Model-Based Development of an Adaptive Vehicle Stability Control System

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

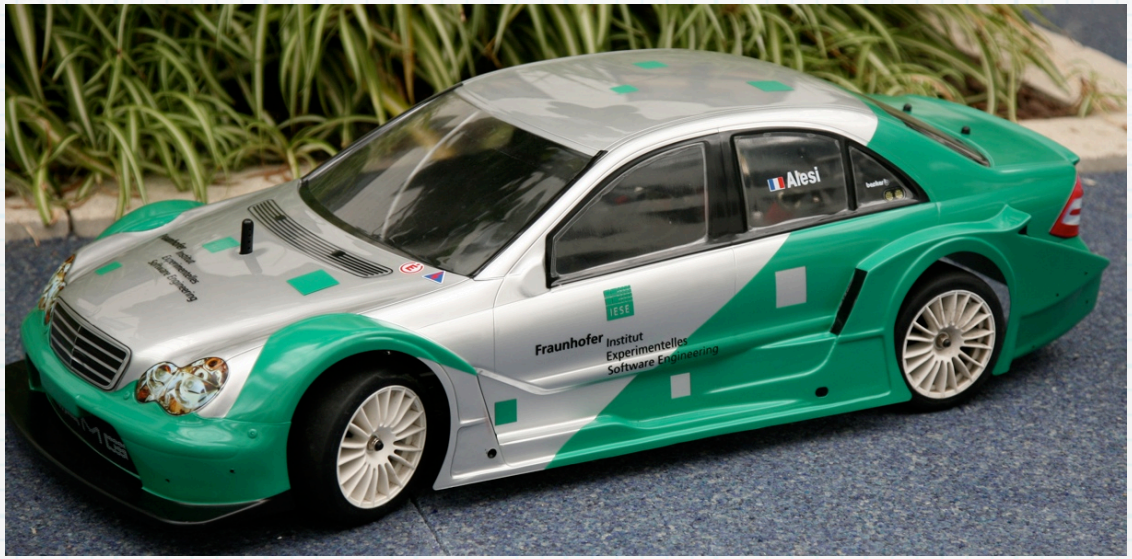
Workshop "Modellbasierte Entwicklung eingebetteter Fahrzeugfunktionen"
14. März 2008
Berlin

Technische Universität Kaiserslautern

SoFTeX Arbeitsgruppe Softwaretechnik

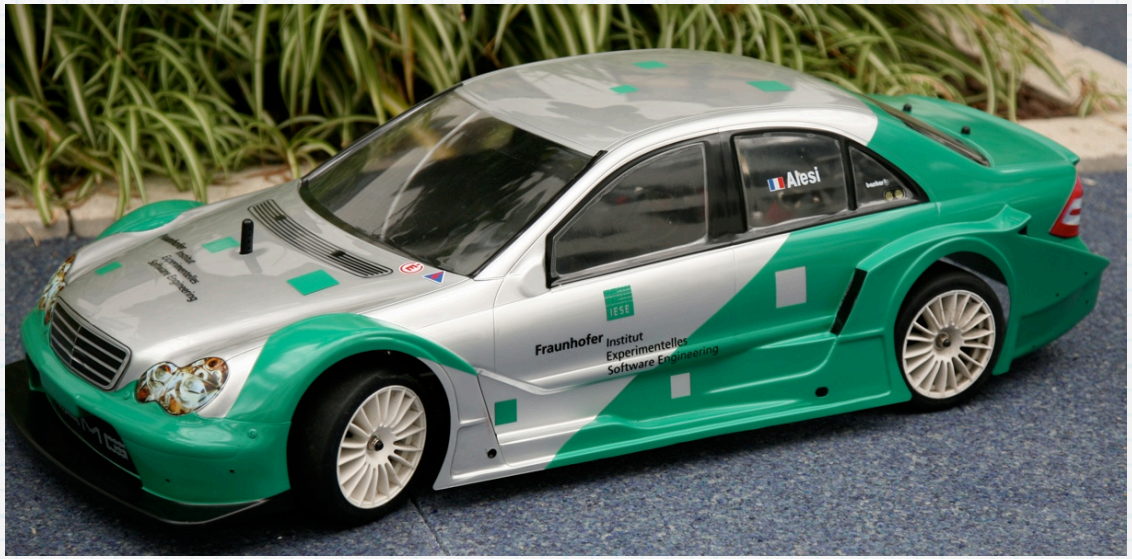
DASMOD Dependable Adaptive Systems and Mathematical Modeling

