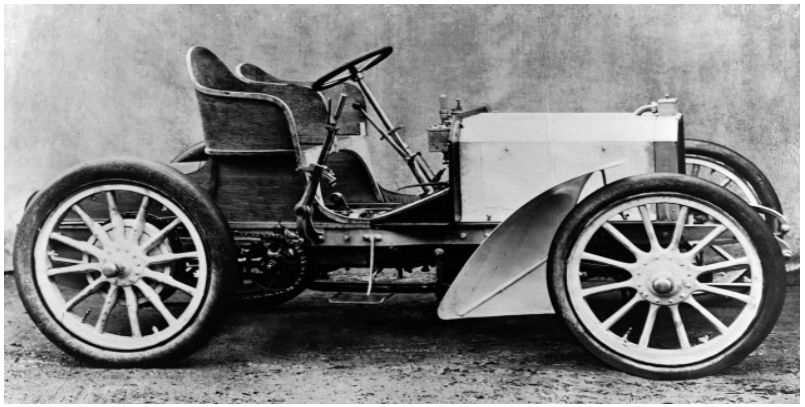
Automatic Discovery of Unspecified Behaviors in Automotive Control Software

Muzammil Shahbaz and Robert Eschbach

Embedded Systems Quality Assurance

Fraunhofer IESE

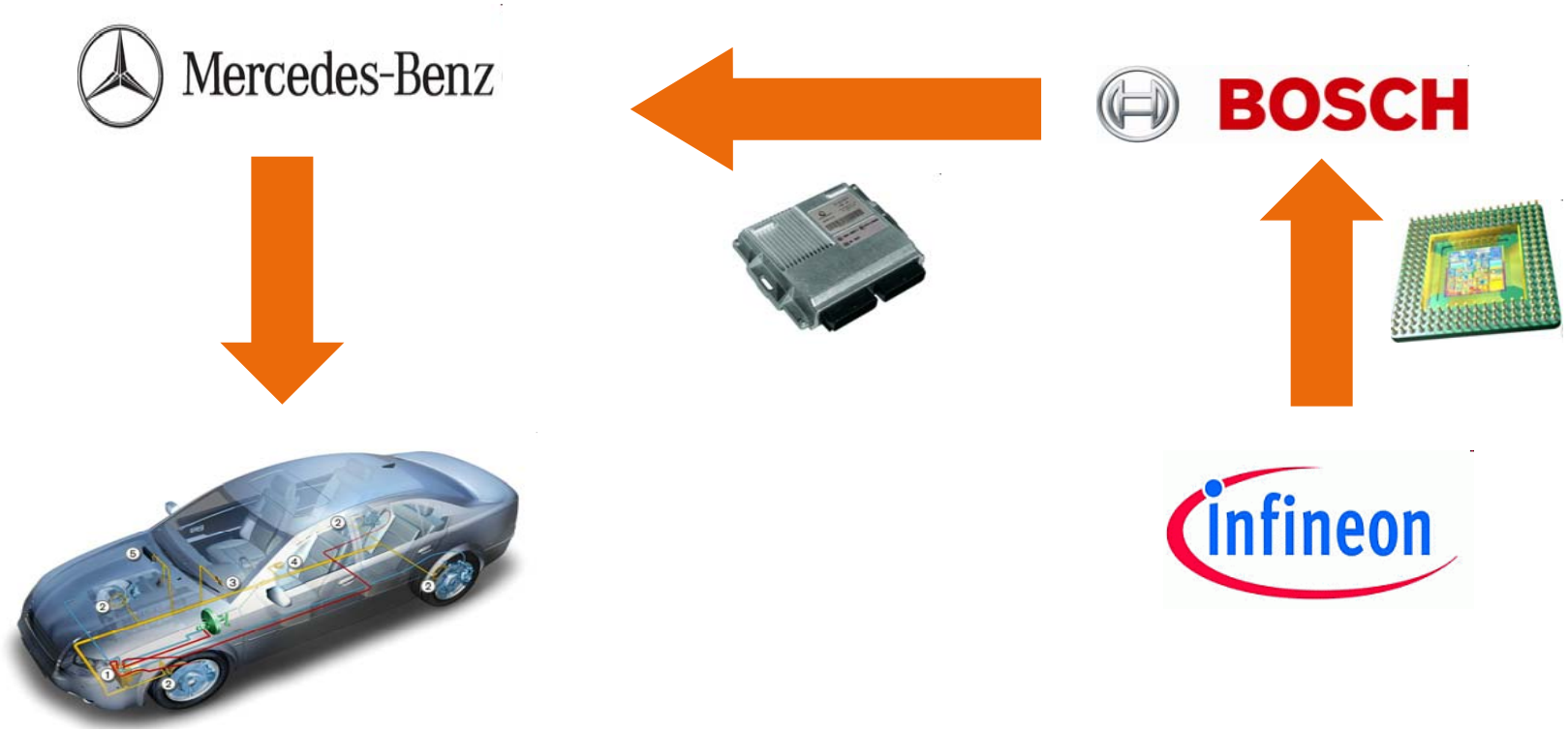
Germany



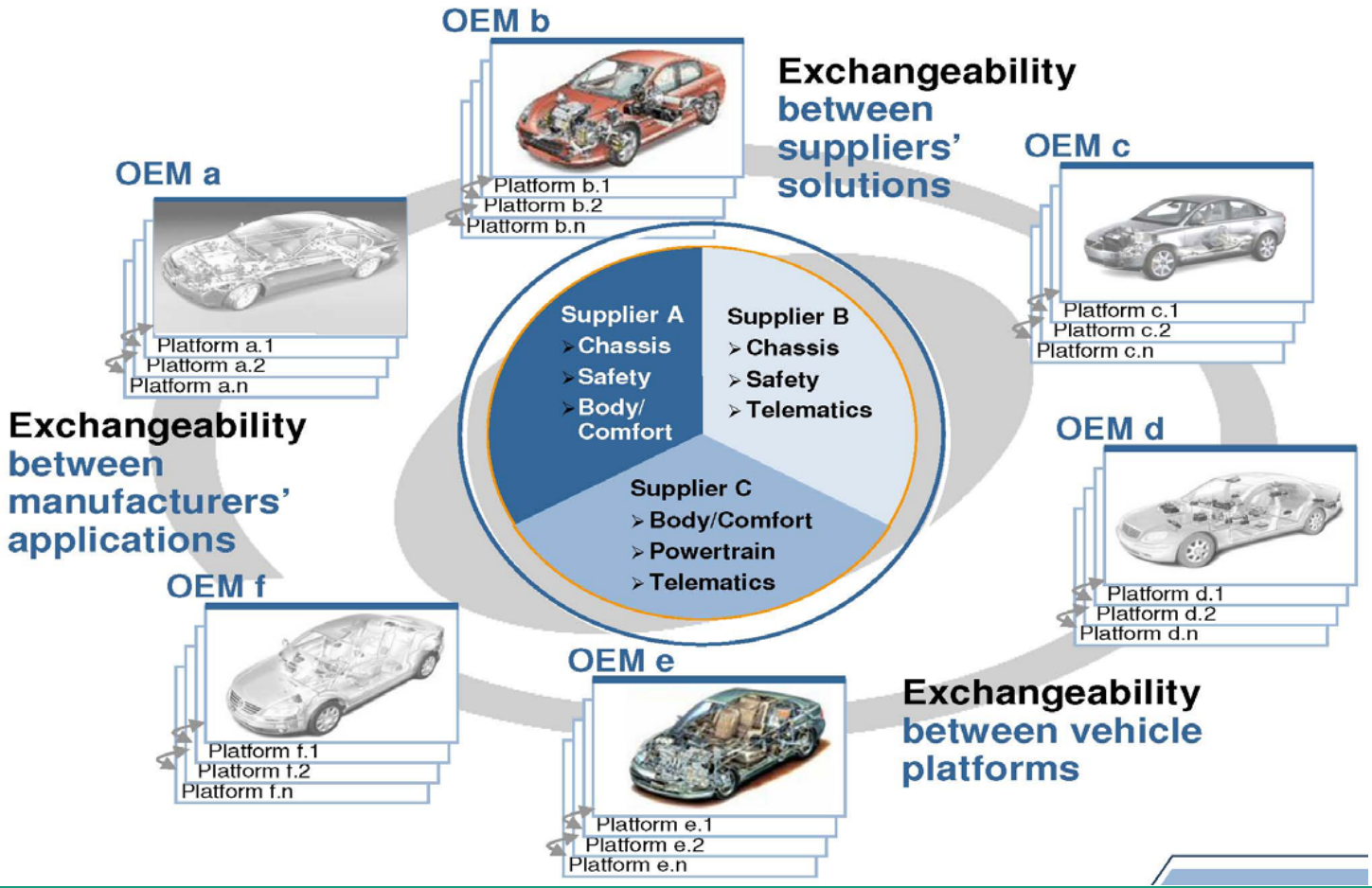
Introduction

- Embedded Systems
  - Challenges: Quality, Reliability and Cost-Efficient
  - Heterogeneity and Multifunctional environment
  - Component Based Engineering approach
- Why challenges are difficult to meet?
  - Component variants and various configurations
  - Stringent specifications: timing, safety, reliability, connectivity
  - Interpretation of requirements
  - Major class of errors: **“Wrong Selection”**

