Test Specifications for Highly Automated Driving Functions: Highway Pilot

Hardi Hungar
Team Leader Verification and Validation Methods
Institute of Transportation Systems, German Aerospace Center (DLR)
Joint work with: Frank Köster, Jens Mazzega

This research was partially funded by the German Federal Ministry for Economic Affairs and Energy, Grant No. 19A15012F (PEGASUS), based on a decision by the Parliament of the Federal Republic of Germany. The responsibility for the content lies with the authors.
Introduction
Application: Highway Pilot

- Automated driving on a highway under regular conditions (SAE level 3)
  - Passenger car
  - Highway or similar equipped road
  - Speed limited to 130 km/h
  - Ordinary weather conditions

Included
- Stop & Go
- Changing lanes
- Overtaking
- Emergency manoeuvres
  - Braking
  - Evasive actions
- Fallback when reaching system boundaries:
  - Driver (with sufficient takeover time)
  - Risk minimizing maneuver (if driver does not respond)

Excluded
- Entering the highway
- Exiting the highway
- Bad weather
  - (very) Slippery surface
  - Heavy rain, snow, fog
Introduction
Problem: How to prove safety of a Highway Pilot?

- **ISO 26262**: Standard „Road Vehicles – Functional Safety“ for developing systems with electronic elements
  - **Risk-based approach to safety**
    - Risk ≈ $\sum_{h \in H} E_h \times C_h \times S_h$
      - $H$: Set of harmful events $h$
      - $E$: probability of occurrence (precisely: expected number per time unit)
      - $C$: controllability (here: probability of not avoiding an accident)
      - $S$: severity of event (injuries, fatalities)

- **Safety requirement**:
  - The risk must be „minimized“
  - The definition of „minimal“ may vary

- Proving safety of an implementation of the Highway Pilot
  - ¿Testing a Highway Pilot on the road under supervision of a safety driver?
  - May take a while (one estimate: some billion kilometers, $\sim 13 \times 10^9$ [1])

Approach
Specification Concept: Scenarios

- A scenario (after [2]) describes a traffic sequence
  - Here: always with one distinguished ego car
  - Consists of
    - scenes (snapshots), connected by
    - actions of the ego car, and
    - events coming from the environment (traffic participants or other)

- Example scenario „Cut In“ (Illustration)
  - 1: Ego vehicle is following Lead vehicle, other vehicle is approaching from behind
  - 2: Other vehicle overtakes and moves into ego lane (events)
  - 3: Other vehicle has cut in (event)

Approach

Hierarchy of Tests: Virtual, Proving Ground, Field

• Simulation
  • Embed HAF control into traffic simulation software
  • Run extensive tests

• Proving Ground
  • Targeted experiments in controlled environments
  • Validation of simulation results

• Field Data
  • Measuring parameters of exposure
  • Evaluating accident data
  • Validating simulation results in reality
Approach
Safety Goal: Outperform the Human Driver

Risk Distribution Human Driver
- Congestion
- Lane change
- Cut in
- Following
- Adverse Weather

Risk Automation
- Congestion
- Lane Change
- Cut in
- Following
- Adverse Weather
- Automation errors
- Safety Gain

Net improvement over human driver
Outperform human in each category

Illustration – not representing valid data

New accident causes
Scene Definition

- A **Scene** describes a particular state
  - Traffic infrastructure
    - Lanes, regulations
    - Geometry: curvature, elevation
  - Environment conditions
    - Surface grip (wetness, …)
    - Perception: Light, sun, fog, sensor obstacles, etc.
  - Traffic
    - Vehicles: Ego and usually other
      - Type
      - Position, speed, orientation
      - Blinker, brake lights
Scenario Definition

- A **Scenario** describes a particular evolution of scenes
  - It consists of
    - A (finite) timed sequence of scenes
    - A fully defined *start scene*
    - Transitions between subsequent scenes, with
      - Actions of the ego vehicle
      - Events from the environment (other vehicles, conditions)
      - Evolutions (passage of time)
  - One line of evolution (of potentially many)
Scenes and Scenarios
Definition (Elaboration)