Self-Adaptive Systems

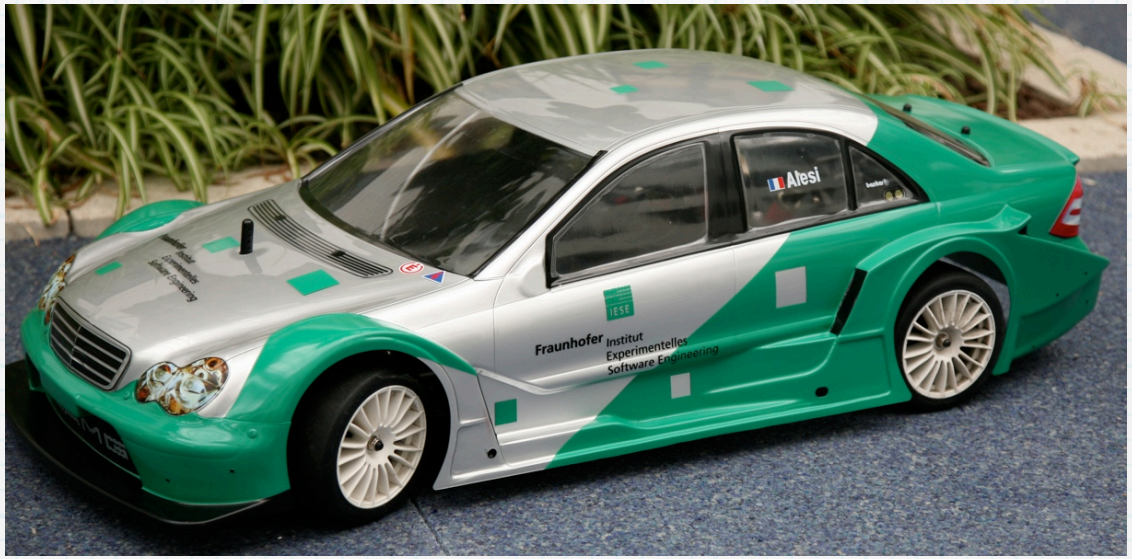


Self-Adaptive Systems

Faults and Environment Changes



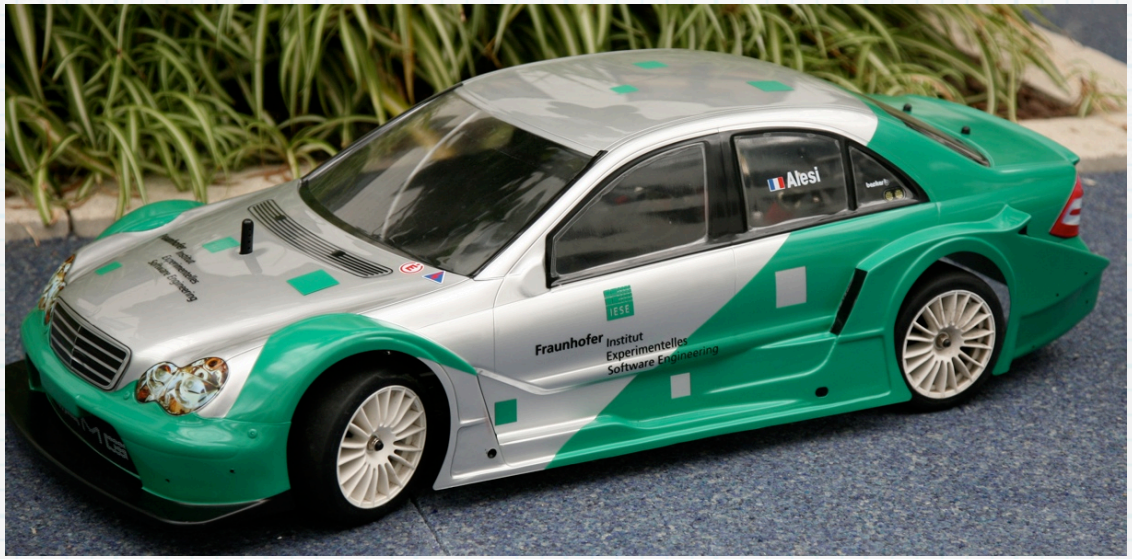
Self-Adaptive Systems



Faults and Environment Changes

Runtime adaptation

Self-Adaptive Systems

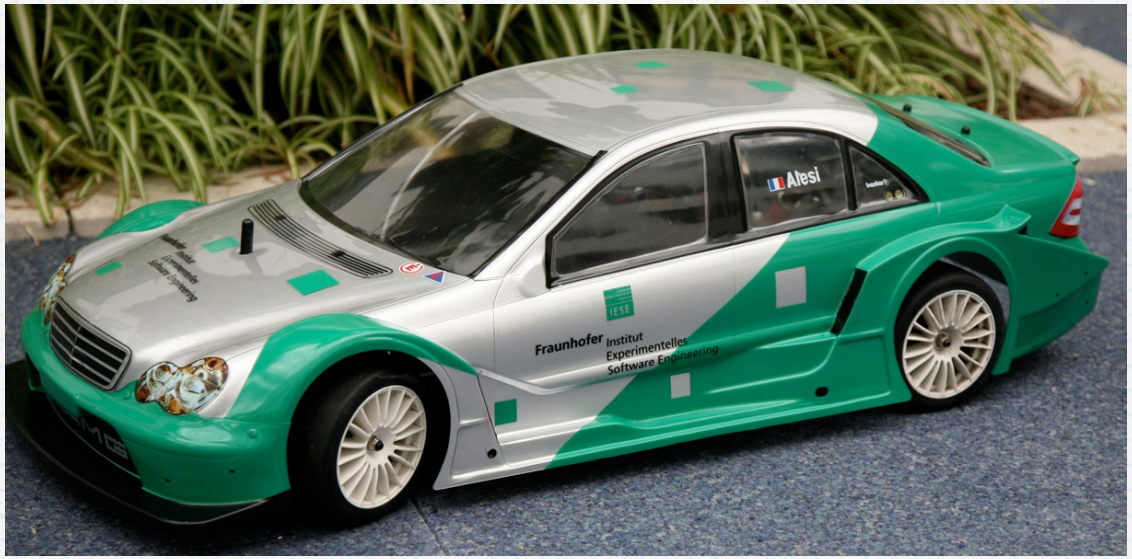


Faults and Environment Changes

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:

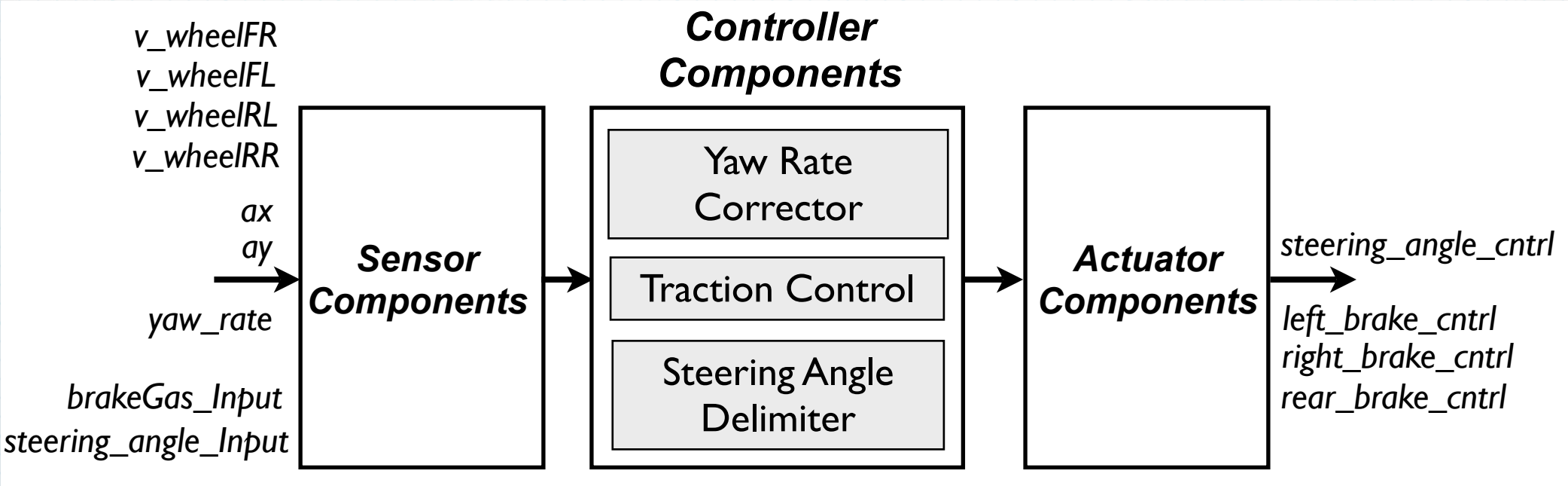
- **Model-Based Design of Adaptive Systems**
- **Integrated with Formal Verification of Adaptation Behaviour**

Outline

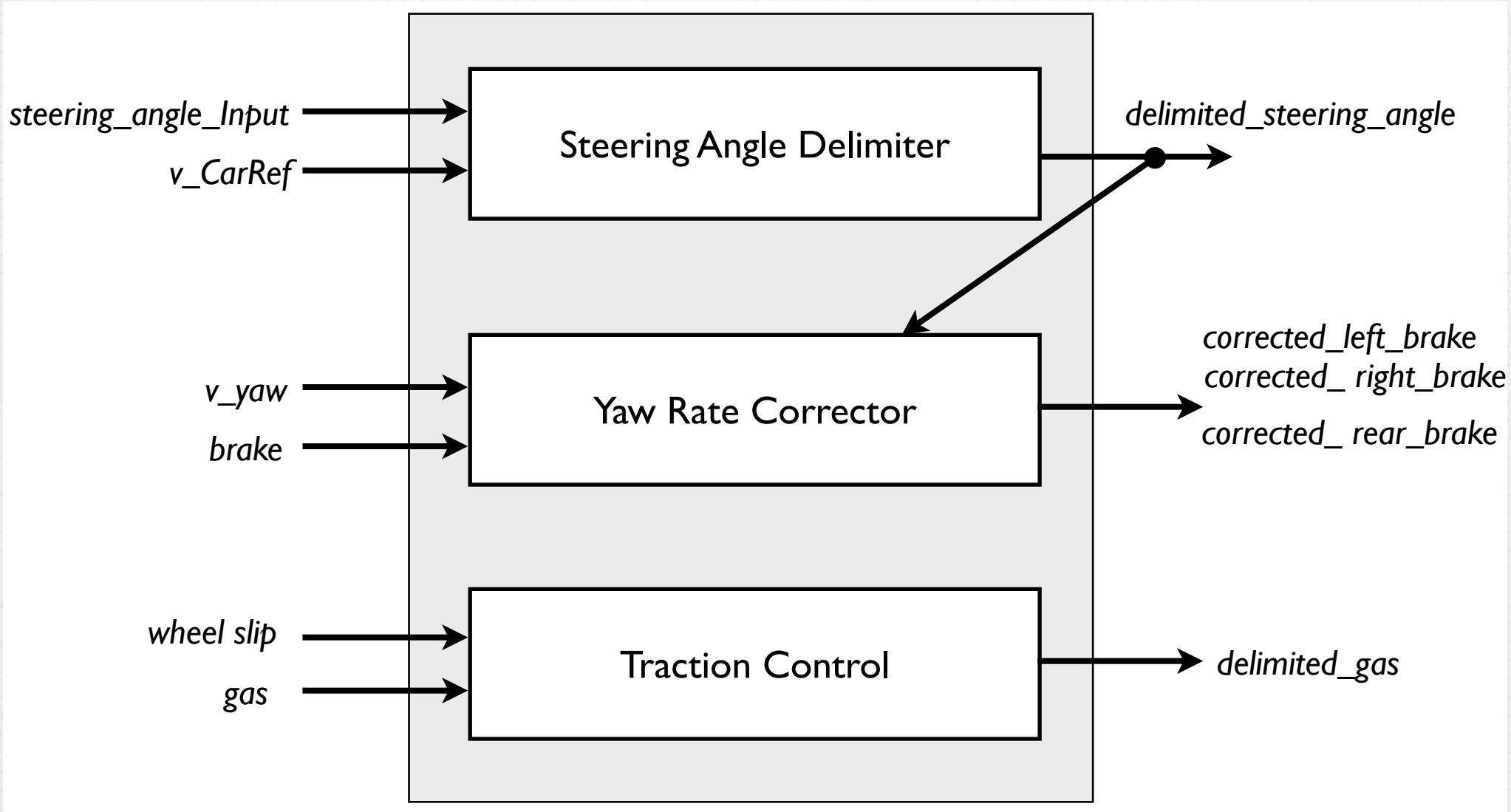
- Case Study: An Adaptive Vehicle Stability Control System
- MARS Modelling Concepts
- Development Process and Verification
- Conclusion and Future Work