Example Paradigm in Auto Engineering (OEM-Supplier relation)

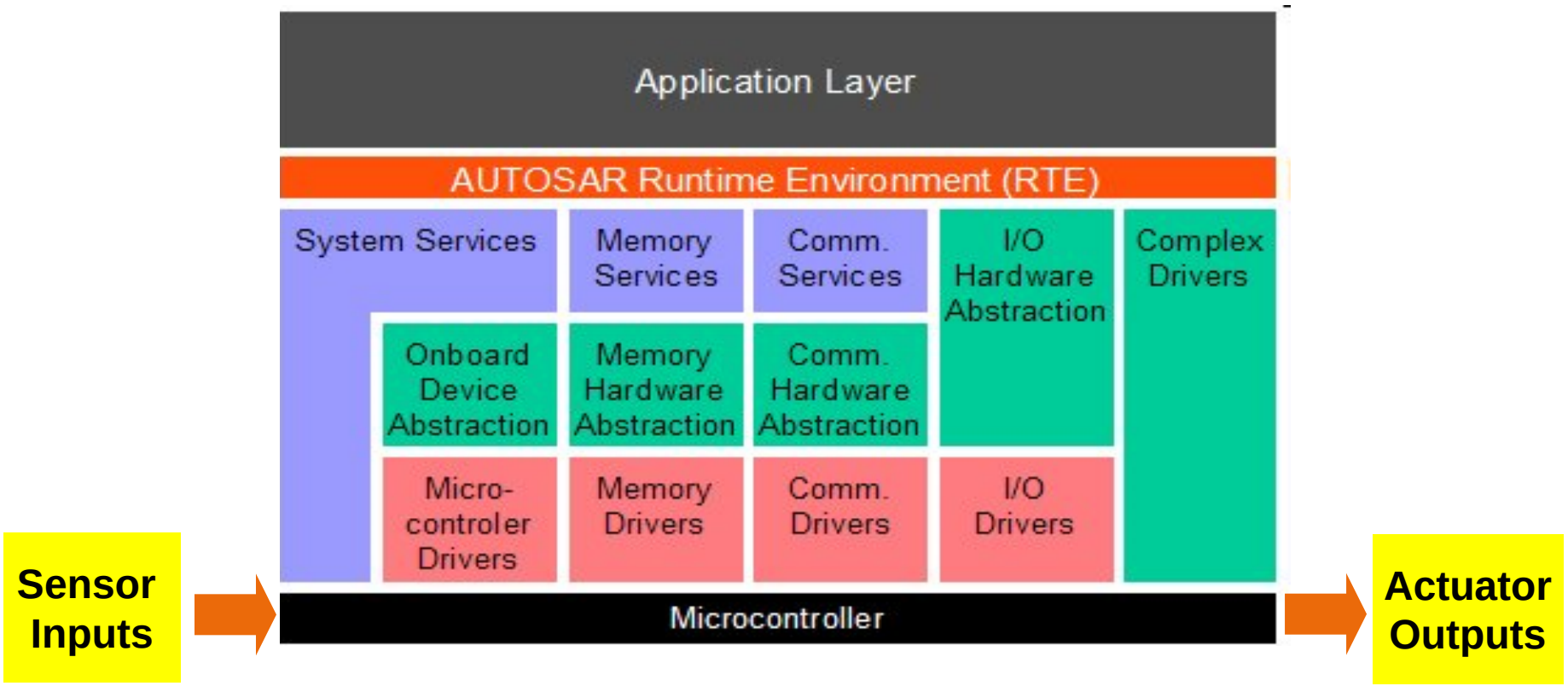


Multiple OEMs-Multiple Suppliers



Courtesy: Stefan Bunzel, spokesman AUTOSAR

Electronic Control Unit (ECU) AUTOSAR architecture



- ***"Cooperate on standards, Compete on implementation"***

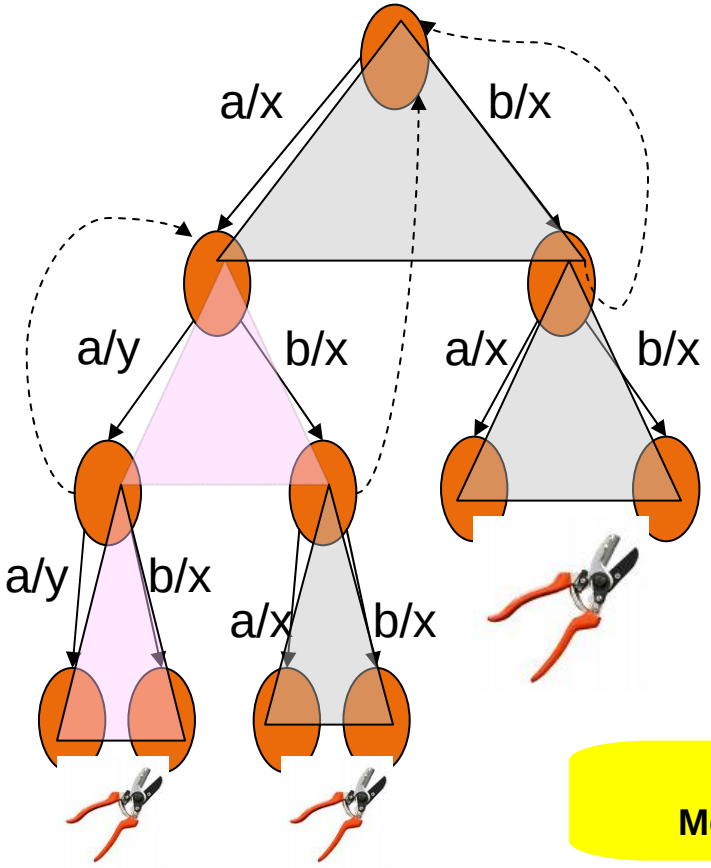
Door Control Unit (DCU) Mercedes-Benz vehicle

- *Inputs* to ECU:
  - User inputs
  - Sensor inputs
  - Messages from other ECUs
- *Outputs* from ECU:
  - Output to actuators
  - Messages to other ECUs

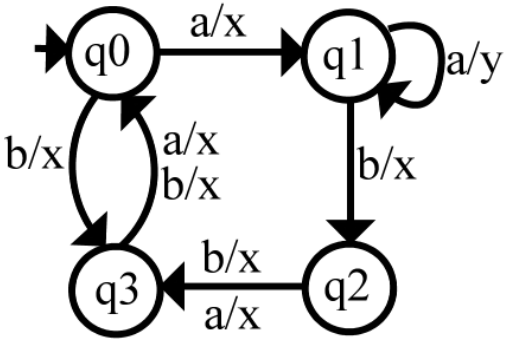
Embedded ECUs
- Power Window
- Side Mirror
- Door Locking

Model Inference Approach

"Mealy Machine Inference". M. Shahbaz and R. Groz. *Formal Methods 2009*.

