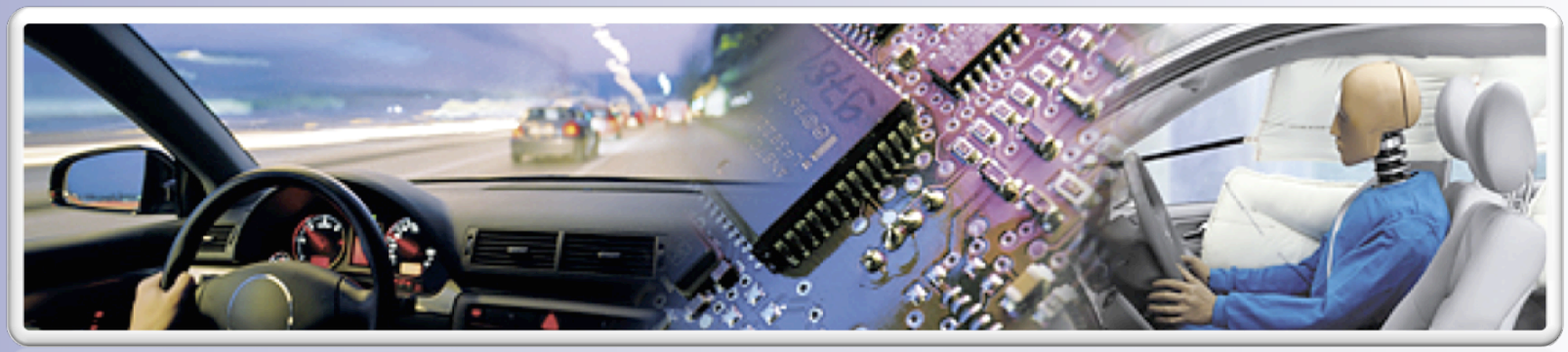
Motivation

„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

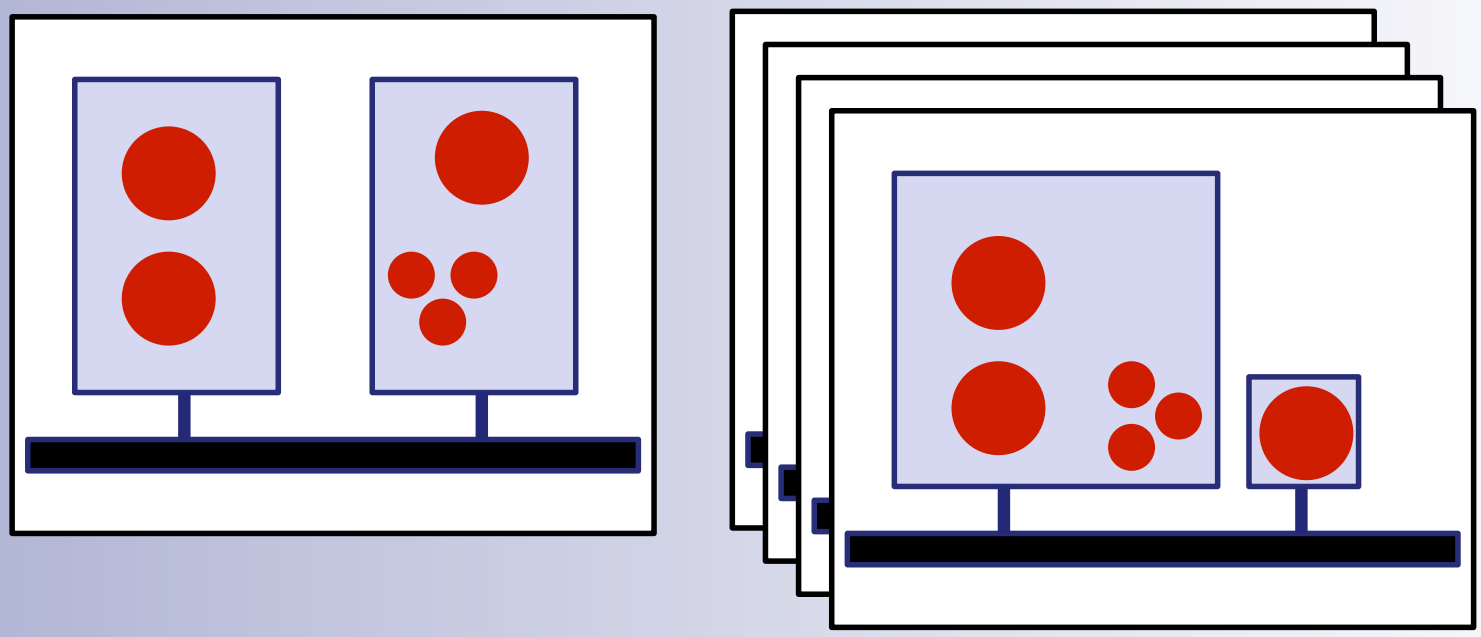
- Automobile turns into time and safety sensitive systems
- Dealing with safety requirements is major challenge

