Model-Based Development of an Adaptive Vehicle Stability Control System

Rasmus Adler, Ina Schaefer, Tobias Schüle
Fraunhofer IESE and TU Kaiserslautern
Germany

Workshop “Modellbasierte Entwicklung eingebetteter Fahrzeugfunktionen”
Berlin
Self-Adaptive Systems

What are the special features of these systems?
adaption of algorithms according to current state of environment
Self-Adaptive Systems

Faults and Environment Changes
Self-Adaptive Systems

- Faults and Environment Changes
- Runtime adaptation
Self-Adaptive Systems

Faults and Environment Changes

Runtime adaptation

Degrade functionality to remain operational by switching to different predetermined configuration
Self-Adaptive Systems

Faults and Environment Changes

Safety Survivability

Runtime adaptation

Degrade functionality to remain operational by switching to different predetermined configuration
Adaptive Systems Development

Adaptation increases design complexity, since

- decentralized adaptation mechanism
- reconfiguration triggers reconfiguration
- complex interdependencies
Adaptive Systems Development

Adaptation increases design complexity, since

- decentralized adaptation mechanism
- reconfiguration triggers reconfiguration
- complex interdependencies

Solution:

- Model-Based Design of Adaptive Systems
- Integrated with Formal Verification of Adaptation Behaviour
Outline

- Case Study: An Adaptive Vehicle Stability Control System
- MARS Modelling Concepts
- Development Process and Verification
- Conclusion and Future Work
Adaptive Vehicle Stability Control

System Architecture

Sensor Components
- v_wheelFR
- v_wheelFL
- v_wheelRL
- v_wheelRR
- ax
- ay
- yaw_rate
- brakeGas_Input
- steering_angle_Input

Controller Components
- Yaw Rate Corrector
- Traction Control
- Steering Angle Delimiter

Actuator Components
- steering_angle_cntrl
- left_brake_cntrl
- right_brake_cntrl
- rear_brake_cntrl
Controller Components

- **steering_angle_Input**
- **v_CarRef**
- **v_yaw**
- **brake**
- **wheel slip**
- **gas**

**Steering Angle Delimiter**

- **delimited_steering_angle**

**Yaw Rate Corrector**

- **corrected_left_brake**
- **corrected_right_brake**
- **corrected_rear_brake**

**Traction Control**

- **delimited_gas**
Main Concepts reducing Design Complexity:

- Modular System Structure
- Propagation of Adaptation by Quality extended Data Types (Datives)
- Separation of Adaptation and Functionality in Components
Qualities

UNAVAILABLE
BASICQT
AVAILABLE
Ay
measured
vYaw_based
V_CarRef
ax_based
wheel_based
SLIP_PROB(low,med,high)
ay_based
vYaw

Ay

BASICQT

V_CarRef

UNAVAILABLE

ay_based

SLIP_PROB(low,med,high)
Adaptive Components

- Input and Output Ports for Functional Data
- Required and Provided Ports for Qualities
- Set of Predetermined Configurations with Pre- and Postconditions on Input and Output Qualities
Component VYawCalc (Adaptation Specification View)

- **yaw_rate**
  - Configuration Measured
  - Pre1
  - P1: VYAW_MEASURED
  - Post1
  - P9 -> SENSOR_BASED

- **v_wheelFR**
  - Configuration SteeringBased
  - Pre2
  - P6: STEERING_ANGLE &
  - (P8: VWHEEL_BASED & SLIP_PROB == low)
  - Post2
  - P9 -> STEERING_BASED

- **v_wheelFL**
  - Configuration FWheelBased
  - Pre3
  - P2: VWHEEL & P3: VWHEEL &
  - P6: STEERING_ANGLE
  - Post3
  - P9 -> FWHEEL_BASED

- **v_wheelRL**
  - Configuration RWheelBased
  - Pre4
  - P4: VWHEEL & P5: VWHEEL
  - Post4
  - P9 -> RWHEEL_BASED

- **v_wheelRR**
  - Configuration AyBased
  - Pre5
  - P7: MEASURED & (P8: AX_BASED ||
  - P8: WHEEL_BASED & SLIP_PROB == low )
  - Post5
  - P9 -> AY_BASED

- **steering_angle Input**
  - Configuration Off
  - Pre6
  - TRUE
  - Post6
  - P9 -> UNAVAILABLE

- **v_CarRef**
  - Configuration Measured
  - Pre6
  - P7: VCARREF
  - Post6
  - P9 -> SENSOR_BASED
Component VYawCalc (Adaptation Specification View)