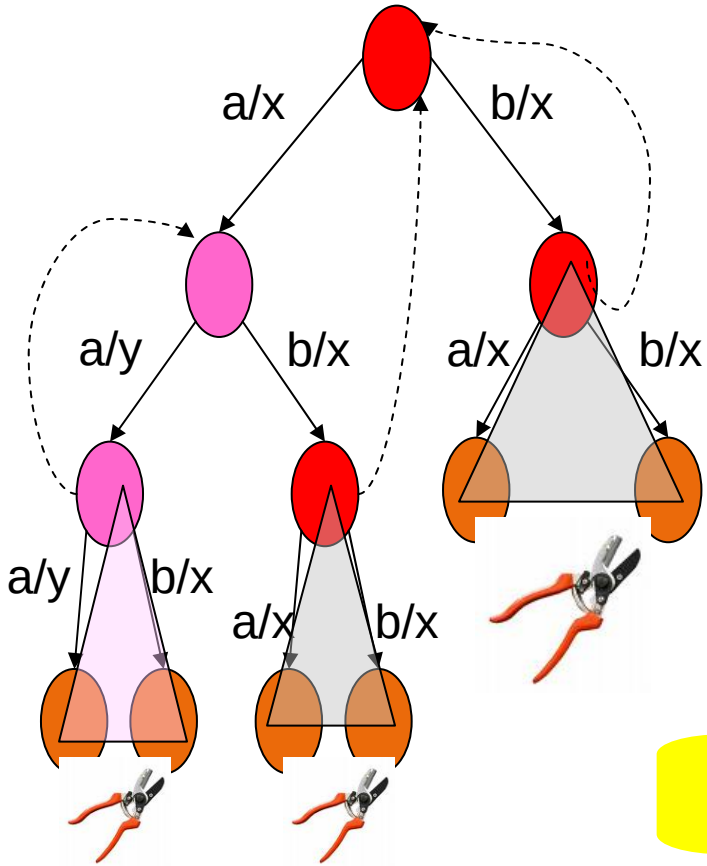


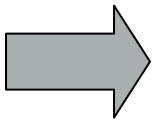
Actual Mealy Machine

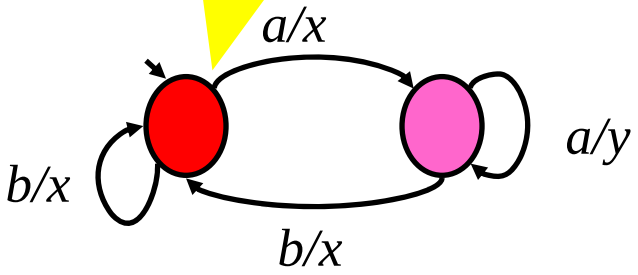


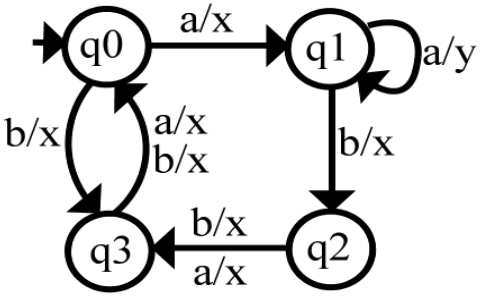
Fraunhofer IESE

Model Inference Approach (2)









Actual
Mealy Machine

Fraunhofer IESE

Stimuli for DCU from the textual specification

Specification

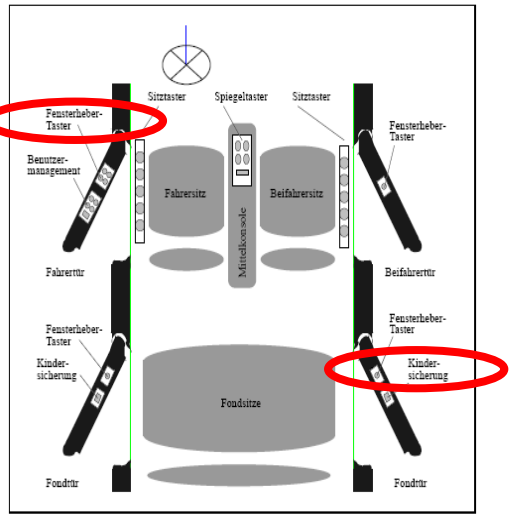


Abbildung 3: Schematische Darstellung der Anordnung der Bedienelemente.

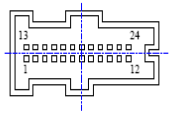


Abbildung 4: Steckerbild S1.

Anschluß	Bezeichnung	In/Out	Beschreibung
1	MASSE	—	Signalmasse
2	FHB_VL	in	Fensterheber–Taster vorne links (i.d. Fahrertür, nicht belegt bei Einbau in Beifahrertür)

Tabelle wird auf der nächsten Seite fortgesetzt

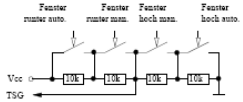


Abbildung 5: Anschlußcharakteristik Fensterhebertaster.

Scheibenbewegung Fenster

Anschlüsse: 6 (F_BEWEG)

Charakteristik: Erzeugt nach einer Scheibenbewegung nach oben oder unten von 1 mm ± 0.3 mm einen entprellten Impuls (Vcc).

Benutzermanagement–Taster

Anschlüsse: 7 (MGMT_1), 8 (MGMT_2), 9 (MGMT_3), 10 (MGMT_4), 11 (MGMT_SET)

Charakteristik: Nicht entprellter [illegible]

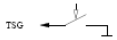


Abbildung 6: Anschlußcharakteristik Benutzermanagement–Taster.

Sensor–Eingänge Türgriff, Fensterendposition, Türverriegelung

Anschlüsse: 12 (T_OFFEN), 13 (T_GRIFF), 16 (F_UNTEN), 17 (F_OBEN), 18 (T_RIEGEL)

Charakteristik: Nicht entprellter Mikroschalter gegen Masse (analog Abbildung 6).

Ausstiegsleuchte

Anschlüsse: 14 (T_LICHT)

Charakteristik: Ansteuerung Ausstiegsleuchte 12 V, 5 W.

Beleuchtung Bedienelemente

Anschlüsse: 15 (B_LICHT)

