A Clearer and More Concise Approach to Specification of Interfaces for Automotive Software Engineering

Research Purpose: To Realise a Clearer and More Concise Approach to Specification of Interfaces for Automotive Software Engineering

Automotive contracts hinge on clarity and conciseness of:
- Software functional and non-functional interface specification
- Emerging standards such as AUTOSAR are based on UML2
- UML2 semantics is textual and informal
- Emerging Standards do not cater for non-functional aspects

Latest Results: A Temporal Logic Enhanced Tabular Expression

<table>
<thead>
<tr>
<th>Eventually &lt;= 1500μs</th>
<th>Standby</th>
<th>SeatBeltUsed</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Child</td>
<td>Deploy at (x / 2) Nm for 2t μs</td>
</tr>
<tr>
<td></td>
<td>Adult</td>
<td>Deploy at x Nm for t μs</td>
</tr>
<tr>
<td></td>
<td>Empty</td>
<td>Standby</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Eventually &gt; 1500μs</th>
<th>Standby</th>
<th>SeatBeltUsed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Development</td>
<td>Child</td>
<td>Deploy at x Nm for t μs</td>
</tr>
<tr>
<td></td>
<td>Adult</td>
<td>Deploy at (x / 2) Nm for 2t μs</td>
</tr>
<tr>
<td></td>
<td>Empty</td>
<td>Standby</td>
</tr>
</tbody>
</table>

Proposal: Use Trace Function Method (Parnas 2006) and Temporal Logic (Pnueli ’77, Gabbay ’80, Pneuli ’81, Clark 1981) To Realise Clearer and More Concise Interface Specification

- TFM uses a predicate logic augmented for partial functions
- Intended to be concise/ readable without compromising logical rigor
- TMF treats module as a black-box, identifying
- Emerging standards do not cater for non-functional aspects
- Temporal logic used to specify reactive system behaviour over time

Results To Date

- Conference Paper on Formal Methods and Automotive Software
- Co-authored report on AUTOSAR for the European Space Agency
- In-depth analysis of TFM and other trace based methods
- In-depth analysis of logics and models of real time

Next Steps

- Examine TFM in light of the Parnas claim: “Time … often considered special in some inexplicable way, also easily considered as global variable and require no special treatment”
- Currently working on mix of timing requirements, such as periodic events, jitter-free events, to see how TFM expresses these and how a combination of Temporal Logic Enhanced Tabular Expressions would express them
- Demonstrate how UML and AUTOSAR can be made clearer and more concise using Temporal Logic Enhanced Tabular Expressions
- Engagement with industry partner currently under discussion for purposes of validating the method

Fig 1 Airbag Control System

Fig 2 Airbag Functionality Trace Example

Fig 3 Airbag Control System Temporal Logid Enhanced Tabular Expression

1. Eventually within 1500μs, it is detected that, the vehicle is in standby, the seatbelt in use and a child occupies the seat. In this case, the airbag is deployed at half of force x and twice duration t.
2. Eventually within 1500μs, it is detected that, the vehicle is in standby, the seatbelt in use and an adult occupies the seat. In this case, the airbag is not deployed.
3. Eventually within 1500μs, it is detected that, the vehicle is in standby, the seatbelt in use and in force x and duration t.
4. Eventually within 1501μs, it is detected that, the vehicle is in standby, the seatbelt in use and a child occupies the seat. In this case, a development diagnostic is logged.