Chapter 5
Vulnerabilities of Secure and Reliable Low-Power Embedded Systems and Their Analysis Methods: A Comprehensive Study

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

Due to the increase in popularity of mobile devices, it has become necessary to develop a low-power design methodology in order to build complex embedded systems with the ability to minimize power usage. In order to fulfill power constraints and security constraints if personal data is involved, test and verification of a design's functionality are imperative tasks during a product's development process. Currently, in the field of secure and reliable low-power embedded systems, issues such as peak power consumption, supply voltage variations, and fault attacks are the most troublesome. This chapter presents a comprehensive study over design analysis methodologies that have been presented in recent years in literature. During a long-lasting and successful cooperation between industry and academia, several of these techniques have been evaluated, and the identified sensitivities of embedded systems are presented. This includes a wide range of problem groups, from power and supply-related issues to operational faults caused by attacks as well as reliability topics.

DOI: 10.4018/978-1-4666-6194-3.ch005

Copyright © 2014, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

INTRODUCTION

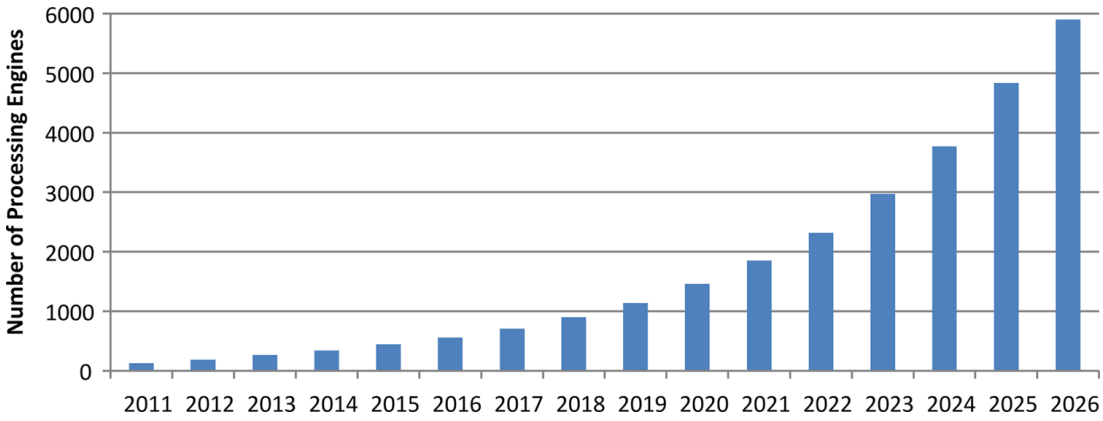
Tremendous steps forward in improving the density of silicon integration in recent years have introduced significant challenges for system engineers. An increasing number of new features have been integrated while development and implementation cycles have simultaneously decreased. This System on Chip (SoC) design complexity trend for portal devices is highlighted by Figure 1, as presented by the International Technology Roadmap for Semiconductors (ITRS Working Group, 2012, ITRS). Apart from consumer electronics, such highly integrated portable SoCs are also used in critical fields with high reliability and security demands. Because of this ever-increasing complexity, exhaustive test coverage of novel designs is difficult to achieve. As a consequence, support of system designers is needed during the whole design phase to test new hardware and software designs for possible weaknesses, as outlined by Ravi et al. (2004).

In addition to design flaws caused by complexity, there is the increasing fault probability provoked by deep sub-micron silicon integration technologies, as outlined by the latest ITRS report (ITRS Working Group, 2012, ITRS). This is a major issue especially for high safety applications (e.g., automotive, space, aviation). Therefore, a wide variety of fault injection techniques have been developed during the last few years to test the resistance of hardware/software designs against random faults, cf. for example Leveugle (2007).

The portable SoCs' trend of complexity increase is accompanied by an increase of power consumption, as depicted by Figure 2. This power consumption increase introduces major problems in several aspects. For example, mobile devices come with a limited power budget due to the limitations of batteries: the higher the power consumption, the lower the operational time. As another example, state-of-the-art integrated circuits use low supply voltage levels. This low-voltage approach causes high changing electrical currents, which requires sophisticated power supply networks to cope with the dynamic impedance of the chip. This is especially a problem for energy harvesting systems such as contactless reader / smart card systems.

In addition to complexity and power consumption challenges, secure embedded systems face the problem of the potential leak of critical information through side channels. A device's power consumption, for example, may disclose such crucial information, because of its data dependency. Thus, an adversary is able to deduce the internal secrets simply by observing the device's power consumption.

Figure 1. Design complexity trend of portable SoCs



19 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/vulnerabilities-of-secure-and-reliable-low-power-embedded-systems-and-their-analysis-methods/116106

Related Content

Method Using Command Abstraction Library for Iterative Testing Security of Web Applications
Seiji Munetohand Nobukazu Yoshioka (2018). *Application Development and Design: Concepts, Methodologies, Tools, and Applications (pp. 192-215).*
www.irma-international.org/chapter/method-using-command-abstraction-library-for-iterative-testing-security-of-web-applications/188208

A Novel Approach for Detection of Moving Objects in Complex Scenes Using Fuzzy Colour Difference Histogram
Prerna Dewan, Nivedita Niveditaand Rakesh Kumar (2021). *International Journal of Software Innovation (pp. 81-101).*
www.irma-international.org/article/a-novel-approach-for-detection-of-moving-objects-in-complex-scenes-using-fuzzy-colour-difference-histogram/277216

A Study on Deep Learning Model Autonomous Driving Based on Big Data
Yoki Donzia Symphorien Karl, Haeng-Kon Kimand Young-Pil Geum (2021). *International Journal of Software Innovation (pp. 143-157).*
www.irma-international.org/article/a-study-on-deep-learning-model-autonomous-driving-based-on-big-data/289174

Towards Construction of Business Components: An Approach to Development of Web-Based Application Systems
Dentcho N. Batanovand Somjit Arch-int (2003). *Practicing Software Engineering in the 21st Century (pp. 178-194).*
www.irma-international.org/chapter/towards-construction-business-components/28118

Knowledge Management in Software Process Improvement: A Case Study of Very Small Entities
Shuib Bin Basriand Rory V. O'Connor (2011). *Knowledge Engineering for Software Development Life Cycles: Support Technologies and Applications (pp. 273-288).*
www.irma-international.org/chapter/knowledge-management-software-process-improvement/52888