Slicing for Model Reduction in Adaptive Embedded Systems Development

Ina Schaefer and Arnd Poetzsch-Heffter
Software Technology Group,
TU Kaiserslautern, Germany

12 May 2008
Adaptive Embedded Systems

- Embedded systems often operate in safety-critical domains.
- Adaptation and graceful degradation increase safety and survivability.

Goal: Formal verification of adaptation behaviour.
Adaptive Systems
Adaptive Systems

Environment

Adaptation Sequence Chart

yaw_rate

steering_angle

measured

measured

t
Adaptive Systems

Environment

Yaw Rate Sensor unavail

Adaptation Sequence Chart

yaw_rate
measured

steering_angle
measured

t

3
Adaptive Systems

Environment

Yaw Rate Sensor unavail

Adaptation Sequence Chart

By Steering Angle

measured

steering_angle

measured

measured

yaw_rate
Adaptive Systems

Environment

Yaw Rate Sensor unavail

Steering Angle unavail

Adaptation Sequence Chart

By Steering Angle

yaw_rate

measured

steering_angle

measured

measured

t
Adaptive Systems

Environment

Yaw Rate Sensor unavail
Steering Angle unavail

Adaptation Sequence Chart

By Steering Angle
measured
By Steering Angle
steering_angle
measured

measured
Off

yaw_rate
steering_angle

Environment

Adaptive Systems

Yaw Rate Sensor unavail
Steering Angle unavail

Adaptation Sequence Chart

By Steering Angle
measured
By Steering Angle
steering_angle
measured

measured
Off

yaw_rate
steering_angle

Environment

Adaptive Systems

Yaw Rate Sensor unavail
Steering Angle unavail

Adaptation Sequence Chart

By Steering Angle
measured
By Steering Angle
steering_angle
measured

measured
Off

yaw_rate
steering_angle

Environment

Adaptive Systems

Yaw Rate Sensor unavail
Steering Angle unavail

Adaptation Sequence Chart

By Steering Angle
measured
By Steering Angle
steering_angle
measured

measured
Off

yaw_rate
steering_angle

Environment

Adaptive Systems

Yaw Rate Sensor unavail
Steering Angle unavail

Adaptation Sequence Chart

By Steering Angle
measured
By Steering Angle
steering_angle
measured

measured
Off

yaw_rate
steering_angle

Environment

Adaptive Systems

Yaw Rate Sensor unavail
Steering Angle unavail

Adaptation Sequence Chart

By Steering Angle
measured
By Steering Angle
steering_angle
measured

measured
Off

yaw_rate
steering_angle

Environment

Adaptive Systems

Yaw Rate Sensor unavail
Steering Angle unavail

Adaptation Sequence Chart

By Steering Angle
measured
By Steering Angle
steering_angle
measured

measured
Off

yaw_rate
steering_angle

Environment

Adaptive Systems

Yaw Rate Sensor unavail
Steering Angle unavail

Adaptation Sequence Chart

By Steering Angle
measured
By Steering Angle
steering_angle
measured

measured
Off

yaw_rate
steering_angle

Environment

Adaptive Systems

Yaw Rate Sensor unavail
Steering Angle unavail

Adaptation Sequence Chart

By Steering Angle
measured
By Steering Angle
steering_angle
measured

measured
Off

yaw_rate
steering_angle

Environment

Adaptive Systems

Yaw Rate Sensor unavail
Steering Angle unavail

Adaptation Sequence Chart

By Steering Angle
measured
By Steering Angle
steering_angle
measured

measured
Off

yaw_rate
steering_angle

Environment

Adaptive Systems

Yaw Rate Sensor unavail
Steering Angle unavail

Adaptation Sequence Chart

By Steering Angle
measured
By Steering Angle
steering_angle
measured

measured
Off

yaw_rate
steering_angle

Environment

Adaptive Systems

Yaw Rate Sensor unavail
Steering Angle unavail

Adaptation Sequence Chart

By Steering Angle
measured
By Steering Angle
steering_angle
measured

measured
Off

yaw_rate
steering_angle

Environment

Adaptive Systems

Yaw Rate Sensor unavail
Steering Angle unavail

Adaptation Sequence Chart

By Steering Angle
measured
By Steering Angle
steering_angle