⇒ Dependability Analyses in Design and Verification Phases



Situation at Early Design Stages

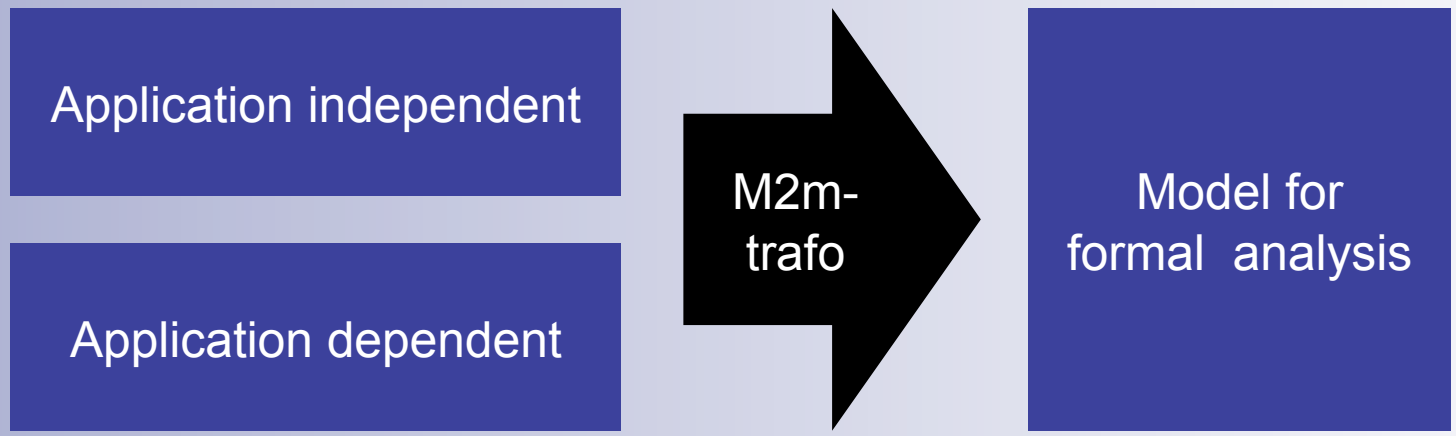
- Rapidly changing requirements and design concepts
- Effects on dependability attributes unknown
  - Analyses time consuming
  - Expert Knowledge required
- Analyses often at later development stages



Fault Tree Synthesis

INI.FAU
Ingolstadt Institute der Friedrich Alexander Universität Erlangen-Nürnberg

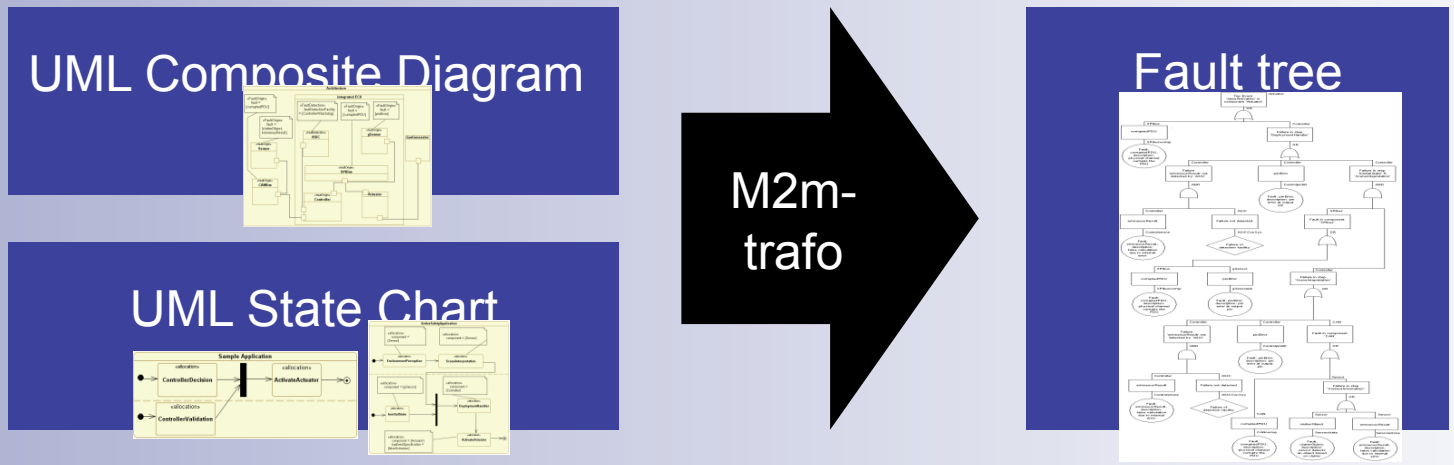
- Model-to-model transformation
- Hide complexity of formal method
- Chose modeling approach to increase reusability of the models
  - Small changes in system architecture require small changes in model
  - Separate application dependent and application independent system views



Fault Tree Synthesis (less businessy)

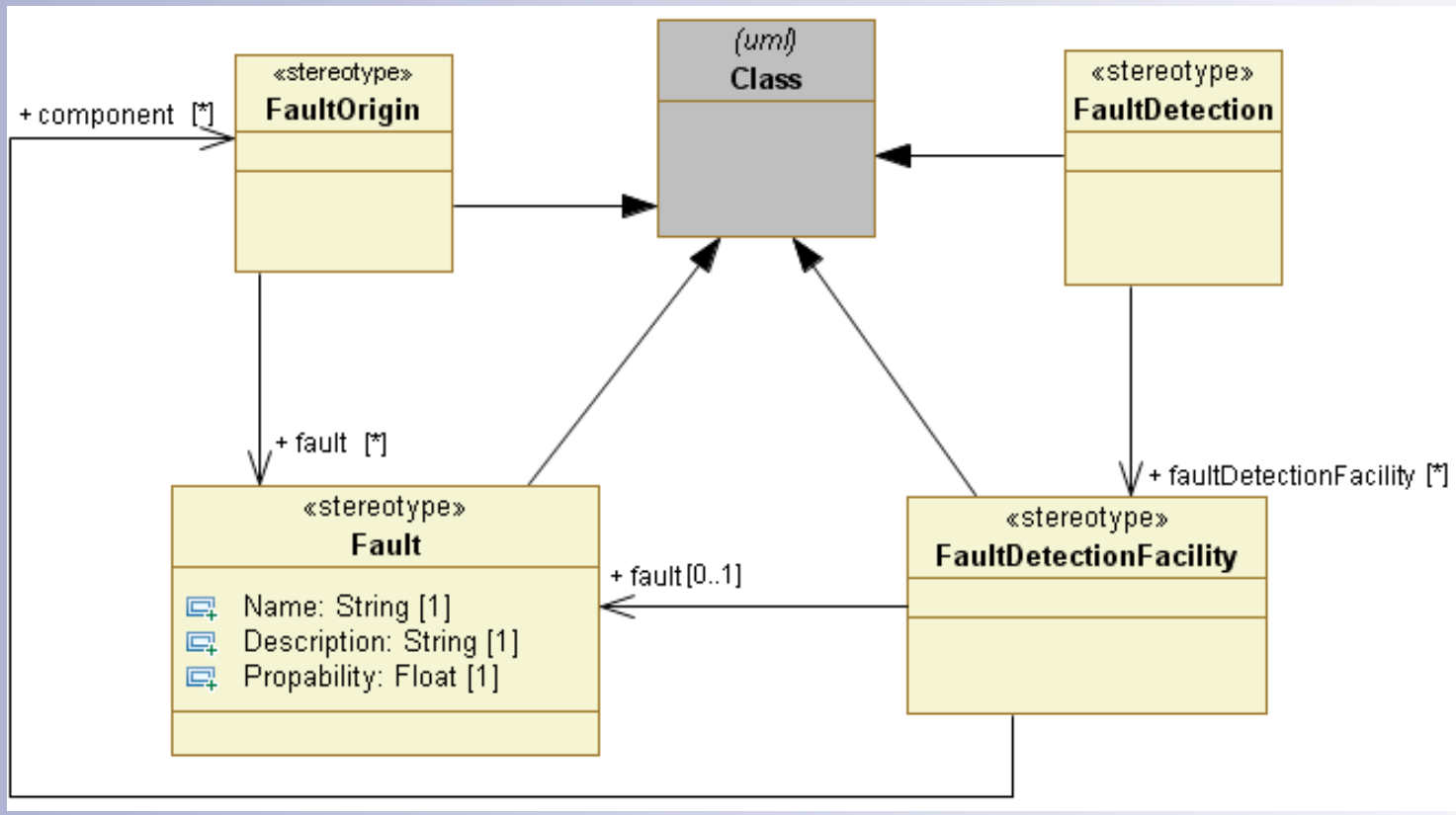
INI.FAU
Ingolstadt Institute der Friedrich Alexander Universität Erlangen-Nürnberg

- 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



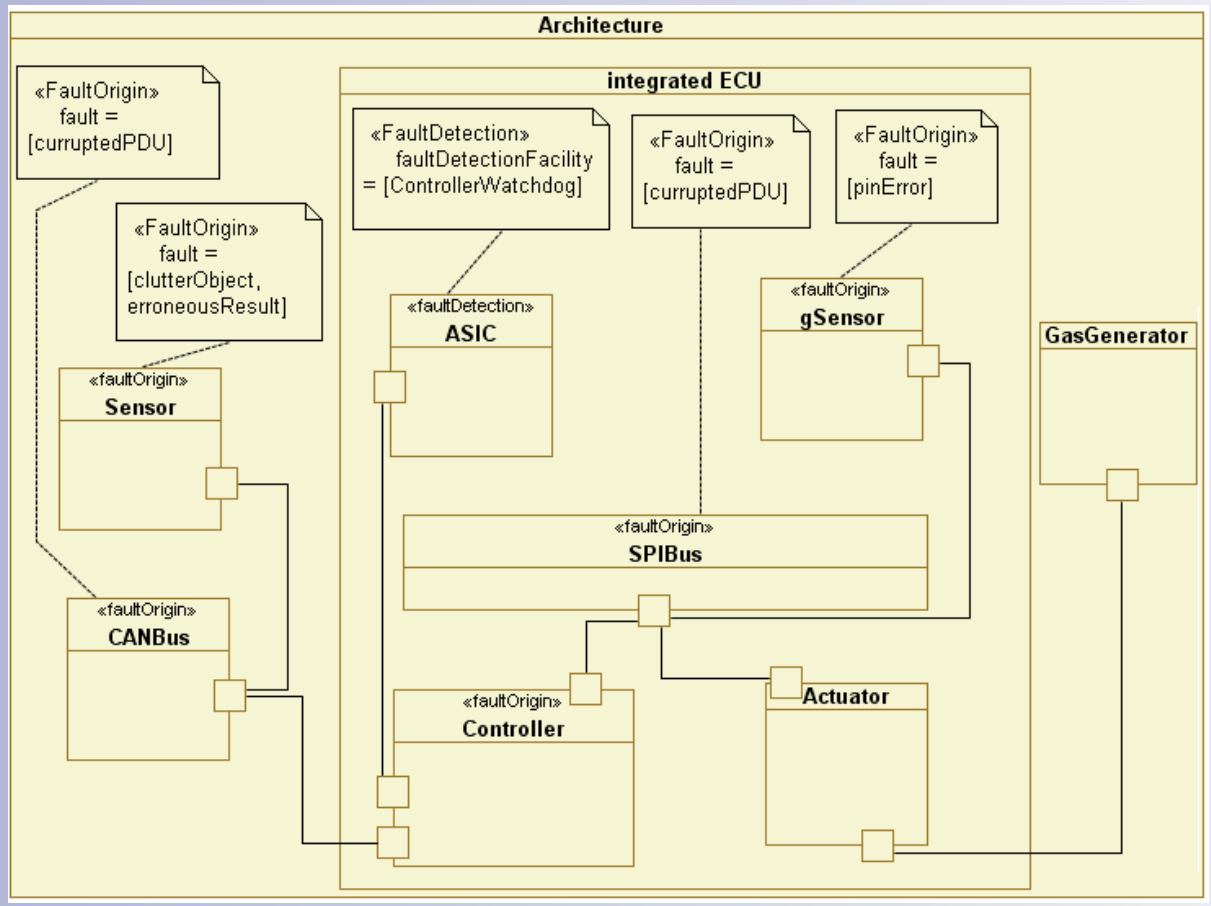
Modeling the HW/SW-Architecture

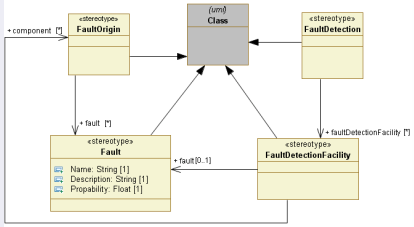
- UML Composite Diagrams



Modeling the HW/SW-Architecture

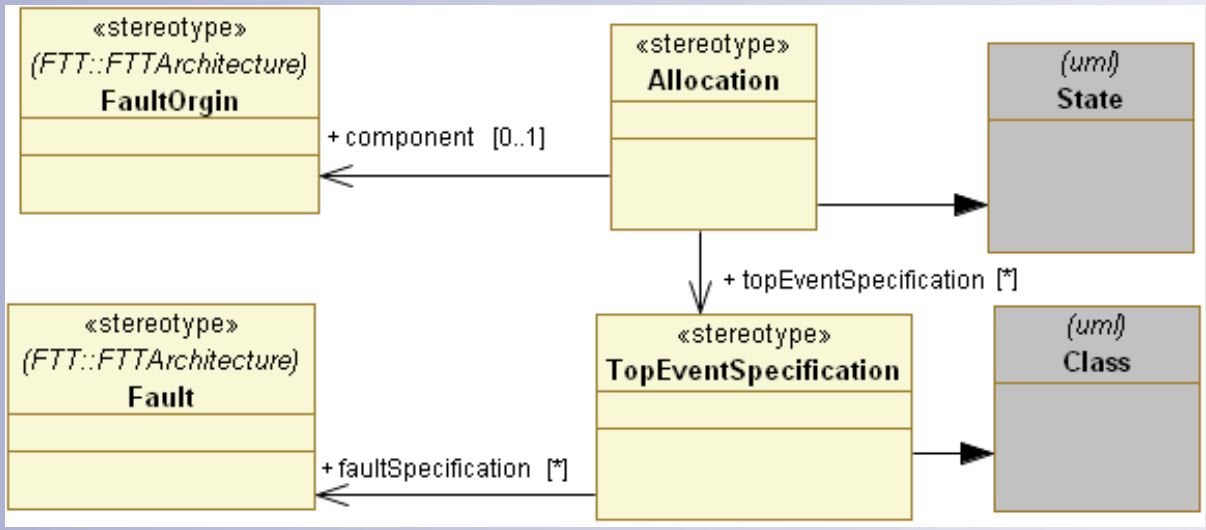
- UML Composite Diagrams

