Chapter 13
Industrial Applications of Emulation Techniques for the Early Evaluation of Secure Low-Power Embedded Systems

Norbert Druml
Graz University of Technology, Austria

Andreas Genser
Infineon Technologies Austria, Austria

Manuel Menghin
Graz University of Technology, Austria

Josef Haid
Infineon Technologies Austria, Austria

Christian Steger
Graz University of Technology, Austria

Holger Bock
Infineon Technologies Austria, Austria

Armin Krieg
Infineon Technologies Austria, Austria

Johannes Grinschgl
Independent Researcher, Austria

ABSTRACT

Embedded systems that follow a secure and low-power design methodology are, besides keeping strict design constraints, heavily dependent on comprehensive test and verification procedures. The large set of possible test vectors and the increasing density of System-on-Chip designs call for the introduction of hardware-accelerated techniques to solve the verification time problem. As already described earlier, emulation-based methodologies based on FPGA evaluation platforms prove capable of providing a solution compared to traditional system simulation. This chapter gives an introduction into a multi-disciplinary emulation-based design evaluation and verification methodology that is based on various techniques that have been presented in chapter 5. Test and verification capabilities are enhanced by the augmentation of this approach using model-based analysis units: gate-level-based power consumption models, power supply network models, event-based performance monitors, and high-level fault modes. The feasible usage of this verification methodology in the field of contactlessly powered smart cards is finally demonstrated using several industrial case studies.

DOI: 10.4018/978-1-4666-6194-3.ch013

INTRODUCTION

Semiconductor industry advances have led to technology capabilities permitting the integration of an increasing number of features on the same chip size. This comes along with a number of challenges, first, the increasing susceptibility of these systems to power and supply voltage variations translating to higher demands in system reliability. Second, a growing number of these highly integrated systems are deployed in security applications (electronic passports, electronic payment, etc.), yielding higher requirements in system security.

In recent years, however, the industry has faced a multitude of design challenges. First, the lack of rich design tools and effective design methodologies has caused an emerging productivity gap between the potential of presently available technology and the exploitation of its potential (ITRS Working Group, 2012, ITRS). Second, the late design phase applicability of many tools has blocked designers from investigating the potential design issues and introducing countermeasures early in the design phase. Early design phase monitoring of the following physical parameters such as, system performance, power and supply voltage, and security-relevant system behavior, is essential in order to reduce the productivity gap and to further push semiconductor advances.

Figure 1 illustrates a typical industrial near-field communication (NFC) system giving a prime example of contemporary power-constrained embedded systems. A smart-phone, a multi-feature and inherently power-constrained device, must provide power to the contactless smart card system (through a wireless air interface, e.g., ISO-14443 standard) by electromagnetic induction. This way of powering a device is described as a loosely power-coupled system. On the smart card end, power management is a critical issue due to the varying nature of its power supply and power consumption. While the strength of the electromagnetic field is set by the reader, the consumption is directly dependent on the smart card functions: it rises according to an increase in activity in its arithmetic and logic units and vice-versa. If power consumption is higher than power supply for a duration that cannot be compensated by draining the capacitor of its charge, then hazardous supply voltage drops can occur, which lead to operational failures. Contrarily, if power supplied is higher than power consumed for a duration that cannot be compensated by charging the capacitor up to its maximum voltage, then the excess energy is bled out of the system

Figure 1. Reader/smart card system and dedicated smart card power/voltage trends. Peak power consumption provokes hazardous supply voltage drops which may compromise the smart card's operational stability.