Automated Vehicle Safety Update for 2021

February 2, 2021
Overview

- Where is the industry in general as of early 2021?

- Beyond the SAE Levels
  - Role of human vs. technology

- Industry trends for 2021
  - Role of standards
  - Technical challenges
  - Organizational challenges
Low Speed Shuttles

- Low speed shuttles
  - Up to 15 passengers
  - Fixed route at perhaps 5-10 mph
  - Demonstrations in cities worldwide

- Safety approach
  - Slow speed limits kinetic energy
  - Often a non-driver safety conductor

- Example Mishaps
  - Shuttle hit by backing truck (Las Vegas, 2017)
  - False alarm emergency stop with passenger injury (Ohio 2020)

NHTSA lifts suspension of EasyMile vehicles

Parcel Delivery

- Parcels to stores, houses
  - Short range delivery
  - Roads, bike lanes, sidewalks
  - Demonstrations in several cities

- Safety approach
  - Early: trailing vehicle
  - Later: remote human

- Example Incidents
  - Sidewalk bot blocks wheelchair ramp (Pittsburgh, 2019)
  - Tension over use of sidewalk space
Automated driving of car or truck
- Continuous driver supervision
- OEMs in production already

Safety approach
- Human driver monitors automation
- Human driver responsible for safety

Example Mishaps
- Multiple fatal Tesla crashes
  - Issue: driver complacency
  - Issue: under 10 seconds from OK to fatal crash
- Tempe Arizona fatality in testing (Tempe, 2018)
Fleet vehicles
- Waymo robotaxis deployed a limited scale
- Middle-mile trucks gained interest in 2020
- Many players pushing hard in this area

Safety approach
- Early: Human safety driver
- Later: Human on-call if car asks for help

Example incidents
- California reports indicate minor incidents in testing
Consolidation in the “race” to autonomy
- It takes huge resources to succeed
- Trend to OEM + ADS supplier teaming
- Smaller players fail, team, or acquired over time

Fully autonomous pivot toward freight
- Low kinetic energy for last mile service
- Middle mile highways less chaotic than urban

Shift of “SAE Level 3” vehicles to L3+
- Strict L3 means human driver supervision
- OEMs shifting to L3+ with car safe stopping on its own

# A User-Centric Classification

<table>
<thead>
<tr>
<th>Operating Mode</th>
<th>Human Role</th>
<th>Driving</th>
<th>Driving Safety</th>
<th>Other Safety</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assistive</td>
<td>Driving</td>
<td><img src="https://via.placeholder.com/15" alt="Human" /></td>
<td><img src="https://via.placeholder.com/15" alt="Human" /></td>
<td><img src="https://via.placeholder.com/15" alt="Human" /></td>
</tr>
<tr>
<td>Supervised</td>
<td>Eyes ON the road</td>
<td><img src="https://via.placeholder.com/15" alt="Car" /></td>
<td><img src="https://via.placeholder.com/15" alt="Human" /></td>
<td><img src="https://via.placeholder.com/15" alt="Human" /></td>
</tr>
<tr>
<td>Automated</td>
<td>Eyes OFF the road</td>
<td><img src="https://via.placeholder.com/15" alt="Car" /></td>
<td><img src="https://via.placeholder.com/15" alt="Car" /></td>
<td><img src="https://via.placeholder.com/15" alt="Human" /></td>
</tr>
<tr>
<td>Autonomous</td>
<td>No human driver</td>
<td><img src="https://via.placeholder.com/15" alt="Car" /></td>
<td><img src="https://via.placeholder.com/15" alt="Car" /></td>
<td><img src="https://via.placeholder.com/15" alt="Car" /></td>
</tr>
</tbody>
</table>

### Vehicle Automation Modes

- Assistive
- Supervised
- Automated
- Autonomous
Standards-Based Engineering Approach

