Effective techniques for systems validation and security

Aleksa Damljanovic

17th September, 2021

Abstract

The increasing number of embedded instruments used to perform test, monitoring, calibration and debug within a semiconductor device has called for a brand new standard—the IEEE 1687. Such a standard resorts to a *Reconfigurable Scan Network* to provide efficient, reliable and flexible access to instruments and to handle complex structures. As it has to deliver reliable service, many approaches, both formal and simulation-based, have been proposed in the literature to perform test, diagnosis, and verification of such networks.

So far, most of the test-generation approaches were either too computationally demanding to be applied in complex cases, or too approximate to yield high-quality tests. A recent idea has been exploited in this thesis in a following manner: the state of a generic reconfigurable scan chain is modeled as a finite state automaton and a low-level fault, as an incorrect transition; it then proposes a new algorithm for generating a functional test sequence able to detect all incorrect transitions far more efficiently than previous ones. Such an algorithm is based on a greedy search, and it is able to postpone costly operations and eventually minimize their number. Experimental results demonstrate that the proposed approach is broadly applicable; has limited computational requirements; and the test sequences are order of magnitudes shorter than the ones previously generated by approximate methodologies. Together with testing the system for defects that may affect the scan chains themselves, the diagnosis of such faults is also important. Therefore, a method has been proposed for generating stimuli to precisely identify permanent high-level faults in a IEEE 1687 reconfigurable scan chain. A chapter is dedicated to the problem of post-silicon validation of a network, a problem that has not been adequately addressed, yet. The mismatches between the specification and its silicon implementation were analyzed, and then a methodology was proposed to detect a subset of them by applying functional patterns and observing the length of the active scan path.

While reconfigurable scan networks are commonly used to provide fault management and embedded instrumentation access, such as safety mechanisms, in advanced safety- and mission-critical electronic systems, a failure in such infrastructure itself has a high severity. Another aspect this thesis addressed is

assessment and mitigation of NBTI aging induced delays in logic paths within IEEE 1687 IJTAG Reconfigurable Scan Networks. This methodology is based on a scalable hierarchical (transistor-to-architecture) modelling of the NBTI impact on timing-critical logic paths in RSN implementations. The evaluation implies analysis of gate input signal probabilities based on the configurations and test data selected for the RSN infrastructure.

A fundamental part of the new IEEE Std 1687 is the Instrument Connectivity Language (ICL), which allows for abstract description of the scan network. The big novelty if compared to legacy solutions like BSDL is the possibility of describing new topology-enabling elements such as the ScanMuxes in a behavioural way which can be easily and efficiently exploited by Test Generation Tools to retarget instrument-level operations to top-level patterns. This means that for a given design, the Developer will have to write both the RTL and the ICL descriptions: to the author's best knowledge there is no automated tool to make the translation RTL to ICL. This methodology is error-prone due to the human factor, the difference in intent in the two descriptions and the syntactic and semantic complexity of the languages. Incoherence between ICL and RTL will result in retargeting errors, so it is fundamental to validate the equivalence between the two descriptions. In this thesis an automated methodology is presented that starting from the ICL description is able to generate a set of RTL testbenches that can be simulated against the original RTL model to detect discrepancies and incoherence, and provides quantitative metrics in terms of code and functional coverage.

Experimental results for these approaches are reported on the set of ITC2016 set of benchmark networks.

Recent trends in integrated circuits industry include decentralization of the production flow by involving different integration teams, third-party IP vendors and other untrusted entities. As a result, this is opening up a door to new types of attacks that may lead to devastating consequences, such as denial of service or data leakage. Therefore, the problem of ensuring hardware security has gained much attention in the last years, especially early in the design cycle, when an attacker may insert malicious circuitry at register transfer (RT) or gate level – a Hardware Trojan. Due to the increased complexity of modern devices, the research community is spending a lot of effort in developing more sophisticated detection methodologies and smarter attacks. However, the main problem is that they are validated on the existing benchmarks that do not reflect the real complexity. Trying to fill this gap, this thesis proposes a set of RT-Level Hardware Trojan benchmarks injected in a RISC-based pipelined microprocessor core. To prove the viability, the impacts on area, power and frequency are presented and discussed. For any proposed Hardware Trojan, the functional description, the implementation details and the effects once activated are provided.

Furthermore, despite the considerable effort that has been invested in this area, the ever-growing complexity of the modern devices always calls for sharper detection methodologies. In this regard, the last chapter of the thesis illustrates a pre-silicon, simulation-based techniques to detect Hardware Trojans.

The technique exploits well-established machine learning algorithms. All of the background concepts are presented together with the methodology and the automatized flow. The validity of the approach has been demonstrated on the *AutoSoC* CPU, an industrial-grade, safety-oriented, automotive benchmark suite. Experimental results demonstrate the applicability and effectiveness of the approach: the proposed technique is highly accurate in pinpointing suspicious code sections. None of the Trojans from the set has been left undetected.