UL 4600
General Stakeholder Overview

October 10, 2019

Deborah Prince, Underwriters Laboratories
Dr. Philip Koopman, Edge Case Research
Webinar Goals

UL 4600: Standard for Safety for the Evaluation of Autonomous Products

- Overview for policy, consumer groups, and general stakeholders

Goals for this Webinar
- Orientation to standard for policy-oriented audience
- How to get a copy and submit comments
- Q&A
Why UL?

- Underwriters Laboratories: working for a Safer World for 125 years
  - Published first safety standard in 1903
  - Focus on research, education, and more than 1,700 standards

- UL’s Standards Development process
  - Consensus process
  - Open, transparent, and timely
  - Continuous standards maintenance
**UL 4600 Standards Technical Panel (STP)**

- **STP is the voting consensus body**

<table>
<thead>
<tr>
<th>Company/Institute</th>
<th>Company/Institute</th>
<th>Company/Institute</th>
<th>Company/Institute</th>
<th>Company/Institute</th>
</tr>
</thead>
<tbody>
<tr>
<td>ANSYS</td>
<td>Beijing Research Institute of Automation for Machinery Industry</td>
<td>Intel Corp</td>
<td>Nanyang Technological University</td>
<td>Robert Bosch LLC</td>
</tr>
<tr>
<td>Argo AI</td>
<td>Center for Auto Safety</td>
<td>Intertek</td>
<td>NIO</td>
<td>UBER ATG</td>
</tr>
<tr>
<td>Aurora Innovations</td>
<td>Consumer Product Safety Commission</td>
<td>Liberty Mutual Insurance Company</td>
<td>Nissan North America Inc</td>
<td>UL LLC</td>
</tr>
<tr>
<td>AXA XL</td>
<td>Daimler Trucks North America</td>
<td>Locomation</td>
<td>Oak Ridge National Laboratory</td>
<td>University of York</td>
</tr>
<tr>
<td>Azevtec Inc</td>
<td>Edge Case Research</td>
<td>The MITRE Corp</td>
<td>Penn DoT</td>
<td>University of Waterloo</td>
</tr>
<tr>
<td>Babst, Calland, Clements &amp; Zomnir</td>
<td>Infineon Technologies AG</td>
<td>Munich Re America</td>
<td>Renesas Electronics Europe GBMH</td>
<td>US DoT</td>
</tr>
</tbody>
</table>
Timeline

- **Initial drafting**
  - July 2018: Announced intent to develop UL 4600

- **STP revisions**
  - June 2019: STP meeting to discuss first full draft
  - Three rounds of STP comment & draft revisions completed

- **Stakeholder comments**
  - Oct 2019: Stakeholder preliminary draft available
  - Stakeholder comments due Nov 1, 2019

- **Target final version release Q1 2020**
Overview

- Orientation to current preview draft version
  - (Recorded technical webinar has more detail)

- UL 4600 Scope
  - Fully Autonomous Vehicle (AV) operation
  - No human driver/supervisor
  - It defines a standard of care, not a road test

- Main principles
  - Safety case is front and center
  - Assessment emphasizes safety case & level of care
UL 4600 Key Policy Ideas

- Methodical way to show use of best practices
  - Why does a developer think their AV is safe?
  - Why should we believe this argument?
  - #DidYouThinkofThat? (Incorporates lessons learned)

- Scope includes entire system lifecycle
  - Design, operations, maintenance, updates, supply chain, ...
  - Monitoring and feedback provide continual safety metric updates

- Transparency via independent assessment
  - Flexible framework; does not pick technology winners
Autonomous systems have unique needs
- Unlike ADAS, there is no human in charge
- System level approach needed

Other standards provide the “how”
- ISO 26262 (functional safety)
- ISO/PAS 21448 (SOTIF), SaFAD (autonomous safety)
- BSI/PAS 1881 (road testing)

UL 4600: “Did you do enough?” and #DidYouThinkofThat?
- Safety case puts pieces from other standards together
- Specifies a level of care for ensuring acceptable system safety
- Provides a template for technical safety report
What UL 4600 Is / Is Not

- **In scope:**
  - Fully autonomous system operation
  - Driving + logistics + maintenance + support
  - Interaction with road users, pedestrians
  - Arguing acceptable risk has been achieved

- **Out of scope:**
  - Human ability to control or supervise vehicle
  - Prescriptive ethics; how safe is safe enough; details of security

- **Does not specify specific tests or a “driving exam”**
  - Developers specify measurement approach as part of safety case
  - Independent Assessment checks the safety case
What’s A Safety Case?

