Dipl.-Ing. Norbert Druml, BSc

Design Evaluation Framework for Secure and Low-Power Embedded Systems

DISSERTATION

zur Erlangung des akademischen Grades

Doktor der technischen Wissenschaften

eingereicht an der

Technischen Universität Graz

Betreuer

Em.Univ.-Prof. Dipl.-Ing. Dr.techn. Reinhold Weiß

Institut für Technische Informatik

Graz, Juni 2014

EIDESSTATTLICHE ERKLÄRUNG

AFFIDAVIT

Ich erkläre an Eides statt, dass ich die vorliegende Arbeit selbstständig verfasst, andere als die angegebenen Quellen/Hilfsmittel nicht benutzt, und die den benutzten Quellen wörtlich und inhaltlich entnommenen Stellen als solche kenntlich gemacht habe. Das in TUGRAZonline hochgeladene Textdokument ist mit der vorliegenden Dissertation identisch.

I declare that I have authored this thesis independently, that I have not used other than the declared sources/resources, and that I have explicitly indicated all material which has been quoted either literally or by content from the sources used. The text document uploaded to TUGRAZonline is identical to the present doctoral dissertation.

Datum / Date

Unterschrift / Signature

Kurzfassung

Im Laufe der letzten Jahrzehnte sind Komplexität und Integrationsdichte integrierter Schaltungen und eingebetteter Systeme exponentiell gewachsen. Diese Entwicklung bringt zahlreiche negative Nebeneffekte mit sich: Unter anderem kommt es zu einer verstärkten Leistungsaufnahme und einer damit einhergehenden erhöhten thermischen Beanspruchung. Daneben führt dieser exponentielle Trend zu einem Anstieg gleichzeitig schaltender Transistoren, wodurch Spannungsversorgungseinbrüche verursacht werden können. Ferner beeinträchtigt die Verwendung neuartiger submikroner Fertigungstechniken die Zuverlässigkeit integrierter Schaltungen und eingebetteter Systeme.

Die vorliegende Arbeit behandelt die dargestellten Probleme, die während der Entwicklung integrierter Schaltungen und komplexer eingebetteter Systeme auftreten können. Sie gliedert sich in die folgenden vier Phasen: Die erste Phase bietet einen Überblick über aktuelle Schwachstellen eingebetteter Systeme, die als sicher gelten und geringe Leistung aufnehmen. Phase zwei präsentiert ein emulations- und simulations-basiertes Framework, das Entwickler in allen Designstadien von eingebetteten Systemen unterstützen soll. Durch die beispielhafte Anwendung des Frameworks an kontaktlosen Leser / Smart Card Systemen (RFID, NFC) zeigt diese Arbeit wie wichtig es ist, eingebettete Systeme in ihrer Gesamtheit zu analysieren. Dabei wird ferner veranschaulicht, dass Designfehler frühzeitig erkannt und behoben werden können. Phase drei sucht mit Hilfe des in Phase zwei eingeführten Frameworks nach Leistungsaufnahme- und Sicherheitsoptimierungen für kontaktlose Leser / Smart Card Systeme. Basierend auf den in Phasen eins bis drei gewonnen Erfahrungen, wird in der letzten Phase dieser Arbeit eine auf RFID und NFC basierende sichere Schnittstellentechnik präsentiert, die in jeglichen elektronischen Geräten integrierbar ist. Diese Schnittstellentechnik benötigt zum Betrieb ausschließlich jene vom magnetischen Feld zur Verfügung gestellte Energie und ermöglicht es, das angesteuerte elektronische Gerät während der Standby-Zeiten komplett abzuschalten.

Abstract

Over the past few decades, integrated circuits and embedded systems have increased exponentially in their complexity and in integration density. This complexity trend entails many negative consequences: amongst others, it leads to a potential increase of power consumption and thermal stress. Moreover, it leads to large numbers of simultaneously switching transistors which may cause power supply issues. In addition, deep-submicron manufacturing processes in conjunction with environmental disturbances adversely affect the reliability properties of integrated circuits and embedded systems.

This doctoral thesis addresses the issues outlined above, which may arise during the development of integrated circuits and complex embedded systems, and is divided into the following four phases: phase one provides an overview of possible vulnerabilities of contemporary secure and low-power embedded systems. Phase two proposes an emulation-based and simulation-based framework that supports engineers throughout the design phases. By applying this framework to secure and contactless reader / smart card systems (RFID, NFC), this work outlines the importance of complete system evaluations. Moreover, this framework is used to detect and resolve design flaws and to evaluate design optimizations early, before the tape-out. Phase three employs the same framework in order to explore and propose optimization possibilities considering the security of reader / smart card systems and their management of electrical power. Based on the experiences made in phase one to three, the last phase presents a secure RFID-based and NFC-based interface for everyday electronic devices. This interface exploits the reader emitted electrical power to provide a secure zero-energy communication interface and to support a zero-energy standby mode for the targeted electronic device.

Acknowledgements

First and foremost, I would like to thank Prof. Reinhold Weiß for the supervision of this doctoral thesis and the opportunity to contribute to this cutting edge field of research. I am especially grateful to Christian Steger for his helpful advice and professional guidance throughout the project.

I would like to express my special appreciation and thanks to Josef Haid for his valuable technical and scientific support. I would also like to thank Holger Bock and Thomas Ruprechter for their efficient project management. In addition, a thank you to Robert Hofer and Christian Goral, who helped with all aspects of firmware and software development.

Special thanks also go to Andreas Genser, Armin Krieg, and Johannes Grinschgl for their useful critiques and constructive discussions during this project. In particular, I would like to express my gratitude to my colleague Manuel Menghin for the great collaboration throughout almost three years of research, his helpful comments, and our creative discussions. I would also like to thank all my students for their contributions.

I wish to acknowledge the help by François Reney for his assiduous and thorough correction work.

Furthermore, I would like to thank the following project partners for enabling and supporting this project:
Austrian Federal Ministry for Transport, Innovation, and Technology
Infineon Technologies Austria AG
Enso Detego GmbH

Finally, my greatest gratitude belongs to my family, friends, and partner for supporting, encouraging, and guiding me throughout my life.

Graz, June 2014 Norbert Druml

Extended Abstract

As Gordon Moore postulated in 1955, we are experiencing a trend that shows an exponential increase in the complexity of integrated circuits and embedded systems. Thanks to the steady improvement of manufacturing processes (e.g., decreasing transistor sizes, three dimensional integration), this complexity trend is still occurring and will continue for a number of years. However, this complexity trend introduces unwanted side effects: high integration densities may increase power consumption and thermal stress as well as accentuate the negative impacts on the power supply if large numbers of transistors switch simultaneously. In addition, dependability issues arise due to the deep-submicron manufacturing processes which make integrated circuits more prone to environmental disturbances.

When integrated circuits and embedded systems are developed, it is highly important to test the hardware and software designs with regards to power, security, and dependability threats. The earlier an issue can be detected during a product's development cycle, the lower the costs are to resolve the issue. In order to evaluate the functionality of a given hardware / software design, simulation-based and hardware emulation-based techniques are generally used. While simulation-based tools are flexible and provide both functional and non-functional analysis data, they tend to require much processing time at low abstraction levels. Emulation-based tools employ prototyping platforms, such as field programmable gate arrays (FPGAs), in order to accelerate time-intense analysis calculations. However, the majority of these emulation-based tools are unable to provide crucial non-functional analysis data such as power consumption and supply voltage behavior. In order to compensate for this gap, the former projects POWERHOUSE and POWER-MODES enhanced the hardware emulation analysis technique with power analysis and fault injection techniques. While these projects focused on the evaluation of single and isolated designs (e.g., a smart card design), they took crucial system aspects related to complex embedded systems only partially into account. The current follow-up project, META[:SEC:][1], aims to close this gap by regarding the system aspect of complex and resource constrained embedded systems, such as reader / smart card systems.

The present doctoral thesis, which is part of the META[:SEC:] project, addresses the highlighted threats when developing integrated circuits and complex embedded systems. It proposes a set of techniques and tools that support engineers during the design phase in order to detect and resolve design flaws and to evaluate design optimizations as soon as possible and preferably before the tape-out. The structure of this thesis can be illustrated in Figure 1 with four fields, containing the initial phase and three follow-up

[1] *Mobile Energy-efficient Trustworthy Authentication Systems with Elliptic Curve based SECurity*, collaborative research project of the Graz University of Technology, Infineon Technologies Austria AG, and Enso Detego GmbH. Funded by the Austrian Federal Ministry for Transport, Innovation, and Technology under the FIT-IT contract FFG 829586.

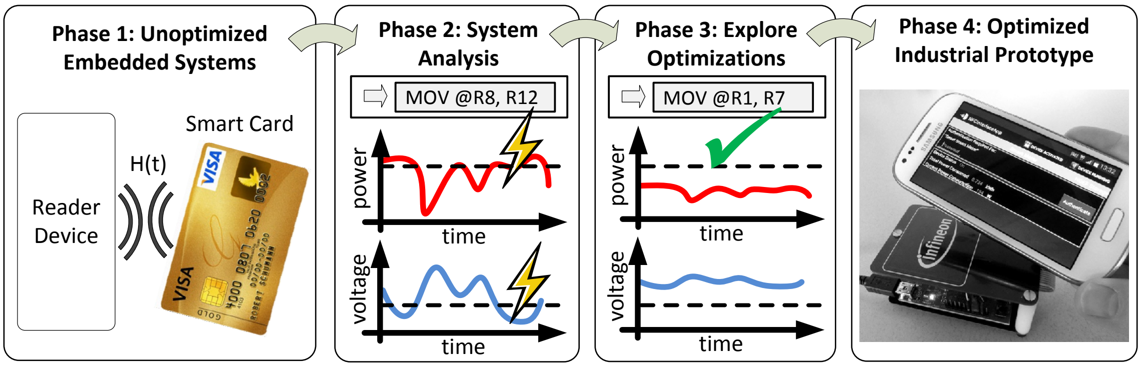


Figure 1: Doctoral thesis' four phases of contributions: starting from an unoptimized contactless reader / smart card system and heading to an optimized industrial prototype of an NFC interface.

phases of *system analysis*, *explore optimizations*, and *optimized industrial prototype*, which will be explained in the following paragraphs. Starting from the initial phase where an unoptimized embedded system (a contactless reader / smart card system) is given and where its vulnerabilities are outlined[2], this thesis presents in phase two a comprehensive emulation-based design evaluation framework[3,4]. This framework enables an engineer to test hardware and software designs with regards to functional and performance behavior, as well as their impact on power consumption and supply voltage levels. The proposed design evaluation technique is then enhanced in order to take into account crucial system aspects related to complex embedded systems[5]. Instead of analyzing isolated designs, such as a smart card, the total system consisting of reader, smart card, and the wireless communication channel can now be analyzed accurately. In a further step, this emulation-based design evaluation methodology is extended with fault injection functionalities[6]. This approach improves the analysis capabilities by emulating the consequences of faults on the system's functionalities. This analysis is especially important for secure and dependable embedded systems. Although state-of-the-art emulation-based techniques deliver accurate analysis results for each clock cycle, they lack in flexibility (e.g., each VHDL/Verilog code change needs to be re-synthesized, which is time consuming). Therefore, a flexible high-

[2] *Druml et al., Vulnerabilities of secure and reliable low-power embedded systems and their analysis methods - A comprehensive study*, Industry and Research Perspectives on Embedded System Design, IGI Global, March 2014.

[3] *Druml et al., Industrial applications of emulation techniques for the early evaluation of secure low-power embedded systems*, Industry and Research Perspectives on Embedded System Design, IGI Global, March 2014.

[4] *Druml et al., Emulation-Based Test and Verification of a Design's Functional, Performance, Power, and Supply Voltage Behavior*, 21st Euromicro International Conference on Parallel, Distributed, and Network-Based Processing (PDP), Belfast, Ireland, 27th of February - 1th of March 2013.

[5] *Druml et al., Emulation-Based Design Evaluation of Reader / Smart Card Systems*, 24th IEEE International Symposium on Rapid System Prototyping (RSP), Montreal, Canada, 3-4th of October 2013.

[6] *Druml et al., Emulation-Based Fault Effect Analysis for Resource Constrained, Secure, and Dependable Systems*, 16th Euromicro Conference on Digital System Design (DSD), Santander, Spain, 4-6th of September 2013.

level SystemC-based framework[7] is proposed, which enables fast but less accurate design analysis. This framework focuses on reader / smart card systems and features, besides functional and power analyses, the analysis of the effects of faults which are caused by, for example, power issues or thermal stress.

With the help of these emulation-based and simulation-based design evaluation techniques, this doctoral thesis' third phase is introduced: system-level power, thermal, and security optimization techniques are explored for reader / smart card systems. The first proposed power optimization approach estimates the smart card's power consumption and its supplied power, the latter being set by the strength of the alternating magnetic field emitted by the reader[8]. Based on these estimates, the smart card's voltage and clock frequency parameters are adapted to save electrical power and to prevent hazardous supply voltage variations. The second power optimization approach scales the strength of the reader emitted magnetic field based on the smart card's executed commands and power consumption[9]. During the smart card's low power consuming commands (e.g., read memory) the magnetic field strength is reduced, during high power consuming commands (e.g., cryptographic operations) the magnetic field strength is increased. As a result, the reader / smart card system is able to save up to 54% of the electrical energy required for its operation compared to static magnetic field strengths that are used nowadays. Such system-level power savings are of high importance in the field of mobile applications (e.g., customs officers read passports with mobile battery powered reader devices). In addition to these power optimizations, a thermal-aware smart card design is proposed for applications that face high magnetic field strengths. This thermal-aware design improves the smart card electronics' life time by up to 11% due to the reduction of thermal hot spots. Finally, optimizations in the research field of elliptic-curve cryptography for resource constrained embedded systems, such as contactless reader / smart card systems, are proposed and evaluated. First, hardware / software partitioning optimizations are analyzed in order to accelerate elliptic-curve-based computations[10]. Second, protocol optimizations are demonstrated that permit a shifting of computational effort from the resource constrained embedded system to the computational powerful reader[11].

During this thesis' last phase, the insights gained from the system design analysis and optimization phases are employed to develop an industrial prototype which introduces a

[7] *Druml et al., Power and Thermal Fault Effect Exploration Framework for Reader / Smart Card Designs*, 16thEuromicro Conference on Digital System Design (DSD), Santander, Spain, 4-6thof September 2013.

[8] *Druml et al., Estimation Based Power and Supply Voltage Management for Future RF-Powered Multi-Core Smart Cards*, Design, Automation & Test in Europe Conference & Exhibition (DATE), Dresden, Germany, 12-16thof March 2012.

[9] *Druml et al., Adaptive Field Strength Scaling - A Power Optimization Technique for Contactless Reader / Smart Card Systems*, 15thEuromicro Conference on Digital System Design (DSD), Izmir, Turkey, 5-8thof September 2012.

[10] *Höller et al., Hardware/Software Co-Design of Elliptic-Curve Cryptography for Resource-Constrained Applications*, 51thACM / EDAC / IEEE Design Automation Conference (DAC), San Francisco, USA, 1-5thof June 2014.

[11] *Druml et al., A Flexible and Lightweight ECC-Based Authentication Solution for Resource Constrained Systems*, 17thEuromicro Conference on Digital System Design (DSD), Verona, Italy, 27-29thof August 2014 (under review).

secure Near Field Communication (NFC) interface for everyday electronic devices[12,13]. This interface employs the electrical power emitted by the reader to provide a zero-energy communication interface and to support a zero-energy standby mode for the targeted electronic device.

The research carried out during this doctoral thesis opens up possibilities for further research topics in the fields of hardware / software design evaluation and of power management. Since the effects of the deep-submicron manufacturing process' variability on hardware and software is becoming a major issue, the emulation-based design evaluation framework in this thesis could be enhanced with process variability parameters, which would enable variability-aware software evaluations. The findings presented in this thesis could also be used in the field of power and thermal behavior analysis of 3D-integrated circuits. Since heat sinks of 3D-integrated circuits are implemented differently, software running on these chips must be aware of this fact in order to prevent harmful thermal hot spots. In addition to these design analysis techniques, power management of future environmental powered and highly integrated circuits offers novel research opportunities. Prediction-based and estimation-based power management techniques may act (e.g., throttling the smart card CPU) before hazardous peak power consumption or supply voltage drops happen. Whereas, state-of-the-art power management techniques that are currently used are only able to react after a peak power consumption or a supply voltage drop have been detected.

[12] *Druml et al., NIZE - A Near Field Communication Interface Enabling Zero Energy Standby for Everyday Electronic Devices*, 8$^{\text{th}}$International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Barcelona, Spain, 8-10$^{\text{th}}$of October 2012.

[13] *Druml et al., A Zero-Energy NFC Solution for Everyday Electronic Devices*, e & i Elektrotechnik und Informationstechnik, November 2013.

Contents

List of Figures

List of Tables

List of Abbreviations

AES	Advanced Encryption Standard
AFSS	Adaptive Field Strength Scaling
ASIP	Application Specific Instruction-set Processor
CMOS	Complementary Metal Oxid Semiconductor
DES	Data Encryption Standard
DPA	Differential Power Analysis
DVFS	Dynamic Voltage and Frequency Scaling
ECC	Elliptic-Curve Cryptography
FIFO	First In - First Out
FPGA	Field Programmable Gate Array
IEEE	Institute of Electrical and Electronics Engineering
IP	Intellectual Property
ITRS	International Technology Roadmap for Semiconductors
MPSoC	Multi-Processor System on Chip
MTTF	Mean Time To Failure
NoC	Network on Chip
NFC	Near Field Communication
PE	Power Emulation
RAM	Random Access Memory
RFID	Radio Frequency Identification
RoTD	Rest of Target Device
RTL	Register Transfer Level
RSA	Ron Rivest, Adi Shamir, and Leonard Adleman
SHA	Secure Hash Algorithm
SoC	System on Chip
SPA	Simple Power Analysis
SPARC	Scalable Processor Architecture
VHDL	Very High Speed Integrated Circuit Hardware Description Language

Glossary

Hardware Emulation
Hardware emulation is a technique that integrates a hardware design into a reconfigurable (e.g., FPGA-based) prototyping platform in order to permit the functional testing of a design-under-test including its firmware. This way both hardware and software can be evaluated in a realistic setting.

Power Emulation
Power emulation extends the hardware emulation technique with power sensors and corresponding power models in order to retrieve estimated power analysis data of the design-under-test.

Supply Voltage Emulation
Supply voltage emulation extends the hardware emulation and power emulation approaches with a model of the design-under-test's power supply network. Thus, design-under-test's supply voltage behavior can be estimated directly by the hardware.

Vulnerability
Vulnerability in the context of electrical engineering describes a certain inability of a system to withstand the effects of an attack in a hostile environment.

Fault Attack
A fault attack is an intentional manipulation of the integrated circuit or its state, with the aim of provoking an error within the integrated circuit in order to move the device into an unintended state. The goal is to access security critical information or to disable internal protection mechanisms.

Error
An error defines a deviation between the expected behavior and the actual behavior of a given system. Errors are caused by faults that were activated.

Smart Card
A smart card is a device with an integrated circuit that includes its own memory and central processing unit. Apart from a standard contact-based interface, it can also be powered contactlessly by means of an alternating and modulated magnetic field, through which contactless communication is also enabled.

System-on-Chip
A System-on-Chip (SoC) represents an integrated circuit integrating all circuits and electronics (such as analog, digital, mixed-signal, or RF components) necessary for a system on a single chip.

Chapter 1

Introduction

1.1 Motivation

1.1.1 Computational Performance Development - The Sixth Paradigm

Raymond Kurzweil, author, inventor, futurist, and director of engineering at Google Inc., portrayed in his book ”The Singularity Is Near: When Humans Transcend Biology”, published in 2005, an exponential progress of human evolution [1]. Currently, major innovations are made approximately every ten years. However, the time between major innovations is decreasing rapidly. Kurzweil predicts that a so-called point of singularity

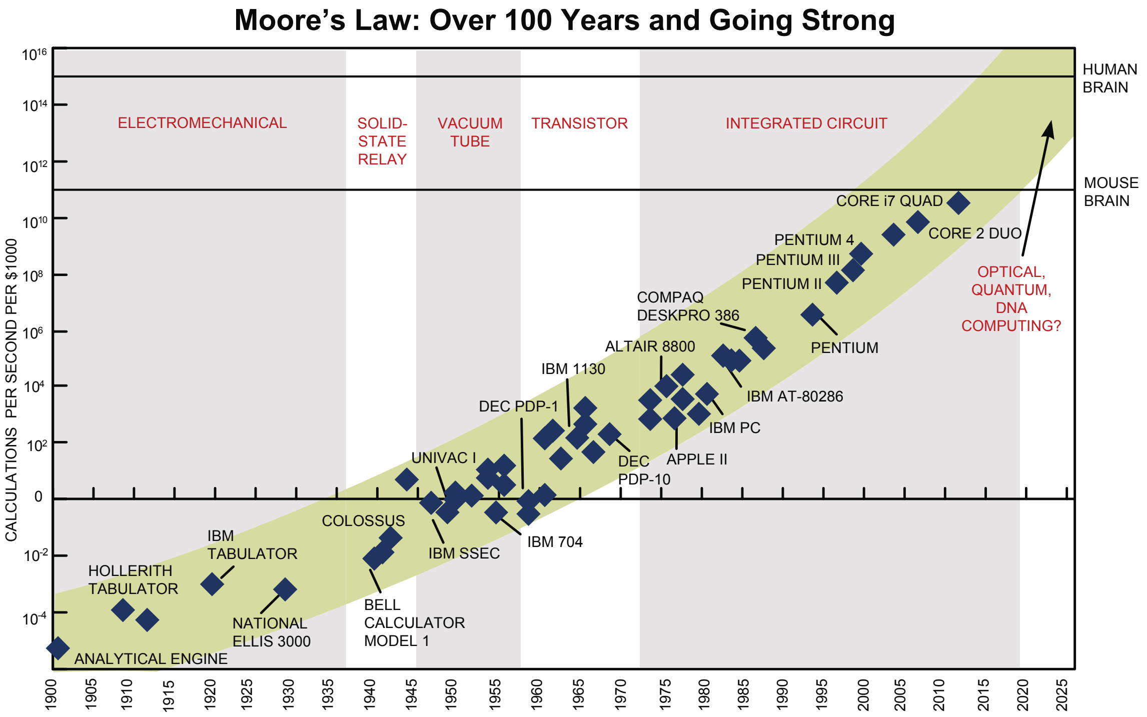


Figure 1.1: Exponential computational performance growth according to [1]. Obtained with changes from [2].

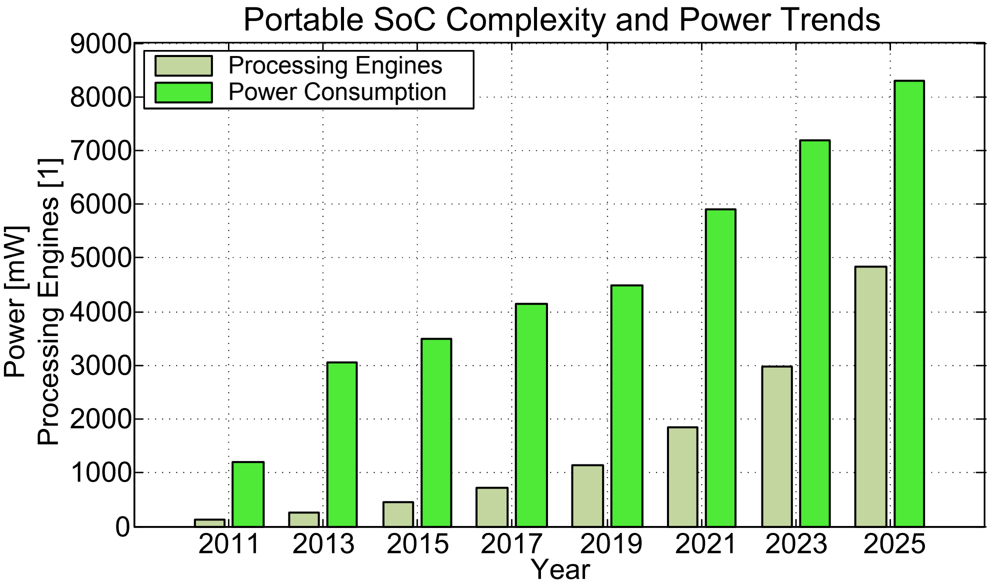


Figure 1.2: Integrated processing engines and power consumption trends of consumer portable SoCs. Obtained with changes from [3].

will be reached once technical progress exceeds the human capability to comprehend it. Apart from the field of computation performance, exponential development trends are experienced in various other fields, such as miniaturization of mechanical devices, DNA sequencing costs, data traffic, solar energy generation, etc. The exponential growth of computation performance and integrated circuits, which has been postulated by Gordon Moore in 1965, is depicted in Figure 1.1. Kurzweil extended Moore's vision and classified the historical computational performance trend into five paradigms starting in 1900: electromechanical, solid-state relays, vacuum tube, transistor, and integrated circuit technologies. He predicted that by around the year 2020 computational resources worth $1,000 will compare to the performance of a human brain. However, at the same time, the semiconductor industry expects to reach the limits of miniaturization in integrated circuit technology. The technology that follows integrated circuits and ushers in the sixth paradigm is still unknown, but nanotube circuits, optical-, quantum-, or DNA-computing are promising candidates according to Kurzweil.

1.1.2 Challenges in Integrated Circuit Technology

Figure 1.2 highlights, according to the International Technology Roadmap for Semiconductors (ITRS) [3], the complexity trends in the field of consumer portable System-on-Chips (SoCs) represented in terms of implemented processing engines (i.e., special purpose processors such as cryptographic cores) and the SoC's expected dissipated electrical power. While the number of embedded processing engines should increase exponentially as predicted by Moore and Kurzweil, ITRS expects the power consumption to increase by a linear factor. This linear power consumption development can be explained by the increasing power awareness of software and hardware engineers, adoption of low-power integrated circuit designs, and advantages gained from scaling the CMOS technology. In [17], Borkar outlines the main goals and achievements when performing a scale of one technology generation by means of the scaling theory:

- a reduction of the gate delay by 30% results in an increased operation frequency of about 43%,
- the vertical and lateral dimension decrease by 30% which results in a doubling of the transistor density,
- and a 65% reduction of energy per transistor switching activity is achieved which saves 50% of the power.

However, due to the physical limits of photolithography, which is used during the photomask fabrication process of semiconductors, integrated circuit scaling is becoming more difficult and more expensive. Apart from these costs, there are three other crucial issues that grow in size as the size of transistors is reduced. First, static leakage power consumption increases due to the reduction of the gate oxide thickness that allows more electrons to tunnel through this gate oxide to the substrate. Second, the variability of the manufacturing process increases which affects, among others, the performance and power consumption behavior of the manufactured chip. Third, external influences such as alpha particles, neutrons, or temperature, may charge nodes and hence cause memory cells or logic latches to flip, which is called a ”single event upset”. As outlined by Borkar in [4] and as illustrated in Figure 1.3, the semiconductor industry is facing an 8% increase of single event upsets from one manufacturing technology to the subsequent smaller one. Chips produced by means of deep-submicron (e.g., 16nm) manufacturing techniques, are approximately 130 times more susceptible to these external influences compared to the 180nm manufacturing technique. Single event upsets in memories can be detected and corrected by means of hardware integrated parity checks and error correction codes. However, if flip-flops are affected, single event upset detection and correction is difficult. Undetected and uncorrected single event upsets are especially dangerous in the field of secure and dependable embedded systems, because reliable operation should be provided even under faulty hardware conditions.

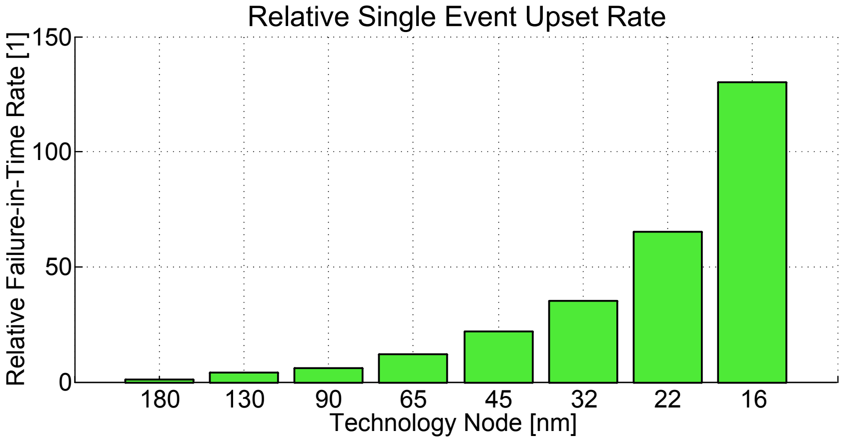


Figure 1.3: Relative single event upset rate depending on the manufacturing technology. Obtained with changes from [4].

1.1.3 Verification Trends in The Semiconductor Industry

Test and verification are essential in order to cope with the issues previously mentioned regarding the ever advancing complexity and scaling trends in integrated circuits. Figure 1.4 highlights the recent trends in the field of design verification in the semiconductor industry, according to [5] and the 2012 Wilson Research Group study. The left graph depicts the usage ratio trend of emulation-based and hardware accelerated design techniques during an Application Specific Integrated Circuit (ASIC) development process. This ratio increased by 117% between the years 2007 and 2012. Considering that complexity and circuit sizes of novel ASIC developments have shown a steady increase, emulation-based and hardware accelerated verification methods are employed frequently in order to cope with the increasing computation time of simulation-based verification approaches. The right graph of Figure 1.4 illustrates the ASIC development effort in terms of mean peak number of design engineers and verification engineers involved per project. Although design complexity and circuit sizes have increased according to Moore's law, the development effort has increased only slightly. This can be explained by the adoption of internal and external Intellectual Property (IP) cores as well as automation-based productivity improvements. However, the peak mean number of verification engineers has increased by a significant 75% during these five years, which approximately equals the amount of design engineering effort invested. This trend stresses the need for hardware accelerated evaluation and verification tools that can be used during early product development phases: the earlier design flaws are detected, the lower the cost are to resolve them.

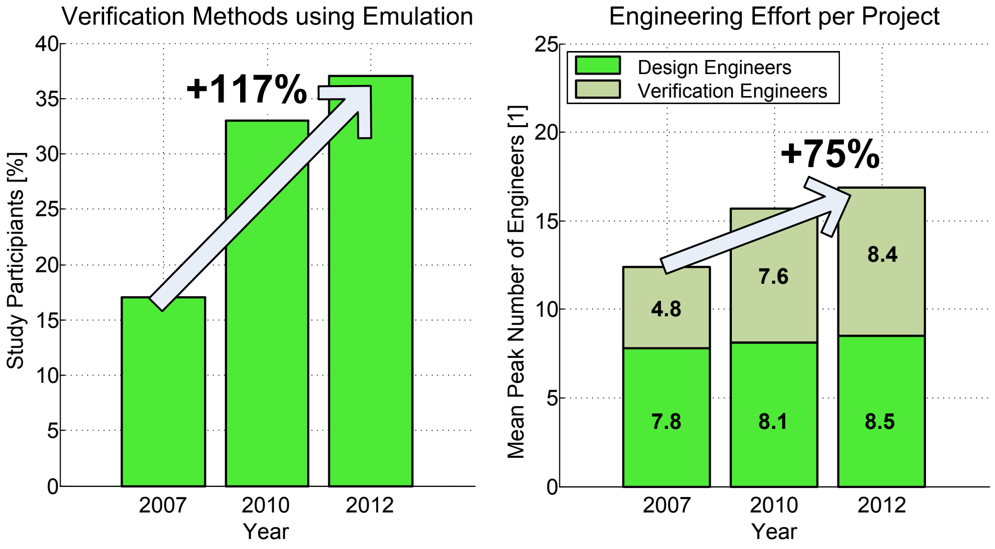


Figure 1.4: Recent trends in the field of design verification in the semiconductor industry. Obtained with changes from [5].

1.1.4 Motivational Example: Contactless Reader / Smart Card System

The number of battery-powered RFID and Near Field Communication (NFC)-based systems has increased significantly over the last few years. The left diagram of Figure 1.5 illustrates a typical setup of a mobile and contactlessly powered reader / smart card system. The reader device emits an alternating magnetic field that is used to power by electromagnetic induction the smart card and to transfer data by means of modulation. Such reader / smart card systems can be found in our everyday life, e.g., in the fields of access control, payment, loyalty and coupons, health care, logistics. According to a market study recently published by IDTechEx (cf. [18]), the market value of RFID-based devices, applications, and services will increase from \$9.2 billion to \$30.4 billion between the years 2014 and 2024. Due to this omnipresence and market penetration, security and power awareness are important concerns in order to make these systems viable for use and cost effective to operate. As illustrated by the right graph of Figure 1.5, contactlessly powered reader / smart card systems are very constrained in terms of available electrical power, computational resources, and chip size. During the smart card's peak power consumption (caused, e.g., by a high power consuming cryptographic algorithm), the supply voltage that is provided by the magnetic field may drop below a hazardous threshold, which may hence disrupt the smart card's operational stability if not handled properly. Due to these power supply constraints, reader devices commonly use high magnetic field strengths in order to allow a smart card to work properly. As a consequence, this approach limits a mobile reader's battery lifetime drastically. In addition, since a contactless communication link is used, security related threats exist, such as eavesdropping, man-in-the-middle attacks, etc. Testing security features of individual components during the product development phases may not be sufficient to cope with state-of-the-art security attacks: multi-attacks that are conducted on both reader and smart card simultaneously could bypass security precautions. Artificially injected faults within the reader could influence the smart card's power supply and, as a consequence, affect the smart card's operational stability. In addition, significant power consumption changes provoked by intentionally injected faults may disclose security relevant countermeasures, such as hardware resets or security traps. Because of these power and security threats, it is imperative that engineers are provided with fast and accurate power as well as security evaluation methodologies at system level during early product development phases.

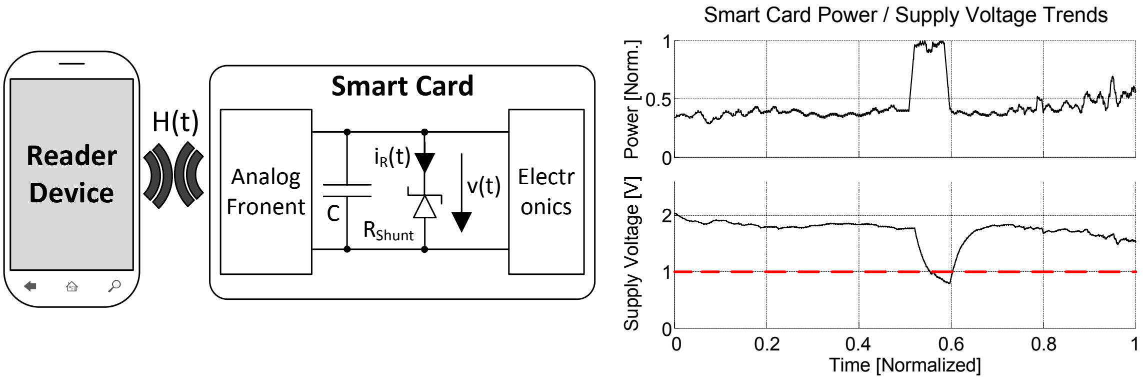


Figure 1.5: Reader / smart card system and its power and supply voltage behavior: peak power consumption may cause hazardous supply voltage drops. Obtained with changes from [6].

1.2 Design Evaluation Framework for Secure and Low-Power Embedded Systems

1.2.1 The META[:SEC:] Project

This thesis is part of the "**M**obile **E**nergy-efficient **T**rustworthy **A**uthentication **S**ystems with **E**lliptic **C**urve based **SEC**urity" project - META[:SEC:][1], which is a collaborative research project of the Graz University of Technology, Infineon Technologies Austria AG, and Enso Detego GmbH. The META[:SEC:] project features the research topics *Design Evaluation Framework*, *Power Optimization Techniques*, *Security and Dependability Concepts*, and *Development Toolbox for Power Optimization* with a focus on secure and contactless reader / smart card systems, as depicted in Figure 1.6. This doctoral thesis places emphasis on the first topic and regards additional research questions from the second and third topics.

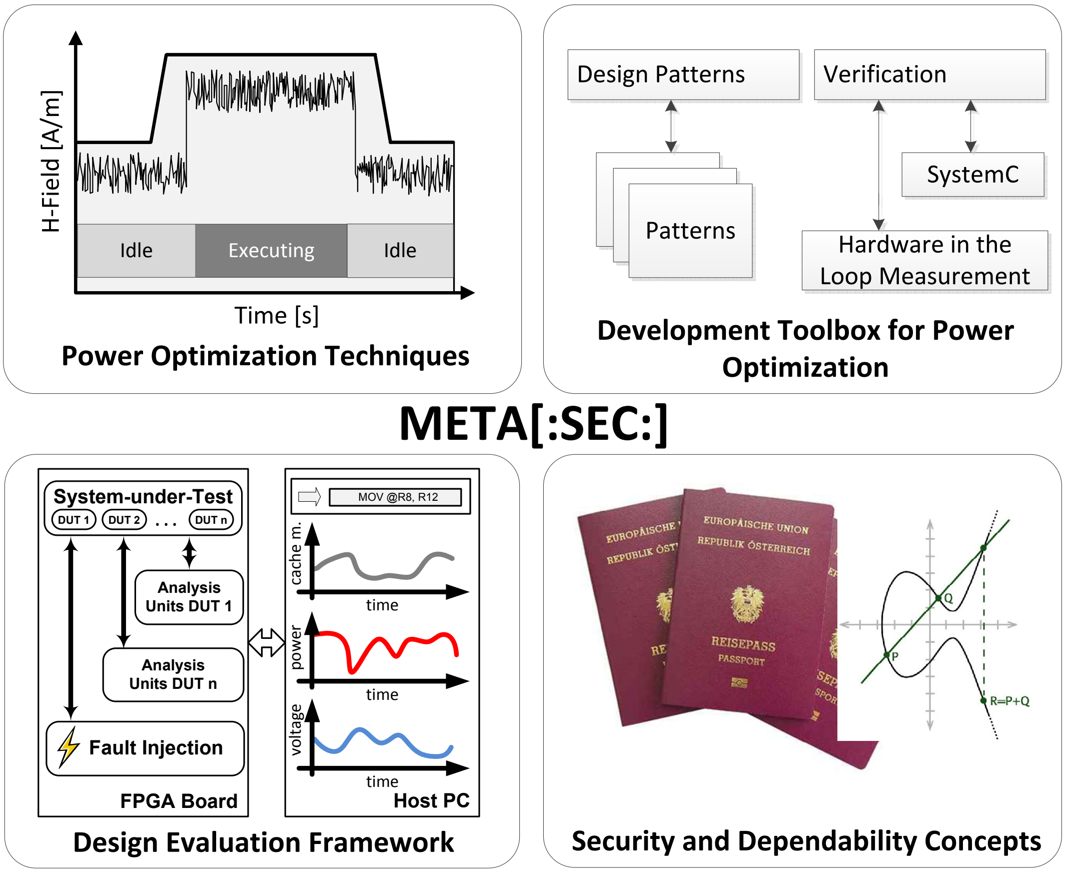


Figure 1.6: The META[:SEC:] project covers power and security topics in the research field of contactlessly powered reader / smart card systems.

[1] Funded by the Austrian Federal Ministry for Transport, Innovation, and Technology under the FIT-IT contract FFG 829586.

1.2.2 Problem Statement

Designing and developing integrated circuits and embedded systems is complex and requires a high amount of test and verification effort, especially in the application field of resource constrained, secure, and dependable embedded systems. This doctoral thesis considers important issues that emerge when developing such secure and low-power embedded systems. These issues can be summarized as follows:

- Exponentially increasing integration density and complexity trends of integrated circuits affect power consumption and fault sensitivity negatively
- Dependability issues arise due to the increasing fault sensitivity of deep-submicron manufactured integrated circuits
- Exhaustive test and verification coverage of novel designs is difficult to achieve due to the exponentially increasing design complexity
- Simulation-based analysis of complex integrated circuits can increase the amount of calculation time needed to a point where getting results in a reasonable amount of time is unfeasible
- Lack of comprehensive hardware accelerated non-functional (power, supply voltage, etc.) analysis data during an integrated circuit's early design phases
- There are unexploited system-level power and security optimization potentials in the application field of secure and low-power embedded systems, such as reader / smart card systems

1.2.3 Contributions and Significance

This doctoral thesis provides the following two major contributions:

1. *Design Evaluation Framework for Secure and Low-Power Embedded Systems:* A comprehensive, hardware emulation-based, and simulation-based design evaluation framework is presented that permits engineers to evaluate not just hardware and software designs but also complete system designs during early design phases. Design flaws can be detected and resolved and design optimizations can be evaluated early on, before the tape-out. Model-based analysis units are employed in order to evaluate functional and performance behavior, as well as their impact on power consumption, supply voltage levels, and thermal behavior. Furthermore, fault injection techniques are featured in order to carry out security and dependability analyses.

2. *Exploration of Innovative Power and Security Optimizations:* The design evaluation framework that is presented is used to explore innovative power management and security optimization techniques in the field of contactlessly powered reader / smart card systems. First, a smart card power management optimization technique is proposed that estimates power consumption and magnetic field supplied voltage levels and counteracts hazardous situations that are detected, such as peak power consumption and supply voltage drops, by means of throttling the smart card's processor core. Second, a system-level power optimization approach is explored and proposed. This

approach adapts the reader emitted magnetic field strength depending on the smart card's instantaneous power requirements. Third, optimization techniques are evaluated that permit a feasible integration of asymmetric cryptography into resource constrained systems.

Based on the insights gained from evaluating embedded systems featuring Near Field Communication, a prototype of a secure Near Field Communication interface is presented that can be integrated into everyday electronic devices. This interface employs the reader emitted electromagnetic power in order to provide a zero-energy communication interface and to support a zero-energy standby mode for the targeted electronic device. Furthermore, this interface can be used in industrial applications and it enables secure configuration, monitor, and control tasks of the electronic device.

1.2.4 Structure of the Work

This thesis is structured as follows. Chapter 2 gives an introduction into the related work. First, selected research work is reviewed covering the topic of design analysis frameworks. Second, power and supply voltage analysis techniques are presented as well as dedicated management methods. Finally, an introduction into the analysis techniques of secure and dependable embedded systems is given. In Chapter 3, the novel design evaluation framework for secure and low-power embedded systems is introduced. Furthermore, it is demonstrated how this analysis framework is used in order to explore and propose novel power and security optimization techniques for contactless reader / smart card systems. Finally, the secure industrial Near Field Communication Interface for everyday electronic devices is presented. In the subsequent Chapter 4, result data is presented which was gained from the usage of the design evaluation framework while analyzing and optimizing embedded system designs, particularly contactless reader / smart card systems. This is followed by Chapter 5, which concludes the doctoral thesis and outlines prospective research possibilities. Finally, Chapter 6 presents a collection of publications, which represent the detailed technical foundation of this doctoral thesis.

Chapter 2

Related Work

This doctoral thesis is based upon the foundation outlined in this chapter and covers three important fields of research. First, functional design analysis frameworks are presented. Then, an introduction into power analysis, which also includes supply voltage and thermal analyses, and power management is given. The last part covers the important field of security as well as dependability aspects in embedded systems. Finally, this chapter is concluded by a short summary and a compilation of contributions and improvements provided by this doctoral thesis.

2.1 Functional Design Analysis Frameworks

Functional design analysis can be performed during various design stages and at various abstraction levels. As an example, high-level SystemC-based evaluation frameworks that were used for design exploration tasks were presented by the authors in [19] and [20]. Such simulation-based methods are widely used for design analysis, test, and verification purposes. However, if design complexity, circuit size, and test periods rise, the amount of calculation time needed may increase to a point where getting results in a reasonable amount of time is unfeasible. In order to avoid such time-intense calculations, the functional hardware emulation technique can be considered. Hardware emulation is a technique that integrates the design-under-test, which must be available in a synthesizable hardware description language, into a prototyping platform (e.g., FPGAs). By using this FPGA hardware support, a major performance increase can be achieved compared to the simulation-based methods. In [21], the authors outlined this advantage. They demonstrated an increase in speed of more than 10^6 compared to the simulation-based approach. One of the first hardware emulation-based approaches, which was used to verify the functionality of the K5 processor, was presented by the authors in [22]. An emulation-based Multi-Processor System-on-Chip (MPSoC) hardware / software evaluation framework was presented in [23]. In the case of big scale embedded systems, such as Multi- and Many-Core processor systems, a multi-FPGA emulation approach can be employed, as described by the authors in [24] and [25]. Further emulation-based design analysis frameworks focusing especially on Network-on-Chip (NoC)-based systems were presented, e.g., in [26] and [27].

2.2 Power Analysis and Management

Due to the fact that integrated circuits and embedded systems grow in complexity exponentially, power analysis and power management represent important fields of research when it comes to coping with the increasing consumption of power. If not handled properly, power mismanagement may cause reduced battery-lifetime in mobile embedded systems, supply voltage drops that harm the operational stability, and increased thermal stress that reduces the reliability of electronics.

2.2.1 Power Analysis

Thanks to the increasing power-awareness in the embedded systems industry, power analysis has become an essential technique to determine the power consumption of electronic circuits. Power analysis techniques can be classified into two major fields: measurement-based and estimation-based techniques. While the measurement-based approach delivers very accurate results, it requires expensive equipment, a manufactured prototype of the targeted electronic circuit, and thus can only be used at a late stage of the product development cycle.

In contrast to measurement-based analysis, the estimation-based power analysis can be performed early on in the product development cycle. Estimation-based approaches can be categorized into simulation-based and hardware accelerated methods, and can be carried out at arbitrary abstraction levels. The work of Bergamaschi et al. [28] can be highlighted as an example of simulation-based power-analysis. The authors presented a model-based methodology to simulate the power and performance behavior of a multi-core processor system. However, simulations of large integrated circuits at low abstraction levels may lead to a significant amount of computation time. To cope with these time-intense computations, the hardware acceleration approach can be used, which integrates the synthesizable analysis algorithm into hardware, e.g., FPGA prototyping platforms. In [29], Joseph and Martonosi demonstrated a hardware accelerated approach, which employed performance events and corresponding performance counters to estimate the power consumption of microprocessors. Performance events (e.g., cache miss, pipeline stall) were then mapped to power estimates by means of a power model. The power emulation methodology, which was coined by Coburn et al. in [30], estimates the power consumption of a dedicated design-under-test hardware accelerated at register-transfer-level with the help of power macromodels. Both, design-under-test and power models are integrated into an FPGA. Power estimates can be gathered for each clock cycle, but a significant hardware overhead is introduced. This power emulation method can also be adapted for higher abstraction levels in order to reduce the hardware overhead, as presented by Genser et al. in [31]. Power sensors were used to monitor component states (e.g., read memory, write memory, cache hit) of the design-under-test. A system-level power model then maps the monitored component states to power estimates. The system-level power models used in this approach are generated during a time consuming gate-level-based power characterization process. Still, this prolonged characterization process can be carried out automatically for any synthesizable hardware design, as demonstrated by Bachmann et al. in [32].

2.2.2 Supply Voltage Analysis

During the past few decades, the number of integrated transistors has increased exponentially. In order to cope with the resulting power consumption increase, supply voltage levels of hardware designs have been decreased. However, the trend of low supply voltage levels and increasing numbers of simultaneously switching transistors, introduced a major problem. According to (2.1), a changing electrical current di/dt provokes a voltage across an inductance L which is defined by the hardware's pins and wires. As the authors highlighted in [33], this induced voltage makes the hardware prone to voltage drops, especially if the hardware's supply voltage is low. As a consequence, state-of-the-art power supplies need to be designed properly to cope with this supply voltage drop issue that is also referred to as the "di/dt problem".

$$v(t) = L \cdot \frac{di}{dt} \tag{2.1}$$

Devices that harvest energy from the environment face additional threats concerning their supply voltage, because the amount of electrical energy generated is very limited. In the case of contactlessly powered smart cards, energy is harvested from alternating magnetic fields and is buffered within capacitors. As a consequence, the smart card's supply voltage fluctuates depending on its power consumption and the electrical power that is provided by the environment. If the smart card's power consumption exceeds a certain limit or if the environment provided power does not suffice, the smart card's supply voltage will drop. If this supply voltage level drops below a hazardous threshold, the smart card's operational stability will be lost because the transistors will not be able to switch states as quickly as expected by the timing of the chip. Thus, it is imperative that energy harvesting-based embedded systems are aware of the supplied power, the consumed power, and the resulting voltage level.

Supply voltage analysis can either be done during design-time or during run-time. During run-time, for example, on-die circuits can be used in order to measure and detect hazardous voltage variations, as demonstrated in [34]. Analog-to-digital converters, cf. [35], and voltage comparators, cf. [36], are further methods that are commonly used in integrated circuits and embedded systems. A simulation-based analysis method, which models a power supply network, was presented by the authors in [33]. An emulation-based approach, which can be used during early phases of the design process, was presented by Genser et al. in [37]. The authors integrated model-based analysis units along with the design-under-test, a contactlessly powered smart card, into an FPGA prototyping platform. Thus, supply voltage estimates were gathered hardware accelerated for each clock cycle.

2.2.3 Dynamic Power and Supply Voltage Management

Dynamic power management comprises of techniques to adapt a system's power consumption during run-time. Dynamic power management methods commonly use an observer / controller approach, as summarized by Benini et al. in [38]. An observer monitors the system's power consumption, performance, load of computation, etc., while the controller adapts certain system parameters based on the information gathered by the observer. For this control purpose, a variety of control algorithms has been previously evaluated. One of the most commonly used control algorithms dynamically scales the system's voltage and frequency parameters (DVFS). According to (2.2), such voltage and frequency parameter adjustments have a cubic dynamic power consumption impact on a CMOS-based system. However, the system's clock frequency $f(t)$ is degraded in a linear way. In addition, voltage and frequency cannot be assigned arbitrary values: for a given frequency value, a minimum voltage level is required for the integrated circuit to operate properly.

$$P(t) \approx v(t)^2 \cdot f(t) \tag{2.2}$$

A vast set of different observer methods were proposed and implemented in the past. A very commonly used technique is the definition and modeling of power states. For example, an embedded system may define an idle state and a run state. When the system transitions from run to idle state, unused system components may be switched off completely or may be reduced in their clock speed, which results in a reduced total power consumption. Other observer implementations use, for example, analog-to-digital converters or analog comparators. If a peak power consumption or a supply voltage drop is detected, the system's clock is throttled or paused completely until the emergency is resolved. However, the sensor delay represents a drawback that limits the efficiency of these approaches.

Apart from observer / controller techniques, decoupling capacitors, asynchronous, or semi-asynchronous architectures can be used in order to shape the electrical current and thus reduce peak power consumption and supply voltage hazards, cf. [39]. In [34], the authors employed on-die circuits to inject electrical currents of up to 100 mA into nodes that faced supply voltage drops. A predictive-based method was presented by Reddi et al. in [40]. Initially, signatures (e.g., micro architectural events such as cache misses, program path sequences) of software programs which caused hazardous supply voltage drops were collected. During run-time, live signatures are compared to the saved emergency signatures. If a match is found, the processor is throttled in order to resolve the emergency situation that was identified. This technique detected 90% of the tested emergency situations but introduced a high amount of overheads.

For the case of energy harvesting-based embedded systems, such as RF-powered contactless smart cards, a proper power and supply voltage management is crucial: sharp power consumption changes of the smart card's electronics may cause hazardous supply voltage drops. This harmful voltage drop behavior is demonstrated by Haid et al. in [41] by means of a simplified smart card power supply model. The authors stress the need for power and supply voltage management implementations that take into account the characteristics and sensibilities of such reader / smart card systems. In [11], Wendt et al. presented a time discrete model of a smart card power supply network. This model is used for the detection and counteraction of power and supply voltage emergencies caused by critical source code regions (e.g., calculation intense cryptographic algorithms).

2.2.4 Thermal and Reliability Analysis

The steadily increasing power consumption trend of recent and future embedded systems, cf. International Technology Roadmap for Semiconductors [3], is a major concern. Since an integrated circuit's consumed power is converted into heat, system engineers have to cope with increasing thermal stress and reliability issues. In [42], the author outlined the hazardous impact of temperature on a hardware's reliability: with increasing temperature, the reliability, i.e. mean time to failure (MTTF), decreases exponentially. Atienza et al. presented in [43] reliability aware design approaches. The authors optimized a compiler's register allocation algorithm. By achieving a spatial and temporal distribution of register accesses, thermal hot spots were reduced. As a consequence, the register file's MTTF was increased by 20 %. In [44], the authors presented a hardware emulation framework that is used to estimate functional, power, and thermal behavior of SoCs. The thermal behavior was calculated in software with the help of the tool HotSpot. HotSpot, which estimates the temperature behavior of individual SoC components by means of their power consumptions and a thermal model, was introduced by Skadron et al. in [45]. The authors employed the duality of heat transfer and linear electrical circuits: a heat transfer problem can be transformed into an equivalent RC circuit that is then solved by means of an ordinary differential equation solver.

2.3 Security and Dependability Aspects of Embedded Systems

Today, secure and dependable embedded systems are omnipresent in our everyday life. They can be found in electronic devices and applications, such as, credit cards, cars, airplanes, etc. According to Avizienis et al. in [46], important attributes of secure and dependable embedded systems are: availability, reliability, safety, confidentiality, integrity, and maintainability. This chapter summarizes the latest developments in the fault injection-based analysis techniques of secure and dependable embedded systems and outlines recent security threats and measures in the field of RFID and NFC-based embedded systems.

2.3.1 Security and Dependability Analysis

Security and dependability analysis aims at achieving confidence in the capability to deliver a service that can be trusted, as coined by Avizienis et al. in [46]. However, given the increasing cost and time-to-market pressure of novel embedded system developments, a high analysis and test coverage is difficult to achieve. Yet, exhaustive test and verification is particularly important in the field of dependable and secure embedded systems: reliable operation should be provided even under faulty hardware conditions. In [47] and [48], the authors stress the challenges during the design phase when developing secure embedded systems. The authors underline the importance of supporting system engineers with proper security-test and dependability-test capabilities during early design phases. For this purpose, fault injection is a commonly used test approach: the reliable execution of a secure or dependable application is tested whilst being affected by faults. This fault injection method can be used during arbitrary product development phases.

During the design specification and concept phase, fault injection can be applied to high-level SystemC models. Rothbart et al. presented in [49] a high-level SystemC-based fault injection framework. The authors carried out attack simulations targeting secure smart card designs. Further SystemC fault injection techniques were presented, for example, by the authors of [50] and [51].

During the embedded system's design phases, as soon as the hardware is available in a hardware description language, faults can be either injected by simulation or by emulation on FPGAs. Simulation-based fault injection tools and methodologies were introduced by the authors in [52] and [53]. Further research work regarded modular fault injection controllers (cf. [54]), improvements to fault injection rates (cf. [55]), automated saboteur as well as mutant placement (cf. [56]), and enhanced multi-level approaches (cf. [57]). Rahimi et al. evaluated in [58] the vulnerability of the LEON3 SoC's instructions while varying temperature and voltage parameters by means of calculation intense gate-level simulations. On the one hand simulation-based fault injection methods are flexible and easy adaptable, but on the other hand, they lack fault injection speeds. A major acceleration can be gained by using hardware emulation-based evaluation and fault injection techniques, as highlighted by the authors in [55] and [59]. An industrial and highly parallelized fault emulation approach was presented in [60]. Multiple fault emulation platforms were used simultaneously to maximize the fault injection rate. Kasper et al. presented in [61] a versatile emulation-based fault injection platform focusing on secure embedded devices. The authors successfully demonstrated a full key recovery from a contactless smart card that featured a Triple-DES security algorithm. Another FPGA-based development platform targeting RFID tags was presented by Plos et al. in [62]. This development platform was used particularly for implementing and evaluating security related attacks.

If the manufactured hardware is available, faults can be injected either by software (e.g., corruption of memory images) or by external sources, such as heat, radiation, voltage variations. Software-based fault injection tools, such as FIAT or FERRARI, were presented in [63] and [64] respectively. In [65], the authors used heat as a source in order to successfully attack and take over JAVA virtual machines.

Apart from pure functional analyses during faulty hardware conditions, an embedded system's power profile also represents important side-channel information. Security related evaluation methodologies, such as Simple Power Analysis (SPA) and Differential Power Analysis (DPA), can be employed to extract an embedded system's internal secrets, as summarized by Mangard et al. in [66]. In addition, significant power profile changes caused, for example, by an injected fault can reveal security relevant countermeasures, such as hardware resets or security traps, while executing security critical code regions. As an example, Krieg et al. presented in [67] an emulation-based methodology which permits power related and fault related security and dependability evaluations.

2.3.2 Security Threats and Measures in Smart Card and RFID Applications

Security controllers embedded in smart cards and RFID-based devices are deployed in many markets in order to protect our privacy and to secure sensitive data. Smart card-based systems are used in government applications (e.g., national IDs, e-passports, e-health insurance cards), access control systems, mobile phones (subscriber identification module), mobile payment applications (credit cards, public transport systems, NFC applications), etc. An overview of various vulnerabilities of such electronic devices that feature RFID and NFC was summarized by Haselsteiner et al. in [68], by Hutter et al. in [69], and by Mangard et al. in [66]. For instance, the authors successfully demonstrated writing faulty values into the RFID tag's memory after a security attack was carried out. In [70] and

[71], the authors successfully attacked secure RFID and NFC tags by means of differential power analysis, differential electromagnetic analysis, and remote side-channel analysis. Further identified security threats are, for example, eavesdropping, man-in-the-middle attacks, and data manipulation attacks. Cryptographic algorithms are commonly employed in order to cope with the highlighted security threats. In [72] and [73], the authors evaluated various cryptographic algorithms (Secure Hash Algorithm, Advanced Encryption Standard, Elliptic-Curve Cryptography, etc.) regarding their security strengths and resource requirements. On the one hand, AES shows low resource requirements, but on the other hand, it suffers from being a symmetric cryptographic approach and the need for carefully implemented key distribution mechanics. ECC, which is an asymmetrical cryptographic method, requires significantly higher resources, but overcomes the key distribution problem of symmetric methods. In [74], [75], and [76], the authors give detailed recommendations regarding key sizes of various symmetric and asymmetric cryptographic methods. As an example, in order to achieve a targeted security level that is equivalent to a symmetric key size of 112 bits, an ECC key size of 224 bits is suggested. Compared to RSA's required key size of 2048 bits, ECC is more suitable to be integrated into resource constrained embedded systems due to the smaller key sizes. Aigner et al. demonstrated in [77] that a low-cost ECC coprocessor can be feasibly integrated into resource constrained embedded systems, such as smart cards. Further ECC implementations for resource constrained embedded systems were presented, for example, by the authors of [78], [79], and [80]. A detailed comparison, which focused on resource consumption and performance, of ECC implementations targeting three famous embedded processors (8-bit Atmel ATmega, 16-bit Texas Instruments MSP430, 32-bit ARM Cortex-M0+) was carried out by Wenger et al. in [81]. However, if not implemented carefully, ECC can be vulnerable to side-channel attacks, as outlined by the authors in [82].

2.4 Summary and Difference to the State-of-the-Art

Functional design analysis is a well-known technique for verifying the functional behavior of a design-under-test. Hardware emulation-based analysis methods are commonly used to accelerate analyses of large designs. However, recent emulation-based analysis approaches only cover non-functional design and application issues, such as power consumption hazards or supply voltage alterations, to some extent. Yet, such non-functional analysis is especially important in the field of power sensitive and resource constrained embedded systems, such as contactless RF-powered smart cards: a drop in power supply, caused for example by a card movement within the magnetic field, can hazardously impact the smart card's functional behavior. Moreover, in the field of secure contactless reader / smart card systems, research concentrated on isolated design analysis. System-level challenges and optimization possibilities (e.g., power consumption, security features) resulting from the wireless connection and interaction between the reader and a contactless smart card have been investigated sparsely. The security-related and dependability-related emulation-based and simulation-based research work that is presented here insufficiently evaluates, apart from operational robustness, power consumption and supply voltage trends during faulty hardware and faulty environmental conditions. In addition, most of the related work regards only single fault event evaluations. As the author highlights in [83], proper security and dependability evaluations require more complex fault models that cope with intentionally injected multiple faults.

This doctoral thesis aims to address these highlighted gaps in literature and related work. With respect to the goals defined in Section 1.2.3, this doctoral thesis makes the following contributions:

- Introduction of a comprehensive emulation-based and simulation-based design evaluation framework for secure and low-power integrated circuits and complex embedded systems. Hardware / software designs can be explored and evaluated respecting functional and crucial non-functional properties (e.g., power, supply voltage, temperature, performance) simultaneously.
- Introduction of a system-level emulation-based analysis approach which is exemplified by means of a secure contactless reader / smart card system.

In addition, this doctoral thesis establishes the following supplemental advances to recent related work:

- Exploration and proposal of innovative power and security optimizations for the application field of secure contactless reader / smart card systems.
- Introduction of a secure NFC interface for everyday electronic devices which enables a zero-energy standby paradigm.

