Automated Vehicles: Risks and Regulatory Challenges

Steven E. Shladover, Sc.D.
University of California PATH Program

ITS Australia Summit, Brisbane
September 28, 2017
Outline

• Automated Driving Systems (ADS) defined in SAE J3016
• How safe is safe enough?
• Regulatory principles
• Federal approach in U.S.
• California approach
• Risks – why this is so difficult
SAE J3016: Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles

- available free at: [http://standards.sae.org/j3016_201609/](http://standards.sae.org/j3016_201609/)
- Automated Driving Systems (ADS) can perform the complete “dynamic driving task” without needing continuous human supervision:
  - Level 3: “fallback-ready user” must be ready to intervene quickly when requested, in situations the ADS can’t handle
  - Level 4: automation limited to use within a defined Operational Design Domain (ODD)
  - Level 5: automation usable under all conditions in which humans can drive
Operational Design Domain (ODD)

The specific conditions under which a given driving automation system is designed to function, including:

- Roadway type
- Traffic conditions and speed range
- Geographic location (boundaries)
- Weather and lighting conditions
- Availability of necessary supporting infrastructure features
- Condition of pavement markings and signage
- (and potentially more...)

PATH
Safety Goal: How Safe?

- Perfection is unattainable
- Human drivers are already remarkably safe based on U.S. statistics:
  - 3.4 M vehicle hours between fatal crashes (390 years of non-stop 24/7 driving)
  - 61,400 vehicle hours between injury crashes (7 years of non-stop 24/7 driving)
- Australian statistics somewhat better than this
- How much safer do ADS need to be for acceptance by society? 2X? 5X? 10X?
- How could a developer prove that their system has reached the target safety level?
Regulatory Challenges

• Automation software breaks the traditional boundary between vehicle equipment and driving behavior
  – Traditional federal and state divisions of responsibilities
• Need to balance protecting public safety and encouraging innovation in vehicle technology
• Absence of technical standards or test procedures → too difficult to define these
• Safety-critical events are rare, strange and not susceptible to codification
Fundamental Considerations in Defining Automation Regulations

- Balancing need to protect public safety (due diligence) with desire to encourage technological innovation
- Trying to ensure that general public really understands limitations of their vehicles
- Detecting unsafe systems as early as possible
- Managing cultural differences between automotive and information technology industries
- Self-certification vs. third-party certification
- Determining where to draw the go/no-go line
NHTSA 2016 Policy Guidance

- Released for public comment and review Sept. 20, 2016
  - 112-page report with 123 footnotes
- Broad statement of balanced approach in four areas:
  - Vehicle performance guidance
  - Model state policy
  - NHTSA’s current regulatory tools
  - Modern (future) regulatory tools
- Applies to “highly automated vehicles”, HAV (SAE Levels 3-5)
- Extensive outreach process
Automated Driving Systems 2.0: A Vision for Safety

- Released Sept. 12, 2017
- 36 pages, 35 footnotes
- Voluntary guidance only
- Tells states to back off
- No enforcement mechanisms
- “Voluntary Safety Self-Assessment”
- “Technical Assistance to States” – legislative and administrative recommendations
- Appears to assume all industry participants are totally competent and conscientious
NHTSA “Safety Self-Assessment”
Elements Retained from 2016 to 2017

- Data recording
- System safety
- Vehicle cybersecurity
- Human-machine interface
- Crashworthiness
- Consumer education and training
- Federal, state and local law
- Post-crash behavior
- Operational design domain
- Object and event detection and response
- Fallback (minimal risk condition)
- Validation methods
NHTSA Changes from 2016 to 2017

Deleted elements:
- Data sharing
- Privacy
- Registration and certification
- Ethical considerations

Added:
“NHTSA strongly encourages states not to codify this Voluntary Guidance (that is, incorporate it into State statutes) as a legal requirement for any phases of development, testing, or deployment of ADSs”
NHTSA 2017 “Technical Assistance to States”

• Legislative:
  – Technology neutrality
  – Licensing and registration
  – Reporting for public safety officials
  – Review regulations that could be barriers

• Administrative
  – Choose a lead agency per state
  – Create an ADS technology committee
  – Address unnecessary barriers to deployment
  – Application for testing
  – Issuing testing permits
  – Assign liability
What now at the U.S. national level?