measured

measured
Off

yaw_rate
steering_angle

Environment

Adaptive Systems

Yaw Rate Sensor unavail
Steering Angle unavail

Adaptation Sequence Chart

By Steering Angle
measured
By Steering Angle
steering_angle
measured

measured
Off

yaw_rate
steering_angle

Environment

Adaptive Systems

Yaw Rate Sensor unavail
Steering Angle unavail

Adaptation Sequence Chart

By Steering Angle
measured
By Steering Angle
steering_angle
measured

measured
Off

yaw_rate
steering_angle

Environment

Adaptive Systems

Yaw Rate Sensor unavail
Steering Angle unavail

Adaptation Sequence Chart

By Steering Angle
measured
By Steering Angle
steering_angle
measured

measured
Off

yaw_rate
steering_angle

Environment

Adaptive Systems

Yaw Rate Sensor unavail
Steering Angle unavail

Adaptation Sequence Chart

By Steering Angle
measured
By Steering Angle
steering_angle
measured

measured
Off

yaw_rate
steering_angle

Environment

Adaptive Systems

Yaw Rate Sensor unavail
Steering Angle unavail

Adaptation Sequence Chart

By Steering Angle
measured
By Steering Angle
steering_angle
measured

measured
Off

yaw_rate
steering_angle

Environment

Adaptive Systems

Yaw Rate Sensor unavail
Steering Angle unavail

Adaptation Sequence Chart

By Steering Angle
measured
By Steering Angle
steering_angle
measured

measured
Off

yaw_rate
steering_angle

Environment

Adaptive Systems

Yaw Rate Sensor unavail
Steering Angle unavail

Adaptation Sequence Chart

By Steering Angle
measured
By Steering Angle
steering_angle
measured

measured
Off

yaw_rate
steering_angle

Environment

Adaptive Systems

Yaw Rate Sensor unavail
Steering Angle unavail

Adaptation Sequence Chart

By Steering Angle
measured
By Steering Angle
steering_angle
measured

measured
Off

yaw_rate
steering_angle

Environment

Adaptive Systems

Yaw Rate Sensor unavail
Steering Angle unavail

Adaptation Sequence Chart

By Steering Angle
measured
By Steering Angle
steering_angle
measured

measured
Off

yaw_rate
steering_angle

Environment

Adaptive Systems

Yaw Rate Sensor unavail
Steering Angle unavail

Adaptation Sequence Chart

By Steering Angle
measured
By Steering Angle
steering_angle
measured

measured
Off

yaw_rate
steering_angle

Environment

Adaptive Systems

Yaw Rate Sensor unavail
Steering Angle unavail

Adaptation Sequence Chart

By Steering Angle
measured
By Steering Angle
steering_angle
measured

measured
Off

yaw_rate
steering_angle

Environment

Adaptive Systems

Yaw Rate Sensor unavail
Steering Angle unavail

Adaptation Sequence Chart

By Steering Angle
measured
By Steering Angle
steering_angle
measured

measured
Off

yaw_rate
steering_angle

Environment

Adaptive Systems

Yaw Rate Sensor unavail
Steering Angle unavail

Adaptation Sequence Chart

By Steering Angle
measured
By Steering Angle
steering_angle
measured

measured
Off

yaw_rate
steering_angle

Environment

Adaptive Systems

Yaw Rate Sensor unavail
Steering Angle unavail

Adaptation Sequence Chart

By Steering Angle
measured
By Steering Angle
steering_angle
measured

measured
Off

yaw_rate
steering_angle

Environment

Adaptive Systems

Yaw Rate Sensor unavail
Steering Angle unavail

Adaptation Sequence Chart

By Steering Angle
measured
By Steering Angle
steering_angle
measured

measured
Off

yaw_rate
steering_angle

Environment

Adaptive Systems

Yaw Rate Sensor unavail
Steering Angle unavail

Adaptation Sequence Chart

By Steering Angle
measured
By Steering Angle
steering_angle
measured

measured
Off

yaw_rate
steering_angle

Environment

Adaptive Systems

Yaw Rate Sensor unavail
Steering Angle unavail

Adaptation Sequence Chart

By Steering Angle
measured
By Steering Angle
steering_angle
measured

measured
Off

yaw_rate
steering_angle

Environment