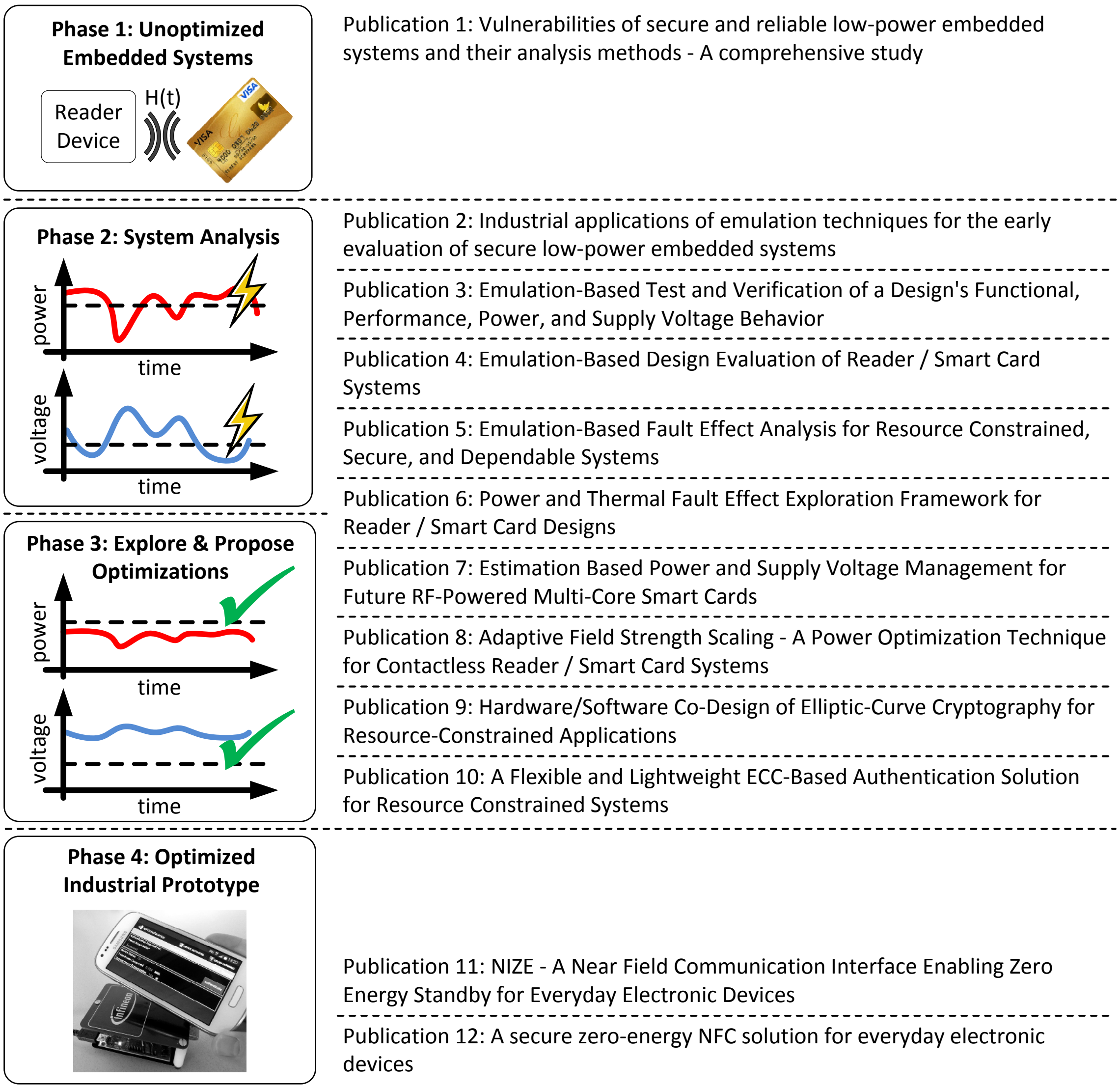
Chapter 3

Design Evaluation Framework for Secure and Low-Power Embedded Systems

3.1 Overview

For integrated circuits and embedded systems, the evaluation of hardware and software designs during early product development phases is essential: the earlier design flaws can be detected, the lower the costs are to resolve these flaws. The framework, techniques, and tools proposed in this chapter aim at improving this crucial evaluation and verification process. Figure 3.1 gives an overview of the contributions provided by this doctoral thesis, which are divided into four phases. While this chapter intends to give an outline of the contributions, Chapter 6 provides detailed information by means of the appended publications.

Phase one initiates the research topic of this doctoral thesis. This initial phase, described in Section 6.1, outlines the vulnerabilities and analysis methods of secure and low-power embedded systems. In phase two, further introductions to the emulation-based analysis techniques (power emulation, supply voltage emulation, performance evaluation, security evaluations) and their application in the field of industrial embedded systems are provided through Section 6.2. The comprehensive emulation-based design evaluation framework, which employs model-based analysis units, is presented in detail in Section 6.3. This framework enables an engineer to test hardware and software designs with regards to functional and performance behavior, as well as their impact on power consumption and supply voltage levels. In Section 6.4, the proposed design evaluation technique is enhanced in order to take into account the crucial system aspect related to complex embedded systems, such as reader / smart card systems. In a further step, this emulation-based design evaluation methodology is extended with fault injection functionality, which is presented in Section 6.5. This approach particularly improves the analysis capabilities for secure and dependable embedded systems. Although emulation-based techniques deliver accurate analysis results for each clock cycle, these techniques lack in flexibility. Therefore, a flexible high-level SystemC-based framework is proposed in Section 6.6, which enables fast but less accurate design analyses, focusing on reader / smart card systems.


Phase 1: Unoptimized Embedded Systems
Reader Device
H(t)
Phase 2: System Analysis
power
time
voltage
time
Phase 3: Explore & Propose Optimizations
power
time
voltage
time
Phase 4: Optimized Industrial Prototype

Publication 1: Vulnerabilities of secure and reliable low-power embedded systems and their analysis methods - A comprehensive study

Publication 2: Industrial applications of emulation techniques for the early evaluation of secure low-power embedded systems

Publication 3: Emulation-Based Test and Verification of a Design's Functional, Performance, Power, and Supply Voltage Behavior

Publication 4: Emulation-Based Design Evaluation of Reader / Smart Card Systems

Publication 5: Emulation-Based Fault Effect Analysis for Resource Constrained, Secure, and Dependable Systems

Publication 6: Power and Thermal Fault Effect Exploration Framework for Reader / Smart Card Designs

Publication 7: Estimation Based Power and Supply Voltage Management for Future RF-Powered Multi-Core Smart Cards

Publication 8: Adaptive Field Strength Scaling - A Power Optimization Technique for Contactless Reader / Smart Card Systems

Publication 9: Hardware/Software Co-Design of Elliptic-Curve Cryptography for Resource-Constrained Applications

Publication 10: A Flexible and Lightweight ECC-Based Authentication Solution for Resource Constrained Systems

Publication 11: NIZE - A Near Field Communication Interface Enabling Zero Energy Standby for Everyday Electronic Devices

Publication 12: A secure zero-energy NFC solution for everyday electronic devices

Figure 3.1: Doctoral thesis' four phases of contributions and the corresponding publications.

With the help of these emulation-based and simulation-based design evaluation techniques, this doctoral thesis' third phase is introduced: system-level power (Section 6.7 and Section 6.8) and security (Section 6.9 and Section 6.10) optimization techniques are explored for reader / smart card systems.

During this thesis' final phase, an industrial prototype that introduces a secure Near Field Communication (NFC) interface for everyday electronic devices is presented in Section 6.11 and Section 6.12. This interface employs the electrical power of the reader emitted magnetic field in order to provide a zero-energy communication interface and to support a zero-energy standby mode for the targeted electronic device.

3.2 Design Evaluation Framework

The design evaluation framework that is presented comprises of three parts: design emulation, system emulation, and high-level simulation. This chapter outlines the working principle of these three approaches.

3.2.1 Design Emulation

Test and verification of hardware and software designs is widely performed by means of software-based and simulation-based approaches. However, if circuit size and test periods increase, the amount of calculation time needed can grow to a point where getting results in a reasonable amount of time is unfeasible. In order to improve test and verification speeds of hardware designs, the hardware emulation technique can be used. Hardware emulation integrates a synthesizable hardware design into a reconfigurable prototyping platform (such as FPGAs), as depicted in Figure 3.2 and described in [22]. However, the main drawback of this functional hardware emulation approach is the reduced coverage of non-functional analysis data, such as power consumption, supply voltage, or performance information. Therefore, this doctoral thesis proposes a comprehensive emulation methodology in order to simultaneously test and verify the functionality, performance, power consumption, and supply voltage behavior of a design-under-test. This is accomplished, using an FPGA as a prototyping platform, by augmenting the design-under-test with data acquisition units that supply model-based information on power, supply voltage, and performance. Figure 3.3 illustrates the basic principle of this approach. The FPGA-based test bench is designed to adapt the model-based analysis models to any specific design-under-test easily. As the design-under-test and the model-based analysis units are integrated in hardware, all analysis and verification data can be gathered in real-time and for each clock cycle. As a consequence, this analysis technique grants a significant increase in speed compared to simulation-based approaches. The FPGA-based test bench also features peripheral interfaces (e.g., Ethernet) that are used by a host PC in order to control and setup the test bench. In addition, all analysis results, whether they are results from functional testing, performance testing, or power and supply voltage analyses, are transferred to the host PC for further offline analysis tasks.

The power analysis approach used in this doctoral thesis is based upon the power emulation technique introduced by Coburn et al. in [30] and which was refined by Genser et al. in [31] for higher abstraction levels. Power sensors monitor the design's component states. Each sensor maps the monitored component state x_i to a power value c_i by means of a power model. The linear combination of $\mathbf{x}$ and $\mathbf{c^T}$ plus a static power consumption

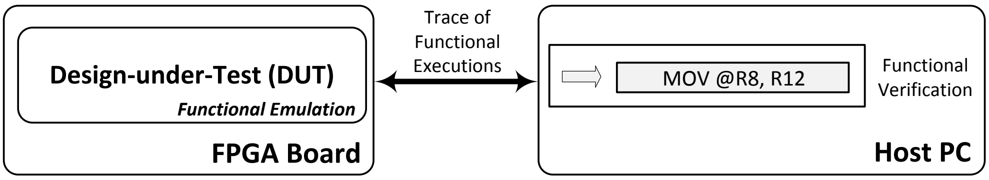


Figure 3.2: Hardware emulation principle: description of the hardware design is synthesized in an FPA board for rapid prototyping and evaluation tasks.

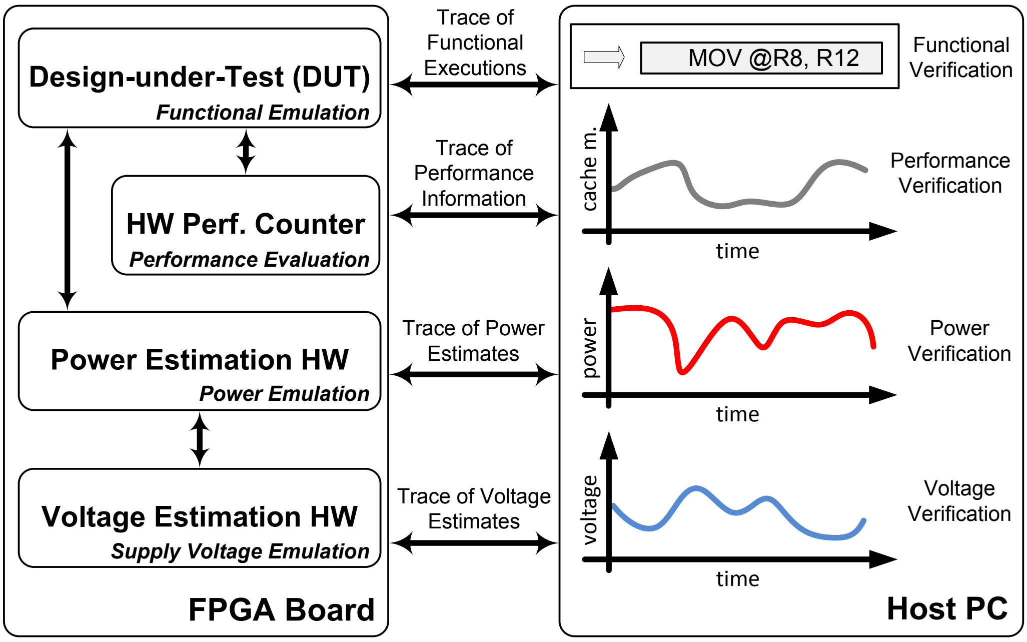


Figure 3.3: Comprehensive design emulation approach. Functional hardware emulation is augmented with model-based non-functional analysis units. Obtained with changes from [6].

c_0 define the total estimated power consumption of the hardware, which is given by (3.1). The average estimation error ϵ is defined by (3.2). The parameters $\mathbf{x}$, $\mathbf{c}^{\mathbf{T}}$, and c_0 are determined during a time consuming gate-level power characterization process. As described by Bachmann et al. in [32], this process can be performed automatically for any given hardware design. If a manufactured hardware of the design-under-test is available (e.g., an ASIC), the power model can be refined with physical power measurements in order to decrease the average estimation error ϵ.

$$\widehat{P}(\mathbf{x}) = c_0 + \sum_{i=1}^{n} c_i \cdot x_i = c_0 + \mathbf{c}^{\mathbf{T}} \cdot \mathbf{x} \tag{3.1}$$

$$P(\mathbf{x}) = \widehat{P}(\mathbf{x}) + \epsilon \tag{3.2}$$

Based on the design-under-test's estimated power consumption, the influence on its supply voltage can be estimated. Therefore, the electrical current $i(t)$ that is drawn by the design-under-test, is calculated by means of the estimated power $\widehat{P}(\mathbf{x})$. The supply voltage behavior is then estimated through a power network model. Due to the fact that power network models are specific to each design, this model needs to be individually designed and implemented by the test bench designer.

Performance is analyzed by the design evaluation framework presented here with the help of hardware performance counters (HPCs): a performance event e (e.g., cache hit, pipeline stall) is defined by a function f over a set of input signals s_n, according to (3.3). Whenever the input signals s_n satisfy the function f, the dedicated performance counter is incremented. This performance data is then collected and transmitted to the host PC for further offline analysis tasks. With the help of this HPC analysis data, hardware and software problems can be detected, which would for example violate worst-case execution time or real-time constraints.

$$e(s) = f(s_1, s_2 ... s_n) \tag{3.3}$$

Further details concerning the presented design emulation concept are provided in Section 6.3.

3.2.2 System Emulation

The design emulation approach presented in the previous Section 3.2.1 permits engineers to evaluate hardware and software designs with regards to their functional and non-functional behavior during early design phases. In a further step, fault injection capabilities are added in order to permit security and dependability analyses. However, evaluating the behavior of individual components under faulty conditions may not be sufficient when it comes to distributed secure systems, such as contactless reader / smart card systems. For example, multi-attacks that are carried out on both smart card and reader simultaneously, could bypass security precautions. Therefore, this design evaluation technique is enhanced in order to take into account crucial system aspects related to complex and secure embedded systems, as illustrated in Figure 3.4.

Figure 3.5 describes the workflow used to setup a system-level emulation test bench. First, the system-under-test, which must be available in a synthesizable hardware description language, is specified and corresponding security constraints (as well as dependability constraints) are defined. During the target characterization and modeling phase, power

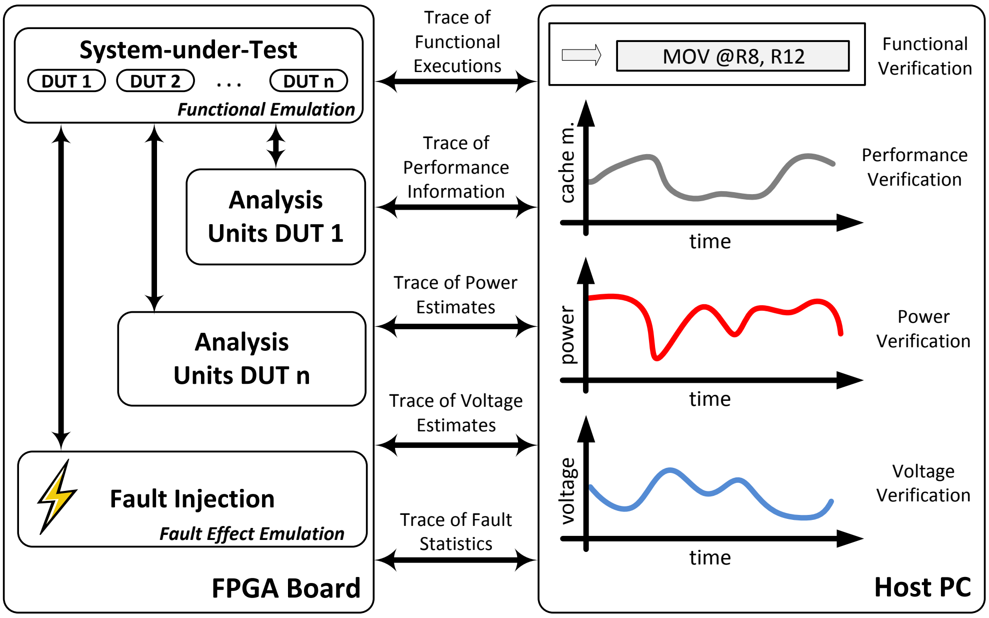


Figure 3.4: System emulation approach. The system-under-test functional emulation is augmented with model-based non-functional analysis units and fault injection techniques. Obtained with changes from [7] and [8].

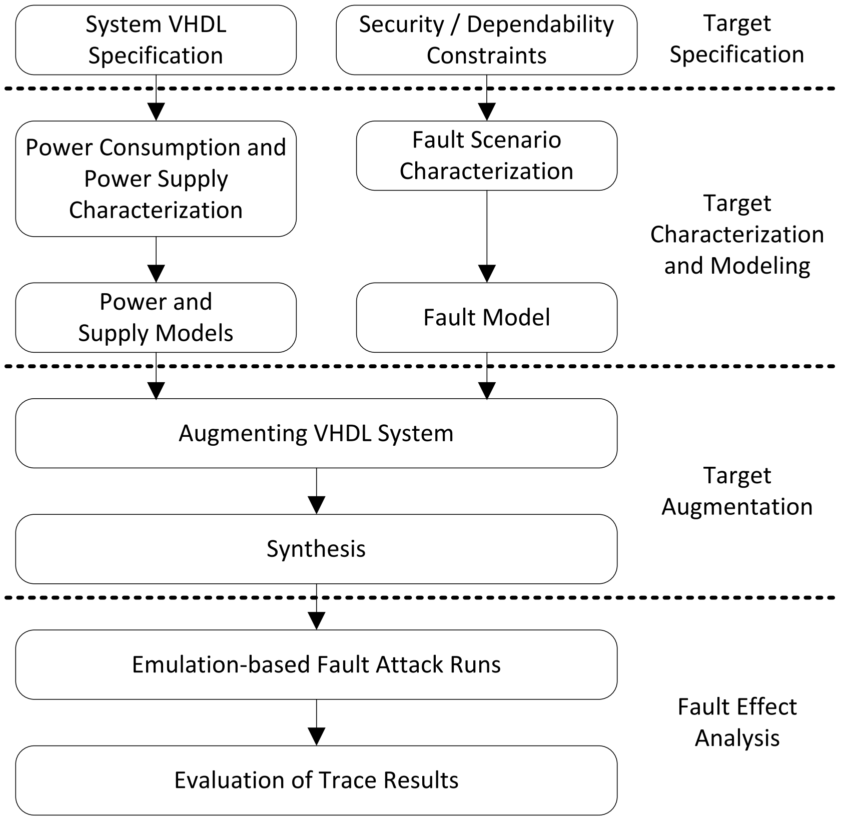

System VHDL Specification
Security / Dependability Constraints
Target Specification
Power Consumption and Power Supply Characterization
Fault Scenario Characterization
Target Characterization and Modeling
Power and Supply Models
Fault Model
Augmenting VHDL System
Target Augmentation
Synthesis
Emulation-based Fault Attack Runs
Fault Effect Analysis
Evaluation of Trace Results

Figure 3.5: Setup workflow of a system emulation test bench. Obtained with changes from [7].

and fault models are developed. The system-under-test is then augmented with these generated models and is synthesized for the reconfigurable prototyping platform during phase three. The final fault effect analysis phase aims to carry out attack runs and to gather all functional and non-functional (power consumption, supply voltage behavior, performance, etc.) trace information for further evaluations.

Security and dependability analysis is performed by evaluating the system-under-test's behavior during intentionally injected faults. Injected faults can either be transient or permanent and are provoked by adapting the emulated system-under-test in order to integrate faulty components or fault-inducing modules. This emulation-based fault injection technique permits high fault injection rates and fast security and dependability evaluations at the cost of loss in flexibility compared to calculation intense but flexible simulation methods. Two fault injection concepts, which are based on the work of Grinschgl et al. [54], are featured:

- A mutant is a replacement of a specific hardware component that behaves identically to the original hardware until it is triggered. If triggered, the replaced hardware's functionality is disturbed according to predefined patterns.
- A saboteur is a small hardware component that interposes a signal line. This saboteur behaves transparently until it is triggered. If triggered, the signal line is disturbed according to predefined patterns.

In addition to fault injection-based analysis, a hardware's power consumption also represents important side-channel information for security evaluation methodologies, such as Simple Power Analysis (SPA) or Differential Power Analysis (DPA). In order to facilitate these security evaluation techniques, the system-level emulation power analysis approach is enhanced with side-channel power analysis capabilities that were originally introduced by Krieg et al. in [84]. The improved power analysis approach is given in (3.4) and (3.5). The state-dependent and control-dependent (e.g., crypto core active state) power is extended with data-dependent (e.g., switching data lines) power dissipation information. This introduced data dependency permits the highlighted security relevant power analyses, such as SPA and DPA, which would be infeasible if using only state-based and control-based power information.

$$\widehat{P}(\mathbf{x}) = c_0 + \sum_{i=1}^{m} c_{si} \cdot x_{si} + \sum_{i=1}^{n} c_{di} \cdot x_{di} \tag{3.4}$$

$$\widehat{P}(\mathbf{x}) = c_0 + \mathbf{c_s^T} \cdot \mathbf{x_s} + \mathbf{c_d^T} \cdot \mathbf{x_d} \tag{3.5}$$

In addition, detailed information regarding the presented system emulation technique and the involved concepts can be found in Section 6.4 and Section 6.5.

3.2.3 High-Level Simulation

Although the emulation-based design evaluation techniques that have been presented deliver fast and accurate analysis results for each clock cycle, they lack in flexibility. Each

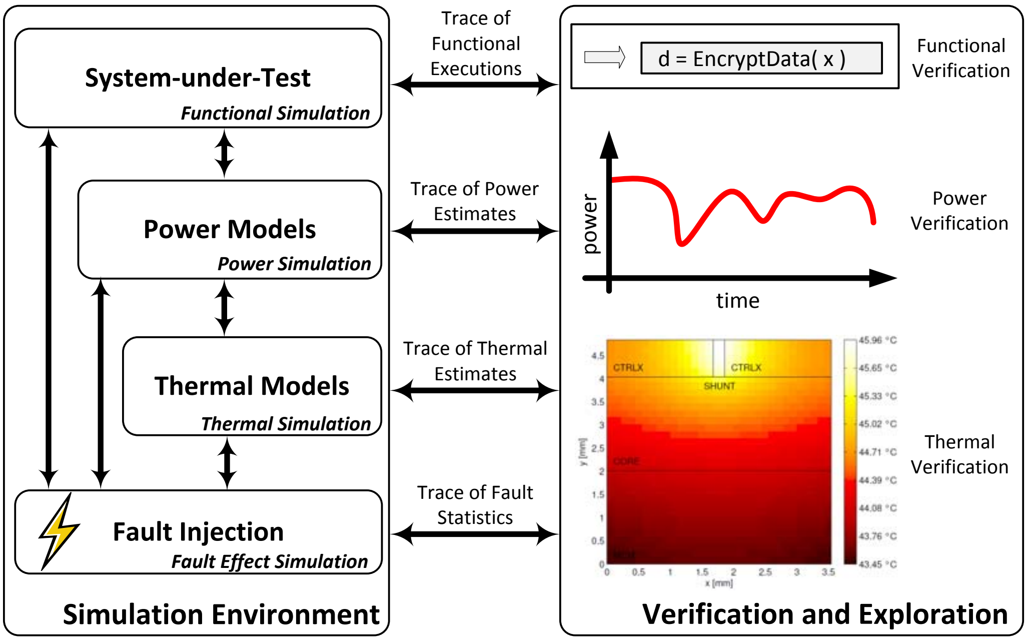


Figure 3.6: Concept of the high-level simulation-based design evaluation approach. Obtained with changes from [9].

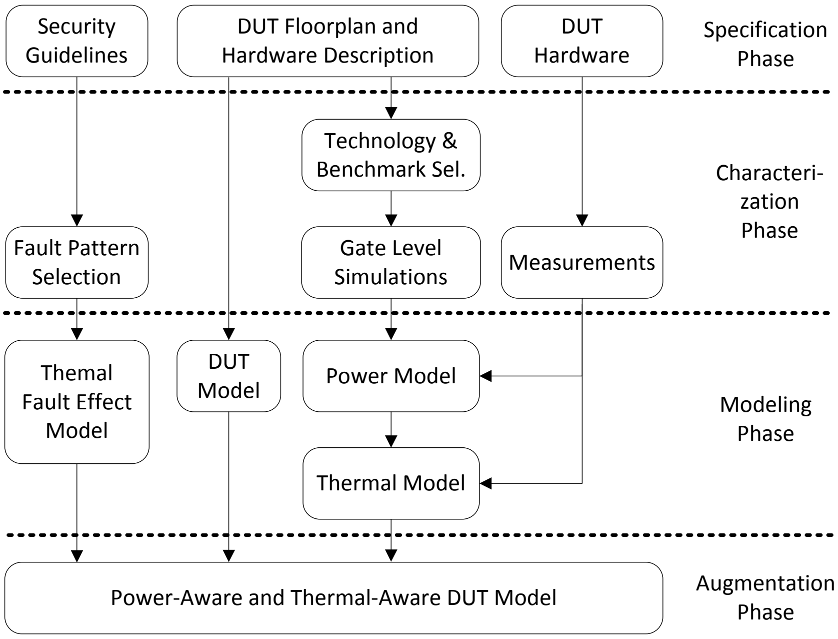


Figure 3.7: Setup workflow of a high-level design evaluation test bench. Obtained with changes from [9].

VHDL/Verilog code change needs to be re-synthesized for the targeted reconfigurable prototyping platform, which may be time consuming in the case of large designs or systems. In addition, these techniques lack the support of engineers during a design's early concept and specification phases. This drawback is addressed by the presented high-level, flexible, and SystemC-based simulation approach, which is described in detail in Section 6.6. The concept of this approach is illustrated in Figure 3.6. A given high-level system-under-test is simulated with power consumption and thermal models. Faults can be induced through software-based fault injectors according to predefined patterns or thermal effect models. Thus, an innovative and comprehensive design exploration and evaluation framework is given which can be used during the whole development cycle and which delivers functional, power, and thermal trace information.

Figure 3.7 presents the workflow used to setup a high-level simulation-based design evaluation framework for a given design-under-test. This workflow is divided into the four phases of specification, characterization, modeling, and augmentation. During the initial specification phase, the design-under-test's floorplan, packaging, and hardware description are defined. The level of detail depends, of course, on the progress of the development process. In addition, security guidelines are specified, with respect to the product's security and certification levels. The following characterization phase aims to characterize the design-under-test's behavior as accurately as possible. This behavior information is required to create corresponding models later on. In order to characterize a design-under-test with regards to its power consumption behavior, the manufacturing technology and extensive benchmarks are selected. If the hardware design is given in a hardware description language, gate-level simulations are carried out. Power models are then developed based on the resulting data. If a manufactured hardware of the design is available, physical measurements of the hardware's power consumption are carried out. In addition, fault injection concepts (e.g., using saboteurs or mutants, where and when to inject faults) and corresponding fault injection patterns are developed. The third phase aims to assemble high-level models. First, a high-level SystemC model of the design-under-test is created. Note, this model's accuracy and level of detail directly influences the accuracy of the power and thermal estimations. A power model maps signal and component activity to power estimates. Its accuracy depends on the number of considered states and signals and can be improved by considering the physical power measurements obtained from a manufactured prototype. A thermal model is constructed with the help of packaging information, floorplan, and the thermal characteristics of the materials used. The resulting thermal fault effect model takes into account the physical effects caused by heat (e.g., electromigration, changes to the critical path delay) and features various fault conditions such as stuck-at and bit flips. During the final augmentation phase, the SystemC-based model of the design-under-test is augmented with the power, thermal, and fault effect models. Furthermore, fault injection units, such as saboteurs and mutants, are integrated into the design according to the previously developed fault injection concept. After this final augmentation phase, the design-under-test can be explored and evaluated regarding functional, power, thermal, and fault behavior.

3.3 Exploration of Optimization Techniques

This doctoral thesis explores and proposes several power and security optimization techniques in the research field of contactless reader / smart card systems. These optimization techniques are presented in the following sections.

3.3.1 Estimation-Based Power Management for Smart Cards

A typical contactless smart card system consists of a reader device and a smart card, as illustrated in Figure 3.8. The smart card is powered through an alternating and modulated magnetic field that is emitted by the reader device. The induced electrical current in the smart card's antenna is used to power the smart card's electronics. The harvested electrical power is very limited. Therefore, attention must be paid to high average power consumption, peak power consumption, and card movements within the RF field. These issues may cause the smart card's supply voltage to fluctuate. If the supply voltage drops hazardously below a certain threshold, the smart card's operational stability is no longer guaranteed. Therefore, this doctoral thesis introduces an estimation-based power management technique in order to cope with these hazardous supply voltage drops on the smart card side.

The principle of the presented management technique works as follows. A power estimation unit monitors the smart card's component states (e.g., crypto core active) and provides power estimation values for each clock cycle. This power estimation principle is based upon an approach introduced by Genser et al. in [31]. The power estimation values are then passed to a voltage estimation unit. Within this unit, the voltage that is supplied to the smart card's electronics is estimated through a model of the reader / smart card system's power supply network. Finally, a power management unit monitors the provided power and supply voltage estimation values. If the power management unit detects a

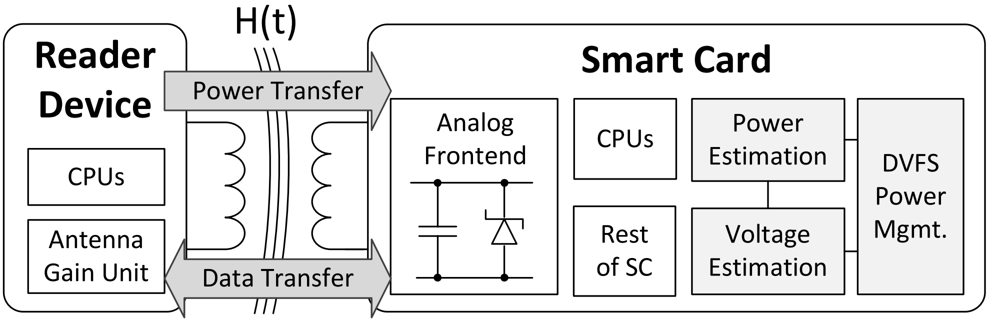


Figure 3.8: Concept of a reader / smart card system. The smart card features estimation-based power management techniques in order to reduce power emergencies such as hazardous voltage drops and peak power consumption.

power or supply voltage emergency, the smart card's processor will be throttled according to an implemented power management policy.

One of the crucial parts of this approach is the model of the power supply network, because supply voltage values need to be estimated quickly and accurately. The hardware accelerated voltage estimation principle presented in this doctoral thesis employs a power supply model that is simplified through the Thévenin equivalent voltage source principle (cf. [11]). Thanks to this simplification method, the complex equations of the original power supply model (cf. [85]) are reduced to a 1$^{\text{st}}$order ordinary differential equation that is given by (3.6). Thus, supply voltage estimates can be feasibly computed in hardware.

$$v(t+1) = \frac{Q_C(t) + \frac{v_i(t)-v(t)}{R_i}\Delta t - i(t)\Delta t}{C} \text{ if } v(t) < V_Z \tag{3.6}$$

As illustrated in Figure 3.9, $v_i(t)$ is defined by the magnetic field and physically related parameters, such as distance between reader and smart card. Capacitor C buffers electrical energy and the shunt resistor (depicted as a Zener diode for simplification purposes) limits the voltage $v(t)$, which is supplied to the electronics. The presented model-based estimation approach permits a hardware accelerated power and supply voltage analysis for each clock cycle featuring a minimized calculation delay. Thus, power and supply voltage management with a small control delay is enabled.

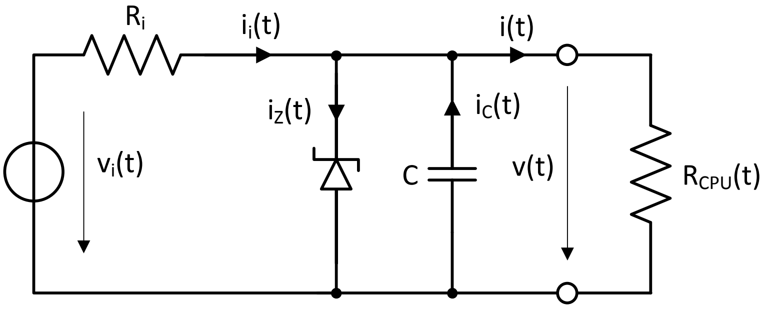


Figure 3.9: Simplified equivalent circuit of a contactles reader / smart card system. Obtained with changes from [10] and [11].

More detailed explanations concerning the presented estimation-based power management technique as well as the concepts involved are presented in Section 6.7.

3.3.2 Adaptive Field Strength Scaling

As outlined in the previous section, a contactless smart card is powered by a reader device through an alternating and modulated magnetic field. The power transferred to the smart card is limited and depends on several system parameters, such as antenna designs, antenna output gain, and smart card orientation as well as movement within the magnetic field. A permanent and sufficient power supply is therefore uncertain. As a consequence, many Near Field Communication (NFC)-based reader devices are designed to emit a magnetic field at a maximum possible strength, although a lower field strength would suffice. However, excessive electrical power is dissipated by the smart card's shunt resistor in order to prevent harmful electric surges. Since this power waste decreases the run-time of mobile battery operated readers, it is of eminent importance to attack this run-time limiting issue. Furthermore, the strong growth of mobile devices (e.g., NFC enabled smart phones) and NFC-based applications (e.g., ticketing, payment, e-passports) makes it a lucrative research field. As a consequence, this doctoral thesis explores and proposes a power optimization technique for reader / smart card systems called Adaptive Field Strength Scaling (AFSS). The working principle of AFSS is shown in Figure 3.10. AFSS is a technique that adapts the strength of the reader emitted magnet field according to the smart card's instantaneous power consumption. While the *H-Field Static* curve represents currently used approaches of generating a magnetic field of maximum strength, *H-Field Adaptated* curve represents the AFSS technique. During periods where the smart card requires a high amount of electrical power (e.g., due to performing cryptographic operations), the reader increases the strength of the magnetic field. During low power consuming periods (e.g., sleep or idle times), the reader decreases the strength of the magnetic field in order to save electrical power. The presented AFSS technique supports two different approaches:

- Each type of request sent from the reader to the smart card provokes a specific

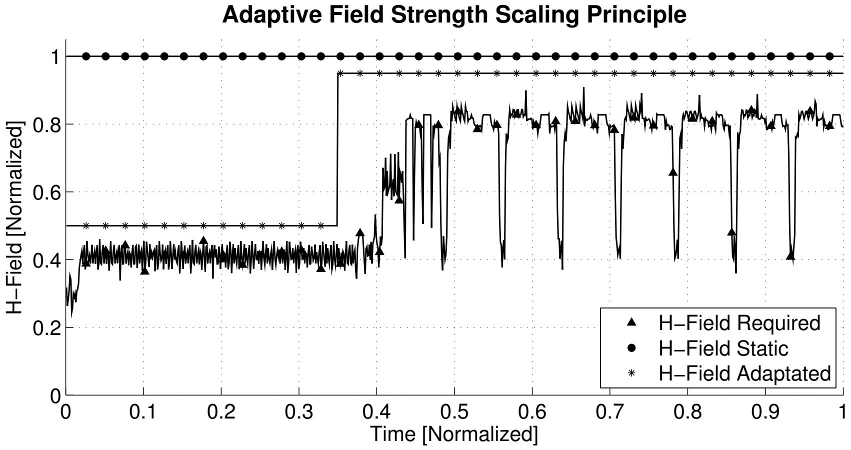


Figure 3.10: Adaptive Field Strength Scaling power saving technique: the magnetic field is adapted to the instantaneous power requirements of the smart card. Obtained from [12].

amount of power consumption at the smart card. The reader / smart card system employs a smart card power model, which is based on this request-based power knowledge, in order to optimize the magnetic field's strength for the request that is currently being processed. This approach can be implemented in software.

- The smart card monitors its instantaneous power consumption and supply voltage level. If power can be saved or a power starvation situation is detected, the smart card requests the reader to adapt the magnetic field strength. The reader / smart card system's power consumption can be optimized precisely, but hardware modifications at reader and smart card side are required.

A detailed description of this field strength scaling concept is given by Section 6.8.

3.3.3 Lightweight ECC-Based Authentication

Smart cards are the device of choice in order for providing authenticity and data integrity in the fields of security related applications. However, it is difficult to integrate state-of-the-art cryptographic methods in resource constrained systems, such as a contactless reader / smart card system, and to maintain a high level of flexibility at the same time. Therefore, this doctoral thesis introduces optimization techniques to permit the feasible integration of an elliptic-curve-based authentication solution into resource constrained systems.

In order to facilitate elliptic-curve-based cryptography in a resource constrained system, as it is given in Figure 3.11, an optimized ECC-based one-way authentication protocol is employed. This authentication protocol, which is based on the work of [78] and on the Diffie-Hellman key exchange method, takes into account the highlighted contactless smart card power constraints and timing constraints. It computes ECC point multiplications with the help of Montgomery Domain transformations and employs only x-coordinates. As a result, it permits a shifting of parts of the computationally intense ECC calculations from the smart card to the computationally powerful reader device. In addition, a maximum level of flexibility can be maintained by employing on the smart card side a state-of-the-art security controller that integrates a small processor core, such as an Application Specific Instruction-set Processor.

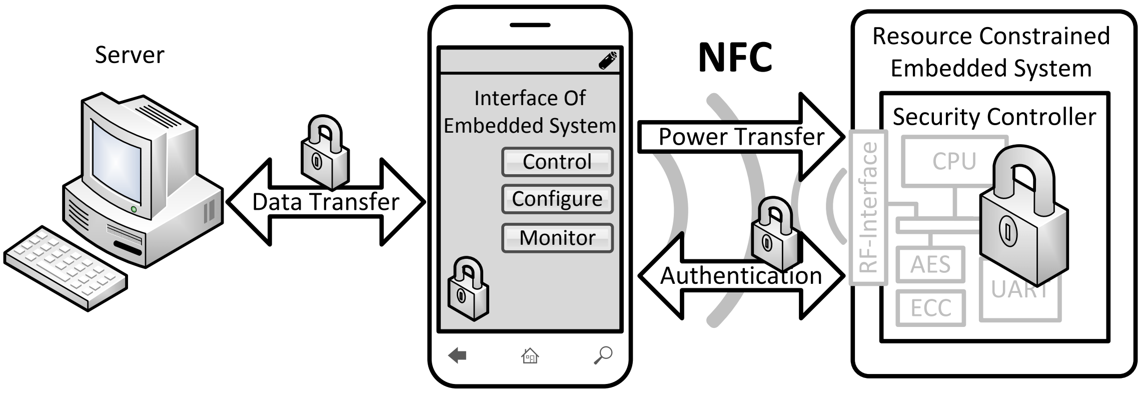


Figure 3.11: Concept of the lightweight authentication system. Obtained from [13].

Detailed explanations concerning the presented security optimization techniques are presented in Section 6.9 and Section 6.10.

3.4 Industrial NFC Interface Prototype

The RFID and NFC technologies can be utilized to implement an electronic device with an ultra-low or even suppressed standby power consumption by employing an innovative communication paradigm. Whilst in standby, the targeted electronic device is switched off completely instead of letting it poll or wait for user activity and hereby wasting electrical standby energy. Only on demand when the user wants to interact with the electronic device, it is powered up with electrical energy that is provided by NFC. Based on this conceptual idea, an industrial prototype of an innovative NFC Interface is presented that provides a zero-energy communication interface and facilitates a zero-energy standby mode for the targeted electronic device. The simplified conceptual design of this NFC Interface is presented in Figure 3.12. Whenever the user starts interacting with the target device, the reader device (e.g., an NFC-enhanced smart phone) emits an alternating and modulated magnetic field. The analog front end of the target device harvests electrical power from the provided magnetic field. The harvested electrical power is forwarded to the power supply control unit that switches on the target device's power supply. Then, the rest of the target device, which represents the actual electronic device the user wants to interact with, starts its operation. After all interactions between user and target device are finished, the power supply control unit switches off the target device's power supply. Thus, no electrical power can be dissipated by the target device during standby and idle times. Apart from standby power management, the presented interface technique features cryptography, innovative hardware abstraction and user interface concepts, and it facilitates configuration, monitor, and control tasks of the targeted electronic device.

Section 6.11 and Section 6.12 provide further detailed information regarding the presented interface technique.

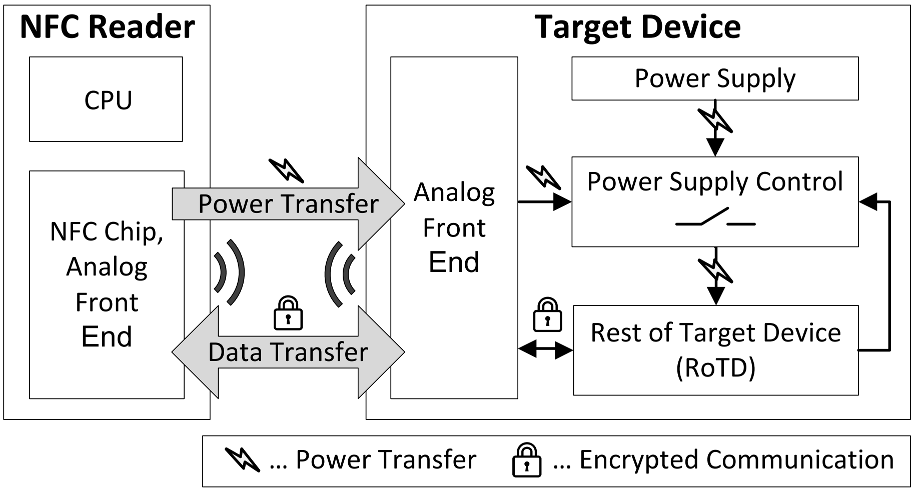


Figure 3.12: Conceptual design of the secure zero-energy NFC Interface. Obtained with changes from [14] and [15].

Chapter 4

Results and Case Studies

This chapter presents the results that were gained during the evaluation of the proposed techniques and tools. First, the involved components and environments that were used during this evaluation process are presented in Section 4.1. Section 4.2 illustrates selected case studies and the detailed approach of the design evaluation framework for secure and low-power embedded systems. This is followed by Section 4.3, which presents selected evaluation results of the previously introduced optimization techniques for contactless reader / smart card systems. Finally, this chapter is concluded by Section 4.4 that shows the industrial prototype which introduces the secure Near Field Communication Interface for everyday electronic devices.

4.1 Evaluation Systems

Two evaluation systems were employed in order to evaluate the techniques and tools presented by this doctoral thesis. The first evaluation system uses Infineon security controllers of the SLE 70 platform. The second evaluation system adopts a freely available LEON3 multi-processor system. Apart from these controllers and SoCs, reconfigurable prototyping platforms are employed to facilitate the emulation-based analyses. For this purpose, Xilinx Spartan 3, Virtex 5, and Virtex 6 FPGA platforms were chosen. Simulation and synthesis tasks were carried out on a six-core AMD Phenom II 3.2 GHz processor system with 16 GB RAM. In the following, the basic architectures and features of the LEON3 and the Infineon security controllers are elucidated.

4.1.1 Infineon Security Controller System

The Infineon SLE 70 security controller platform represents a prime example of contemporary low-power and secure embedded systems. For instance, the SLE 77CFX2400P, which is a derivative of the SLE 70 platform [86], implements a 16-bit processor core that runs with a clock frequency of up to 30 MHz. This security controller is manufactured with a 90nm process and features hardware integrated crypto cores to accelerate symmetric (AES, DES, 3DES) and asymmetric crypto implementations (ECC, RSA). Furthermore, it features state-of-the-art side-channel countermeasures. Apart from the contactless interface, this security controller also supports a contact-based interface.

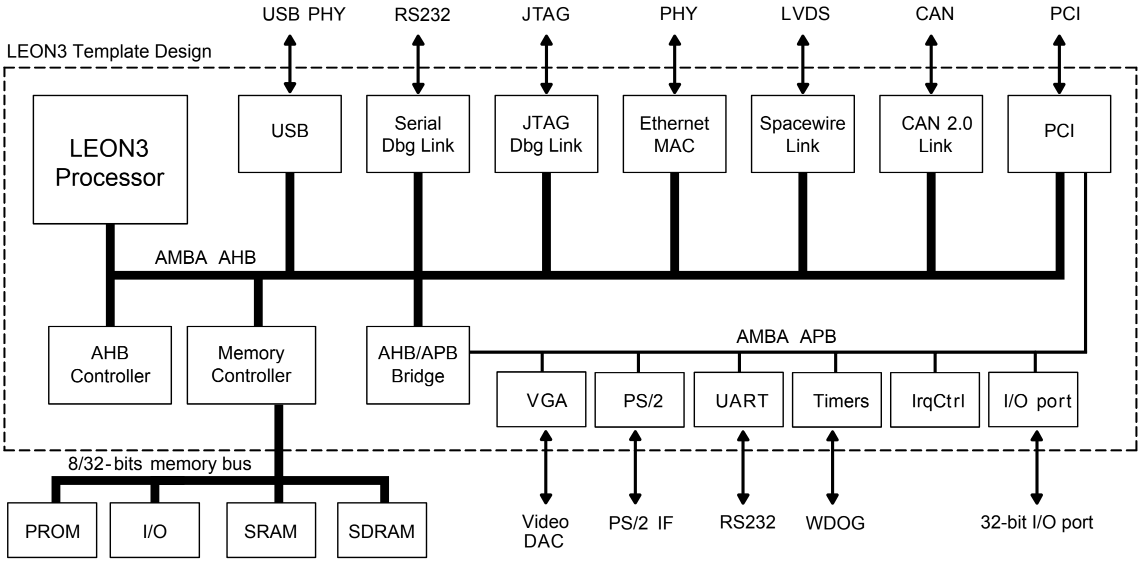


Figure 4.1: Architectural overview of the LEON3 processor core and a set of supported peripherals. Obtained with changes from [16].

4.1.2 LEON3 Open Source Processor System

The LEON3 processor is a VHDL-based IP core developed by Aerflox Gaisler on behalf of the European Space Agency. It is a 32-bit multi-core processor, compliant with the SPARC V8 architecture, and is available under the GNU GPL license that permits an unlimited use for research. This processor comes with a variety of additional modules and peripherals, which makes it very suitable for System-on-Chip solutions. Its basic architecture is depicted in Figure 4.1. Thanks to its open architecture, it can be easily adapted, extended, and employed in FPGA-based prototyping environments.

4.2 Design Evaluation Framework

The comprehensive design evaluation framework, which was introduced in Section 3.2, was evaluated thoroughly on various Xilinx prototyping platforms. Selected results relating to the design emulation, system emulation, and high-level simulation techniques are presented in the following.

4.2.1 Design Emulation

Figure 4.2 shows the architecture of an emulation-based test bench that features the proposed design emulation technique from Section 3.2.1. A design-under-test is integrated into a prototyping platform, such as an FPGA, with model-based analysis units. A power estimation unit, which is connected to the design-under-test, monitors the design-under-test's internal states $\mathbf{x}(t)$. This power estimation unit delivers power estimates $\widehat{P}(\mathbf{x}(t))$ according to its integrated power model and the monitored states $\mathbf{x}(t)$. The power estimates are then scaled by an attached dynamic voltage and frequency scaling (DVFS) unit in accordance with the currently set voltage $V_{DD}(t)$ and frequency $f(t)$ parameters. The

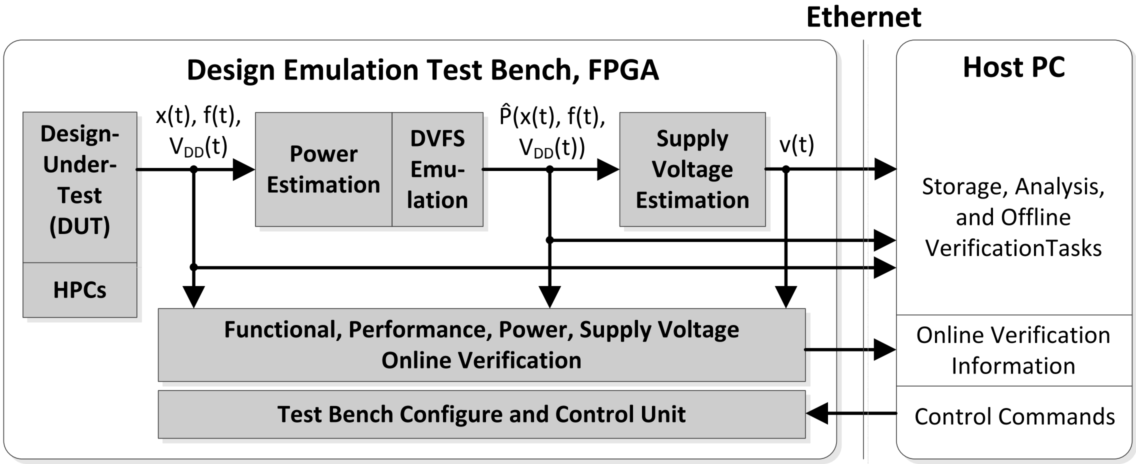

Ethernet
Design Emulation Test Bench, FPGA
Host PC
Design-Under-Test (DUT)
HPCs
x(t), f(t), V_DD(t)
Power Estimation
DVFS Emu-lation
P̂(x(t), f(t), V_DD(t))
Supply Voltage Estimation
v(t)
Storage, Analysis, and Offline VerificationTasks
Functional, Performance, Power, Supply Voltage Online Verification
Online Verification Information
Test Bench Configure and Control Unit
Control Commands

Figure 4.2: Architecture of the proposed design emulation test bench. The design-under-test is integrated into an FPGA along with model-based analysis and verification units. The gained analysis data is transferred to a host PC. Obtained with changes from [6].

resulting power estimates $\widehat{P}(\mathbf{x}(t), f(t), V_{DD}(t))$ are then forwarded to the supply voltage estimation unit, which models the design-under-test's power supply network. This unit estimates the design-under-test's supply voltage behavior $v(t)$ based on its power consumption and the implemented power network model.

The online verification unit surveys the provided functional, performance, power, and supply voltage data with regards to predefined constraints and breakpoints. If a predefined constraint is violated or a breakpoint is reached, the design-under-test is stopped and a step-by-step debugging can be carried out. In addition, the test bench features an Ethernet-based control and debug interface. This control and debug interface is employed by a host PC to control and setup the test bench with specific test patterns and verification constraints. Moreover, all analysis data, whether they are results from functional testing, performance testing, or power and supply voltage analyses, are transferred through this interface from the test bench to the host PC. Then, on the PC side, this data can be archived or used by software tools for further offline analysis and verification tasks.

For the following test, a contactlessly powered smart card design is synthesized in a Xilinx Spartan 3 FGPA board. During this test, it is evaluated whether the smart card is able to execute a software-based AES encryption feasibly without violating certain power or timing constraints. The left graph of Figure 4.3 illustrates the smart card's behavior while using a clock frequency of 31 MHz. The monitored power consumption profile reveals a low-power initialization phase of the application and three high-power consuming AES encryption phases. The smart card's supply voltage profile shows hazardous voltage drops below a critical threshold of 1 V as soon as the calculation intense and high-power consuming AES encryption starts. As a consequence, the smart card's operational stability would be compromised. The right graph of Figure 4.3 demonstrates a possible solution for the detected power issue. If the smart card reduces the clock frequency of its CPU during the AES encryption, the smart card will dissipate less power and its supply voltage level will stay above the crucial 1 V threshold. As a result, the smart card's operational stability is provided at the cost of an increased benchmark run-time of 17%.

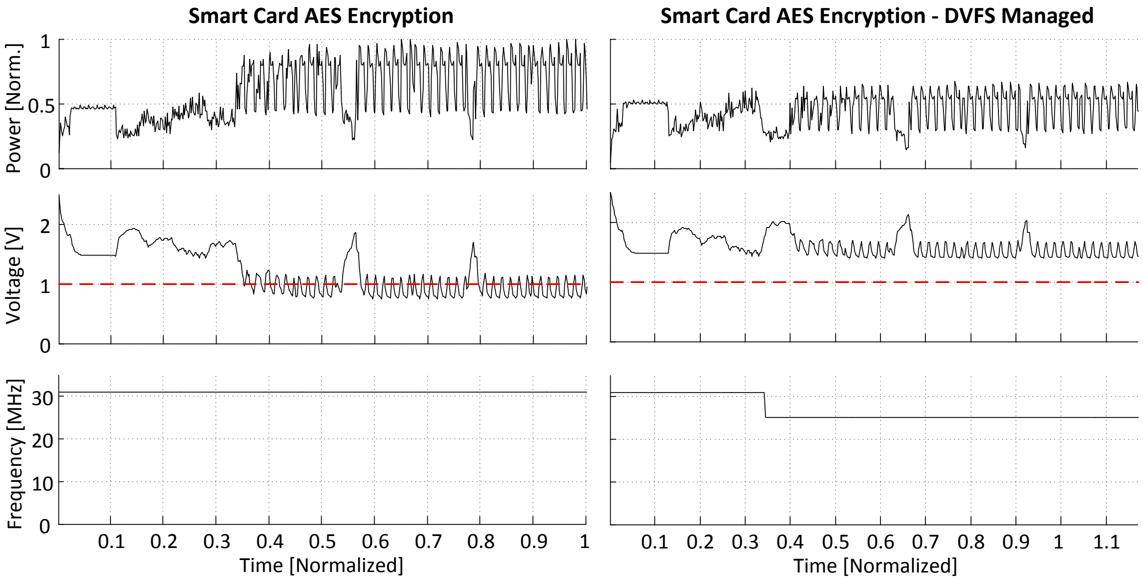


Figure 4.3: Impact of a contactless smart card's clock frequency scaling functionality: if the frequency is reduced, power dissipation and supply voltage drops will be reduced during the calculation intense AES encryption. As a result, the smart card's operational stability is provided. Obtained with changes from [6].

Table 4.1 demonstrates the acceleration of the analysis process that can be gained by employing the design emulation approach. This table shows several benchmarks and the corresponding consumed time for simulation and emulation approaches. Simulations were performed with Mentor Graphics' ModelSim on a six-core AMD Phenom II 3.2 GHz processor system with 16 GB RAM. Note, a certain amount of time is needed to setup a design emulation test bench. Since this initial setup is required only once, it is not regarded in this comparison.

Table 4.1: Comparison of Simulation and Design Emulation Analysis Speeds, cf. [6].

Benchmark	RTL Simulation Time	Emulation Time	Speed-up
String Search	18 min 52 sec	5.5 ms	20581
FFT	22 min 39 sec	7.7 ms	17142
Basicmath	49 min 50 sec	17.3 ms	17283
Quicksort	31 min 43 sec	9.9 ms	19222

4.2.2 System Emulation

The system emulation approach extends the previously presented design emulation approach. Now, the crucial system aspect is taken into account and techniques are employed in order to enhance security and dependability related analysis. For this purpose, fault injection techniques are used and the power emulation technique is improved to permit side-channel analysis. Figure 4.4 shows the architecture of a test bench that evaluates a trustworthy mobile authentication system with elliptic-curve based security. The evalu-

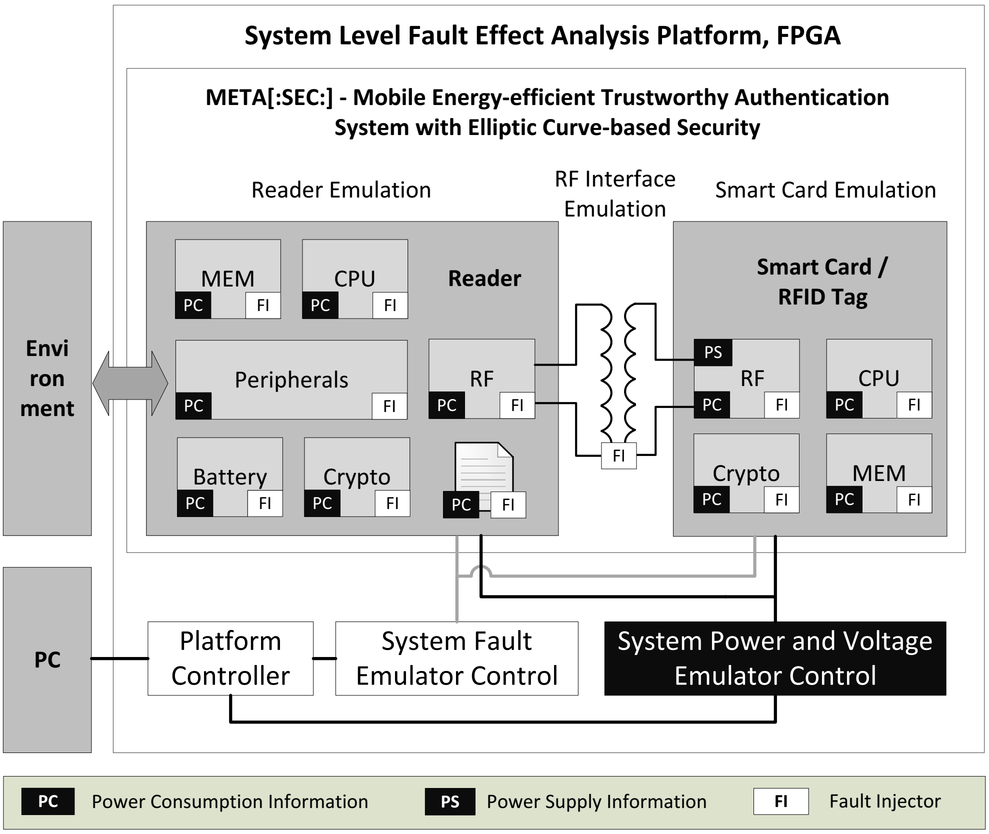

System Level Fault Effect Analysis Platform, FPGA
META[:SEC:] - Mobile Energy-efficient Trustworthy Authentication System with Elliptic Curve-based Security
Reader Emulation
RF Interface Emulation
Smart Card Emulation
Envi ron ment
Reader
MEM
CPU
Peripherals
RF
Battery
Crypto
PC
FI
PS
Smart Card / RFID Tag
RF
CPU
Crypto
MEM
PC
Platform Controller
System Fault Emulator Control
System Power and Voltage Emulator Control
PC Power Consumption Information
PS Power Supply Information
FI Fault Injector

Figure 4.4: Architecture of a test bench featuring a reader / smart card system emulation. All components are integrated into an FPGA. Relevant components are augmented with power sensors and fault injectors. Obtained with changes from [7].

ated system consists of a reader, smart card, and a model of the contactless RFID-based communication interface. All components are synthesized into an FPGA-based prototyping board. Those components that are relevant for analysis are augmented with fault injectors (saboteurs or mutants) and model-based power consumption as well as supply voltage analysis units. A platform controller provides interfaces for test engineers to configure the test bench. In addition, all analysis data that is gathered is transferred to a host PC through the platform controller's interface. Further offline data analysis tasks can then be carried out on the host PC. This innovative system-level evaluation approach permits a test engineer to implement novel analysis methods and attack scenarios, which are unfeasible if only individual components are considered.

The following test demonstrates the usage of the system emulation test bench by a verification engineer. The pictured test evaluates the data transmission resistance against corrupted data packets of the contactless communication link between reader and smart card. Apart from malicious attacks, such data corruption effects can also be caused, for instance, by radiation or electromagnetic interference induced by an industrial environment. The basic concept of this data corruption test is illustrated in Figure 4.5. Data packets are generated within the reader device and are marked with an incrementing number. The packets are sent through the faulty channel to the smart card and then back to

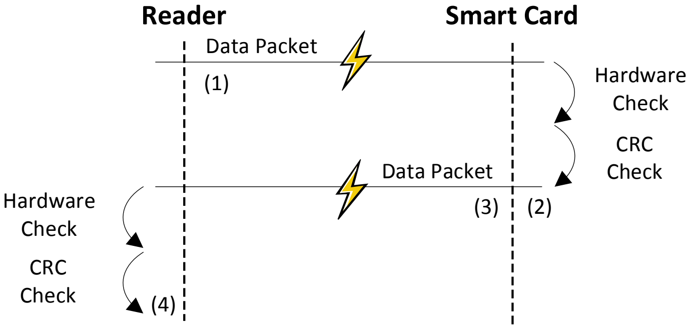


Figure 4.5: Concept for evaluation of a reader / smart card system's resistance against data corruption attacks. Obtained with changes from [7].

the reader. In this example, the data corruption effect is emulated by injecting stuck-at multi-bit-upsets randomly into the hardware FIFOs of the data interfaces of reader and smart card. Both reader and smart card carry out hardware checks and CRC checks in order to detect corrupted data packets. If a corrupted packet is detected, the packet will be dropped.

Table 4.2 shows the results of the conducted data corruption test. More than 300,000 faults were injected into the hardware FIFOs of reader and smart card. However, not every injected fault also results in a corrupted data packet. According to the obtained test results, the data consistency checks performed within reader and smart card were able to detect all corrupted packets. As a consequence, the implementations of the tested data interfaces can be considered as resistant against this specific data corruption fault attack.

Table 4.2: Data Corruption of Reader / Smart Card Data Channel, cf. [7]

Seq. #	Component	Packets Sent	Corrupted Packets Dropped
1	Reader	9148	-
2	Smart Card	-	963
3	Smart Card	8185	-
4	Reader	-	995

Table 4.3 summarizes the FPGA utilization of the system emulation test bench that features the reader / smart card system. This test bench was synthesized with Xilinx ISE and targeted a ML507 prototyping board from Xilinx. The highest area is consumed by the platform controller that implements a small CPU. Thanks to this CPU-based approach a maximum level of flexibility can be maintained.

