Autonomous Vehicle Safety

CCC
October 16, 2019
Brute Force AV Validation: Public Road Testing

- Good for identifying “easy” cases – but 1 billion+++ miles(!)
  - Expensive and potentially **dangerous**

“Edge Cases” Are the Hard Part

- Novel objects (missing from zoo) are “triggering events”
Example Triggering Events via Hologram

- Mask-R CNN: examples of systemic problems

Notes: These are baseline, un-augmented images. (Your mileage may vary on your own trained neural network.)
UL 4600 Key Ideas

- **Goal:** structured way to argue that AV sufficiently safe
  - Emphasize safety case, not engineering process
  - Checks and balances (self-audit and independent)

- **Monitoring and feedback**
  - Detect invalid assumptions & gaps in coverage

- **System Level + Life Cycle approach**
  - Includes fault recovery, supply chain issues, expected misuse

- **Reference lists to improve completeness**
  - Prompts & epistemic defeaters for coverage (#DidYouThinkofThat?)
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**

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

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

**SAFETY CASE WELL FORMED**
- ADDRESSES PROMPT ELEMENTS
- TRACEABILITY WITHIN SAFETY CASE & TO UL 4600
- REASONABLE INDUCTIVE STEPS / AVOIDS PITFALLS
- METRICS MONITOR SAFETY CASE VALIDITY
- SELF-AUDITS
- INDEPENDENT ASSESSMENT

**RISKS MITIGATED**
- HAZARDS MAPPED TO RISK-BASED INTEGRITY
- FAULT RESPONSE & ODD VIOLATION STRATEGY
- MITIGATIONS IDENTIFIED & SUFFICIENT
- DEPENDABILITY ISSUES ADDRESSED
- FEEDBACK TO MANAGE UNKNOWNS

© 2019 Edge Case Research