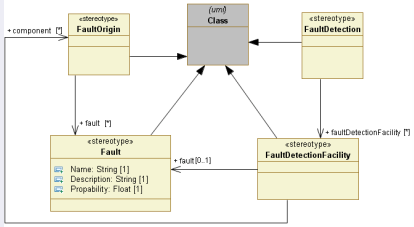


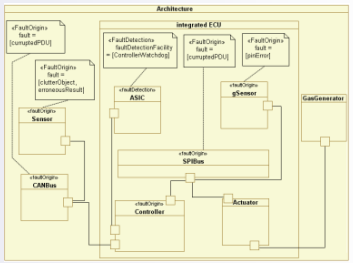


Modeling the Applications

- UML State Charts

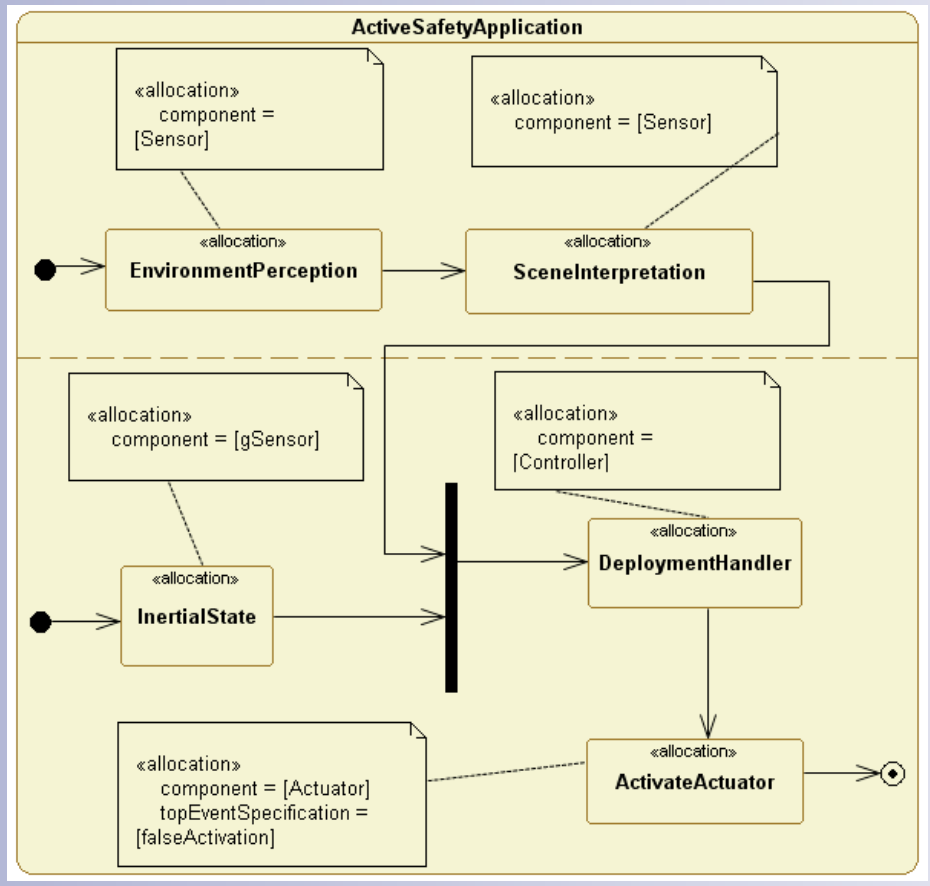


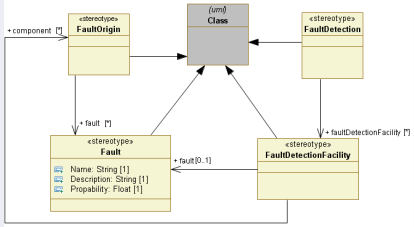


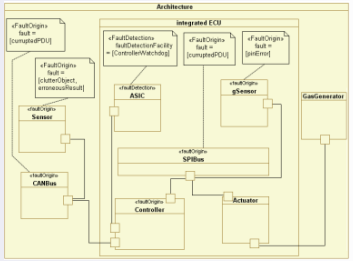


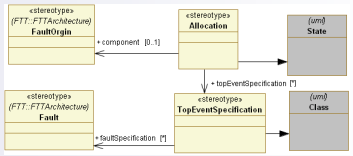
Modeling the Applications

- UML State Charts



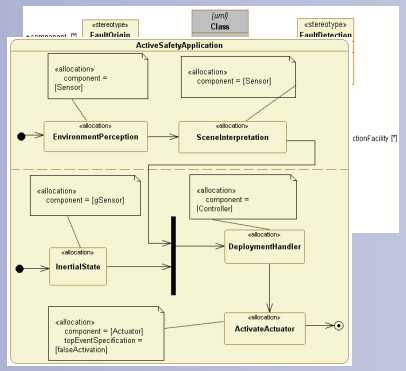


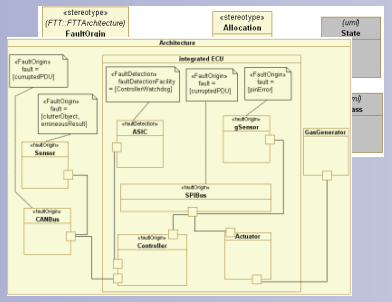




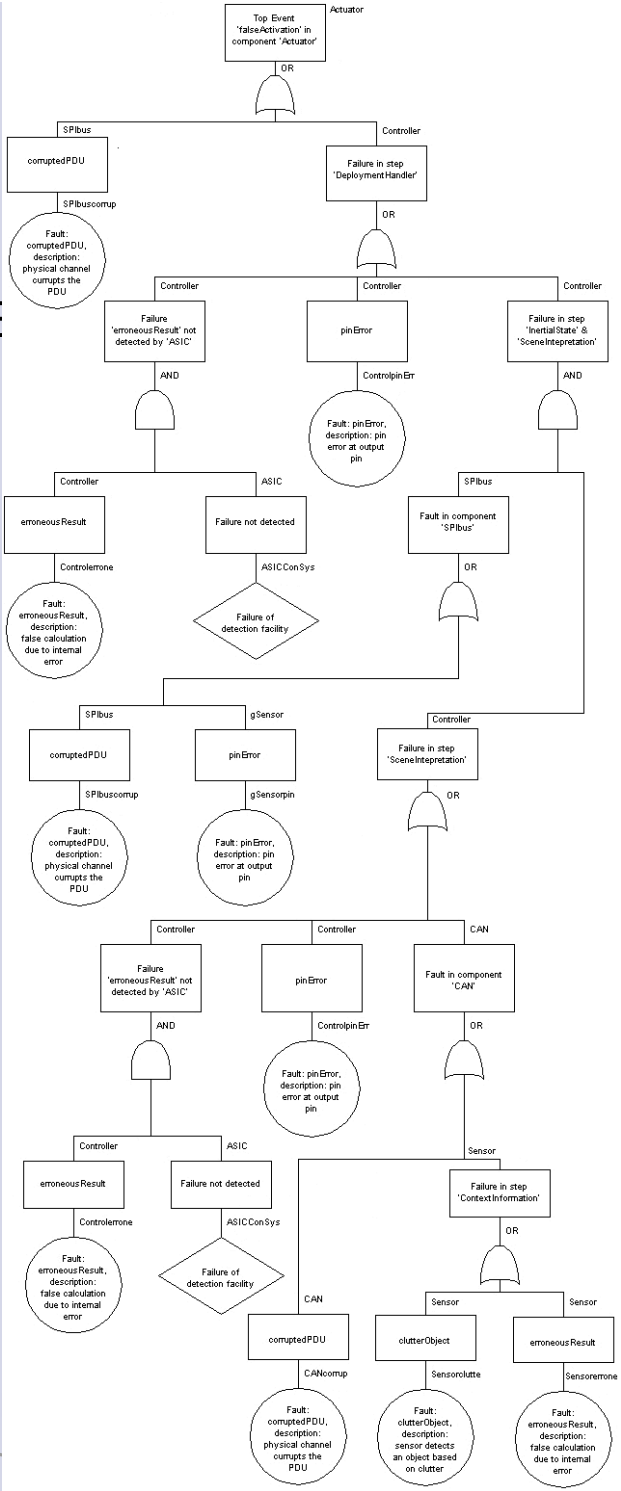
The Transformation Ste

- Model-to-model transformation (E

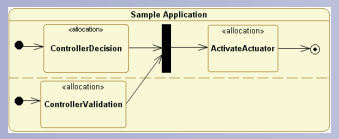


