We test autonomous driving systems by simulating different scenarios and checking that the system's behavior is adequate (e.g. no crash, safety distances respected, …)

How to know that the scenarios we use are enough to stress the system and thoroughly test it? We apply the principle of mutation analysis:

○ We create "mutant" systems by changing the original decision taking method
○ We run these mutants on the same scenarios we used on the system

We look at the difference $\Delta$ between the original system's performance and the mutants.

○ If the mutants behave very differently, this shows the strength of our scenarios. We are reassured about the quality of the system
○ If the mutants behave similarly, our scenarios are not stressing some aspect of the system. The mutants point us to some missing scenarios
Optimization-based Falsification

Problem:

\( \mathbf{u} \) : input
\( \mathcal{M}(\mathbf{u}) \) : model
\( \varphi \) : specification in STL

- **Robustness:** \( \mathcal{M}(\mathbf{u}), \varphi \)
  - How robustly \( \mathcal{M}(\mathbf{u}) \) satisfies \( \varphi \)
  - E.g. \( \square (\text{speed < 120}) \)

Solution:

- goal: \( \min |\mathcal{M}(\mathbf{u}), \varphi| \)
- technique: hill-climbing optimization

Robustness

- A configuration is one particular instantiation
- We identify three types of parameters:
  - production parameters (e.g., type of sensors or tires)
  - environmental parameters (e.g., type of road, weather conditions)
  - behavioral parameters (e.g., acceleration, initial velocity)
- A configuration is one particular instantiation

Stability Analysis for Safety of Automotive Multi-Product Lines (Paolo Arcaini)

(1) **Automotive Multi-Product Lines (Multi-PL):**
- We consider Simulink models of automotive systems
- Such models contain different sources of variability
- In [1], we view the automotive product as a Multi-Product Line containing different parameters
- We identify three types of parameters:
  - production parameters (e.g., type of sensors or tires)
  - environmental parameters (e.g., type of road, weather conditions)
  - behavioral parameters (e.g., acceleration, initial velocity)
- A configuration is one particular instantiation

(2) **Robustness:**
- We assess the satisfaction/violation of a safety requirement in a quantitative way
- Robustness (rob) gives the degree of satisfaction/violation of a requirement given an output signal \( w \)

(3) **Instability of Automotive Multi-PLs:**
- If a pair of similar configurations exhibits quite different behaviors in terms of safety (i.e., large difference in robustness), this pair of configurations is a witness of the instability
- Defining similarities and differences requires domain knowledge (that we don’t have)
- Therefore, we search for pairs of configurations that could be unstable
- Those will be inspected by the engineers

(4) **Multi-objective problem:**
- We state the problem of detecting instability as a multi-objective problem
- Let \( \Sigma \) be the set of feasible configurations, \( c,d \) be two configurations, and \( D(c,d) \) be the configuration difference between \( c \) and \( d \). The multi-objective optimization problem is:
  \( \max_{c,d \in \Sigma} \min \{\text{rob}(c), \text{rob}(d)\} \)

(5) **Case study:**
- A car drives on a straight lane and spots an obstacle in front of it
- When the driver pushes the brake pedal, an active safety feature is also triggered
- The active safety feature decides whether and when to shut down the engine (if it is necessary to avoid an accident)

Safety requirement: “The car should not crash into the obstacle; if a collision is unavoidable, the car should collide at the lowest possible speed.”

Robustness: \( \text{rob}(c) = \begin{cases} \text{distance}(c), & \text{if distance}(c) > 0, \\ -\text{V_{collision}}(c), & \text{otherwise}. \end{cases} \)

Production parameters
- T_safe: engine shut down time
- Radius_tire: tires radius
- Power_max: maximum horsepower
- Torque_max: maximum torque
- Weight_car: weight of the car

Environmental parameters
- T_i: initial inter-vehicle time
- V_i: initial car speed
- A_b: backward acceleration

Behavioral parameters
- T_i: initial inter-vehicle time
- T_b: reaction time
- V_i: initial car speed
- R_g: wheel RPM

(6) **Case study - Results:**

<table>
<thead>
<tr>
<th>Config.</th>
<th>rob</th>
<th>T_safe</th>
<th>Power_max</th>
<th>Torque_max</th>
<th>T_i</th>
<th>A_b</th>
<th>T_b</th>
<th>V_i</th>
<th>R_g</th>
</tr>
</thead>
<tbody>
<tr>
<td>c_1^{T_safe}</td>
<td>0.189</td>
<td>3.132</td>
<td>128.041</td>
<td>217.062</td>
<td>3.063</td>
<td>0.881</td>
<td>4.076</td>
<td>54.775</td>
<td></td>
</tr>
<tr>
<td>c_2^{T_safe}</td>
<td>-13.873</td>
<td>3.255</td>
<td>128.041</td>
<td>217.062</td>
<td>3.063</td>
<td>0.881</td>
<td>4.076</td>
<td>54.775</td>
<td></td>
</tr>
<tr>
<td>c_{A_b}</td>
<td>-20.188</td>
<td>4.482</td>
<td>94.084</td>
<td>306.560</td>
<td>2.119</td>
<td>0.825</td>
<td>4.263</td>
<td>68.544</td>
<td></td>
</tr>
<tr>
<td>c_{V_i}</td>
<td>0.333</td>
<td>4.482</td>
<td>94.084</td>
<td>306.560</td>
<td>2.119</td>
<td>0.825</td>
<td>4.263</td>
<td>68.544</td>
<td></td>
</tr>
<tr>
<td>c_{R_g}</td>
<td>0.539</td>
<td>3.366</td>
<td>120.473</td>
<td>447.615</td>
<td>4.547</td>
<td>0.112</td>
<td>1.064</td>
<td>64.748</td>
<td></td>
</tr>
<tr>
<td>c_{V_i}</td>
<td>0.106</td>
<td>3.366</td>
<td>120.473</td>
<td>447.615</td>
<td>4.547</td>
<td>0.106</td>
<td>1.064</td>
<td>64.748</td>
<td></td>
</tr>
</tbody>
</table>

References