- A structured argument backed by evidence
- SubGoal/Claim: “AV will not hit pedestrians”
  - Hypothetical Arguments
    - “AV will detect pedestrians of all types”
    - “AV will stop or avoid collision detected pedestrians”
    - “We have identified & mitigated risks caused by difficult to detect pedestrians”
  - Hypothetical Evidence
    - “Here are results of detect & avoid tests”
    - “Here is analysis of coverage of different types of pedestrians”
    - “Reliability growth data shows high pedestrian coverage”
Lists of Best Practices

- Extensive lists of: #DidYouThinkofThat? (“prompts”)
  - Good practices & Pitfalls (lessons learned & bad practices to avoid)

- Repository to capture lessons learned over time
  - Seeded by proposal authors with extensive safety experience:
    - Phil Koopman: automotive, chemical process, consumer appliances, ...
    - Uma Ferrell: aviation (FAA DER)
    - Frank Fratrik: military systems (US DoD test experience)
  - Plus comments from automotive industry STP and stakeholders

- Prompts mean: “include this topic in safety case”
  - Deviations permitted if prompt is inapplicable to a design
  - Can modify ODD to avoid problematic issues
UL 4600 ODD Prompt Excerpts

- **Travel infrastructure**
  EXAMPLES: types of road surfaces, road geometries, bridge restrictions

- **Object coverage** (i.e., objects within ODD)

- **Event coverage**
  EXAMPLES: interactions with infrastructure

- **Behavioral rules**
  EXAMPLES: traffic laws, system path conflict resolution priority, local customs, justifiable rule breaking for safety

- **Environmental effects**
  EXAMPLES: weather, illumination

- **Vulnerable populations**
  EXAMPLES: pedestrians, motorcycles, bikes, scooters, other at-risk road users, other road users

- **Seasonal effects**
  EXAMPLES: foliage changes, sun angle changes, seasonally-linked events (e.g., Oktoberfest)

- **Support infrastructure, if any is relied upon**
  EXAMPLES: types of traffic signs, travel path geometry restrictions, other markings

- **Localization support, if relied upon**
  EXAMPLES: GNSS availability, types of navigation markers, DSRC, other nav aids

- **Compliance strategy for traffic rules**
  EXAMPLE: enumeration of applicable traffic regulations and ego vehicle behavioral constraints

- **Special road user rules**
  EXAMPLES: bicycles, motorcycles/lane splitting, construction systems, oversize systems, snowplows, sand/salt trucks, emergency response systems, street sweepers, horse-drawn systems

- **Road obstructions**
  EXAMPLES: pedestrian zone barriers, crowd control barriers, police vehicles intentionally blocking traffic, post-collision vehicles and associate debris, other road debris, other artificial obstructions
System, Environment, Lifecycle

Safety case covers:
- Autonomy (sensors, algorithms, actuators)
- Vehicle (safety related within autonomy purview)
- Maintenance and inspection procedures
- Lifecycle issues and supply chain
- Data sources, maps, communications, ML training

Assumptions & supporting requirements
- ODD characterization
- Road infrastructure support
- Procedural support (e.g., safety related inspections)
Role of Humans

- No human to be “captain of the ship”
  - But, system must still be safe
- Humans still do maintenance
  - Who does “pre-flight” inspection?
- Interacting with people
  - Occupants, cargo handlers
  - Pedestrians and mobility device users
  - Other vehicles & human drivers
  - Especially vulnerable populations
  - Misuse, malfeasant, pranks
- Safety culture for all stakeholders
UL 4600 Scope

