How to make a complete hazard analysis and risk assessment for autonomous vehicles?

FUSE Final Seminar 2016-09-23
From driver assistance to driver replacement

Driving on highway - ADAS
- ACC
- Lane departure warning

Driving on highway - AD
- Lane keeping
- Emergency break
- Automated overtake

- AD in complete control of the vehicle and has to handle all situations that may arise...
- But how do we know we’ve found them all?
Problem: Completeness of items for AD

- ISO 26262 HA&RA - item definition is input
  - Risk: Specification of function is too narrow
- Proposal: Use HA&RA to help define scope
  - Iteratively refine HA&RA and function
  - HA&RA objective: set of items for AD is complete within its known limitations
- Item definition and safety goals are outputs
Iterative HA&RA and function refinement process
Preliminary feature description

- Input to iterative HA&RA and function refinement
  - Describes end-user benefit...
  - ...and known limitations

<table>
<thead>
<tr>
<th>Automated Emergency Brake (AEB) — User stories</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>As a driver, I want AEB for crossing animals, so that my automated car doesn’t run into animals.</em></td>
</tr>
<tr>
<td><em>As a driver, I want AEB for other motor vehicles, so that my automated car doesn’t hit vehicles making unexpected maneuvers.</em></td>
</tr>
<tr>
<td><em>As a driver, I want AEB for tricycles, so that my automated car doesn’t hit children on tricycles.</em></td>
</tr>
</tbody>
</table>
Situation analysis: Generic operational situation tree

- Properties of a situation classified in a tree structure
- Combine tree leaves to find relevant operational situations

**Situation**: “Automatic drive on highway or rural road with animal obstacle”
Implicit: Valid in all physical environments, road layouts, and speeds.
Hazard identification: Generic hazard tree

- Potential hazards classified in tree structure
- Tactical level hazards new challenge for AD

**Hazardous event:** Hazard "Undetected object" in situation "Automatic drive on highway or rural road with animal obstacle"
Why the trees?

- Escape the focusing effect
  - Forced to consider situations that might be less obvious

- Find potential gaps in analysis
  - Possible to keep track of which properties have been considered

- Structured knowledge base that can be continuously improved

- Reduce risk for ambiguities in situation and hazard definitions
Dimensioning hazardous events*

- Remove HEs that will not make unique safety goal
- Identify missing candidates

# Function refinement

## Input
- Existing requirements
- New provisional list of hazardous events

## Actions
- Refine HEs, function requirements and trees

<table>
<thead>
<tr>
<th>HE</th>
<th>Operational Situation</th>
<th>Hazard</th>
<th>E</th>
<th>C</th>
<th>S</th>
<th>ASIL</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>AD on highway/rural road with animal obst.</td>
<td>Undetected object</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>A</td>
</tr>
<tr>
<td>2</td>
<td>AD with tricycle obstacle</td>
<td>Undetected object</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>B</td>
</tr>
<tr>
<td>3</td>
<td>AD with other vehicle obstacle</td>
<td>Loss of braking</td>
<td>4</td>
<td>3</td>
<td>3</td>
<td>D</td>
</tr>
<tr>
<td>4</td>
<td>AD in bright light with other vehicle obst.</td>
<td>Loss of braking</td>
<td>4</td>
<td>3</td>
<td>3</td>
<td>D</td>
</tr>
<tr>
<td>5</td>
<td>AD in high speed with stationary object obst.</td>
<td>Mode confusion</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>A</td>
</tr>
</tbody>
</table>
Function refinement - AEB

- Break down HEs too abstract or general to use for requirements and safety goals
  - Difficult to handle small and fast animals → AEB handles only heavy land animals
- Identify HEs where restricting the scope of the function is necessary
  - AEB feasible only on highways → Tricycles very rare and becomes QM
- Identify HEs that will increase the scope of the function and add new requirements
  - Expand scope to stationary objects

<table>
<thead>
<tr>
<th>HE</th>
<th>Operational Situation</th>
<th>Hazard</th>
<th>E</th>
<th>C</th>
<th>S</th>
<th>ASIL</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>AD on highway/rural road with animal obst.</td>
<td>Undetected object</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>A</td>
</tr>
<tr>
<td>1b</td>
<td>AD on highway with land animal &lt;20 kg obst.</td>
<td>Undetected object</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>A</td>
</tr>
<tr>
<td>2</td>
<td>AD with trike obstacle</td>
<td>Undetected object</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>B</td>
</tr>
<tr>
<td>2h</td>
<td>AD on highway with trike/vehicle obstacle</td>
<td>Undetected object</td>
<td>0</td>
<td>3</td>
<td>3</td>
<td>QM</td>
</tr>
<tr>
<td>3</td>
<td>AD on highway with other vehicle obstacle</td>
<td>Loss of braking</td>
<td>4</td>
<td>3</td>
<td>3</td>
<td>D</td>
</tr>
<tr>
<td>5</td>
<td>AD on highway in high speed with stationary object obstacle</td>
<td>Mode confusion</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>A</td>
</tr>
</tbody>
</table>
Reffined function: User story format

<table>
<thead>
<tr>
<th>Automated Emergency Break (AEB) – User stories</th>
</tr>
</thead>
<tbody>
<tr>
<td>As a driver, I want AEB available on highways where my car can drive automatically, so that I don’t risk collisions when I don’t monitor the driving.</td>
</tr>
<tr>
<td>As a driver, I want AEB for crossing heavy land animals, so that my automated car doesn’t run into them.</td>
</tr>
<tr>
<td>As a driver, I want AEB for other motor vehicles, so that my automated car doesn’t hit vehicles making unexpected maneuvers.</td>
</tr>
<tr>
<td>As a driver, I want AEB for stationary objects, so that my automated car doesn’t crash into them.</td>
</tr>
<tr>
<td>As a driver, I want AEB for tricycles, so that my automated car doesn’t hit children on tricycles.</td>
</tr>
</tbody>
</table>
Updated situation tree
When to stop iterating?

- Sufficient situation and hazard coverage
  - Trees fully covered - rationale if not relevant
  - Clear which HEs are within or outside scope

- Clarity for continued design process
  - HEs have right level of abstraction to create useful safety goal
  - Function defined in enough detail to support next steps in design process

- Final set of hazardous events used to create safety goals
- Function requirements used to finalize item definition
Questions?

Reference: