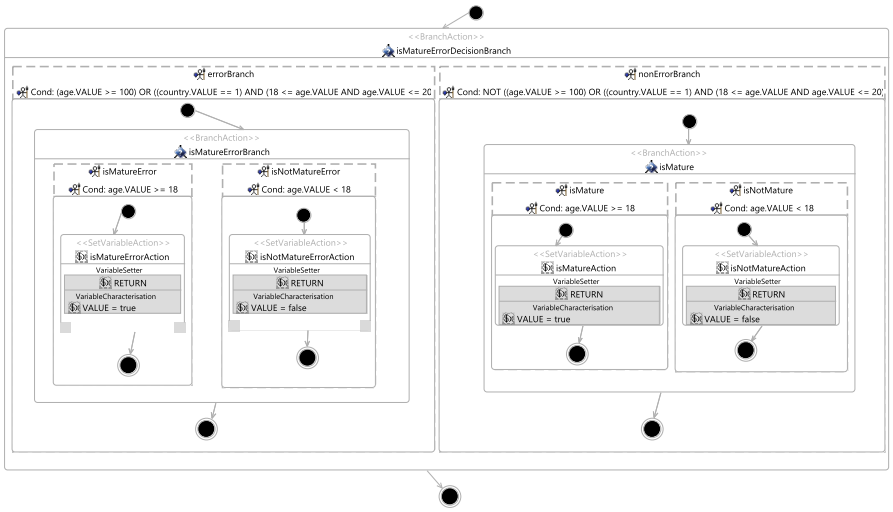
Karlsruher Institut für Technologie

Institute of Information Security and Dependability (KASTEL)
Application-oriented Formal Verification
Prof. Dr. Bernhard Beckert

Master Thesis / Praxis der Forschung

Closing the Gap between Models and Programs



Background. Palladio is a tool to model component-based software architectures. A Palladio model consists of *components* that provide *services*. In addition, it contains service-effect specifications (SEFFs), which model relevant parts of a service's behavior. A SEFF's semantics differ depending on the use case: For example, SEFFs can be used to model information-flow properties, performance properties, or functional properties. Model-based analyses allow us to validate a system early in its design phase.

When we later implement the model as an object-oriented program, we want to ensure that the results of these analyses are still valid. To do this, the program must be a *refinement* of the model: The behavior of every implemented service must be in the boundaries described by its SEFF, such that the analysis of the SEFF can be transferred to its implementation.

Task. Your task is: (1) to define a formal semantics for SEFFs and suitable refinement notions for the different use cases described above; (2) to build a decision procedure that allows the user to establish a refinement relationship between a given SEFF and its implementation. Depending on the use case, different tools and techniques may be used for this, among them the Java Modeling Language (JML) and the JML deductive verification tool KEY.

Contact
Florian Lanzinger lanzinger@kit.edu Office 50.34R227