4.2.3 High-Level Simulation

Figure 4.6 illustrates the basic architecture of the high-level SystemC-based simulation test bench that permits power-aware and thermal-aware evaluations. In this case study, the presented simulation test bench targets a contactless reader / smart card system, which consists of three transaction-based components: reader model, RF channel model, and augmented smart card model. As shown in the figure, the reader emits a magnetic field that is generated by the electrical current $i_R(t)$. The transferred data $d(t)$ and

Table 4.3: FPGA Utilization of Components of the System Emulation Test Bench, cf. [7]

Test Bench Component	Slices	LUTs
System Fault Emulation Controller	437	436
Fault Trigger Module	70	150
Power Consumption Emulation	206	440
RF and Power Supply Emulation	464	756
Platform Controller (CPU)	5752	4308

transferred power $P(t)$ to the smart card is represented by the model of the RF channel. The power aware and thermal aware smart card model is made of several sub-modules. The power model provides power consumption estimates according to the smart card's internal states $\mathbf{x(t)}$ and its current temperature $T(t)$. These power estimates $P_{CPU}(t)$, $P_{Shunt}(t)$, etc. are then forwarded to the thermal model unit. This unit simulates the temperature behavior of the smart card according to its floor plan, packaging, temperature coefficients of used materials, etc. A modified version of the tool HotSpot, which was developed and introduced by the authors in [45], is used for the temperature computations $T(t)$. These temperature estimates $T(t)$ are forwarded to the thermal effect model, which estimates the effects of thermal stress, such as Mean Time To Failure (MTTF) and critical path delays. Finally, a fault injection controller translates these thermal fault effects into the modeled functionality of the reader / smart card system by controlling saboteur and mutant units. Faults $F(t)$ can be either injected into reader, into the RF channel, or into the smart card. Thus, a comprehensive design exploration, evaluation, and verification environment is created, which can support engineers during the whole development process of a contactless reader / smart card system.

The following test analyzes the temperature behavior of a smart card. Both graphs of

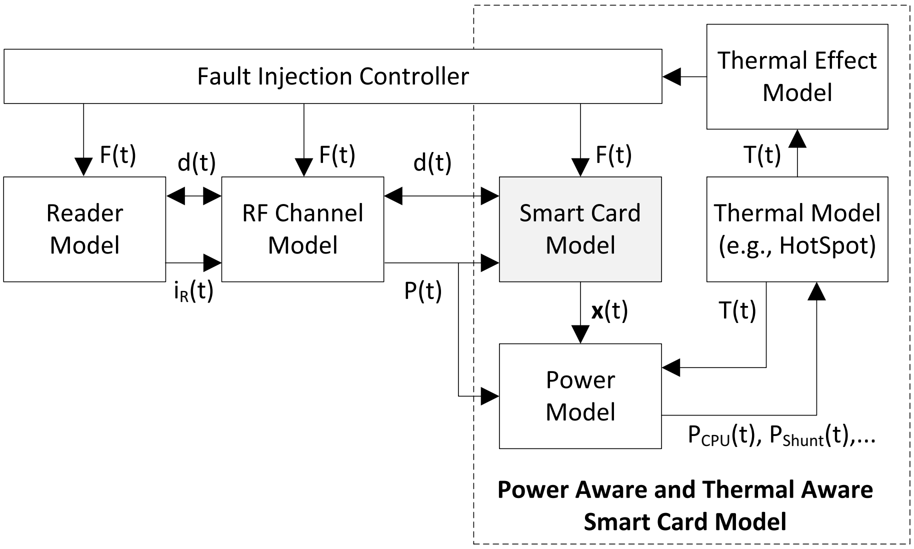


Figure 4.6: Architecture of the high-level power-aware and thermal-aware simulation framework that features a contactless reader / smart card system. Obtained from [9].

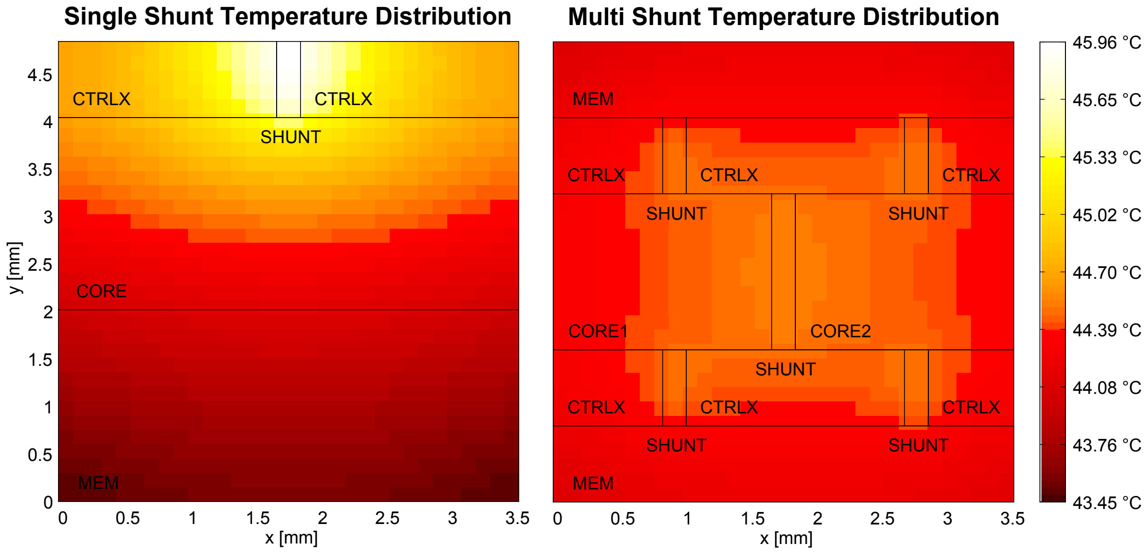


Figure 4.7: Steady-state temperature distribution of a smart card featuring a single shunt resistor and a smart card featuring a distributed shunt resistor. Obtained with changes from [9].

Figure 4.7 illustrate a smart card's steady-state temperature distribution while applying a high magnetic field of 7 A/m with an environmental temperature of 20 °C. The left graph shows a smart card that implements a single shunt resistor. The simulation shows a single hot spot of 45.96 °C, which is caused by the shunt resistor's high power consumption. The power dissipation and temperature influence of all other smart card units is diminishing at a low level in the case of such a high magnetic field strength. The right graph of Figure 4.7 demonstrates an innovative floor plan approach to partitioning the shunt resistor into five parts and distributing it evenly throughout the chip. Therefore, the shunt resistor distributes its generated heat better and the maximum chip temperature decreases to 44.52 °C. As a consequence, the lifetime of the smart card's electronics is prolonged by 11%, which is especially important in application fields, such as automotive industries, that require an extremely low or even zero chip error rate.

4.3 Exploration of Optimization Techniques

This section presents selected results that were obtained whilst exploring and evaluating the optimization techniques, which were introduced in Section 3.3, for contactless reader / smart card systems.

4.3.1 Estimation-Based Power Management for Smart Cards

The architecture of a multi-core smart card that is enhanced with the estimation-based power management technique, which was introduced in Section 3.3.1, is shown in Figure 4.8. Each power estimation unit monitors a processor core's states $\mathbf{x}_i(t)$ and provides corresponding power consumption estimates $\widehat{P}(\mathbf{x}_i(t))$. These power estimates are then scaled by a DVFS unit according to currently set voltage V_{DDi} and frequency f_i parameters. The power consumption results of each process core $\widehat{P}(\mathbf{x}_i(t), f_i(t), V_{DDi}(t))$ are then

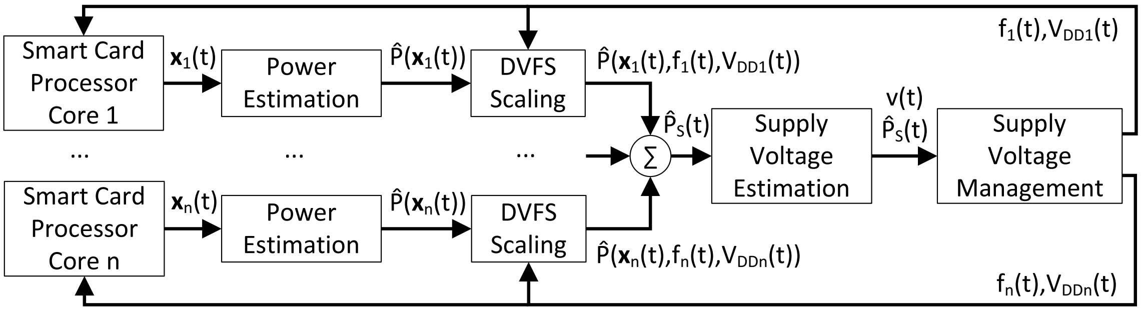


Figure 4.8: Architecture of the multi-core smart card design that features estimation-based power management. Obtained from [10].

collated and are forwarded to the supply voltage estimation unit. This unit estimates the smart card's supply voltage behavior $v(t)$ with the help of a model of the reader / smart card power supply network. The power consumption $\widehat{P}_S(t)$ and supply voltage $v(t)$ estimates are then evaluated by the supply voltage management unit. Finally, this unit adapts the individual smart card cores' DVFS parameters V_{DDi} and f_i, according to certain guidelines, in order to flatten the power consumption profile and to reduce hazardous supply voltage drops.

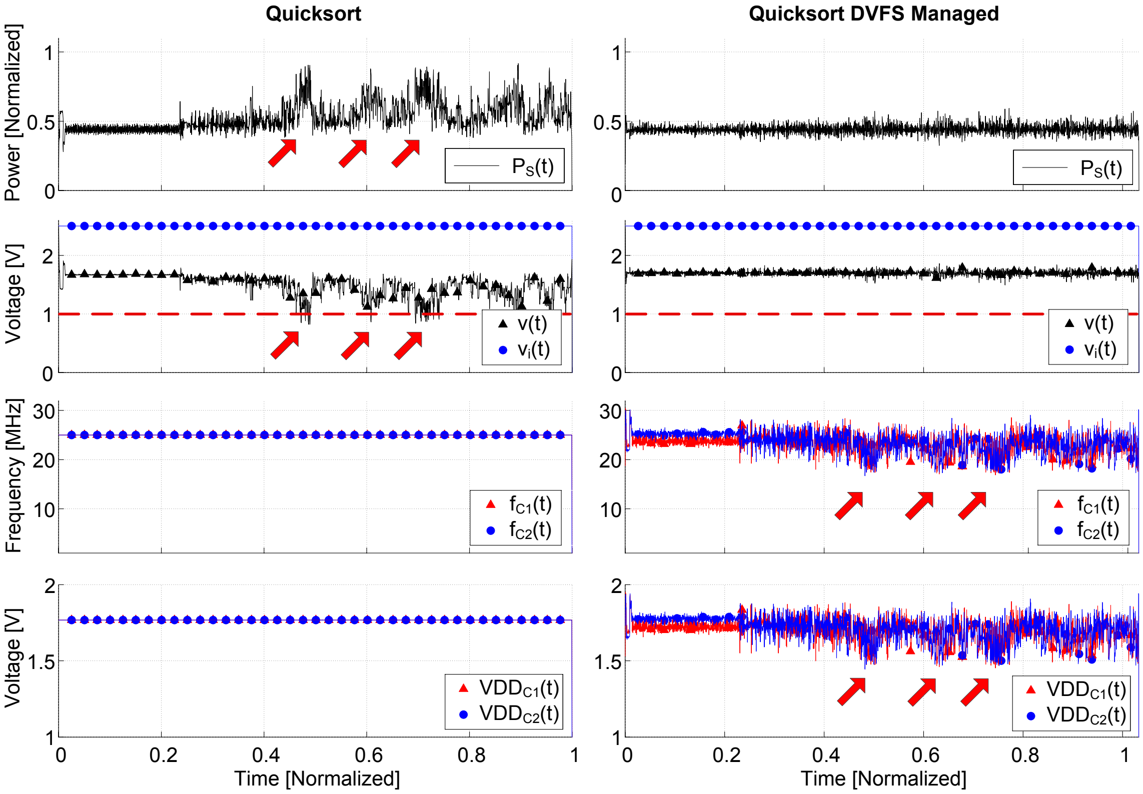


Figure 4.9: The left graph shows the unmanaged smart card behavior with hazardous voltage drops below 1 V. The right graph shows the managed smart card behavior with reduced peak power consumption and supply voltage drops. Obtained with changes from [10].

The presented estimation-based power management approach was evaluated with the help of the design evaluation framework that was introduced in Section 3.2 and Section 4.2. The left graph of Figure 4.9 shows the unmanaged smart card's power and supply voltage behavior during the execution of a Quicksort benchmark. Arrows mark critical peak power consumptions $\widehat{P}_S(t)$. These power consumption hazards cause the smart card's supply voltage to drop below the crucial threshold of 1 V. As a consequence, the smart card's operational stability is compromised. The right graph of Figure 4.9 shows the managed smart card behavior. The power consumption profile is flattened and a defined supply voltage setpoint of 1.7 V is maintained. Thus, the smart card's operational stability is maintained. However, due to the DVFS adaptions, the run-time of the Quicksort benchmark increased by 3.3%.

4.3.2 Adaptive Field Strength Scaling

This section presents a detailed case study and evaluation results of the Adaptive Field Strength Scaling technique for contactless reader / smart card systems, which was introduced in Section 3.3.2. AFFS supports two basic approaches, the *request-based AFSS* and the *instantaneous power consumption-based AFSS*. The concept of the request-based AFSS approach is illustrated in Figure 4.10. The reader generates a request r and sends it to the smart card. The smart card evaluates the power requirements in order to process the request r by means of a power model. This power model takes into account certain parameters, such as current power consumption or strength of the magnetic field, and provides a power estimate $\widehat{P}(r)$. The AFSS policy unit then decides whether the strength of the magnetic field suffices, needs to be increased to meet the power requirement $\widehat{P}(r)$, or decreased to save electrical energy. If the strength of the magnetic field needs to be adapted, then a corresponding message hr is transmitted to the reader. Finally, the reader receives this message hr and adapts the magnetic field strength accordingly.

The Adaptive Field Strength Scaling principle was evaluated thoroughly with the help of the previously presented design evaluation framework. Figure 4.11 depicts the resulting behavior of a smart card design that supports the request-based AFSS technique. During the high power consuming cryptographic operations, the reader was requested to increase the field strength. As a consequence $v_i(t)$, which is defined by the magnetic field, equaled 3.9 V. During the low power consuming operations, the magnetic field strength was reduced and $v_i(t)$ decreased to 3 V. Only a small amount of electrical power was wasted by

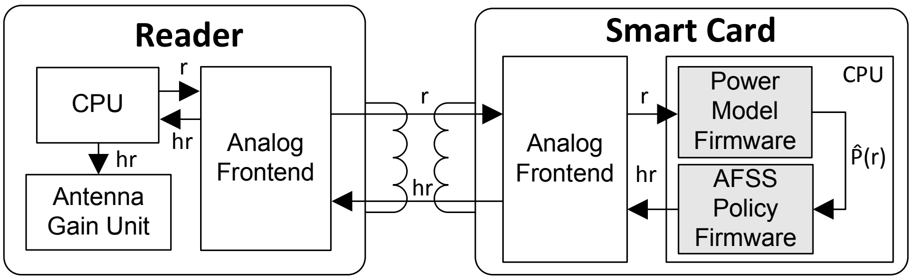


Figure 4.10: Concept of the request-based AFSS power optimization technique. The magnetic field strength can be adapted according to the smart card's power requirement. Obtained from [12].

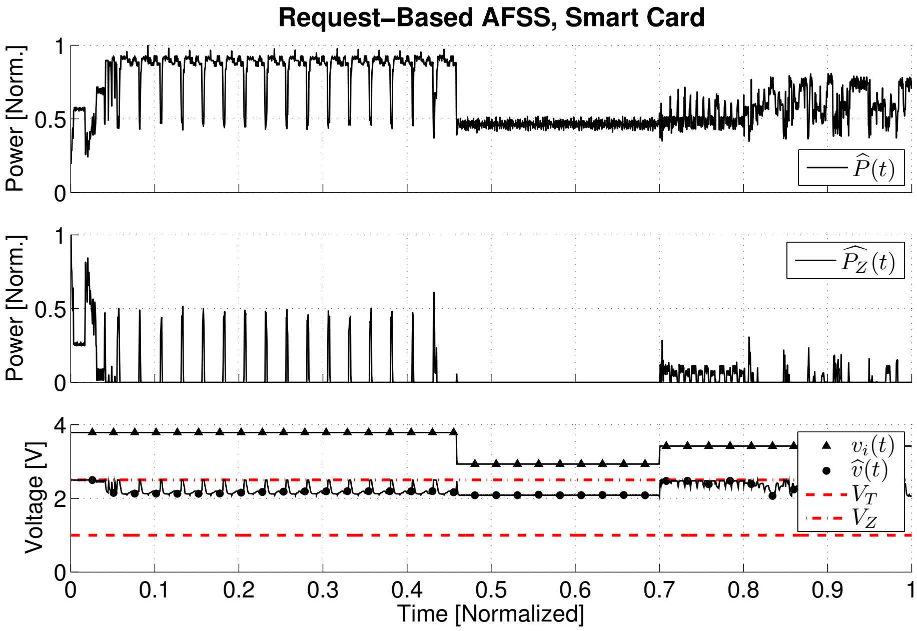


Figure 4.11: Behavior of a smart card that features the request-based AFSS technique. The magnetic field strength is adapted according to the current power requirements. Obtained from [12].

the reader / smart card system, which is demonstrated by the Zener diode's minimized power consumption $\widehat{P}_Z(t)$. 25% of the electrical energy was saved during this benchmark compared to a reader / smart card system without AFSS support. In addition, the crucial voltage $\widehat{v}(t)$, which is provided to the smart card's electronics, did not drop below the hazardous threshold V_T. Thus, the smart card's operational stability was maintained.

4.3.3 Lightweight ECC-Based Authentication

A proof of concept of the lightweight ECC-based authentication solution, which was introduced in Section 3.3.3, was implemented. This section gives more detailed implementation information and evaluation results with regards to this proof of concept that features a contactless reader / smart card system. Figure 4.12 depicts the sequence of the one-way authentication between reader and smart card. The reader computes a challenge $\widetilde{x}_A$, which was transformed into the Montgomery Domain, and sends it to the smart card. The smart card computes the response $\widetilde{x}_B$. $\widetilde{x}_B$, the public key x_T, and a signature S_T are then sent back to the reader. The reader verifies the signature, computes $\widetilde{x}_C$, and transforms $\widetilde{x}_C$ and $\widetilde{x}_B$ back to the original domain. Finally, if x_C equals x_B, an authentication was successfully completed. The smart card can process this one-way authentication protocol very efficiently, because only one Montgomery operation *Mont* needs to be carried out and only x-coordinates are considered.

This protocol was evaluated with the help of an Android 4.3 Samsung Galaxy i9300 S3 smart phone as a reader device and a smart card featuring an Infineon security controller running at 30 MHz. The NFC-based communication link was configured to the lowest possible transmission rate of 106 kBit/s. Figure 4.13 illustrates the timing behavior of the

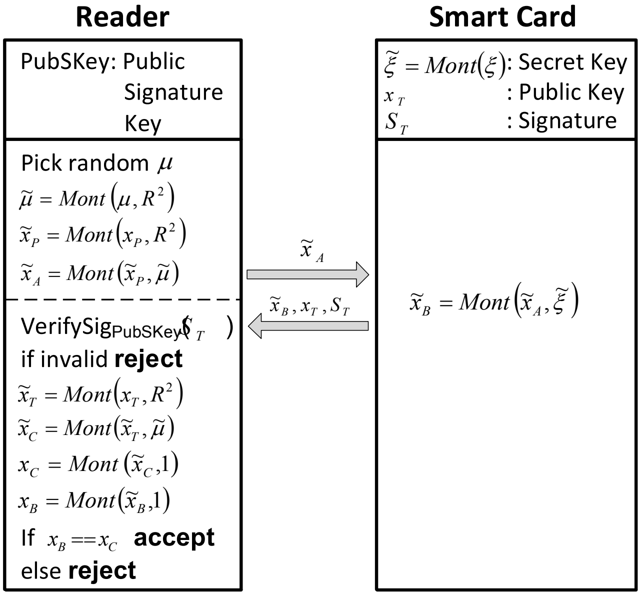

Reader
Smart Card
PubSKey: Public Signature Key
Pick random μ
$\tilde{\mu} = Mont(\mu, R^2)$
$\tilde{x}_P = Mont(x_P, R^2)$
$\tilde{x}_A = Mont(\tilde{x}_P, \tilde{\mu})$
VerifySig$_{PubSKey}$(S_T)
if invalid reject
$\tilde{x}_T = Mont(x_T, R^2)$
$\tilde{x}_C = Mont(\tilde{x}_T, \tilde{\mu})$
$x_C = Mont(\tilde{x}_C, 1)$
$x_B = Mont(\tilde{x}_B, 1)$
If $x_B == x_C$ accept
else reject
$\tilde{x}_A$
$\tilde{x}_B, x_T, S_T$
$\tilde{\xi} = Mont(\xi)$: Secret Key
x_T : Public Key
S_T : Signature
$\tilde{x}_B = Mont(\tilde{x}_A, \tilde{\xi})$

Figure 4.12: ECC-based one-way authentication protocol used between reader and smart card. Computation effort is shifted from the smart card to the reader device by operating in the Montgomery Domain. Obtained from [13].

one-way authentication protocol, which was executed 500 times, without the signature verification process. The average amount of time required to process the protocol was as low as 26.2 ms. Note, the non-deterministic timing spikes in Figure 4.13 were caused by the Android operating system. These benchmark results show that the authenticity of a resource constrained embedded system, such as a smart card, can be verified very efficiently if the whole authentication system is aware of the given constraints.

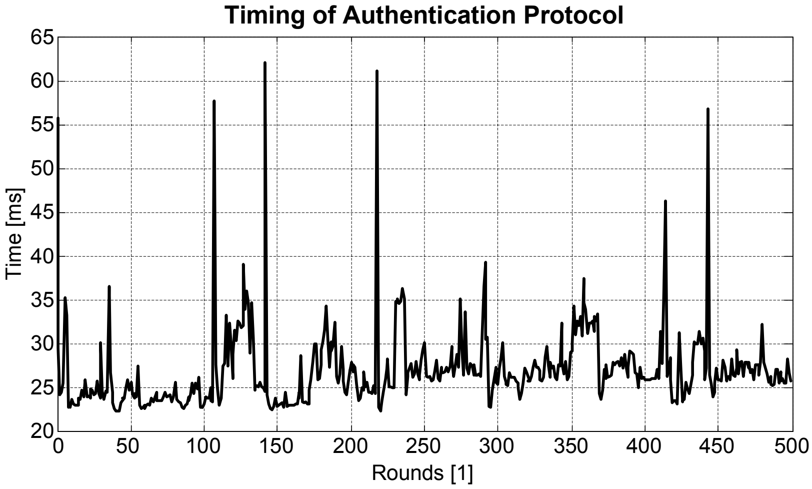


Figure 4.13: Required time for processing the ECC-based authentication protocol without signature verification while using an NFC data rate of 106 kBit/s. Obtained from [13].

4.4 Industrial NFC Interface Prototype

This section presents implementation details and results of a proof of concept that features the industrial NFC Interface prototype, which was introduced in Section 3.4. The architecture of an exemplary system that is enhanced with this NFC Interface is shown in Figure 4.14. According to this figure, the system consists of an NFC-enabled reader device (e.g., an NFC-enabled smart phone) and a target device. The reader device comprises of an NFC Interface software stack and the NFC chip with its analog frontend. The target device consists of an analog frontend, a magnetic field-powered NFC Interface chip, power supply and control units, the rest of the target device (RoTD) and its optional interface chip. The RoTD represents the actual electronic device the user wants to interact with (e.g., payment terminal, access control terminal). The conceptual idea works as follows. During idle and standby modes, the RoTD is disconnected from its power supply. Electrical power is transferred from the reader to the target device only when the user wants to interact with the RoTD. This transferred electrical energy is then used to switch on the RoTD's power supply. After the RoTD has finished its designated tasks, it goes back into standby mode and its power supply is switched off. Thus, no electrical power is dissipated whilst in standby mode. Apart from standby power management, the NFC Interface supports further important tasks, such as monitoring, configuration, and control of the RoTD, as well as authentication and secured data transfer. Thus, a secured field-powered communication interface is given that supports a zero-energy standby mode for the targeted electronic device.

As a proof of concept, a contactless smart card-based access control terminal was enhanced with the NFC Interface concept. Whilst in standby, the access control terminal (RoTD) is switched off and no standby power is dissipated. When a user wants to perform an authentication, he or she activates NFC on the NFC-enabled smart phone. The emitted magnetic field powers up the access control terminal. Then, the smart phone starts the NFC communication and performs the secured authentication. If the authentication was successful, the access control terminal opens the door. After the door closed, the RoTD returns to the zero-energy standby mode by disconnecting its power supply. Figure 4.15

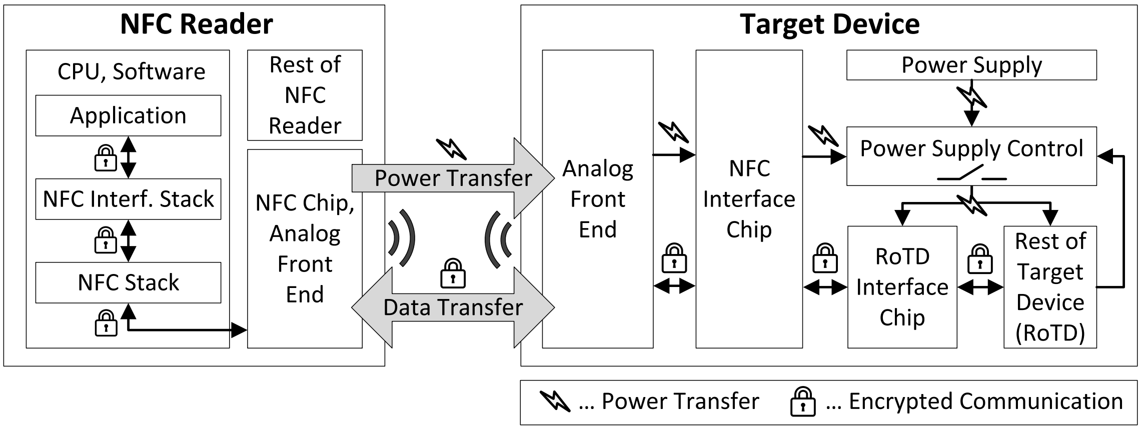


Figure 4.14: Architecture of the secure zero-energy NFC interface solution for everyday electronic devices. Obtained from [15].

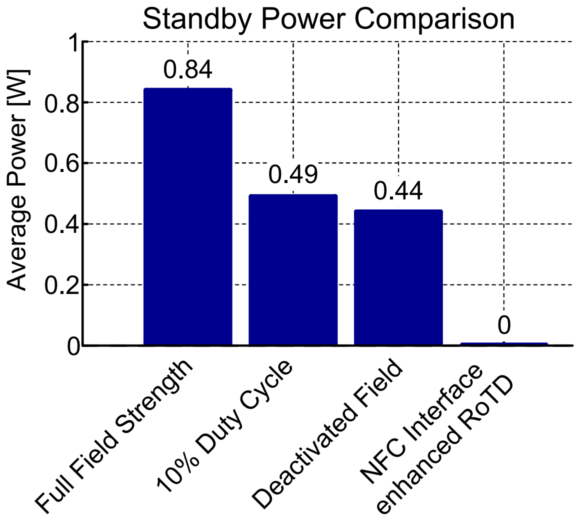


Figure 4.15: While the original access control terminal dissipated at least 0.44 W during standby, the NFC Interface enhanced version eliminated standby power dissipation. Obtained with changes from [14].

shows the standby power savings that were achieved with the NFC Interface enhanced access control terminal. The card reader hardware of the original terminal consumed on average 0.49 W if the magnetic field and a card detection polling duty cycle of 10% were activated. In contrast, the NFC Interface enhanced access control terminal reduced any standby power consumption to 0 W.

Figure 4.16 shows an industrial prototype assembly of a target device that features the NFC Interface. In this case, the RoTD implemented a simulation of a smart meter device.

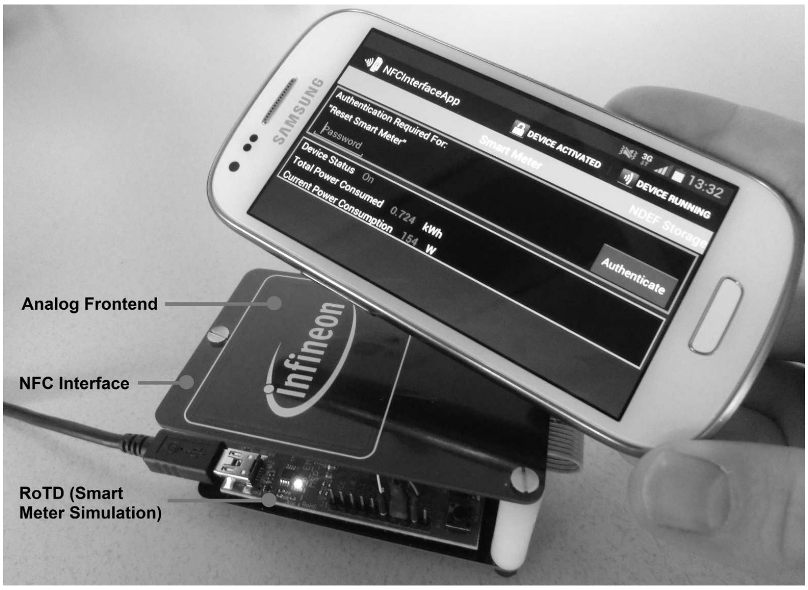


Figure 4.16: This figure shows the NFC Interface demonstrator featuring a smart meter target device simulation. Obtained from [15].

Chapter 5

Conclusion and Future Work

5.1 Conclusion

Integrated circuits and embedded systems have increased exponentially in their complexity and integration density over the past few decades. However, this complexity trend introduces negative side effects that need to be tackled by engineers, such as, a potential increase of power consumption accompanied by thermal stress and power supply issues caused by large numbers of simultaneously switching transistors. Furthermore, deep-submicron manufacturing processes make the integrated circuits more prone to environmental disturbances and therefore increase dependability issues. These issues, in combination with increasing time-to-market pressures and shorter product development cycles, make it difficult to achieve a high verification coverage for innovative designs.

This doctoral thesis addresses the highlighted issues when developing integrated circuits and complex embedded systems. It proposes a comprehensive design evaluation framework that supports engineers during the design phase in order to detect and resolve design flaws and to evaluate design optimizations early, before the tape-out. This evaluation framework enables an engineer to test hardware and software designs with regards to functional and performance behavior, as well as their impact on power consumption and supply voltage levels. Analysis data can be obtained hardware accelerated and for each clock cycle. This framework also stresses the importance to take into account crucial system aspects when developing complex embedded systems. In addition to this system evaluation approach, fault injection techniques are added to the framework, which improves its analysis capabilities particularly for secure and dependable embedded systems. Although the presented hardware accelerated analysis techniques deliver accurate data for each clock cycle, they lack in flexibility. This drawback is addressed by extending the analysis framework with a flexible high-level SystemC-based analysis approach. This high-level solution enables fast but less accurate design analysis and focuses on contactless reader / smart card systems.

The next part of this doctoral thesis explores innovative power, thermal, and security optimizations for secure and contactless reader / smart card systems, which were evaluated with the previously introduced design evaluation framework. First, an estimation-based power optimization technique is presented. This power optimization technique regards a smart card's power constraints and is able to reduce peak power consumption and supply voltage drops. Second, a system-level power optimization approach is explored and proposed that adapts the reader emitted magnetic field strength depending on the smart card's instantaneous power requirements. This part of the doctoral thesis is concluded with optimizations in the research field of elliptic-curve cryptography for resource constrained systems. While hardware/software partitioning optimizations are proposed to accelerate ECC point multiplications, protocol optimizations are demonstrated that shift computational effort from the constrained device to the powerful reader.

The final part of this doctoral thesis introduces a secure Near Field Communication Interface for everyday electronic devices, which was designed with the insights gained from the preceding design analysis and optimization phases. This interface employs the electrical power emitted by the reader to provide a zero-energy communication interface and to support a zero-energy standby mode for the targeted electronic device.

5.2 Directions for Future Work

The research carried out during this doctoral thesis opens up possibilities for further research topics in the fields of integrated circuit analysis, embedded system analysis, and power management techniques.

5.2.1 Process Variability Emulation

Transistor sizes continually grow smaller due to the improving semiconductor manufacturing processes. However, the smaller the feature sizes, the higher the variability of the manufactured transistors. This trend negatively affects an integrated circuit's power consumption, performance, fault sensitivity, etc. In addition, this process variability not only affects different chips, but also sub-components of large heterogeneous SoCs. The emulation-based design evaluation framework, which was introduced in this doctoral thesis, could be extended in order to take into account these crucial variability effects. This extension would permit variability-aware hardware and software evaluations, which will be highly important for future circuits built using deep-submicron manufacturing processes.

5.2.2 Hardware Accelerated Thermal Analysis for 3D-Integrated Chips

3D-integration is one of those technologies that will push the limits of integration density and performance capabilities of integrated circuits even further. However, heat management of future 3D-integrated chips is becoming a major problem. Traditional heat sinks are not able to efficiently remove the generated heat due mainly to physical reasons (e.g., small surface for heat dissipation, chip's material composition, limitation in temperature difference between the chip and the environment). Thus, an accurate understanding of the thermal behavior of 3D-integrated chips is a huge and important field of research. This includes, for instance, thermal modeling and thermal simulation of 3D-integrated chips in order to detect hazardous thermal hot spots. However, these models and simulations are complex and costly to calculate. If hardware accelerated analysis techniques are employed, these complex simulations (e.g., how to remove the heat from within the 3D-chip efficiently) will be solved many times faster and in a feasible way. As a consequence, the development of complex 3D-integrated chips will be accelerated and Moore's law would be kept alive for a longer period of time.

5.2.3 Prediction-based Power Management

Next generation SoCs and embedded systems will integrate more transistors in their design and will run at lower supply voltage levels compared to contemporary systems. As a consequence, supply voltage emergencies that are caused by high numbers of simultaneously switching transistors will occur more frequently. In addition, next generation energy harvesting-based embedded systems will face even worse supply voltage behaviors due to their constrained power supplies. Prediction-based methods that are based on power and supply voltage estimation techniques are promising candidates for future power management techniques to cope with these challenges. These prediction-based approaches may act (e.g., throttling the embedded system's CPU) before a hazardous peak power consumption or supply voltage drop occurs. Whereas, traditional power management techniques rely on analog components in order to measure these electrical parameters. As a consequence, they are only able to react with a certain delay after an emergency has been detected.

Chapter 6

Publications

This chapter presents the contributions provided by this doctoral thesis. The highlighted publications give detailed information concerning the methodology that is contributed and introduced by Chapter 3. In addition to Chapter 4, further case studies and evaluation results are depicted. Furthermore, the related work of each involved concept, which was summarized in Chapter 2, is analyzed thoroughly.

Publication 1: Druml et al., *Vulnerabilities of secure and reliable low-power embedded systems and their analysis methods - A comprehensive study*, Industry and Research Perspectives on Embedded System Design Book, IGI Global, 2014.
Publication 2: Druml et al., *Industrial applications of emulation techniques for the early evaluation of secure low-power embedded systems*, Industry and Research Perspectives on Embedded System Design Book, IGI Global, 2014.
Publication 3: Druml et al., *Emulation-Based Test and Verification of a Design's Functional, Performance, Power, and Supply Voltage Behavior*, 21st Euromicro International Conference on Parallel, Distributed, and Network-Based Processing (PDP), Belfast, Irland, February-March, 27th – 1th 2013.
Publication 4: Druml et al., *Emulation-Based Design Evaluation of Reader / Smart Card Systems*, 24th IEEE International Symposium on Rapid System Prototyping (RSP), Montreal, Canada, October, 3th – 4th 2013.
Publication 5: Druml et al., *Emulation-Based Fault Effect Analysis for Resource Constrained, Secure, and Dependable Systems*, 16th Euromicro Conference on Digital System Design (DSD), Santander, Spain, September, 4th – 6th 2013.
Publication 6: Druml et al., *Power and Thermal Fault Effect Exploration Framework for Reader / Smart Card Designs*, 16th Euromicro Conference on Digital System Design (DSD), Santander, Spain, September, 4th – 6th 2013.
Publication 7: Druml et al., *Estimation Based Power and Supply Voltage Management for Future RF-Powered Multi-Core Smart Cards*, Design, Automation & Test in Europe Conference & Exhibition (DATE), Dresden, Germany, March, 12th – 16th 2012.
Publication 8: Druml et al., *Adaptive Field Strength Scaling - A Power Optimization Technique for Contactless Reader / Smart Card Systems*, 15th Euromicro Conference on Digital System Design (DSD), Izmir, Turkey, September, 5th – 8th 2012.
Publication 9: Höller et al., *Hardware/Software Co-Design of Elliptic-Curve Cryptography for Resource-Constrained Applications*, 51th ACM / EDAC / IEEE Design Automation Conference (DAC), San Francisco, USA, June, 1th – 5th 2014.
Publication 10: Druml et al., *A Flexible and Lightweight ECC-Based Authentication Solution for Resource Constrained Systems*, 17th Euromicro Conference on Digital System Design (DSD)

(Under Review), Verona, Italy, August, 27th – 29th 2014.
Publication 11: Druml et al., *NIZE - A Near Field Communication Interface Enabling Zero Energy Standby for Everyday Electronic Devices*, 8th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Barcelona, Spain, October, 8th – 10th 2012.
Publication 12: Druml et al., *A secure zero-energy NFC solution for everyday electronic devices*, e & i Elektrotechnik und Informationstechnik, November, 2013.

Figure 3.1 gives an overview of the contributions provided by this doctoral thesis, which are divided into four phases. Publication 1, which is shown in Section 6.1, initiates this doctoral thesis. It outlines the vulnerabilities and analysis methods of secure and low-power embedded systems.

Section 6.2 introduces phase two and gives further introductions to the emulation-based

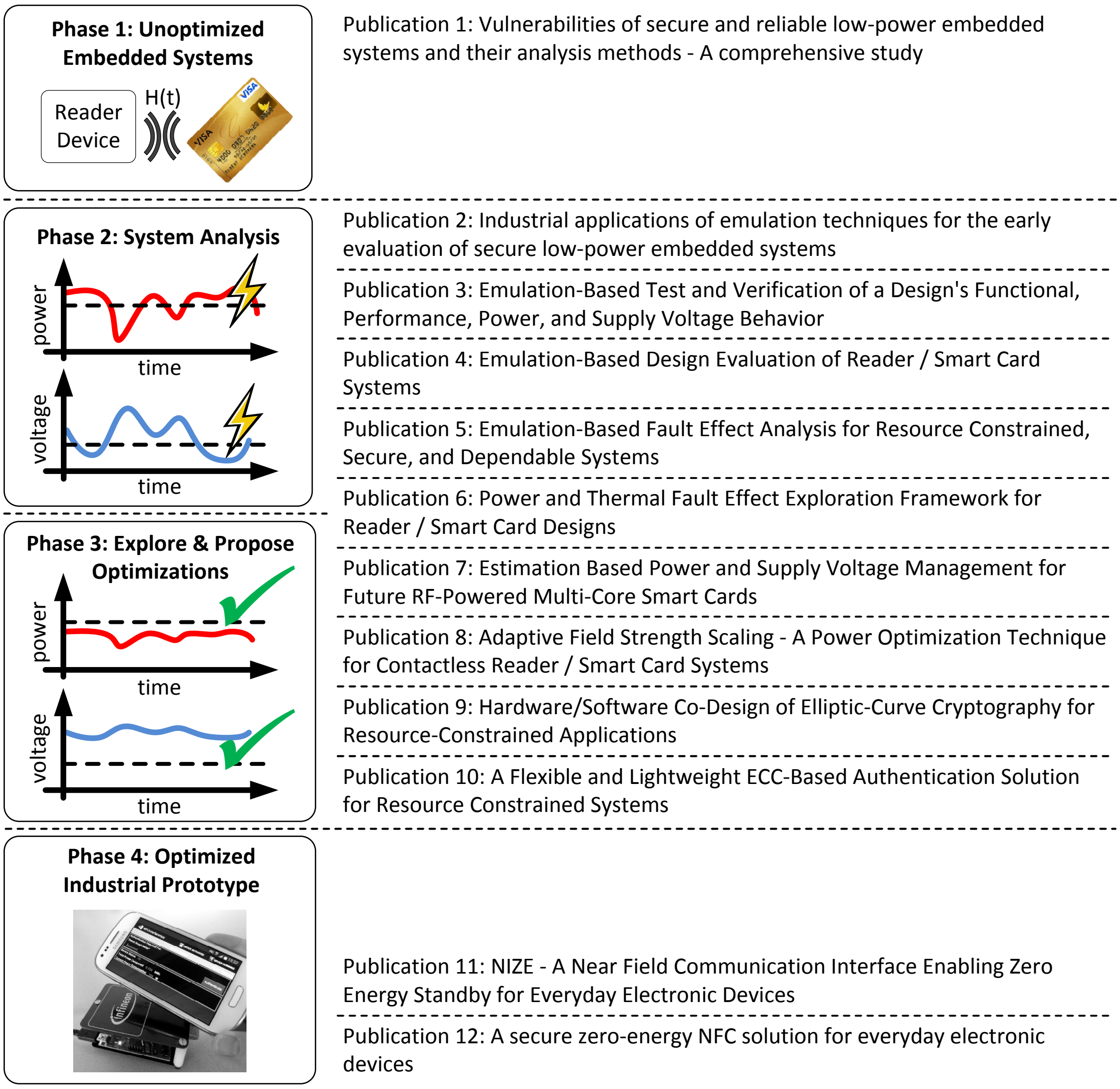

Phase 1: Unoptimized Embedded Systems
Reader Device
H(t)
Publication 1: Vulnerabilities of secure and reliable low-power embedded systems and their analysis methods - A comprehensive study
Phase 2: System Analysis
power
time
voltage
time
Publication 2: Industrial applications of emulation techniques for the early evaluation of secure low-power embedded systems
Publication 3: Emulation-Based Test and Verification of a Design's Functional, Performance, Power, and Supply Voltage Behavior
Publication 4: Emulation-Based Design Evaluation of Reader / Smart Card Systems
Publication 5: Emulation-Based Fault Effect Analysis for Resource Constrained, Secure, and Dependable Systems
Publication 6: Power and Thermal Fault Effect Exploration Framework for Reader / Smart Card Designs
Phase 3: Explore & Propose Optimizations
power
time
voltage
time
Publication 7: Estimation Based Power and Supply Voltage Management for Future RF-Powered Multi-Core Smart Cards
Publication 8: Adaptive Field Strength Scaling - A Power Optimization Technique for Contactless Reader / Smart Card Systems
Publication 9: Hardware/Software Co-Design of Elliptic-Curve Cryptography for Resource-Constrained Applications
Publication 10: A Flexible and Lightweight ECC-Based Authentication Solution for Resource Constrained Systems
Phase 4: Optimized Industrial Prototype
Publication 11: NIZE - A Near Field Communication Interface Enabling Zero Energy Standby for Everyday Electronic Devices
Publication 12: A secure zero-energy NFC solution for everyday electronic devices

Figure 6.1: Doctoral thesis' four phases of contributions and the corresponding publications.

analysis techniques (such as power emulation, supply voltage emulation, performance evaluation, security evaluations) and their uses in the field of industrial embedded systems. Section 6.3 introduces the comprehensive emulation-based design evaluation framework. This is followed by Section 6.4, which enhances the proposed design evaluation technique in order to take into account crucial system aspects related to complex embedded systems, such as reader / smart card systems. Section 6.5 extends this system-level design evaluation methodology with fault injection functionality, which particularly improves the analysis capabilities for secure and dependable embedded systems. The publication of Section 6.6 introduces a flexible high-level SystemC-based evaluation framework in order to cope with the lack of flexibility in emulation-based analysis methods. This high-level analysis approach enables fast but less accurate design analyses and focuses on contactless reader / smart card systems.

Based on these analysis techniques, Section 6.6 starts this doctoral thesis' phase three, which concerns the exploration of power and security optimization techniques in the field of contactless reader / smart card systems. Section 6.7 introduces an estimation-based power management technique for contactlessly powered smart cards. Section 6.8 explores and proposes a power optimization technique called Adaptive Field Strength Scaling, which takes into account the critical power constraints of contactless reader / smart card systems. In Section 6.9, hardware / software partitioning optimizations are evaluated in order to accelerate elliptic-curve-based computations. Protocol optimizations are demonstrated in Section 6.10 that permit a shifting of computational effort from the resource constrained embedded system to the reader which has more computation power.

This thesis' final phase presents in Section 6.11 and Section 6.12 an industrial prototype that introduces a secure zero-energy Near Field Communication Interface for everyday electronic devices.

Vulnerabilities of secure and reliable low-power embedded systems and their analysis methods – A comprehensive study

Norbert Druml, Manuel Menghin, Christian Steger
Graz University of Technology, Institute for Technical Informatics, Austria
Armin Krieg, Andreas Genser, Josef Haid, Holger Bock
Infineon Technologies Austria, Design Center Graz, Austria
and Johannes Grinschgl
Linz, 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 book chapter will present 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.

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).

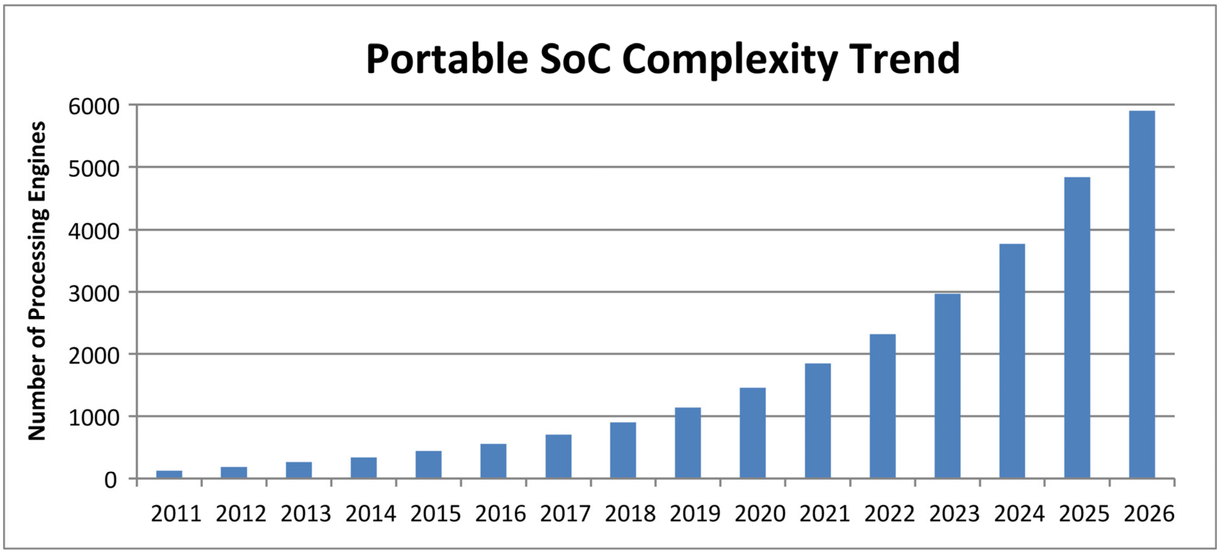


Figure 1: Design complexity trend of portable SoCs.

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.

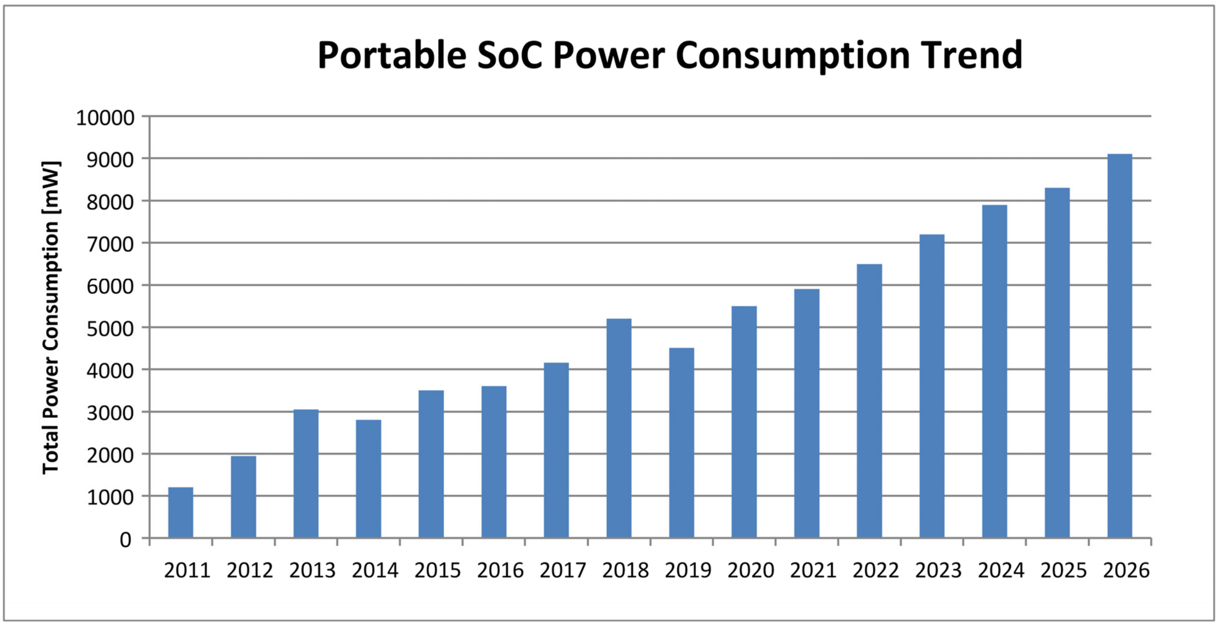


Figure 2: Power consumption trend of portable SoCs.

OBJECTIVES

Given all these complexity, power consumption, and security related issues, system engineers face difficult design challenges these days. Therefore, the objective of this chapter is to present an extensive study of recent challenges in designing low-power and secure embedded systems. Furthermore, this chapter will highlight state-of-the-art design evaluation methodologies used in the industry and will propose some industry-proven design recommendations used to cope with the outlined design challenges.

BACKGROUND

The background of this chapter outlines state-of-the-art methods in the fields of power analysis, supply voltage analysis, performance and benchmarking analysis, as well as fault resistance analysis. With the help of these methods, an embedded system's vulnerabilities in these mentioned fields can be identified. Based on this knowledge, design optimization techniques can be proposed to counteract these vulnerabilities.

Power Analysis

With the advent of low-power digital design techniques, power profiling has emerged as a standard method in order to evaluate their effectiveness. Power profiling can be performed in manifold ways that can be subdivided in two main categories, (i) measurement-based and (ii) estimation-based methods.

If prototypes are available, measurement-based methods benefit from taking actual physical measurements, which results in high accuracy compared to all other methods. However, additional measurement equipment is required.

Estimation-based power profiling makes expensive measurement equipment obsolete by modeling the power consumption of embedded systems, even before sample implementations of the embedded system are available. Power modeling is usually less accurate compared to pure measurements and requires more computational effort. However, it provides more flexibility, since power modeling can be carried out on multiple layers of abstraction.

Measurement-based methods

In Flinn (1999), PowerScope gives an energy profiling tool for mobile applications. A run-time measurement is automatically carried out by a digital multimeter. Measurement data is transferred to a host computer to be processed for further analysis.

Texas Instruments has proposed another measurement power profiling technique (Texas Instruments, 2002). They developed a proprietary visualization in order to display current measurement data in their software development environment.

Estimation-based methods

Estimation-based methods for power analysis can be carried out on multiple levels of abstraction influencing estimation accuracy. Furthermore, the level of abstraction impacts on computational effort. In the following, an overview on academic and industrial research contributions is given tackling challenges accompanying the diverse field of power estimation.

Power estimation started with simulation-based methods by executing algorithms in simulators in order to acquire power information by evaluating power models integrated into these simulators. In recent years, an increasing number of hardware-accelerated methods have emerged that diminish a major drawback of estimation-based methods: their increased run-time compared to measurement approaches. Power models are integrated into hardware, which can yield power profiling speedups of multiple factors compared to purely simulation-based approaches. Real-time power profiling is limited to hardware-accelerated approaches.

Industry state-of-the-art power estimation tools operate on a low level of abstraction, e.g., gate- or register transfer level (RTL) (Flynn et al., 2005). This requires extensive computational effort, which is the reason that these simulations are most often performed on server farms. Estimation accuracies are comparably high, however the extensive run-times limit this approach to organizations that can afford to provide this high degree of computational power. Hence, raising the level of abstraction by compromising the estimation accuracy has been a recent way in order to relieve this burden and provide power estimation tools to embedded software developers as well.

Tiwari et al. (1994) proposed a simulation-based power estimation method on instruction-level. The implemented power model considers base costs and circuit state overhead costs, which translates to the power consumption during instruction execution and the power consumption during the transition of two consecutive instructions, respectively. Additional micro-architectural effects, in order to improve the instruction-level power model, are considered by Sami et al. (2002). The authors extended the power model by means of pipeline awareness for Very-Long-Instruction-Word (VLIW) architectures. Lajolo et al. (2002) introduced a co-simulation approach for power estimation for System-on-Chips (SoCs). The power estimation is performed on system-level. If higher accuracy is required, various system components can be simulated on a lower-abstraction level. Another SoC power estimation approach is proposed by Lee et al. (2006). Power models are implemented for the processor, memories, and custom IP blocks. The simulator provides power values cycle-accurately in a dedicated power profile viewer.

Hardware-accelerated power estimation migrates power models from software to hardware. These power models map states of hardware blocks (CPU idle/active, memory read/write, etc.) to dedicated power values, which have been determined during a power characterization process.

Bellosa (2000) implemented hardware event counters in order to derive thread-specific energy information from operating systems. According to Joseph et al. (2001) the system's power consumption is derived by exploiting performance counters of a microcontroller. A coprocessor dedicated for power estimation has been proposed by Haid et al. (2003). The central controller tracks energy sensors deployed in the system. It requires extra hardware but also speeds up power estimation compared to simulation-based methods.

Finally, power emulation has emerged as an alternative approach for hardware-accelerated power estimation. A system equipped with power estimation hardware is deployed on an FPGA-platform. These platforms can then be used to carry out not only functional verification but also real-time power estimations.

The power emulation principle has first been proposed by Coburn et al. (2005) claiming run-time improvements of about 10x to 500x compared to commercial state-of-the-art power estimation tools. Moreover they proposed hardware overhead reduction techniques. Ghodrat et al. (2007) extended this approach to a hybrid power estimation methodology for complex SoCs by combining simulation and emulation techniques. This reduces power profiling times by a large amount. Power emulation in order to guide process migration between different cores has been proposed by Bhattacharjee et al. (2008).

Supply voltage issues, analyses, and countermeasures

The fact that embedded systems grow in complexity means that the number of simultaneously switching transistors during operation grows as well. At the same time, the operational voltage level of high-end integrated circuits decreases. As a consequence, such high-end integrated circuits provoke significant electrical current changes during a relatively small amount of time. This situation introduces several problems for power supply networks and the integrated circuit itself:

A. Using a low supply voltage reduces the noise margin. Thus, the integrated circuit's vulnerability against voltage drops increases and, e.g., the following hazardous affects may arise: false triggering logic, missing clocked pulses, or double clocking.

B. Power supply networks come with significant parasitic inductances, due to wires, pins, etc. Electrical current changes across an inductance cause voltage variations, according to (1), as demonstrated by Grochowski et al. (2002). If these voltage variations exceed a certain limit, the electronics may malfunction. This issue is referred to as the di/dt problem.

$$V = L \cdot \frac{di}{dt} \tag{1}$$

C. Voltage variations are caused within power and ground busses if a high electrical current flows between these busses. According to Bai et al. (2001), the gate delay and thus the critical path are affected by these voltage variations. This is a problem especially for integrated circuits that are operated at high clock frequencies.
D. Energy harvesting embedded systems (e.g., contactlessly powered smart cards) obtain their electrical energy from the environment. Since this very limited available electrical energy is buffered within capacitors, sharp electrical current changes of the electronics may cause hazardous supply voltage drops.

Supply voltage issues can be coped with either during design-time or during run-time. For example, by using semi-asynchronous architectures or by adding decoupling capacitors, supply voltage hazards can be reduced during design-time. A simulation approach was presented by Grochowski et al. (2002). Based on a current simulator and a detailed power supply network model, the supply voltage behavior is estimated. A feedback loop is then used to control the supply voltage by means of activating/deactivating processor components and deactivating the clock. The presented approach was also tested on a processor die. Only little performance and power degradation was introduced. Hardware emulation solutions were proposed by Genser et al. (2011) and Druml et al. (2013). The design-under-test, which was integrated into an FPGA prototyping board, was augmented with model-based power and supply voltage analysis units. Thus, supply voltage estimates were gathered in real-time and for each clock cycle.

During run-time, hazardous supply voltage drops can be measured with on-die circuits as Holtz et al. (2008) demonstrated. By injecting electrical current into selected nodes, supply voltage drops can be reduced. Analog-to-digital converters and voltage comparators represent further sensing approaches. However, the sensor delay is a drawback that limits their efficiency. Grochowski et al. (2002) proposed shift registers to delay clock gated processor components. As a result, the number of simultaneously switching transistors was reduced and a reduction of voltage alterations was achieved. A predictive approach was presented by Reddi et al. (2009). First, signatures (program path sequences and micro architectural events such as cache misses, etc.) of programs which provoked hazardous voltage drops were collected. During runtime, if the currently executed program's signature matched an emergency signature, the processor was throttled. This approach detected 90% of the tested emergency situations but introduced a high amount of overhead. An estimation-based technique to reduce supply voltage drops was presented by Druml et al. (2012). The authors enhanced the design of a contactlessly powered smart card with model-based analysis units at low hardware overhead costs. If a supply voltage hazard was detected, the smart card's processor was throttled.

Performance analysis and benchmark characterization

In order to carry out performance measurements and activity analyses, hardware performance counters (HPCs) are commonly used in modern processor systems and embedded systems. Typically, an HPC consists of a counter and dedicated trigger logic, which monitors the hardware component or circuitry of interest. This approach enables the analysis of low-level processor events (e.g., cache misses, pipeline stalls) without the need for time-consuming simulations at RTL level. Sweeney et al. (2004) demonstrate the importance of providing software developers with low-level activity and performance information by means of the Java virtual machine. With the help of such analysis data, software/hardware issues can be found which violate real-time constraints or worst-case execution time requirements. In addition, software-based performance optimization can be explored. HPCs are also used in computing centers, as outlined by the Ganesan et al (2008). They measured the workload of IBM's Blue Gene supercomputer. Based on such workload analysis data, software developers can then optimize the workload distribution to increase the overall computing performance. Apart from pure performance analyses, HPCs are also used to estimate the momentary power consumption of embedded systems with the help of power models, as presented for example by Bhattacharjee et al. (2008).

The generation of well-balanced power models and accurate fault models is based on the characterization of the system using benchmark applications. Generic benchmark applications are used for the performance evaluation of high-level system properties and hence, are usually done at a very high software level, where system calls, instructions, and runtimes are evaluated. First basic rules for the task of benchmark characterization have been described by Conte et al. (1991). In this work, several benchmarks and the corresponding evaluation results are shown for different cache configurations and physical memory sizes. Micro-architecture dependent and independent characteristics are described in the work introduced by John et al. (1998). Further investigations specializing in the temporal and spatial locality properties of selected applications have been presented. Still, small embedded systems were not well covered in literature concerning workload characterization. Therefore, Guthaus et al. (2001) introduced the MiBench suite directly targeting such implementations. The characterization methodology is still the same as used in applications used for larger scale systems. For the sake of completeness we would also like to mention the new EEMBC benchmark suite introduced by Poovey et al. (2009), which has also been characterized for memory activity, parallelism, and branch efficiency.

Concerning fault and power modeling there is therefore still significant work needed to lay a foundation for the generation of accurate models.

Fault Injection for the evaluation of reliable and secure systems

Systems operated in very harsh environments, such as radioactive or space flight applications, are prone to suffer from reliability issues caused by operational faults. These problems lead to the publication of a wide range of works concerning test techniques using fault injection techniques. The system level on which such fault injection runs are applied can be varied depending on the evaluation target. Depending on this abstraction level different injection methods are needed, e.g., completely manufactured devices can be attacked using radiation. Early stage testing during the design phase can be realized using manipulation of the hardware description.

Simulation techniques for high-level hardware descriptions can be applied at very early stages when only very rough models exist. This advantage can also be exploited for the implementation of fault injection using standardized simulation tools.

MEFISTO was a first attempt to implement a fault-aware simulation methodology for VHDL models, cf. Jenn et al. (1998). To integrate saboteur and mutant models into such a simulation-based setup, the principle has been enhanced using automatized insertion strategies in the VFIT tool (Baraza et al., 2005). In addition to improvements of the injection simulation performance, emulation approaches have been shown in the work of Valderas et al. (2007).

While simulation certainly provides a high grade of flexibility, the need for higher fault injection coverage made it necessary to increase research activity on hardware-accelerated emulation methodologies. The expected significantly higher injection rates of such implementations have been shown (Leveugle et al., 2000). Emulation promises and also enables the possibility to evaluate more possible fault configurations than using simulation. The introduction of novel partial reconfiguration capabilities of certain new FPGAs allowed fault injection without modification of the system hardware description, as described by Antoni et al. (2003). Performance and practicality of this approach have been continuously improved in many following publications, such as the works by Zheng et al. (2008) and Daveau et al. (2009). While previous techniques mostly relied on the emulation of RTL-level descriptions, the work presented by Guzman-Miranda et al. (2009) showed how the import of netlists into an FPGA-based evaluation platform can be done. Furthermore, proximity information is used for correct and fast Multi-Bit Upset (MBU) robustness investigations.

Up to this point, the main reason behind these works has been reliability evaluations using random fault patterns. If this random fault model is replaced by the model of an adversary that intentionally injects faults into a system, (security) evaluations result in more complex fault scenarios. This is first caused by the possibility that such an attacker injects multiple faults at once. Such an MBU scenario now has to be considered for modern deep sub-micron process technologies as well. Hence, Leveugle et al. (2007) suggested considering multiple fault models. Contrary to dependability testing, such security investigations also have to handle cases where an adversary knows where to place faults to gain best results; the worst case is the most likely one.

In the automotive industries domain, hardware-accelerated emulation-based system fault testing is already widely accepted (Abke et al., 1998). Gate-level fault emulation is often the first choice, which has the advantage of being very accurate but on the other hand can only be applied at a late stage which could be unwanted for early software evaluations. Especially for automotive communication systems the work presented by

Corno et al. (2004) and Armengaud et al. (2008) introduced systematic high-level methodologies. A parallelized approach, as presented by Daveau et al. (2009), can help to increase emulation capacity and performance, but still the authors of this work only considered random fault distributions and single hardware modules. Hence, a bridge between low-level hardware and higher level system verification needs to be created to avoid possible evaluation gaps.