• **Scene** parameters need not be fully defined
  • **Field data**: Precise values (ground truth) are not always available
  • **Specifications**: Ranges serve to capture a class of similar situations

• **Scenarios**
  • **Action**, **event** and **time** parameters can be imprecise
  • The **discrete structure** remains **fixed** in one scenario
    • E.g.: Lane change performed vs. lane change aborted go into different scenarios
  • **Discrete variability** captured in sets/**classes** of scenarios
Scenario Classes
Functional and Concrete Scenarios

• **Functional Scenario**
  • Textual / graphical description of a class of scenarios
  • Rough parameter ranges (if at all restricted)
  • May include discrete variability
  • **Usage:** High-level specification
  • Examples: Cut-in, Cut-through, Lane Change, Overtaking, etc.

• **Concrete Scenario**
  • Fully defined sequence
  • Parameters within tight bounds
  • One line of evolution
  • **Usage:**
    • Capture field data or simulation runs
    • Define test cases

Capture and discuss different classes of evolutions

Essentially one specific evolution

One functional scenario describes a large set of concrete scenarios
Scenario Classes
Functional Scenarios

• Functional Scenario
  • Textual / graphical description of a class of scenarios
  • Rough parameter ranges (if at all restricted)
  • May include discrete variability
  • Usage: High-level specification
  • Examples: Cut-in, Cut-through, Lane Change, Overtaking, etc.

• List of functional scenarios
  • Free driving
  • Following
  • Lane change
  • Overtaking
  • Cut-in
  • Leave lane
  • Cut-through
  • Slow traffic
  • Stop & Go
  • Jam
  • Lane violation
  • Incident traffic
  • Wrong-way driver
  • Obstacle
  • Incident environment
Scenario Classes

Functional Scenario Examples: Cut-in / Incident Environment

**Cut-in**
- **Start situation**
  - Ego car (E) drives on highway lane
  - Other vehicle (C) on adjacent lane
  - Potentially further vehicles involved
- **Evolution**
  - C moves into E-lane in front of E
- **Criticalities**
  - C cuts in with little distance to E
  - C brakes after cutting in
  - Low TTC(E,C)

**Incident Environment**
- **Start situation**
  - Ego car (E) drives on highway lane
  - Varying traffic situations
- **Evolution**
  - Sudden change of environment conditions affecting traffic
    - Heavy rain/snow
    - Fog, low standing sun
    - Wet road surface, ice/white frost
- **Criticalities**
  - Sensor reliability reduced
  - Grip reduced/lost

TTC: Time to collision
Scenario Classes

Logical Scenarios

- **Functional Scenario**
  - **Usage**: High-level specification

- **Logical Scenario**
  - One line of evolution
  - Parameter ranges with occurrence probability distributions
  - Represents set of concrete scenarios
  - **Usage**: Main constituent in the test specification

- **Concrete Scenario**
  - **Usage**: Define test cases

Cut-in (left, from behind) (regular traffic situation)

- Step 1:
  - Velocity [m/sec]: E, L: [22-36]; E-L: [-4,4]; C: [23-67]; C-E: [1,45];
  - Position [m]: L-E: [33,100]; E-C: [0,30];
  - Distributions: may be multivariate binomial (nontrivial correlations), or multivariate gamma-distributions

- Step 2: Cut-in starts (C crosses lane marking) \( \Delta t: [2,20] \)
  - Velocity [\( \Delta \) m/sec]: L: [-7,+7]; C: [-50,+5]; C-E: [-5,40]; C-L:[-12,50]
  - Position [m]: L-E: [25,110]; C-E: [1,60]; L-E: [5,100]

- Step 3: Cut-in completed (C has crossed lane marking halfway) \( \Delta t: [0.5,4] \)
  - Velocity [\( \Delta \) m/sec]: …
  - …

Figures given as illustration
**Deriving Scenarios**

**Logical Scenarios** are derived systematically from Functional Scenarios
- One Functional Scenario (or a combination of Functional Scenarios) gives rise to a number of Logical Scenarios
- Cut-in (left, from behind)
- Cut-in (left, front)
- Cut-in (left, fall-back)
- Cut-in (right, from behind)
- ...