Adaptive Vehicle Stability Control

System Architecture



Controller Components

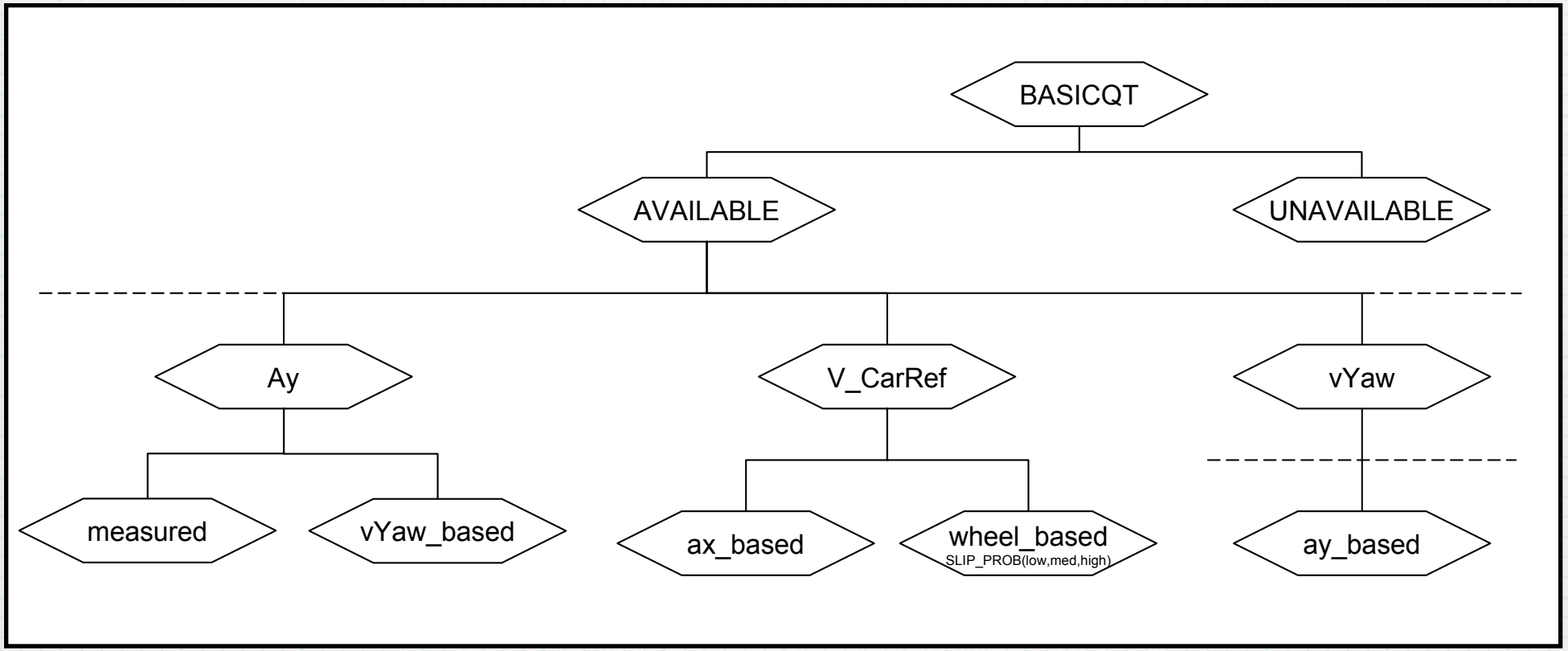


Adaptive System Modelling (MARS)

Main Concepts reducing Design Complexity:

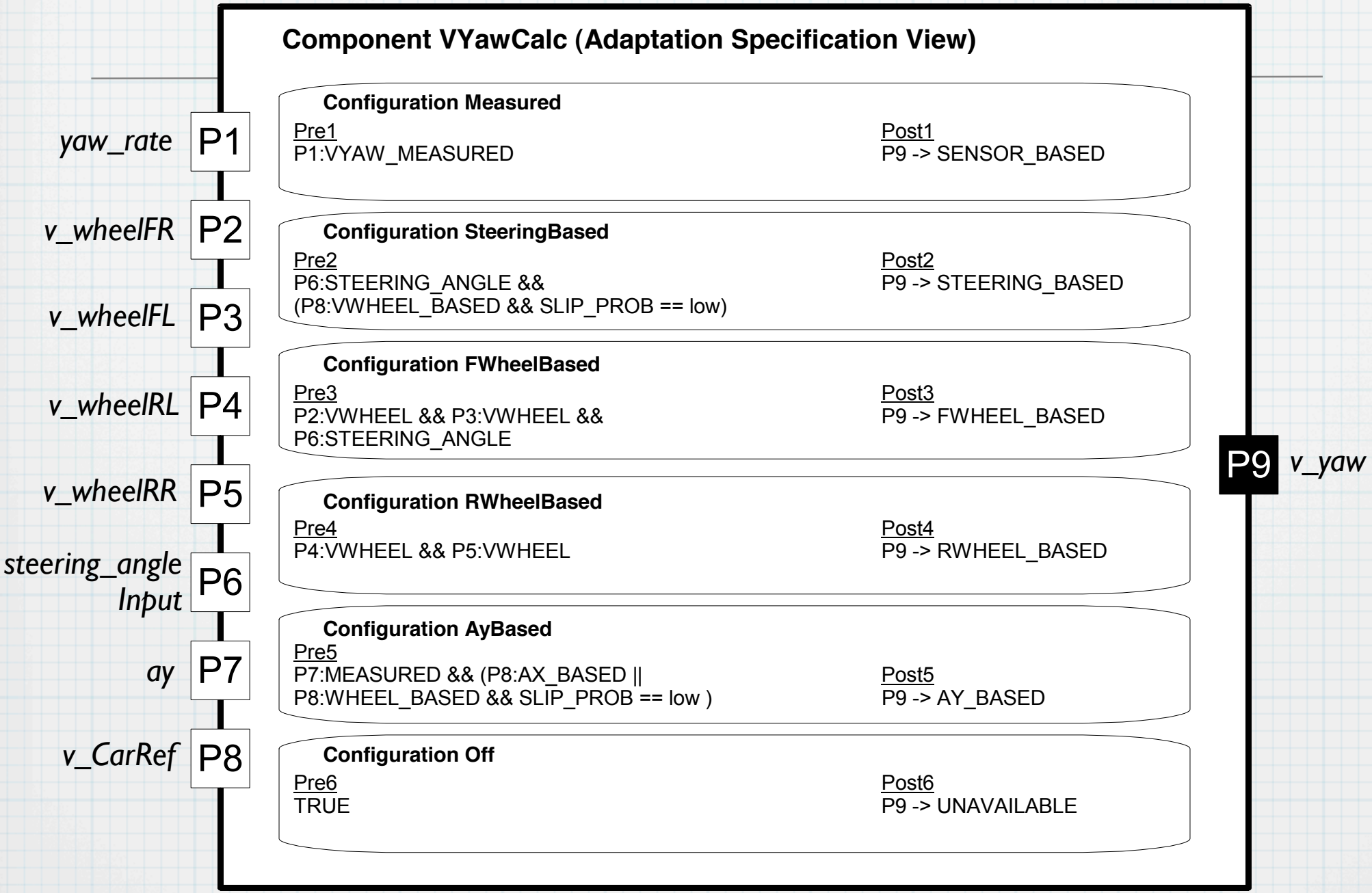
- **Modular System Structure**
- **Propagation of Adaptation by Quality extended Data Types (Datives)**
- **Separation of Adaptation and Functionality in Components**