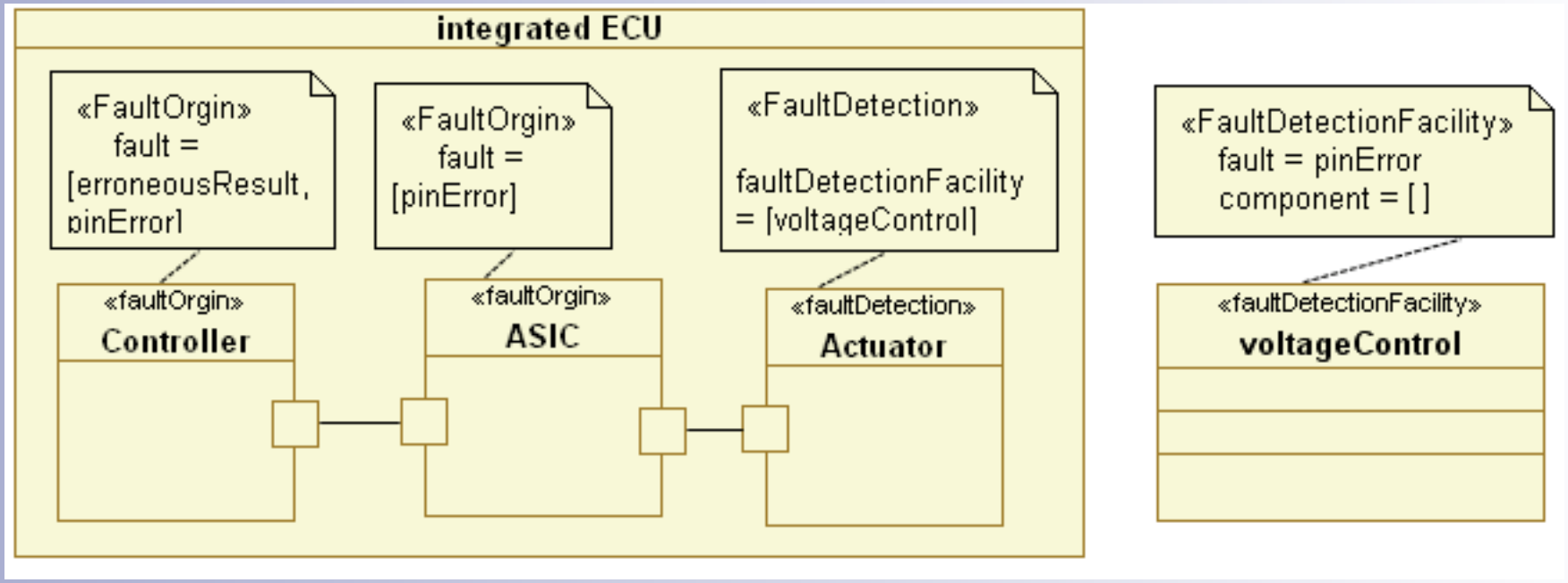


M2m-trafo

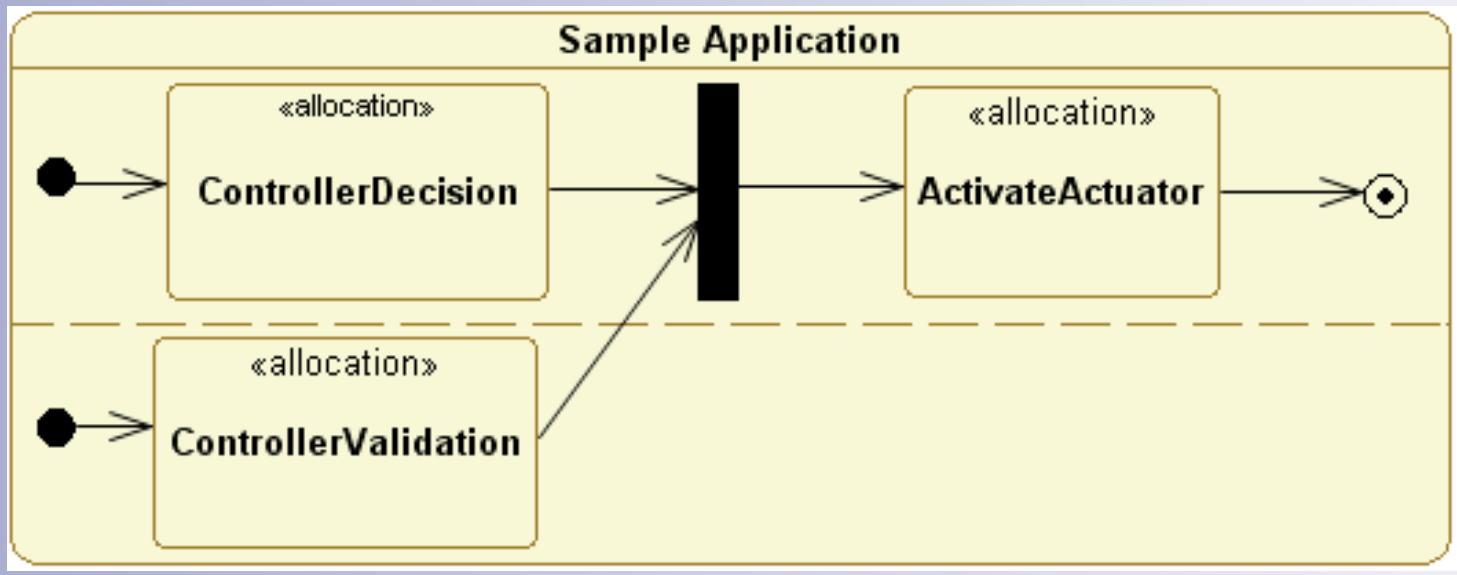


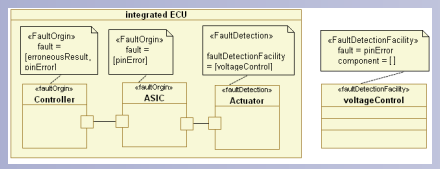
Example System



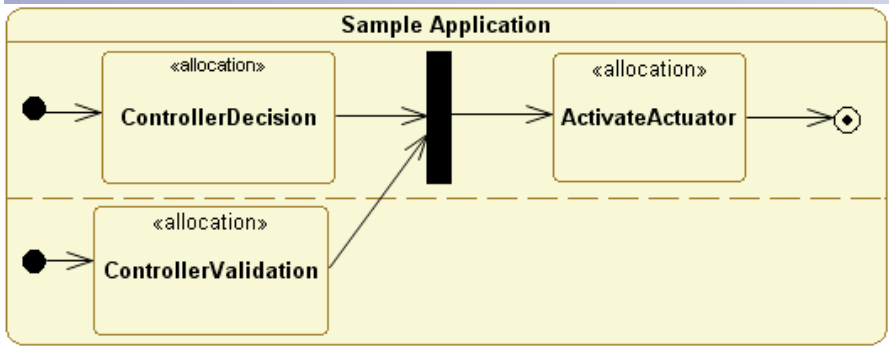


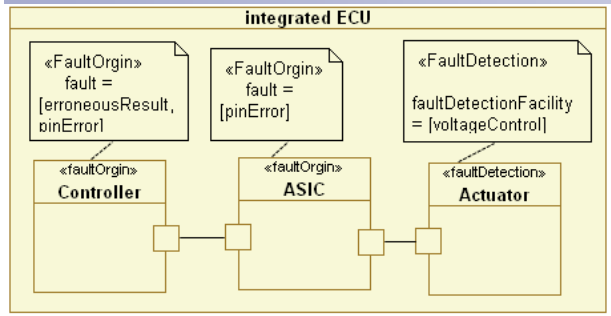
Example Application