Therefore, the introduction of hybrid platforms combining the advantage of state-of-the-art verification systems (Baronti et al., 2011), multi-level testing environments (Entrena et al., 2012), and deep low-level emulation methodologies (Myaing et al., 2011), is needed. If information leakage is an evaluator's primary concern, our work presented by Krieg et al. (2011a) highlighted the importance of using accelerated evaluation techniques for software security verification.

SENSITIVITY OF LOW-POWER EMBEDDED SYSTEMS

Secure and reliable low-power embedded systems face important sensitivity issues that a system designer must be aware of, e.g., peak power consumption and consequently supply voltage drops, as well as fault induced security and reliability interferences. This section highlights these sensitivity issues and outlines commonly used techniques used in industry to deal with these issues.

Sensitivity to power and supply voltage

The adequate availability of supply voltage and power is a major requirement to ensure reliable embedded systems operation. However, sharp changes of an embedded system's electrical current consumption caused, for example, by a high number of simultaneously switching transistors, may provoke hazardous supply voltage drops. If the supply voltage drops below a certain threshold, the hardware's operational stability is compromised. As a consequence, the analysis of the hardware's power consumption and supply voltage behavior are of high importance, especially in the field of resource constrained embedded systems.

As a well-known example for low-power embedded systems, this section highlights the power and supply voltage vulnerabilities of an industrial smart card. Applications for smart cards have increased drastically during the last years. Applications can be found in our everyday life, for example, in the fields of payment, loyalty and coupons, transportation, healthcare, logistics, and access control. However, a secure, RF-powered, contactless smart card is very constrained in terms of power supply and computational resources: power is transferred from a reader device to the smart card by means of a time-varying magnetic field. The induced electrical voltage is rectified and electrical energy is then buffered within a capacitor. A shunt resistor protects the smart card's electronics from power surges and reduces security-related side channel footprints. Data is transferred by means of Amplitude Shift Keying (from reader to smart card) and load modulation (from smart card to reader). Because of the smart card's low power budget, it may face hazardous supply voltage drops and power starvation periods, e.g., due to the following reasons. For example, variations in the magnetic field's strength or changes of the smart card's orientation within the magnetic field can cause a loss in harvestable electrical power. As a consequence, the smart card's internal capacitor discharges and the voltage which is supplied to the electronics drops accordingly. Another example of supply voltage emergency is depicted in Figure 3. The smart card performs a certain benchmark application. During the processor's peak power consumption, more electrical power is consumed than electrical power can be harvested from the magnetic field. As a consequence, the smart card's capacitor discharges and the electronics' supply voltage drops hazardously below a level of 1 V. If a certain threshold is crossed, then the operational stability is lost.

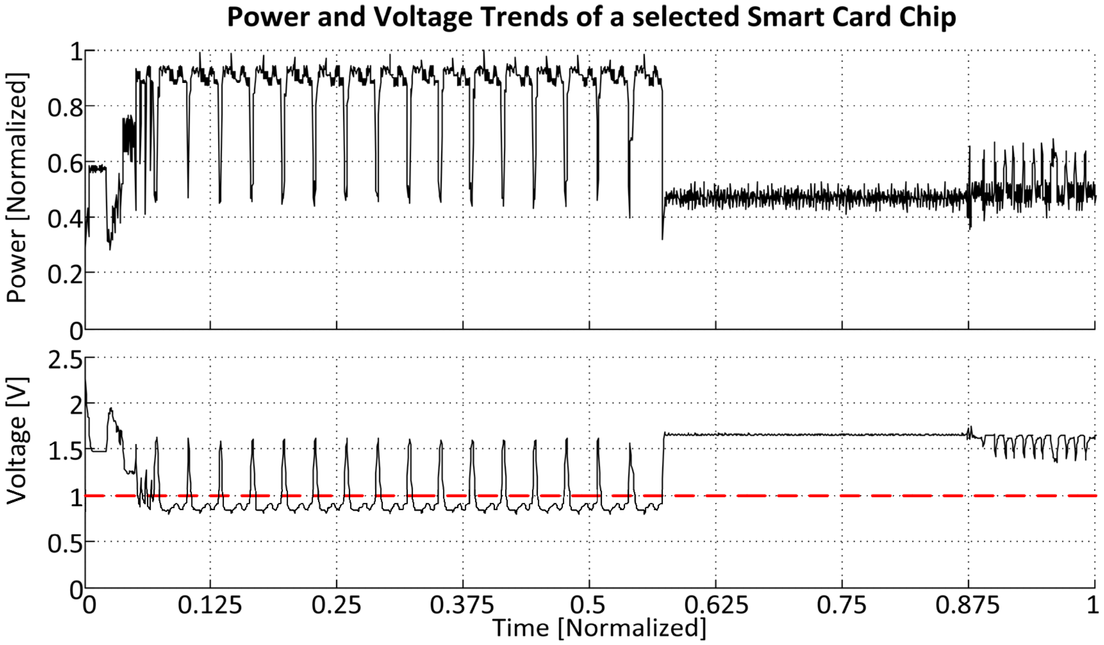
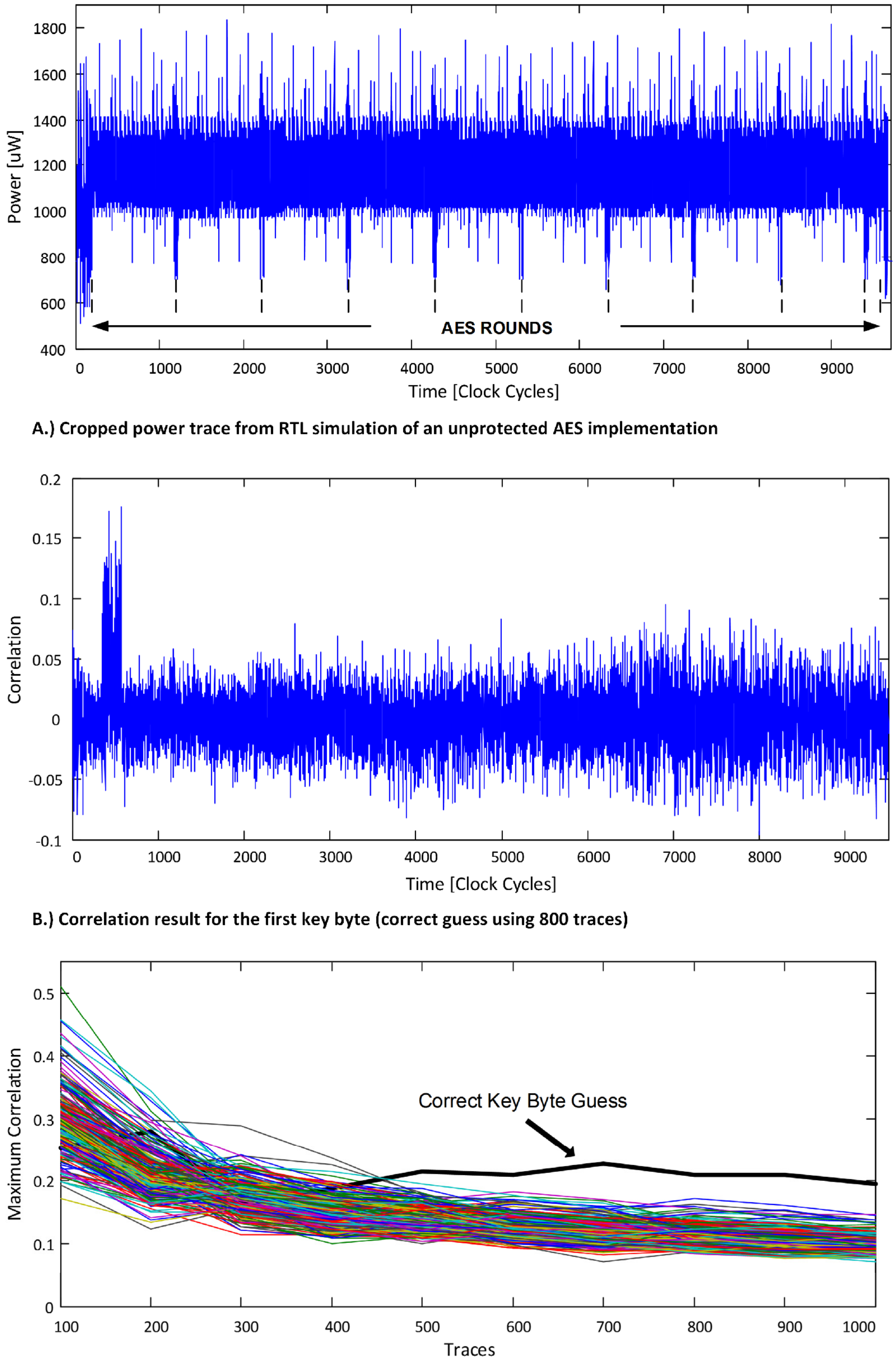


Figure 3: Supply voltage emergencies during peak power consumption.

Besides operational stability concerns, an embedded system's data dependent power consumption analysis is of high interest for security-related side channel evaluations, such as Simple Power Analysis (SPA) or Differential Power Analysis (DPA) methodologies. SPA and DPA techniques can be used, e.g., to extract internal secrets from an embedded system's power profile while performing cryptographic operations. In addition, significant changes of the embedded system's power consumption may reveal security relevant countermeasures (e.g., security traps or hardware resets) against intentionally provoked hardware faults. Thus, an attacker may detect when security critical code is executed. Figure 4 illustrates an example of applying the DPA technique on an embedded system's power profile while the embedded system performs cryptographic operations. As highlighted by the figure, DPA can successfully extract the embedded system's secret key, if the system is not properly protected. This example demonstrates the worst possible scenario for a supposed 'secure' embedded system, because internal secrets, like cryptographic keys, must not be disclosed.



A.) Cropped power trace from RTL simulation of an unprotected AES implementation

B.) Correlation result for the first key byte (correct guess using 800 traces)

C.) Maximum correlation for the first key byte over the amount of used traces

Figure 4: DPA-based key extraction from power profiles

Recommendation – Power analysis and power management techniques

Given the described power and supply voltage vulnerability of low-power and secure embedded systems, several improvements and solutions have been developed in recent years. Here we outline the most important and most commonly used industry-proven techniques.

Dynamic power management

Dynamic power management encompasses techniques to adapt a system's power consumption during runtime. Dynamic power management methods often use an observer / controller approach, as summarized by Benini et al. (2000). The observer monitors the system's performance, load of computation, power consumption, etc. Based on this information, certain system parameters are manipulated by the controller with the help of a dedicated control algorithm. Various control techniques are used in state-of-the-art embedded systems. A very well-known way to control an embedded system's power consumption is the dynamic scaling of its voltage or frequency parameters (DVFS). According to (2), voltage and frequency alterations have a cubic impact on the power consumption of a CMOS-based system. However, voltage and frequency cannot be assigned arbitrary values. There are certain constraints that need to be considered when designing a system featuring the DVFS technique (e.g., when setting a certain frequency value, a minimum voltage level is required to operate the circuitry properly).

$$P_{CMOS}(t) \approx V^2(t) \cdot f(t) \tag{2}$$

In the past, a lot of observer techniques have been proposed and implemented. A common technique is the modeling and definition of system power states. For example, an embedded system's idle state may define minimized computational activities. If the system enters this state, unused system components (e.g., coprocessors, peripherals) may be reduced in their clock speed or switched off completely. Another commonly implemented observer approach is the usage of fast analog comparators. If the comparator detects a power or supply voltage emergency, the system's clock is throttled or paused completely until the emergency is resolved.

Offline power analysis techniques

Besides online power management techniques, offline analysis methodologies are commonly also used. Such simulation-based and emulation-based techniques can be used early during a product's development cycle. They are able to estimate power consumption profiles based on the executed source code and power models. Then, analyses can be carried out to detect source code regions which provoke power or supply voltage hazards. If such critical source code regions are detected, engineers can then resolve these issues using the following techniques given as example: by modifying the source code or by throttling the processor core while being in this critical code region. As an example of application, Figure 5 illustrates an emulation-based power estimation approach, according to Genser et al. (2009) with extensions. Power models are used to estimate the embedded system's state dependent (SD) and data dependent (DD) power consumption hardware accelerated while performing a benchmark application. Estimation errors of less than 9% can be achieved. Emulation-based supply voltage analysis techniques, as presented for example by Druml et al. (2012), achieve estimation errors of approximately 2%.

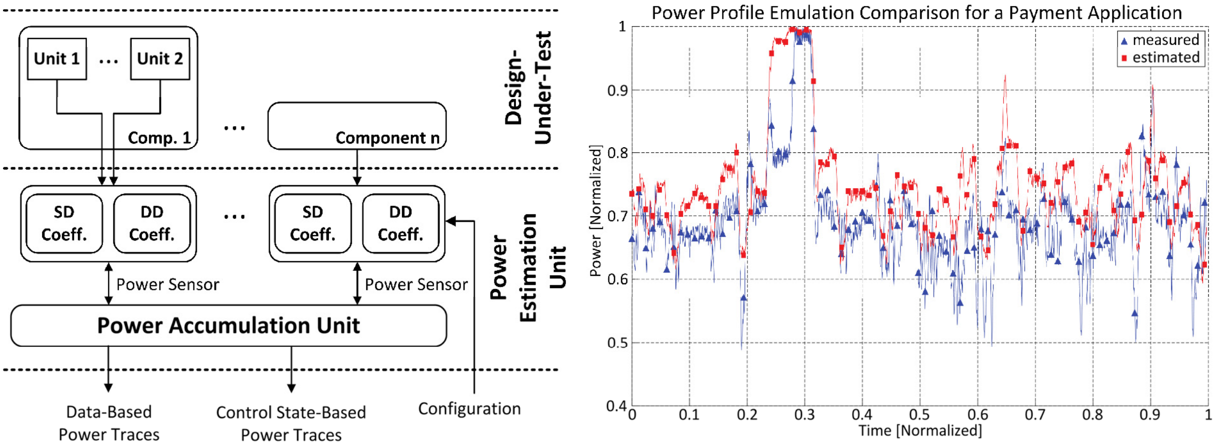


Figure 5: Model-based power estimation technique used for offline analyses.

Side channel information suppression

It is of high importance for a secure embedded device to prevent internal secrets to be leaked to adversaries through side channels, such as the power consumption profile. This field of research is moving at a high pace because novel attack methods and corresponding countermeasures are being constantly developed.

A commonly used method of hiding an embedded system's data dependent power profile works as follows. The embedded system adds a variable amount of power consumption to its original changing power consumption to achieve permanently constant total power consumption. This approach makes it complicated for an adversary to extract data dependent side channel information. However, as a drawback, the total embedded system's power consumption increases.

Another commonly used and easy to implement side channel suppression method was demonstrated by Krieg et al. (2011b). The power profile is randomly scrambled with the help of available on-chip units. For example, during security critical calculations cache flushes are randomly provoked or unused processor units are activated or deactivated. As a consequence, an adversary requires a lot more effort to extract internal secrets. This side channel suppression method requires no additional hardware components, but as a drawback the embedded system's performance may be reduced.

Sensitivity to fault attacks and semiconductor reliability issues

The continuous increase in semiconductor implementation density has been strongly driven by the shrinkage of technology nodes to a level where isolation thickness decreases to few atomic layers. With the exception of leakage power (which is significantly worsened if manufacturing techniques such as Silicon-on-Insulator (SOI) are not used), small transistor sizes have a positive effect on power consumption. On the other hand, available chip integration space, thinner isolation, and shorter transistor channels introduce problematic reliability issues. Novel problems also include accelerated device aging and process variability that impact operation stability of modern processing systems. The significance of the latter is visualized in Figure 6 showing fault probabilities based on data from the latest ITRS report (ITRS Working Group, 2012, ITRS).

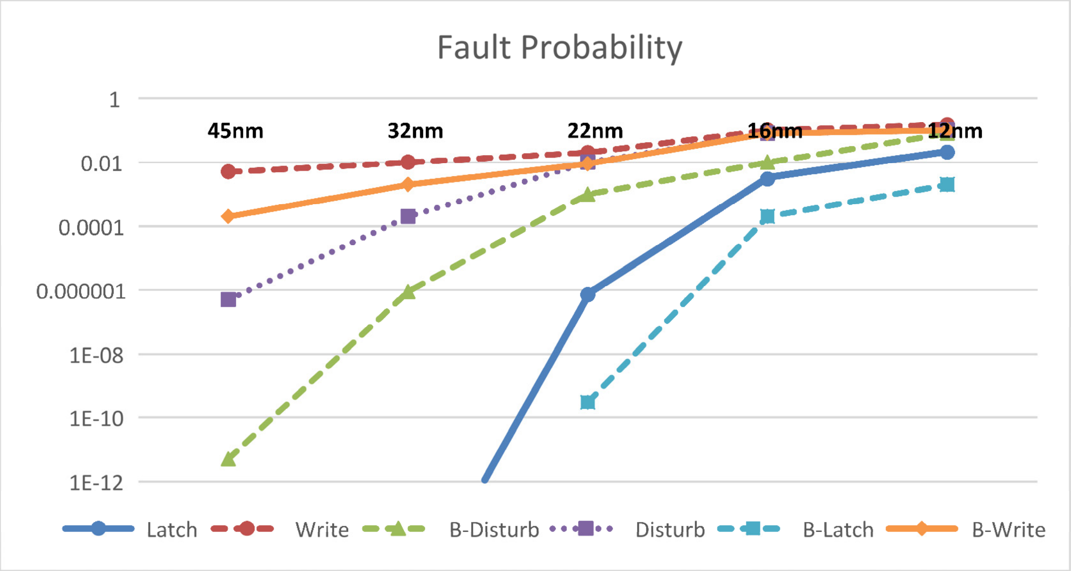


Figure 6: Fault probabilities for deep sub-micron technologies

A wide variety of research concerning fault detection, recovery, and fault-robust devices has been triggered by this development. In high-reliability, security, and safety implementations system-level duplication, such as triple-module-redundancy, is still the preferred choice. In low-cost embedded systems though, the additional hardware effort cannot be spent, hence, novel strategies for such system-level techniques that do not rely on duplication are strongly needed.

Processes, as described above, are of a random nature, unlike faults resulting from fault attack scenarios. This results from the fact that an attacker deliberately injects faults into a system to change the system behavior while having knowledge where an attack is the most efficient. Therefore, significant precautions have to be taken as such attacks can be easily applied because of the huge number of external parameters an attacker has access to. As introduced earlier, intensive research has provided a wide variety of different tools to simulate or emulate fault scenarios during early design phases. Particularly, the influence of fault sources on the design can be evaluated using fault emulation in a very efficient way. Especially the tremendously increasing capacity of modern FPGAs provides the flexibility that is needed to make FPGA-based investigation platforms a reasonable alternative to simulation-based approaches.

Until recently, system emulation came with the disadvantage of not being able to allow the concurrent investigation of the power consumption side-channel while performing fault injections. As shown in Figure 7, this side-channel can give information to an adversary if the attack had a successful effect on the system or not. As described beforehand, the introduction of power emulation made the concurrent evaluation of the attack and its side-channel finally possible.

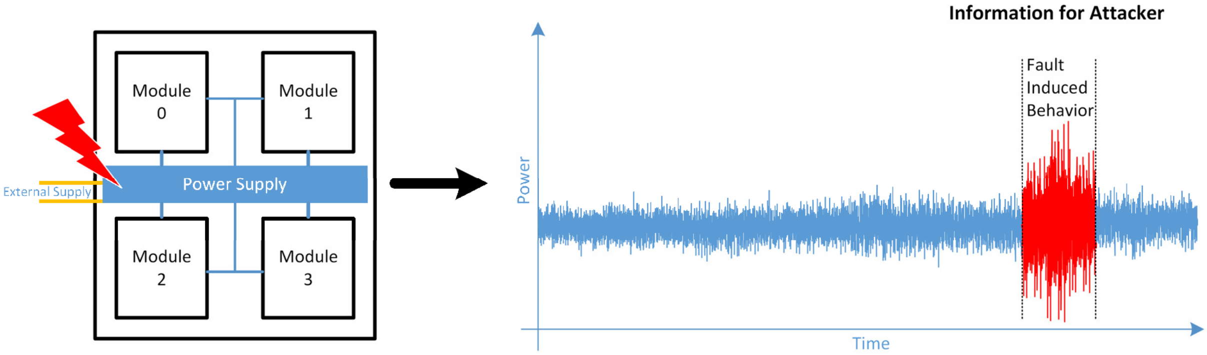


Figure 7: Power consumption side-channel during fault attacks

Modern reliability or fault attack evaluations call for a multi-bit fault model resulting in significantly more complex fault interdependencies than in SEU models. In the case of attacks, the time frame and location space of such faults is even larger as these have to be considered as being of a non-random nature. Thus, in dependability evaluations, similar types of sensitive sub-circuits will much likely fail at the same time. In security analyses, this dependency is defined by the attack scheme of the adversary.

Recommendation – System-level fault detection and recovery

Under the assumption that faults can threaten system integrity at any point of time, the detection of operational faults during the execution of critical software sequences is urgent. Hence, this topic has been a very active field of research for many decades. For this work, we will mainly consider signature-based approaches to detect and manage faults on three different abstraction levels: only the software-level using software-based signature mechanisms, on the hardware-level using hardware-based signature mechanisms, and complete hardware-software co-design solutions.

Software-Based Signature Mechanisms

The automatic or semi-automatic generation of source-code signatures is the technique of choice if signature checking is to be done on the software-level. Based on these signatures, changes in the program control flow, resulting from tampering or environmental influences, can be detected. While directly embedding them into the executed binaries allows the checking procedure itself to be done using processor internal resources, this could detrimentally influence the program run-time.

The application of extensive redundancy was the first choice to achieve software fault detection and recovery. Additionally, control flow checking can be applied to recognize unforeseen execution behavior. By generating these signatures during compile time, no hardware needs to be involved in any stage of the generation process. On the other hand, software-only approaches have the significant disadvantage of influencing the execution performance (up to 40 - 600% performance and memory overhead). From a security perspective such software checks have also to be considered as an additional risk in security critical systems, as they could be manipulated by an adversary.

Hardware-Based Signature Mechanisms

Historically, integrity checking of hardware blocks has been commonly solved by the integration of hardware monitors. The applicability of this approach depends highly on the way in which pre-computed signatures are stored while the hardware implementation can be done in highly efficient way. On the other hand when large memories are needed for storage, this is often not affordable in low-cost designs. Also, the current state-of-the-art does not sufficiently cover the selection of the monitored system region. The heterogeneous nature of modern System-on-Chip designs calls for approaches that cover more than only a processor's pipeline. If hardware monitors are to be used in such configurations, system complexity could be dramatically increased, decreasing area efficiency.

Another point that has to be considered concerning monitoring hardware blocks is the impact of the monitoring process on the execution performance. In order to significantly reduce it, direct access to hardware resources needs to be granted. Therefore, dedicated monitoring hardware has been introduced to enable control flow-monitoring implementations. Initially watchdog-type modules have been used for dedicated monitoring purposes. The integration of specialized monitoring circuits has been described by Mao et al. (2010) and Lukovic et al. (2010) specifically targeting sensitive parts of the system.

Contrary to techniques that rely on an external view of the supervised elements, on-line control flow evaluation methods make use of the modification of a processor's pipeline. Such techniques are very effective when evaluating applications that mostly rely on a central processor, but again, lack proper applicability for heterogeneous System-on-Chip implementations. These could be System-on-Chips that include various different processing units like coprocessors or dedicated DSPs.

Hardware/Software Co-Design Solutions

Wide fault detection coverage in recent years has resulted in various hardware/software co-design based methodologies. These techniques make use of the possibility to adapt both software and hardware layers to solve the detection coverage problem with low memory overhead and performance degradation. Application-specific instruction-set processors (ASIP) are by design optimal for the direct integration of fault detection functionality, as introduced by several publications such as Patel et al. (2011). For other than in ASIP-based architectures such methodologies can only be used in cases of highly adaptable target architectures or when strong interventions in existing development flows are allowed because of an early stage in the design process.

An alternative, if these changes in the design flow cannot be applied, is the generation of representative signature values to enable tracking of control changes. There are various different possible sources for these values, for example the test infrastructure such as scan-out-chains. Unfortunately, the on-line testing property is only partially applicable in case of test reuse, because periodic tests influence the operational performance (although the hardware area overhead is quite low). If the architectural state needs to be directly analyzed, fingerprinting techniques based on system hash-values can be applied. The high frequency of the changing hash-values in high performance systems leads to high demands on circuit bandwidth that cannot always be provided. Large chip multi-processors require additional improvements and extensions to this technique such as those introduced by Khan et al. (2011).

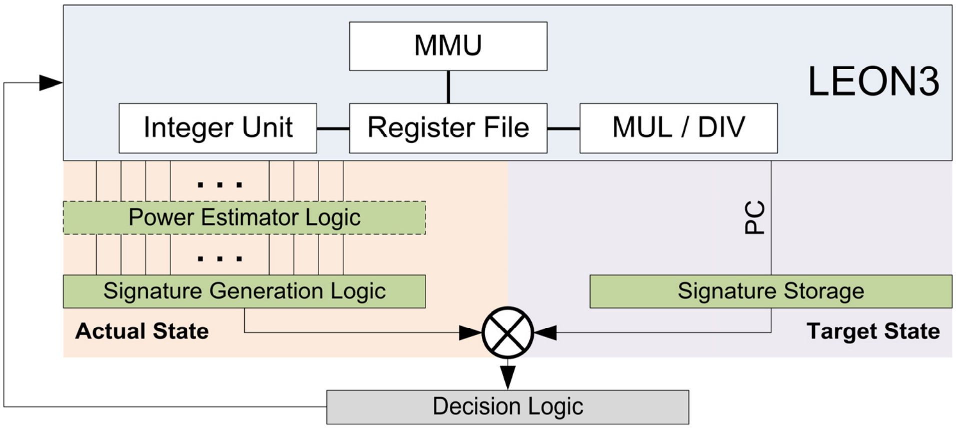


Figure 8: Power estimator-based fault detection

We have shown (Krieg et al., 2012) that emulation-based power estimation infrastructure can also be used as a source for the on-line generation of operation signatures. These signatures can then be checked during operation in order to detect execution variations that could have been a result of an attack or a reliability issue. Such architecture is depicted in Figure 8, but different implementations are possible depending on the target system.

FUTURE RESEARCH DIRECTIONS

Variability analysis

As shown in Figure 6 and described in previous sections the fault sensitivity of circuits increases tremendously with the reduction of the semiconductor feature size. A novel problem that has been identified in state-of-the-art System-on-Chips is strong process variations not only between different chips, but inside large heterogeneous SoCs. A very good overview is given by Gupta et al. (2013) over the many problems resulting from this issue.

As the evaluation of System-on-Chip implementations as well as the corresponding software is of highest priority, first steps to conquer this problem have been taken in recent years. Kozhikkottu et al. (2011) introduced a novel methodology to enable the evaluation of variability effects on an FPGA-based evaluation platform.

Thermal analysis management for 3D-integration

The limits of 2D-silicon integration density are about to be reached. 3D-integration is one of those technologies which enables a further density and performance increase. However, 3D-integration introduces major challenges in handling the generated heat, because computational elements are stacked above each other. The heat density increases, but standard heat sinks are insufficient to remove the generated heat; cf. Coskun et al. (2009).

A very important future research field is the thermal understanding of 3D-integrated circuits. This includes, for example, thermal modeling and thermal simulation of 3D-integrated chips while running dedicated benchmark applications to detect hazardous thermal hot spots. With the help of this analysis data, novel heat sink techniques (e.g., integration of mini heat pipes within the package) are about to be integrated. Furthermore, novel task distribution and power management algorithms are required to regard the 3rd dimension and to reduce these hazardous thermal hot spots. If these methods are applied properly, the circuit's reliability and lifetime can be significantly increased.

CONCLUSION

The integration capability of the semiconductor industry has increased tremendously during the last years. Thanks to these improvements, the supported features of recent embedded systems have increased exponentially. However, this increase in complexity introduces problems that a system engineer needs to be aware of: a high amount of simultaneously switching transistors causes abruptly changing electric currents; deep sub-micron silicon integration technology is prone to random faults that need to be coped with during runtime, etc.

In this chapter, we presented a comprehensive study of issues that engineers face when developing embedded systems. We described design analysis methodologies that were presented in recent years, and we outlined state-of-the-art techniques from industry to cope with the presented issues. These topics were discussed with a focus on reliable and secure low-power embedded systems, which play an important role in our more and more mobile environment.

ACKNOWLEDGEMENTS

The authors would like to thank the Austrian Federal Ministry for Transport, Innovation, and Technology, which funded the POWERHOUSE, POWER-MODES, and META[:SEC:] projects under the corresponding FIT-IT contracts FFG 815193, 825749, and 829586.

REFERENCES

Journal articles:

Antoni, L., Leveugle, R., & Fehér, B. (2003, October). Using run-time reconfiguration for fault injection applications. *Instrumentation and Measurement, IEEE Transactions on*, *52*(5), 1468-1473.

Armengaud, E., Steininger, A., & Horauer, M. (2008, August). Towards a systematic test for embedded automotive communication systems. *Industrial Informatics, IEEE Transactions on*, *4*(3), 146-155.

Baronti, F., Petri, E., Saponara, S., Fanucci, L., Roncella, R., Saletti, R., D'Abramo, P., & Serventi, R. (2011, March). Design and verification of hardware building blocks for high-speed and fault-tolerant in-vehicle networks. *Industrial Electronics, IEEE Transactions on*, *58*(3), 792-801.

Benini, L., Bogliolo, A., & De Micheli, G., (2000, June). A survey of design techniques for system-level dynamic power management. *Very Large Scale Integration (VLSI) Systems, IEEE Transactions on*, 8(3). 299-316.

Conte, T. M., & Hwu, W. M. (1991, January). Benchmark characterization. *Computer*, 24(1), 48-56.

Entrena, L., Garcia-Valderas, M., Fernandez-Cardenal, R., Lindoso, A., Portela, M., & Lopez-Ongil, C. (2012, March). Soft error sensitivity evaluation of microprocessors by multilevel emulation-based fault injection. *Computers, IEEE Transactions on*, *61*(3), 313-322.

Gupta, P., Agarwal, Y., Dolecek, L., Dutt, N., Gupta, R. K., Kumar, R., Mitra, S., Nicolau, A., Rosing, T.S., Srivastava, M.B., Swanson, S., & Sylvester, D. (2013, January). Underdesigned and opportunistic computing in presence of hardware variability. *Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on*, *32*(1), 8-23.

Guzman-Miranda, H., Aguirre, M. A., & Tombs, J. (2009, May). Noninvasive fault classification, robustness and recovery time measurement in microprocessor-type architectures subjected to radiation-induced errors. *Instrumentation and Measurement, IEEE Transactions on*, *58*(5), 1514-1524.

Khan, O., & Kundu, S. (2011, September-October). Hardware/software codesign architecture for online testing in chip multiprocessors. *Dependable and Secure Computing, IEEE Transactions on*, *8*(5), 714-727.

Leveugle, R. (2007, October). Early analysis of fault-based attack effects in secure circuits. *Computers, IEEE Transactions on*, *56*(10), 1431-1434.

Lajolo, M., Raghunathan, A., Dey, S., & Lavagno, L. (2002, June). Cosimulation-based power estimation for system-on-chip design. *Very Large Scale Integration (VLSI) Systems, IEEE Transactions on*, *10*(3), 253-266.

Mao, S., & Wolf, T. (2010, June). Hardware support for secure processing in embedded systems. *Computers, IEEE Transactions on*, *59*(6), 847-854.

Myaing, A., & Dinavahi, V. (2011, January). FPGA-based real-time emulation of power electronic systems with detailed representation of device characteristics. *Industrial Electronics, IEEE Transactions on*, *58*(1), 358-368.

Patel, K., Parameswaran, S., & Ragel, R. G. (2011, September). Architectural Frameworks for Security and Reliability of MPSoCs. *Very Large Scale Integration (VLSI) Systems, IEEE Transactions on*, *19*(9), 1641-1654.

Poovey, J. A., Conte, T. M., Levy, M., & Gal-On, S. (2009, August). A benchmark characterization of the eembc benchmark suite. *Micro, IEEE*, *29*(5), 18-29.

Sami, M., Sciuto, D., Silvano, C., & Zaccaria, V. (2002, September). An instruction-level energy model for embedded VLIW architectures. *Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on*, *21*(9), 998-1010.

Tiwari, V., Malik, S., & Wolfe, A. (1994, December). Power analysis of embedded software: a first step towards software power minimization. *Very Large Scale Integration (VLSI) Systems, IEEE Transactions on*, *2*(4), 437-445.

Conference Papers:

Abke, J., Böhl, E., & Henno, C. (1998, July). Emulation based real time testing of automotive applications. *4th IEEE International On-Line Testing workshop* (pp. 28-31). IEEE.

Bai, G., Bobba, S., & Hajj, I.N., (2001). Static Timing Analysis Including Power Supply Noise Effect on Propagation Delay in VLSI Circuits. *Proceedings of the 38th Design Automation Conference* (pp. 295-300). IEEE.

Baraza, J. C., Gracia, J., Gil, D., & Gil, P. J. (2005, November). Improvement of fault injection techniques based on VHDL code modification. *High-Level Design Validation and Test Workshop, 2005. Tenth IEEE International* (pp. 19-26). IEEE.

Bellosa, F. (2000, September). The benefits of event-driven energy accounting in power-sensitive systems. *Proceedings of the 9th workshop on ACM SIGOPS European workshop: beyond the PC: new challenges for the operating system* (pp. 37-42). ACM.

Bhattacharjee, A, Contreras, G., & Martonosi, M. (2008, August). Full-system chip multiprocessor power evaluations using FPGA-based emulation. *Low Power Electronics and Design (ISLPED), 2008 ACM/IEEE International Symposium on* (pp. 335-340). IEEE.

Coburn, J., Ravi, S., & Raghunathan, A. (2005, June). Power emulation: a new paradigm for power estimation. *Proceedings of the 42nd annual Design Automation Conference* (pp. 700-705). ACM.

Corno, F., Esposito, F., Sonza Reorda, M., & Tosato, S. (2004, October). Evaluating the effects of transient faults on vehicle dynamic performance in automotive systems. *Test Conference, 2004. Proceedings. ITC 2004. International* (pp. 1332-1339). IEEE.

Coskun, A.K., Ayala, J.L., Atienza, D., Rosing, T.S., & Leblebici, Y. (2009, April). Dynamic thermal management in 3D multicore architectures. *Design, Automation & Test in Europe Conference & Exhibition* (pp.1410-1415). IEEE.

Daveau, J. M., Blampey, A., Gasiot, G., Bulone, J., & Roche, P. (2009, April). An industrial fault injection platform for soft-error dependability analysis and hardening of complex system-on-a-chip. *Reliability Physics Symposium, 2009 IEEE International* (pp. 212-220). IEEE.

Druml, N., Steger, C., Weiss, R., Genser, A., & Haid, J. (2012, March). Estimation Based Power and Supply Voltage Management for Future RF-Powered Multi-Core Smart Cards. *Design Automation and Test in Europe Conference and Exhibition* (pp. 358-363). IEEE.

Druml, N., Menghin, M., Steger, C., Weiss, R., Genser, A., Bock, H., & Haid, J. (2013, February). Emulation-Based Test and Verification of a Design's Functional, Performance, Power, and Supply Voltage Behavior. *21st Euromicro International Conference on Parallel, Distributed, and Network-Based Processing* (pp. 328-335). IEEE.

Flinn, J., & Satyanarayanan, M. (1999, February). Powerscope: A tool for profiling the energy usage of mobile applications. *Mobile Computing Systems and Applications, 1999. Proceedings. WMCSA'99. Second IEEE Workshop on* (pp. 2-10). IEEE.

Ganesan, K., John, L., Salapura, V., & Sexton, J. (2008, September). A Performance Counter Based Workload Characterization on Blue Gene/P. *37th International Conference on Parallel Processing* (pp. 330-337), IEEE.

Genser, A., Bachmann, C., Haid, J., Steger, C., & Weiss, R. (2009, July). An Emulation-Based Real-Time Power Profiling Unit for Embedded Software. *International Conference on Embedded Computer Systems: Architectures, Modeling and Simulation* (pp. 67-73), IEEE.

Genser, A., Bachmann, C., Steger, C., Weiss, R., & Haid, J., (2011, April). Voltage Emulation Platform for DVFS Voltage Drop Compensation Explorations. *International Symposium on Performance Analysis of Systems and Software* (pp. 129-130). IEEE.

Ghodrat, M. A., Lahiri, K., & Raghunathan, A. (2007, June). Accelerating system-on-chip power analysis using hybrid power estimation. *Design Automation Conference, 2007. DAC'07. 44th ACM/IEEE* (pp. 883-886). ACM.

Grochowski, E., Ayers, D., & Tiwari, V. (2002, February). Microarchitectural simulation and control of di/dt-induced power supply voltage variation. *High-Performance Computer Architecture, 2002. Proceedings. Eighth International Symposium on* (pp. 7-16). IEEE.

Guthaus, M. R., Ringenberg, J. S., Ernst, D., Austin, T. M., Mudge, T., & Brown, R. B. (2001, December). MiBench: A free, commercially representative embedded benchmark suite. *Workload Characterization, 2001. WWC-4. 2001 IEEE International Workshop on* (pp. 3-14). IEEE.

Haid, J., Kaefer, G., Steger, C., & Weiss, R. (2003, January). Run-time energy estimation in system-on-a-chip designs. *Proceedings of the 2003 Asia and South Pacific Design Automation Conference* (pp. 595-599). ACM.

Holtz, M., Narasimhan, S., & Bhunia, S. (2008, December). On-Die CMOS Voltage Droop Detection and Dynamic Compensation. *Proceedings of the 18th ACM Great Lakes symposium on VLSI* (pp. 35-41). ACM.

Jenn, E., Arlat, J., Rimen, M., Ohlsson, J., & Karlsson, J. (1994, June). Fault injection into VHDL models: the MEFISTO tool. *Fault-Tolerant Computing, 1994. FTCS-24. Digest of Papers., Twenty-Fourth International Symposium on* (pp. 66-75). IEEE.

John, L. K., Vasudevan, P., & Sabarinathan, J. (1999). Workload characterization: Motivation, goals and methodology. *Workload Characterization: Methodology and Case Studies, 1998* (pp. 3-14). IEEE.

Joseph, R., & Martonosi, M. (2001, August). Run-time power estimation in high performance microprocessors. *Proceedings of the 2001 international symposium on Low power electronics and design* (pp. 135-140). ACM.

Kozhikkottu, V. J., Venkatesan, R., Raghunathan, A., & Dey, S. (2011, March). VESPA: Variability emulation for System-on-Chip performance analysis. *Design, Automation & Test in Europe Conference & Exhibition (DATE)* (pp. 1-6). IEEE.

Krieg, A., Bachmann, C., Grinschgl, J., Steger, C., Weiss, R., & Haid, J. (2011, June). Accelerating early design phase differential power analysis using power emulation techniques. *Hardware-Oriented Security and Trust (HOST), 2011 IEEE International Symposium on* (pp. 81-86). IEEE.

Krieg, A., Grinschgl, J., Steger, C., Weiss, R., & Haid, J. (2011, July), A side channel attack countermeasure using system-on-chip power profile scrambling. *On-Line Testing Symposium (IOLTS), 2011 IEEE 17th International* (pp. 222-227), IEEE.

Krieg, A., Grinschgl, J., Steger, C., Weiss, R., Genser, A., Bock, H., & Haid, J. (2012, May). Characterization and handling of low-cost micro-architectural signatures in MPSoCs. *Test Symposium (ETS), 2012 17th IEEE European* (pp. 1-6). IEEE.

Ikhwan Lee, Hyunsuk Kim, Peng Yang, Sungjoo Yoo, Eui-Young Chung, Kyu-Myung Choi, Jeong-Taek Kong, Soo-Kwan Eo (2006, January). PowerViP: Soc power estimation framework at transaction level. *Proceedings of the 2006 Asia and South Pacific Design Automation Conference* (pp. 551-558). IEEE.

Leveugle, R. (2000, October). Fault injection in VHDL descriptions and emulation. *Defect and Fault Tolerance in VLSI Systems, 2000. Proceedings. IEEE International Symposium on* (pp. 414-419). IEEE.

Lukovic, S., Pezzino, P., & Fiorin, L. (2010, April). Stack Protection Unit as a step towards securing MPSoCs. *Parallel & Distributed Processing, Workshops and Phd Forum (IPDPSW), 2010 IEEE International Symposium on* (pp. 1-4). IEEE.

Reddi, V.J., Gupta, M.S., Holloway, G., Wei, G., Smith, M.D., & Brooks, D. (2009, February). Voltage Emergency Prediction Using Signatures to Reduce Operating Margins. *15th International Symposium on High Performance Computer Architecture* (pp. 18-29). IEEE.

Sweeney, P.F., Hauswirth, M., Cahoon, P., Cheng, A., Diwan, A., Grove, D., & Hind, M. (2004). Using hardware performance monitors to understand the behavior of java applications. *Proceedings of the 3rd USENIX Virtual Machine Research and Technology Symposium* (pp. 57-72). ACM.

Valderas, M. G., Garcia, M. P., Cardenal, R. F., Lopez Ongil, C., & Entrena, L. (2007, June). Advanced simulation and emulation techniques for fault injection. *Industrial Electronics, 2007. ISIE 2007. IEEE International Symposium on* (pp. 3339-3344). IEEE.

Zheng, H., Fan, L., & Yue, S. (2008, December). FITVS: A fpga-based emulation tool for high-efficiency hardness evaluation. *Parallel and Distributed Processing with Applications, 2008. ISPA'08. International Symposium on* (pp. 525-531). IEEE.

White papers/Application reports:
Flynn, J., & Waldo, B. (2005). Power management in complex soc design.*Synopsys White Paper*.

Texas Instruments (2002), Analyzing Target System Energy Consumption in Code Composer Studio IDE. *Texas Instruments*, Application Report

ADDITIONAL READING SECTION

Authored Books:
Mangard, S., Oswald, E., & Popp, T. (2007). *Power analysis attacks: Revealing the secrets of smart cards* (Vol. 31). Springer.

Journal Articles:
Baraza, J., Gracia, J., Blanc, S., Gil, D., & Gil, P. (2008, June) Enhancement of fault injection techniques based on the modification of VHDL code, *IEEE Transactions on Very Large Scale Integration Systems*, 16(6), 693-706.

Grinschgl, J, Krieg, A., Steger, C., Wei, R., Bock, H., Haid, J., Aichinger, T., & Ulbricht, C. (2013, March). Case study on multiple fault dependability and security evaluations. *Elsevier Microprocessors and microsystems, 37*(2), 218-227.

Conference Papers:
Bachmann, C., Genser, A., Haid, J., Steger, C., & Weiss, R. (2010, September). Automated Power Characterization for Run-Time Power Emulation of SoC Designs. *13th Euromicro Conference on Digital System Design* (pp. 587-594). IEEE.

Kocher, P., Jaffe, J., & Jun, B. (1999, January). Differential power analysis. In *Advances in Cryptology—CRYPTO'99* (pp. 388-397). Springer Berlin Heidelberg.

KEY TERMS & DEFINITIONS

Fault:
A fault constitutes a deviation of normal internal system states or signals. Such deviation could lead to the generation of wrong results, but it could also be masked by the current system state.

Error:
An error describes a deviation from the expected system behavior caused by a fault. Therefore, an error is a final consequence after a fault was activated and the result is stored by internal or external resources.

Fault Attack:
A fault attack is an intentional manipulation of the integrated circuit or its state, with the aim to provoke an error within the integrated circuit in order to move the device into an unintended state. The goal is to access security critical information or to disable internal protection mechanisms.

Vulnerability:
Vulnerability describes a certain inability of a system to withstand the effects of an attack in a hostile environment.

Hardware Emulation:
Hardware emulation is a technique that integrates a hardware design into a reconfigurable (e.g. FPGA-based) prototyping platform in order to allow the functional testing of a design-under-test including its firmware. This way both hardware and software can be evaluated in a realistic performance setting.

Power Emulation:
Power emulation extends the hardware emulation technique with power sensors and corresponding power models in order to gather estimated power analysis data of the design-under-test.

Smart Card:
A smart card is a device with an integrated circuit including its own memory and central processing unit. Besides a standard contact-based interface, it can also be powered

contactlessly by means of an alternating and modulated magnetic field, through which contactless communication is also enabled.

System-on-Chip:
A System-on-Chip (SoC) is an integrated circuit integrating all circuits and electronics (such as analog, digital, mixed-signal, or RF components) necessary for a system on a single chip.

Industrial applications of emulation techniques for the early evaluation of secure low-power embedded systems

Norbert Druml, Manuel Menghin, Christian Steger
Graz University of Technology, Institute for Technical Informatics, Austria
Armin Krieg, Andreas Genser, Josef Haid, Holger Bock
Infineon Technologies Austria, Design Center Graz, Austria
and Johannes Grinschgl
Linz, 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 book 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 the chapter “Vulnerabilities of secure and reliable low-power embedded systems and their analysis methods - A comprehensive study”. 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.

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 via the shunt resistor R_{Shunt}, which is depicted by a Zener diode in a simplified way. Its purpose is to protect the smart card electronics against power surges and to reduce side-channel information leakage.

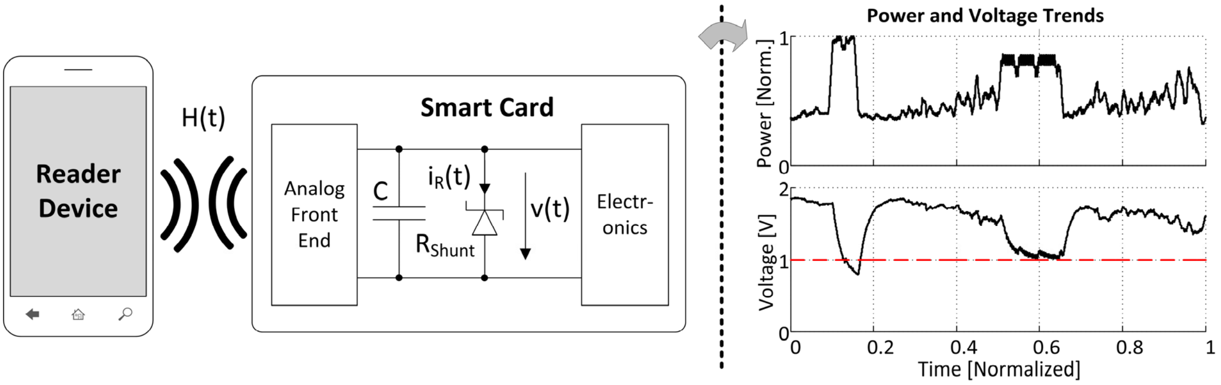


Figure 1: Reader / smart card system and dedicated smart card power / voltage trends. Peak power consumption provokes hazardous supply voltage drops which may compromise the smart card's operational stability.

In addition, smart card systems may be the target of security attacks. Such attacks must be countered by the smart card and, at the same time, it has to perform its normal functions in a reliable fashion and, whenever it is possible, with the best possible performance.

OBJECTIVES

Figure 2 shows our proposed comprehensive early design phase evaluation platform. It enables functional, power consumption and supply voltage, as well as performance and fault-attack investigations of power-constrained embedded systems.
A characterization process is required initially in order to model power consumption and supply voltage as well as performance and fault-attacks. The design-under-test is then synthesized on an FPGA prototyping platform incorporating all models. The functional emulation of the design-under-test coupled with all established models on the prototyping platform delivers much information (i.e., power, supply voltage, performance information, etc.) about all system parameters, as discussed previously.

The objectives are to gain insights by using early evaluation based on emulation techniques and to integrate the effective feedback of this information into the development process. They are essential in order to reach truly secure and power-aware embedded systems.

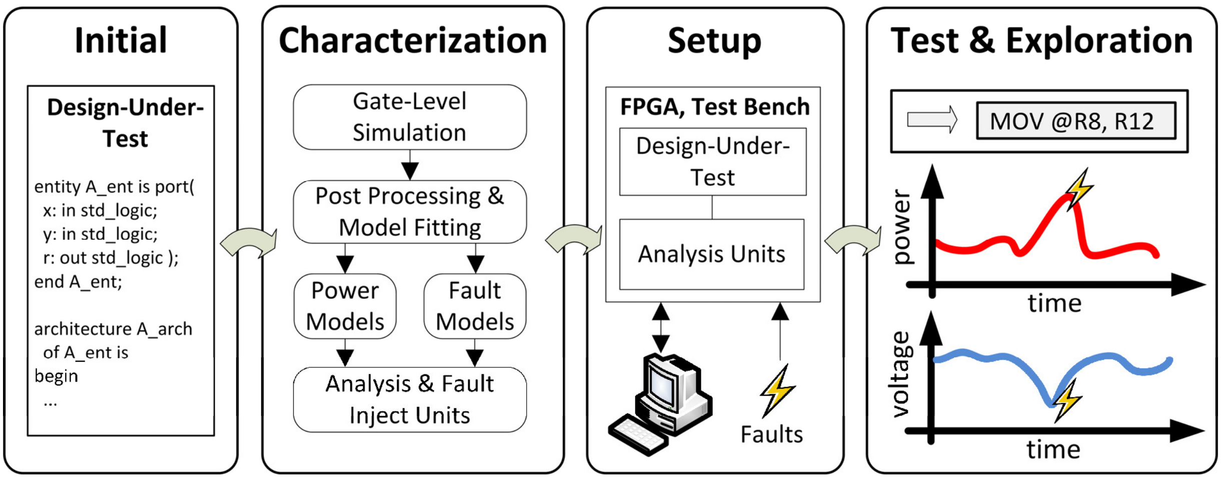


Figure 2: Principle of the early design phase evaluation flow.

Background

Smart card applications in power-constrained insecure and secure environments

Security controllers embedded in smart cards are deployed in many today's markets in order to secure sensitive data and to protect our privacy. Smart card systems are used in government applications such as national IDs, e-passports, or e-health insurance cards. Moreover, they are used in mobile phones (subscriber identification module), in mobile payments (credit cards, NFC applications, public transport systems) or secure platforms such as personal computers or pay-TV applications.

Critical infrastructure

New markets for smart cards are evolving in critical infrastructure. Efficiency enhancements and a sustainable energy supply are crucial to our society. Future smart-grids must cope with highly heterogeneous energy supply networks incorporating many decentralized energy producers. A highly automated smart-grid together with smart-metering is required in order to automate the network's load control and the customer billing system. Moreover, the customer can remotely control their home's energy consumers. Hence, these systems can be vulnerable to hacker attacks. Smart card systems can act as security anchors that control data integrity and prevent unauthorized manipulations.

Industrial control

The German government coined an initiative Industrie4.0. One focus is 'smart factories' to connect decentralized fully automated production sites. In addition, the initiative targets 'smart production' having a logistics network of multiple companies.
Supervisory Control and Data Acquisition (SCADA) has been introduced to control and monitor industrial processes that can range over multiple sites and long distances.
Data integrity of all involved components, remote terminals, or deployed sensors must be ensured. Smart cards are the device of choice in order to sustain hacker attacks and maintain secure system operation in Industrie4.0 applications.

The impact of failures in industrial environments on the safety of humans and the environment requires highly reliable and secure data processing and transactions, while these systems are often deployed in power-constrained environments. These smart cards must fulfill highest security requirements, hence they are complex System-on-Chips holding analog components as well as a multitude of peripherals (I2C, SPI, USB, etc.). Not to mention that these systems are loosely powered via their contactless power interface.

In order to fulfill the security requirements for a broad range of industrial application fields, Infineon has released a new security concept called Integrity Guard. Integrity Guard stores and processes on-chip data (including computations in the CPU itself) entirely encrypted. Moreover, to allow comprehensive error detection, the concept of two redundant on-chip CPUs checking each other's results is utilized.

The increasing complexity of these systems renders the maintenance of high test coverage a challenge, not only from a functional perspective, but also from the system's power and supply voltage behavior, as well as fault attack resistance.
Increasingly long redesign cycles emerge if potential failures are not detected in an early design phase before the first prototype is available.

We believe that emulation techniques provide early design phase investigation tools to fulfill comprehensive verification of complex System-on-Chips, while maintaining high test coverage. This early design phase approach avoids long redesign cycles and moreover decreases time-to-market.

EMULATION TECHNIQUES FOR THE EARLY DESIGN EVALUATIONS

In this section, we will present a comprehensive emulation methodology that is used in industry for design evaluations early in a product's development cycle. This methodology comprises power consumption analysis, supply voltage analysis, performance and activity analyses, as well as fault injection techniques for security and reliability analyses. The presented methodology uses hardware emulation techniques. It is performed by hardware-accelerated calculations, design-under-test evaluations are carried out in real time, and results are delivered for each clock cycle. Thus, engineers are supported with accurate and fast tools to explore and evaluate novel hardware/software designs.

Power Emulation

Power emulation, first introduced by Coburn et al. (2005) as a variant of estimation-based power profiling techniques, derives power information from evaluating power models. In principle, these power models can be implemented on various levels of abstraction, which influences their accuracy and complexity. Power emulation is operated on a relatively high level of abstraction in order to limit the model complexity and in turn hardware costs, which is a key requirement for low-power implementations of contactless smart cards. Models on this level of abstraction are often based on linear regression methods as depicted in (1).

$$\hat{P}(\mathbf{x}) = c_0 + \sum_{i=1}^{m} c_i \cdot x_i \qquad (1)$$

$x = [x_1, x_2, ... x_n]$ gives the vector of model parameters and $c = [c_1, c_2, ... c_n]$ represents the model's coefficients. In its simplest form, model parameters are mapped to system states such as smart card's low-power modes (e.g., sleep / halt) or memory read / write accesses. The vector of model coefficients c_i contains power information that is dissipated during the active phase of a certain system state x_i. The linear combination of the model coefficients c_i and the model parameters x_i form the power estimate $\hat{P}(\mathbf{x})$. Model coefficients c_i are determined in a power characterization process (Krieg et al., 2011), which is explained in further detail below.

Apart from performing pure power profiling on an embedded system (e.g., contactless smart cards), the hardware's power consumption gives important information for security evaluation methodologies as well. Simple Power Analysis (SPA) and Differential Power Analysis (DPA) are representatives of this group. Moreover, faults injected by such security evaluation techniques can induce significant power

consumption changes. If these are detectable by power estimation methods, security relevant countermeasures can be exploited (e.g., security traps or hardware resets).
The proposed system-level fault analysis concept extends the power emulation approach based on linear regression models explained above. Security relevant power information leakage can be extracted and evaluated, which gives room for design corrections before tape-out. The concept is illustrated by Krieg et al. (2012). The power model stated in (1) is extended according to (2).

$$\hat{P}(\mathbf{x}) = \hat{P}_{Static} + \hat{P}_{StateDynamic}(\mathbf{x}) + \hat{P}_{DataDynamic}(\mathbf{x}) \tag{2}$$

The model distinguishes between static power consumption $\hat{P}_{Static}$ and dynamic power consumption $\hat{P}_{Dynamic}$. Moreover, it allows for the separation of state-dependent $\hat{P}_{StateDynamic}$ and data-dependent power consumption information $\hat{P}_{DataDynamic}$. State-dependent power consumption information is covered by the simple power model in (1). The power estimates' data dependency is introduced in order to support security relevant power analysis, such as SPA and DPA as shown in (3).

$$\hat{P}(\mathbf{x}) = c_0 + \sum_{i=1}^{m} c_{si} \cdot x_i + \sum_{i=1}^{n} c_{di} \cdot x_i \tag{3}$$

Relevant signal states x_{si} and x_{di} and corresponding model coefficients c_{si} and c_{di}, respectively, are determined during a power characterization process (Krieg et al., 2011). A vector-based representation of the power model is given in (4). The difference between the real power consumption and the estimates given by the developed model is described by ε as depicted in (5). The average estimation error ε can be reduced by considering more system information in the form of additional states and their corresponding model coefficients. Finally, power sensors map state-dependent (SD) and data-dependent (DD) system states of the system-under-test to corresponding power value estimates. Estimation accuracies of greater than 90% compared to physical measurements can be achieved.

$$\hat{P}(\mathbf{x}) = c_0 + \mathbf{c}_s\mathbf{x} + \mathbf{c}_d\mathbf{x} \tag{4}$$

$$P(\mathbf{x}) = \hat{P}(\mathbf{x}) + \varepsilon \tag{5}$$

Power Characterization

The established power model highly influences power-profiling quality. The choice of model parameters that represent most power-relevant system states are of great importance. Model parameters and their corresponding model coefficients are determined during the power characterization process as illustrated in Figure 3. The proper number and the right choice of these model parameters impacts on the model's complexity and accuracy.

First, an exhaustive benchmarking suite is executed on the design-under-test on a gate-level basis. These benchmarks should be designed in a way that they cause system activity across the entire system in order to reach representative results in terms of power consumption.

These simulations uncover activity information for any signal of interest within the system. Once acquired, they form the basis for power simulations resulting in corresponding power values.

Activity and power information is processed in the model-parameter selection process. A relevancy analysis using statistical methods must be performed in order to select the most relevant power parameters. Finally, a linear regression model fitting process is performed determining relevant power model coefficients c_0, $\mathbf{c}_s$, and $\mathbf{c}_d$.

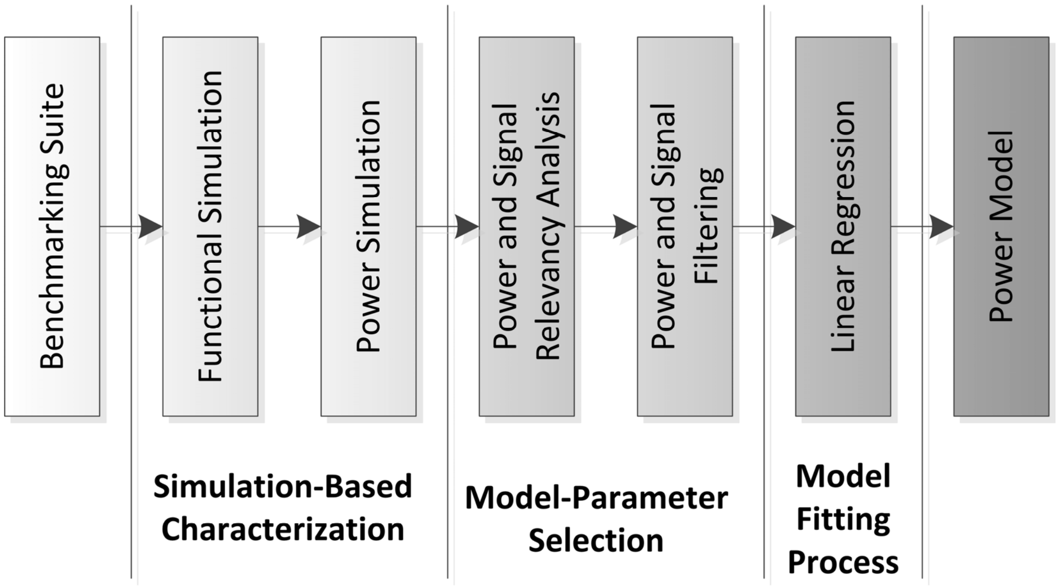

Benchmarking Suite
Functional Simulation
Power Simulation
Power and Signal Relevancy Analysis
Power and Signal Filtering
Linear Regression
Power Model
Simulation-Based Characterization
Model-Parameter Selection
Model Fitting Process

Figure 3: Power characterization flow.

Supply voltage estimation techniques form another important field of research. Supply voltage information of a system can shed light on its susceptibility to supply voltage variations and, in turns, to its reliability. This is of particular importance for contactless smart card systems.

Because of the mathematical relationship between power and voltage, power information is a key prerequisite in order to gain insights into supply voltage behavior. Hence, power emulation provides a good basis for supply voltage analysis emulation techniques.

Supply voltage characterization and emulation

A smart card system's contactless power transfer is very limited. As a consequence, a smart card is prone to supply voltage drops caused for example by high power consuming computations or an insufficient magnetic field strength. A smart card hardware/software engineer must be aware of these power supply issues. Therefore, it is of high importance to support engineers with accurate and fast supply voltage and power consumption estimation tools early during the design phase. Here we present a methodology featuring the evaluation of a contactlessly powered smart card's supply voltage behavior early during its hardware/software design time. This methodology comprises the following three phases: power network model characterization and model creation, augmentation, and emulation.

During the first phase, the power supply network of the reader / smart card system is characterized. A contactless smart card is powered by a magnetic field that is emitted by a reader device. Figure 4 illustrates the equivalent circuit of a reader / smart card system, as introduced by Finkenzeller (2003). It is analytically defined by (6). This analytical approximation is based on the law of Biot-Savat and is therefore only valid for rectangular shaped antennas. The reader generates a magnetic field with the help of a fixed voltage v_1, the resonance circuit C_R, L_R, and R_R, and an alterable resistor $R_{\mathrm{Re}l}(t)$. By means of inductive coupling, electrical power is transferred contactlessly to the smart card. The coupling factor between smart card and reader is defined by the parameter k. After rectification, electrical energy is buffered within the capacitor C_B. The capacitor's charge level $Q_c(t)$ sets the crucial voltage $v(t)$, which is supplied to the electronics. The shunt resistor R_{Shunt}, which is depicted in a simplified form of a Zener diode, prevents the adjacent electronics from power surges and reduces security related side-channel information leakage. The changing resistor of the smart card's CPU is given by $R_{CPU}(t)$. $R_L(t)$ comprises the smart card electronics' total changing resistance. Depending on the smart card CPU's power consumption and the power provided by the magnetic field, capacitor C_B charges or discharges. It is crucial to provide a proper voltage level $v(t)$ to the electronics. If this voltage $v(t)$ drops below a certain threshold, the electronics' operational stability is lost.