Qualities

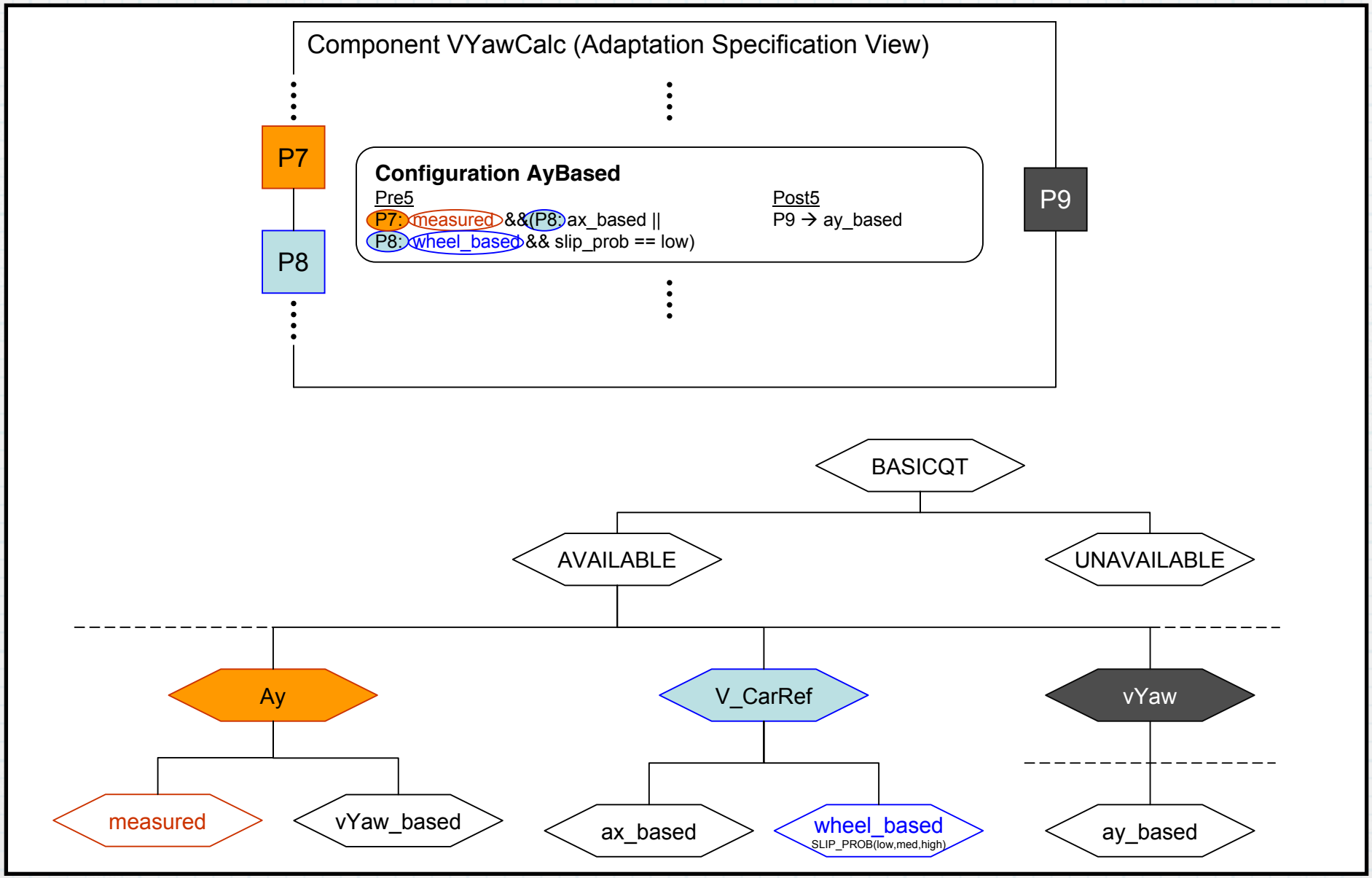

BASICQT
AVAILABLE
UNAVAILABLE
Ay
V_CarRef
vYaw
measured
vYaw_based
ax_based
wheel_based
SLIP_PROB(low,med,high)
ay_based

Adaptive Components

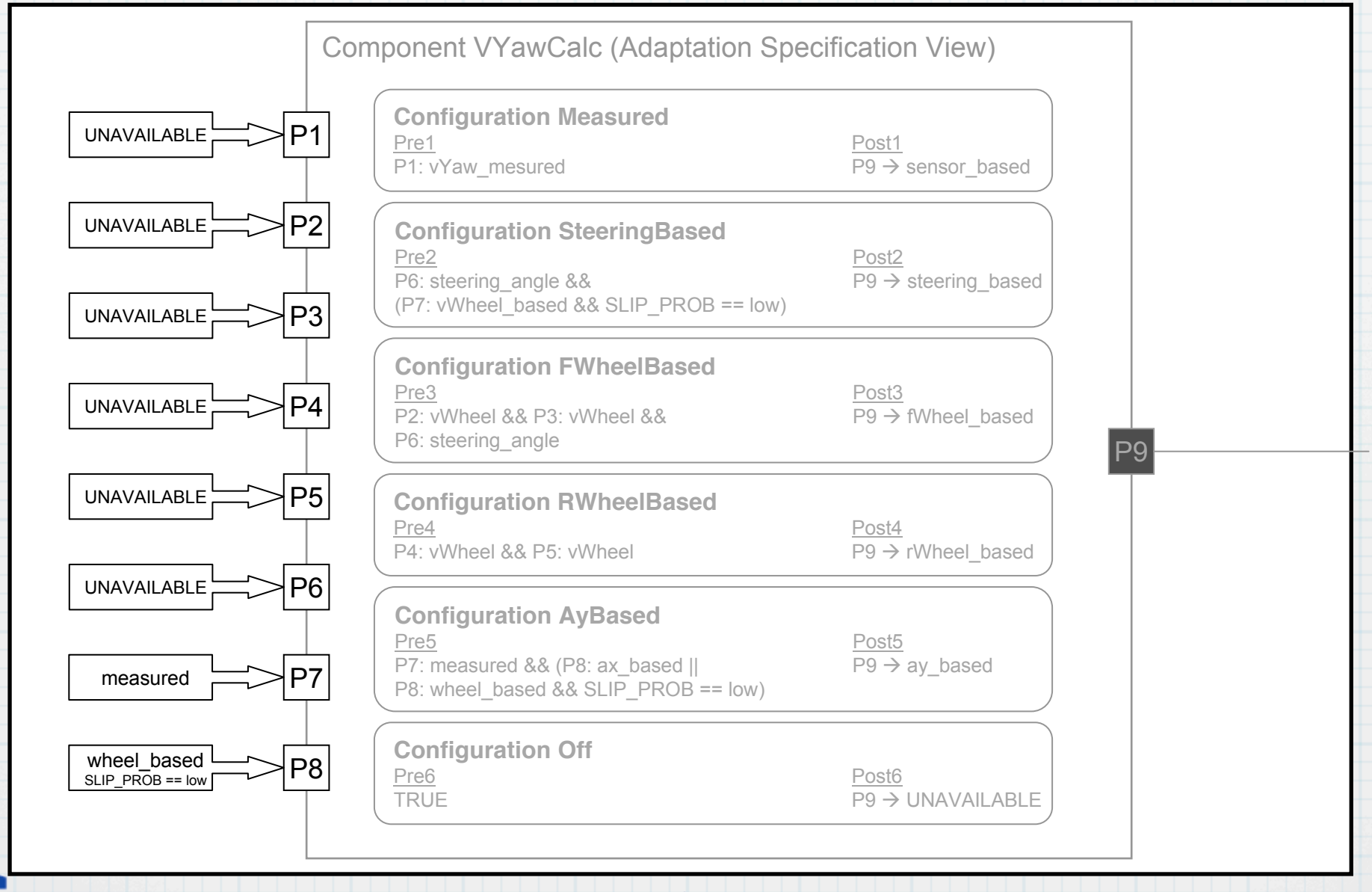
- Input and Output Ports for Functional Data
- Required and Provided Ports for Qualities
- Set of Predetermined Configurations with Pre- and Postconditions on Input and Output Qualities


Component VYawCalc (Adaptation Specification View)
yaw_rate
P1
v_wheelFR
P2
v_wheelFL
P3
v_wheelRL
P4
v_wheelRR
P5
steering_angle Input
P6
ay
P7
v_CarRef
P8
Configuration Measured
Pre1
P1:VYAW_MEASURED
Post1
P9 -> SENSOR_BASED
Configuration SteeringBased
Pre2
P6:STEERING_ANGLE &&
(P8: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
v_yaw