Adaptive Systems

Yaw Rate Sensor unavail
Steering Angle unavail

Adaptation Sequence Chart

By Steering Angle
measured
By Steering Angle
steering_angle
measured

measured
Off

yaw_rate
steering_angle

Environment

Adaptive Systems

Yaw Rate Sensor unavail
Steering Angle unavail

Adaptation Sequence Chart

By Steering Angle
measured
By Steering Angle
steering_angle
measured

measured
Off

yaw_rate
steering_angle

Environment

Adaptive Systems

Yaw Rate Sensor unavail
Steering Angle unavail

Adaptation Sequence Chart

By Steering Angle
measured
By Steering Angle
steering_angle
measured

measured
Off

yaw_rate
steering_angle

Environment
Adaptive Systems

Environment

Yaw Rate Sensor unavail

Steering Angle unavail

Adaptation Sequence Chart

By Steering Angle

quality = unavail

Off

measured

measured

yaw_rate

steering_angle

3
Adaptive Systems

Environment

Yaw Rate Sensor unavail
Steering Angle unavail

Adaptation Sequence Chart

By Steering Angle
measured

By Steering Angle
measured

By Wheels
Off

Steering_angle

yaw_rate
measured

quality = unavail

measured
measured

Off
Off

t
The Gap...

Adaptive System Models and Properties

Verification Tools
The Gap...

- Models are too large for automatic verification.
- Internal structure of models cannot be represented.
- Data types and operations used in models are not supported by verification tools.
Bridging the Gap....

Adaptive System Models and Properties

Verification Tools
Bridging the Gap....

Formal Intermediate Layer

Adaptive System Models and Properties

Verification Tools
Bridging the Gap....

Formal Intermediate Layer

Adaptive System Models and Properties

SAS + Property

Verification Tools
Bridging the Gap....

Formal Intermediate Layer

Adaptive System Models and Properties

SAS + Property

Model Reduction

SAS’ + Property’

Verification Tools
Bridging the Gap....

Formal Intermediate Layer

Adaptive System Models and Properties

SAS + Property

Model Reduction

SAS' + Property'

Verification Tools
Bridging the Gap....

Formal Intermediate Layer

Adaptive System Models and Properties

SAS + Property

Model Reduction by Slicing

SAS’ + Property’

Verification Tools
Outline

- Formal Intermediate Models and Properties
- Slicing for Model Reduction
- Experimental Evaluation
- Conclusion and Outlook
Synchronous Adaptive Systems (SAS)
Synchronous Adaptive Systems (SAS)

SAS Module
Synchronous Adaptive Systems (SAS)

SAS Module

Configuration 1

next_state
next_out
Guard

Local State

Configuration m

next_state
next_out
Guard

in
out

 [...]
Synchronous Adaptive Systems (SAS)

SAS Module

Adaptation Aspect

adapt_in

adapt_out

in

out

next_state

next_out

Guard

Local State

Configuration 1

Configuration m

next_state

next_out

Guard

[...]

Local State

Configuration 1

Configuration m
Synchronous Adaptive Systems (2)

SAS System

M1 → M2

M2 → M3

M3 → M4

M4 → M2
Synchronous Adaptive Systems (2)

SAS System

M₁ → M₂ → M₃ → M₄

Diagram showing the interconnections between M₁, M₂, M₃, and M₄ in a SAS System.
Properties of Adaptation Behaviour

* No module gets stuck in the default configuration ‘off’:
  \[ AG \left( useconf = Off \rightarrow EF \ useconf \neq Off \right) \]

* Every module can reach all configurations at all times:
  \[ AG \left( \bigwedge_i EF \ useconf = config_i \right) \]

* No inconsistent states can be reached:
  \[ AG \left( \bigvee_i useconf = config_i \right) \]

* No configuration is always only transient:
  \[ \bigwedge_i EF \ EG \ useconf = config_i \]
Integration Framework

Formal Intermediate Layer

Adaptive System Models and Properties → SAS + Property → SAS’ + Property’ ← Verification Tools

Model Reduction by Slicing
**Theorem 1**  (Preservation by Bisimulation).

