Safety Challenges for Automated Driving Systems (ADS)

Steven E. Shladover, Sc.D.
California PATH Program (Retired)
Institute of Transportation Studies
University of California, Berkeley

Texas A&M Transportation Technology Conference
May 1, 2019
How safe will CAV be?

- It depends on the level of automation:
  - Level 1 (only speed control OR steering control) – driver is still driving, so the system *augments* driver vigilance
  - Level 2 (speed + steering control, but requiring driver supervision) – depends on driver’s level of engagement in driving
  - Level 3+ (Automated Driving Systems) – depends on how robust the technology is, so NOBODY KNOWS

- *Claims of dramatic safety improvements are completely unsupportable*
ADS Safety Cannot be Taken on Faith

• Humans are creating the automation systems, so they will be imperfect
  – Automation replaces human driving errors with human engineering/software development errors

• The companies developing the systems will differ widely in technical and managerial skills, safety culture and ethical standards

• Even the best will be subject to strong pressure to release systems before they’re ready:
  – Ego-Maniac CEO promised it by this month
  – Investors will pull the plug if we don’t release it now
  – Our competitors released their system already
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)
- 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, ...)
- Strong 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
Environment Perception (Sensing)
Challenges for Automated Driving Systems

- **Recognizing** all relevant objects within vehicle path
- **Predicting** future motions of all mobile objects (vehicles, pedestrians, bicyclists, animals…)
- Must *at least* match perception capabilities of experienced human drivers under all environmental conditions within Operational Design Domain (ODD)
- No single “silver bullet” sensor; will need to fuse:
  - Radar AND
  - Lidar AND
  - High-precision digital mapping/localization AND
  - Video imaging AND
  - Wireless communication
Threat Assessment

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

• Ignore conspicuous but harmless targets
  – Metallized balloon
  – Empty paper bag

• Serious challenges to sensor technologies

• How to set threshold sensitivity to reach zero false negatives (missed hazards) and near-zero false positives?
Safety – Functionality Trade-offs

• False positive vs. false negative hazard detection

• Safety requires virtually zero false negatives (always detect real hazards)
  – Limit speed to improve sensor discrimination capability with more samples
  – When in doubt, stop the vehicle

• Functionality requires very low false positives
  – Avoid spurious emergency braking
  – Maintain high enough speed to provide useful transportation service
The Safety Baseline Challenge

• Current U.S. traffic safety sets a very high bar:
  – 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)

• This will improve with growing use of collision warning and avoidance systems

• How do these numbers compare with your laptop, tablet or “smart” phone?

• How much testing would you have to do to show that an automated system is equally safe?
  – RAND study – multiple factors longer
Evidence from Recent AV Testing

- California DMV testing rules require annual reports on safety-related disengagements.
- Waymo (ex-Google) well ahead of the others:
  - But their reports are based on reconstructions of disengagement cases in simulations (critical event if it had continued after disengagement).
  - Estimated ~11,000 miles between critical events based on 2018 data.
- Human drivers in U.S. traffic safety statistics:
  - ~2 million miles per injury crash (maybe ~300,000 miles for property damage crash).
  - 100 million miles per fatal crash.
Traffic Safety Challenges for Highly Automated Driving

• 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...)

• No driver available to provide fallback
How to Ensure It’s “Safe Enough”?

- What combinations of input conditions to assess?

- What combination of closed track testing, public road testing, and simulation?
  - How much of each is needed?
  - How to validate simulations?

- What time and cost?
  - Aerospace experience shows software V&V representing 50% of new aircraft development cost (for much simpler software, with continuous expert oversight)
What certification test suite?

• Beware analogy to driver licensing exam – a road network full of newly-licensed drivers would be much less safe than today, and computers lack human learning ability and adaptability

• Safety-critical events generally happen when multiple things go wrong around the same time, not under simple conditions

• How to design the suite of test cases to identify the ability of an AV system to manage these complex circumstances?
  - Virtually infinite combinations of rare events
  - Avoid developers “gaming” the system by just designing to the test
Learning Systems to the Rescue?