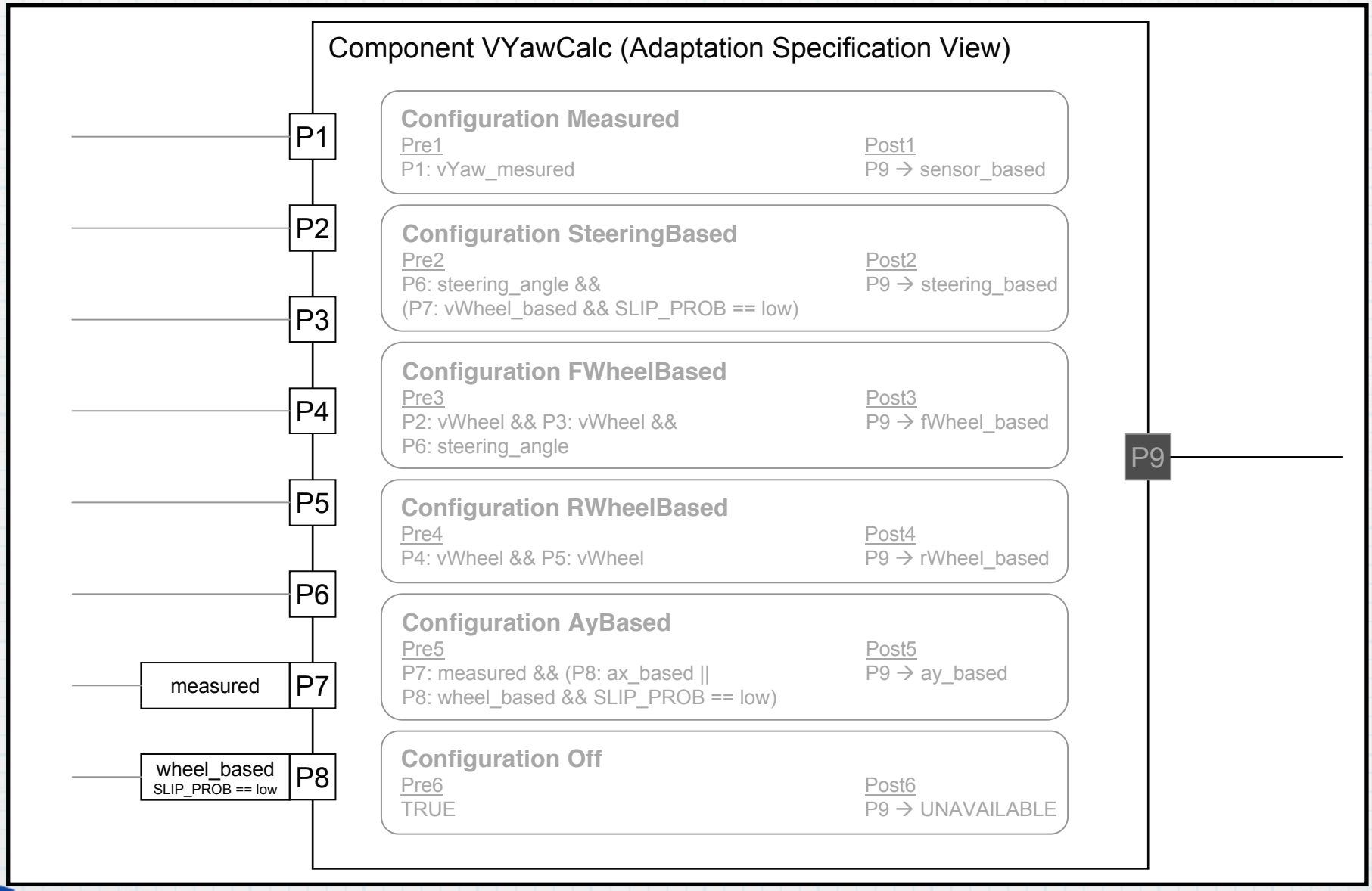
Adaptive Components (3)