However, in order to develop an appropriate model of a smart card's power network which can be feasibly calculated by dedicated Arithmetic and Logic Units (ALUs) within an FPGA prototyping board, further simplifications need to be performed. Therefore, the electrical current and voltage characteristics of the reader / smart card system are measured. Based on these characteristics, a Thévenin voltage source is introduced, as proposed by Wendt et al. (2008) and depicted by Figure 4. The resulting equivalent circuit can now be expressed by a first order differential equation (if the shunt resistor's functionality is simplified). With the help of a charge-based approach, which is defined by (7), the behavior of the supply voltage $v(t)$ can be easily computed in hardware. It should be noted that the voltage level of $v_i(t)$ depends on physically related parameters such as antenna characteristics, distance between reader and smart card, orientation of the smart card within the magnetic field, etc. The amount of electrical current $i(t)$ that is consumed by the smart card's CPU is estimated by the dedicated power estimation unit, which was introduced in the previous section. The presented model-based supply voltage analysis technique accounts for a maximum estimation error of only 2%, according to Wendt et al. (2008) and Druml et al. (2012).

$$v_2(t) = \frac{\omega k \sqrt{L_R L_T}\, i_R}{\sqrt{\left(\frac{\omega L_T}{R_L} + \omega R_T C_T\right)^2 + \left(1 - \omega^2 L_T C_T + \frac{R_T}{R_L}\right)^2}} \qquad (6)$$

$$v(t+1) = \frac{Q_C(t) + \frac{v_i(t) - v(t)}{R_i}\Delta t - i(t)\Delta t}{C} \quad \text{if } v(t) < V_Z \qquad (7)$$

During the augmentation phase, a smart card design-under-test is enhanced with the presented power supply network model and the dedicated power emulation unit. All components, which are available in a hardware description language, are then synthesized in an FPGA prototyping board. Now, the design-under-test is ready and can be emulated. Supply voltage and power consumption estimates are gathered in real-time and for each clock cycle.

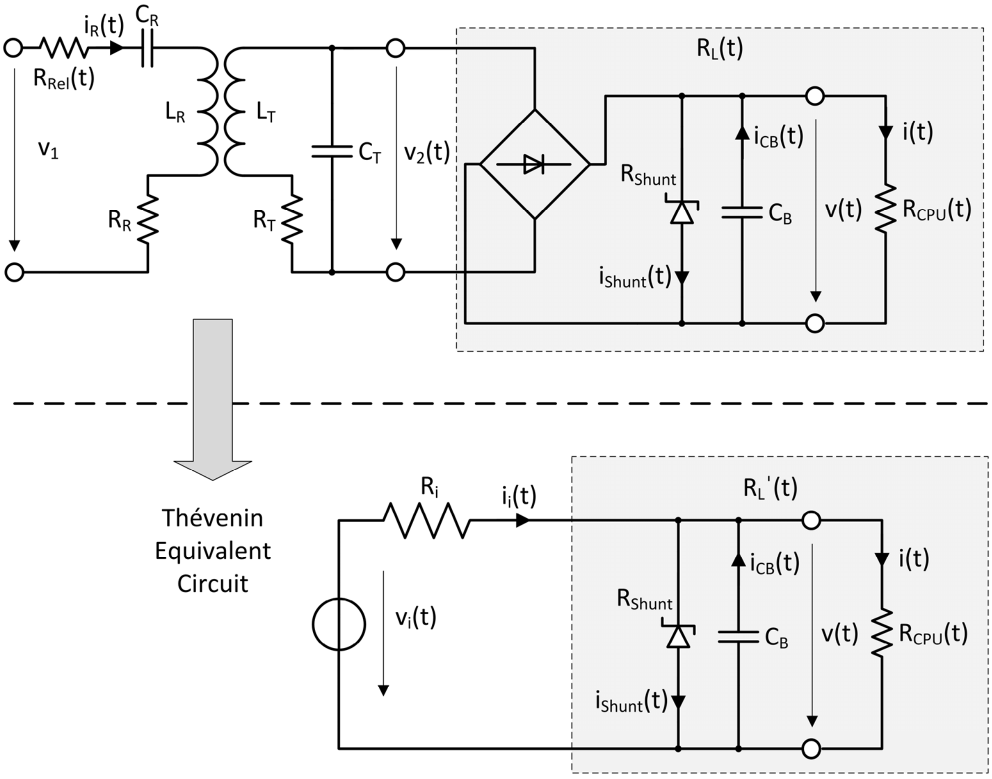


Figure 4: Equivalent circuits of a reader / smart card system's power supply network.

Emulation-based fault-attack and bit-flip emulation

In the previous section, an evaluation platform for power and supply voltage investigation was presented, which was tested in an industrial environment. In this section, we will show how the integration of fault models can extend its functionality to mimic fault attacks or reliability issues. For this specific case study, we introduce an emulation methodology for attacks on the memory sub-system of a smart card. Attack scenarios are mapped on the cache data bus of the target, which can be a LEON3 processor or security controller, using integrated saboteur modules (specific hardware elements to influence selected parts of the system in a controlled manner). A programmable fault injection controller controls these attack runs. It is connected to the verification system's serial interface. This enables the parameterization through standard APDU (Application Protocol Data Unit) commands. This simple modification already allows for a wide variety of security robustness tests of fault-attack hardened smart card operating systems. The APDU command integration permits the seamless integration of the platform into a standard software verification system. For more details on this emulation system please refer to the work shown in Grinschgl et al. (2013).

The high performance of the FPGA-based emulation platform allows high fault attack coverage of real-world applications using a multitude of attack vectors. On the other hand, as described in Krieg et al. (2013), a saboteur-based implementation for dependability evaluation has to be created in a completely different way. The random nature of these fault effects comes with the need of the integration of a large number of saboteurs. For this type of fault-injection testing, zones in the target implementation have to be defined, where faults would most likely directly result in disturbed operation.

Performance emulation

If a design-under-test is given which needs to fulfill certain real-time or performance constraints, it is of high importance to carry out performance evaluations during early design stages in order to detect hardware/software design flaws as soon as possible. For this performance analysis purpose, the use of Hardware Performance Counters (HPC) represents a common technique. An HPC represents a small circuit that is integrated into the design-under-test and monitors performance events e of signals or hardware units of interest. Given the fact that the design-under-test is available in a hardware description language, HPCs can be added to any component easily without changing the component's original functionality. A performance event e is triggered if a logical function f over a set of input signals s_n is satisfied, according to (8). These trigger events are captured by incrementing their dedicated performance counters. For example, if a processor system is being evaluated regarding its performance, performance events of interest can be memory accesses, cache misses, pipeline stalls, etc. within a certain period of time. The HPC data is gathered and can then be evaluated online by the design-under-test's software or hardware components. If HPCs are used in an early design phase prototyping board, as presented in this paper, all HPC data is transferred to a host PC in order to perform offline analysis and verification tasks. The presented performance analysis technique helps detect and correct hardware and software problems, which would otherwise violate worst-case execution time or real-time requirements.

$$e(s) = f(s_0, s_1, s_2, ...s_n) \tag{8}$$

Activity emulation

The first task includes the analysis of the LEON3 processor implementation in order to collect all relevant control signals of the system. A set of general benchmark applications is then executed to retrieve global control signal activity values. For this purpose, we relied on an adapted version (for the SPARC architecture) of the benchmark programs described in the following work (Bachmann et al., 2010). These applications are partially based on widely used benchmark suites like MiBench, Dhrystone, and Coremark. Furthermore, standard algorithms such as the quick-sort and AES encryption implementations have been added to better cover the application used on our embedded system.

The generated temporal tracing results are, for example, extracted from the Coremark benchmark by evaluating three system modules of the LEON3 processor. Detailed activity information can be extracted from such traces to be used in accurate fault injection models. Such an investigation for the Coremark benchmark shows a high even activity in the integer unit and MMU, but quite low control activity in the cache management modules. Fault injection into these cache management modules would therefore not be successful for targeted attack runs.

Also power estimation models are in need for such activity evaluations as, for example, large data buses have an impact on power consumption of System-on-Chip designs, which cannot be ignored. Hence, a characterization process also needs to include data signals to reduce the estimation error. However, bus line capacitances, which are the cause for this kind of power consumption, are only available after at least a preliminary physical implementation has been prepared.

The following metrics have been defined as a base for activity emulation evaluations:

N_{max} = number of observed signal lines (9)

N_{cycles} = number of observed clock cycles (10)

$N_{bc}[t] = \sum_{i=1}^{N\max} is\_changed(bit(i))[t]$ … number of changed signals (11)

$A[t] = \frac{N_{bc}[t]}{N_{\max}}$ … cycle activity at a certain point of time (12)

$A = \frac{\sum_{i=0}^{N_{cycles}} A[i]}{N_{cycles}}$ … global activity over the observed time frame (13)

Industrial Case Studies

In the following two sections, we outline evaluation results of our emulation methodology which was applied to an industrial smart card design and a freely available LEON3 processor design. We evaluated power and supply voltage behaviors, and we evaluated the design's resistance against fault attack test runs.

Case study - smart card power and supply voltage evaluations

Figure 5 depicts the basic setup of the early design phase emulation platform. It consists of an FPGA prototyping board and a host PC. The FPGA board implements the design-under-test, which must be available in a hardware description language (e.g., VHDL, Verilog). Power consumption sensors, supply voltage sensors, activity sensors, and fault injectors are added to any component of interest. The data of each individual sensor is gathered by dedicated control units in real-time and for each clock cycle. The fault injection controller's task is to inject faults into specified components at specified points in time by means of saboteur or mutant techniques. Trigger units are used for this decision process, which monitors specified signals (providing trigger information of the selected target application or hardware module). If the monitored signals match a specified pattern, a fault is triggered to be injected into the predefined target component. A platform controller is used to configure and control all units of the emulation platform. Furthermore, it temporarily buffers all gathered analysis data into the FPGA board's memory. At the same time, the analysis data is transmitted to the host PC by means of a high-data-rate interface. On the host PC, the data is archived and offline analyses can be carried out.

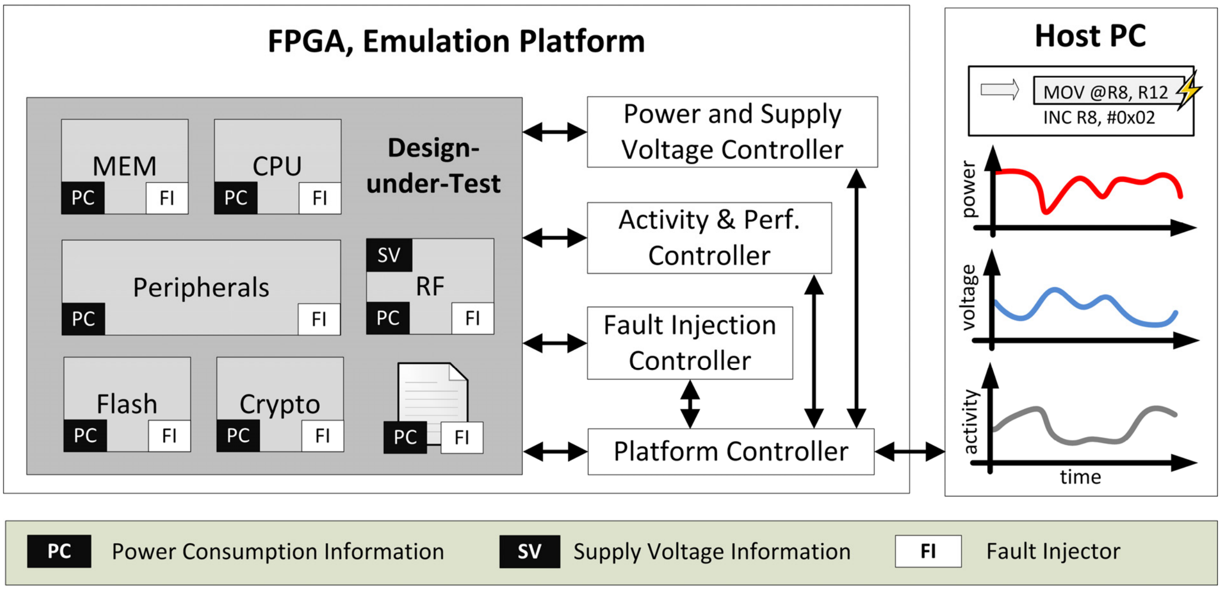


Figure 5: This figure depicts the basic emulation platform setup consisting of the FPGA prototyping board and a host PC for offline analysis tasks.

The presented early design phase emulation platform was set up for an industrial RF-powered contactless smart card design, which was used as design-under-test; cf. Druml et al. (2013). The aim of this test was the evaluation of the question whether an AES encryption application can be feasibly implemented. The left subplot of Figure 6 illustrates the smart card's power consumption and supply voltage behavior when operating the smart card with a maximum clock frequency of 31 MHz. The monitored power consumption profile reveals a low power consuming initialization phase and high power consuming cryptographic operations. During these cryptographic operations, the smart card's supply voltage drops below the crucial threshold of 1 V. As a consequence, the operational stability of the smart card would be compromised. Because of these early design phase evaluation capabilities, an engineer is able to detect power and supply voltage issues caused by hardware and software implementations before the tape-out or before software is released.

Thanks to dynamic voltage and frequency capabilities of the smart card, the detected instability can be resolved, for example by reducing the hardware's clock frequency. The right subplot of Figure 6 depicts this approach. After the low power consuming initialization phase, the hardware's clock frequency is reduced to 25 MHz programmatically. As a consequence, the AES encryptions dissipate less electrical power and hazardous supply voltage drops can be omitted. The smart card's operational stability is maintained. However, due to the clock frequency reduction, the total execution of this test case is prolonged by 17%.

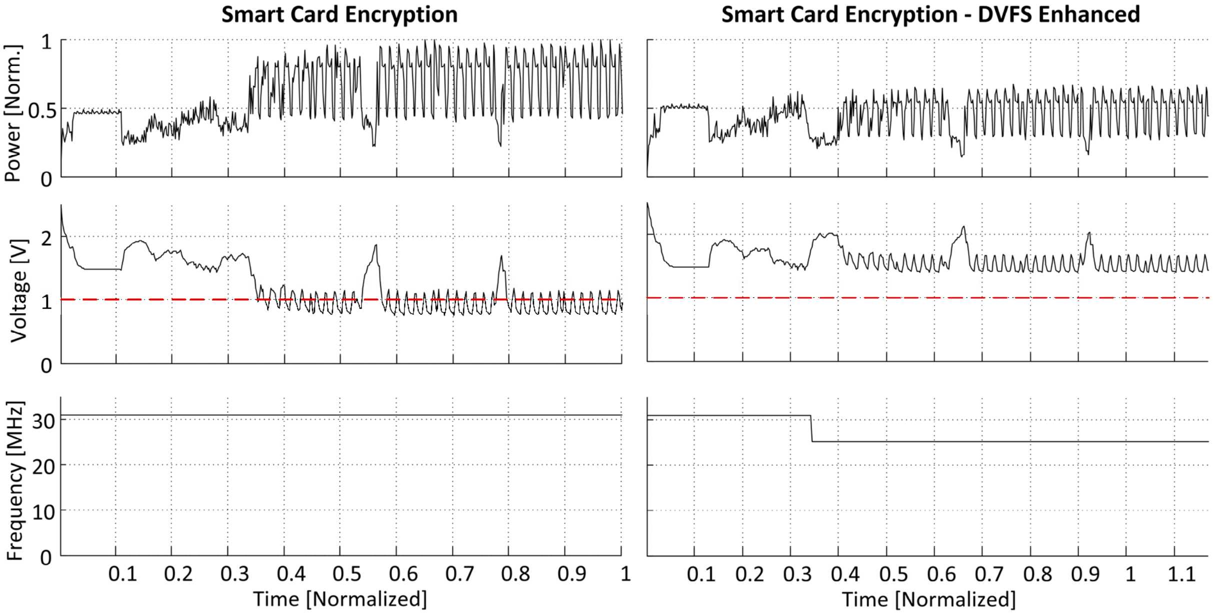
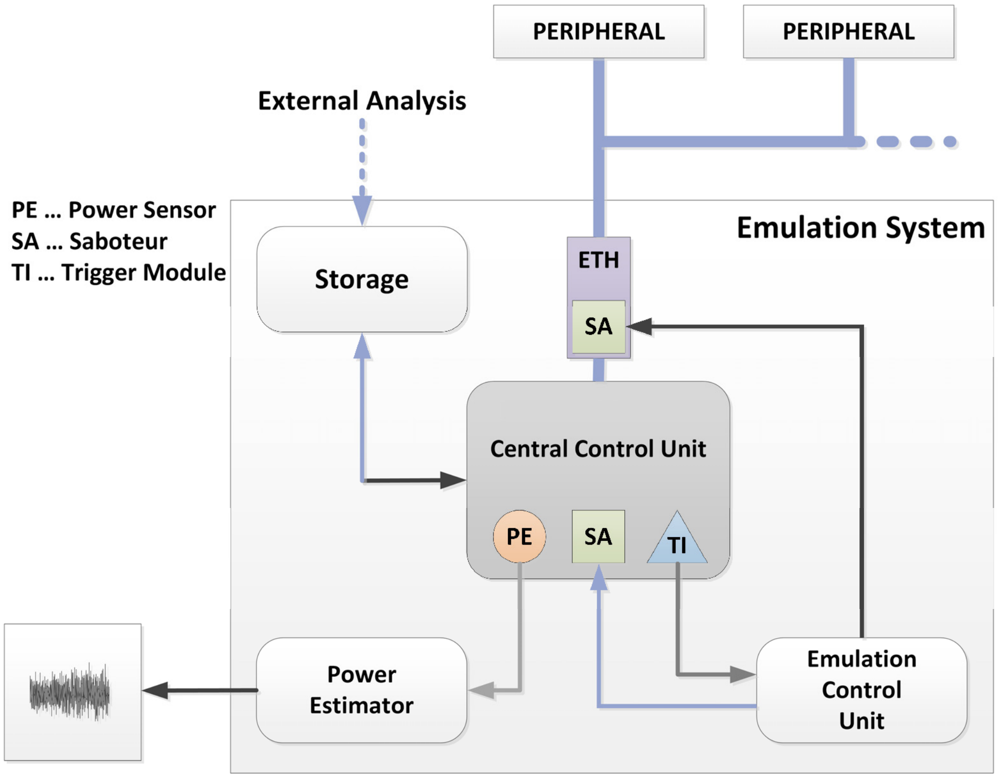


Figure 6: Power, supply voltage, and clock frequency trends of a smart card performing AES encryptions.

Case study - LEON3 fault attacks

As described in previous sections, an industrial fault injection platform has been created that permitted the automated long-term testing of smart card systems. The combination of a high-security operating system and controller implementation resulted in strongly secured system that could not be successfully attacked. For the documentation of these results, please refer to the work presented in Grinschgl et al. (2013). For demonstration purposes, a more general approach based on the LEON3 System-on-Chip will be presented. Please note that this configuration cannot be directly transferred to a smart card system (e.g., there is no Ethernet interface in smart cards) but the same principles apply. For a general dependability evaluation, saboteurs have been placed at various positions of the design such as the integer pipeline and an Ethernet interface controller. The injection architecture for these tests and the injection results is depicted in Figure 7.



Fault Injection into Ethernet Communication					
Benchmark	Injected Faults	CRC Fails	Sent Packages	Received Packages	Lost [%]
Basicmath_small (client)	>255000	0	13860	9761	29,6
Basicmath_small (server)	>255000	0	9761	9761	-
Basicmath_large (client)	>162000	0	1900	302	84,1
Basicmath_large (server)	>162000	0	302	302	-

Fault Injection into Ethernet Controller Memory					
Benchmark	Injected Faults	CRC Faults	Sent Packages	Received Packages	Lost [%]
Basicmath_small (client)	>260000	10	7929	7019	11,5
Basicmath_small (server)	>260000	835	7094	7929	-
Basicmath_large (client)	>248000	3	1608	1361	15,4
Basicmath_large (server)	>248000	157	1451	1608	

Fault Injection into Embedded Processor Memory				
Benchmark	Injected Faults	Calculations	Corrupted	Corrupted [%]
Basicmath_small (client)	>1460000	5637182	590432	10,47
Basicmath_large (client)	>791000	3048202	264451	8,68

Evaluation of Processor Self-Test Routines				
Self-Test	Injection Type	Injected Faults	Detected Faults	Fault Coverage
Multiplier	Stuck-At 1	1000	1000	100%
Multiplier	Transient 1	1000	1000	100%
ALU	Stuck-At	1000	1000	100%
ALU	Transient	1000	1000	100%
Shifter	Stuck-At	1000	1000	100%
Shifter	Transient	1000	1000	100%

Figure 7: Long-time fault injection implementation

The following conclusions can be drawn from these tests:

- Fault injection into the communication channel itself results in lost data packages, meaning data failures are correctly detected and the packets are not accepted. The larger benchmark results in more lost packages because of the longer turn-around time.
- The second set of tests shows that if faults do not happen in the communication channel but within the controller memory, fault detection in the communication protocol fails and corrupted packets are transmitted.
- The same characteristics can be observed if faults happen in the processor memory itself, again the communication protocol provides no protection.
- Self-test routines provide very high fault coverage by design, which could also be verified using fault injection into the processor hardware.

In conclusion, our saboteur-based approach allows simplified automated fault evaluation at various levels of communication abstractions.

Case study - Improving fault injection evaluation and power characterization

As described in Section "Power Characterization", benchmark characterization tasks have to be executed, after which an existing power modeling flow can be evaluated. To achieve optimal characterization applications, the generated activity information can be used in a further process.

Another important field of application for fault injection testing is self-test routines as they are used in the safety domain. Such software-based self-tests for processor cores need to have a deterministic behavior while providing high stuck-at fault coverage. Such deterministic applications and their evaluation have been shown in the work of Paschalis et al. (2001) introducing tests with a high fault coverage. We extended these test applications after a first exhaustive investigation to provide testing of all investigated sub-modules. For such simple self-tests, a very evenly distributed and high activity could be identified for both control and data signals.

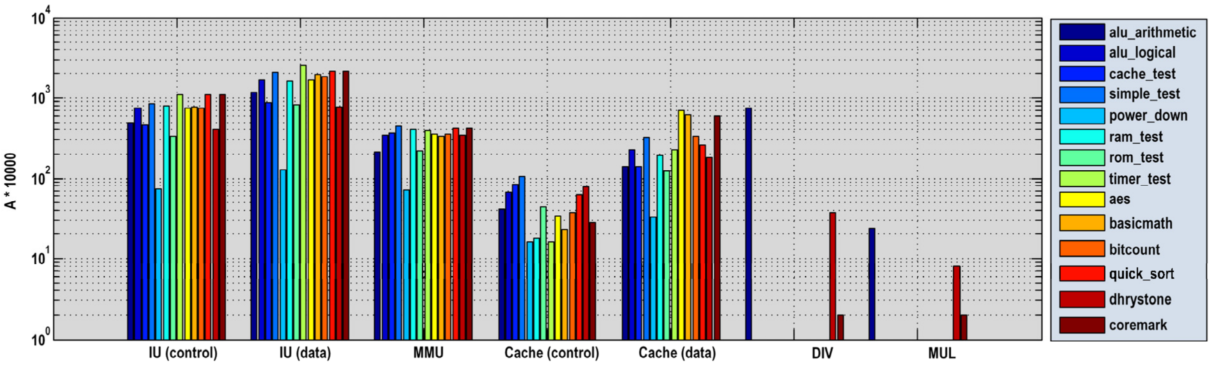


Figure 8: Benchmark characterization

To enable a comparison of a benchmark-based power characterization processes using traditional test applications and an emulation-supported activity analysis approach, we retrieved the application sets from the work shown in Bachmann et al. (2010). We applied power and signal correlation filters to select model coefficients, the same way it has been done in previous work. For the hardware implementation and application behavior characterization both approaches have been integrated into a LEON3-based FPGA system. By using a new application selection based on our activity emulation approach, we achieved similar power emulation accuracy while reducing the size of the power macro model by up to 20%. This allows for less complicated characterization and simpler hardware implementation, simplifying the testing of large multi-processor systems.

Recommendation – Application-specific benchmarks

The following conclusions can be drawn from such application investigations. First, as expected the automotive application of the MiBench suite shows similar signal activity. Further temporal evaluations of the associated signal traces also show that their temporal performance is similar, as expected from a domain-specific benchmark. Second, MiBench, quick-sort, most memory test and AES cryptography applications did not make use of any specialized arithmetic hardware like multipliers and dividers. Therefore, these and the remaining test candidates that also only resulted in little impact on arithmetic hardware activity were not well suited for an accurate power characterization process.

Data from exhaustive activity evaluations suggests the selection of less domain-specific characterization benchmark applications. Hence, applications with an evenly distributed high activity spectrum have been chosen. In the end, a final selection consisted of generic arithmetic; logical, cache, and RAM test applications. The control set contained benchmarks from the widely used Coremark and Dhrystone suites.

As described earlier, although the coefficient set shrunk by about one fifth because of the better activity mix, comparison showed similar or even better emulation results. This results in a strong call for more specific testing suites, and evaluation systems that allow a detailed look into the target system.

FUTURE RESEARCH DIRECTIONS

Static and formal analysis for high-level power and security properties

A major challenge during and after the design of a novel implementation is the provision of trust between the manufacturer and a customer of high security products. In order to enable a defined level of trust between all participants, system certification aims at securing the supply chain of security critical products. Common Criteria, for example, defines such assurance levels to describe how well documented the design process (besides other processes) of such a product needs to be. High assurance levels, as applied to certain types of smart cards, include the necessity that certain fault attack scenarios are tested by independent test laboratories. The software verification platform introduced in this work is targeted at the preparation of software and hardware implementations for such artificial tests and real-world attacks. It has to be noted that such emulation-based testing as well as physical tests are suspect to limitations concerning observability. Therefore, they cannot provide a guarantee that the investigated system covers all possible attack scenarios.

Another point that has to be taken care of is the increasing complexity of smart card systems, which also causes a widened evaluation space. The verification problem that is also known from functional verification creates a strong need for an extended use of formal methods during the design and verification phases of the implementation. Recently published literature shown in academia and industry tried to solve these problems, but so far, it has not been possible to find comprehensive solutions responding to the specific needs of this industry sector (secure embedded systems).

System-level power and security evaluations of mobile systems

Payment and personal ID sectors have seen a massive introduction of smart cards in recent years that have come with an increasing introduction of mobile reader systems that are needed to communicate with these devices. Smart card and reader systems are closely examined for the power and security related challenges they are facing. Unfortunately, research has concentrated on the resolution of issues for only these isolated problem domains. Challenges resulting from the wireless connection and interaction between a contactless smart card and the reader system have not been sufficiently investigated. Therefore, possible security problems could have been missed and power consumption issues on the reader side could emerge, as the transmission power is kept at a maximum level at all time. The latter results from the fact that currently neither smart card nor reader system have detailed information about transmission channel properties.

Estimation-based and prediction-based power-management strategies for lower-power systems

Power emulation can serve the needs for novel power management techniques, without requiring analog components. In traditional approaches, analog measurements provide information to power management algorithms. Instead, power information from emulation techniques enables power management with low hardware overhead in a purely digital manner. This reduces the power management complexity and eases on-chip integration.

This approach can directly steer dynamic voltage and frequency scaling (DVFS) approaches that vary system frequency and supply voltage in order to optimize the system’s power consumption.

Next generation embedded systems that harvest energy from the environment require even more sophisticated power management techniques. High load changes can severely harm these systems and compromise reliable system operation. Power and supply voltage emulation techniques extended with prediction techniques can help to tackle these challenges. Monitoring internal system information in order to estimate power and supply voltage information could be complemented with observing pipeline information in order to predict future load changes and supply voltage drops.

Conclusion

In this chapter we presented a multi-disciplinary early design evaluation methodology that is capable of evaluating a design-under-test's functionality, power and supply voltage behavior, performance, temporal activity of components, and fault robustness. The design-under-test was integrated into an FPGA prototyping board along with model-based analysis and fault-injection units. Results were gathered hardware accelerated in real-time and for each clock cycle.

Smart cards are enabler products for new industrial applications in critical infrastructures such as smart-grids or cloud-controlled industrial fabrication sites.

We demonstrated the applicability of our approach on a number of case studies executed on our evaluation platform. The reliability of a smart card system was investigated by power and supply voltage profiling in order to detect harmful supply voltage drops. Security strength was illustrated in a fault-attack scenario carried out on the emulation-based evaluation platform. A benchmarking characterization study showed how to improve power and fault injection characterization by means of emulation techniques.

ACKNOWLEDGEMENTS

The authors would like thank the Austrian Federal Ministry for Transport, Innovation, and Technology, which funded the POWERHOUSE, POWER-MODES, and META[:SEC:] projects under the corresponding FIT-IT contracts FFG 815193, 825749, and 829586.

REFERENCES

Authored Books:

Finkenzeller, K. (2003). *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification, 2nd ed.* New York, NY, USA: John Wiley & Sons, Inc.

Journal articles:

Grinschgl, J, Krieg, A., Steger, C., Wei, R., Bock, H., Haid, J., Aichinger, T., & Ulbricht, C. (2013, March). Case study on multiple fault dependability and security evaluations. *Elsevier Microprocessors and microsystems, 37*(2), 218-227.

Krieg, A., Preschern, C., Grinschgl, J., Kreiner, C., Steger, C., Weiss, R., Bock, H., & Haid, J. (2013, May). Power And Fault Emulation For Software Verification and System Stability Testing in Safety Critical Environments. *IEEE transactions on industrial informatics, 9*(2), 1199-1206.

Conference Papers:

Bachmann, C., Genser, A., Haid, J., Steger, C., & Weiss, R. (2010, September). Automated Power Characterization for Run-Time Power Emulation of SoC Designs. *13th Euromicro Conference on Digital System Design* (pp. 587-594). IEEE.

Coburn, J., Ravi, S., & Raghunathan, A. (2005, June). Power emulation: a new paradigm for power estimation. *Proceedings of the 42nd annual Design Automation Conference* (pp. 700-705). ACM.

Druml, N., Steger, C., Weiss, R., Genser, A., & Haid, J. (2012, March). Estimation Based Power and Supply Voltage Management for Future RF-Powered Multi-Core Smart Cards. *Design Automation and Test in Europe Conference and Exhibition* (pp. 358-363). IEEE.

Druml, N., Menghin, M., Steger, C., Weiss, R., Genser, A., Bock, H., & Haid, J. (2013, February). Emulation-Based Test and Verification of a Design's Functional, Performance, Power, and Supply Voltage Behavior. *21st Euromicro International Conference on Parallel, Distributed, and Network-Based Processing* (pp. 328-335). IEEE.

Krieg, A., Grinschgl, J., Steger, C., Wei, R., Bock, H., & Haid, J. (2012, April). System side-channel leakage emulation for HW/SW security coverification of MPSoCs. *Design and Diagnostics of Electronic Circuits & Systems (DDECS), 2012 IEEE 15th International Symposium on* (pp.139-144). IEEE.

Krieg, A., Bachmann, C., Grinschgl, J., Steger, C., Weiss, R., & Haid, J. (2011, June). Accelerating early design phase differential power analysis using power emulation techniques. *Hardware-Oriented Security and Trust (HOST), 2011 IEEE International Symposium on* (pp. 81-86). IEEE.

Paschalis, A., Gizopoulos, D., Kranitis, N., Psarakis, M., & Zorian, Y. (2001, March). Deterministic software-based self-testing of embedded processor cores. *Proceedings of the conference on Design, automation and test in Europe* (pp. 92-96). IEEE Press.

Wendt, M., Grumer, C., Steger, C., Weiss, R., Neffe, U., & Muehlberger, A. (2008, November). System Level Power Profile Analysis and Optimization for Smart Cards and Mobile Devices. *ACM Symposium on Applied Computing*, November (pp. 118–121). ACM.

ADDITIONAL READING SECTION

Authored Books:

Mangard, S., Oswald, E., & Popp, T. (2007). *Power analysis attacks: Revealing the secrets of smart cards* (Vol. 31). Springer.

Journal articles:

Antoni, L., Leveugle, R., & Fehér, B. (2003, October). Using run-time reconfiguration for fault injection applications. *Instrumentation and Measurement, IEEE Transactions on*, *52*(5), 1468-1473.

Armengaud, E., Steininger, A., & Horauer, M. (2008, August). Towards a systematic test for embedded automotive communication systems. *Industrial Informatics, IEEE Transactions on*, *4*(3), 146-155.

Baraza, J., Gracia, J., Blanc, S., Gil, D., & Gil, P. (2008, June) Enhancement of fault injection techniques based on the modification of VHDL code, *Very Large Scale Integration Systems*, *IEEE Transactions on,* 16(6), 693–706.

Baronti, F., Petri, E., Saponara, S., Fanucci, L., Roncella, R., Saletti, R., D'Abramo, P., & Serventi, R. (2011, March). Design and verification of hardware building blocks for high-speed and fault-tolerant in-vehicle networks. *Industrial Electronics, IEEE Transactions on*, *58*(3), 792-801.

Conte, T. M., & Hwu, W. M. (1991, January). Benchmark characterization. *Computer*, 24(1), 48-56.

Guzman-Miranda, H., Aguirre, M. A., & Tombs, J. (2009, May). Noninvasive fault classification, robustness and recovery time measurement in microprocessor-type architectures subjected to radiation-induced errors. *Instrumentation and Measurement, IEEE Transactions on*, *58*(5), 1514-1524.

Leveugle, R. (2007, October). Early analysis of fault-based attack effects in secure circuits. *Computers, IEEE Transactions on*, *56*(10), 1431-1434.

Myaing, A., & Dinavahi, V. (2011, January). FPGA-based real-time emulation of power electronic systems with detailed representation of device characteristics. *Industrial Electronics, IEEE Transactions on*, *58*(1), 358-368.

Poovey, J. A., Conte, T. M., Levy, M., & Gal-On, S. (2009, August). A benchmark characterization of the eembc benchmark suite. *Micro, IEEE*, *29*(5), 18-29.

Conference papers:

Abke, J., Böhl, E., & Henno, C. (1998, July). Emulation based real time testing of automotive applications. *4th IEEE International On-Line Testing workshop* (pp. 28-31).

Baraza, J. C., Gracia, J., Gil, D., & Gil, P. J. (2005, November). Improvement of fault injection techniques based on VHDL code modification. *High-Level Design Validation and Test Workshop, 2005. Tenth IEEE International* (pp. 19-26). IEEE.

Corno, F., Esposito, F., Sonza Reorda, M., & Tosato, S. (2004, October). Evaluating the effects of transient faults on vehicle dynamic performance in automotive systems. *Test Conference, 2004. Proceedings. ITC 2004. International* (pp. 1332-1339). IEEE.

Daveau, J. M., Blampey, A., Gasiot, G., Bulone, J., & Roche, P. (2009, April). An industrial fault injection platform for soft-error dependability analysis and hardening of complex system-on-a-chip. *Reliability Physics Symposium, 2009 IEEE International* (pp. 212-220). IEEE.

Genser, A., Bachmann, C., Haid, J., Steger, C., & Weiss, R. (2009, July). An Emulation-Based Real-Time Power Profiling Unit for Embedded Software. *International Conference on Embedded Computer Systems: Architectures, Modeling and Simulation* (pp. 67-73), IEEE.

Genser, A., Bachmann, C., Steger, C., Weiss, R., & Haid, J., (2010, October). Power emulation based DVFS efficiency investigations for embedded systems*. International Symposium on System on Chip* (pp. 173-178). IEEE.

Grießnig, G., Mader, R., Steger, C., & Weiß, R. (2009, April). Fault insertion testing of a novel CPLD-based fail-safe system. *Proceedings of the Conference on Design, Automation and Test in Europe* (pp. 214-219). European Design and Automation Association.

Guthaus, M. R., Ringenberg, J. S., Ernst, D., Austin, T. M., Mudge, T., & Brown, R. B. (2001, December). MiBench: A free, commercially representative embedded benchmark suite. *Workload Characterization, 2001. WWC-4. 2001 IEEE International Workshop on* (pp. 3-14). IEEE.

Jenn, E., Arlat, J., Rimen, M., Ohlsson, J., & Karlsson, J. (1994, June). Fault injection into VHDL models: the MEFISTO tool. *Fault-Tolerant Computing, 1994. FTCS-24. Digest of Papers., Twenty-Fourth International Symposium on* (pp. 66-75). IEEE.

John, L. K., Vasudevan, P., & Sabarinathan, J. (1999). Workload characterization: Motivation, goals and methodology. *Workload Characterization: Methodology and Case Studies, 1998* (pp. 3-14). IEEE.

Kocher, P., Jaffe, J., & Jun, B. (1999, January). Differential power analysis. *Advances in Cryptology - CRYPTO'99* (pp. 388-397). Springer Berlin Heidelberg.

Leveugle, R. (2000, October). Fault injection in VHDL descriptions and emulation. *Defect and Fault Tolerance in VLSI Systems, 2000. Proceedings. IEEE International Symposium on* (pp. 414-419). IEEE.

Valderas, M. G., Garcia, M. P., Cardenal, R. F., Lopez Ongil, C., & Entrena, L. (2007, June). Advanced simulation and emulation techniques for fault injection. *Industrial Electronics, 2007. ISIE 2007. IEEE International Symposium on* (pp. 3339-3344). IEEE.

Zheng, H., Fan, L., & Yue, S. (2008, December). FITVS: A fpga-based emulation tool for high-efficiency hardness evaluation. *Parallel and Distributed Processing with Applications, 2008. ISPA'08. International Symposium on* (pp. 525-531). IEEE.

KEY TERMS & DEFINITIONS

Fault:
A fault constitutes a deviation of normal internal system states or signals. Such deviation could lead to the generation of wrong results, but it could also be masked by the current system state.

Error:
An error describes a deviation from the expected system behavior caused by a fault. Therefore, an error is a final consequence after a fault was activated and the result is stored by internal or external resources.

Fault Attack:
A fault attack is an intentional manipulation of the integrated circuit or its state, with the aim to provoke an error within the integrated circuit in order to move the device into an unintended state. The goal is to access security critical information or to disable internal protection mechanisms.

Vulnerability:
Vulnerability describes a certain inability of a system to withstand the effects of an attack in a hostile environment.

Hardware Emulation:
Hardware emulation is a technique that integrates a hardware design into a reconfigurable (e.g. FPGA-based) prototyping platform in order to allow the functional testing of a design-under-test including its firmware. This way both hardware and software can be evaluated in a realistic performance setting.

Power Emulation:
Power emulation extends the hardware emulation technique with power sensors and corresponding power models in order to gather estimated power analysis data of the design-under-test.

Smart Card:
A smart card is a device with an integrated circuit including its own memory and central processing unit. Besides a standard contact-based interface, it can also be powered contactlessly by means of an alternating and modulated magnetic field, through which contactless communication is also enabled.

System-on-Chip:
A System-on-Chip (SoC) is an integrated circuit integrating all circuits and electronics (such as analog, digital, mixed-signal, or RF components) necessary for a system on a single chip.

2013 21st Euromicro International Conference on Parallel, Distributed, and Network-Based Processing

Emulation-Based Test and Verification of a Design's Functional, Performance, Power, and Supply Voltage Behavior

Norbert Druml, Manuel Menghin, Christian Steger
and Reinhold Weiss
Institute for Technical Informatics
Graz University of Technology
Graz, Austria
{norbert.druml, manuel.menghin, steger, rweiss}@tugraz.at

Andreas Genser, Holger Bock
and Josef Haid
Design Center Graz
Infineon Technologies Austria AG
Graz, Austria
{andreas.genser, holger.bock, josef.haid}@infineon.com

***Abstract*—Test and verification are essential parts during a product's development cycle. Simulation and emulation are well known techniques to test and verify the functionality of a design-under-test (DUT) before its tape-out. However, there are additional issues like peak power consumption and supply voltage drops, which can compromise a hardware's functionality. These issues are only partly covered by nowadays functional hardware emulation test and verification approaches.**

This paper presents a comprehensive emulation methodology. It combines functional hardware emulation with model-based performance, power, and supply voltage analysis techniques. The DUT, which has to be available in a hardware description language, is integrated into a FPGA along with designated analysis units. These analysis units implement models of the DUT's performance, power consumption, and supply voltage behavior. The presented emulation methodology allows a designer to test designs in such a way that the cycle accurate results are taken online, in real-time, and verify both functional and performance behavior, as well as power consumption and supply voltage levels.

The proposed comprehensive emulation methodology is used, as an example of application, to verify the design of a LEON3 multi-core processor system as well as a RF-powered contactless smart card. The depicted results demonstrate that this emulation approach is suitable to detect functional misbehavior caused by power and supply voltage hazards and how they influence the performance of the system.

***Index Terms*—Verification, Test, System Abstraction Level, Power Estimation, Supply Voltage Estimation**

I. Introduction

Simulation-based approaches are widely used for test and verification purposes of hardware designs. However, if circuit size and test periods rise, the amount of *calculation time* needed can increase to a point where getting results in a reasonable amount of time is unfeasible. To improve the test and verification speed of hardware designs, functional hardware emulation can be used. In [1], the authors demonstrate a speed-up exceeding 10^6 gained by functional hardware emulation over software simulations. Functional hardware emulation is a technique that integrates the synthesizable hardware design into a FPGA prototyping platform. In [2], a microprocessor functional hardware emulation flow used for test and verification purposes is presented.

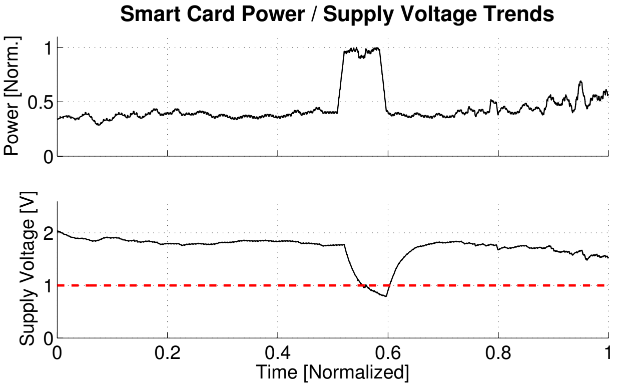


Fig. 1. This graph illustrates the severe influences of high power consumption changes on a RF-powered contactless smart card's supply voltage. If the supply voltage drops below a critical threshold, the functionality of the smart card's electronics is compromised.

However, functional hardware emulation approaches cover important design and application issues, like *power consumption hazards* or *supply voltage alterations*, only to some extent. In [3], the authors highlight the severity of supply voltage variations and supply voltage drops, which are caused by fast and high electrical current changes. Fig. 1 illustrates the impact of high power consumption changes on the supply voltage by means of a RF-powered contactless smart card. If the supply voltage drops below a hazardous threshold, the functionality of the smart card's electronics is compromised. Approaches to detect power consumption and supply voltage hazards have been presented by [4] and [5]: model-based estimation techniques are added to a functional hardware emulation environment. Thus, the power consumption and the

We would like to thank the Austrian Federal Ministry for Transport, Innovation, and Technology, which funded the project META[:SEC:] under the FIT-IT contract 829586.

1066-6192/12 $26.00 © 2012 IEEE
DOI 10.1109/PDP.2013.54

supply voltage behavior of a target device can be estimated cycle accurately and in real-time. If a power consumption or a supply voltage hazard is detected, countermeasures can then be performed.

Furthermore, it is important to test for performance related issues as well, in order to see if the design-under-test (DUT) is able to perform its function while respecting its real-time constraints. In [6], the number of cache misses, pipeline stalls, etc., are analyzed and optimization possibilities are investigated. Typically, hardware performance counters (HPCs) are used for such analysis purposes. The usage of HPCs in a hardware emulation environment is practicable. The HPCs can be easily embedded into a DUT that is available as synthesizable code.

This paper makes the following contributions:

- It presents a comprehensive emulation methodology. A DUT's functional hardware emulation is enhanced with performance as well as model-based power and supply voltage analysis techniques.
- Functional, performance, power consumption, as well as supply voltage tests and verifications of a DUT are performed online, cycle accurately, and in real-time.
- It introduces an innovative design debugging technique using functional, performance, power consumption, as well as supply voltage breakpoints.

This paper is structured as follows. Section II gives a short introduction into the related work covering the topics power, supply voltage, performance analysis, and hardware emulation frameworks. In Section III our emulation-based design space exploration approach is presented. Followed by Sections IV and V demonstrating the evaluation of a LEON3 System-on-Chip (SoC) and a state-of-the-art RF-powered smart card processor with the help of our emulation framework. Finally, our results are concluded and some details about our future work are given in Section VI.

II. Related Work

A. Power Analysis

Power analysis describes methods to determine the power consumption of electric circuits. There are two basic techniques: measurement-based or estimation-based. Estimation-based power analysis can be conducted at any abstraction level and can be subdivided into simulation-based and hardware accelerated techniques. Simulations of large circuits at low abstraction levels may cause a significant amount of calculation time. A high level simulation-based approach for power analyses and power management evaluations is presented by the authors in [7]. To speed up these time intense calculations, a hardware accelerated approach can be used. This is achieved by integrating the analysis algorithms in hardware, e.g., FPGA-based prototyping platforms. A hardware accelerated power analysis approach is presented in [8]. Coburn et al. introduced in [9] the *Power Emulation* methodology. The power consumption is estimated by integrating a dedicated DUT as well as register-transfer-level power macromodels into a FPGA. Thus, power information is gained cycle accurately. The power emulation technique can also be conducted at system-abstraction level, as presented in [4].

B. Supply Voltage Analysis

Supply voltage analysis is a methodology that is used to determine the supply voltage of integrated electric circuits. This can either be done at run-time or at design-time. In [3], a simulation-based approach is presented, which models a power network. On-die circuits are used in [10] to measure the voltage level and to detect hazardous voltage drops. Voltage comparators [11] or analog-to-digital converters [12] can also be used for hazardous supply voltage level detections. Hardware emulation approaches using model-based analysis units, as described in [4] or [5], are also feasible for supply voltage analysis tasks. The DUT as well as a supply voltage analysis unit are integrated into a FPGA. Thus, supply voltage estimates are delivered cycle accurately and in real-time.

C. Performance Analysis

Hardware performance counters (HPCs) are commonly used in nowadays processor systems for performance measurements. With the help of these HPCs, the occurrences of certain processor internal events (e.g., cache misses, pipeline stalls) are measured. The low level system behavior can be evaluated without the need of slow hardware simulations. The authors of [13] highlight the importance of supporting software developers with such low level application behavior information: Java applications are exemplarily analyzed regarding their low level performance. Based on such analysis data new performance optimizations can then be developed to respect certain real-time or worst-case execution time constraints. In [6], the authors describe the usage of HPCs to measure the workload of IBM's Blue Gene supercomputer. HPCs are also used in conjunction with power models to estimate a processor's power consumption, as presented in [14] and [15].

D. Hardware Emulation Frameworks

Several hardware emulation frameworks were presented to cope with the speed limitations of software simulation approaches. One of the first processor verifications using functional hardware emulation was performed by the authors of [2]. In [15], the authors present a hardware emulation framework using hardware performance counters to analyze a design's power consumption behavior. A method to explore and validate Multi-Processor System-on-Chip (MPSoC) designs is depicted by [16]. Another MPSoC emulation framework, with particular emphasis on Network-on-Chip (NoC) based systems, is presented in [17]. Besides Xilinx tools, analytic models are used to estimate technology-related parameters of prospective ASIC implementations.

Our comprehensive emulation approach combines state-of-the-art functional, performance, power, and supply voltage analysis techniques with innovative test and verification methods within one single framework. Thus, system developers are assisted during the whole development process with cycle accurate analysis data, which is provided in real-time.

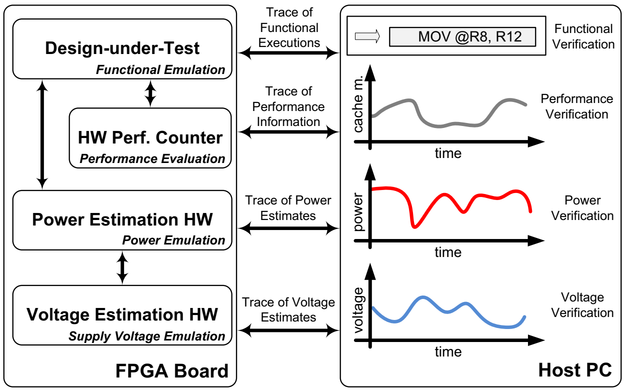


Fig. 2. Principle of the comprehensive emulation methodology. The DUT is synthesized along with dedicated analysis units within a FPGA prototyping board. Trace information is acquired in real-time and is sent to a host PC for further analysis tasks.

III. Comprehensive Emulation Approach

Our comprehensive emulation approach represents a methodology to test and verify a DUT's functionality, performance, power consumption, and supply voltage behavior simultaneously. This is achieved by developing a FPGA-based emulation test bench. This test bench integrates and emulates the DUT and uses model-based analysis and verification units. The test bench's architecture is designed to adapt the analysis models to any specific DUT easily. Fig. 2 illustrates the basic principle of the presented emulation methodology. The fact that DUT, the model-based analysis units, as well as an online verification unit are integrated in hardware, all analysis and verification tasks are performed cycle accurately and in real-time. The presented technique grants a significant speed-up compared to simulation-based approaches.

The architecture of the proposed emulation test bench is depicted in Fig. 3. The DUT is integrated into a FPGA. A power estimation unit is attached to the DUT and monitors the DUT's internal system states $\mathbf{x}(t)$. The DUT's power consumption $\widehat{P}(\mathbf{x}(t))$ is estimated according to these system states $\mathbf{x}(t)$ by means of the power estimation unit's power model. If a DUT supports the dynamic voltage and frequency scaling (DVFS) power management technique, a DVFS emulation unit is used. This unit models the DUT's currently selected voltage $V_{DD}(t)$ and frequency $f(t)$ parameters and outputs the corresponding power estimates $\widehat{P}(\mathbf{x}(t), f(t), V_{DD}(t))$. This power consumption information is then forwarded to the supply voltage estimation unit. This unit implements a model of the DUT's power network. Based on the power consumption information and the power network model, the DUT's supply voltage behavior $v(t)$ is estimated. An online verification unit monitors the provided functional, performance, power, and supply voltage information. All status information is then analyzed and verified according to predefined constraints and breakpoints. If these predefined verification constraints are violated, the DUT is stopped and a step-by-step debugging can be performed.

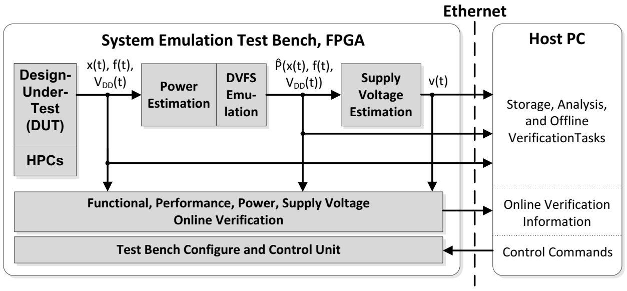

Ethernet
System Emulation Test Bench, FPGA
Design-Under-Test (DUT)
HPCs
x(t), f(t), V_DD(t)
Power Estimation
DVFS Emu-lation
P̂(x(t), f(t), V_DD(t))
Supply Voltage Estimation
v(t)
Functional, Performance, Power, Supply Voltage Online Verification
Test Bench Configure and Control Unit
Host PC
Storage, Analysis, and Offline VerificationTasks
Online Verification Information
Control Commands

Fig. 3. Architecture of the proposed comprehensive emulation test bench. The DUT is synthesized within a FPGA along with dedicated model-based analysis and verification units observing the DUT. Gathered analysis data is forwarded to the host PC.

The presented emulation test bench supports an Ethernet-based control and debug interface. This interface is used by a host PC to control and setup the test bench with specific test patterns and verification constraints. Furthermore, all test results, whether they are results from functional testing, performance testing, or power and supply voltage analyses, are transmitted from the test bench to the host PC. At the PC side, the data is archived and sophisticated software tools can be used for further offline analysis and verification tasks. In the following, each test bench component is described in detail.

A. Power Estimation

The power estimation technique used in our emulation approach is similar to a method described by the authors in [4]. A linear regression based power model is featured, which is presented by the authors in [18]. Fig. 4 illustrates the working principle of the power estimation technique. The DUT's internal system states x_i (e.g., CPU idle, cache hit, memory write) are monitored by dedicated power sensor units. A power model coefficient c_i defines the amount of power dissipated while being in the corresponding system state x_i. Then, the system states x_i and power coefficients c_i are concentrated into the vectors $\mathbf{x} = [x_1, x_2, x_3, ...]$ and $\mathbf{c^T} = [c_1, c_2, c_3, ...]^T$, respectively. Based upon the system states $\mathbf{x}$ and the corresponding power model coefficients $\mathbf{c^T}$,

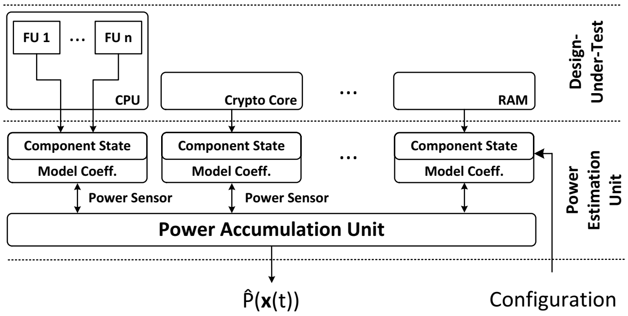


Fig. 4. Power estimation unit observes the DUT's system states. Power sensors map component states to power values. Obtained with changes from [4].

the DUT's power consumption is estimated according to (1) and (2). The linear combinations of $\mathbf{x}$ and $\mathbf{c^T}$ plus c_0, which defines the static leakage power dissipation, form the power estimates $\widehat{P}(\mathbf{x})$. The difference between power estimates $\widehat{P}(\mathbf{x})$ and the real power consumption $P(\mathbf{x})$ is covered by the error ϵ, according to (3). Because system states can change at any clock cycle, a time dependency is finally introduced by $\widehat{P}(\mathbf{x}(\mathbf{t}))$.

$$\widehat{P}(\mathbf{x}) = \widehat{P}_{stat} + \widehat{P}_{dyn} \tag{1}$$

$$\widehat{P}(\mathbf{x}) = c_0 + \sum_{i=1}^{n} c_i \cdot x_i = c_0 + \mathbf{c^T} \cdot \mathbf{x} \tag{2}$$

$$P(\mathbf{x}) = \widehat{P}(\mathbf{x}) + \epsilon \tag{3}$$

To determine the power model parameters c_0, $\mathbf{c^T}$, and $\mathbf{x}$ for a given DUT, a power characterization process is conducted. This characterization flow can be performed automatically for any synthesizable hardware design, as described by the authors in [19]. The estimation error ϵ depends on the number of considered system states during the DUT's power characterization process: the more system states considered, the lower the estimation error.

B. DVFS Emulation

Power estimates $\widehat{P}(\mathbf{x}(\mathbf{t}))$ are based upon a DUT, which is operated at a fixed clock frequency f. This fixed clock frequency is selected during the previously executed DUT's power characterization procedure. To cope with DUTs that alter their processor clock frequencies, a DVFS emulation unit is attached to the power estimation unit. In this case, the power estimation unit delivers power estimates $\widehat{P}(\mathbf{x}(\mathbf{t}))$, which are based on a clock frequency of 1 MHz. These power estimates $\widehat{P}(\mathbf{x}(\mathbf{t}))$ are then scaled according to (4) with the currently set processor clock frequency $f(t)$ and the processor's voltage level $V_{DD}(t)$.

$$\widehat{P}(\mathbf{x}(\mathbf{t}), f(t), V_{DD}(t)) = \widehat{P}(\mathbf{x}(\mathbf{t})) \cdot f(t) \cdot {V_{DD}}^2(t) \tag{4}$$

A lookup table (LUT) approach is used to map each supported processor clock frequency $f(t)$ to a dedicated needed voltage level $V_{DD}(t)$. The architecture of the hardware integrated DVFS emulation unit is depicted in Fig. 5.

C. Supply Voltage Estimation

Fig. 6 illustrates the principle of the supply voltage estimation unit. First, the electrical current $i(t)$ that is drawn by the DUT, is calculated by means of the DUT's power estimates $\widehat{P}(\mathbf{x}(t), f(t), V_{DD}(t))$. Then, the DUT's supply voltage $v(t)$ is estimated by means of a dedicated power network model. The calculation of $i(t)$ as well as the power network model are specific to each DUT and need to be implemented by the test bench designer.

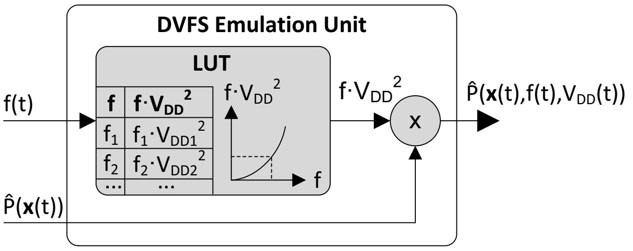


Fig. 5. Architecture of the DVFS emulation unit. A lookup table approach is used to scale the 1 MHz based power estimates $\widehat{P}(\mathbf{x}(\mathbf{t}))$.

D. Performance Evaluation

HPCs are used to evaluate performance matters of the DUT. Due to the fact that the DUT is available in a synthesizable hardware description language, HPCs can be added to any DUT component of interest easily.

A performance event e is defined by a function f over a set of input signals s_n, according to (5). Whenever the input signals s_n satisfy the function f, the dedicated counter is incremented. If a processor system is given as DUT, typical performance events of interest are cache misses, memory accesses, pipeline stalls, etc. The HPC data is then collected and evaluated against predefined constraints within the online verification unit. Additionally, the HPC data is transmitted to the host PC for storage as well as further offline analysis and verification tasks. With the help of these HPC analysis data, hardware and software problems can be detected, which would violate real-time or worst-case execution time constraints.

$$e(s) = f(s_1, s_2 ... s_n) \tag{5}$$

E. Online Verification

The online verification unit monitors and verifies information such as: function, performance, power consumption, and supply voltage. This information is cycle accurate and is available in real-time. The online verification unit is configured by the host PC with dedicated test patterns and verification constraints. A set of innovative *emulation breakpoints* can be specified by the test bench operator for debugging purposes:

- A *functional breakpoint* is triggered if a predefined instruction or a sequence of instructions is processed by the target design.

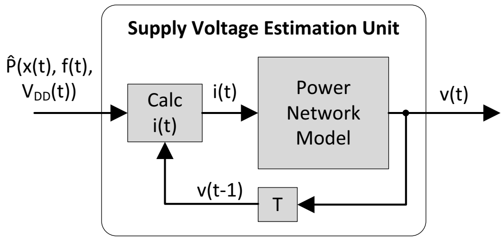
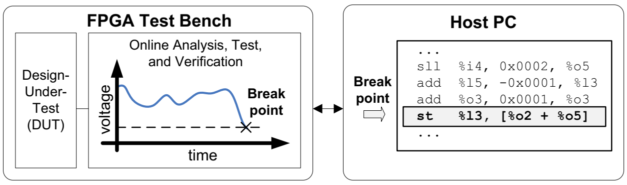


Fig. 6. Principle of the supply voltage estimation unit. The supply voltage $v(t)$ is estimated with the help of the power consumption information and an appropriate power supply network model.



```
...
sll  %i4, 0x0002, %o5
add  %l5, -0x0001, %l3
add  %o3, 0x0001, %o3
st   %l3, [%o2 + %o5]
...
```

Fig. 7. Working principle of functional, performance, power, and supply voltage breakpoints. If a breakpoint is triggered, the responsible sequence of instructions can be determined.

- A *performance breakpoint* is triggered if the dedicated performance constraint is violated, e.g., the number of cache misses reaches a maximum allowed number.
- A *power breakpoint* is triggered if the dedicated power consumption constraint is violated, e.g., the DUT's power consumption exceeds the defined threshold.
- A *supply voltage breakpoint* is triggered if the dedicated supply voltage constraint is violated, e.g., the DUT's supply voltage drops below the defined threshold.

Fig. 7 illustrates the principle of the breakpoint mechanics. If a breakpoint is triggered, the execution of the DUT is stopped by deactivating its clock. The host PC, which receives all status and verification data, can then perform a detailed offline analysis, e.g., which kind of instruction sequence triggered the specific breakpoint.

F. Configure and Control Unit

The configure and control unit provides two important functionalities. First, it is used to configure the emulation test bench with specific test patterns, verification constraints, and breakpoint settings. Second, a step-by-step debugging functionality is supported by controlling the DUT's clock accordingly. In conjunction with the online verification unit's breakpoints, a test bench operator is able to monitor step-by-step the propagation of a fault within the DUT.

IV. Case Study: LEON3 Processor

This case study demonstrates a comprehensive emulation test bench for a two-core LEON3 processor system. LEON3 is a SPARC V8 open source processor [20], which has been developed by the company Aeroflex Gaisler on behalf of the European Space Agency. This case study analyzes the LEON3's power consumption behavior during benchmark executions. A voltage stabilized power supply is used. Power breakpoints are used to detect and to debug hazardous power consumption peaks, which may destabilize the system.

A. LEON3 Processor Power Network

The architecture of the LEON3's power network as well as its voltage / current characteristic is depicted in Fig. 8. In this very simplified case study, the LEON3 processor is operated with a regulated, constant voltage source $v(t)$. If the electrical current $i(t)$ rises above a critical threshold, then the supply voltage $v(t)$ drops to zero. The electrical current $i(t)$ is derived from the LEON3's power consumption, which is estimated by the designated power estimation unit.

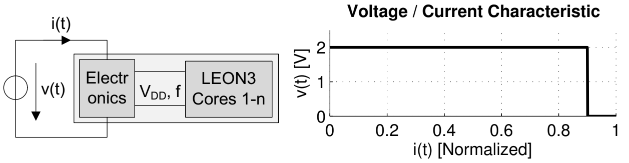


Fig. 8. Power network and supply voltage / current characteristic of the LEON3 processor case study. If the drawn current $i(t)$ exceeds a certain value, the supply voltage $v(t)$ drops hazardously.