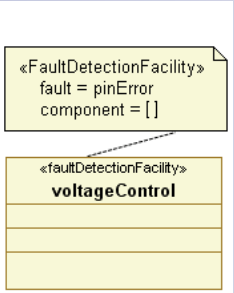


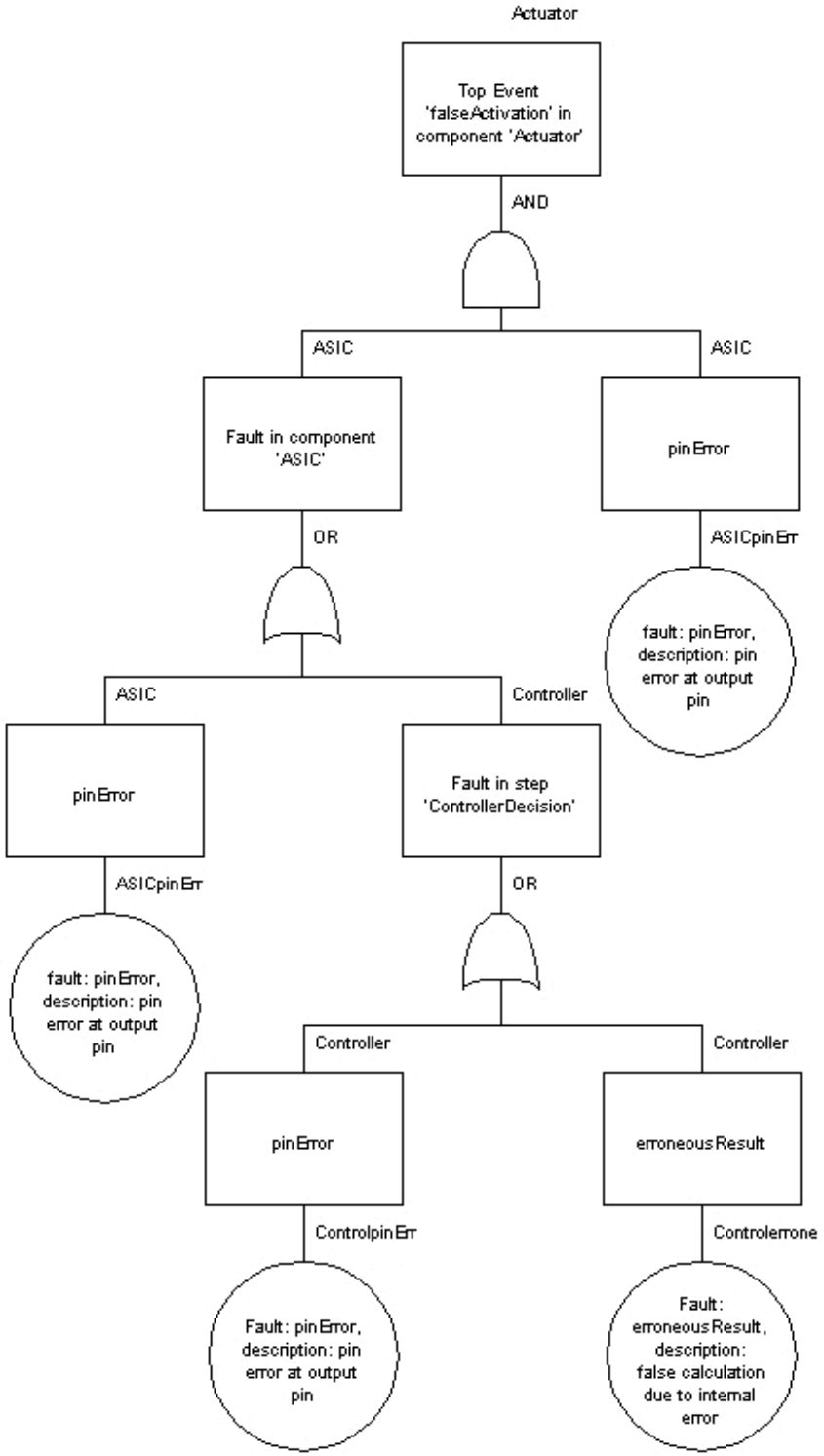


Example Tree1

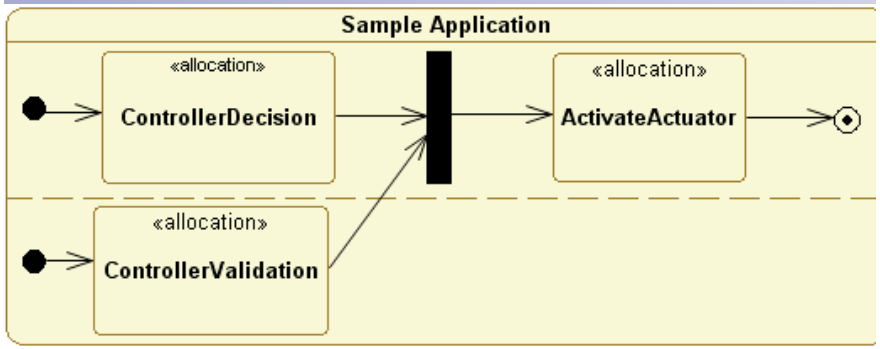


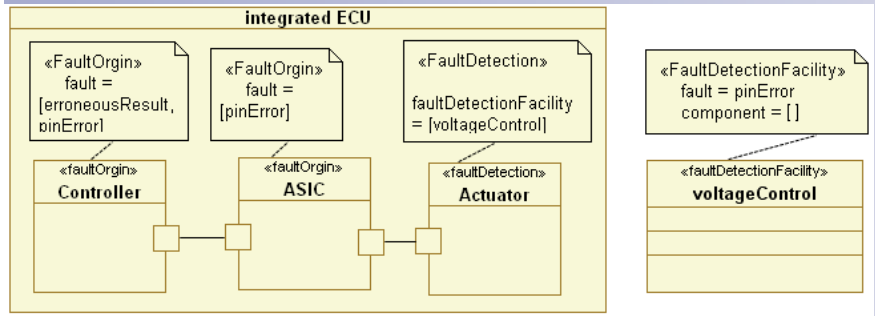


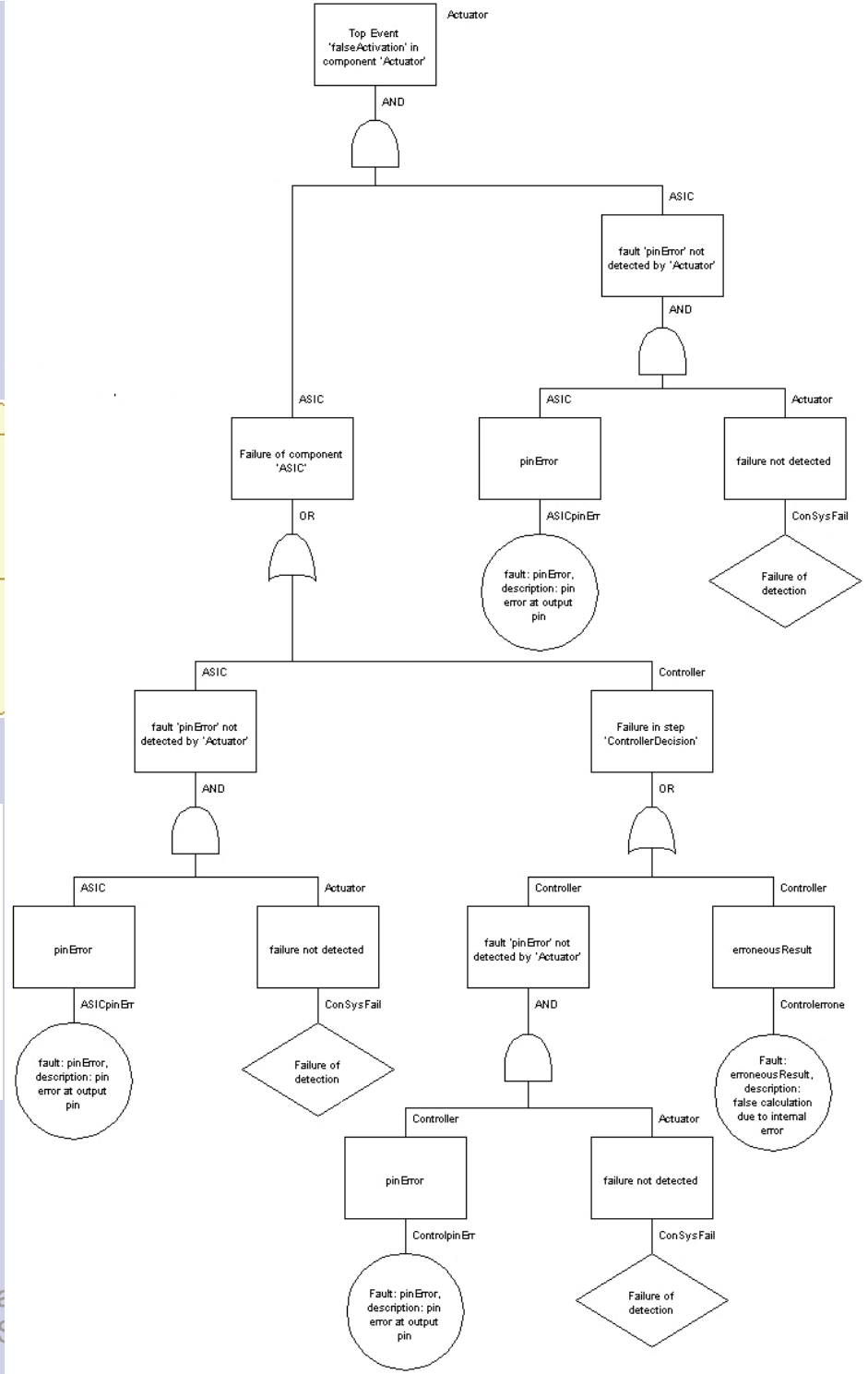




Example Tree2







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