Abstract

The increasing complexity and safety-criticality of modern-day systems has introduced the need for comprehensive validation and provable safety assurance of these designs based on formal analysis. During the development phase, the designers need to consider four critical aspects of design, namely – *functional correctness*, *end-to-end timing*, *power performance* and *functional reliability*. Formal methods have been traditionally confined to ensuring functional correctness of a system using methods such as model checking and design intent verification. Recent research also focuses on guaranteeing stringent timing requirements of a system by choosing the timing layout for the constituent components.

However, functional correctness is only one of many aspects in modern engineering design. Performance parameters such as power, reliability etc. have become equally dominant aspects in determining the acceptability of a design. The work presented in the thesis is an enabler for early-stage formal certification of performance requirements, such as power intent and functional reliability. In particular, we have the following contributions:

Architectural Power Intent Validation: The rapid increase in design complexity and a stringent low-power budget make the power management schemes highly sophisticated. The logic behind these strategies are decided at the architectural level. Today there is a disconnection between the high-level architectural power management strategy which relates multiple power domains and the low-level assertions for controlling individual power domains. This poses two challenges in validating the power performance, namely:

- Verifying that the architectural power management strategy has been correctly implemented in the power-managed designs, and
- Estimating the power performance of an architectural power management strategy depending on typical usage profiles.

The first aspect is addressed in our proposed verification framework, based on our proposed tool, named `POWER-TRUCTOR`, that attempts to bridge the disconnect between high-level properties capturing the architectural power management strategy and the implementation of the power management control logic using low-level per-domain control signals. The second aspect is addressed by our proposed tool, named `POWER-SIM`, while deciding the power architecture of the integrated circuit and converging into the best power domain partitions before the power management logic is laid out.

Functional Reliability Analysis: Reliability is one of the critical factors in the development of safety-critical embedded designs such as automotive and avionic control systems, nuclear reactors, navigation/signaling systems etc. In the foreseeable future, reliability guarantees will become an integral part of safety-critical specifications, and will need to be formally specified and certified upfront in the design flow. This introduces the following three facets in reliability analysis:

- Formally expressing the functional reliability requirements leveraging the spatial and temporal redundancy provisions,
- Analyzing the system reliability (at an early-stage) as entailed by the reliability specifications of its constituent components, and
- Deriving the reliability gap from the given reliability choices of component-level properties and indicating the solution space to bridge the gap.

To address the above objectives, we provide novel formalisms to overlay reliability specifications on the functionality of a design and propose suitable methods to compute system reliability. Further, this work introduces the formal notion of reliability gap and proposes a divide-and-conquer algorithm to bridge the same.

Keywords: *Formal Verification, Power Management, VLSI / Integrated Circuits, Reliability*