B. Results

The LEON3 specific emulation test bench is integrated in a Xilinx Spartan 3 FPGA board. The MiBench benchmarking suite [21] has been chosen for reproducible testing purposes. Fig. 9 illustrates the execution of a string search algorithm while operating the LEON3 processor cores at a clock frequency $f(t)$ of 31 MHz. The first subplot shows the total power consumption of the LEON3 cores. Although the LEON3 is operated mostly within the power consumption margin, several power consumption peaks exceed the crucial threshold and trigger power consumption breakpoints. In this special use case, the power supply is not able to compensate these power peaks. Thus, the supply voltage drops to zero and the operational stability of the real LEON3 hardware would be lost. The third subplot of Fig. 9 illustrates the application of HPCs to count the number of cache events. In this simplified performance evaluation approach, a cache event is either a data or instruction cache hit or miss. The presented curve depicts the sum of all cache events during a specific time segment. Comparing both subplots with each other reveals the high correlation between cache events and the power consumption of the LEON3. Based on such performance information, a

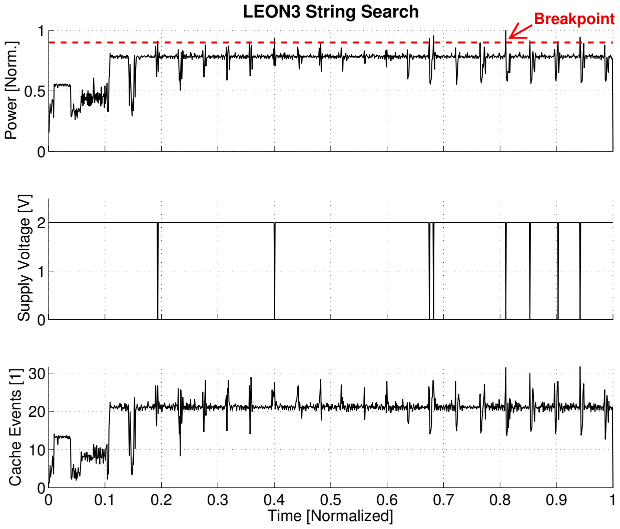


Fig. 9. LEON3 behavior during a string search benchmark. Power peaks above the threshold cause supply voltage drops and trigger power and supply voltage breakpoints. The operational stability is compromised.

TABLE I
COMPARISON OF HARDWARE SIMULATION AND REAL-TIME HARDWARE EMULATION SPEEDS.

Benchmark	RTL Sim. Time	Emu. Time	Speed-up
String Search	18 min 52 sec	5.5 ms	20581
FFT	22 min 39 sec	7.7 ms	17142
Basicmath	49 min 50 sec	17.3 ms	17283
Quicksort	31 min 43 sec	9.9 ms	19222

developer is able to analyze already during design time if an application running on the DUT would violate its real-time and worst-case execution time constraints. Fig. 10 depicts the sequence of operations triggering the power consumption breakpoint, which is marked with an arrow in Fig. 9. To resolve the demonstrated system instabilities, the following three approaches could be applied exemplary:

- Modifying the source code to reduce the number of cache misses, which cause additional power dissipation by accessing the RAM.
- Reducing the clock frequency of the LEON3 processor cores.
- Adding a capacitor to the LEON3's power supply network to reduce the hazardous supply voltage drops.

Table I illustrates the speed-up gained by the presented real-time emulation approach compared to hardware register transfer level simulations in Mentor Graphics ModelSim. Simulations are performed on a six-core AMD Phenom II 3.2 GHz processor system with 16 GB RAM. However, the initial setup of such a comprehensive emulation framework takes some time, which is not regarded in this comparison.

V. CASE STUDY: RF-POWERED SMART CARD

This case study exemplifies a comprehensive emulation test bench for a state-of-the-art single-core RF-powered contactless smart card CPU. Fig. 11 depicts the basic setup of a reader / smart card system. The reader device generates a magnetic field $H(t)$, which is used to power the contactless smart card and to communicate with it. Thus, smart card application designers need to be aware of the very limited power supply. Peak power consumption or a high average power consumption result in a dropping supply voltage of the smart card's electronics. If the supply voltage drops below a hazardous threshold, the smart card's operational stability is compromised.

```
             ...
             2827737ns CPU2: 0x4000265c  sll  %i4, 0x0002, %o5
             2827771ns CPU2: 0x40002660  add  %l5, -0x0001, %l3
             2827804ns CPU1: 0x4000a864  bne  0x4000a8c8
             2827804ns CPU2: 0x40002664  add  %o3, 0x0001, %o3
             2827804ns CPU1: 0x4000a868  ldub [%o1], %g1
Break point ⇨ 2827837ns CPU2: 0x40002668  st   %l3, [%o2 + %o5]
             ...
```

Fig. 10. This figure depicts the identified sequence of instructions that provoked the marked power consumption peak from Fig. 9. The online verification unit stopped the DUT. The test bench operator is able to analyze step-by-step the cause and the propagation of this power bug.

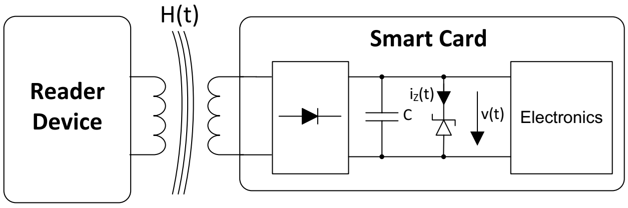


Fig. 11. Principle of a smart card / reader system. The reader generates a magnetic field, which is used to power the smart card and for communication purposes. The capacitor stores electrical energy and the Zener diode prevents the electronics from power surges.

The smart card design presented in this case study supports basic DVFS power management functionalities. The CPU's clock frequency $f(t)$ and voltage $V_{DD}(t)$ parameters can be modified programmatically. If power management algorithms are applied correctly, power consumption, and supply voltage hazards can be minimized.

A. 13.56 MHz Contactless Smart Card Power Network

Fig. 12 depicts the equivalent circuit of a contactless smart card's power network using a 13.56 MHz magnetic field, as presented by the authors in [22]. An implementation of a smart card power network model has been demonstrated by the authors of [4] using a charge-based approach, according to (6).

$$v(t) = \frac{Q_C(t)}{C} \tag{6}$$

A similar implementation approach has been chosen for the supply voltage estimation unit used in this smart card emulation test bench: the rectified voltage $v_i(t)$ is supplied by the magnetic field and powers the smart card. A Zener diode protects the smart card's electronics from power surges. The capacitor C buffers electrical charges and defines the supply voltage $v(t)$ according to (7). $v(t)$ is supplied to the smart card's electronics.

$$v(t+1) = \frac{Q_C(t) + \frac{v_i(t)-v(t)}{R_i}\Delta t - i(t)\Delta t}{C} \quad \text{if } v(t) < V_Z \tag{7}$$

Depending on the CPU's power consumption, the capacitor C is charged or discharged. Thus, the supply voltage $v(t)$ alters

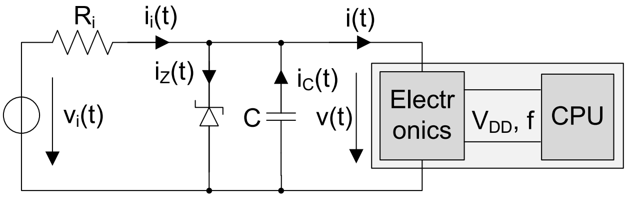


Fig. 12. Equivalent circuit of a smart card power network, obtained with changes from [22]. The rectified voltage $v_i(t)$ is supplied by the magnetic field. Capacitor C buffers electrical energy during undersupply periods and a Zener diode protects the electronics from power surges.

accordingly: if the smart card CPU's power consumption is too high, the voltage $v(t)$ drops consequently. If this supply voltage $v(t)$ drops below a certain hazardous threshold, the functionality of the smart card's electronics is compromised. According to [22] and [4], an average power estimation error of 8.4% and an average supply voltage estimation of 2% are introduced by the presented smart card power network model.

B. Results

The emulation test bench for a RF-powered contactless smart card has been integrated in a Xilinx Spartan 3 FPGA board. The smart card design is tested with an AES encryption application. Fig. 13 shows the smart card's behavior while applying a clock frequency of 31 MHz. According to the monitored power consumption profile, the application's initialization phase and three AES encryptions are identifiable. The supply voltage drops hazardously below a level of 1 V as soon as the calculation intense AES encryption algorithm starts. Thus, the smart card's operational stability would be compromised. Supply voltage breakpoints are triggered by the emulation test bench and the faulty source code can be identified. The fact that the tested smart card design supports DVFS functionalities, the demonstrated instability can be resolved by reducing the smart card CPU's clock frequency. Fig. 14 depicts this approach. After the application's initialization phase is finished, the smart card CPU's clock frequency is reduced to 25 MHz programmatically within the application's source code. Thus, the power consumption of the calculation intense AES encryption algorithm is reduced and no hazardous supply voltage drop occurs. The smart card's operational stability is given. Because the clock frequency is reduced to 25 MHz, the total execution time of the benchmark application is increased by 17%.

TABLE II
EMULATION TEST BENCH AREA CONSUMPTION BREAKDOWN.

Component	Area Overhead
Configure and Control Unit	60%
Power Estimation Unit	8.1%
Supply Voltage Estimation Unit	5.5%
Online Verification Unit	4.2%

The presented smart card specific emulation test bench requires an additional area overhead of 77%. A detailed area breakdown is depicted by Table II. The highest amount of area is required by the configure and control unit, because it implements a processor core to ease configuration and control tasks. These results are gained from synthesis on a Xilinx Spartan 3 FPGA platform.

The presented smart card specific power estimation and supply voltage estimation units can also be used in a smart card ASIC for high sophisticated on-chip power management. With the help of these analysis units and DVFS techniques, a smart card's operational stability can be optimized. Hence, these units are downsized to implement only the most important functionality. Verification and control units are omitted.

VI. Conclusion

Test and verification are indispensable tasks during a hardware's development process. Simulation and functional hardware emulation approaches are commonly used for these purposes. However, not all design and application issues can be verified practicably, like hazardous peak power consumption or supply voltage drops.

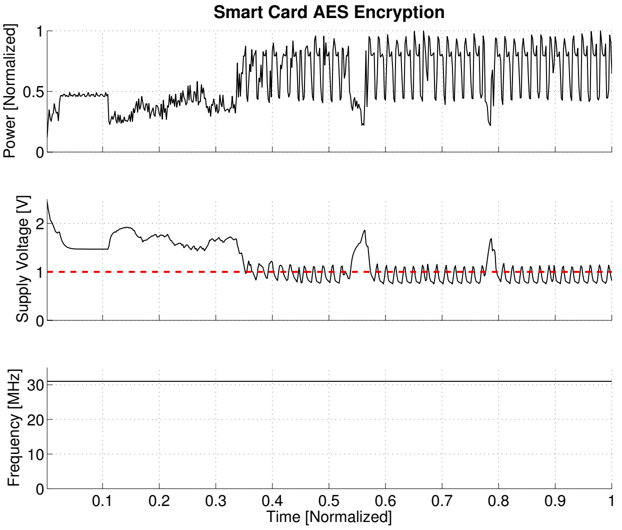


Fig. 13. This figure illustrates a RF-powered contactless smart card performing an AES encryption benchmark. During the AES encryption rounds high power consumption peaks cause hazardous supply voltage drops, which would compromise the smart card's stability.

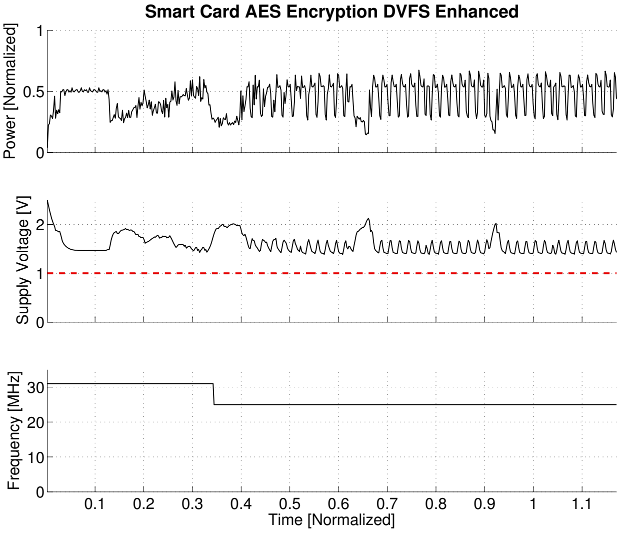


Fig. 14. This figure depicts the usage of the RF-powered contactless smart card's DVFS functionality. During the AES encryption rounds the power consumption is reduced and hazardous supply voltage drops are minimized. The smart card's operational stability is preserved.

This paper presents a comprehensive emulation methodology: the functional hardware emulation approach is enhanced with model-based analysis techniques and real-time verification capabilities. Such a comprehensive emulation test bench is constructed by integrating a DUT as well as additional analysis and verification units into a FPGA-based prototyping platform. Thus, the DUT's functional, performance, power consumption, and supply voltage behavior can be analyzed online, cycle accurately, and in real-time. A hardware integrated online verification unit monitors and verifies the gathered analysis data according to predefined constraints. Functional, performance, power, and supply voltage breakpoints can be defined for innovative hardware debugging purposes. If triggered, the responsible sequence of instructions can be determined.

The presented case studies depict the suitability of our emulation methodology to detect application and hardware design bugs affecting functional, performance, power, and supply voltage behaviors already during a product's design phase. As an example of application, a LEON3 multi-core processor system is verified. A dedicated emulation test bench reveals power supply issues if the LEON3's power consumption rises. A second case study verifies the design of a RF-powered contactless smart card. The presented smart card test bench is able to detect hazardous supply voltage drops. The usage of power and supply voltage breakpoints reveals the responsible source code sequences. Based on the gained debug information, the source code is adapted to reduce the processor's clock frequency programmatically. Thus, the smart card's operational stability is regained.

Our future work concerns the integration of fault effect analysis into our design space exploration framework. This is accomplished by adding emulation-based fault injection techniques to our comprehensive design space exploration framework. Thus, faults affecting a DUT's functionality, performance, power, and supply voltage can be evaluated already during the design phase.

ACKNOWLEDGMENTS

We would like to thank our industrial partners Infineon Technologies Austria AG as well as Enso Detego GmbH for their support.

REFERENCES

[1] C. Chang, K. Kuusilinna, B. Richards, A. Chen, N. Chan, R. Brodersen, and B. Nikolic, "Rapid Design and Analysis of Communication Systems Using the BEE Hardware Emulation Environment," in *IEEE International Workshop on Rapid Systems Prototyping*, June 2003, pp. 148–154.

[2] G. Ganapathy, R. Narayan, C. Jorden, M. Wang, and J. Nishimura, "Hardware Emulation for Functional Verification of K5," in *Design Automation Conference*, June 1996, pp. 315–318.

[3] E. Grochowski, D. Ayers, and V. Tiwari, "Microarchitectural simulation and control of di/dt-induced power supply voltage variation," in *Proceedings of the 8th International Symposium on High Performance Computer Architecture*, February 2002, pp. 7–16.

[4] N. Druml, A. Genser, J. Haid, C. Steger, and R. Weiss, "Estimation Based Power and Supply Voltage Management for Future RF-Powered Multi-Core Smart Cards," in *Design Automation and Test in Europe Conference and Exhibition*, March 2012, pp. 358–363.

[5] A. Genser, C. Bachmann, J. Haid, C. Steger, and R. Weiss, "Supply Voltage Emulation Platform for DVFS Voltage Drop Compensation Explorations," in *IEEE International Symposium on Performance Analysis of Systems and Software*, April 2011, pp. 129–130.

[6] K. Ganesan, L. John, V. Salapura, and J. Sexton, "A Performance Counter Based Workload Characterization on Blue Gene/P," in *International Conference on Parallel Processing*, September 2008, pp. 330–337.

[7] R. Bergamaschi, G. Han, A. Buyuktosunoglu, H. Patel, I. Nair, G. Dittmann, G. Janssen, N. Dhanwada, Z. Hu, P. Bose, and J. Darringer, "Exploring Power Management in Multi-Core Systems," in *Asia and South Pacific Design Automation Conference*, March 2008, pp. 708–713.

[8] R. Joseph and M. Martonosi, "Run-Time Power Estimation in High Performance Microprocessors," in *International Symposium on Low Power Electronics and Design*, 2001, pp. 135–140.

[9] J. Coburn, S. Ravi, and A. Raghunathan, "Power Emulation: A New Paradigm for Power Estimation," in *Design Automation Conference, Proceedings*, June 2005, pp. 700–705.

[10] M. Holtz, S. Narasimhan, and S. Bhunia, "On-Die CMOS Voltage Droop Detection and Dynamic Compensation," in *Proceedings of the 18th ACM Great Lakes symposium on VLSI*, 2008, pp. 35–40.

[11] T. Nakura, M. Ikeda, and K. Asada, "Preliminary Experiments for Power Supply Noise Reduction using Stubs," in *Asia-Pacific Conference on Advanced System Integrated Circuits*, August 2004, pp. 286–289.

[12] E. Alon, V. Stojanovic, and M. Horowitz, "Circuits and Techniques for High-Resolution Measurement of On-Chip Power Supply Noise," *IEEE Journal of Solid-State Circuits*, vol. 40, no. 4, pp. 820–828, April 2005.

[13] P. F. Sweeney, M. Hauswirth, B. Cahoon, P. Cheng, A. Diwan, D. Grove, and M. Hind, "Using hardware performance monitors to understand the behavior of java applications," in *Proceedings of the 3rd Conference on Virtual Machine Research And Technology Symposium*, 2004.

[14] F. Bellosa, "The Benefits of Event-Driven Energy Accounting in Power-Sensitive Systems," in *Proceedings of the 9th ACM SIGOPS European Workshop*, 2000.

[15] A. Bhattacharjee, G. Contreras, and M. Martonosi, "Full-System Chip Multiprocessor Power Evaluations Using FPGA-Based Emulation," in *ACM/IEEE International Symposium on Low Power Electronics and Design (ISLPED)*, August 2008, pp. 335–340.

[16] P. Del Valle, D. Atienza, I. Magan, J. Flores, E. Perez, J. Mendias, L. Benini, and G. De Micheli, "Architectural Exploration of MPSoC Designs Based on an FPGA Emulation Framework," in *Proceedings of XXI Conference on Design of Circuits and Integrated Systems (DCIS)*, November 2006, pp. 12–18.

[17] P. Meloni, S. Secchi, and L. Raffo, "An FPGA-Based Framework for Technology-Aware Prototyping of Multicore Embedded Architectures," *IEEE Embedded Systems Letters*, vol. 2, no. 1, pp. 5–9, March 2010.

[18] A. Bogliolo, L. Benini, and G. De Micheli, "Regression-based RTL power modeling," in *Transactions on Design Automation of Electronic Systems*, vol. 5, no. 3, July 2000, pp. 337–372.

[19] C. Bachmann, A. Genser, J. Haid, C. Steger, and R. Weiss, "Automated Power Characterization for Run-Time Power Emulation of SoC Designs," in *DSD*, September 2010, pp. 587–594.

[20] Aeroflex Gaisler, *GRLIB IP Core User's Manual Version 1.1.0 - B4108*, 2011.

[21] M. R. Guthaus, J. S. Ringenberg, D. Ernst, T. M. Austin, T. Mudge, and R. B. Brown, "MiBench: A free, commercially representative embedded benchmark suite," in *IEEE International Workshop on Workload Characterization*, December 2001, pp. 3–14.

[22] M. Wendt, C. Grumer, C. Steger, and R. Weiss, "System Level Power Profile Analysis and Optimization for Smart Cards and Mobile Devices," in *ACM Symposium on Applied Computing*, 2008, pp. 1884–1888.

Emulation-Based Design Evaluation of Reader / Smart Card Systems

Norbert Druml, Manuel Menghin, Daniel Kroisleitner,
Christian Steger, Reinhold Weiss
Institute for Technical Informatics
Graz University of Technology
Graz, Austria
{norbert.druml, manuel.menghin, steger, rweiss}@tugraz.at
daniel.kroisleitner@student.tugraz.at

Holger Bock, Josef Haid
Design Center Graz
Infineon Technologies Austria AG
Graz, Austria
{holger.bock, josef.haid}@infineon.com

***Abstract*—Design exploration and evaluation are essential tasks during a product's development cycle. Simulation and hardware emulation are common techniques to explore and evaluate the functionality of hardware / software designs. However, when it comes to distributed secure applications, like contactless reader / smart card systems, non-functional design properties and system aspects (e.g., conctactless power transfer, power consumption) have to be regarded too. State-of-the-art simulation-based and emulation-based design exploration tools cover these design issues and system aspects only to some extent.**

Here we present a design exploration framework for complete reader / smart card systems using state-of-the-art model-based emulation and estimation techniques. This novel system-based approach is of high importance because of the high availability of battery powered mobile readers (i.e. smart phones) and novel mobile application fields. Contactless power transfer and power consumption analyses of reader and smart cards can be performed for each clock cycle and in real time. Thus, novel system-level power and security optimization techniques can be evaluated considering the reader / smart card system as a whole. We demonstrate the application of our exploration framework by means of a typical Diffie-Hellman key exchange between reader and smart card and highlight power optimization possibilities.

***Index Terms*—Design Exploration, Hardware Emulation, Power Emulation, RF Channel Emulation**

I. Introduction

The number of available mobile battery-powered RFID and Near Field Communication (NFC)-enhanced readers (i.e. smart phones) and mobile applications has increased drastically during the last years. Such applications can be found in our everyday life, e.g., in the fields of transportation, payment, loyalty and coupons, logistics, healthcare, access control. Thus, a reader / smart card system's security and power consumption characteristics are of high importance. Fig. 1 depicts the working principle of such a reader / smart card system. The reader emits an alternating magnetic field, which is used to power the smart card and to exchange data with it. As depicted by Fig. 2, smart cards are very constrained in terms of available electrical power, chip size, and computational resources. During a smart card's peak power consumption or during low magnetic field supply periods, the smart card's supply voltage may drop below a hazardous threshold, which would result in a loss of operational stability. Given these constraints, mobile reader devices commonly use high magnetic field strengths to ensure a proper working smart card. This approach limits the reader's battery lifetime drastically. However, during a smart card's low power consuming period, a reduced magnetic field strength would suffice and would prolong the reader's battery lifetime. Thus, it is imperative to support hardware and software designers with evaluation tools that provide a system-view of reader / smart card systems. This is the only way of evaluating and implementing novel system-level power optimizations and security concepts.

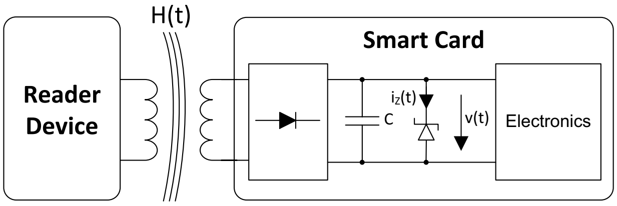


Fig. 1. This figure illustrates the working principle of a reader / smart card system. A reader emits a magnetic field which is used for powering the smart card and for communication purposes. Obtained with changes from [1].

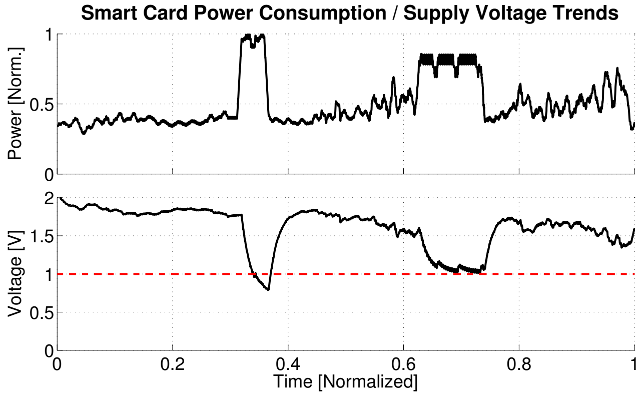


Fig. 2. Power consumption and supply voltage trends of a contactlessly powered smart card. Peak power consumption causes hazardous supply voltage drops. Obtained with changes from [1].

State-of-the-art simulation and emulation tools, which are used for design exploration and evaluation tasks, cover these system-based power and security aspects only to some extent. Our presented reader / smart card exploration framework supports hardware and software developers with accurate system-level power, functional, and RF channel analysis data during the design time. Thus, novel system-level power optimizations and security concepts can be explored and validated. Furthermore, system-level power and security bugs can be found early during a product's development process, which reduces development costs and time-to-market intervals.

This paper makes the following contributions:

- It introduces an innovative emulation-based and estimation-based design exploration approach encompassing complete reader / smart card system designs.
- It features an RF channel model supporting power and data transfer evaluations.
- It demonstrates the evaluation of a typical Diffie-Hellman key exchange by means of the proposed framework and highlights system-level power optimization possibilities.

This paper is structured as follows. Section II gives a short introduction into the related work covering the topics hardware emulation frameworks, hardware accelerated power estimation, and RF power transfer. In Section III our emulation-based design exploration approach is presented. Followed by Section IV demonstrating the evaluation of a Diffie-Hellman key exchange between a reader and an RF-powered smart card. Furthermore, it is demonstrated how our framework is used for rapid software prototyping and verfication tasks. Finally, our results are concluded and some details about our future work are given in Section V.

II. Related Work

A. Functional Hardware Emulation

Hardware emulation is a common technique to evaluate hardware / software designs: the hardware design, which must be available in a synthesizable hardware description language, is integrated into an FPGA-based prototyping platform. Thus, a major performance improvement can be achieved compared to simulation-based approaches. The authors of [2] demonstrated a speed-up of more than 10^6. One of the first hardware emulation approaches, which verified the functionality of the K5 processor, was introduced by the authors of [3]. A technique to evaluate Multi-Processor System-on-Chip (MPSoC) designs was presented by [4]. In [17], the authors depicted another MPSoC emulation framework with particular emphasis on Network-on-Chip (NoC) based systems.

B. Hardware Accelerated Power Estimation

Hardware accelerated power estimation is performed by adding dedicated estimation hardware to a given system. The author of [5] used hardware event counters to estimate the thread specific power consumption of operating systems. Bircher et al. demonstrated in [6] the power characterization of a complete embedded system by means of performance counters. They achieved an estimation error of less than 9%. In [7], the authors augmented the functional hardware emulation technique with hardware performance counters for power analysis purposes. Coburn et al. [8] combined the hardware emulation method with power analysis techniques using register-transfer-level power models. Thus, a hardware accelerated anaylsis method is given, which speeds up power analyses compared to simulation-based techniques. A higher-level power emulation solution was presented by the authors of [9]. They were able to reduce the hardware overhead, but analysis accuracy decreased at the same time. In [1] and [10], the authors used power models and estimation techniques to optimize a smart card's power consumption by means of dynamic voltage and frequency scaling.

C. RF Power Transfer

In [11], the authors outlined the relation between the strength of the reader emitted magnetic field and the maximum communication distance. Further analyses were performed by [12] and the main conclusion was that the maximum power that can be transferred within an NFC-based system from reader to transponder is as high as 100 mW. However, state-of-the-art smart cards are designed to be operated with only a few mW of transferred electrical power. Considering these facts, the authors of [13] proposed a power stepping RFID inventory algorithm to reduce the overall power consumption of RFID readers. In [14], a verification methodology was presented, which evaluates the provided RF power and the actual consumed power of the smart card's electronics. In [15], the authors presented a reader / smart card RF channel simulation framework using high level SystemC models. The power optimization techniques presented there were also verified on a real reader / smart card system.

Especially in the field of mobile and secure reader / smart card systems, it is imperative to regard all system aspects like power transfer, power consumption of reader and smart card, etc. The gap in literature of fast emulation-based design exploration and prototyping frameworks focusing on these important system aspects and regarding complete reader / smart card systems, is addressed in our work.

III. Design Exploration Framework

Fig. 3 depicts the concept of our reader / smart card system design exploration framework. The hardware designs of reader and smart card are integrated into an FPGA prototyping board along with control and model-based analysis units. Functional (executed instructions) and non-functional (power consumption, supply voltage, performance, etc.) traces are gathered for each clock cycle and in real time. These traces are then sent via Ethernet to a host PC for further sophisticated analyses. Given such an exploration framework, software and hardware can be prototyped, tested, and verified rapidly. Furthermore, the presented exploration methodology grants a significant speed-up compared to register-transfer-level simulations.

The architecture of the framework is depicted by Fig. 4. Power sensors are placed throughout the design to gather power consumption estimates for each component of reader

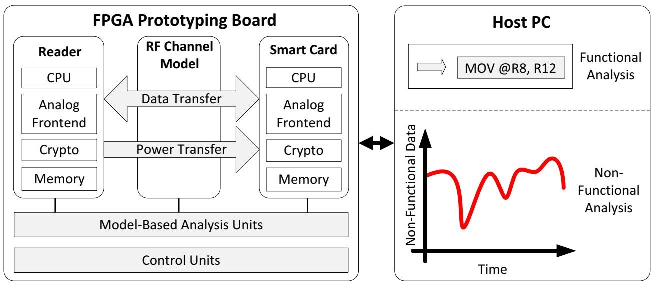


Fig. 3. This figure depicts the concept of our design exploration framework. Reader, smart card, and model-based analysis units are integrated into an FPGA prototyping board along with model-based analysis units. Functional and non-functional traces are transmitted to a host PC for analysis purposes.

and smart card. The smart card's power supply information is estimated by the model-based RF channel emulation approach. A framework controller unit represents the interface to the host PC, controls the reader, smart card, and analysis units, and gathers all available analysis information. In the following, the individual concepts are explained in more detail.

A. Power Emulation

Our power estimation approach is based upon the power emulation technique introduced by [8] and [9]. The working principle of the power estimation unit is depicted by Fig. 5 and is defined by (1) and (2). Power sensors monitor the hardware's internal component states $\mathbf{x}$. Each sensor maps its dedicated component state x_i to a corresponding model coefficient c_i, which defines the amount of dissipated power. The linear combination of $\mathbf{x}$ and $\mathbf{c^T}$ plus a static power consumption c_0 defines the total estimated power consumption. The average estimation error ϵ, which is given by (3), can be as low as 4.71% for a characterized smart card architecture, as highlighted by the authors of [16].

$$\widehat{P}(\mathbf{x}) = \widehat{P}_{stat} + \widehat{P}_{dyn} \tag{1}$$

$$\widehat{P}(\mathbf{x}) = c_0 + \sum_{i=1}^{n} c_i \cdot x_i = c_0 + \mathbf{c^T} \cdot \mathbf{x} \tag{2}$$

$$P(\mathbf{x}) = \widehat{P}(\mathbf{x}) + \epsilon \tag{3}$$

$\mathbf{x}$, $\mathbf{c^T}$, and c_0 are determined during a gate-level power characterization process, which can be performed automatically for any given hardware design, as described by the authors of [16]. The more component states considered during the characterization process, the lower the estimation error ϵ. If the manufactured ASIC hardware of the design-under-test is available, the power model can be further refined with physical measurements to reduce the estimation error.

B. Power Characterization

To determine the power model parameters c_0, $\mathbf{c^T}$, $\mathbf{x}$, and ϵ for a given design-under-test, a power characterization process is conducted. Fig. 6 depicts this power characterization process, which can be performed automatically for any synthesizable hardware design. It is based on an approach presented by [16]. First, the design-under-test, its target technology, and an exhaustive benchmark affecting all design components are selected. Then, gate-level simulations are executed to get the raw activity and power data. Thereafter, this power and activity data needs to be post-processed. During this task, unneeded and redundant data is filtered. Finally, after a regression-based model fitting process, which is similar to the method presented by [17], the relevant power data $\mathbf{c^T}$, c_0, and system states $\mathbf{x}$ are identified. If an ASIC hardware of the design-under-test is already available, the power model can be further refined with power measurements to decrease the power model's estimation error ϵ.

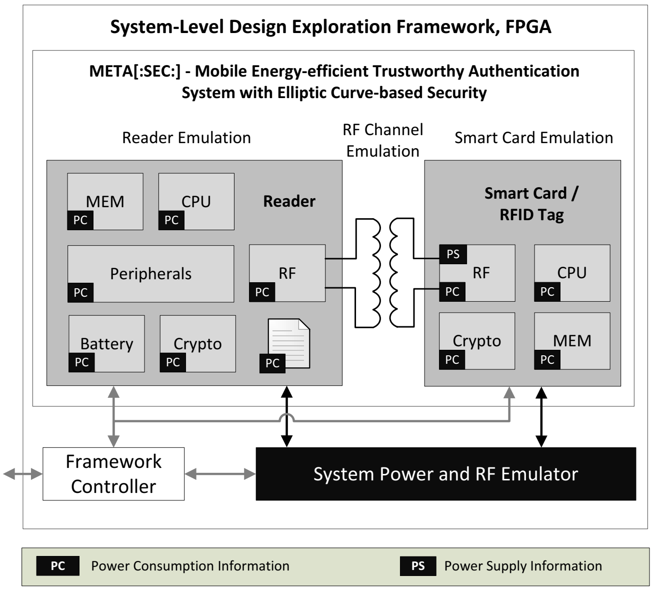

System-Level Design Exploration Framework, FPGA
META[:SEC:] - Mobile Energy-efficient Trustworthy Authentication System with Elliptic Curve-based Security
Reader Emulation
RF Channel Emulation
Smart Card Emulation
MEM
CPU
Reader
Peripherals
RF
Battery
Crypto
Smart Card / RFID Tag
RF
CPU
Crypto
MEM
PC
PS
Framework Controller
System Power and RF Emulator
PC Power Consumption Information
PS Power Supply Information

Fig. 4. Architecture of the reader / smart card evaluation framework. Power sensors gather power estimates from any component of interest. Wireless power and data transfer are modeled by the RF emulation unit. A controller unit is used to configure and control the framework by means of a host PC.

C. RF Power Emulation

An imperative part of this work consists of the emulation of the RF channel between reader and smart card. With the help

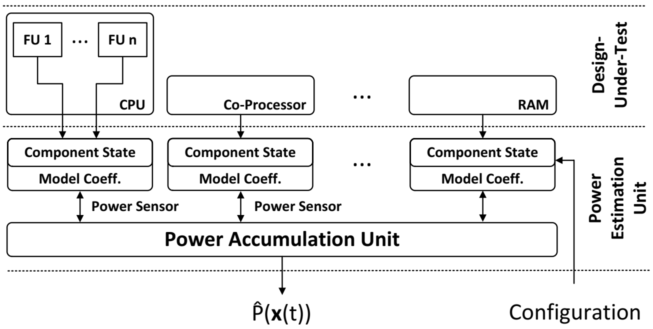


Fig. 5. Working principle of the power emulation approach. Power sensors monitor component states and provide corresponding power estimates. Obtained with changes from [16].

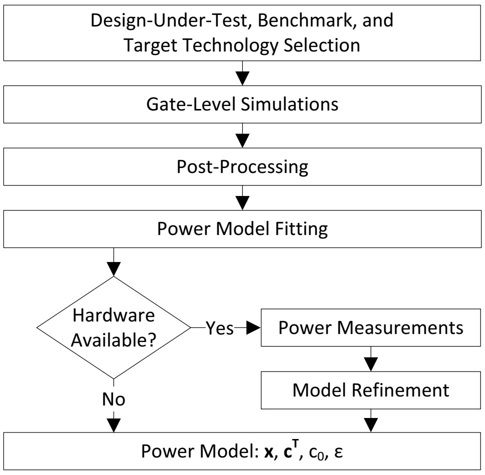


Fig. 6. The used power characterization flow consists of gate-level simulations, post-processing, and model fitting tasks. If a prototype hardware is already available, the power model can be refined, which results in a reduction of the model's estimation error ϵ. Obtained with changes from [16].

of power transfer and data transfer models, the reader / smart card system's behavior can be explored during various physical conditions (e.g., distance, antenna alignments, antenna parameters). Fig. 7 depicts the equivalent circuit of the RF channel's power transfer, according to [18]. This RF channel model is defined by (4), as presented by [15]. The reader sets a magnetic field strength with the help of the fixed voltage v_1 and the adjustable resistance $R_{Rel}(t)$. Electrical power is transferred contactlessly to the smart card by means of inductive coupling and a resonance circuit. k defines the coupling factor between reader and smart card. The total smart card's resistance is given by $R_L(t)$. A shunt resistor, depicted as a Zener diode, prevents the smart card's electronics from power surges and reduces leaking side channel information. After a rectification, which is performed by diodes D1 up to D4, electrical energy is buffered in capacitor C, which defines the crucial voltage $v(t)$. This capacitor C is either charging or discharging depending on the strength of the supplied magnetic field and the changing smart card CPU's power consumption. As a consequence, the voltage level $v(t)$ fluctuates during operation. To guarantee a proper working smart card, it is imperative to prevent $v(t)$ from dropping below a crucial threshold V_T.

$$v_2 = \frac{\omega k\sqrt{L_R L_T}\, i_R}{\sqrt{(\frac{\omega L_T}{R_L} + \omega R_T C_T)^2 + (1 - \omega^2 L_T C_T + \frac{R_T}{R_L})^2}} \qquad (4)$$

However, to integrate a model of an RF channel feasibly in an FPGA prototyping hardware, the presented analytical model needs to be simplified. A feasible simplification approach was presented by the authors of [19]. By measuring the current / voltage characteristics of the reader / smart card system, a Thévenin voltage source can be introduced, which is defined by voltage v_i and resistance R_i. The resulting equivalent circuit is depicted by Fig. 8. This reader / smart card power transfer model accounts for a maximum estimation error of only 2%. As highlighted by the authors in [1] and [15], the voltage level v_i of (5) depends on physical relation parameters like distance d between reader and smart card, antenna characteristics, field strength, orientation of the smart card within the field, etc. The final RF channel model is defined by (6). By using this electrical charge-based approach, the voltage $v(t)$ can be calculated in hardware feasibly.

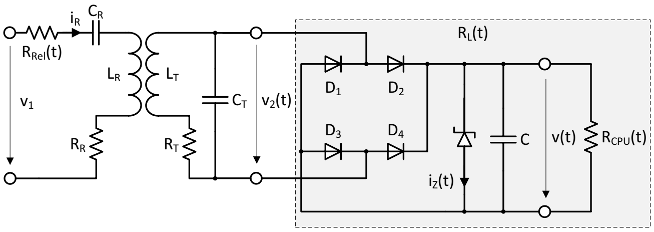


Fig. 7. Equivalent circuit of a reader / smart card system. Power is transferred by means of inductive coupling and resonance circuits. Obtained with changes from [18].

$$v_i(t) = f(d(t), AntennaCharacteristic, ...) \qquad (5)$$

$$v(t+1) = \frac{Q_C(t) + \frac{v_i(t)-v(t)}{R_i}\Delta t - i(t)\Delta t}{C} \quad \text{if } v(t) < V_Z \qquad (6)$$

D. RF Data Emulation

The RF data transfer model features bidirectional FIFOs between reader and smart card hardware. Data rates can be adapted according to the ISO standards. Furthermore, it supports the emulation of a faulty RF channel with increased bit error rates. It is of high importance to test if security related software is resistant against such faulty data transmission conditions.

E. RF Channel Emulation Unit

The final RF channel emulation unit is depicted by Fig. 9. It consists of RF data emulation and RF power emulation units. Bus accesses are provided to configure the individual units and to exchange data between reader and smart card with the help of the data emulation approach. RF power transfer is emulated by defining a certain reader emitted magnetic field strength. Based on the given magnetic field strength value,

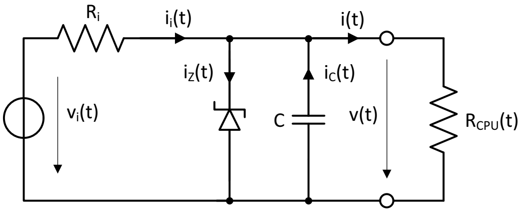


Fig. 8. Simplified equivalent circuit of the reader / smart card power transfer. $v_i(t)$ is defined by the magnetic field. Capacitor C buffers electrical energy and the Zener diode limits the voltage $v(t)$, which is supplied to the electronics. Obtained with changes from [1] and [19].

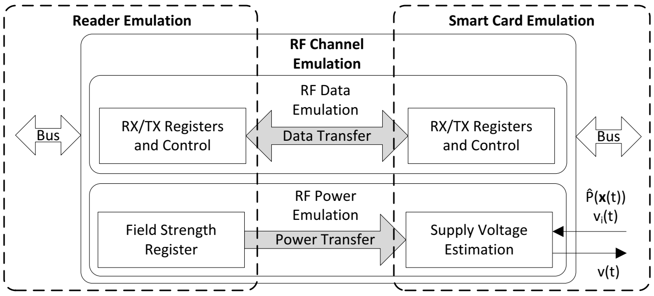


Fig. 9. RF channel emulation unit consisting of RF data emulation and RF power emulation units.

the smart card sets the voltage level of $v_i(t)$, which respects the physical relation (distance, orientation within field, etc.) between reader and smart card. Finally, based on the smart card's power consumption $\widehat{P}(\mathbf{x})$ and $v_i(t)$, the crucial voltage $v(t)$ is calculated hardware accelerated, in real-time, and for each clock cycle according to (6).

F. Framework Controller

The framework controller represents the interface between the user and the emulation framework. It is accessed from a host PC over Ethernet and is responsible to configure and control all analysis units and designs-under-test. To ease these configuration and controlling tasks, it implements a dedicated processor core. It gathers and buffers all analysis data and forwards it to the host PC for further evaluation tasks. Furthermore, to facilitate software verification tasks, predefined conditions can be set (e.g., the smart card's supply voltage must be higher than 1 V during operation). If such a condition is violated, the emulation framework is paused. Such functionality supports hardware and software designers the find the root causes of identified issues.

IV. Case Studies

A. Case Study - Key Exchange

This case study evaluates a typical Diffie-Hellman key exchange procedure between a reader and a smart card in terms of power consumption and timing. Due to security related disclosure policies, the original reader / smart card designs were adapted. Both reader and smart card hardware designs were exchanged with LEON3-based designs. LEON3 is a SPARC V8 open source processor [20]. Fig. 10 illustrates the used key exchange procedure. Reader and smart card decide on using the public information g and p. Reader generates A based on its secret a and sends it to the smart card. The smart card computes B based on its secret b and sends it to the reader. Both reader and smart card are then capable to compute the shared secret s.

Fig. 11 depicts the power and voltage analyses of this case study. $\widehat{P}_R$ represents the reader's power consumption. After computing and sending A, it waits for the smart card's response. During this period, the reader's power consumption is reduced. When the reader receives the response, it computes

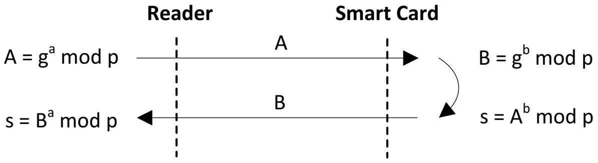


Fig. 10. Use case of a Diffie-Hellman key exchange between reader and smart card.

the shared secret s and as a result its power consumption rises again. $\widehat{P}_{SC}(t)$ denotes the smart card's power consumption. During idle times, the smart card stays in a sleep state and consumes very low power. $\widehat{P}_Z(t)$ shows the power consumption trend of the smart card's Zener diode. Any power dissipated by this component can be considered as wasted power, which could be saved by the reader. Therefore, one aims to keep $\widehat{P}_Z(t)$ as low as possible to make the reader / smart cart system more efficient in terms of electrical energy usage. This efficiency analysis is of high importance if a battery-operated mobile reader is given. The voltage trends are shown by the last graph. $v_i(t)$ denotes the voltage which is provided by the magnetic field, V_Z represents the Zener voltage, and V_T shows the crucial electronics' threshold voltage. If $v(t)$ drops below V_T, the smart card's operational stability will be lost. In summary, the smart card is operated properly (no $v(t)$ voltage drops below V_T) but inefficiently ($\widehat{P}_Z(t) > 0$).

Based on the presented traces, a system engineer is able to analyze the reader / smart card system's power and timing behavior and is able to explore system-level optimization possibilities. To increase the system's power consumption efficiency, the strength of the reader emitted magnetic field could be adapted according to the smart card's power requirements:

- During the smart card's sleep state, a minimized magnetic field strength is supplied thanks to the reduced power supply requirements.
- The power requirements for each smart card request are evaluated and maximum transmission ranges are defined. The reader then adapts the magnetic field to fulfill these power requirements. For example, high power consuming cryptographic operations require higher magnetic field strengths than operations accessing only the smart card's memory.

Due to the lower emitted magnetic field strengths, the reader's power consumption is then reduced as well. This idealized approach is depicted by Fig. 12. $v_i(t)$ is lowered during the smart card's idle times and is only increased if the smart card is performing the power intense Diffie-Hellman calculations. According to the presented power and voltage traces, $v(t)$ stays above the crucial threshold V_T and $\widehat{P}_Z(t)$ is minimized. Thus, the smart card is operated in a stable state and the reader's battery life time can be prolonged at the same time. If such a system-level power optimization technique is deployed on a real reader / smart card system, energy savings of more than 26% are achievable, as demonstrated in [15].

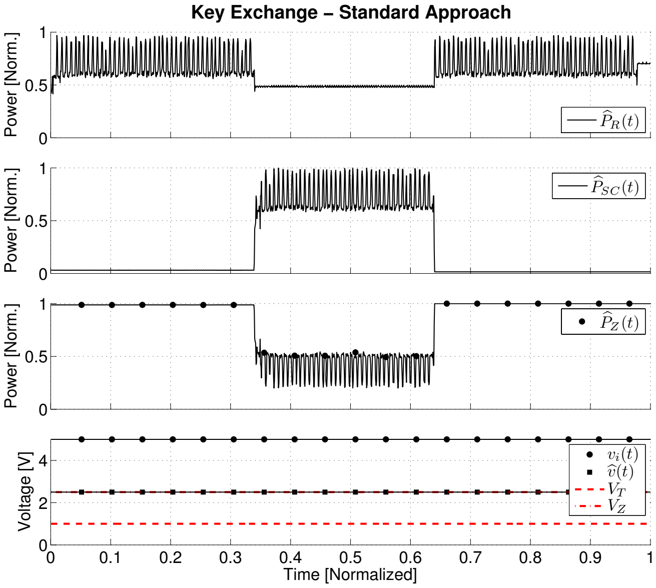


Fig. 11. Power and voltage traces of a typical Diffie-Hellman key exchange procedure. The reader emits a magnetic field of high strength and is unaware of the smart card's low power consuming periods. Thus, power $P_Z(t)$ is wasted within the smart card's protection circuit.

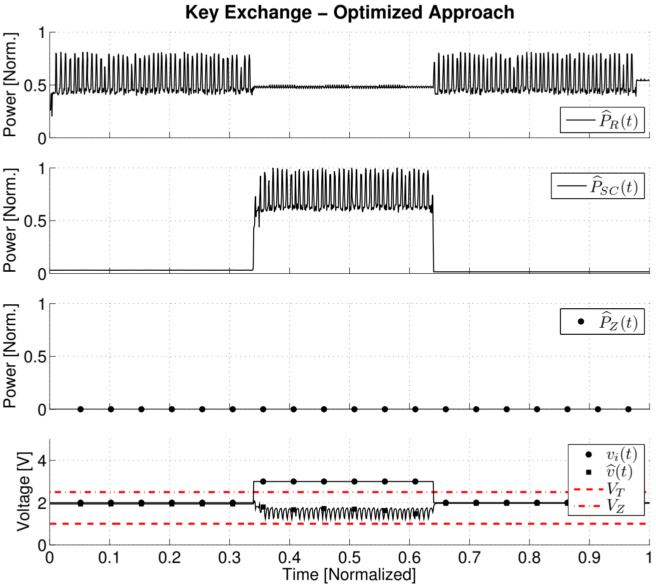


Fig. 12. Optimized Diffie-Hellman key exchange procedure. The reader is aware of the smart card's low power consuming periods and decreases the magnetic field $v_i(t)$ accordingly. Only during high power consuming periods, the magnetic field is increased. Thus, power can be saved by the reader.

B. Case Study - Faulty Key Exchange, Software Verification

Besides software and hardware design explorations, the presented reader / smart card emulation framework can also be used for rapid software prototyping and verification tasks. For this purpose, the manufactured hardware is characterized precisely, by considering a lot of component states, according to the presented characterization flows. Thus, the provoked estimation error ϵ is minimized.

Fig. 13 illustrates the non-functional verification of a faulty key exchange software implementation. The traces of the smart card's supply voltage $v(t)$ as well as voltage $v_i(t)$, which depends on the magnetic field strength, show sharp drops. Because $v(t)$ drops below the crucial V_T threshold, an important verification rule is violated. The smart card faces a power starvation period and its stability is not provided anymore. The software developer is now able to analyze the functional traces (executed instructions) and non-functional traces. By repeating the tests and defining functional or non-functional breakpoints, the software developer is able to find the potential root cause of such an error.

If this test was performed on a real reader / smart card system, this smart card power supply violation would not be found because of the following reasons:

- The smart card's emergency power management precautions (e.g., pausing the clock) would be able to compensate the power starvation period. Thus, the software developer would not recognize any power starvation issues. However, the capabilities of these compensation circuits are limited and would fail for longer lasting starvation periods.
- If the distance between reader and smart card is shorter than intended, the smart card will receive more electrical power. Therefore, there will not be any power starvation.

C. FPGA Area Overhead

Table I highlights the FPGA area needed by our reader / smart card emulation framework, based on a Xilinx Virtex-6 LX240T synthesis. The total area overhead of all analysis, control, and debug units is as high as 5654 slices and 9461 LUTs. The high amount of area needed by the control and debug units is due to the integration of a processor core to ease control and debugging tasks.

V. Conclusion

Design exploration and evaluation represent essential tasks during a product's development process. In the application field of mobile, contactlessly powered, and secure reader / smart card systems, it is imperative to regard system aspects like power transfer, power consumption, security, etc. to provide a proper working system. However, state-of-the-art design evaluation approaches consider these system aspects only to some extent. Furthermore, recent mobile reader devices operate smart cards with a high magnetic field strength without respecting a smart card's low power consuming periods. By disregarding these important system aspects, battery lifetime of mobile readers is reduced drastically.

TABLE I
Framework - FPGA Area Consumption Breakdown

Component	Slices	LUTs
Reader Model (LEON3-Based)	3829	7574
Smart Card Model (LEON3-Based)	3834	7576
Power Estimation Units	260	497
RF Power Transfer Model	216	609
RF Data Transfer Model	430	428
Control and Debug Units	4748	7927
Total Area Overhead	5654	9461

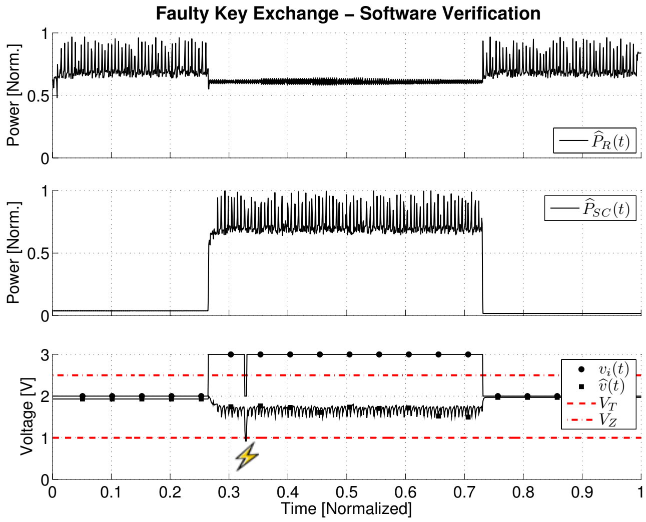


Fig. 13. Rapid software prototyping and verification: an error in the reader's software causes a drop of the magnetic field's strength. The smart card's supply voltage drops therefore below the crucial threshold and its operational stability is not provided anymore.

This paper presents a design exploration framework for reader / smart card systems. By emulating reader, smart card, and a model of the RF interface, an important system view is provided to hardware and software developers early during the product's development process. The framework supports state-of-the-art power estimation techniques to provide power consumption and power transfer information of reader, smart card, and the RF channel. Functional and non-functional traces are acquired for each clock cycle and in real time. Thus, novel system-based power and security optimization techniques can be explored and evaluated. We depict the feasible application of our framework by means of a typical reader / smart card key exchange procedure. We demonstrate the exploitation of the smart card's low power consuming periods to reduce the reader's magnetic field and thus to prolong the reader's battery lifetime.

Our future work concerns the integration of fault effect analysis into our reader / smart card system exploration framework. This is accomplished by adding emulation-based fault injection techniques. Thus, faults affecting the reader's or the smart card's functionality, performance, power consumption, and power supply can be evaluated early during the design phase.

Acknowledgments

We would like to thank the Austrian Federal Ministry for Transport, Innovation, and Technology, which funded the project META[:SEC:] under the FIT-IT contract 829586. Furthermore, we would like to thank our industrial partners Infineon Technologies Austria AG as well as Enso Detego GmbH for their support.

References

[1] N. Druml, C. Steger, R. Weiss, A. Genser, and J. Haid, "Estimation Based Power and Supply Voltage Management for Future RF-Powered Multi-Core Smart Cards," in *Design Automation and Test in Europe Conference and Exhibition (DATE)*, March 2012, pp. 358–363.

[2] C. Chang, K. Kuusilinna, B. Richards, A. Chen, N. Chan, R. Brodersen, and B. Nikolic, "Rapid Design and Analysis of Communication Systems Using the BEE Hardware Emulation Environment," in *IEEE International Workshop on Rapid Systems Prototyping (RSP)*, June 2003, pp. 148–154.

[3] G. Ganapathy, R. Narayan, C. Jorden, M. Wang, and J. Nishimura, "Hardware Emulation for Functional Verification of K5," in *Design Automation Conference (DAC)*, June 1996, pp. 315–318.

[4] P. Del Valle, D. Atienza, I. Magan, J. Flores, E. Perez, J. Mendias, L. Benini, and G. De Micheli, "Architectural Exploration of MPSoC Designs Based on an FPGA Emulation Framework," in *Proceedings of XXI Conference on Design of Circuits and Integrated Systems (DCIS)*, November 2006, pp. 12–18.

[5] F. Bellosa, "The Benefits of Event-Driven Energy Accounting in Power-Sensitive Systems," in *Proceedings of the 9th workshop on ACM SIGOPS European workshop: beyond the PC: new challenges for the operating system*, 2000, pp. 37–42.

[6] W. Bircher and L. John, "Complete System Power Estimation: A Trickle-Down Approach Based on Performance Events," in *IEEE International Symposium on Performance Analysis of Systems Software (ISPASS)*, 2007, pp. 158–168.

[7] A. Bhattacharjee, G. Contreras, and M. Martonosi, "Full-System Chip Multiprocessor Power Evaluations Using FPGA-Based Emulation," in *ACM/IEEE International Symposium on Low Power Electronics and Design (ISLPED)*, August 2008, pp. 335–340.

[8] J. Coburn, S. Ravi, and A. Raghunathan, "Power Emulation: A New Paradigm for Power Estimation," in *Design Automation Conference (DAC)*, June 2005, pp. 700–705.

[9] A. Genser, C. Bachmann, J. Haid, C. Steger, and R. Weiss, "An Emulation-Based Real-Time Power Profiling Unit for Embedded Software," in *International Conference on Embedded Computer Systems: Architectures, Modeling and Simulation*, July 2009.

[10] N. Druml, M. Menghin, C. Steger, R. Weiss, A. Genser, H. Bock, and J. Haid, "Emulation-Based Test and Verification of a Design's Functional, Performance, Power, and Supply Voltage Behavior," in *21st Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP)*, 2013, pp. 328–335.

[11] D. Cheng, Z. Wang, and Q. Zhou, "Analysis of Distance of RFID Systems Working under 13.56MHz," in *4th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM)*, October 2008, pp. 1–3.

[12] E. Strommer, M. Jurvansuu, T. Tuikka, A. Ylisaukko-oja, H. Rapakko, and J. Vesterinen, "NFC-Enabled Wireless Charging," in *4th International Workshop on Near Field Communication (NFC)*, March 2012, pp. 36–41.

[13] X. Xu, L. Gu, J. Wang, G. Xing, and S.-C. Cheung, "Read More with Less: An Adaptive Approach to Energy-Efficient RFID Systems," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 8, pp. 1684–1697, 2011.

[14] J. Mercier, C. Dufaza, and M. Lisart, "Signoff Power Methodology for Contactless Smartcards," in *ACM/IEEE International Symposium on Low Power Electronics and Design (ISLPED)*, August 2007, pp. 407–410.

[15] M. Menghin, N. Druml, C. Steger, R. Weiss, H. Bock, and J. Haid, "Using field strength scaling to save energy in mobile HF-band RFID-systems," *EURASIP Journal on Embedded Systems*, no. 1, 2013.

[16] C. Bachmann, A. Genser, J. Haid, C. Steger, and R. Weiss, "Automated Power Characterization for Run-Time Power Emulation of SoC Designs," in *13th Euromicro Conference on Digital System Design (DSD)*, September 2010, pp. 587–594.

[17] A. Bogliolo, L. Benini, and G. De Micheli, "Regression-based RTL power modeling," in *Transactions on Design Automation of Electronic Systems*, vol. 5, no. 3, July 2000, pp. 337–372.

[18] K. Finkenzeller, *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification*, 2nd ed. New York, NY, USA: John Wiley & Sons, Inc., 2003.

[19] M. Wendt, C. Grumer, C. Steger, R. Weiss, U. Neffe, and A. Muehlberger, "System Level Power Profile Analysis and Optimization for Smart Cards and Mobile Devices," in *ACM Symposium on Applied Computing*, November 2008, pp. 118–121.

[20] Aeroflex Gaisler, *GRLIB IP Core User's Manual Version 1.1.0 - B4108*, 2011.

Emulation-Based Fault Effect Analysis for Resource Constrained, Secure, and Dependable Systems

Norbert Druml, Manuel Menghin, Daniel Kroisleitner,
Christian Steger and Reinhold Weiss
Institute for Technical Informatics
Graz University of Technology
Graz, Austria
{norbert.druml, manuel.menghin, steger, rweiss}@tugraz.at
daniel.kroisleitner@student.tugraz.at

Armin Krieg, Holger Bock and
Josef Haid
Design Center Graz
Infineon Technologies Austria AG
Graz, Austria
{krieg.external, holger.bock, josef.haid}@infineon.com

***Abstract*—Testing hardware and software components regarding their fault detection and fault handling capabilities is of vital importance. However, considering the fact that security systems are built using several distributed hardware components (e.g., reader / smart card authentication system), testing each component individually is insufficient. Because novel system-wide multi-fault attack campaigns can be conducted, fault propagation as well as fault handling of the entire system must be regarded. State-of-the-art emulation-based fault analysis approaches neglect this system aspect as well as the fault impact on power dissipation and power supply.**

Here, we present a novel analysis methodology that characterizes the behavior of complete systems during the design phase, in terms of fault handling, power dissipation, and power supply. Emulation-based techniques are applied to provide cycle accurate analysis information of the system-under-test in real time. The presented approach is of importance when it comes to test resource constrained, dependable, and high secure system designs. We demonstrate the application of this approach by means of a reader / smart card authentication system. Furthermore, we show how system level-based multi-fault attacks can be emulated and how the resulting system behavior (e.g., power consumption, power supply, information leakage) can be exploited to extract security relevant information.

***Index Terms*—Fault Emulation, Hardware Emulation, Estimation-based Techniques, Power Analysis**

I. Introduction

Given the cost and time-to-market pressure of novel hardware and software developments, exhaustive test coverage is difficult to achieve. Especially in the field of dependable and high secure systems, test and verification are very important. The authors of [1] and [2] present the challenges when facing the area of secure embedded system designs. These publications highlight the importance to support the system engineers with security-test capabilities already during a product's design state. Functional hardware emulation can be used for this purpose, which is a technique that integrates the synthesizable hardware design into an FPGA prototyping platform. However, functional hardware emulation covers important design and application issues, like hazardous power consumption or power supply alterations, only to some extent. A combination of functional hardware emulation with state-of-the-art estimation-based power consumption, power supply, and information-leakage analyses, enables engineers to test and verify hardware designs as well as dedicated software more precisely. Thus, design and implementation problems can be detected and fixed in time before the tape-out, as demonstrated in [3]. Fig. 1 demonstrates a power emulation of a passively-powered contactless smart card performing an AES encryption benchmark. In this example, peak power consumption affects the electronics' supply voltage stability hazardously, which may disrupt the smart card's functionality if not handled properly.

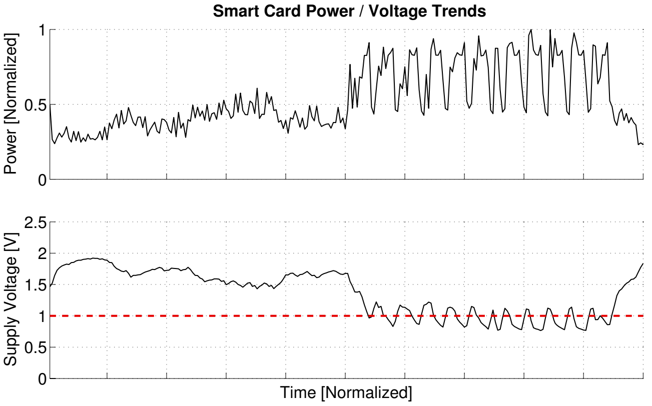


Fig. 1. Power consumption and supply voltage trends of a passively-powered contactless smart card performing AES encryptions. High power consumption peaks cause the capacitor's voltage level to drop. If the voltage drops below a certain threshold, the smart card's operational functionality is compromised.

However, evaluating the behavior of individual components under faulty conditions is insufficient when it comes to distributed high security systems, such as reader / smart card systems. The complete system's behavior must be regarded: for example, multi-attacks, which are conducted on both reader and smart card side simultaneously, could bypass security precautions. Faults within the reader could impact the smart card's power supply and, as a consequence, affect the operational stability of the smart card. Furthermore, significant power consumption changes provoked by intentionally injected faults can reveal security relevant internal countermeasures, e.g., security traps or hardware resets. Because of these threats, it is imperative to provide fast fault injection as well as fault effect evaluation methodologies at system level already during a product's design phase.

This paper makes the following contributions:

- It presents a novel fault effect analysis methodology not only for individual components or chips but for complete system approaches as well.
- State-of-the-art emulation-based and model-based techniques are used to evaluate faults that affect power dissipation, power supply, and information leakage in targeted designs. Cycle accurate analysis information is provided in real time.
- It exemplifies the application of system level fault attack scenarios encompassing and affecting an entire distributed mobile energy-efficient trustworthy authentication system.

This paper is structured as follows. Section II gives a short introduction into the related work covering the topics fault injection and security analysis in application fields of RFID and smart cards. In Section III our fault effect analysis approach is presented. Followed by Section IV demonstrating the fault effect evaluation of an RF-powered reader / smart card system with the help of our approach. Finally, our results are concluded in Section V.

