Motivation

"IN THE PAST VEHICLE SAFETY HAS BEEN CONSTRUCTED;
IN THE FUTURE IT IS GOING TO BE IMPLEMENTED IN SOFTWARE."

Dr. U. Widmann, AUDI AG, Head of Vehicle Safety

- Automobile turns into time and safety sensitive systems
- Dealing with safety requirements is major challenge

⇒ Dependability Analyses in Design and Verification Phases
Situation at Early Design Stages

- Rapidly changing requirements and design concepts
- Effects on dependability attributes unknown
  - Analyses time consuming
  - Expert Knowledge required
- Analyses often at later development stages
Fault Tree Synthesis

- Model-to-model transformation
- Hide complexity of formal method
- Chose modeling approach to increase reusability of the models
  - Small changes in system architecture require small changes in model
  - Separate application dependent and application independent system views

Application independent

Application dependent

M2m-trafo

Model for formal analysis
Fault Tree Synthesis (less businessy)

- Model HW/SW-Architecture in UML Composite Diagrams
- Model Applications in UML State Charts
- Run synthesis algorithm to transform the model into a fault tree representation for further analyses
Modeling the HW/SW-Architecture

- UML Composite Diagrams

```
+ component [*]
<stereotype> FaultOrigin

+ fault [*]
<stereotype> Fault
Name: String [1]
Description: String [1]
Probability: Float [1]

(uml)
Class

<stereotype> FaultDetection

+ faultDetectionFacility [*]
<stereotype> FaultDetectionFacility

Christoph Lauer, Modeling and Analysis of Advanced Automotive ECU Architectures at Early Design Stages Using EMF and Model Transformation
```
Modeling the HW/SW-Architecture

- UML Composite Diagrams
Modeling the Applications

- UML State Charts
Modeling the Applications

- UML State Charts
The Transformation Step

• Model-to-model transformation (EMF implementation)

M2m-trafo
Example System

Christoph Lauer, Modeling and Analysis of Advanced Automotive ECU Architectures at Early Design Stages Using EMF and Model Transformation
Example Application

Sample Application

«allocation»
ControllerDecision

«allocation»
ActivateActuator

«allocation»
ControllerValidation
Example Tree1
Example Tree2
Conclusions

• Automatic and model based FTA „interesting“ for early design stages
• Modeling in UML from two different perspectives
  • Application independent
  • Application dependent
• Low remodeling effort suggests reusability
  • No proof given, though
• Transformation leads to plausible fault trees
  • Optimization possible

• Lots of research potential