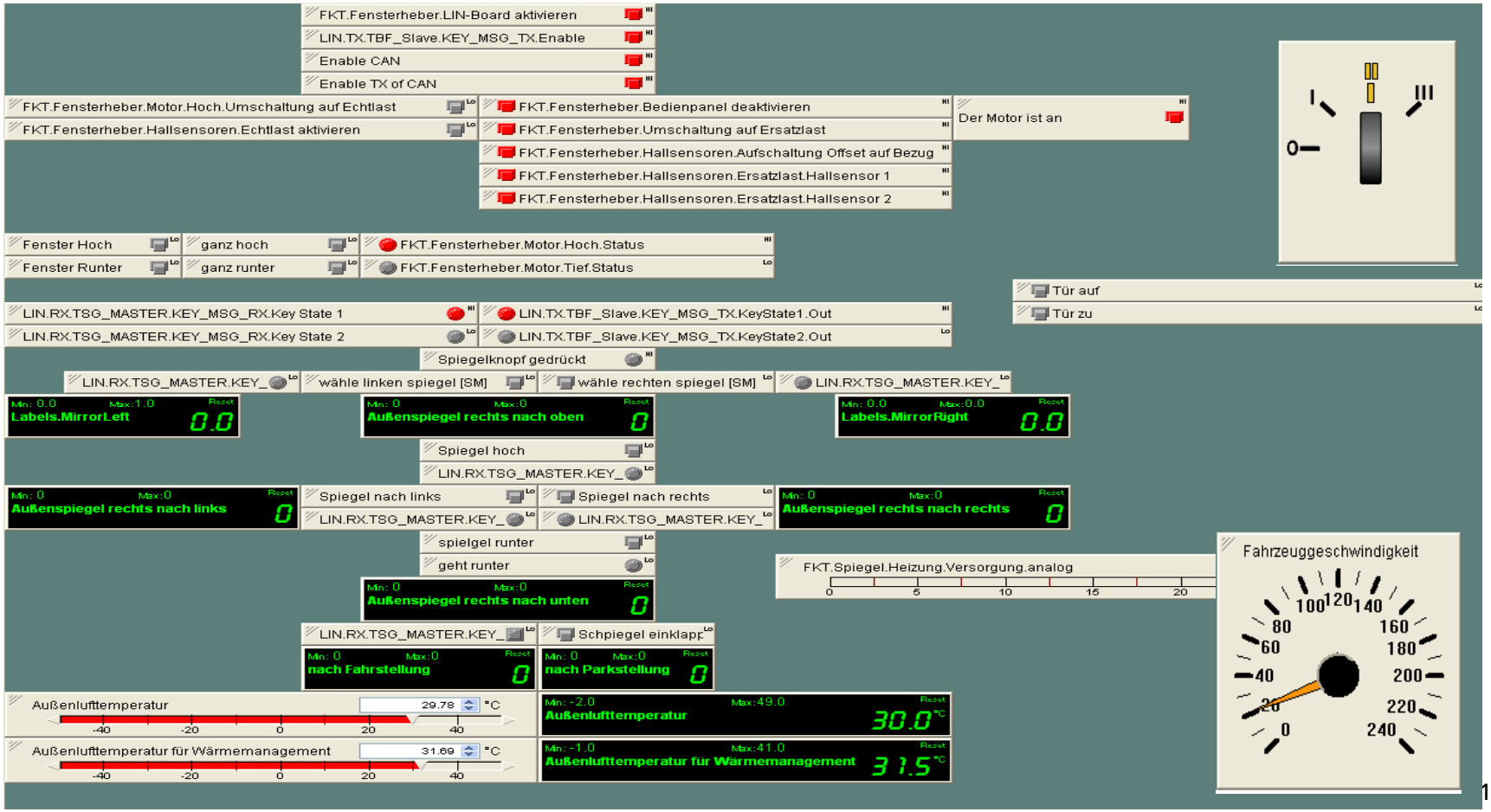
Charakteristik: Ansteuerung LED; 2.3 V, 10 LED à 20 mA, Parallelschaltung

Schloßnußschalter

Anschlüsse: 19 (KEY_STATE)

Fraunhofer IESE

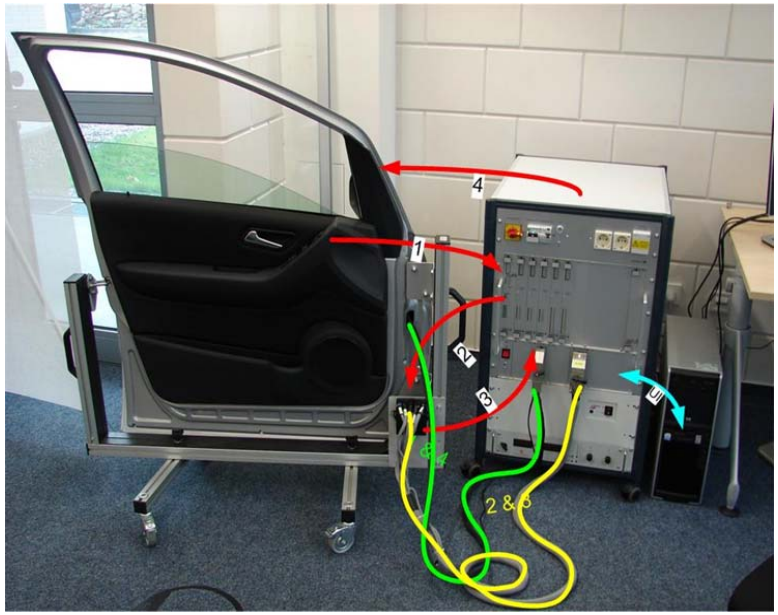
Stimuli for DCU from the interfacing tool

