailing everything from brake hoses to rearview mirrors
- Testing procedures against standards

Introduction

Using avionics as a model

- What we can learn from the avionics industry

Testing and verification

- KeYmaera verification tool
- Methods seen in industry

Introduction

Certification and verification in software

- Current standards that exist
- How they are enforced

Legislation and standards for software

- IEC 61508 - Functional safety
- ISO 26262 - Road vehicles: Functinal safety

NHTSA

National Highway Traffic Safety Administration

- Established in 1970 due to public outcry over vehicle safety
- Responsible for:
  1. maintaining/developing standards
  2. enforcing standards

- First standard was FMVSS 209 on Seatbelt Assemblies

NHTSA and automated vehicles

Issued a statement with:

1. Recognition of benefits of these technologies
2. Acknowledging own role in the future of these technologies
3. Recommended principles for States

Most thorough response to new technologies

NHTSA and automated vehicles

Level 0 - No automation

Level 1 - Function-specific automation (i.e. Electronic Stability Control)

Level 2 - Combined function automation

Level 3 - Limited self-driving automation

Level 4 - Full self-driving automation

Recommendation from the NHTSA

1. Ensure drivers know how to operate a self-driving vehicle safely
2. Ensure that on-road testing minimizes risk to others
3. Make sure testing environment is suitable to technology
4. Establish reporting requirements to monitor performance while testing

Recommendations from the NHTSA

1. Ensure that transition from autonomy to driver is “safe, simple, and timely”
2. Be able to detect failures
3. No self-driving technologies should disable any federally regulated safety features
4. Record information about the self-driving technology in the event of a crash

FMVSS

Federal Motor Vehicle Safety Standards and Regulations

Broken into three main sections:

1. Crash avoidance (100-series)
2. Crashworthiness (200-series)
3. Post-crash survivability (300-series)

FMVSS

No standard in the FMVSS covers software found in vehicles.

Standard most important to us:

- 101: Controls and Displays. All controls must be within reach of a belted driver
  - May have implications for autonomous vehicles

FMVSS

Large hole in standards covering issues for autonomous vehicles

Such as issues we've discussed:

- Pedestrian detection
- Collision avoidance

Testing procedures

NHTSA website has 5 pages of test procedures.

Highlights

- Rigid Pole and Side Impact Protection
  - 214P/214D
- Occupation Crash Protection
  - 208-14/208-13
  - This is typically what people think of when they think of vehicle safety testing

NHTSA Crash Safety Test

Safety Ratings

NHTSA will issue a safety rating out of 5-stars based on their testing

Insurance Institute for Highway Safety (IIHS) also issues ratings for vehicle safety out of 5-stars

Quality control during manufacturing

- Vendors must subject components to quality assurance before sending to manufacturer
- Discretion of individual manufacturers

Example:

- Toyota plant in Georgetown, KY randomly selects 150-175 cars a day to be sent to a test track for thorough inspection

Analogous standards abroad

Canada: CMVSS

Australia: ADR, Australian Design Rules

Korea: KMVSS

Japan: Test Requirements and Instructions for Automobile Standards

India: AIS, Automotive Industry Standards

International: ECE, United Nations Economic Commision for Europe

Data collection

Issues with privacy

- Constant video being captured, possibly audio
- Telemetry data collection
  - GPS
  - Fuel economy
  - Speed
- Personally identifiable information (PII)

Current laws in place

US legislation a “patchwork quilt”

- No dedicated protection laws
- Differ by industry
- Developed on both state and federal levels

Examples:

- Electronic Communications Privacy Act
- Driver’s Privacy Protection Act

Who enforces these laws?

1. Department of Justice
2. Department of Health and Human Services
3. Federal Trade Commission

Currently the FTC would have enforcement authority

- For entities not subject to industry specific regulation

Driver's Privacy Protection Act

Information held by the Departments of Motor Vehicles can only be released to "authorized recipients" such as:

1. Government agencies
2. Employers
3. Insurance companies
4. Licensed private investigation agencies

Driver's Privacy Protection Act

Should in-car data be covered by this law?

- DMV probably not equipped to handle the bulk data
- Having a list of "authorized recipients" would be a start

Industry has been calling for additional government regulation

CES 2014

At CES 2014, Jim Farley, Ford's Executive VP of Global Marketing:

"We know everyone who breaks the law; we know when you're doing it. We have GPS in your car, so we know what you're doing"

"By the way, we don't supply that data to anyone."

Ford’s response to Farley’s comment

Data only used for “customer-relationship management purposes” - Mark Fields, COO

Global Automakers Association issued a FAQ on Consumer Privacy Protection Principles

Global Automakers FAQ

Highlights:

1. PII is collected
2. Customers have to opt-in to share data (signatures, verbal agreement, etc.)
3. Customers can review *some* data collected
4. Cannot turn off data collection
5. 19 automakers have agreed to the principles starting in 2016 (2017 model year)

Recommendations

1. New section in FMVSS standards dedicated to autonomous functionality
2. Creation of auto industry specific data protection laws that are enforced by a specific government agency like the NHTSA
3. Testing auto specific software for security and safety flaws

Sources

http://www.toyotageorgetown.com/qualdex.asp

http://www.bloomberg.com/news/articles/2014-01-14/ford-ceo-says-auto-industry-needs-privacy-boundaries-set-by-law

http://www.globalautomakers.org/sites/default/files/Global%20Automakers%20Privacy%20FAQs.pdf

http://www.nhtsa.gov/Laws-Regs

https://www.law.cornell.edu/uscode/text/18/2721