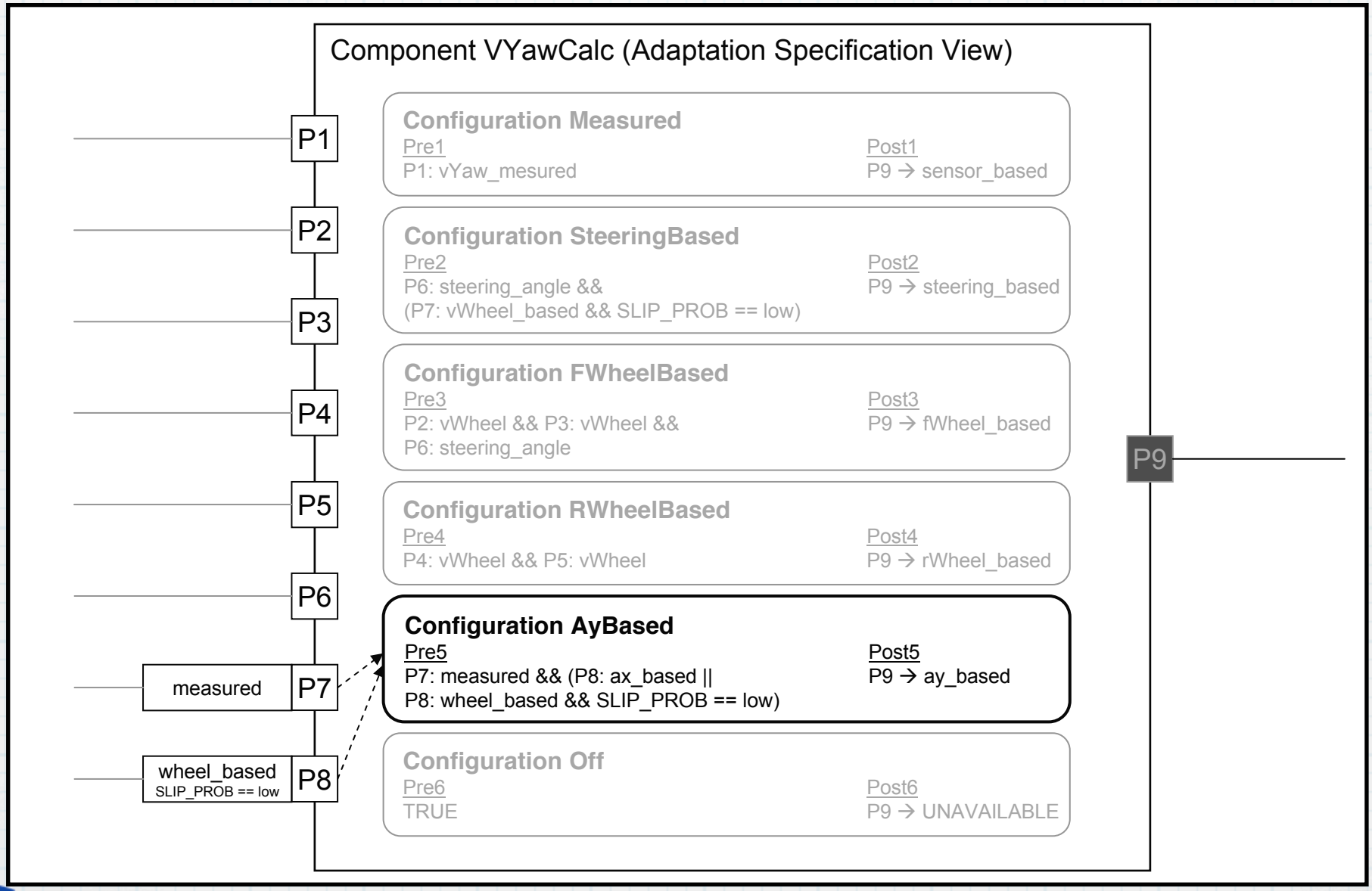
Modelling Adaptation



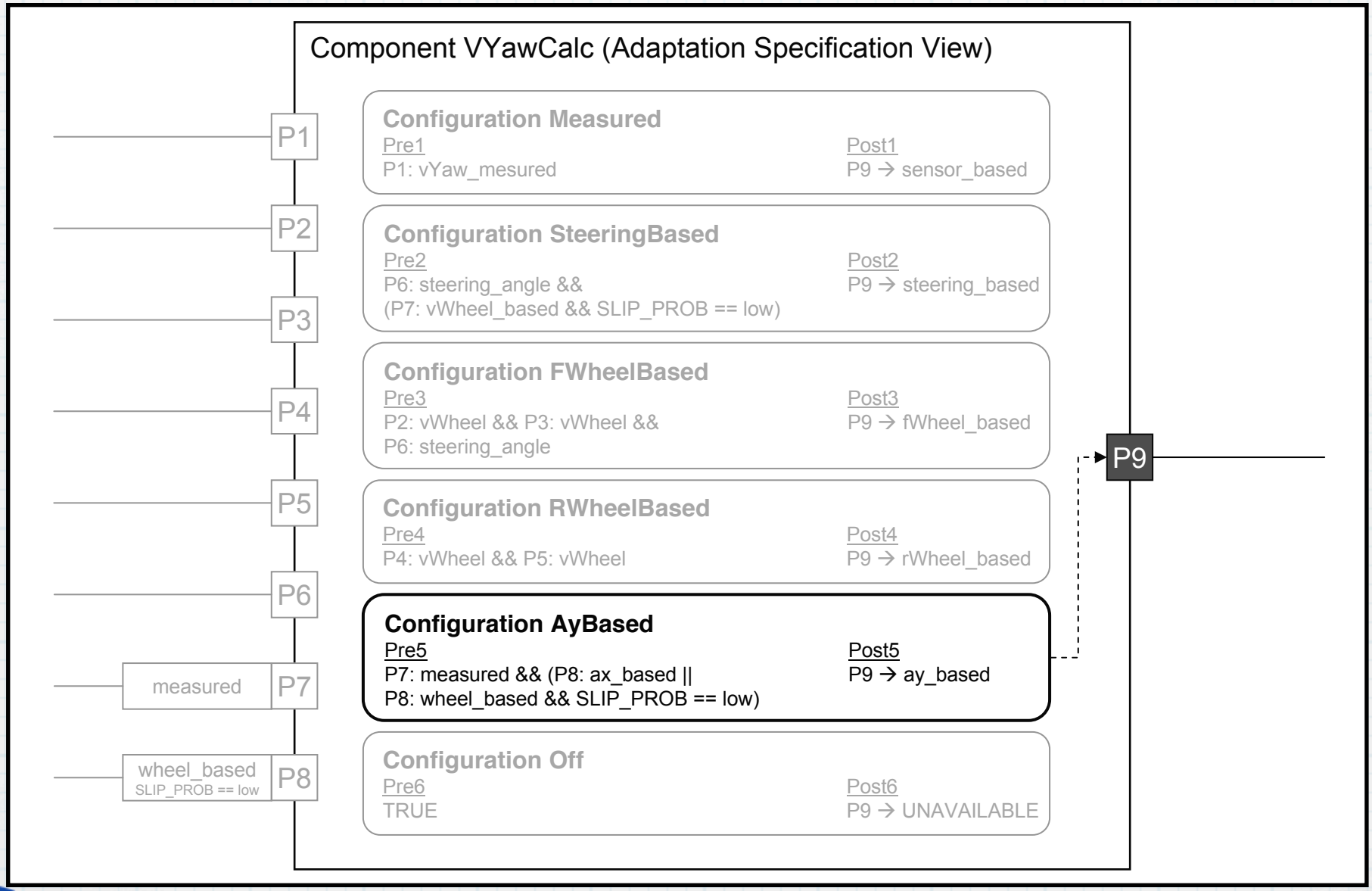
Modelling Adaptation



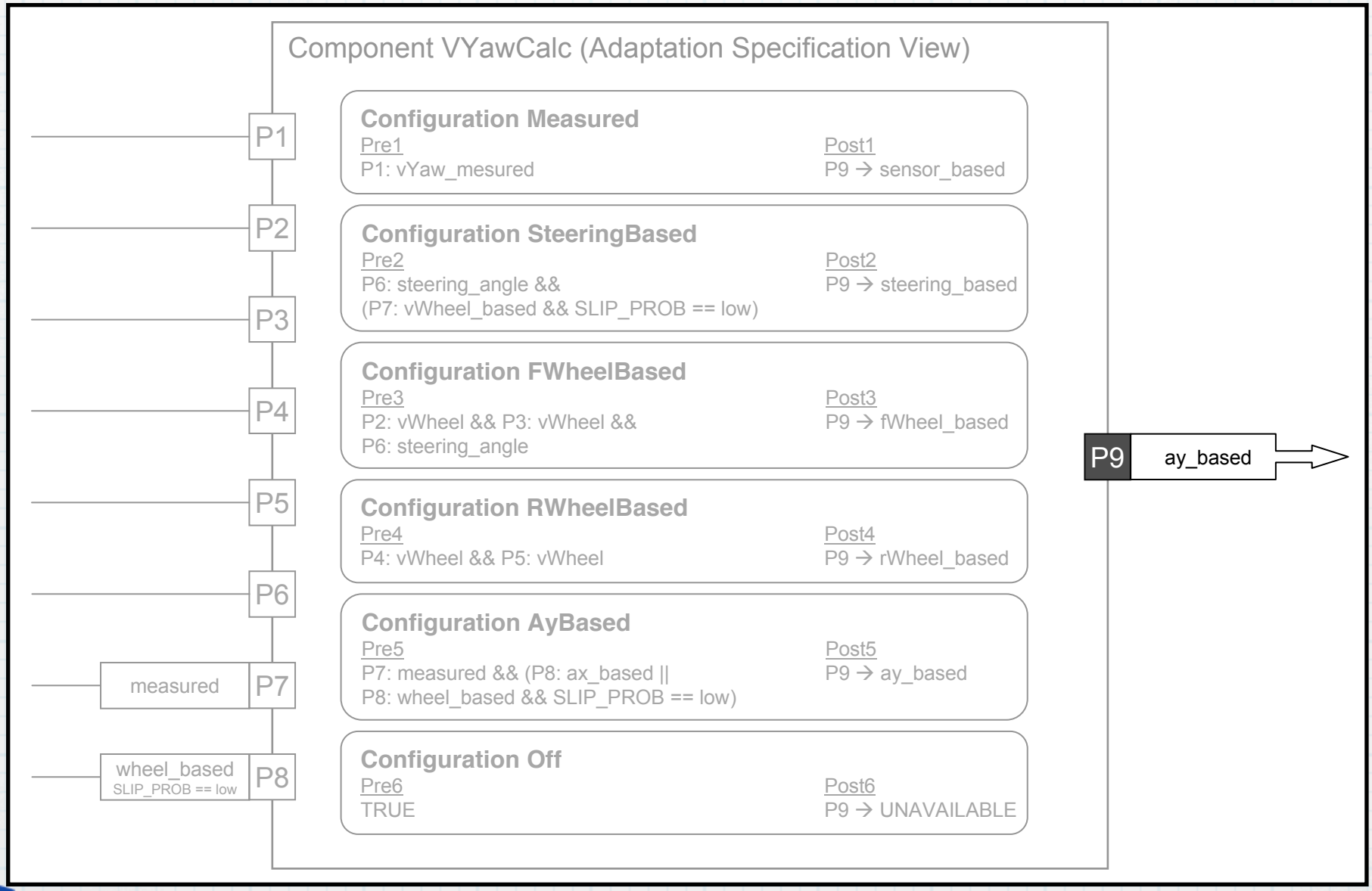
Modelling Adaptation



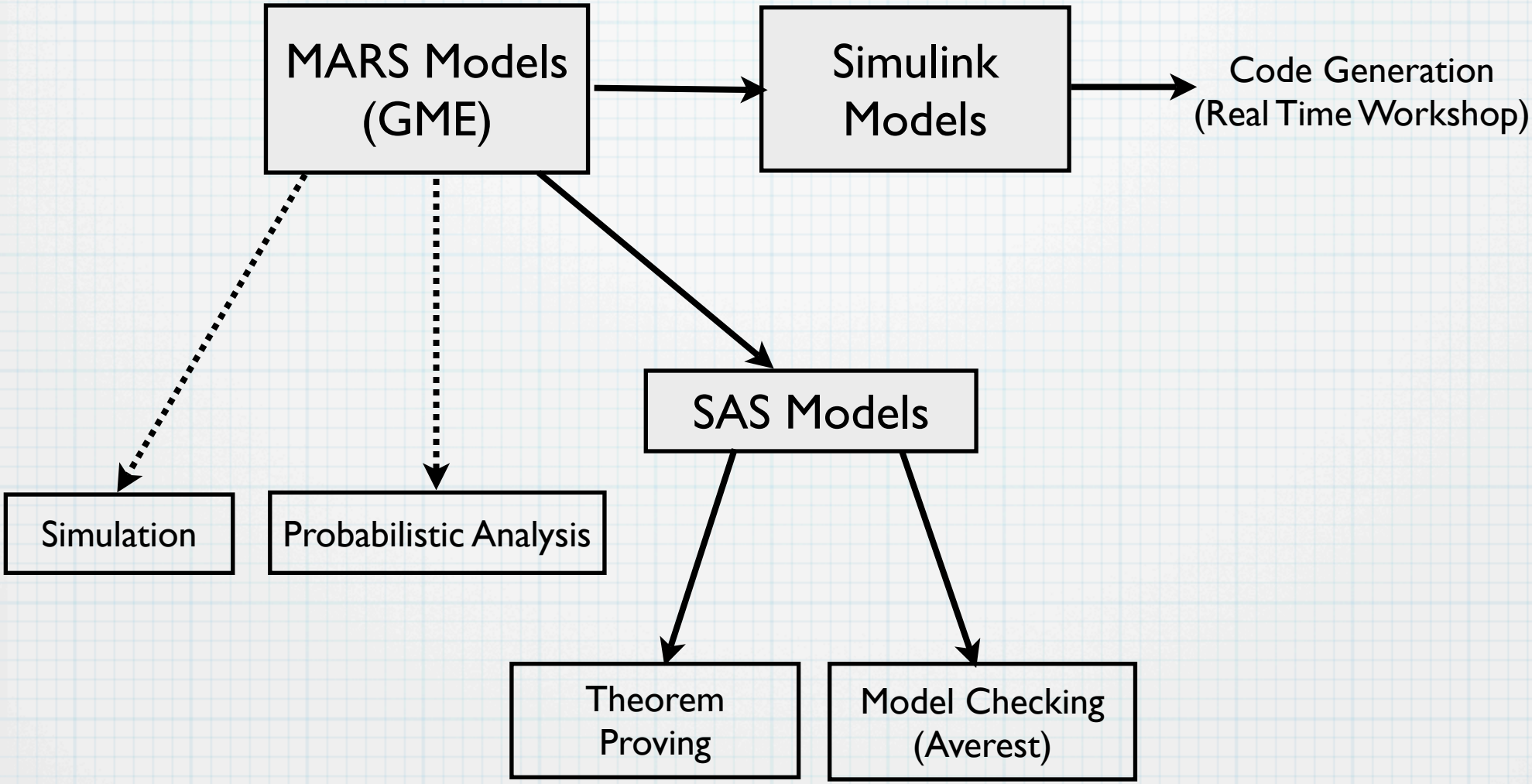
Modelling Adaptation



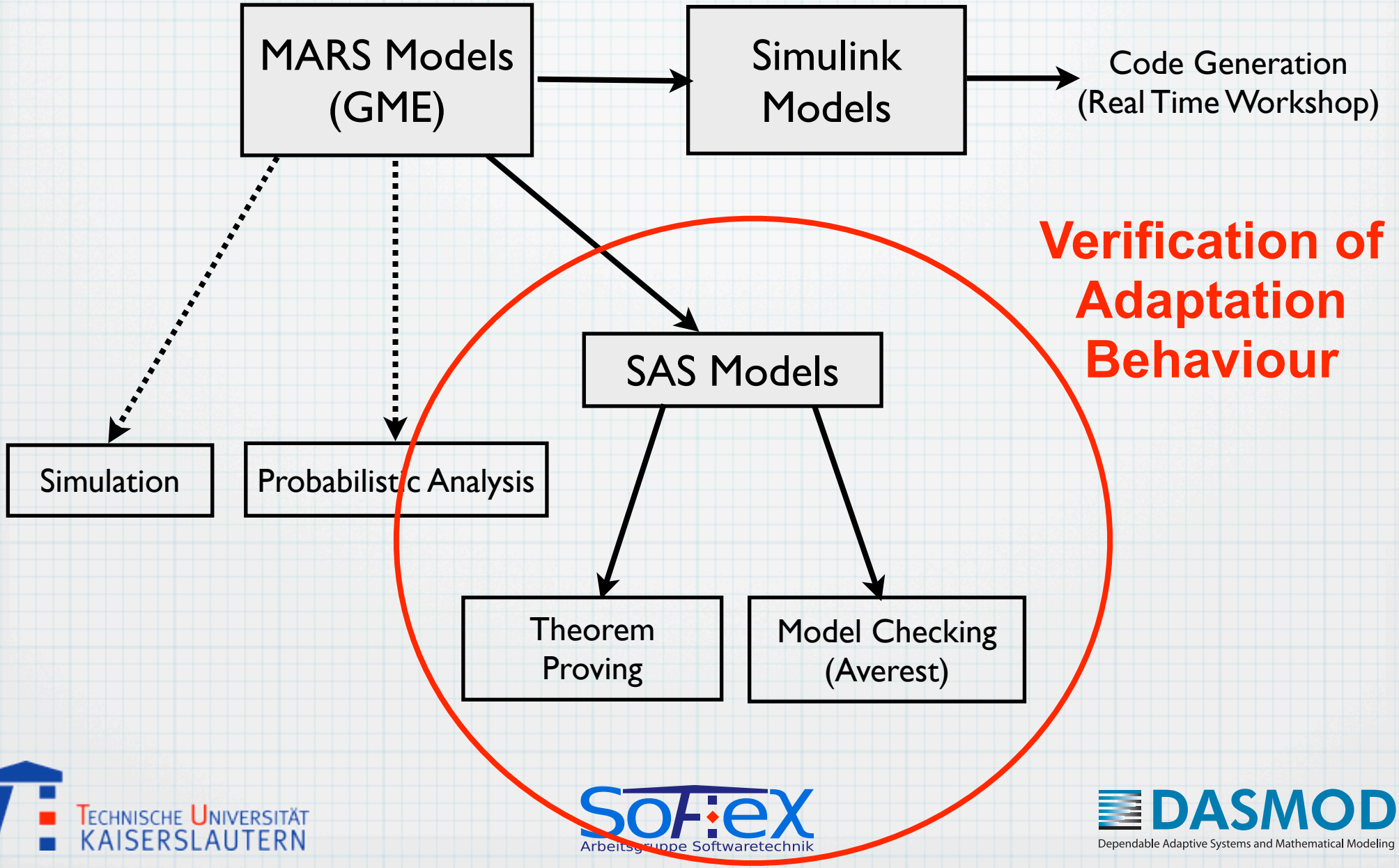
Modelling Adaptation



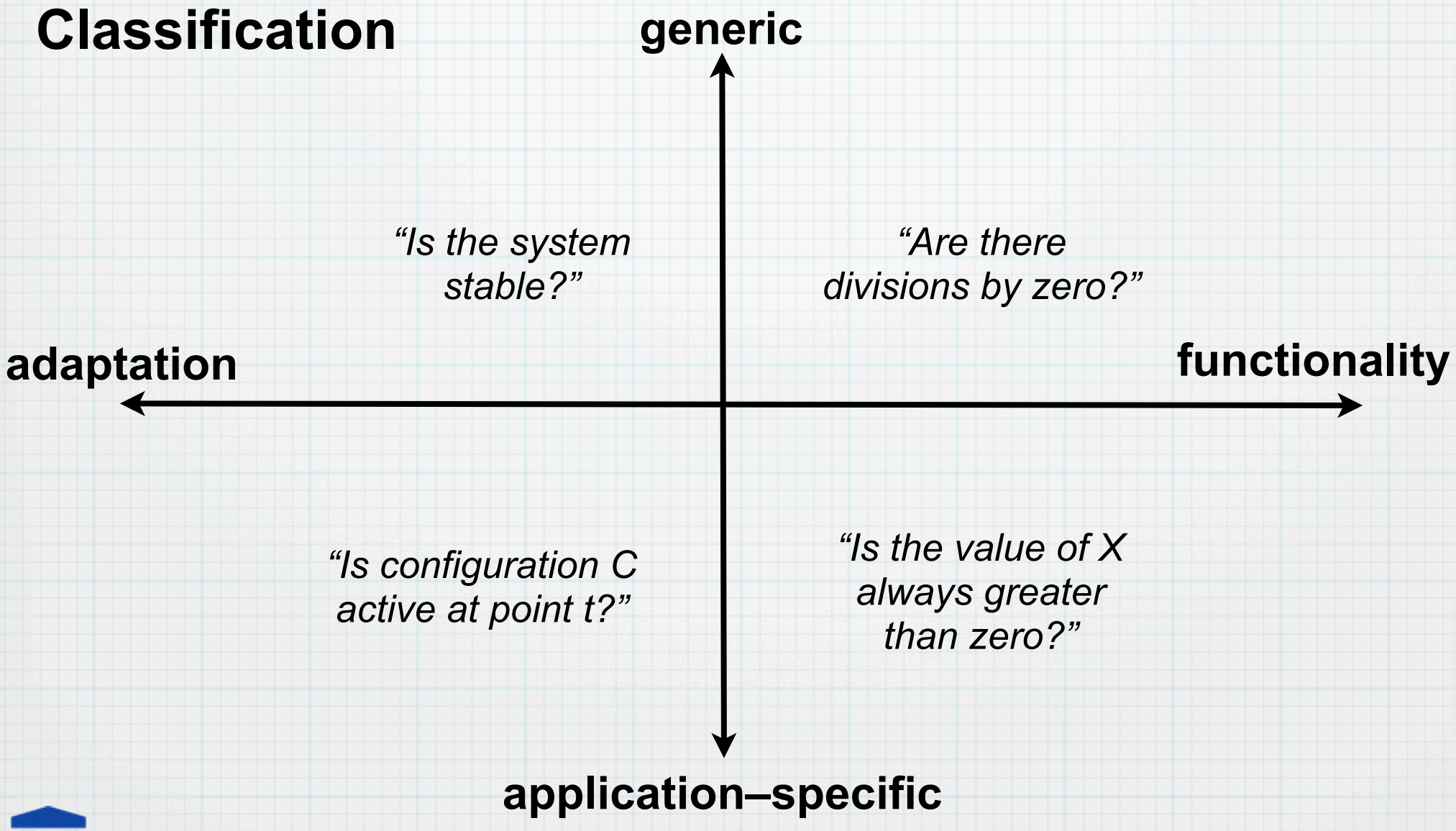
Development Process



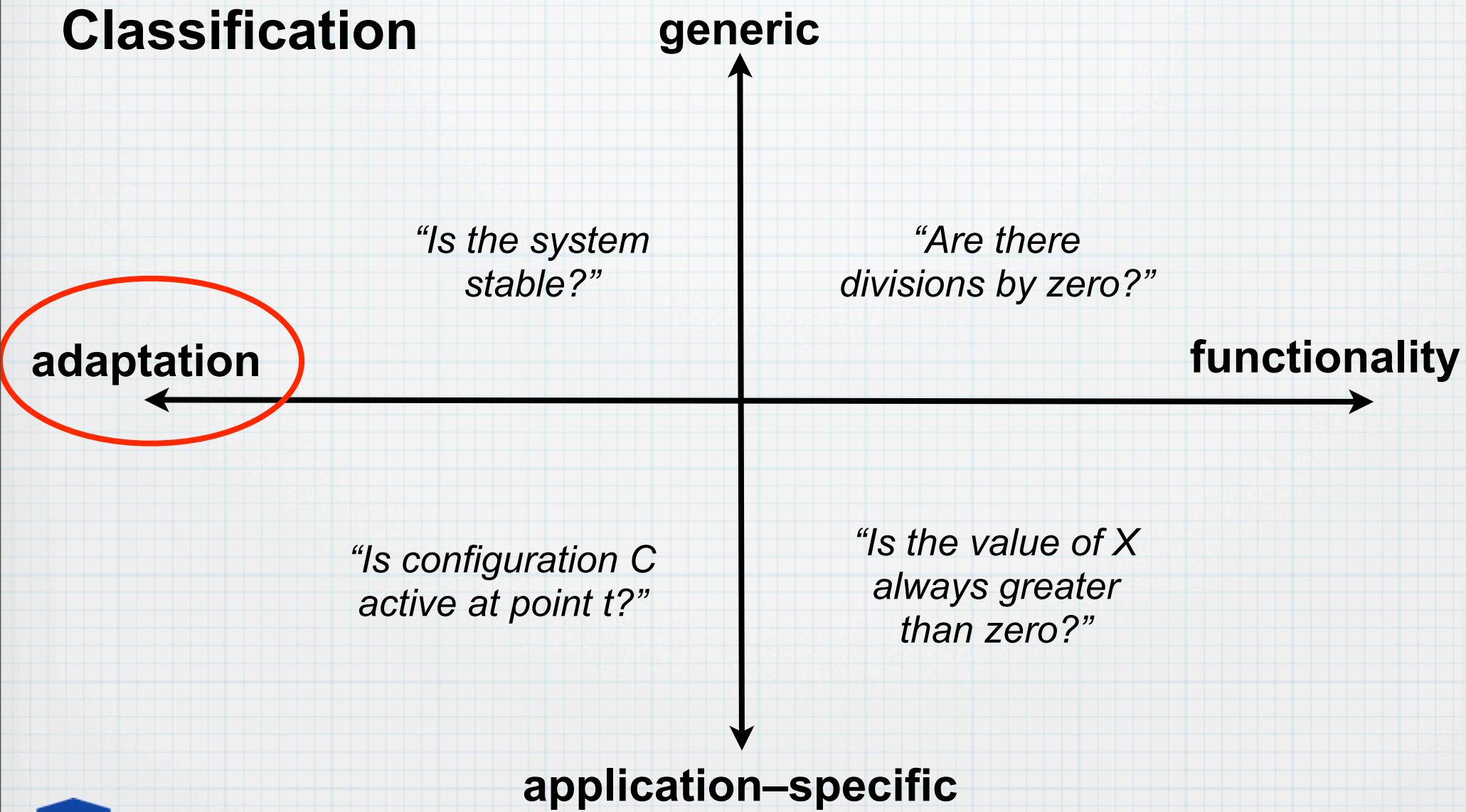
Development Process



System Properties



System Properties



Adaptive Generic Properties

- **No module gets stuck in the default configuration ‘off ’:**

$$\mathsf{AG}(c = \text{off} \rightarrow \mathsf{EF} c \neq \text{off})$$

- **Every module can reach all configurations at all times:**