<table>
<thead>
<tr>
<th>SYSTEM SAFETY</th>
<th>UL 4600</th>
<th>Safety Beyond Dynamic Driving</th>
</tr>
</thead>
<tbody>
<tr>
<td>DYNAMIC DRIVING FUNCTION</td>
<td>ISO/PAS 21448</td>
<td>SaFAD/ISO TR 4804</td>
</tr>
<tr>
<td>FUNCTIONAL SAFETY</td>
<td>ISO 26262</td>
<td></td>
</tr>
<tr>
<td>CYBER-SECURITY</td>
<td>SAE J3061</td>
<td>SAE 21434</td>
</tr>
<tr>
<td>VEHICLE SAFETY</td>
<td>FMVSS</td>
<td>NCAP</td>
</tr>
</tbody>
</table>

HIGHLY AUTOMATED VEHICLE SAFETY CASE

UL 4600

© 2021 Philip Koopman
Perception & prediction
- Safety of machine learning-based functions
- Need more than object motion tracking

Safety of Intended Function (SOTIF)
- Drive/Fix/Drive iteration with lots of testing
  - Waymo: 6M test miles; 65K deployed miles
- How will safety be argued for larger fleets?
  - Likely will involve UL 4600 concepts and safety cases

Getting from “works OK” to “safe”
- You can brute force the first few “nines” … but not all of them.
- Field feedback into safety cases
Still an open world with unknowns & changes
- Want “Positive Risk Balance” (safer than human driver)
- But ... *no human driver responsible*

Use Positive Trust Balance
- Engineering rigor
- Practicable validation
- Strong safety culture
  .... and ...
- Field feedback to handle surprises

UL 4600 ties feedback to Safety Case
Safety Arguments (Safety Case)

- **Claim** – a property of the system
  - “System avoids pedestrians”
- **Argument** – why this is true
  - “Detect & maneuver to avoid”
- **Evidence** – supports argument
  - Tests, analysis, simulations, ...
- **Sub-claims/arguments address complexity**
  - “Detects pedestrians” // evidence
  - “Maneuvers around detected pedestrians” // evidence
  - “Stops if can’t maneuver” // evidence
Safety Performance Indicators (SPIs)

- SPIs monitor the validity of safety case claims (UL 4600)

Vehicle is Safe

Avoids Crashes

Detects Objects

Sensors Effective

Data Fusion Effective

Sensor Cleaning

SW Quality

Test Coverage

CLAIMS-ONLY VIEW OF SAFETY CASE

LAGGING METRICS

LEADING METRICS
Examples of SPIs

- “Acts dangerously” is only one dimension of SPIs
  - Violation rate of pedestrian buffer zones
  - Time spent too close per following distance math

- Components meet safety related requirements
  - False negative/positive detection rates
  - Correlated multi-sensor failure rates

- Design & Lifecycle considerations
  - Design process quality defect rates
  - Maintenance & inspection defect rates

- Is it relevant to safety? ➔ Safety Case ➔ SPIs
2021 Safety Themes

- Positive Trust Balance:
  - Engineering Rigor, Validation, Feedback, Safety Culture
  - Standards-driven safety
  - Transparency

- Safety Performance Indicators (SPIs)
  - Continual improvement & updates
  - Field feedback: development; deployed

- Scalability past pilot vehicles
  - Accurate perception/prediction is still work in progress
  - Transition from brute force data to safety case approach
2021 Organizational Safety Challenges

- Significant pressure to deploy
  - Flurry of empty driver seat demos in late 2020
  - Can teams take the time needed for safety?

- Industry transparency needed
  - Safety collaboration rather than competition
  - Public trust in face of an adverse news event

- Ensuring robust safety cultures
  - Silicon Valley culture + automotive culture + no human driver
  - We need to get this right to succeed!

https://youtu.be/nhqyrze30bk
Yandex demo video, Ann Arbor MI, Aug 2020
WE DELIVER THE PROMISE OF AUTONOMY

EDGE CASE RESEARCH