# The Place of Scenarios in a Holistic Safety Assurance Approach

**Steven E. Shladover, Sc.D.**
**University of California PATH Program**
**V&V Methods Final Event (Virtual-Stuttgart)**
**November 22, 2023**

# Holistic View of ADS Safety

- Obey traffic laws
- Interact politely with other road users to facilitate traffic
- Avoid crashes (even when other road users misbehave)
- Interact appropriately with emergency responders
- Appropriate minimal risk condition actions (i.e., When is stopping in lane appropriate? How to restore to service?)
- Exercise appropriate post-crash duty of care
- Provide effective remote human support to ADS
- Maintain ADS operations through natural disasters
- Manage system-level faults (e.g., comm networks)

CALIFORNIA PATH

# Attributes of Safety-Critical Scenarios

**Combinations of variations in:**

- **Road geometry and traffic control devices**
- **Locations and motion vectors of all road users**
- **Weather and lighting conditions**
- **Vehicle and ADS fault conditions**
- **Traffic incidents and emergency response events**
- **External events – GNSS and comm outages, crime scenes, natural disasters, terrorist incidents,…**

** **Seek realistic extreme corner cases** **

CALIFORNIA PATH

# Role of Scenarios in Safety Case Argumentation

- Implement Safety Management System
- Define use case and ODD to determine behavioral competencies needed
- Identify relevant hazards and strategies for managing each
- Functional safety analysis and design
- Design, development and testing of prototype system for each individual relevant hazard condition (simple scenarios)
- Assessment of prototype system safety under combined hazard conditions
  - Selection of worst-case scenarios for simulation and for subsystem and system testing on proving grounds

CALIFORNIA PATH

# Safety Case Challenges Beyond Crash Avoidance

- Non-deterministic behavior of machine learning systems
- Unexplainable AI making debugging challenging
- Roles of remote human support staff and their interfaces with ADS (technical and procedural)
- Safe responses to uncontrollable external events (power failures, comm failures, natural disasters)
- Transferability of safety case data and methods across geographic boundaries
  - Standardization of model validation methods and criteria
  - Sharing of realistic worst-case scenarios
- Transparency to earn credibility vs. developer IP protection
  - Public perception of safety vs. actual safety

CALIFORNIA PATH