- 90% success recognizing objects in a fairly complex environment is considered very good
- What’s needed to match average human driving?
  - Moderate density highway driving – estimate 1 object per second (3600 per hour)
    - 3.4 M hours = 12.2 x 10^9 objects ≈ 10^{10}
    - Missing one for a fatal crash → 99.99999999% success rate
  - High density urban driving – estimate 10 objects per second
    - Missing one for a fatal crash → 99.999999999% success rate
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 methodological breakthroughs:
• System design errors
• System specification errors
• Software coding bugs
Needed Breakthroughs

• Software safety design, verification and validation methods to overcome problems with:
  – Formal methods (complexity)
  – Brute-force testing (cost and time)
  – Learning systems (opaque, non-deterministic)

• 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 design processes for Cyber-Physical Sys.

• Cyber-security protections
### Measure of Difficulty – Orders of Magnitude

<table>
<thead>
<tr>
<th>Measure</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 (~10⁶)</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 (~10⁶)</td>
<td>-4</td>
</tr>
<tr>
<td>Sum total of orders of magnitude</td>
<td>10</td>
</tr>
</tbody>
</table>
Making automated driving as safe as humans is like climbing Mt. Everest…

<table>
<thead>
<tr>
<th>Automated Driving System</th>
<th>Climbing Mt. Everest</th>
</tr>
</thead>
<tbody>
<tr>
<td>My system handles <strong>90%</strong> of the scenarios it will encounter on the road</td>
<td>I flew from San Francisco to New Delhi, covering 90% of the distance to Everest</td>
</tr>
<tr>
<td>My system handles <strong>99%</strong> of the scenarios it will encounter on the road</td>
<td>I flew from New Delhi to Katmandu, so I’m 99% of the way to Everest</td>
</tr>
<tr>
<td>My system handles <strong>99.9%</strong> of the scenarios it will encounter on the road</td>
<td>I flew to the airport closest to Everest Base Camp</td>
</tr>
<tr>
<td>My system handles <strong>99.99%</strong> of the scenarios it will encounter on the road</td>
<td>I hiked up to Everest Base Camp</td>
</tr>
</tbody>
</table>

**And now comes the really hard work!**

<table>
<thead>
<tr>
<th>Automated Driving System</th>
<th>Climbing Mt. Everest</th>
</tr>
</thead>
<tbody>
<tr>
<td>My system handles <strong>99.99999999%</strong> of the scenarios it will encounter, so it’s comparable to an average skilled driver</td>
<td>I made it to the summit of Mt. Everest</td>
</tr>
</tbody>
</table>
ADS Safety Regulations are Needed

- Protect public safety from immature systems
- Protect industry good actors from bad actors
  - Souring public attitudes by killing innocents
  - Pressures to release products prematurely
- Avoid regulatory “race to the bottom” preempting states from seeking better safety
- Recognize that complexity of automated driving systems far exceeds that of prior vehicle systems
  - Traditional FMVSS approach of performance requirement with test procedure does not scale to this domain
Are Regulations Impeding Progress?

• California has strictest regulations on AV testing in the U.S., but we have (as of 4/2019):
  – 62 companies with testing licenses for 688 test vehicles and 2650 test drivers
• Regulations need to balance protecting the public from unsafe, immature systems with encouraging safe innovations
• When AV developers can convincingly prove safety of their systems, regulators will eagerly approve them because of public demand
  – But proving safety is really hard!
How to Reconcile My Caution With the Optimism You See in the Media?

- Public is eager to gain the benefits of automation
- Media are eager to satisfy public hunger, and science fiction is sexier than science fact
- Industry is in “fear of missing out” (FOMO) on the “next big thing”
- Each company seeks image of technology leader, so they exaggerate their claims
  - Journalists lack technical insight to ask the right probing questions
- Companies are manipulating media reports
- CEO and marketing claims don’t match the reality of what the engineers are actually developing
How to maximize progress now?

• Focus on implementing systems that are technically feasible now to enhance performance and gain public confidence:
  – Level 1, 2 driving automation
  – DSRC communications (V2V, I2V)

• Develop more highly automated systems within well-constrained ODDs to ensure safety, then gradually relax ODD constraints as technology advances

• Work toward the fundamental breakthroughs needed for high automation under general (relatively unconstrained) conditions