II. Related Work

There is a lot of ongoing research covering the topics of fault awareness and fault injection. If the final hardware is available, faults can be injected either by *software* (e.g., corrupting memory images) or by external sources, such as *radiation*. During a hardware's design phase, faults can be injected by modifying the hardware description. If such hardware description modifications are conducted, fault injections can either be *simulated* or *emulated* on FPGAs. Early fault injection tools and methodologies were proposed by the authors of [4] and [5], focusing on the simulation technique. High level simulation approaches using SystemC were presented by [6] and [7]. Many tools were introduced in the field of software-based fault injection, e.g., FIAT [8] or FERRARI [9]. Further research work focused on modular fault injection controllers [10], automated saboteur as well as mutant placement [11], improving fault injection rates [12], and enhanced multi-level approaches [13].

On the one hand simulation and software-based fault evaluation techniques are flexible and easy to adapt, but on the other hand, they lack in fault injection speeds. A speed-up can be established by using hardware emulation-based injection and evaluation methods, as highlighted by the authors in [12] and [14]. A partial reconfiguration approach was presented by the authors of [15]. In [16], the authors presented a highly parallelized fault emulation approach. Multiple fault emulation platforms are used simultaneously to increase the fault injection rate. Disadvantageous is the usage of netlists, which are available late in the chip design process and represent high security properties in the field of reader / smart card systems.

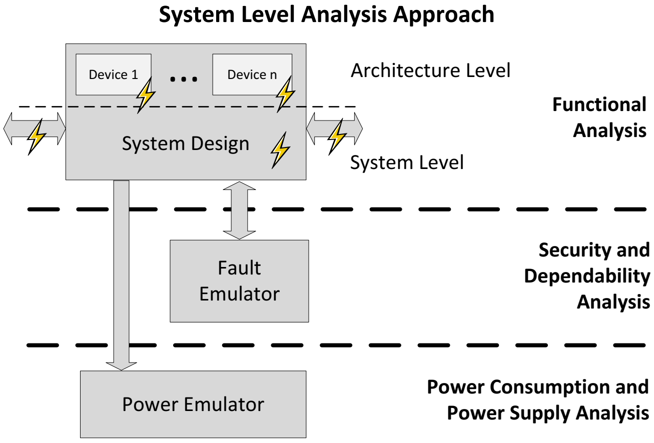


Fig. 2. Concept of the presented system level fault analysis methodology. A system-under-test design is enhanced with various emulator techniques. Thus, functional, fault, power consumption, as well as power supply analyses can be conducted during a system's design phase.

In the application field of RFID-based systems, the authors of [17] summarize feasible fault attacks on the physical device. They demonstrate the vulnerability of such systems by making it possible to write faulty values into tag memories. In [18], the authors highlight sever security issues in the field of RFID-based credit cards. In [19], an FPGA-based RFID-tag development platform was presented, which can be also used for implementing and evaluating security attacks.

However, none of the presented simulation-based or emulation-based research work is able to observe power dissipation and power supply trends during faulty environmental or faulty internal conditions. Furthermore, most of the related work focuses on single fault event evaluations. As the author highlights in [20], proper security evaluations require more complex fault models capable to cope with intentionally injected multiple faults.

III. System Level Fault Effect Analysis Concept

The concept of our system level fault analysis approach is depicted in Fig. 2. The target system, which may consist of several distributed subcomponents, is extended with model-based fault injection, power consumption, and power supply sensor units. Functional, security and dependability, power consumption, and power supply analysis can be performed cycle accurately and in real time. Fig. 3 describes the flow to generate a system level fault effect testbench, which is divided into four phases. At first, the system-under-test, which must be available in a synthesizable hardware description language, and appropriate security as well as dependability constraints are specified. Based on these specifications, power and fault models are generated during the second phase. Phase three augments the target system with the generated models. After the synthesis on FPGA, the attack campaigns are conducted and all gathered functional, fault, power consumption, and power supply trace information is evaluated. In the following paragraph, the individual concepts are described in more detail.

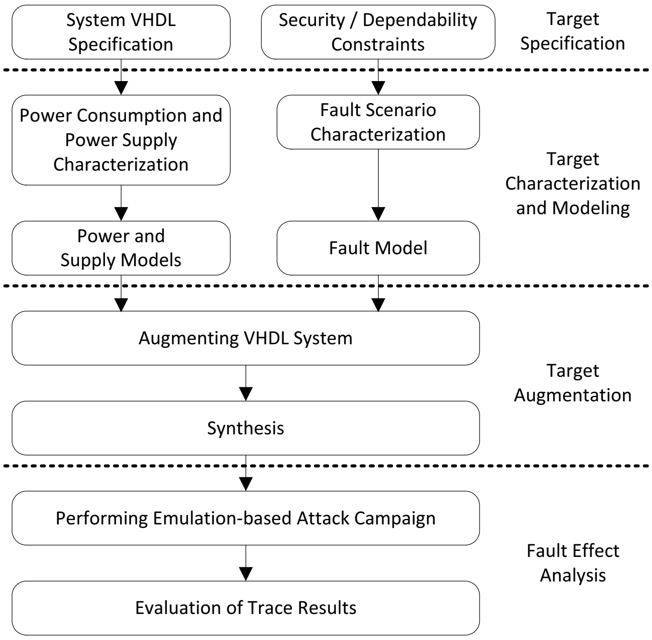

System VHDL Specification
Security / Dependability Constraints
Target Specification
Power Consumption and Power Supply Characterization
Fault Scenario Characterization
Target Characterization and Modeling
Power and Supply Models
Fault Model
Augmenting VHDL System
Target Augmentation
Synthesis
Performing Emulation-based Attack Campaign
Fault Effect Analysis
Evaluation of Trace Results

Fig. 3. Emulation-based fault effect analysis flow, consisting of the phases specification, characterization and modeling, augmentation, and fault effect analysis.

A. Security and Dependability Analysis

Security and dependability analyses are conducted by evaluating and verifying the system-under-test's behavior during intentionally injected faults. Faults can be transient or permanent and are injected either in a simulation of the system-under-test or by adapting the system-under-test to integrate fault-inducing modules or faulty components. The simulation-based approach is very flexible. However, if circuit size and test periods rise, the amount of calculation time needed can increase to a point where getting results in a reasonable amount of time is unfeasible. Thus, the presented system level fault analysis concept favors the adaptation-based analysis approach. The adaptation-based fault injection method modifies the behavior of selected components in the target design, which must be available as synthesizable code. If adaptation-based techniques are used in conjunction with functional hardware emulation, high fault injection rates can be accomplished. However, emulation-based fault injections come at the cost of flexibility loss. Two approaches of adaptation-based fault injections are featured by our concept:

- Mutants are replacements of specific hardware components. Mutants behave like the original hardware until they are triggered. If triggered, the hardware component's functionality is disturbed according to predefined patterns.
- Saboteurs are small hardware components that are plugged into signal lines. Saboteurs behave transparently until they are triggered. If triggered, the signal line is disturbed according to predefined patterns.

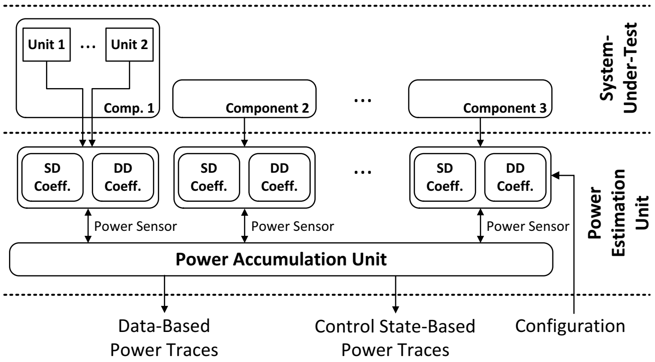


Fig. 4. The power estimation principle: The system-under-test is enhanced with power sensors monitoring the system's state and data activity. Power estimation traces are then forwarded to further analysis units. Obtained with changes from [22].

B. Power Consumption Analysis

A hardware's power consumption represents an important side channel information for security evaluation methodologies, such as Simple Power Analysis (SPA) or Differential Power Analysis (DPA). Furthermore, significant power consumption changes provoked by an injected fault can reveal security relevant countermeasures, e.g., security traps or hardware resets. Thus, security critical code execution can be detected. Our proposed system level fault analysis concept supports state-of-the-art power analyses based on estimation techniques, which can be used during early design phases. Thus, security relevant power information leakage can be evaluated and then, the design can be corrected, if required, in time before its tape-out. Fig. 4 illustrates the power estimation concept used. It is based upon the power emulation principle introduced by [21]. According to (1), (2), and (3) the estimated power consumption $\widehat{P}(\mathbf{x})$ can be subdivided into dynamic and static power $\widehat{P}_{Static}$. The dynamic power itself is composed of state-dependent $\widehat{P}_{StateDynamic}$ (e.g., crypto core active) and data-dependent $\widehat{P}_{DataDynamic}$ (e.g., switching data lines) power dissipation. The data dependency $\widehat{P}_{DataDynamic}$ is introduced to support security relevant power analyses, such as SPA and DPA, which would be unfeasible using only control-based power information. A power characterization process, as described for example by the authors in [22], spots relevant signals / states, x_{si} as well as x_{di}, and associated power coefficients, c_{si} as well as c_{di}. Power sensors finally map the state-dependent (SD) and data-dependent (DD) activity of the system-under-test's components to corresponding power value estimates. A vector-based representation is introduced by (3). The difference between real power $P(\mathbf{x})$ and estimated power $\widehat{P}(\mathbf{x})$ is finally given by ϵ in (4). This average estimation error can be reduced by considering more states and more power coefficients during the characterization process. Finally, these power information traces are then forwarded to attached power evaluation units.

$$\widehat{P}(\mathbf{x}) = \widehat{P}_{Static} + \widehat{P}_{StateDynamic} + \widehat{P}_{DataDynamic} \quad (1)$$

$$\widehat{P}(\mathbf{x}) = c_0 + \sum_{i=1}^{m} c_{si} \cdot x_{si} + \sum_{i=1}^{n} c_{di} \cdot x_{di} \tag{2}$$

$$\widehat{P}(\mathbf{x}) = c_0 + \mathbf{c_s^T} \cdot \mathbf{x_s} + \mathbf{c_d^T} \cdot \mathbf{x_d} \tag{3}$$

$$P(\mathbf{x}) = \widehat{P}(\mathbf{x}) + \epsilon \tag{4}$$

C. Power Characterization

A power characterization process needs to be conducted to determine the power model parameters c_0, $\mathbf{c^T}$, $\mathbf{x}$, and ϵ for a given design. This power characterization process is depicted by Fig. 5 and is based on an approach presented by [23]. Such a power characterization process can be performed automatically for any synthesizable hardware design. At first, the design-under-test, its target technology, and exhaustive benchmark are selected. These benchmarks should affect all design components available by the design-under-test. Then, gate-level simulations are performed. As a result, activity information and power information are gained. This power and activity information is then post-processed by filtering unneeded and redundant information. During the final step, a regression-based model fitting process is conducted, which identifies relevant power information $\mathbf{c^T}$, c_0, and system states $\mathbf{x}$. If a manufactured hardware of the design-under-test is available (e.g., an ASIC), the power model can be further refined with power measurements to decrease the estimation error ϵ.

D. Power Supply Analysis

Reliable hardware operation is, at least, dependant on adequate availability of voltage and power. Power supply analysis is especially important in the field of resource constrained applications. In the case of environment powered smart cards, electrical power is supplied to the smart card by the reader via a time-varying magnetic field of sufficient amplitude. The smart card operation could be compromised if, after the result of a fault in the reader, the magnetic field strength drops below the safe operation level. Furthermore, supply voltage fluctuation could occur in the smart card if it is involved in high power consuming operations, such as cryptographic calculations, without taking into account how much power the reader can give at any given time. It is essential for such a high security hardware to detect and handle these power supply and supply voltage variations properly. Thus, it is mandatory to test a hardware's behavior during harsh and faulty environmental conditions regarding its low power and low supply voltage handling.

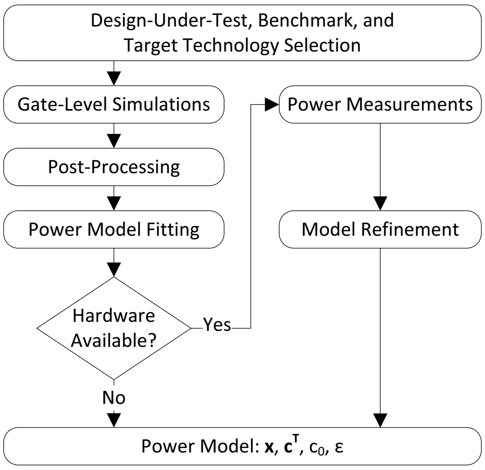


Fig. 5. The used gate-level-based power characterization flow. Obtained with changes from [23].

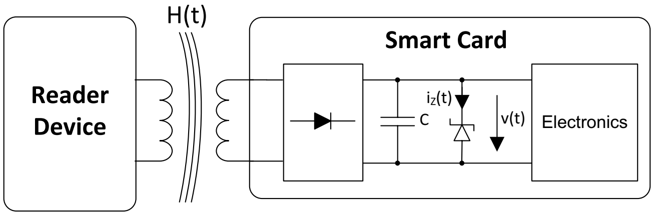


Fig. 6. Working principle of contactless authentication system. The reader emits an alternating magnetic field to power the smart card and to exchange data with it.

Our emulation-based fault effect analysis methodology features power supply analysis by means of emulation-based models. A power supply model is generated by a dedicated characterization process. The characterization process and the resulting power supply model are specific to each system-under-test and need to be implemented by the test bench designer. For example, in the application field of reader / smart card systems, current / voltage characteristics are measured during the characterization process. With the help of these characteristics, a simplified equivalent circuit is developed, which can be feasibly used as an emulation-based power supply model.

IV. Case Study - META[:SEC:]

This case study demonstrates the system level fault emulation methodology's potential by means of the META[:SEC:] project, which focuses on **M**obile **E**nergy-efficient **T**rustworthy **A**uthentication **S**ystems with **E**lliptic **C**urve based **SEC**urity. Fig. 6 illustrates the principle of such a contactless authentication system. A reader device emits an alternating magnetic field, which induces a voltage within the smart card's antenna. This contactless power transfer is used to power the smart card. Data is transmitted by means of magnetic field modulation. A capacitor is used to buffer electrical energy for magnetic field undersupply periods. A shunt resistor, depicted as a Zener diode, prevents the electronics from power surges. Fig. 7 shows the platform's architecture, which is used to evaluate the authentication system's behavior and fault resistance. Reader, smart card, and models of communication interfaces as well as peripheral interfaces are available as synthesizable code. All components, which are relevant for tests and analyses, are extended with fault injection, power consumption sensor, and power supply sensor units. Then, they are integrated into an FPGA along with dedicated control units. A platform controller unit is

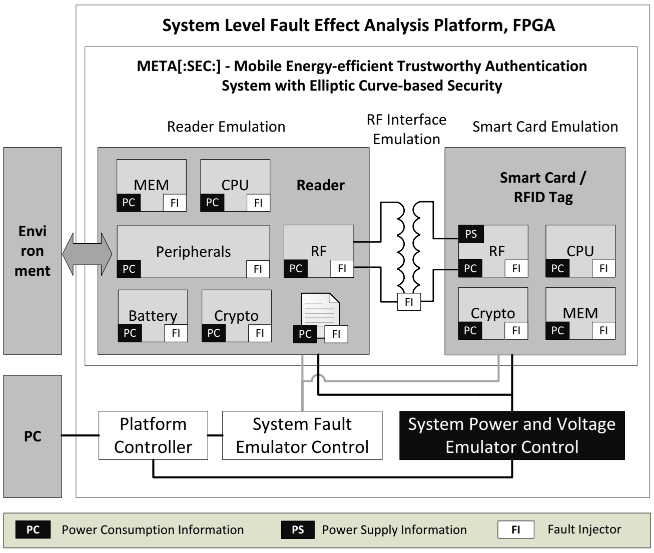

System Level Fault Effect Analysis Platform, FPGA
META[:SEC:] - Mobile Energy-efficient Trustworthy Authentication System with Elliptic Curve-based Security
Reader Emulation
RF Interface Emulation
Smart Card Emulation
Envi ron ment
MEM
CPU
Reader
Peripherals
RF
Battery
Crypto
Smart Card / RFID Tag
PS
RF
CPU
Crypto
MEM
PC
FI
PC
Platform Controller
System Fault Emulator Control
System Power and Voltage Emulator Control
PC Power Consumption Information
PS Power Supply Information
FI Fault Injector

Fig. 7. Architecture of the reader / smart card system fault emulation platform. Reader and smart card designs as well as an RF model are integrated into an FPGA. Components of interest are enhanced with power sensors and fault injectors. Thus, comprehensive information about functional, power consumption, and power supply effects caused by faults can be gathered.

used as interface between test engineer and platform for configuration and online analysis tasks. All gathered analysis data is finally forwarded to a PC for further evaluation tasks. This innovative approach allows a test engineer to implement novel attack scenarios and analysis methods, which are unfeasible if only individual components are considered. In the following section the platform components are described in detail.

A. Power Emulation

Our conducted gate-level-based power characterization process resulted in a power model causing an average estimation error ϵ of 8.4%. If a higher accuracy is needed, this estimation error can be further reduced by considering more states $\mathbf{x}$ and more power coefficients $\mathbf{c^T}$ during the characterization process.

B. Power Supply Emulation - RF Interface Emulation

RF interface emulation units are introduced in both reader and smart card designs. These units model the power as well as the data transfer between reader and smart card. The power transfer model is based upon approaches from [24], [25], and [26], which is depicted in Fig. 8. The magnetic field, which is emitted by the reader, induces a varying voltage within the smart card's antenna. Thus, power is transferred from the reader to the smart card. With the help of measurements the system's current / voltage characteristics are recorded and a Thevenin voltage source, $v_i(t)$ and R_i, is introduced, which models this power transfer (see [25]). Capacitor C buffers the electrical charges. Its charge level $Q_C(t)$ sets the voltage $v(t)$. A shunt resistor, in the form of a Zener diode, protects the adjacent electronics from electric surges. If the smart card's electronics dissipates more electrical power than the magnetic field is able to supply, then the capacitor's charge level decreases and its voltage level $v(t)$ drops accordingly. It is imperative for a smart card's power management to keep its supply voltage always above a safe operation level. If the voltage drops hazardously below this level, the functionality of the smart card's electronics would be compromised. The smart card's RF interface emulation unit implements a charge based mathematical model of the shown equivalent circuit, which is given by (5) and (6). The vital smart card's supply voltage can therefore be estimated with an average estimation error that is as high as 2%.

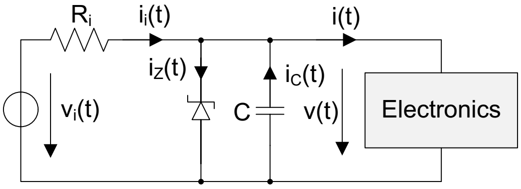


Fig. 8. Simplified equivalent circuit of a contactlessly powered smart card. $v_i(t)$ represents the magnetic field induced and rectified voltage. A Zener diode protects the electronics from electrical surges. The charge level of the capacitor C sets the voltage $v(t)$, which must not drop below a certain threshold. Obtained with changes from [24] and [25].

$$v(t) = \frac{Q_C(t)}{C} \tag{5}$$

$$v(t{+}1) = \frac{Q_C(t) + \frac{v_i(t)-v(t)}{R_i}\Delta t - i(t)\Delta t}{C} \quad \text{if } v(t) < V_Z \tag{6}$$

C. Fault Emulation

Simulation-based and adaptation-based fault emulation techniques are supported by our presented concept. In the presented use case, adaptation-based methods are used to facilitate high fault injection rates. This section presents our fault emulation controller, which is based on work from [10], in a generic way: trigger modules T_n monitor program counters, cache addresses, any signal line of interest, etc. and output a logic high signal if a predefined set of input conditions $f_{Ti}()$ masked by M_{Ti} is met, given by (7). The trigger outputs of T_n are forwarded to the fault emulation controller. $f_{Pi}()$, which is shown by (8), defines which kind of pattern P_i is used, given a certain set of trigger conditions T_n and a mask M_{Pi}. A pattern

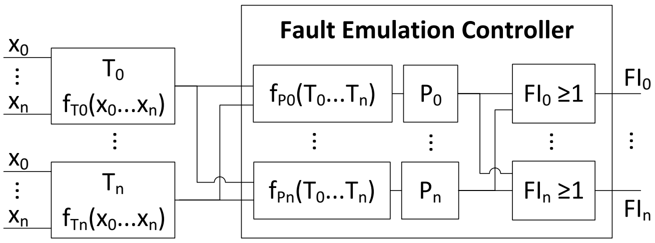


Fig. 9. Generic architecture of the fault emulation controller. Fault injectors FI_n are triggered based on patterns P_n, logical conditions f_{Pn}, and input conditions T_n.

TABLE I
SUPPORTED FAULT MODELS

Fault	Fault Type	Description
Stuck-at-0	Permanent	Signal is set to 0 until reset
Stuck-at-1	Permanent	Signal is set to 1 until reset
Bridging Fault	Permanent	No output propagation until reset
Indetermination	Permanent	Undefined value until reset
Negation of Input	Permanent	Input is negated
Delay	Transient	Delay of input to output
Bit flip	Transient	Flips the value of a signal

P_i represents a table that defines which fault injectors FI_i (i.e. mutants or saboteurs) are activated or deactivated. All pattern outputs, which drive the same fault injector FI_i, are finally combined in a dedicated logical OR element. Fig. 9 depicts the generalized fault injection controller's architecture. During runtime, the masks M_{Tn} and M_{Pn}, patterns P_n, as well as certain trigger settings can be configured by software. Table I summarizes the supported fault models.

$$f_{Ti} = f(x_0, x_1, ..., x_n) \wedge M_{Ti} \quad (7)$$

$$f_{Pi} = f(T_0, T_1, ..., T_n) \wedge M_{Pi} \quad (8)$$

V. EXAMPLES OF APPLICATION

In the following two sections we demonstrate the potential of our fault analysis approach. Multiple faults are injected into the system-under-test, which was presented in the case study section, by means of two attack scenarios. Fault effects on functionality, power consumption, and power supply are analyzed cycle accurately and in real time. There is no fault emulation or fault simulation work, to the best of our knowledge, capable to analyze fault effects in a similar comprehensive, accurate, and rapid way at the same time.

A. Example of Application - Authentication, Replay Attack

This test aims to compromise the emulated reader / smart card system in a specific way to make a replay attack possible. It checks if the emulated reader as well as the smart card hardware and software parts are designed properly to withstand such a replay attack. As the authors of [18] highlight, certain RFID based reader / smart card devices are vulnerable against replay attacks. Fig. 10 and Fig. 11 illustrate the principle flow of a replay attack by means of an asymmetric authentication procedure. The reader transmits a challenge to the smart card. The smart card generates a challenge response based on its internal private key and transmits the result back to the reader. This response is recorded by an attacker device, which is able to monitor any communication conducted within the magnetic field. The reader then verifies this challenge response. If the verification succeeds, the smart card is authenticated. The next time an authentication is performed, the smart card is disturbed. This disturbance is achieved by detuning the magnetic field with the help of the attacker device, which is not powered by the magnetic field. As a consequence, the smart card is not supplied sufficiently. It slows its clock regularly to reduce its power consumption, but enters a power supply trap or is reset after a certain time period of power starvation. After the smart card was disturbed properly, the attacker device sends the recorded challenge response to the reader. The replay attack succeeded, if the attacker device is authenticated at the reader properly.

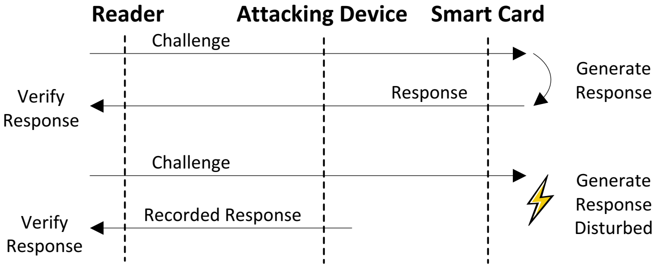


Fig. 10. This figure illustrates the replay attack principle. The smart card's challenge response is recorded by the attacker device. Further smart card challenge responses are disturbed by the attacker device (e.g., by detuning the magnetic field) and the recorded response is sent instead.

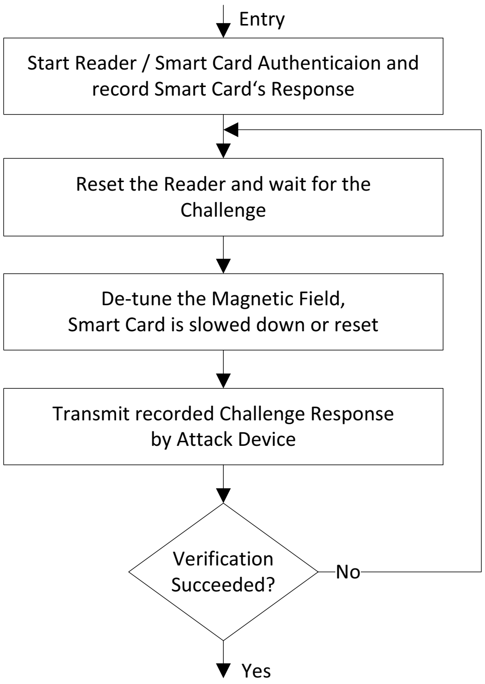

Entry
Start Reader / Smart Card Authenticaion and record Smart Card's Response
Reset the Reader and wait for the Challenge
De-tune the Magnetic Field, Smart Card is slowed down or reset
Transmit recorded Challenge Response by Attack Device
Verification Succeeded?
No
Yes

Fig. 11. Flow graph of the emulated replay attack. After a smart card's challenge response is recorded an attack iteration starts: The reader is reset, the magnetic field is detuned to disturb the smart card, and the recorded challenge response is sent to the reader. If the attacker device is able to authenticate itself at the reader, the attack was successful.

State-of-the-art high security reader / smart card systems are in general resistant against replay attacks. Countermeasures, such as timestamps or one-time numbers, are used. However, besides undetected design bugs in novel products, there are several scenarios that can make reader / smart card systems vulnerable against replay attacks, e.g.:

- Timestamps are derived from the reader's reset event.
- Random number generators may be affected by artificial

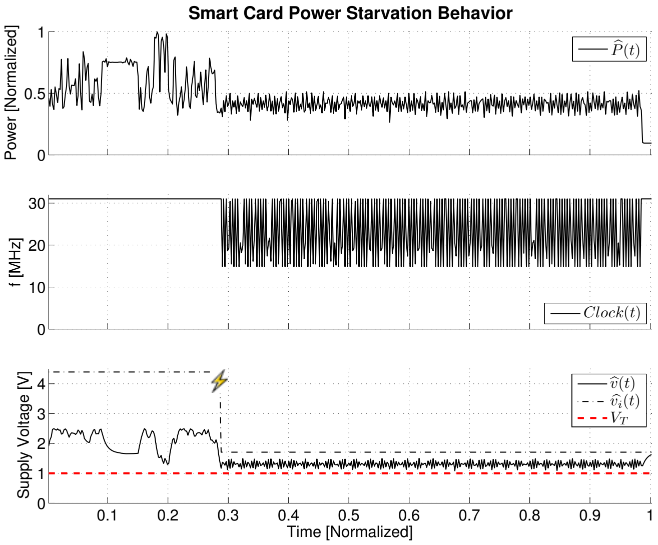


Fig. 12. Smart card behavior during the replay attack. When the magnetic field is detuned, the smart card's power supply $\widehat{v_i}(t)$ drops. As a consequence, the clock is slowed regularly to reduce power consumption $\widehat{P}(t)$. After a certain time period the smart card enters a power supply trap and is deactivated.

radiation to generate predictable values.
- Counters with insufficient bit lengths may overflow.

Thus, it is imperative to test secure reader / smart card designs before tape-out and product releases whether predefined security requirements are met.

Fig. 12 illustrates the smart card's power and voltage trends during the emulated attack campaign. Note, due to disclosure policies, the presented traces are approximated. At the moment the challenge is received, the attacker device detunes the magnetic field, which results in a hazardous $\widehat{v_i}(t)$ power supply drop within the smart card. The smart card detects this power starvation problem and slows its clock regularly to reduce its power consumption $\widehat{P}(t)$. After a certain amount of time a power supply trap is triggered, and the smart card deactivates itself. The monitored power and voltage trends verify that the smart card handles this power fault situation properly. The voltage $\widehat{v}(t)$ never drops below the crucial threshold V_T, which would otherwise lead to a nondeterministic logic behavior of the smart card's electronics. In addition, the attacker device was not able at all to authenticate itself with the recorded challenge response at the reader. This was verified with the help of functional trace information. The reader's software implementation worked properly. Thus, the system emulation test bench verified that the emulated reader / smart card system is resistant against this specific attack type.

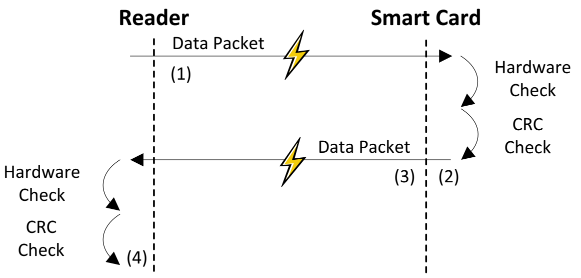


Fig. 13. Concept of the data corruption attack. Data packets are sent from the reader to the smart card and back. Packets may be corrupted for example by electromagnetic interferences. Hardware and CRC checks are performed to detect corrupted packets.

TABLE II
DATA CORRUPTION OF READER / SMART CARD DATA CHANNEL

Seq. #	Component	Packets Sent	Corrupted Packets Dropped
1	Reader	9148	-
2	Smart Card	-	963
3	Smart Card	8185	-
4	Reader	-	995

B. Example of Application - Data Corruption

This test exemplifies the evaluation of a reader / smart card system's data transmission resistance against data corruptions. The effect of corrupted data can be caused, for example, by electromagnetic interferences within the RF channel, as depicted in Fig. 13. This effect is emulated by injecting stuck-at multi-bit-upsets randomly into the data interfaces' hardware FIFOs of reader and smart card. Data packets are generated within the reader and are branded with an incrementing number. The packets are then sent from the reader to the smart card. Within the smart card, a data interface hardware check and a CRC check are conducted. Corrupted packets are dropped and non-corrupted packets are sent back to the reader. Again, a hardware check and a CRC check are conducted within the reader.

Table II highlights the results of this data corruption test. More than 300.000 faults were injected into reader and into smart card hardware FIFOs. Note, not every injected fault results in a corrupted packet. Hardware checks within the controller hardware combined with CRC checks detected all corrupted packets. Thus, the tested software and hardware implementations of the data interface are resistant against this specific data corruption effect.

C. FPGA Utilization

Table III highlights the FPGA utilization of important platform components that are available to the public. These hardware components were synthesized with Xilinx ISE targeting a ML507 evaluation board from Xilinx. Note, the size of trigger modules varies because of different trigger conditions. Moreover, the fault emulation controller was synthesized to support 32 different fault patterns P_n.

TABLE III
FPGA UTILIZATION OF PLATFORM COMPONENTS

Component	Slices	LUTs
System Fault Emulation Controller	437	436
Fault Trigger Module	70	150
Power Consumption Emulation	206	440
RF and Power Supply Emulation	464	756
Platform Controller CPU	5752	4308

VI. Conclusion

It is of high importance to test dependable as well as high security hardware and software systems under faulty conditions. However, testing individual hardware components against single event upsets may not be sufficient. Because novel system-wide multi-fault attacks can be conducted, the fault propagation and fault behavior of the complete system must be regarded. Furthermore, information leakage by means of control-based and data-based power dissipation must be regarded. For the case where the system-under-test contains resource constrained components, like passively-powered contactless smart cards, it is imperative to test if power supply starvation periods are handled properly.

In this paper we present a novel approach of evaluating a complete system's fault behavior during its design phase. State-of-the-art estimation and emulation techniques are used to evaluate functional stability, power dissipation, as well as power supply issues. Thus, novel, comprehensive, and system-wide fault propagation and fault effect analyses can be performed in real time and for each clock cycle. Power and security bugs can be detected and fixed in time before the tape-out. We demonstrate our concept's usability by means of a secure contactless reader / smart card system. A system-wide multi-attack campaign is conducted exemplarily and functional, power, and security, fault effects are evaluated.

Our future work concerns the evaluation of efficient fault recovery methodologies in the application field of secure reader / smart card systems.

Acknowledgments

We would like to thank the Austrian Federal Ministry for Transport, Innovation, and Technology, which funded the project META[:SEC:] under the FIT-IT contract 829586. Furthermore, we would like to thank our industrial partners Infineon Technologies Austria AG as well as Enso Detego GmbH for their support.

References

[1] S. Ravi, A. Raghunathan, P. Kocher, and S. Hattangady, "Security in embedded systems: Design challenges," *ACM Transactions on Embedded Computing Systems (TECS)*, vol. 3, no. 3, pp. 461–491, August 2004.

[2] P. Kocher, "Complexity and the challenges of securing SoCs," in *Design Automation Conference (DAC)*, June 2011, pp. 328–331.

[3] N. Druml, M. Menghin, C. Steger, R. Weiss, A. Genser, H. Bock, and J. Haid, "Emulation-Based Test and Verification of a Design's Functional, Performance, Power, and Supply Voltage Behavior," in *21st Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP)*, 2013, pp. 328–335.

[4] J. Arlat, M. Aguera, L. Amat, Y. Crouzet, J.-C. Fabre, J.-C. Laprie, E. Martins, and D. Powell, "Fault injection for dependability validation: a methodology and some applications," *IEEE Transactions on Software Engineering*, vol. 16, no. 2, pp. 166–182, February 1990.

[5] E. Jenn, J. Arlat, M. Rimen, J. Ohlsson, and J. Karlsson, "Fault injection into VHDL models: the MEFISTO tool," in *International Symposium on Fault-Tolerant Computing, Digest of Papers*, June 1994, pp. 66–75.

[6] C. Bolchini, A. Miele, and D. Sciuto, "Fault models and injection strategies in systemc specifications," in *11th EUROMICRO Conference on Digital System Design Architectures, Methods and Tools (DSD)*, September 2008, pp. 88–95.

[7] R. Shafik, P. Rosinger, and B. Al-Hashimi, "SystemC-Based Minimum Intrusive Fault Injection Technique with Improved Fault Representation," in *14th IEEE International On-Line Testing Symposium (IOLTS)*, July 2008, pp. 99–104.

[8] J. Barton, E. Czeck, Z. Segall, and D. Siewiorek, "Fault injection experiments using FIAT," *IEEE Transactions on Computers*, vol. 39, no. 4, pp. 575–582, April 1990.

[9] G. Kanawati, N. Kanawati, and J. Abraham, "FERRARI: a tool for the validation of system dependability properties," in *International Symposium on Fault-Tolerant Computing*, July 1992, pp. 336–344.

[10] J. Grinschgl, A. Krieg, C. Steger, R. Weiss, H. Bock, J. Haid, T. Aichinger, and C. Ulbricht, "Case study on multiple fault dependability and security evaluations," *Microprocessors and Microsystems*, vol. 37, no. 2, pp. 218–227, March 2013.

[11] J. Baraza, J. Gracia, D. Gil, and P. Gil, "Improvement of fault injection techniques based on VHDL code modification," in *IEEE International High-Level Design Validation and Test Workshop*, 2005, pp. 19–26.

[12] M. Valderas, M. Garcia, R. Cardenal, C. Lopez Ongil, and L. Entrena, "Advanced Simulation and Emulation Techniques for Fault Injection," in *IEEE International Symposium on Industrial Electronics*, June 2007, pp. 3339–3344.

[13] L. Entrena, M. Garcia-Valderas, R. Fernandez-Cardenal, A. Lindoso, M. Portela, and C. Lopez-Ongil, "Soft Error Sensitivity Evaluation of Microprocessors by Multilevel Emulation-Based Fault Injection," *IEEE Transactions on Computers*, vol. 61, no. 3, pp. 313–322, March 2012.

[14] R. Leveugle, "Fault injection in VHDL descriptions and emulation," in *IEEE International Symposium on Defect and Fault Tolerance in VLSI Systems*, October 2000.

[15] H. Guzman-Miranda, M. Aguirre, and J. Tombs, "Noninvasive Fault Classification, Robustness and Recovery Time Measurement in Microprocessor-Type Architectures Subjected to Radiation-Induced Errors," *IEEE Transactions on Instrumentation and Measurement*, vol. 58, no. 5, pp. 1514–1524, May 2009.

[16] J.-M. Daveau, A. Blampey, G. Gasiot, J. Bulone, and P. Roche, "An Industrial Fault Injection Platform for Soft-Error Dependability Analysis and Hardening of Complex System-On-a-Chip," in *IEEE International Reliability Physics Symposium*, April 2009, pp. 212–220.

[17] M. Hutter, J.-M. Schmidt, and T. Plos, "RFID and its Vulnerability to Faults," in *International workshop on Cryptographic Hardware and Embedded Systems (CHES)*, August 2008, pp. 363–379.

[18] T. Heydt-Benjamin, D. Bailey, K. Fu, A. Juels, and T. O'Hare, "Vulnerabilities in First-Generation RFID-enabled Credit Cards," in *International Conference on Financial Cryptography and Data Security*, 2007, pp. 2–14.

[19] T. Plos, M. Aigner, T. Baier, M. Feldhofer, M. Hutter, T. Korak, and E. Wenger, "Noninvasive Fault Classification, Robustness and Recovery Time Measurement in Microprocessor-Type Architectures Subjected to Radiation-Induced Errors," *International Journal of RFID Security and Cryptography*, vol. 1, no. 1, pp. 16–24, 2012.

[20] R. Leveugle, "Early Analysis of Fault-based Attack Effects in Secure Circuits," *IEEE Transactions on Computers*, vol. 56, no. 10, pp. 1431–1434, October 2007.

[21] J. Coburn, S. Ravi, and A. Raghunathan, "Power Emulation: A New Paradigm for Power Estimation," in *Design Automation Conference (DAC)*, June 2005, pp. 700–705.

[22] A. Krieg, C. Bachmann, J. Grinschgl, C. Steger, R. Weiss, and J. Haid, "Accelerating early design phase differential power analysis using power emulation techniques," in *IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, June 2011, pp. 81–86.

[23] C. Bachmann, A. Genser, J. Haid, C. Steger, and R. Weiss, "Automated Power Characterization for Run-Time Power Emulation of SoC Designs," in *13th Euromicro Conference on Digital System Design (DSD)*, September 2010, pp. 587–594.

[24] K. Finkenzeller, *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification*, 2nd ed. New York, NY, USA: John Wiley & Sons, Inc., 2003.

[25] M. Wendt, C. Grumer, C. Steger, R. Weiss, U. Neffe, and A. Muehlberger, "System Level Power Profile Analysis and Optimization for Smart Cards and Mobile Devices," in *ACM Symposium on Applied Computing*, November 2008, pp. 118–121.

[26] N. Druml, C. Steger, R. Weiss, A. Genser, and J. Haid, "Estimation Based Power and Supply Voltage Management for Future RF-Powered Multi-Core Smart Cards," in *Design Automation and Test in Europe Conference and Exhibition (DATE)*, March 2012, pp. 358–363.

Power and Thermal Fault Effect Exploration Framework for Reader / Smart Card Designs

Norbert Druml*, Manuel Menghin*, Tobias Rauter*, Christian Steger*, Reinhold Weiss*
Christian Bachmann†, Holger Bock‡, Josef Haid‡
*Graz University of Technology, Graz, Austria
{norbert.druml, manuel.menghin, steger, rweiss}@tugraz.at
tobias.rauter@student.tugraz.at
†Holst Centre/imec, Eindhoven, The Netherlands
christian.bachmann@imec-nl.nl
‡Infineon Technologies Austria AG, Graz, Austria
{holger.bock, josef.haid}@infineon.com

***Abstract*—Power consumption and thermal behavior are important characteristics that need to be explored and evaluated during a product's development cycle. If not handled properly, the consequences are, for example, increased mean-time-to-failure and fatal timing variations of the critical path. In the field of contactlessly powered reader / smart card systems, a magnetic field strength exceeding the allowed maximum threshold may harm the smart card's hardware. Thus, secure smart cards must be designed to cope with faults provoked by power oversupply and thermal stress. Proper fault detection and fault handling are imperative tasks to protect internal secrets. However, state-of-the-art design exploration tools cover these smart card specific power and thermal stress issues only to some extent.**

Here we present an innovative high level simulation approach used for exploring and simulating secure reader / smart card systems, focusing on magnetic field oversupply and thermal stress evaluations. Gate-level-based power models are used besides RF-channel models, thermal models, and thermal effect models. Furthermore, fault injection techniques are featured to evaluate the fault resistance of a smart card system's software implementation. This framework grants software and hardware designers a novel opportunity to detect functional, power, thermal, and security issues during the design time. We demonstrate the usage of our exploration framework and show an innovative hardware design approach to prolong the lifetime of smart card electronics, which are exposed to high magnetic field strengths.

***Index Terms*—Smart Card, Power Simulation, Thermal Simulation, Fault Effect Simulation**

I. Introduction

The number of RFID and NFC applications in our every days life has increased drastically during the last years. Applications can be found, e.g., in the fields of healthcare, access control, and payment. Thus, security and reliability concerns are of high importance. The working principle of such an RFID-based contactless reader / smart card system is depicted by Fig. 1. The reader emits an alternating magnetic field. This magnetic field induces an alternating voltage within the smart card's coil, which is used to power the smart card's electronics. Data is transferred by means of magnetic field modulation. A capacitor buffers electrical energy that is used during magnetic field undersupply periods. The shunt resistor (depicted as a Zener diode) prevents the electronics from power surges. If the distance between reader and smart card is low and the magnetic field strength is high, this shunt resistor dissipates a high amount of power and heats up the smart card's electronics. For example, in the field of industrial applications, transponders face harsh ambient conditions (high environmental temperatures, electromagnetic pollution, etc.) and may require high magnetic field strengths for proper operation. As a result, this power and thermal stress makes the electronics prone to silicon interconnection fatigue, junction fatigue, electrical parameter shifts, etc. Being unaware of these faulty conditions may cause unpredictable hardware and software behavior. Especially in the field of high secure smart cards, software must be designed in way to not disclose internal secrets even under faulty hardware conditions.

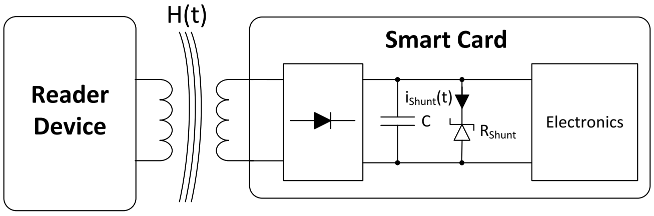


Fig. 1. Working principle of a reader / smart card system. The reader emits a magnetic field for power and communication purposes. A shunt resistor protects the electronics from power surges. High magnetic field strength causes the shunt resistor to heat up the smart card, which may cause hazardous material fatigue.

Given the highlighted smart card specific design challenges, it is imperative to support hardware and software designers with appropriate tools to explore a reader / smart card system's power and thermal behavior. Furthermore, it is imperative to test a secure smart card design's resistance against fault effects caused by magnetic field oversupply and thermal stress. Several tools haven been proposed so far dealing to some extent with low-level smart card power evaluations [1], thermal evaluations of integrated circuits in general [2], or high-level fault injections [3]. However, there is a major gap in literature combining these important research fields for the application field of secure reader / smart card systems, which is addressed by our work.

This paper makes the following contributions:

- It presents a novel high level power aware and thermal aware design exploration and evaluation framework focusing on secure reader / smart card systems.
- It features an RF channel model and fault effect models supporting magnetic field oversupply and thermal stress evaluations.
- It demonstrates the evaluation of a reader / smart card system by means of the framework and proposes a thermal optimized hardware design approach.

This paper is structured as follows. Section II gives a short introduction into the related work covering the topics power and thermal analyses, high level fault injection, and high level design exploration frameworks. In Section III and Section IV our high-level design exploration approach is presented. Followed by Section V demonstrating the evaluation of an RF-powered reader / smart card system with the help of our framework. Finally, our results are concluded in Section VI.

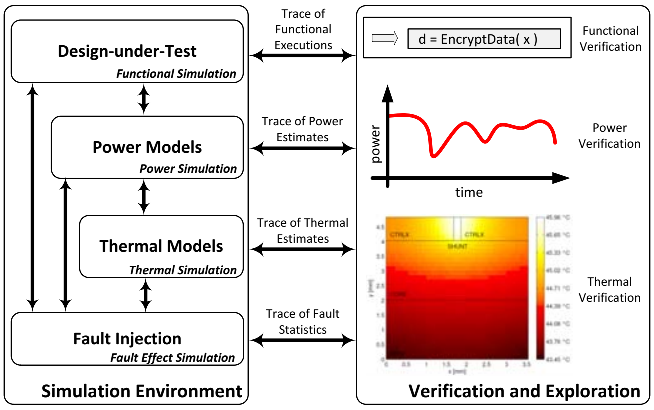


Fig. 2. Concept of the presented power aware and thermal aware reader / smart card design exploration framework.

II. Related Work

Power analysis in the field of reader / smart card systems has been performed by the authors of [1], [4], and [5]. In [6], the authors regarded the power transfer between a reader and a smart card. Based on this power analysis, they were able to optimize the system's power consumption by adapting the magnetic field strength. Various antenna tag classes were analyzed by the authors of [7]. Depending on the antenna size and the physical relation (distance, orientation, etc.) between reader and tag, different amounts of power are extractable from the magnetic field. Thus, if a reader system is designed to operate with various antenna classes, class 1 tags are facing power oversupply. Skadron et al. introduced in [2] the software tool HotSpot, which is used to estimate the temperature behavior of individual SoC components based on their power consumptions. The impact of temperature on a hardware's reliability was outlined by [8]. Reliability aware design approaches were presented by [9]. By optimizing a compiler's register allocation algorithm, they were able to reduce thermal hotspots. Thus, the register file's mean time to failure was increased by 20 %. In [10], Atienza et al. presented a hardware emulation framework to estimate functional and power behavior of SoCs. Furthermore, thermal estimations in software were featured. The used thermal estimation method was based on the work of [2].

A lot of research has been conducted in the fields of fault injection and security analysis. Early simulation-based fault injection tools were presented by the authors of [11] and [12]. In [13], Kasper et al. presented a versatile fault injection platform focusing on secure embedded devices. They demonstrated successfully a full key recovery from a contactless smart card which features Triple-DES security algorithms. In [14], the authors used heat to successfully attack JAVA virtual machines. By provoking single bit errors they were able to take over the virtual machines. In [15], the authors evaluated the vulnerability of instructions during temperature and voltage variations. Gate-level simulations of a LEON3 SoC were analyzed. The authors of [16] outlined hazardous CMOS delay variations due to temperature fluctuations. Furthermore, they presented a design methodology to reduce this temperature induced delay variation. Hutter et al. summarized in [17] the vulnerability of RFID devices against artificially induced errors. In [3], the authors presented a SystemC-based fault injection framework. Their work focused on security attack simulations of smart cards. Further SystemC fault injection tools were presented for example by [18] and [19].

The presented related work is admittedly trend-setting. However, it lacks in combining and applying these research fields (power analysis, thermal analysis, as well as security and reliability analyses) to the very important domain of secure reader / smart card systems, where disclosure of internal secrets may lead to huge financial loss.

III. Simulation Framework

This chapter presents our power aware and thermal aware exploration framework. It is divided into the following parts. At first the concept and the flow to setup the exploration framework are described. Then, the architecture and our fault injection approach are shown.

A. Concept

Fig. 2 illustrates the concept of our presented exploration framework. A given high-level reader / smart card design-under-test (DUT) is simulated along with RF power transfer, power consumption, and thermal models. Faults can be injected into the design based on predefined patterns or thermal effect models. Functional, power, and thermal trace information is gathered, analyzed, and verified according to predefined constraints. Thus, an innovative and comprehensive design exploration, evaluation, and verification tool is given, which supports engineers during the whole development cycle of a reader / smart card system.

B. Framework Setup Flow

Fig. 3 depicts the framework's setup flow. It is divided into the phases specification, characterization, modeling, and

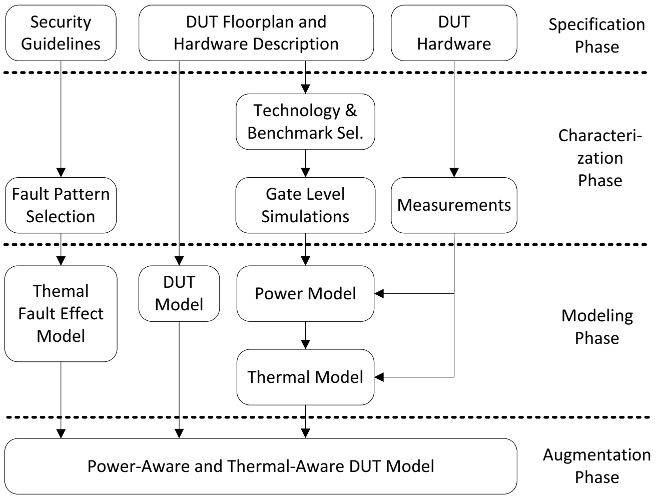


Fig. 3. Exploration framework setup flow, which consists of the phases specification, characterization, modeling, and augmentation.

augmentation. In the following, each phase is described in detail.

1) Specification Phase: During this initial phase, the DUT's floorplan, packaging, and hardware description are specified. Furthermore, security guidelines are defined, which respect the product's security and certification levels. If a manufactured hardware is available, it can be used later on for measurements and model refinements.

2) Characterization Phase: This phase aims to characterize the DUT's behavior as accurate as possible. This information is later on needed to create corresponding models. To characterize the DUT in terms of power consumption, the target technology and exhaustive benchmarks are selected. Then, gate-level simulations are conducted, resulting in signal switching activity and power information. In a final step, irrelevant and unneeded data is filtered. If the manufactured hardware is available, power consumption measurements are conducted. Based on the security specifications made beforehand, dedicated fault injection concepts (e.g., where to inject faults, using saboteurs or mutants) are evaluated and fault injection patterns are developed.

3) Modeling Phase: Based on the characterization data, a high-level power model is constructed. This power model maps signal and component activity to corresponding power estimates. The model's accuracy can be adjusted: the more signals and states are considered, the more accurate is the correlation between activity and power. The thermal model is developed with the help of the DUT's floorplan, packaging information, and the thermal characteristics of the used materials. If power or thermal measurements of the manufactured hardware are available, both models are refined to reduce estimation errors. The thermal effect model describes the physical effects caused by heat, e.g., electromigration, changes to the critical path delay. Based on these physical effects, a fault model is developed, which describes fault effects caused by heat, e.g., bit flips, stuck-at conditions. Furthermore, a SystemC-based high-level model of the DUT is created. The level of detail and accuracy of this model directly influences the accuracy of power and thermal estimations.

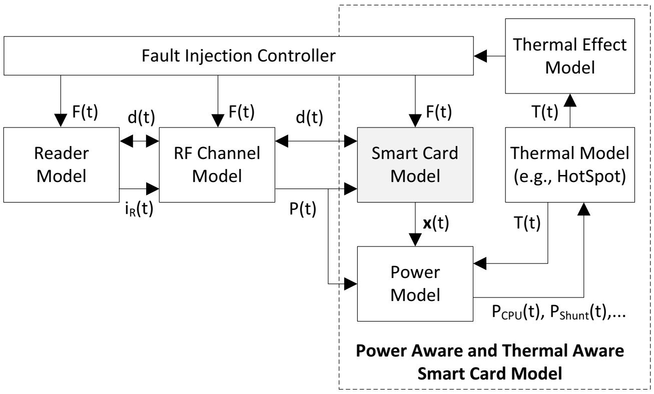

Fault Injection Controller
Thermal Effect Model
F(t)
d(t)
F(t)
d(t)
F(t)
T(t)
Reader Model
RF Channel Model
Smart Card Model
Thermal Model (e.g., HotSpot)
i_R(t)
P(t)
x(t)
T(t)
Power Model
P_{CPU}(t), P_{Shunt}(t),...
Power Aware and Thermal Aware Smart Card Model

Fig. 4. Architecture of the power aware and thermal aware reader / smart card exploration framework.

4) Augmentation Phase: During this phase, the SystemC-based DUT model is augmented with the power model, thermal model, and fault effect model. Fault injection units, i.e. saboteurs and mutants, are placed in the design according to the predefined fault injection concept. After this integration, the power aware and thermal aware reader / smart card design can be explored and evaluated. Functional, power, thermal, and fault injection traces are logged and can be evaluated afterwards with sophisticated software tools.

C. Architecture of the Framework

Fig. 4 depicts the architecture of the presented power aware and thermal aware reader / smart card design exploration framework. It consists of three transaction-based components: the reader model, the RF channel model, and the augmented smart card model. The reader is responsible to initiate the communication and sets the strength of the magnetic field by means of $i_R(t)$. Data $d(t)$ and power transfer $P(t)$ to the smart card are modeled by the RF channel model. For this purpose, an equivalent circuit of the smart card power supply network is used. The power aware and thermal aware smart card consists of several modules. A power model estimates the smart card's power consumption by means of its internal states $\mathbf{x(t)}$ and its current temperature $T(t)$. The power estimates of the smart card's modules $P_{CPU}(t)$, $P_{Shunt}(t)$, etc. are forwarded to the thermal model. This unit contains accurate information of the smart card's floorplan, packaging, temperature coefficients of used materials, etc. A modified version of HotSpot, which was introduced by the authors of [2], is used to simulate the temperature behavior of the individual smart card components. Note, any other thermal simulator could be used as well, thanks to the framework's modular approach. The temperature information $T(t)$ is then forwarded to a thermal effect model. This model estimates the effects of thermal stress to the smart card hardware, e.g., mean time to failure (MTTF), critical path delays. Finally, fault injection units are used to evaluate

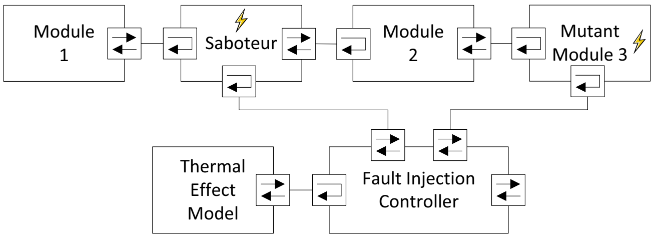


Fig. 5. Demonstration of using saboteurs and mutants, which are triggered by a controller unit, to simulate the effect of hardware faults. Obtained with changes from [3].

the resistance of reader and smart card software against fault effects caused for example by thermal stress or RF channel disturbances. Faults $F(t)$ can be either injected into reader, into RF channel, or into smart card.

D. High-Level Fault Injection

Testing a secure hardware / software design during faulty hardware behavior is an important task during the product's development cycle. Our framework is capable of simulating fault effects caused by malfunctioning hardware. Thus, software can be tested whether a required level of fault resistance is actually achieved or not, e.g., is the used CRC algorithm able to cope with a certain amount of RF channel errors. In general, faults can be either permanent or transient and are injected during the simulation. This high-level, simulation-based, and adaption-based approach is very flexible compared to low-level hardware emulation approaches. Our fault injection technique is based upon a method proposed by the authors of [3]. The design-under-test can be adapted with mutants or saboteurs.

- A mutant represents a replacement of a module. The mutant behaves like the original module until it is triggered. If triggered, the module's functionality is disturbed according to predefined patterns.
- A saboteur is a small module that is plugged into module connections. A saboteur behaves transparently until it is triggered. If triggered, the connection's functionality is disturbed according to predefined patterns.

Fig. 5 depicts the usage of fault injection controller, saboteurs, and mutants. The fault injection controller unit is connected to the power and thermal effect model units. If one of these units triggers a fault, the controller unit is notified to trigger the dedicated saboteur or mutant. Table I highlights the supported fault modes.

TABLE I
SUPPORTED FAULT MODELS

Fault	Fault Type	Description
Stuck-at-X	Permanent	Signal is set to X until reset
Bridging Fault	Permanent	No output propagation until reset
In-determination	Permanent	Undefined value until reset
Bit Flip	Transient	Change of the value
Delay	Transient	Delay of input to output

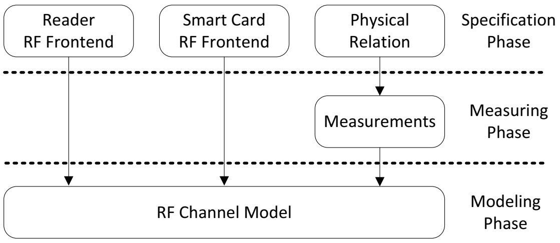


Fig. 6. Development flow of an RF channel model consisting of the phases characterization, measuring, and modeling.

IV. SIMULATION FRAMEWORK - USED MODELS

The following chapter describes the RF, power, and thermal models used in our reader / smart card exploration framework. Furthermore, we highlight how these models are developed.

A. RF Channel Model

To simulate the power and data transfer between reader and smart card, an RF channel model is used. The verification if software and hardware designs work properly during oversupply and undersupply is of high importance. The flow to develop a proper RF channel model is depicted by Fig. 6. At first, the reader's and the smart card's analog RF frontend need to be specified, e.g., number of coils, resonance frequency, maximum reader output power. In addition, the physical relation between reader and smart card is defined. This physical relation describes further attributes that influence the power transfer, e.g., distance, smart card's orientation within the magnetic field. Finally, measurements need to be performed to refine and calibrate the model.

Fig. 7 represents a reader / smart card system's equivalent circuit. This model, which is given by (1), is based on [20], [4], and observations made by [6]. The reader sets the magnetic field output power with the help of the fixed output voltage v_1 and the adjustable resistance $R_{Rel}(t)$. By means of inductive coupling and a resonance circuit, electrical power is transferred contactlessly to the smart card. The coupling factor between reader and smart card is defined by k. A rectification is conducted by the diodes $D1$ up to $D4$. Capacitor C_B buffers electrical energy and sets the voltage $v(t)$. $R_L(t)$ represents the changing resistance of the smart card's electronics. Depending on the smart card CPU's power consumption and the amount of power gained from the magnetic field, the capacitor C_B is either charging or discharging. The shunt

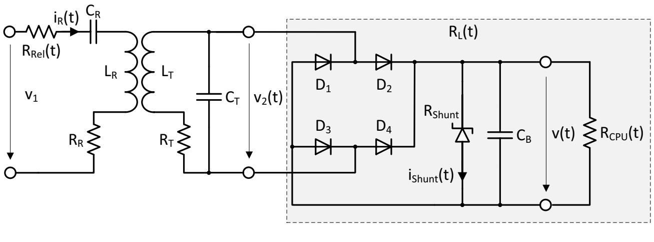


Fig. 7. Equivalent circuit of a reader / smart card system. Obtained with changes from [20].

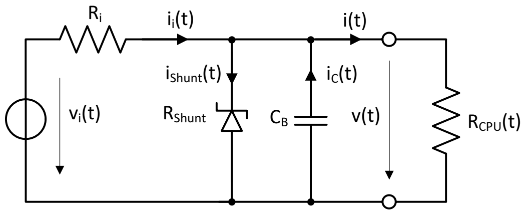


Fig. 8. Simplified equivalent circuit of a reader / smart card system. Obtained with changes from [4].

resistor R_{Shunt} (depicted by a Zener diode) prevents the smart card's electronics from power surges. In case of a low distance between reader and smart card and a high magnetic field strength, this shunt resistor generates a significant amount of heat. If not handled properly, this heat source may influence the hardware's dependability hazardously.

$$v_2 = \frac{wk\sqrt{L_R L_T} i_R}{\sqrt{(\frac{(wL_T)}{R_L} + wR_T C_2)^2 + (1 - w^2 L_T C_2 + \frac{R_T}{R_L})^2}} \quad (1)$$

The equivalent circuit of Fig. 7 can be further simplified by introducing a Thevenin voltage source v_i and resistance R_i. Fig. 8 illustrates this simplification approach. The values of v_i and R_i are determined by measuring the power supply network's voltage / current characteristics. According to [4], an estimation errors of only 2% can be achieved with such a simplified equivalent circuit model. Voltage $v(t)$ can now be easily computed for example with a charge-based approach, as depicted in (2).

$$v(t{+}1) = \frac{Q_C(t) + \frac{v_i(t) - v(t)}{R_i}\Delta t - i(t)\Delta t}{C} \quad \text{if } v(t) < V_Z \quad (2)$$

B. Power Model

The framework's power estimation model is based upon a technique from the authors of [21] and [5]. To generate an appropriate power model, a power charaterization process must be conducted beforehand. According to [5], such a characterization can be performed automatically for any kind of design which is available in a hardware description language. At first, the target technology is selected and exhaustive benchmarks are defined, which have to cover every functionality provided by the design. Then, gate-level simulations of these benchmarks are executed resulting in signal activity and power information. After a post processing step, only relevant power and activity data remains. Finally, a linear regression technique is used to fit signal activity x_i to model coefficients c_i. A model coefficient c_i defines the amount of power that is dissipate during the corresponding state x_i. The total power estimation $\widehat{P}(\mathbf{x})$ is calculated by the linear combination of $\mathbf{x}$ and c plus a static power consumption c_0, according to (3).

$$\widehat{P}(\mathbf{x}) = \widehat{P}_{stat} + \widehat{P}_{dyn} = c_0 + \sum_{i=1}^{n} c_i \cdot x_i = c_0 + \mathbf{c}^{\mathbf{T}} \cdot \mathbf{x} \quad (3)$$

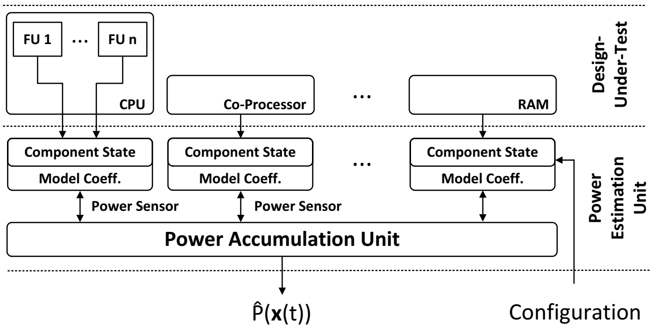


Fig. 9. Working principle of the power estimation unit. Power sensors monitor component states and provide corresponding power estimates. Obtained with changes from [5].