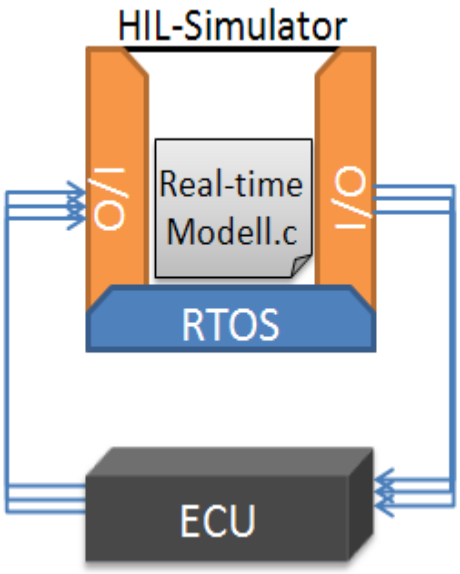


Snapshot of ProveTech:TA

Fraunhofer IESE

Test Automation



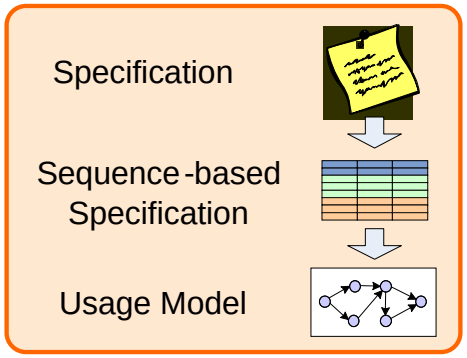


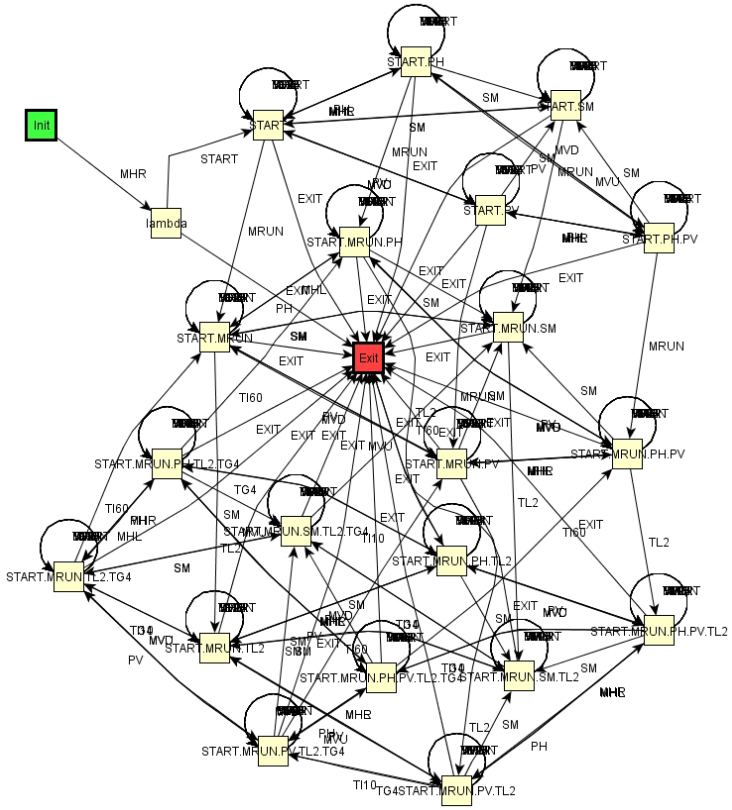
Tools:

- RALT (Fhr), ProveTech:TA (MBTech), HiL Simulator (dSpace)