Let $T$ and $\hat{T}$ be two SAS transition systems and $\varphi$ a property such that $T$ and $\hat{T}$ are consistently bisimilar with respect to $\varphi$, $T \cong_{[\varphi]} \hat{T}$. Then, $\hat{T} \models \varphi$ is true iff $T \models \varphi$ is true.
Slicing of Intermediate Models

- Slicing on System Level
- Slicing on Module Level
- Adaptive Slicing
System Slicing
\[ AG \ (x_3 > 0 \land \text{useconf}_3 = \text{derived}) \]
System Slicing

\[ AG \left( x_3 > 0 \land \text{useconf}_3 = \text{derived} \right) \]
AG ( x_3 > 0 && useconf_3 = derived)
AG (x₃ > 0 && useconf₃ = derived)
Module Slicing

Adaptation Aspect

Configuration 1
- next_state
- next_out
- Guard

Local State

Configuration m
- next_state
- next_out
- Guard

adaptn_in

adaptn_out

in1

out1

in2

out2

...
Module Slicing

adapt_in → Adaptation Aspect → adapt_out

in_1 → next_state
next_out
Guard

next_state
next_out
Guard

Configuration 1

[in...]

Configuration m

A G ( in_1 > 0 → out_1 = 5)
Module Slicing

Adaptation Aspect

Configuration 1

next_state
next_out
Guard

Local State

Configuration m

A G ( in_1 > 0 \rightarrow out_1 = 5)
Module Slicing

Adaptation Aspect

A G (in₁ > 0 \rightarrow out₁ = 5)
Module Slicing

Adaptation Aspect

[...]

Local State

next_state

next_out

Guard

Configuration 1

in_1

out_1

adapt_in

adapt_out

A G ( in_1 > 0 \rightarrow out_1 = 5 )
Module Slicing is iteratively performed on system modules.
Adaptive Slicing

M_1 → M_2 → M_3 → M_4
Adaptive Slicing

AG (useconf = Off → EF useconf ≠ Off)
Adaptive Slicing

AG ( useconf = Off $\rightarrow$ EF useconf $\neq$ Off )
## Experimental Evaluation

### Case Study: Adaptive Vehicle Stability Control System

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Modules</td>
<td>20</td>
</tr>
<tr>
<td>Number of Configurations</td>
<td>70</td>
</tr>
<tr>
<td>Lines of Generated Code</td>
<td>40 k</td>
</tr>
<tr>
<td>Number of Reachable States</td>
<td>$\approx 5 \times 10^{18}$</td>
</tr>
</tbody>
</table>

Properties verified:

- All modules satisfy generic adaptation properties.
- Controller modules correctly implement of fallback layer.
Experimental Evaluation

![Graph showing analysis time for different systems]

- Averest (generic)
- Averest (fail-safe)
- NuSMV (generic)
- NuSMV (fail-safe)

Legend:
- Original System
- Adaptive Sliced
- System Sliced
- Module Sliced
Related Work


- Slicing for model checking, e.g.
  - Cone of influence reduction [Clarke et al.:1999]
  - BANDERA [Hatcliff et al.:2000]
  - SPIN [Millett & Teitelbaum:2000]

- Slicing of Design Level Models, e.g.
  - Software Architectures [Colangelo et al.:2006]
  - SAL [Bensalem et al., 2000]
  - IF [Bozga et al., 2004]
Conclusion

Main Results:

- Integration of model-based development with formal verification for adaptive systems
- Automatic verification complexity reduction by slicing of design models
Future Work

- More fine-grained property analysis for better reductions by slicing
- Further verification complexity reduction by abstraction and compositional reasoning