A Modelica Sub- and Superset for Safety-Relevant Control Applications

Bernhard Thiele* Bernhard.Thiele@dlr.de
Stefan-Alexander Schneider† stefan-alexander.schneider@bmw.de
Pierre R. Mai‡ pmai@pmsf.de

* German Aerospace Center (DLR), Institute for Robotics and Mechatronics, Germany
† BMW AG, 80788 München, Germany
‡ PMSF IT Consulting, Marzling, Germany

More and more embedded software components are specified in models representing the so-called high-level application that is then automatically transformed (usually via embedded C-code) into binary code that is executable on the embedded target. Despite Modelica's obvious suitability to efficiently create appropriate high fidelity system models, the utilization of Modelica for developing discrete control functions is not yet wide spread.

This can be attributed to: a) a somewhat too limited expressiveness in modeling discrete controller functions; b) the lack of a flexible, seamless development approach from the controller model comprising the *logical functions* to the *technical system architecture* (i.e., code running on the target platform) and last but not least c) because *safety-relevant software functions need means to achieve a high assurance level*, which is not supported with current Modelica (tools).

The aim of the paper is to study impacts of a safety-relevant development process (based on validated tools) to high-level, domain-oriented modeling languages (see Figure 1). In particular it proposes a sub- and superset of the modeling language Modelica suitable for safety-relevant software development, including tool validation. To illustrate the development using the proposed language elements an exemplary library (referred to as SAFEDISCRETECONTROL library) is presented and applied at an exemplary use case.

Keywords: embedded systems; functional safety; simulation; code generation; compiler; formal methods; validation; verification

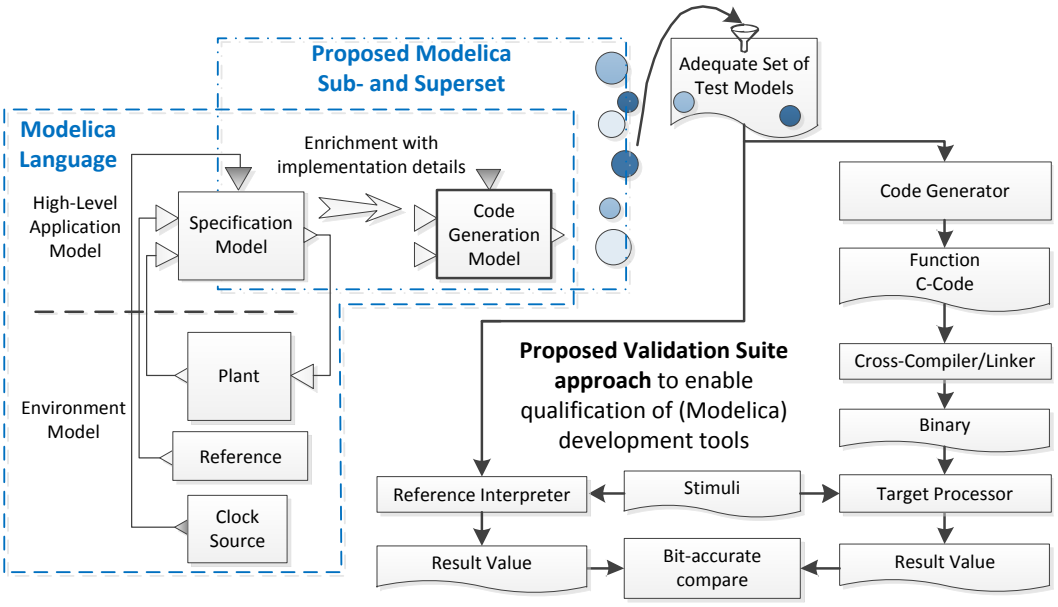

Figure 1: From High-Level Application Models (Specification Models) to code generation models utilizing a qualifiable sub- and superset of the Modelica language.