Configuration AyBased

Pre₅:
P7: measured & (P8: ax_based || (P6: wheel_based && slip_prob == low))
Post₅:
P9 → ay_based

V_CarRef

wheel_based

Ay

measured

vYaw_based

ax_based

wheel_based (SLIP_PROB(low, med, high))

ay_based
Component VYawCalc (Adaptation Specification View)

- **Configuration Measured**
  - Pre1
  - Post1
  - P1: vYaw_mesured
  - P9 \(\rightarrow\) sensor_based

- **Configuration SteeringBased**
  - Pre2
  - Post2
  - P6: steering_angle
  - P9 \(\rightarrow\) steering_based

- **Configuration FWheelBased**
  - Pre3
  - Post3
  - P2: vWheel
  - P3: vWheel
  - P6: steering_angle
  - P9 \(\rightarrow\) fWheel_based

- **Configuration RWheelBased**
  - Pre4
  - Post4
  - P4: vWheel
  - P5: vWheel
  - P9 \(\rightarrow\) rWheel_based

- **Configuration AyBased**
  - Pre5
  - Post5
  - P7: measured
  - P8: wheel_based \&\& SLIP_PROB
  - P9 \(\rightarrow\) ay_based

- **Configuration Off**
  - Pre6
  - Post6
  - TRUE
  - P9 \(\rightarrow\) UNAVAILABLE
## Modelling Adaptation

### Component VYawCalc (Adaptation Specification View)

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Pre 1</th>
<th>Post 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Measured</td>
<td>P1: vYaw measured</td>
<td>P9 → sensor_based</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Pre 2</th>
<th>Post 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>SteeringBased</td>
<td>P6: steering_angle &amp;</td>
<td>P9 → steering_based</td>
</tr>
<tr>
<td></td>
<td>(P7: vWheel_based &amp; SLIP_PROB == low)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Pre 3</th>
<th>Post 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>FWheelBased</td>
<td>P2: vWheel &amp; P3: vWheel &amp; vWheel &amp;</td>
<td>P9 → FWheel_based</td>
</tr>
<tr>
<td></td>
<td>P6: steering_angle</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Pre 4</th>
<th>Post 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>RWheelBased</td>
<td>P4: vWheel &amp; P5: vWheel</td>
<td>P9 → rWheel_based</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Pre 5</th>
<th>Post 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>AyBased</td>
<td>P7: measured &amp; (P8: ax_based</td>
<td></td>
</tr>
<tr>
<td></td>
<td>P8: wheel_based &amp; SLIP_PROB == low)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Pre 6</th>
<th>Post 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Off</td>
<td>TRUE</td>
<td>P9 → UNAVAILABLE</td>
</tr>
</tbody>
</table>

---

**Notes:***
- `vYaw`: Yaw velocity
- `vWheel`: Wheel velocity
- `SLIP_PROB`: Slip probability
- `Pre`: Precondition
- `Post`: Postcondition
- `TRUE`: True
- `FALSE`: False
Modelling Adaptation

Component VYawCalc (Adaptation Specification View)

Configuration Measured
Pre1
P1: vYaw_measured
Post1
P9 \rightarrow sensor_based

Configuration SteeringBased
Pre2
P6: steering_angle &&
(P7: vWheel_based && SLIP_PROB == low)
Post2
P9 \rightarrow steering_based

Configuration FWheelBased
Pre3
P2: vWheel && P3: vWheel &&
P6: steering_angle
Post3
P9 \rightarrow fWheel_based

Configuration RWheelBased
Pre4
P4: vWheel && P5: vWheel
Post4
P9 \rightarrow rWheel_based

Configuration AyBased
Pre5
P7: measured && (P8: ax_based ||
P8: wheel_based && SLIP_PROB == low)
Post5
P9 \rightarrow ay_based

Configuration Off
Pre6
TRUE
Post6
P9 \rightarrow UNAVAILABLE
Modelling Adaptation

Component VYawCalc (Adaptation Specification View)

Configuration Measured
Pre1
P1: vYaw_mesured
Post1
P9 \(\rightarrow\) sensor_based

Configuration SteeringBased
Pre2
P6: steering_angle &
(P7: vWheel_based & SLIP_PROB == low)
Post2
P9 \(\rightarrow\) steering_based

Configuration FWheelBased
Pre3
P2: vWheel & P3: vWheel &
P6: steering_angle
Post3
P9 \(\rightarrow\) fWheel_based

Configuration RWheelBased
Pre4
P4: vWheel & P5: vWheel
Post4
P9 \(\rightarrow\) rWheel_based