**Concrete Scenarios** are instantiations of Logical Scenarios
- One Logical Scenario represents a large (infinite) number of Concrete Scenarios
- Step 1:
  - Velocity [m/sec]: E, L: [22, 36]; E-L: [-4,4]; C: [23-67]; C-E: [1.45];
  - Position [m]: L-E: [33, 100]; E-C: [0, 30];
  - Distributions: may be multivariate binomial (nontrivial correlations), or multivariate gamma-distributions
- Parameter instantiations
  - Relative frequencies according to probability distributions
Criticality of Scenarios

- **Criticality** of a scenario
  - \( \sum_{h \in H} C_h \cdot S_h \)
  - \( H \): Set of harmful outcomes \( h \)
  - \( C \): probability of occurrence of the outcome
  - \( S \): severity of the outcome (injuries, fatalities)

- **Severity**
  - Classes in ISO 26262
    - S0: No injuries
    - S1: Light and moderate injuries
    - S2: Severe and life-threatening injuries (survival probable)
    - S3: Life-threatening injuries (survival uncertain), fatal injuries

  - **Refined severity classes required, e.g.**:
    - S0, S1 remain
    - S2A: Severe injuries
    - S2B: Potentially life-threatening injuries
    - S3A: Life-threatening injuries
    - S3B: Probably fatal injuries
    - S3C: Fatal injuries

- **Numeric scale** for summation required (tbd.)
  - E.g. based on Abbreviated Injury Score
Criticality of Scenarios

- **Criticality** of a scenario
  - $\sum_{h \in H} C_h \cdot S_h$
  - $H$: Set of harmful outcomes $h$
  - $C$: probability of occurrence of the outcome
  - $S$: severity of the outcome (injuries, fatalities)

- **Probability**
  - Classes in ISO 26262 (controllability)
    - C0: controllable in general
    - C1: Simply controllable ($\geq 99\%$ of all drivers)
    - C2: normally controllable ($\geq 90\%$ of all drivers)
    - C3: difficult to control or uncontrollable ($< 90\%$ of all drivers)

- Numeric probabilities required, or refined semi-numeric scale
  - Estimated range: $10^{-10}$ to $1 (= 10^0)$
Frequency of Scenarios

A logical scenario is to be weighted with two frequency figures (exposure): expected number of occurrence per time unit

- $E_{\text{driver}}$: average over human drivers
- $E_{\text{HAF}}$: automation to be tested

Together with severity and probability this fixes the risk associated with the scenario.

Determining frequencies

- $E_{\text{driver}}$: average over human drivers
  - Field data
  - Simulations with validated driver models
  - Adjustments/estimations by experts

- $E_{\text{HAF}}$: automation to be tested
  - Simulations with HAF
  - Adjustments/estimations by experts
Risk Computation Illustration
Scenario „Cut-in“:
Accident Probability

Visualization of accident probability for cut-in depending on

- $\Delta v \, [\text{m/sec}]$: velocity difference between Ego and Cut-in vehicle:
  - “5” means: Cut-in vehicle is 5 m/sec slower (dangerous)

- $\text{gap} \, [\text{m}]$: gap between Cut-in and Ego vehicle
  - “1” means: Cut-in happens with minimal distance (dangerous)

$\text{gap} = \Delta p - 2$
Risk Computation Illustration
Scenario „Cut-in“:
Accident Probability

Cut-in (left, from behind)
- Step 1:
  - Velocity [m/sec]: E, L: [22]; C-E: [1,45];
  - Position [m]: L-E: [33,100]; E-C: [0,30];
  - ...
- Step 2: Cut-in starts (C crosses lane marking) ∆t: [2,20]
  - Velocity [m/sec]: ∆L: [-7,+7]; ∆C: [-40,+4];
    C-E: [-5,2]; C-L: [-9,12]
  - Position [m]: L-E: [25,110]; C-E: [3,12]; L-E: [15,100]
  - ...
- Step 3: Cut-in completed (C has crossed lane marking halfway) ∆t: [0.5,4]
  - Velocity [∆ m/sec]: ...
  - ...

