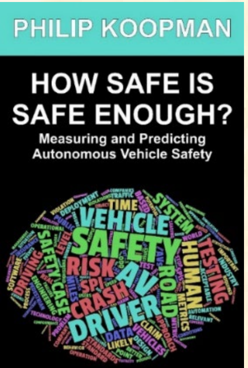
Safety Case Considerations For Scenario-Based Assurance

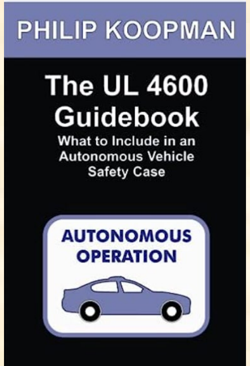
Prof. Philip Koopman



PHILIP KOOPMAN

HOW SAFE IS SAFE ENOUGH?

Measuring and Predicting Autonomous Vehicle Safety



PHILIP KOOPMAN

The UL 4600 Guidebook

What to Include in an Autonomous Vehicle Safety Case

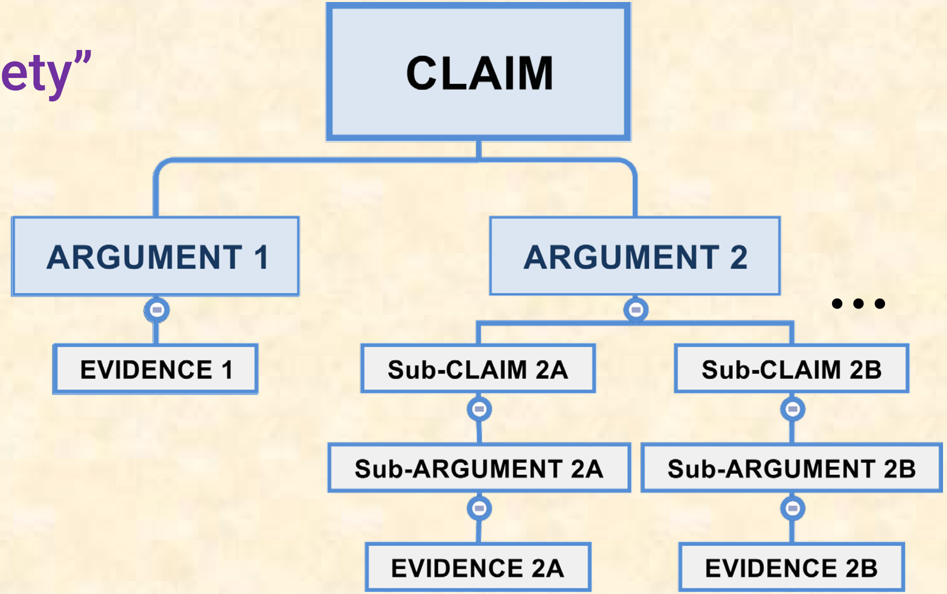
ARTS 2023

July 12, 2023

Carnegie Mellon University

Safety Case

- Claim – what you think is true
  - “Scenario-based testing proves safety”
- Argument – why this is true
  - “A & B & C & D and not E”
- Evidence – supports argument
  - Tests, analysis, simulations, …
- Sub-claims/arguments address complexity
  - “No loss events in scenario simulations”
  - “Simulation results predict real-world safety”
  - *… other considerations we’ll discuss today …*



Limits To Simulation Scope?

- What, exactly, is out of scope for scenario-based validation?
  - Perception limitations?
    - Misclassified objects, age-related degradation, …
  - Equipment failures (e.g., degraded modes)?
    - Camera lens cleaning system failure
  - Infrastructure failures?
    - Missing/degraded road markings
    - HD map missing a bridge collapse
  - Novel road users, objects, events
    - Tumblegeddon (Jan. 2020, WA state)
- Track these for resolution in safety case