- No FMVSS likely in this administration
- No federal restrictions to limit bad behaviors by irresponsible or incompetent developers until after people have been killed or injured
- Need a non-government mechanism to pressure industry to behave responsibly
  - Leadership from well-respected independent institutions (National Academies, etc.)
  - Independent experts’ review and vetting of “safety self-assessments” while protecting IP
  - Shaming the bad actors
California Background

- SB 1298 amended Vehicle Code in July 2012
- Rules apply to SAE Level 3+ driving automation
- Testing regulations effective Sept. 2014
  - Permission for specific vehicles, drivers
  - Strict test driver requirements
  - Describe prior closed-course testing
  - No heavy vehicle, motorcycle testing now
  - Report certain driver interventions, but all crashes
- Permits for 42 manufacturers, 269 vehicles, 975 test drivers
  - (July 2016: 14 mfgrs., 111 vehicles, 428 drivers)
Extensions to CA Testing Regulations

- CA DMV released draft for formal review and public comment on March 10, 2017 (prior to NHTSA update):
  - Clarified identification of covered vehicles (SAE L3-5) and importance of Operational Design Domain (ODD)
  - Extended validity of permit to 2 years
  - No paying passengers during testing
  - More specific requirements on disengagement reports
  - New set of regulations for testing without driver onboard
Testing without an onboard driver

For vehicles designed for “driverless” operation:

- Manufacturer assumes liability for collisions
- Notify all local authorities within ODD
- Wireless communication with properly licensed remote operator to monitor status
- FMVSS compliance or NHTSA exemption
- Law enforcement interaction plan, with multiple specific requirements
- Submit copy of NHTSA Safety Assessment Letter
- Disclose any personally identifiable data collection to passengers
California Deployment Regulation Principles and Background

- Public safety now depends on the technology, not on the trained test drivers
- Treat all developers equally
- Clear and unambiguous requirements representing real transportation needs to avoid temptations to “game the test”
- Transparency of results to gain public confidence, without jeopardizing developers’ intellectual property
- *March 10, 2017 draft for public comment, prior to NHTSA update*
CA Deployment Permit Proposal (1/2)

- Define ODD and certify that “autonomous mode” cannot operate outside ODD
- EDR to record sensor data for 30 s before and 5 s after any crash
- Comply with FMVSS or have NHTSA exemption
- Comply with CA Vehicle Code, including updates at least annually
- Self-diagnostics against cyber-attacks
- Consumer education plan – ODD restrictions, with submittal of language used, and access for law enforcement, EMR and used-vehicle purchasers
- How it will come to a complete stop after a failure
CA Deployment Permit Proposal (2/2)

• Show test data proving performance within ODD:
  – VMT within each ODD inside and outside CA
  – How system was validated
  – Safety-critical incidents encountered in testing
  – Description of collisions and how they will be avoided in the future

• Submit copy of NHTSA “Safety Assessment Letter”

• If no driver is required, add:
  – Communication with remote operator
  – Display owner/operator info. for law enforcement
  – FMVSS compliance or NHTSA exemption
Additional CA Draft Provisions

• File amendment “prior to implementing a material change in the capabilities or performance…”
• Report safety-related defects
• Suspend permit based on failures to disclose, misrepresentations, recalls, safety concerns
  – Manufacturer must notify vehicle owners
• Disclose to owner any collection of information not necessary for safe operation
  – Owner opt-in to collection of identifiable data
• Manufacturer liable for crashes in “autonomous mode”, but driver responsible otherwise
• Truth in advertising about “autonomous” capabilities
Traffic Safety Challenges for High and Full Automation (SAE Levels 4, 5)

- Extreme external conditions arising without advance warning (failure of another vehicle, dropped load, lightning,...)
- NEW CRASHES caused by automation:
  - Strange circumstances the system designer could not anticipate
  - Software bugs not exercised in testing
  - Undiagnosed faults in the vehicle
  - Catastrophic failures of vital vehicle systems (loss of electrical power...)
- Driver not available to act as the fall-back
Why this is a super-hard problem

• Software intensive system (no technology available to verify or validate its safety under its full range of operating conditions)
• Electro-mechanical elements don’t benefit from Moore’s Law cost reductions
• Cannot afford to rely on extensive hardware redundancy for protection from failures
• Harsh and unpredictable hazard environment
• Non-professional vehicle owners and operators cannot ensure proper maintenance and training
Dynamic External Hazards (Examples)