Fraunhofer IESE

Usage Model Derived from Specification





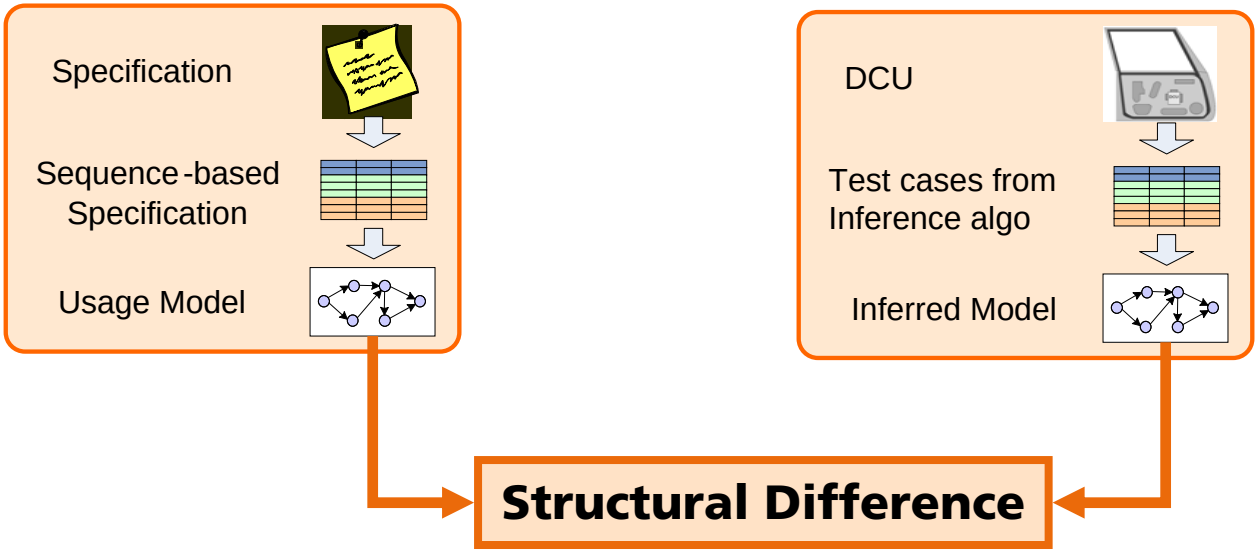
- States: 23
- transitions: 305
- Input size:

14 x signal values

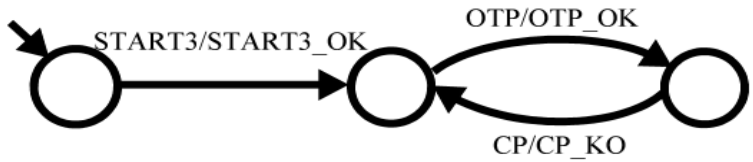
- S. J. Prowell and J. H. Poore. “Foundations of sequence-based software specification”. IEEE Trans. Softw. Eng., 2003.

Fraunhofer IESE

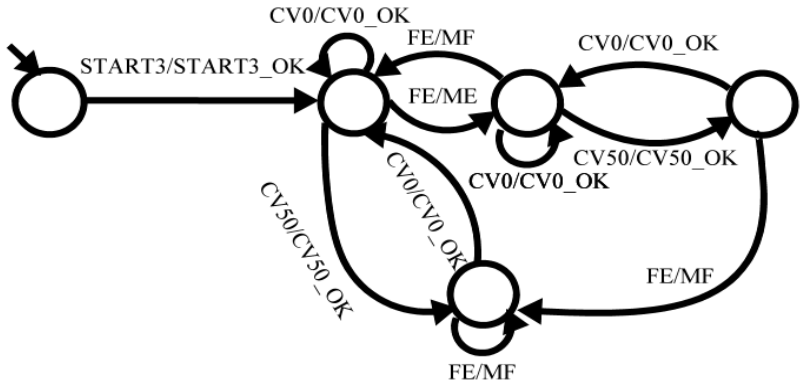
Methodology



Inference Results
Snippets depicting unspecified behaviors



- Power Window
  - *States:* 5
  - *Time:* 30 min
  - *Queries:* 802
  - *Discovered Behaviors: 2*



- Mirror
  - *States:* 9
  - *Time:* 120 min
  - *Queries:* 1952
  - *Discovered Behaviors: 3*

Fraunhofer IESE

Other Findings

- Number of signals and their possible values were identified during experimentation
- Few other actuators were identified during experimentation
- ECU behaviors are different in other type of vehicles
- Variable timing delays change behaviors
- Specification in the natural language was ambiguous

- Enjoyed challenge of reverse engineering real black box system ☺

Conclusion

- Model Inference approach is promising in uncovering the unknowns
  - Beneficial for V&V activities and “fitness for use” for components
  - Inference of relatively good approximation in embedded systems
- But
  - Embedded systems are very time-sensitive
    - Appropriate modeling notations are required for hybrid systems
  - Interfacing with real systems is hard
    - Scarcity of tools for I/O interface automation for black box systems

Perspectives

"Those who believe they have found truth are called dogmatic.
Skeptics are those who continue in their research"

-Inspired from Phrrhonian Hypothesis

- Hunting for more discoveries, improvements, better modeling
- Next in line:
  - Adaptive Cruise Control
  - Blind Spot Detection