https://bit.ly/3COCkrg

Tool Qualification

Carnegie Mellon University

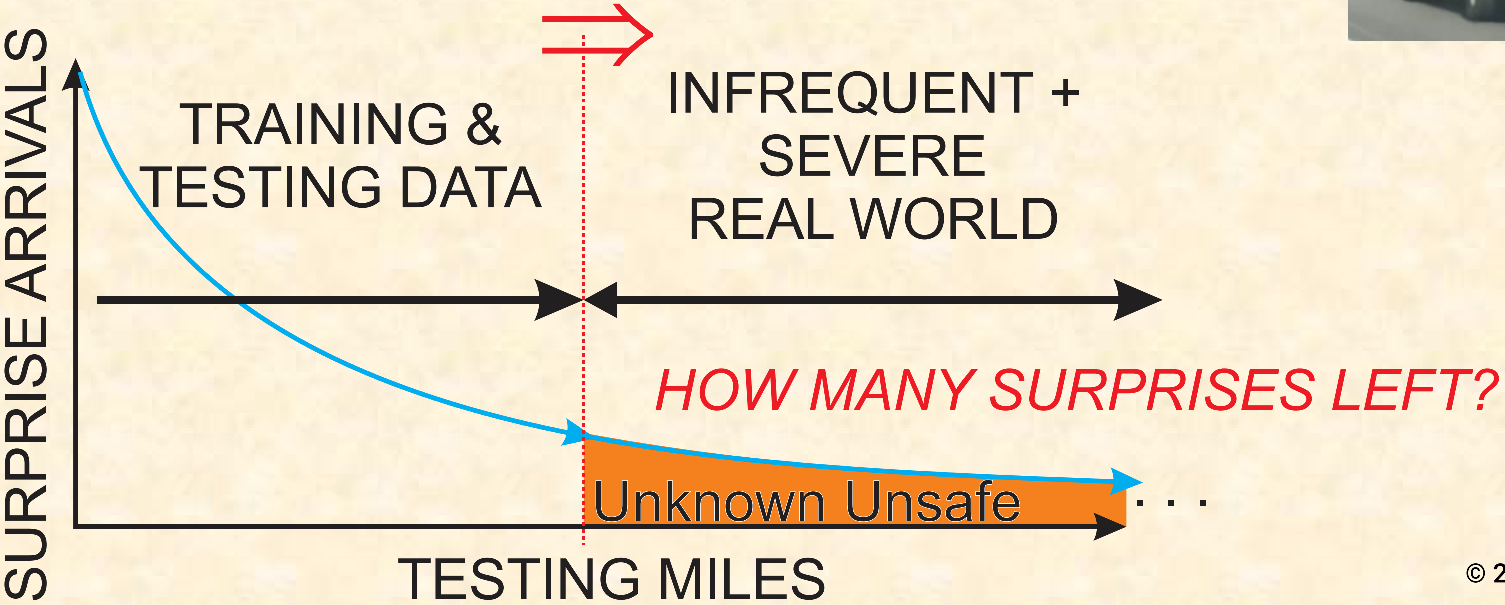
- Could someone die because of a tool defect?
  - Simulations are life critical if they replace road testing
- Simulation software quality
- Simulated object/event completeness
  - Do you have 1 billion miles of weirdness captured?
- Simulation campaign management
  - Simulations being run correctly?
  - Low probability * high consequence accounted for?
  - Pass/fail criteria defined and reported accurately?
  - Results recorded & reported accurately?

https://bit.ly/3Xt30ay

Surprises

- Claim: “Scenario set is complete”
  - ➔ Every surprise is a safety case defect
- Need to instrument surprise arrival rate
  - – Ideas from Software Reliability Modeling

https://bit.ly/444r4TB



Acceptable Safety

- Set robust pass/fail expectations
  - Getting lucky is not enough for safety!
  - Did AV violate traffic laws?
  - Did AV honor safety buffers?
  - Is prediction capability accurate enough?
- Prioritize lack of negligent driving
  - Average driver improvement is not enough
  - Compare to a Reasonable Driver
    (i.e., lack of negligent behaviors)

https://bit.ly/46oAYkn

Take-Aways

- Use a written safety case
  - It helps expose gaps in safety thinking
- Simulations are doomed to succeed
  - Ensure safety even if holes in scenario set
- Tooling just got life critical
  - If you skip any part of real-world validation…
    … that simulation is now life critical
  - That includes models, test orchestration, report spreadsheets, …
- The real world does not follow your rules
  - “That wasn’t supposed to happen” … will find a way to happen

https://on.gei.co/2r2rjzg

You Might Forget the Rare Events

…

But They Won’t Forget You!