\[ C \approx \] accident probability

\[ \Delta v \text{ [m/sec]} \]

\[ \text{gap [m]} \]

\[ \text{gap} = \Delta p - 2 \]
Risk Computation Illustration
Scenario „Cut-in“:
Exposure

Visualization of frequency of cut-in depending on

- $\Delta v \text{[m/sec]}$: velocity difference between Ego vehicle and Cut-in vehicle
  - The frequency decreases for relatively slower Cut-in vehicle
  - Usually, the Cut-in vehicle is faster than the Ego vehicle (negative values of $\Delta v$)

- gap [m]: gap between Cut-in and Ego vehicle:
  - The frequency increases with gap size
  - Usually, the gap is reasonably large
Risk Computation Illustration
Scenario „Cut-in“:
Risk

Visualization of \textit{risk*} of cut-in

- Risk is highest for
  - a rather high velocity difference \(\Delta v \approx 4 \text{ [m/sec]}\)
  - A narrow (but not minimal) gap \(\text{gap} \approx 9 \text{ [m]}\)
  - The highly dangerous situations occur less often
- The numeric risk is to be computed as the integral of the risk function

* The \textit{severity} is assumed to be constant, here
Risk Computation Illustration
Scenario „Cut-in“:
Risk Integral

Computation by approximate discrete summation

• Like Riemann integral approximation

• Each column represents the result of a test run (simulation / proving ground / field)

• Lower test density in regions with low accident probability
Test Specification and Test Definition

- The **test specification** consists of
  - The full set of **logical scenarios**
  - Annotated with **frequencies (HAF)**
    - Scenario overlap taken into account:
      Evolutions are counted only once

- The **test cases** of the **test definition** are **dynamically constructed**
  - **Concrete scenarios** sampling the risk function
  - Low risk: low density of sampling points
  - High risk: high density of sampling points

<table>
<thead>
<tr>
<th>Scenario Type</th>
<th>Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cut-in (left, from behind)</td>
<td>0.04</td>
</tr>
<tr>
<td>Cut-in (left, front)</td>
<td>0.002</td>
</tr>
<tr>
<td>Cut-in (left, fall-back)</td>
<td>0.0003</td>
</tr>
<tr>
<td>Cut-in (right, from behind)</td>
<td>0.006</td>
</tr>
<tr>
<td>Cut-through (left, from behind)</td>
<td>0.002</td>
</tr>
<tr>
<td>Cut-through (left, front)</td>
<td>0.0005</td>
</tr>
<tr>
<td>Cut-through (left, fall-back)</td>
<td>0.00001</td>
</tr>
<tr>
<td>Cut-through (right, from behind)</td>
<td>0.0008</td>
</tr>
</tbody>
</table>
Summary

- **Test definition** based on Scenarios
  - **Functional**: high-level specification
  - **Logical**: precise specification
  - **Concrete**: test cases

- **Formalization** of test definition
  - Systematic derivation process
  - Supporting risk estimation by testing

- Usage for **safety case** along the lines of ISO 26262
  - More complex argumentation required for HAF homologation than foreseen in the standard
Risk Computation Illustration
Scenario „Cut-in“:
Accident Probability

\[ C \approx \frac{\max(\min(\Delta v * \text{abs}(\Delta v)/(2 * \text{gap}) + 3/\text{gap}, 5), 0.5) - 0.5)}{\text{gap [m]}} \]
Risk Computation Illustration
Scenario „Cut-in“:
Exposure

\[ E \approx \left( \frac{(\Delta v - 6)^4}{4096} \right) \cdot \left( \frac{((19^4 - (\text{abs}(\text{gap} - 20))^4))}{(19^4 - 10^4)} \right) \]
Risk Computation Illustration
Scenario „Cut-in“:
Risk

\[ R \approx \max(\min(\Delta v \cdot \text{abs}(\Delta v)/(2 \cdot \text{gap}) + 3/\text{gap}, 5), 0.5) - 0.5) \times \frac{((\Delta v - 6)^4)/4096 \times ((19^4 - (\text{abs}(\text{gap} - 20)^4)))/(19^4 - 10^4)} \]