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**

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

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

Carnegie Mellon University

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

Why UL 4600?

- **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:**
  - **<u>Fully autonomous</u>** 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"**
  - <u>Developers specify measurement approach as part of safety case</u>
  - Independent Assessment checks the safety case

9

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 navaids

- **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)

13

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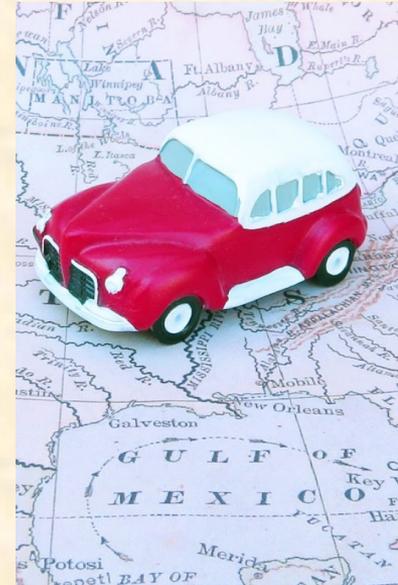
- **No human to be "captain of the ship"**
  - But, system must still be safe
- **Humans still do maintenance**
  - Who does "pre-flight" inspection?
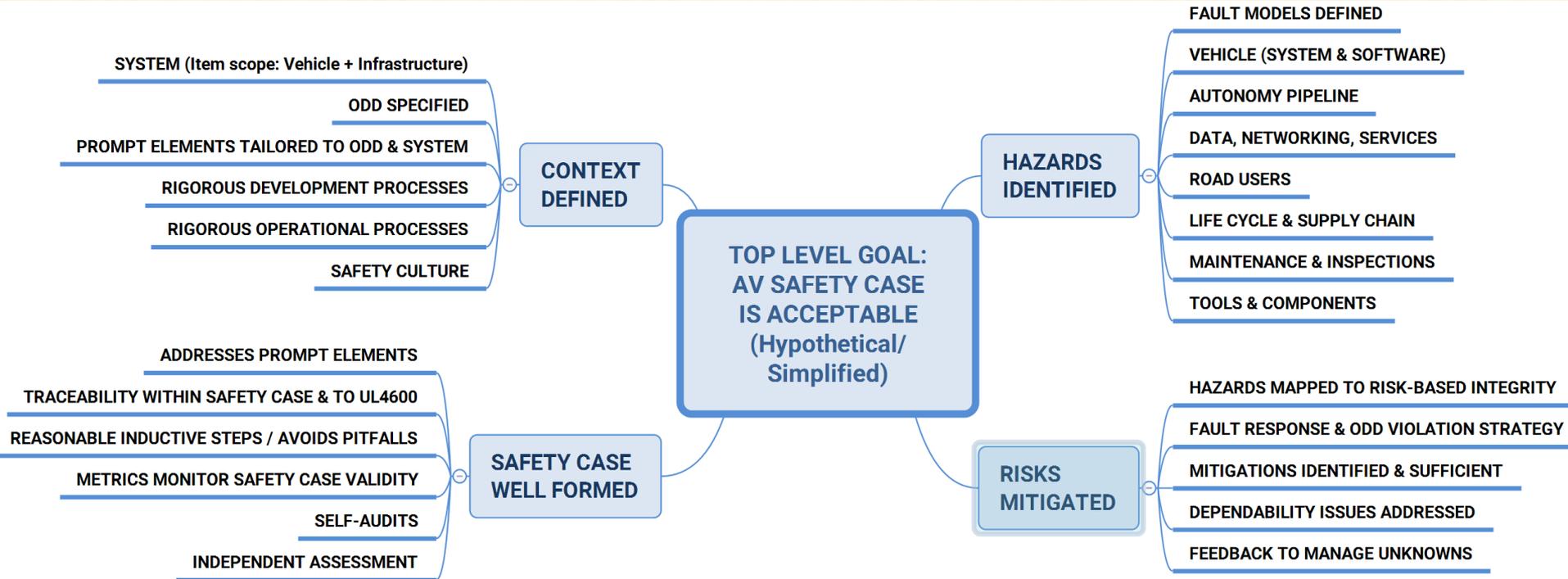- **Interacting with people**
  - Occupants, cargo handlers
  - Pedestrians and mobility device users
  - Other vehicles & human drivers
  - Especially vulnerable populations
  - Misuse, malfeasance, pranks
- **Safety culture for all stakeholders**

https://bit.ly/2GvDkUN

Is it safe to drive now?

14

- **System level safety for autonomous operation & lifecycle**

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

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

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

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

What About Measurements?

UL 4600 does <u>not</u> 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

16

UL 4600 Policy Takeaways
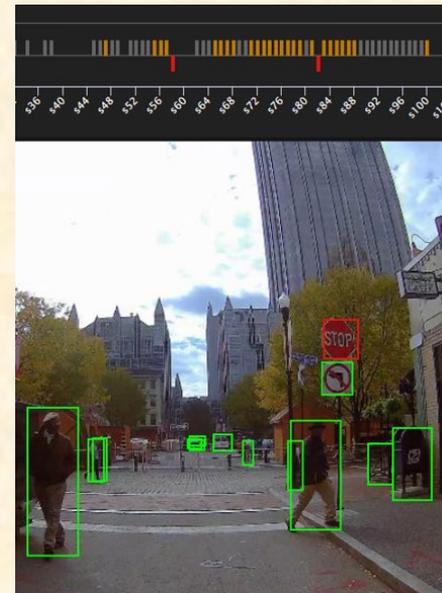
- **Methodical way to show use of best practices**
  - Why does a developer think an AV is safe?
  - Why should we believe this argument?
  - #DidYouThinkofThat? (Incorporates lessons learned)

UL4600.com

- **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

Reviewing Organization:			PUT YOUR ORGANIZATION HERE		
Point of Contact:			PUT YOUR NAME and e-mail address HERE; please combine comments		
#	Page	Clause	Old text	New text	Discussion
1	54	5.2.3.3.c.1	Quote the old text before change	Your proposed new text with change	Explain (could be just "typo" or "format" if that is the issue).
2					
3					

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
  - Target for approved standard: Q1 2020.
- **Will Stakeholder names be public?**
  - Stakeholder list itself is private
  - However, all preliminary review comments are public & attributed to commenter