System level safety for autonomous operation & lifecycle

- SYSTEM (Item scope: Vehicle + Infrastructure)
  - ODD SPECIFIED
  - PROMPT ELEMENTS TAILORED TO ODD & SYSTEM
  - RIGOROUS DEVELOPMENT PROCESSES
  - RIGOROUS OPERATIONAL PROCESSES
  - SAFETY CULTURE

- CONTEXT DEFINED

- TOP LEVEL GOAL: AV SAFETY CASE IS ACCEPTABLE (Hypothetical/Simplified)

- SAFETY CASE WELL FORMED
  - ADDRESSES PROMPT ELEMENTS
  - TRACEABILITY WITHIN SAFETY CASE & TO UL4600
  - REASONABLE INDUCTIVE STEPS / AVOIDS PITFALLS
  - METRICS MONITOR SAFETY CASE VALIDITY
  - SELF-AUDITS
  - INDEPENDENT ASSESSMENT

- HAZARDS IDENTIFIED
  - FAULT MODELS DEFINED
  - VEHICLE (SYSTEM & SOFTWARE)
  - AUTONOMY PIPELINE
  - DATA, NETWORKING, SERVICES
  - ROAD USERS
  - LIFE CYCLE & SUPPLY CHAIN
  - MAINTENANCE & INSPECTIONS
  - TOOLS & COMPONENTS

- RISKS MITIGATED
  - HAZARDS MAPPED TO RISK-BASED INTEGRITY
  - FAULT RESPONSE & ODD VIOLATION STRATEGY
  - MITIGATIONS IDENTIFIED & SUFFICIENT
  - DEPENDABILITY ISSUES ADDRESSED
  - FEEDBACK TO MANAGE UNKNOWNS
UL 4600 does **not** have a specified road test

- For now, each AV design is unique
  - One-size-fits-all road test is insufficient for safety
  - Engineering rigor + system-specific tests required

UL 4600 approach:

- Explain specifically why system is safe
  - Required coverage of traffic rules, define ODD, etc.
- Developer defines & provides specific evidence
  - Defined test plan & results
  - Simulation, analysis, HIL tests, road tests, etc.
  - Testing tied directly to safety for that vehicle design

What About Measurements?
UL 4600 Policy Takeaways

- Methodical way to show use of best practices
  - Why does a developer think an AV is safe?
  - Why should we believe this argument?
  - #DidYouThinkofThat? (Incorporates lessons learned)

- System-level safety view; works with other standards
  - Can use results from ISO 26262 & ISO/PAS 21448
  - Future road testing standards provide evidence for the safety case

- Transparency via independent assessment
  - Developers define & monitor continual safety metric feedback
Get Involved: Submit Comments

- Commenting requires registering as stakeholder
  - E-mail to: <Deborah.Prince@ul.com>

- Use supplied spreadsheet for consideration
  - Please make as concrete & actionable as possible

<table>
<thead>
<tr>
<th>Reviewing Organization:</th>
<th>PUT YOUR ORGANIZATION HERE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Point of Contact:</td>
<td>PUT YOUR NAME and e-mail address HERE; please combine comments</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>#</th>
<th>Page</th>
<th>Clause</th>
<th>Old text</th>
<th>New text</th>
<th>Discussion</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>54</td>
<td>5.2.3.3.c.1</td>
<td>Quote the old text before change</td>
<td>Your proposed new text with change</td>
<td>Explain (could be just &quot;typo&quot; or &quot;format&quot; if that is the issue).</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Comments & Timeline

- Official version & comment spreadsheet via UL CSDS
  - Other public materials and draft at: UL4600.com

- Timeline:
  - Comments due Friday Nov 1st via CSDS upload
  - Potentially voting draft in December

- Will Stakeholder names be public?
  - Stakeholder list itself is private
  - However, all preliminary review comments are public & attributed to commenter