• Behaviors of other vehicles:
  – Entering from blind driveways
  – Violating traffic laws
  – Moving erratically following crashes with other vehicles
  – Law enforcement (sirens and flashing lights)
• Pedestrians (especially small children) and bicyclists
• Officers directing traffic
• Animals (domestic pets to large wildlife)
• Opening doors of parked cars
• Unsecured loads falling off trucks
• Debris from previous crashes
• Landslide debris (sand, gravel, rocks)
• Any object that can disrupt vehicle motion
Environmental Conditions (Examples)

- Electromagnetic pulse disturbance (lightning)
- Precipitation (rain, snow, mist, sleet, hail, fog,...)
- Other atmospheric obscurants (dust, smoke,...)
- Night conditions without illumination
- Low sun angle glare
- Glare off snowy and icy surfaces
- Reduced road surface friction (rain, snow, ice, oil...)
- High and gusty winds
- Road surface markings and signs obscured by snow/ice
- Road surface markings obscured by reflections off wet surfaces
- Signs obscured by foliage or displaced by vehicle crashes
Internal Faults – Functional Safety Challenges

Solvable with a lot of hard work:
• Mechanical and electrical component failures
• Computer hardware and operating system glitches
• Sensor condition or calibration faults

Requiring more fundamental breakthroughs:
• System design errors
• System specification errors
• Software coding bugs
Safety Challenges for Full Automation

• Must be “significantly” safer than today’s driving baseline (2X? 5X? 10X?)
  – Fatal crash MTBF > 3.4 million vehicle hours
  – Injury crash MTBF > 61,400 vehicle hours
• Cannot prove safety of software for safety-critical applications
• Complexity – cannot test all possible combinations of input conditions and their timing
• How many hours of testing would be needed to demonstrate safety better than today?
• How many hours of continuous, unassisted automated driving have been achieved in real traffic under diverse conditions?
Evidence from Recent Public Testing

- California DMV testing rules require annual reports on safety-related disengagements
- Waymo (Google) far ahead of others:
  - All disengagements reconstructed in detailed simulations (what if allowed to continue?)
  - Simulations showed ~8000 km between critical events in 2016 (2.5 factor improvement over 2015)
- Human drivers in U.S. traffic safety statistics:
  - ~ 3 million km per injury crash
  - 150 million km per fatal crash
Needed Breakthroughs

- Software safety design, verification and validation methods to overcome limitations of:
  - Formal methods
  - Brute-force testing
  - Non-deterministic learning systems
- Robust threat assessment sensing and signal processing to reach zero false negatives and near-zero false positives
- Robust control system fault detection, identification and accommodation, within 0.1 s response
- Ethical decision making for robotics
- Cyber-security protection
Threat Assessment Challenge

• Detect and respond to every hazard, including those that are hard to see:
  – Negative obstacles (deep potholes)
  – Inconspicuous threats (brick in tire track)

• Ignore conspicuous but innocuous targets
  – Metallized balloon
  – Paper bag

• Serious challenges to sensor technologies

• How to set detection threshold sensitivity to reach zero false negatives (missed hazards) and near-zero false positives?
# Much Harder than Commercial Aircraft Autopilot Automation

<table>
<thead>
<tr>
<th>Measure of Difficulty – Orders of Magnitude</th>
<th>Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of targets each vehicle needs to track (~10)</td>
<td>1</td>
</tr>
<tr>
<td>Number of vehicles the region needs to monitor (~10&lt;sup&gt;6&lt;/sup&gt;)</td>
<td>4</td>
</tr>
<tr>
<td>Accuracy of range measurements needed to each target (~10 cm)</td>
<td>3</td>
</tr>
<tr>
<td>Accuracy of speed difference measurements needed to each target (~1 m/s)</td>
<td>1</td>
</tr>
<tr>
<td>Time available to respond to an emergency while cruising (~0.1 s)</td>
<td>2</td>
</tr>
<tr>
<td>Acceptable cost to equip each vehicle (~$3000)</td>
<td>3</td>
</tr>
<tr>
<td>Annual production volume of automation systems (~10&lt;sup&gt;6&lt;/sup&gt;)</td>
<td>-4</td>
</tr>
<tr>
<td><strong>Sum total of orders of magnitude</strong></td>
<td>10</td>
</tr>
</tbody>
</table>
What to do now?

- Focus on connected vehicle capabilities (I2V, V2I, V2V) to provide technology for cooperation
- For earliest public benefits from automation, focus on transit and trucking applications in protected rights of way
  - Professional drivers and maintenance
  - Direct economic benefits
- Capitalize on managed lanes to concentrate equipped vehicles together
- Develop enabling technologies for Level 5 automation (software verification and safety, real-time fault identification and management, hazard detection sensing,...)