$$\mathsf{AG}(\bigwedge_{i=1}^{n} \mathsf{EF}\ c = \text{config}_i)$$

- **No inconsistent states can be reached:**

$$\mathsf{AG}(\bigvee_{i=1}^{n} c = \text{config}_i)$$

- **No configuration is always only transient:**

$$\bigwedge_{i=1}^{n} \mathsf{EFEG}\ c = \text{config}_i$$

Properties of VSC System

Controller Modules correctly implement Fail-Safe Layer.

Traction Control:

$$\mathsf{AG}((gas\_output.quality = available \wedge gas\_input.quality = available) \rightarrow c_{traction\_control} \neq Off)$$

Steering Angle Delimiter:

$$\mathsf{AG}((steering\_angle\_input.quality = available \wedge steering\_angle\_servo.quality = available) \rightarrow c_{steering\_angle\_delimiter} \neq Off)$$

Yaw Rate Correction:

$$\mathsf{AG}((wheel\_brakeFL.quality = available \wedge wheel\_brakeFR.quality = available \wedge wheel\_rearBrake.quality = available \wedge brake\_input.quality = available \rightarrow c_{yaw\_rate\_corrector} \neq Off)$$

Experimental Results

Characteristics of Vehicle Stability Control System

Number of components	28
Number of configurations	70
Lines of code	≈ 2500
Number of reachable states	$\approx 5 \cdot 10^{18}$
Number of properties	151

Analysis Times for Generic Adaptive Properties

Property	**Time [seconds]**			
	Min.	**Avg.**	**Max.**	**Total**
P1 (liveness)	< 0.1	3.1	71.5	84.0
P2 (reachability)	< 0.1	2.4	52.1	63.8
P3 (safety)	< 0.1	0.1	0.2	0.7
P4 (persistence)	< 0.1	0.3	4.5	19.6

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**