Configuration AyBased
Pre5
P7: measured & (P8: ax_based ||
P8: wheel_based & SLIP_PROB == low)
Post5
P9 \(\rightarrow\) ay_based

Configuration Off
Pre6
TRUE
Post6
P9 \(\rightarrow\) UNAVAILABLE
Modelling Adaptation

Component VYawCalc (Adaptation Specification View)

Configuration Measured
Pre1
P1: vYaw_mesured
Post1
P9 → sensor_based

Configuration SteeringBased
Pre2
P6: steering_angle &
(P7: vWheel_based & SLIP_PROB == low)
Post2
P9 → steering_based

Configuration FWheelBased
Pre3
P2: vWheel & P3: vWheel &
P6: steering_angle
Post3
P9 → fWheel_based

Configuration RWheelBased
Pre4
P4: vWheel & P5: vWheel
Post4
P9 → rWheel_based

Configuration AyBased
Pre5
P7: measured & (P8: ax_based ||
P8: wheel_based & SLIP_PROB == low)
Post5
P9 → ay_based

Configuration Off
Pre6
TRUE
Post6
P9 → UNAVAILABLE

P9 → ay_based
Development Process

- MARS Models (GME)
- Simulink Models
- Code Generation (Real Time Workshop)
- Simulation
- Probabilistic Analysis
- SAS Models
- Verification of Adaptation Behaviour
- Theorem Proving
- Model Checking (Averest)
“Is the system stable?”

“Are there divisions by zero?”

“Is configuration C active at point t?”

“Is the value of X always greater than zero?”
System Properties

Classification

adaptation

generic

functionality

application–specific

"Is the system stable?"

"Are there divisions by zero?"

"Is configuration C active at point t?"

"Is the value of X always greater than zero?"
Adaptive Generic Properties

- No module gets stuck in the default configuration ‘off’: 
  \[ AG(c = \text{off} \rightarrow EFc \neq \text{off}) \]

- Every module can reach all configurations at all times: 
  \[ AG(\bigwedge_{i=1}^{n} EFc = \text{config}_i) \]

- No inconsistent states can be reached: 
  \[ AG(\bigvee_{i=1}^{n} c = \text{config}_i) \]

- No configuration is always only transient: 
  \[ \bigwedge_{i=1}^{n} EFEGc = \text{config}_i \]
Properties of VSC System

Controller Modules correctly implement Fail-Safe Layer.

Traction Control:
AG((gas_output.quality = available
  ∧ gas_input.quality = available)
  → ctraction_control ≠ Off)

Steering Angle Delimiter:
AG((steering_angle_input.quality = available
  ∧ steering_angle_servo.quality = available)
  → csteering_angle_delimiter ≠ Off)

Yaw Rate Correction:
AG((wheel_brakeFL.quality = available
  ∧ wheel_brakeFR.quality = available
  ∧ wheel_rearBrake.quality = available
  ∧ brake_input.quality = available
  → cyaw_rate_corrector ≠ Off)
Experimental Results

Characteristics of Vehicle Stability Control System

<table>
<thead>
<tr>
<th>Number of components</th>
<th>28</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of configurations</td>
<td>70</td>
</tr>
<tr>
<td>Lines of code</td>
<td>$\approx 2500$</td>
</tr>
<tr>
<td>Number of reachable states</td>
<td>$\approx 5 \cdot 10^{18}$</td>
</tr>
<tr>
<td>Number of properties</td>
<td>151</td>
</tr>
</tbody>
</table>

Analysis Times for Generic Adaptive Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Time [seconds]</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Min.</td>
</tr>
<tr>
<td>P1 (liveness)</td>
<td>&lt; 0.1</td>
</tr>
<tr>
<td>P2 (reachability)</td>
<td>&lt; 0.1</td>
</tr>
<tr>
<td>P3 (safety)</td>
<td>&lt; 0.1</td>
</tr>
<tr>
<td>P4 (persistence)</td>
<td>&lt; 0.1</td>
</tr>
</tbody>
</table>
Related Work

Modelling and Verification of Adaptive Systems

- [Bradbury et al.; 2004]:
  Survey on Self-Managed Software Architectures

- [Zhang, Cheng; 2005/06]:
  Modelling and Verification of Adaptation Behaviour based on Petri Nets

- [Schneider, Schüle, Trapp; 2006]:
  Direct Translation of Modelling Concepts to Verification Tools
Conclusion

- Modelling Concepts for Adaptive Systems
- Integration of Model-based Development and Formal Verification
Future Work

- Extension of Modelling Concepts with Intuitive Property Specification at Modelling Level
- Further Development of Verification Techniques
- Propagation of Verification Results back to Modelling Level