The difference between power estimates and real power consumption $P(\mathbf{x})$ is defined by ϵ, according to (4). The more states $\mathbf{x}$ considered, the lower this estimation error ϵ.

$$P(\mathbf{x}) = \widehat{P}(\mathbf{x}) + \epsilon \quad (4)$$

Fig. 9 depicts the working principle of the power estimation unit, which is used in our framework. Power sensors observe the component states x_i (e.g., memory read, memory write, crypto core active) and provide corresponding power estimates c_i. The individual power estimates are then forwarded to the thermal model and are summed up to form the total smart card's power consumption.

C. Thermal Model

Fig. 10 illustrates the basic flow of our thermal model's development. This development process can be subdivided into two phases. During the initial specification phase, the chip's floorplan, the packaging dimensions, and the thermal characteristics of the used materials are defined. Afterwards,

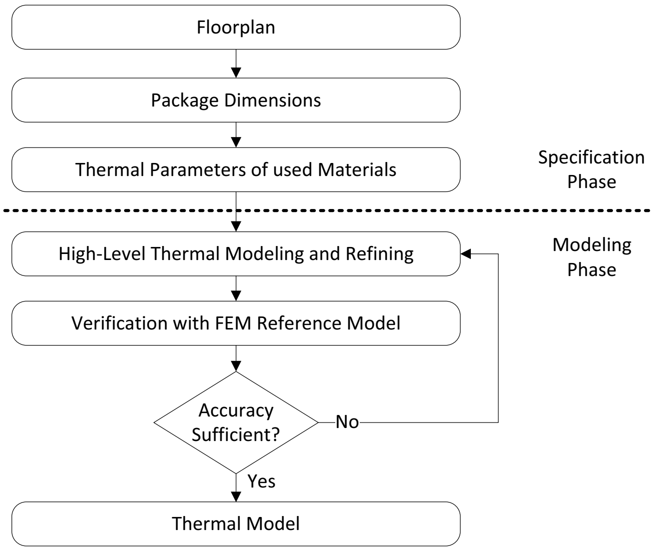

Floorplan
Package Dimensions
Thermal Parameters of used Materials
Specification Phase
High-Level Thermal Modeling and Refining
Modeling Phase
Verification with FEM Reference Model
Accuracy Sufficient?
No
Yes
Thermal Model

Fig. 10. Development flow of our thermal model, which is subdivided in specification and modeling phases.

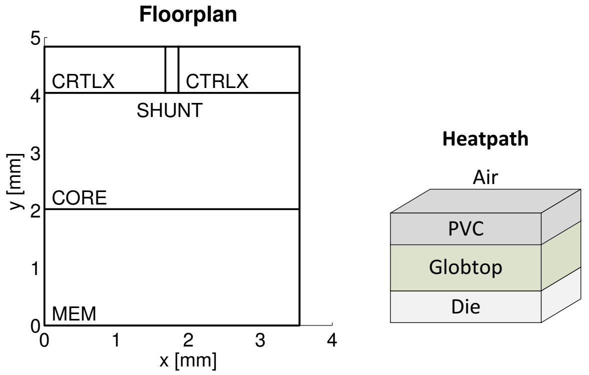


Fig. 11. The left subplot shows the floorplan of the smart card chip consisting of CPU, memory, shunt resistor, and additional units denoted by CTRLX. The right subplot depicts the modeled heatpath in the middle of the smart card chip, consisting of die, globtop, and PVC.

during the modeling phase, the smart card's thermal behavior is modeled by means of an equivalent RC network in a modified version of the software tool HotSpot, which was originally introduced by [2]. The accuracy of this RC network thermal model is then verified against a very accurate, but complex and time-consuming, finite element method (FEM) thermal reference model. Finally, the HotSpot RC network model is further refined until a required thermal estimation accuracy is reached. A low-single-digit percentage estimation error is achievable.

The left subplot of Fig. 11 depicts the smart card chip's floorplan. It consists of memory unit, the CPU core, the shunt resistor unit, and several co-processors denoted by CTRX. The shunt unit represents the most important component during high magnetic field strengths, because it dissipates the most amount of power and therefore heats up the smart card chip. The right subplot of Fig. 11 illustrates the modeled heatpath in the middle of the smart card chip. Due to security disclosure reasons, the floorplan and the heatpath are only approximated for publication.

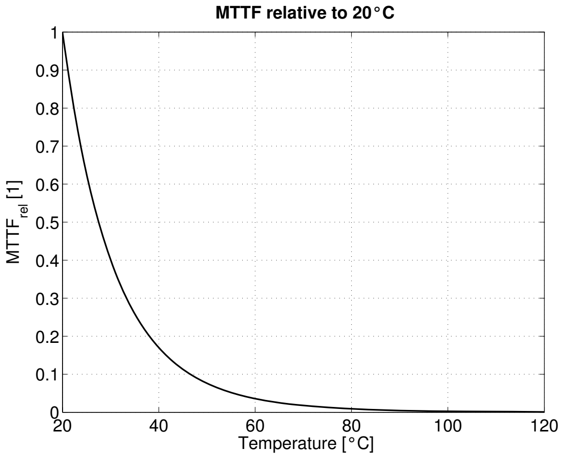


Fig. 12. MTTF trend compared to a MTTF reference at a temperature of 20 °C, according to (5).

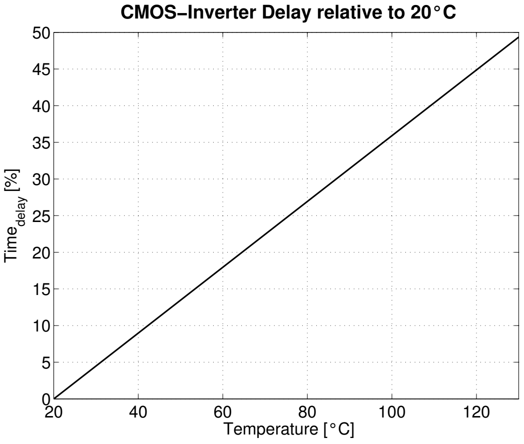


Fig. 13. Trend of the simplified CMOS inverter delay model, according to [22].

D. Thermal Effect Models

Thermal stress provokes errors like electromigration, time-dependent dielctric-breakdown, stress migration, etc., as outlined by [9]. Due to disclosure policies, this work uses a relative value for the MTTF analysis, given by (5), where E_a denotes the activation energy and k the Boltzmann's constant. The relation between a reference temperature T_{ref} and the actual temperature T, provides information to analyze how design variations in hardware and software affect the aging of the circuitry. Fig. 12 illustrates the trend of $MTTF_{rel}$ compared to a reference temperature of 20 °C.

$$MTTF_{rel} = \frac{MTTF(T_{ref})}{MTTF(T)} = exp\{\frac{E_a}{k} \cdot (\frac{1}{T_{ref}} - \frac{1}{T})\} \quad (5)$$

The framework implements also models to estimate variations in the circuit's critical path delay. Again, because of disclosure policies, the presented framework uses a simplified CMOS inverter delay model, which was introduced by the authors of [22]. By comparing these values to a reference value at 20 °C, a worsening prediction of the delay depending on the target temperature can be made, as shown in Fig. 13. To estimate when a fault occurs due to timing violations, critical path variation data from the authors of [15] is used. This data was gathered by gate-level simulations made on a LEON3 open source processor platform.

V. Case Studies and Results

In the following, various case studies and results are presented demonstrating the application of the reader / smart card exploration framework. Due to security related disclosure reasons, the accuracy of the used functional, power, and thermal models has been reduced. However, the focus of this paper is to highlight the conceptual possibilities provided by this design exploration framework.

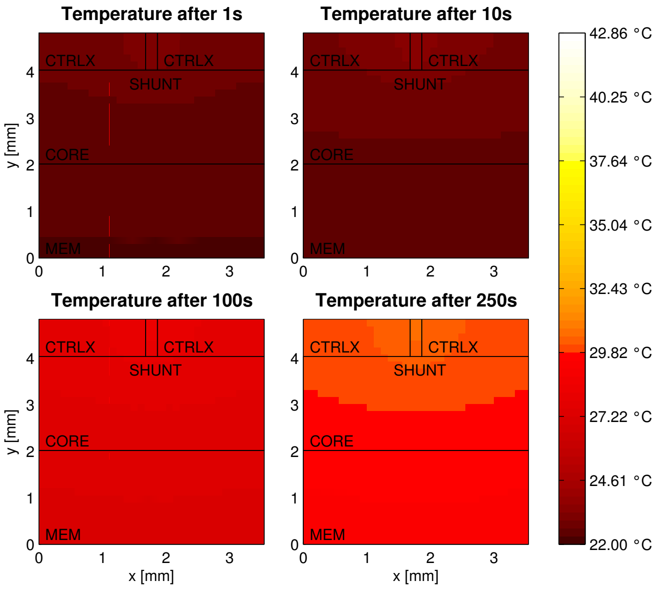


Fig. 14. Transient thermal analysis during a magnetic field strength of 3 A/m and 20 °C environmental temperature.

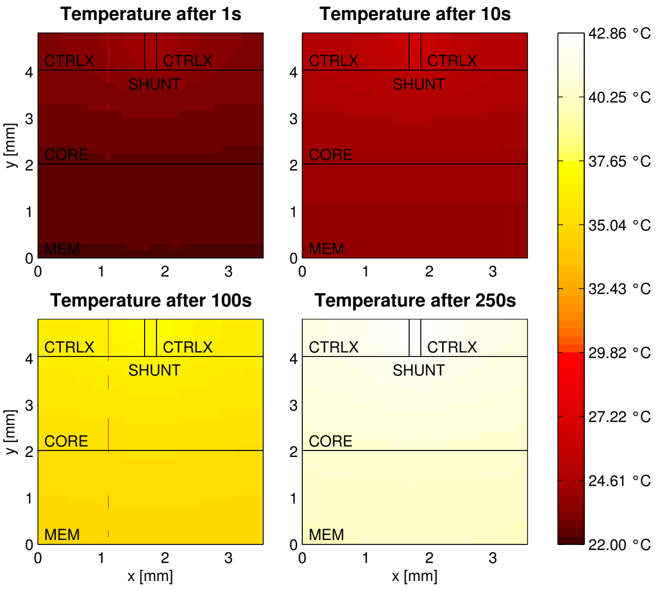


Fig. 16. Transient thermal analysis during a magnetic field strength of 7 A/m and 20 °C environmental temperature.

A. Transient Temperature Evaluations

Fig. 14 and Fig. 16 depict transient temperature trends for 3 A/m and 7 A/m magnetic field strengths. Because the ISO/IEC 14443-2 standard defines a maximum magnetic field strength of 7.5 A/m, RFID and NFC applications must be evaluated during high magnetic field strength corner cases. During both evaluations an environmental temperature of 20 °C is given. No temperature hotspots are detectable. However, the shunt resistor heats up the whole chip. As expected, a magnetic field strength of 7 A/m causes more heat and thermal stress than a magnetic field strength of only 3 A/m.

B. Steady-State Temperature Evaluations

Fig. 15 illustrates the steady-state temperature distribution while applying a high magnetic field strength of 7 A/m. An environmental temperature of 20 °C is given. Due to the high power dissipation of the smart card's shunt resistor, the chip's maximum temperature rises to a value of 45.96 °C. The power dissipation caused by all other units is vanishing low and hardly affects the temperature distribution, in case of such high magnetic field strengths. Compared to the 3 A/m approach,

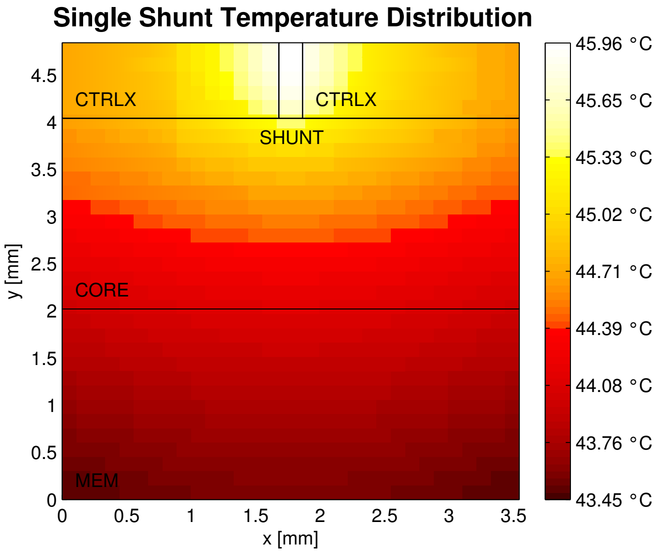


Fig. 15. Steady-state temperature distribution during 20 °C environmental temperature and a magnetic field of 7 A/m. The shunt resistor dissipates the highest amount of power and thus heats the chip most.

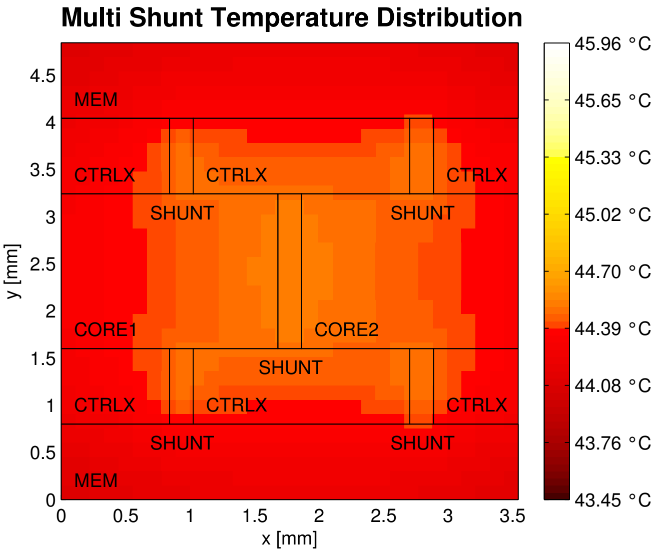


Fig. 17. Steady-state temperature distribution during 20 °C environmental temperature and a magnetic field of 7 A/m. Shunt resistor is evenly distributed over the chip area.

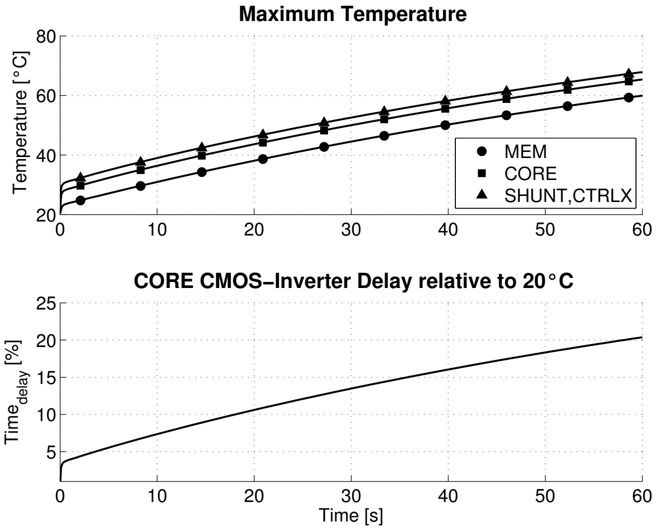


Fig. 18. Varying CMOS inverter delay depending on the chip's temperature, based on the model of [22].

which causes a maximum steady-state chip temperature of only 32.48 °C, the MTTF is reduced by 59%.

Fig. 17 shows an innovative approach of dividing the shunt resistor into five parts and distributing it evenly throughout the chip. Thus, the heat generated by the shunt resistors is now distributed better. The maximum temperature caused by the 7 A/m approach is decreased from 45.96 °C down to 44.52 °C. As a consequence, the MTTF value is increased by 11%. Thus, the electronics' lifetime is prolonged by 11%. Such temperature and aging explorations and optimizations are of high importance in applications fields that require an extremly low or even zero chip error rate, e.g., automotive industries.

C. Thermal Aware Fault Injection

This use case demonstrates the usage of the fault injection capabilities by means of a very simplified software evaluation. Fault effects are simulated, which are caused by thermal stress. For demonstration and disclosure purposes, the smart card uses a LEON3 processor design and LEON3 temperature effect models, given by [15]. The reader emits a very high magnetic field and an environmental temperature of 80 °C is given. This results in a CPU core temperature of 125 °C. Such high temperature and high magnetic field environments can be found for example in the field of industrial applications, where transponders are exposed to harsh ambient conditions. Fig. 18 highlights the transient CMOS inverter delay variations based on a simplified model presented by [22]. Such delay variations may cause serious problems to a processor's critical path. According to [15], a LEON3 multiply instruction is failing under similar conditions with a probability of 4.2%, because of its sensitivity to critical path delays. In the outlined work, the hardware is operated at a voltage level of 1.1 V.

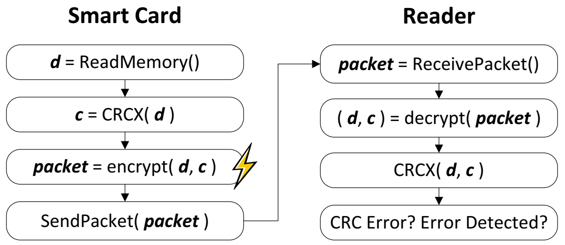


Fig. 19. Thermal-based fault effect testing of a simplified data exchange protocol, which features a software-based encryption algorithm.

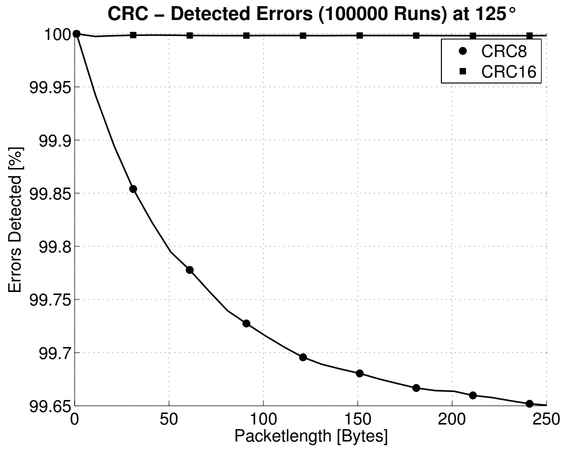


Fig. 20. CRC8 and CRC16 algorithms' detection rate of injected thermal effect faults.

Based on these assumptions, the reliability of a software-based encryption protocol is evaluated against temperature-based fault effect. Fig. 19 illustrates the conducted evaluation sequence. The smart card reads data d from its memory and performs a CRC calculation. The CRC result c and the data d are then encrypted and assembled in a packet. Afterwards, this packet is sent to the reader, which conducts a decryption and a CRC check. The aim of this test is the evaluation if the used error detection algorithms (CRC8 and CRC16) are sufficient to counteract the error prone multiply instruction, which is used by the encryption algorithm.

The presented test procedure was executed 100.000 times for various data lengths and two different CRC implementations. Fig. 20 illustrates how many injected bit flip faults were detected by the individual CRC versions. As expected, the CRC16's error detection rate is superior over the CRC8 version and should be used to counteract the fault effects caused by thermal stress.

However, state-of-the-art secure smart cards use on-chip temperature sensors for monitoring purposes. If the monitored temperature exceeds a certain threshold, which would affect the critical path delay hazardously, the smart card enters a thermal trap and stops executing its software. Thus, thermal induced critical path delays are typically counteracted. Note, the fault injection use case presented here can also be used for RF channel disturbance analyses.

TABLE II
SIMULATION TIME NEEDED FOR ONE SECOND REAL TIME

Simulation Mode	Average Time Needed
Without Thermal Model	0.01 s
With Transient Thermal Block Model	0.85 s
With Transient Thermal Grid Model	148 s

D. Simulation Time

Table II illustrates the framework's average consumed simulation time needed to calculate power and temperature values for one second of real time. The simulations were performed on an Intel four-core i5-760 2.80GHz CPU featuring 4 GB RAM.

VI. CONCLUSION

Power and thermal effect evaluations are important tasks during a product's development. Especially in the field of secure contactless reader / smart card systems, hardware and software must be tested against fault effects caused by magnetic field oversupply and thermal stress. Internal secrets must not be revealed, even under faulty conditions.

This paper presents a novel high-level design exploration framework focusing on secure contactless reader / smart card systems and thermal stress effects caused by high magnetic field strengths. Fault injection techniques are used to test software designs against fault effects caused by power oversupply and thermal stress. Thus, a framework is given, which allows hardware and software engineers to test their designs and explore design alternatives early during a product's development phase. We demonstrate the usage of this framework by means of a typical reader / smart card system. Furthermore, we present an innovative hardware design alternative to prolong the lifetime of smart card electronics, which is exposed to high magnetic field strengths.

Our future work concerns the integration of the thermal models into an emulation-based reader / smart card exploration framework. This approach enables fast hardware accelerated power and thermal behavior explorations.

ACKNOWLEDGMENTS

We would like to thank the Austrian Federal Ministry for Transport, Innovation, and Technology, which funded the project META[:SEC:] under the FIT-IT contract 829586. Furthermore, we would like to thank our industrial partners Infineon Technologies Austria AG as well as Enso Detego GmbH for their support.

REFERENCES

[1] N. Druml, M. Menghin, C. Steger, R. Weiss, A. Genser, H. Bock, and J. Haid, "Emulation-Based Test and Verification of a Design's Functional, Performance, Power, and Supply Voltage Behavior," in *21st Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP)*, 2013, pp. 328–335.

[2] K. Skadron, M. R. Stan, K. Sankaranarayanan, W. Huang, S. Velusamy, and D. Tarjan, "Temperature-aware microarchitecture: Modeling and implementation," *ACM Transactions on Architecture and Code Optimization (TACO)*, vol. 1, no. 1, pp. 94–125, March 2004.

[3] K. Rothbart, U. Neffe, C. Steger, R. Weiss, E. Rieger, and A. Muehlberger, "High level fault injection for attack simulation in smart cards," in *Asian Test Symposium (ATS)*, November 2004, pp. 118–121.

[4] M. Wendt, C. Grumer, C. Steger, R. Weiss, U. Neffe, and A. Muehlberger, "System Level Power Profile Analysis and Optimization for Smart Cards and Mobile Devices," in *ACM Symposium on Applied Computing*, November 2008, pp. 118–121.

[5] C. Bachmann, A. Genser, J. Haid, C. Steger, and R. Weiss, "Automated Power Characterization for Run-Time Power Emulation of SoC Designs," in *13th Euromicro Conference on Digital System Design (DSD)*, September 2010, pp. 587–594.

[6] M. Menghin, N. Druml, C. Steger, R. Weiss, H. Bock, and J. Haid, "The PTF-Determinator: A Run-Time Method Used to Save Energy in NFC-Systems," in *Fourth International EURASIP Workshop on RFID Technology (EURASIP RFID)*, September 2012, pp. 92–98.

[7] M. Gebhart, W. Eber, W. Winkler, D. Kovac, and H. Krepelka, "From power to performance in 13.56 MHz Contactless Credit Card technology," in *6th International Symposium on Communication Systems, Networks and Digital Signal Processing (CNSDSP)*, July 2008, pp. 301–305.

[8] P. Lall, "Tutorial: Temperature as an Input to Microelectronics-Reliability Models," *IEEE Transactions on Reliability*, vol. 45, no. 1, pp. 3–9, March 1996.

[9] D. Atienza, G. De Micheli, L. Benini, J. Ayala, P. Del Valle, M. DeBole, and V. Narayanan, "Reliability-aware design for nanometer-scale devices," in *Asia and South Pacific Design Automation Conference (ASP-DAC)*, March 2008, pp. 549–554.

[10] D. Atienza, P. G. Del Valle, G. Paci, F. Poletti, L. Benini, G. D. Micheli, J. M. Mendias, and R. Hermida, "HW-SW emulation framework for temperature-aware design in MPSoCs," *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, vol. 12, no. 3, pp. 26:1–26:26, May 2008.

[11] J. Arlat, M. Aguera, L. Amat, Y. Crouzet, J.-C. Fabre, J.-C. Laprie, E. Martins, and D. Powell, "Fault injection for dependability validation: a methodology and some applications," *IEEE Transactions on Software Engineering*, vol. 16, no. 2, pp. 166–182, February 1990.

[12] E. Jenn, J. Arlat, M. Rimen, J. Ohlsson, and J. Karlsson, "Fault injection into VHDL models: the MEFISTO tool," in *Twenty-Fourth International Symposium on Fault-Tolerant Computing, Digest of Papers*, June 1994, pp. 66–75.

[13] T. Kasper, D. Oswald, and C. Paar, "A Versatile Framework for Implementation Attacks on Cryptographic RFIDs and Embedded Devices," in *Transactions on Computational Science X*, ser. Lecture Notes in Computer Science, 2010, vol. 6340, pp. 100–130.

[14] S. Govindavajhala and A. Appel, "Using memory errors to attack a virtual machine," in *Symposium on Security and Privacy*, May 2003, pp. 154–165.

[15] A. Rahimi, L. Benini, and R. Gupta, "Analysis of instruction-level vulnerability to dynamic voltage and temperature variations," in *Design, Automation Test in Europe Conference Exhibition (DATE)*, March 2012, pp. 1102–1105.

[16] R. Kumar and V. Kursun, "Impact of temperature fluctuations on circuit characteristics in 180nm and 65nm CMOS technologies," in *IEEE International Symposium on Circuits and Systems (ISCAS)*, May 2006.

[17] M. Hutter, J.-M. Schmidt, and T. Plos, "RFID and its Vulnerability to Faults," in *Proceedings of the 10th international workshop on Cryptographic Hardware and Embedded Systems (CHES)*, 2008, pp. 363–379.

[18] C. Bolchini, A. Miele, and D. Sciuto, "Fault models and injection strategies in systemc specifications," in *11th EUROMICRO Conference on Digital System Design Architectures, Methods and Tools (DSD)*, September 2008, pp. 88–95.

[19] R. Shafik, P. Rosinger, and B. Al-Hashimi, "SystemC-Based Minimum Intrusive Fault Injection Technique with Improved Fault Representation," in *14th IEEE International On-Line Testing Symposium (IOLTS)*, July 2008, pp. 99–104.

[20] K. Finkenzeller, *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification*, 2nd ed. New York, NY, USA: John Wiley & Sons, Inc., 2003.

[21] J. Coburn, S. Ravi, and A. Raghunathan, "Power Emulation: A New Paradigm for Power Estimation," in *Design Automation Conference (DAC)*, June 2005, pp. 700–705.

[22] L. Chang, K. Vo, and J. Berg, "A simplifierd Model to predict the Linear Temperature Coefficient of a CMOS Inverters Delay Time," *IEEE Transactions on Electron Devices*, vol. 34, no. 8, pp. 1834–1837, August 1987.

Estimation Based Power and Supply Voltage Management for Future RF-Powered Multi-Core Smart Cards

Norbert Druml, Christian Steger and Reinhold Weiss
Institute for Technical Informatics
Graz University of Technology
Graz, Austria
{norbert.druml, steger, rweiss}@tugraz.at

Andreas Genser, Josef Haid
Design Center Graz
Infineon Technologies Austria AG
Graz, Austria
{andreas.genser, josef.haid}@infineon.com

***Abstract*—RF-powered smart cards are constrained in their operation by their power consumption. Smart card application designers must pay attention to power consumption peaks, high average power consumption and supply voltage drops. If these hazards are not handled properly, the smart card's operational stability is compromised.**

Here we present a novel multi-core smart card design, which improves the operational stability of nowadays used smart cards. Estimation based techniques are applied to provide cycle accurate power and supply voltage information of the smart card in real time. A supply voltage management unit monitors the provided power and supply voltage information, flattens the smart card's power consumption and prevents supply voltage drops by means of a dynamic voltage and frequency scaling (DVFS) policy.

The presented multi-core smart card design is evaluated on a hardware emulation platform to prove its proper functionality. Experimental tests show that harmful power variations can be reduced by up to 75% and predefined supply voltage levels are maintained properly. The presented analysis and management functionalities are integrated at a minimal area overhead of 10.1%.

I. Introduction

A smart card system is generally divided into two components: A reader device and the smart card itself. The reader device generates an RF field, which is used for both power supply and communication purposes. This RF field induces an electrical current in the smart card's antenna to power the smart card's electronics. Fig. 1 illustrates this principle. In order to ensure a reliable operation of the smart card, the following aspects need to be considered.

The available electrical power is very limited and depends on the distance between smart card and reader device, antenna design and orientation, etc. Attention must be paid to high average power consumption, high power peaks and card movements within the RF field. These issues may cause the processor's supply voltage to fluctuate. In case the supply voltage drops below a certain threshold, the system's operational stability can not be guaranteed anymore. Fig. 2 shows the severe impact of high power consumption changes on the smart card's supply voltage: The greater the power consumption increase, the more severe the supply voltage drops. A smart card power management system must consider the following crucial points:

- The power consumption needs to be flattened to reduce the possibility for supply voltage drops.
- The processor's supply voltage must not drop below a certain threshold to avoid malfunctions.

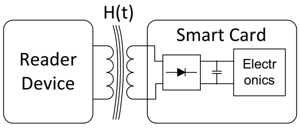


Fig. 1. Principle of a smart card system consisting of the smart card and a reader device, which generates a RF field for power supply and communication purposes.

978-3-9810801-8-6/DATE12/©2012 EDAA

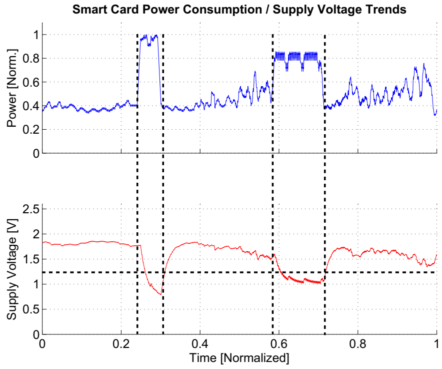


Fig. 2. This graph shows the influences of power consumption changes on the smart card system's supply voltage. The greater the power consumption increases, the more severe the supply voltage drops. If the supply voltage drops below the threshold, operation stability is lost.

This paper makes the following contributions. It presents a novel multi-core smart card design, which is enhanced with estimation based power and supply voltage analysis capabilities to detect hazards, such as high average power consumption, power consumption peaks and supply voltage drops. Furthermore, a supply voltage management unit is used to dynamically adapt the smart card processor cores' clock frequency and voltage parameters. With the help of a dynamic voltage and frequency scaling (DVFS) policy, the smart card's power consumption is being flattened and supply voltage drops are avoided. Thus, the stability of the smart card is improved.

II. Related Work

A. Power Analysis

Power analysis is a technique to determine the power consumption of electric circuits. It is basically done either *measurement based* or *estimation based*. Power estimation is conducted at any abstraction level and can be further subdivided into *simulation based* and *hardware accelerated* techniques. Depending on the abstraction level and the circuit size, simulation based approaches can consume a significant amount of calculation time. Hardware accelerated power estimation is performed to speed up the complex and time intense calculations. It is achieved by integrating synthesizeable power simulation algorithms and estimation algorithms in hardware. Implementations are presented in [1] and [2]. Coburn et al. coined in [3] the term *Power Emulation* by integrating a design-under-test as well as register transfer level power macromodels into an FPGA to estimate the power consumption of the design-under-test. A system-level power emulation implementation is presented in [4].

B. Power Management

Dynamic power management describes techniques to save power in integrated circuits according to their states of operation. Tiwari et al. describe in [5] several methodologies like clock gating, guarded evaluation, bus deactivation, etc. In contrast to other dynamic power management methods, DVFS offers an elegant way for power consumption adjustments of integrated circuits according to the CMOS dynamic power consumption equation. Multi-core DVFS approaches can be divided into per-core and chip-wide DVFS. Investigations regarding these two strategies are conducted in [6] and show that power saving improvements of up to 21% can be achieved if per-core DVFS strategies are applied in a four-core processor system. Various DVFS policy implementations are evaluated in [7] and [8].

C. Supply Voltage Analysis

Supply voltage analysis covers methodologies to determine the supply voltage of electric circuits. Supply voltage analysis is either done at design time or at run time. A simulation based approach, which models a power supply network, is presented in [9]. Voltage drops are detected in [10] with the help of on-die circuits. Analog-to-digital converters [11] and voltage comparators [12] are further possibilities to detect hazardous supply voltage levels. A supply voltage emulation approach is suggested in [13]. In this estimation based method, the design-under-test as well as a supply voltage analysis unit are integrated into an FPGA. Supply voltage estimates are performed in hardware and in real time.

D. Supply Voltage Management

Supply voltage management methods are based upon supply voltage analysis techniques and are applied to control an electric circuit's supply voltage level. On-die circuits are presented in [10] to compensate supply voltage drops. Up to 100 mA are injected into specific nodes. In [14], supply voltage drops are prevented by shaping the electrical current with the help of a semi-asynchronous architecture. A predictive approach is presented in [15]. Signatures of the running program are compared to hazardous patterns. In case of a match, the processor is throttled and the supply voltage regenerates. Supply voltage emulation approaches, as presented in [13], are also used in conjunction with DVFS techniques to prevent supply voltage hazards.

III. Estimation Based Power / Voltage Analysis and Management

The proposed novel smart card design consists of a symmetric dual-core processor, which is enhanced with estimation based power consumption and supply voltage analysis units as well as a supply voltage management unit. In the following paragraph, each smart card component will be described in detail.

A. Power Estimation Unit

The used power estimation unit is based upon an approach from [4]. Its task is to derive power consumption information of the smart card processor cores based on their internal system states. The basic functionality is depicted in Fig. 3. The power estimation unit features a linear regression based smart card power model, which is based upon [16]. This hardware integrated power model is defined by (1) and (2).

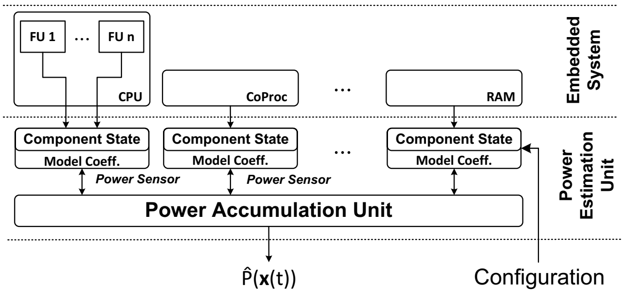


Fig. 3. Power estimation unit gathering power information by observing the system activity, obtained with changes from [4].

$$\widehat{P}(\mathbf{x}) = \widehat{P}_{stat} + \widehat{P}_{dyn} = c_0 + \sum_{i=1}^{n} c_i \cdot x_i = c_0 + \mathbf{c^T} \cdot \mathbf{x} \quad (1)$$

$$P(\mathbf{x}) = \widehat{P}(\mathbf{x}) + \epsilon \quad (2)$$

$\mathbf{x} = [x_1, x_2, x_3, ...]$ is a vector, whose elements specify a certain system state (e.g., memory read, memory write, CPU running, etc). Every system state x_i has a model coefficient c_i from the vector $\mathbf{c^T} = [c_1, c_2, c_3, ...]^T$ assigned to itself. A model coefficient c_i defines how much power is dissipated while being in the corresponding system state x_i. These model coefficients c_i and the leakage power consumption c_0 are obtained from a power model characterization process. The linear combinations of x_i and c_i plus c_0 form the power estimates $\widehat{P}(\mathbf{x})$. The difference between the estimated value $\widehat{P}(\mathbf{x})$ and the real value $P(\mathbf{x})$ is given by the error ϵ. A time dependency is introduced by $\widehat{P}(\mathbf{x}(t))$, because system states may change at any clock cycle.

B. DVFS Scaling

Power estimates $\widehat{P}(\mathbf{x})$ are based upon a smart card processor core, which is operated at a clock frequency f of 1 MHz. To respect the possibility of operating a processor core at various clock frequencies and voltage parameters, a DVFS scaling unit is introduced. This unit scales the 1 MHz based power estimates $\widehat{P}(\mathbf{x(t)})$ according to (3).

$$\widehat{P}(\mathbf{x(t)}, f(t), V_{DD}(t)) = \widehat{P}(\mathbf{x(t)}) \cdot f(t) \cdot {V_{DD}}^2(t) \quad (3)$$

A lookup table (LUT) approach is used in this unit, which maps each supported processor clock frequency $f(t)$ to a dedicated voltage $V_{DD}(t)$. The architecture of the hardware integrated DVFS scaling unit is depicted in Fig. 4.

C. Supply Voltage Estimation Unit

According to [17], an equivalent electrical circuit of a contactless smart card power supply network can be drawn as depicted in Fig. 5. $v_i(t)$ represents the rectified voltage, which is supplied by the RF

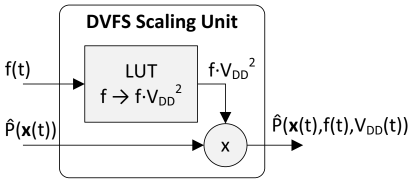


Fig. 4. Architecture of the DVFS scaling unit.

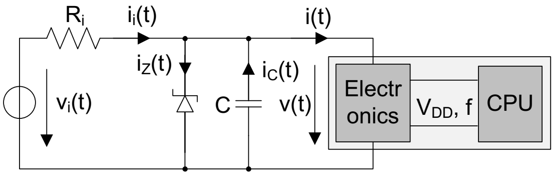


Fig. 5. Equivalent circuit of a smart card power supply network, obtained with changes from [17]. $v(t)$ represents the crucial supply voltage, which is applied to the smart card's electronics.

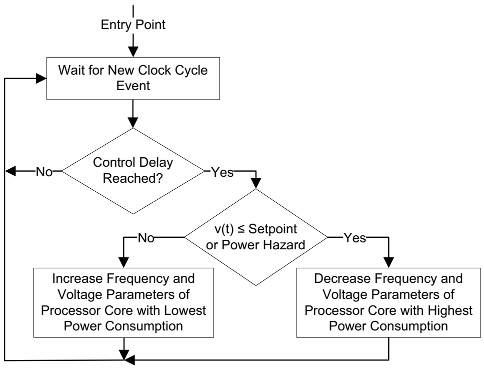

Entry Point
Wait for New Clock Cycle Event
Control Delay Reached?
No
Yes
v(t) ≤ Setpoint or Power Hazard
No
Yes
Increase Frequency and Voltage Parameters of Processor Core with Lowest Power Consumption
Decrease Frequency and Voltage Parameters of Processor Core with Highest Power Consumption

Fig. 7. Flow chart of the proposed per-core DVFS policy dealing with supply voltage and power consumption hazards.

field to the smart card's antenna. A voltage sensor is typically used to retrieve the voltage level of $v_i(t)$. Capacitor C buffers electrical charges and is charged / discharged depending on the processor's power consumption. The charge level of this capacitor C defines the supply voltage $v(t)$ of the smart card's electronics according to (4).

$$v(t) = \frac{Q_C(t)}{C} \tag{4}$$

$i(t)$ is derived from the power consumption information, which is estimated and delivered by the power estimation unit. An electrical charge based mathematical model computes the crucial supply voltage $v(t+1)$ according to (5). Δt represents the reciprocal value of the currently set processor clock frequency. The presented calculations can be implemented in hardware easily. Modeling the transient behavior of a switching capacitor is normally expressed by an exponential based function. With the help of the introduced charge based approach, an expensively hardware integrated exponential function is bypassed.

$$v(t+1) = \frac{Q_C(t) + \frac{v_i(t)-v(t)}{R_i}\Delta t - i(t)\Delta t}{C} \tag{5}$$

The functionality of the hardware integrated supply voltage estimation unit has been verified with SPICE simulations of the underlying model. A mean squared error in the range of only 10^{-5} is detectable. Fig. 6 illustrates the results. Note, according to [17], the maximum error between physical measurements and the smart card's power supply network model is as high as 2%.

D. Supply Voltage Management Unit

The DVFS technique is used to modify the power consumption of each smart card processor core by modifying voltage V_{DD} and frequency f parameters. DVFS has a cubic impact on the power consumption but a linear impact on the performance. Fig. 7 illustrates the per-core DVFS policy, which is optimized for multi-core smart cards. This policy uses the provided supply voltage and power consumption estimates for DVFS control decisions. Therefore, fast power consumption changes as well as slightly slower and delayed supply voltage variations are handled simultaneously. The DVFS policy supports a user defined supply voltage setpoint.

- For the case where the instantaneous supply voltage $v(t)$ is lower than the supply voltage setpoint or a power consumption hazard is detected, the processor core with the highest power consumption has its clock frequency f and voltage level V_{DD} decreased.
- Otherwise, if the instantaneous supply voltage $v(t)$ is higher than the supply voltage setpoint and no power consumption hazard is detected, the processor core with the lowest power consumption is accelerated and its voltage level is increased.

A control delay is added to cope with the switching delays and settling times of on-chip voltage and frequency regulators. This DVFS policy is designed to flatten the smart card's power consumption and to prevent supply voltage drops simultaneously. Furthermore, the performance of the smart card is optimized regarding the defined supply voltage setpoint constraint.

E. Power and Supply Voltage Aware Smart Card

Fig. 8 shows the proposed architecture of the novel power and supply voltage aware multi-core smart card. The processor cores' system states $\mathbf{x}_i(t)$ are monitored and their associated power consumption information $\widehat{P}(\mathbf{x}_i(t))$ is delivered by power estimation units. Then, $\widehat{P}(\mathbf{x}_i(t))$ is scaled according to the currently set voltage V_{DDi} and frequency f_i parameters. The results, $\widehat{P}(\mathbf{x}_i(t), f_i(t), V_{DDi}(t))$ are summed up and form the power consumption value $\widehat{P_S}(t)$. $\widehat{P_S}(t)$ is then forwarded to the supply voltage estimation unit. The supply

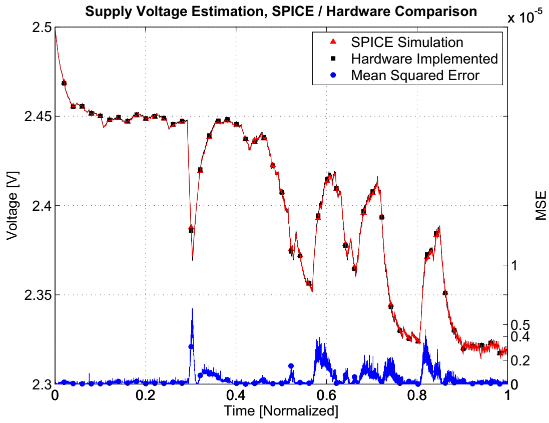


Fig. 6. Accuracy comparison of the hardware integrated supply voltage estimation unit and SPICE simulations of the underlying model.

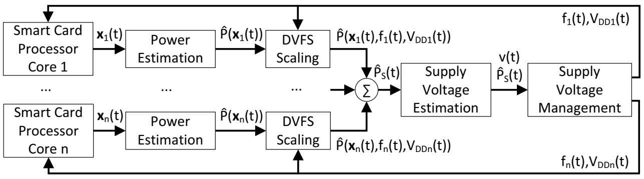

Smart Card Processor Core 1
x_1(t)
Power Estimation
P̂(x_1(t))
DVFS Scaling
P̂(x_1(t),f_1(t),V_DD1(t))
f_1(t),V_DD1(t)
P̂_S(t)
Σ
Supply Voltage Estimation
v(t)
P̂_S(t)
Supply Voltage Management
...
Smart Card Processor Core n
x_n(t)
Power Estimation
P̂(x_n(t))
DVFS Scaling
P̂(x_n(t),f_n(t),V_DDn(t))
f_n(t),V_DDn(t)

Fig. 8. Architecture of the proposed power and supply voltage aware multi-core smart card.

voltage estimation unit delivers the supply voltage $v(t)$ information of the smart card's electronics by means of the presented power supply network model. The supply voltage $v(t)$ and power consumption $\widehat{P}_S(t)$ information is then forwarded to the supply voltage management unit. This unit controls the smart card processor cores' DVFS parameters V_{DDi} and f_i according to the proposed per-core DVFS policy.

IV. Hardware Emulation

Experimental results are gained by performing functional emulation as well as power and supply voltage emulation of the proposed future multi-core smart card. Fig. 9 illustrates the basic concept of this emulation approach. The emulation system is built by integrating the smart card processor cores as well as the power estimation, supply voltage estimation and management units into a Xilinx Spartan 3 FPGA. Relevant trace information is generated and transmitted with the help of an Ethernet interface to a host PC. The data is collected by the PC and further analysis and verification tasks are performed. This method allows power consumption and supply voltage analysis of a design-under-test early in its design stage. Power bugs within the smart card design can be found and corrected before the tape-out.

V. Experimental Results

The smart card's power estimation and supply voltage estimation units are used to survey the power consumption and supply voltage behavior while executing various benchmarks. The supply voltage management unit is used during these tests to monitor and control the stability of the smart card. A supply voltage setpoint of 1.7 V is defined and DVFS techniques are applied to maintain it. MiBench [18], a representative benchmarking suite for embedded systems, is used for reproducible testing purposes. Table I explains the shown parameters of the following figures.

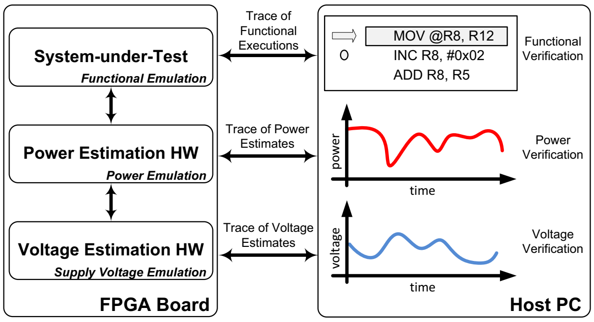


Fig. 9. Principle of the emulation system, obtained with changes from [4].

TABLE I
Description of the Used Figure Parameters

Parameter	Description
$\widehat{P}_S(t)$	Processor cores 1 and 2 power consumption summation.
$v(t)$	Supply voltage, which is applied to the smart card's electronics.
$v_i(t)$	Rectified supply voltage, which is generated by the RF field.
f_{Ci}	Clock frequencies, which are applied to processor cores 1 and 2.
VDD_{Ci}	Voltage values, which are applied to processor cores 1 and 2.

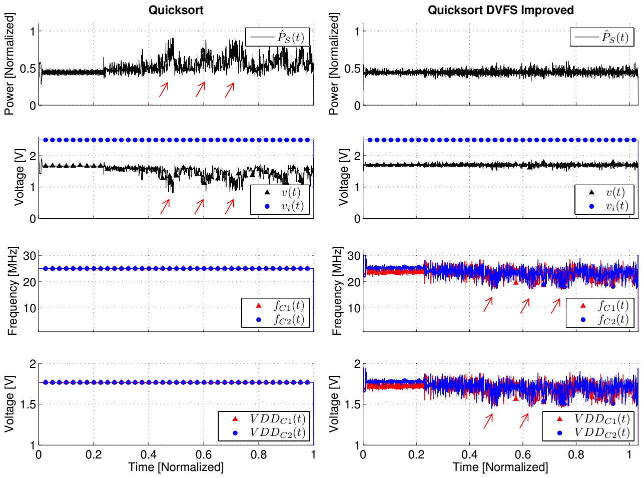


Fig. 10. The left subplots show the unmanaged behavior of the smart card while performing a Quicksort benchmark and applying a fixed clock frequency of 25 MHz. $v(t)$ drops below 1 V. The right subplots show the DVFS managed smart card behavior. The power consumption $\widehat{P}_S(t)$ is flattened and $v(t)$ supply voltage drops are avoided.

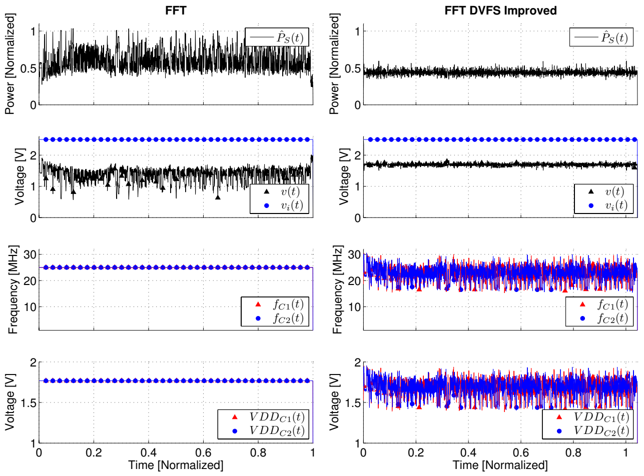


Fig. 11. The left subplots show the unmanaged behavior of the smart card while performing an FFT benchmark and applying a fixed clock frequency of 25 MHz. $v(t)$ drops below 1 V. The right subplots show the DVFS managed smart card behavior. The power consumption $\widehat{P}_S(t)$ is flattened and $v(t)$ supply voltage drops are avoided.

The left subplots of Fig. 10 and Fig. 11 illustrate the unmanaged curves of FFT and Quicksort benchmarking tests while operating the smart card at a fixed clock frequency of 25 MHz. Arrows mark significant $\widehat{P}_S(t)$ power consumption increases. These power consumption hazards cause supply voltage drops below 1 V. Thus, the operational stability of the smart card is compromised. The right subplots of Fig. 10 and Fig. 11 show the curves of the smart card's behavior while taking advantage of the supply voltage management unit. The user defined supply voltage setpoint of 1.7 V is maintained and the power consumption $\widehat{P}_S(t)$ is flattened simultaneously. Arrows mark significant DVFS parameter reductions when $v(t)$ supply voltage hazards are recognized. Thus, the smart card's operational stability is provided. Due to the DVFS interventions, the total runtime of Quicksort and FFT benchmarks are increased by 3.3% and 4.4%, respectively.

Table II shows standard deviation delta values of the total power

TABLE II
COMPARISON OF STANDARD DEVIATION AND PERFORMANCE VALUES

Benchmark	Setpoint	$\Delta\sigma(\widehat{P}_S(t))$	$\Delta\sigma(v(t))$	Perf. Degrad.
Quicksort	1.70 V	-69%	-72%	3.3%
Basicmath	1.70 V	-75%	-78%	13.6%
FFT	1.70 V	-75%	-76%	4.4%
Quicksort	1.66 V	-68%	-72%	0%
Basicmath	1.50 V	-62%	-67%	0%
FFT	1.61 V	-71%	-74%	0%

consumption $\widehat{P}_S(t)$ and the supply voltage $v(t)$ as well as performance degradation values of three selected benchmarks. The standard deviation metric is an indicator for the severity of power consumption peaks and supply voltage drops. The higher the power consumption standard deviation, the higher the possibility for severe supply voltage drops, and consequently the lower the smart card's stability. Comparisons are done between an unmanaged smart card running at 25 MHz and the DVFS managed smart card, which is controlled at a supply voltage setpoint of 1.7 V. Furthermore, results of benchmarks with supply voltage setpoints are presented, which do not cause any performance degradation compared to the 25 MHz reference. This is achieved by reducing a supply voltage setpoint, which speeds up the processor cores. According to the presented results, power consumption standard deviation reductions of up to 75% can be obtained during the FFT benchmark while degrading the performance by only 4.4% . If the FFT benchmark's supply voltage setpoint is reduced by 0.09 V, a power consumption standard deviation reduction of 71% can still be accomplished without degrading the performance.

A. Performance Degradation Investigations

If DVFS modifications are conducted, then the runtime of the executed program can be influenced. Fig. 12 illustrates the performance degradation trend of the FFT benchmark depending on the selected supply voltage setpoint. Results are obtained from hardware emulations. A smart card constantly running at 25 MHz is used as performance reference. The higher the supply voltage setpoint, the lower the power dissipation, but the higher the performance degradation.

If the smart card's electronics allow a supply voltage setpoint reduction, then the processor cores can be operated at a higher clock frequency than the 25 MHz reference. According to Fig. 12, a FFT benchmark performance increase is detectable if supply voltage setpoints of less than 1.61 V are applied.

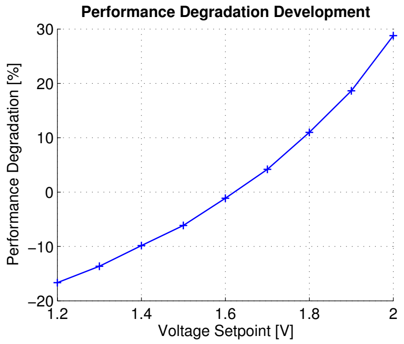


Fig. 12. FFT benchmark performance degradation, compared to a reference smart card running at 25 MHz. The higher the supply voltage setpoint, the higher the performance degradation.

B. Accuracy of the Results

The accuracy of the proposed smart card's analysis and management units is mainly controlled by the power estimation unit: Supply voltage estimates are based upon power consumption estimates and DVFS decisions are based upon supply voltage estimates. According to [4], the maximum average error of the power estimation unit is as high as 8.4%. Comparisons are conducted between power consumption estimates and gate-level power simulations. The power estimation unit's accuracy can be improved easily by considering more signals of the smart card's processor during the power model characterization process.

[17] shows that the model of the smart card's power supply network, which is implemented in the supply voltage estimation unit, accounts for an average error of 2%. The difference between SPICE and hardware integrated power supply network model is in the range of only 10^{-5} and can therfore be neglected.

C. Area Overhead

The proposed enhanced smart card design requires only an additional area overhead of 10.1%. Table III shows a detailed area breakdown of each smart card component. These results are gained from synthesis on a Xilinx Spartan 3 FPGA platform. There is still optimization potential available. For example, the size of the power and supply voltage estimation units can be reduced significantly if less accuracy would be sufficient or if only one processor core would be supported.

VI. Case Study: Smart Card Movements

In the following case study, a reader device generates an RF field and the smart card is moved within this field. Fig. 13 depicts the case study's setup. Due to the smart card movement, the smart card is exposed to a varying RF field strength. A varying RF field strength induces a varying electrical current in the smart card's antenna. Consequently, the supply voltage $v_i(t)$, the charge level $Q_C(t)$ of the capacitor C as well as the smart card electronics' supply voltage $v(t)$ are affected. The smart card movement is modeled by a triangular characteristic of $v_i(t)$. The aim of this case study is to verify if the proposed power and supply voltage aware smart card is able to cope with such instable environmental conditions.

The left subplots of Fig. 14 illustrate the unmanaged power consumption, supply voltage and DVFS parameter curves of the Quicksort benchmark while $v_i(t)$ changes. As a result, the crucial

TABLE III
AREA CONSUMPTION BREAKDOWN OF THE PROPOSED POWER AND SUPPLY VOLTAGE AWARE MULTI-CORE SMART CARD

Component	Area Overhead
Two-Core Smart Card Processor	-
Power Estimation Units	4.8%
Supply Voltage Estimation Unit	3.8%
Supply Voltage Management Unit	1.4%
Total Area Overhead	10.1%

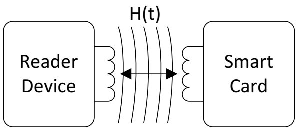


Fig. 13. Illustration of the case study's setup. The smart card is moved within the RF field. Therefore, a varying amount of electrical power is drawn from the RF field.

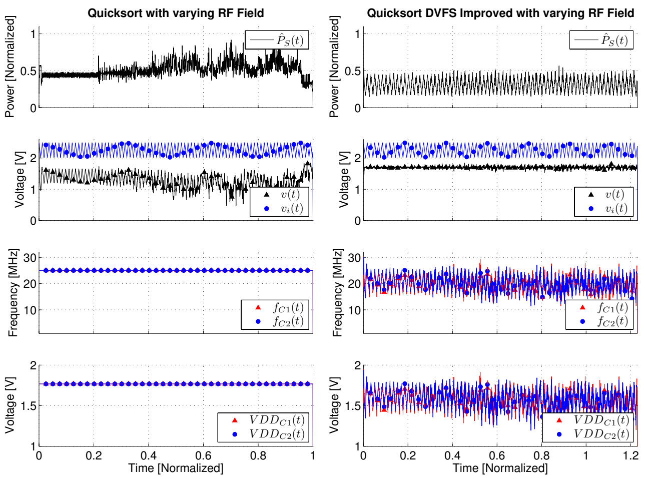


Fig. 14. The left subplots show the unmanaged smart card behavior while moving the smart card within the RF field and performing a Quicksort benchmark. No $v(t)$ stability is given. The right subplots show the same test but with activated DVFS management. $v(t)$ stability is provided properly.

supply voltage $v(t)$ shows a high amount of instability and drops several times down to 0.5 V. The operational stability of the smart card is compromised. The right subplots of Fig. 14 show the behavior of the DVFS enhanced smart card. It is able to stabilize the supply voltage $v(t)$ at the predefined setpoint of 1.7 V properly. No hazardous supply voltage drops are detectable, even under these challenging environmental conditions. Thus, the smart card's operational stability is given. As a further consequence of DVFS interventions, a performance degradation of 22% is observable.

VII. Conclusion

RF-powered smart cards are constrained in their operation by their power consumption. At the time a smart card and its corresponding application is designed, attention must be paid to high average power consumption, power peaks and supply voltage drops. If these power and supply voltage variations are not handled properly, the operational stability of a smart card can be compromised.

This paper proposes a novel multi-core smart card design, which is enhanced with analysis and management functionalities to cope with power consumption and supply voltage hazards. Power estimation and supply voltage estimation units are used to provide cycle accurate power consumption and supply voltage information of the smart card in real time. This information is passed to a supply voltage management unit. The supply voltage management unit flattens the smart card's power consumption, prevents supply voltage drops and optimizes the smart card's performance for a predefined supply voltage setpoint by means of a DVFS policy. Experimental results show that the smart card's power consumption standard deviation can be reduced by up to 75%. The enhanced smart card design also copes with varying RF field strengths and maintains a predefined supply voltage threshold properly. The suggested analysis and management units can be integrated into a smart card design with an additional needed area overhead of only 10.1%.

Acknowledgments

We would like to thank our industrial partners Infineon Technologies Austria GmbH as well as RF-iT Solutions GmbH for their support. Furthermore, we would like to thank the Austrian Federal Ministry for Transport, Innovation, and Technology, which funded the projects META[:SEC:] and POWERHOUSE under the FIT-IT contracts FFG 829586 and FFG 815193, respectively.

References

[1] R. Joseph and M. Martonosi, "Run-Time Power Estimation in High Performance Microprocessors," in *International Symposium on Low Power Electronics and Design*, 2001.

[2] J. Haid, G. Kaefer, C. Steger, and R. Weiss, "Run-Time Energy Estimation in System-On-a-Chip Designs," in *Proceedings of the 2003 Asia and South Pacific Design Automation Conference*, 2003.

[3] J. Coburn, S. Ravi, and A. Raghunathan, "Power Emulation: A New Paradigm for Power Estimation," in *Design Automation Conference*, 2005.

[4] A. Genser, C. Bachmann, J. Haid, C. Steger, and R. Weiss, "An Emulation-Based Real-Time Power Profiling Unit for Embedded Software," in *International Conference on Embedded Computer Systems: Architectures, Modeling and Simulation*, 2009.

[5] V. Tiwari, R. Donnelly, S. Malik, and R. Gonaalea, "Dynamic Power Management for Microprocessors: A Case Study," in *International Conference on VLSI Design*, 1997.

[6] W. Kim, M. Gupta, G. Wei, and D. Brooks, "System Level Analysis of Fast, Per-Core DVFS using On-Chip Switching Regulators," in *IEEE International Symposium on High Performance Computer Architecture*, 2008.

[7] S. Herbert and D. Marculescu, "Analysis of Dynamic Voltage/Frequency Scaling in Chip-Multiprocessors," in *ACM/IEEE International Symposium on Low Power Electronics and Design*, 2007.

[8] C. Isci, A. Buyuktosunoglu, C. Cher, P. Bose, and M. Martonosi, "An Analysis of Efficient Multi-Core Global Power Management Policies: Maximizing Performance for a Given Power Budget," in *IEEE/ACM International Symposium on Microarchitecture*, 2006.

[9] E. Grochowski, D. Ayers, and V. Tiwari, "Microarchitectural simulation and control of di/dt-induced power supply voltage variation," in *International Symposium on High-Performance Computer Architecture*, 2002.

[10] M. Holtz, S. Narasimhan, and S. Bhunia, "On-Die CMOS Voltage Droop Detection and Dynamic Compensation," in *Proceedings of the 18th ACM Great Lakes symposium on VLSI*, 2008.

[11] E. Alon, V. Stojanovic, and M. Horowitz, "Circuits and Techniques for High-Resolution Measurement of On-Chip Power Supply Noise," in *IEEE Journal of Solid-State Circuits*, vol. 40, 2005.

[12] T. Nakura, M. Ikeda, and K. Asada, "Preliminary Experiments for Power Supply Noise Reduction using Stubs," in *Proceedings of IEEE Asia-Pacific Conference on Advanced System Integrated Circuits*, 2004.

[13] A. Genser, C. Bachmann, J. Haid, C. Steger, and R. Weiss, "Supply Voltage Emulation Platform for DVFS Voltage Drop Compensation Explorations," in *IEEE International Symposium on Performance Analysis of Systems and Software*, 2011.

[14] M. Badaroglu, K. Tiri, S. Donnay, P. Wambacq, I. Verbauwhede, G. Gielen, and H. De Man, "Clock Tree Optimization in Synchronous CMOS Digital Circuits for Substrate Noise Reduction Using Folding of Supply Current Transients," in *Design Automation Conference*, 2002.

[15] V. Reddi, M. Gupta, G. Holloway, G. Wei, M. Smith, and D. Brooks, "Voltage Emergency Prediction Using Signatures to Reduce Operating Margins," in *International Symposium on High Performance Computer Architecture*, 2009.

[16] A. Bogliolo, L. Benini, and G. De Micheli, "Regression-based RTL power modeling," in *ACM Transactions on Design Automation of Electronic Systems*, vol. 5, 2000.

[17] M. Wendt, C. Grumer, C. Steger, and R. Weiss, "System Level Power Profile Analysis and Optimization for Smart Cards and Mobile Devices," in *Proceedings of the 2008 ACM Symposium on Applied Computing*, 2008.

[18] M. R. Guthaus, J. S. Ringenberg, D. Ernst, T. M. Austin, T. Mudge, and R. B. Brown, "MiBench: A free, commercially representative embedded benchmark suite," in *IEEE International Workshop on Workload Characterization*, 2001.

2012 15th Euromicro Conference on Digital System Design

Adaptive Field Strength Scaling – A Power Optimization Technique for Contactless Reader / Smart Card Systems

Norbert Druml, Manuel Menghin,
Christian Steger and Reinhold Weiss
Institute for Technical Informatics
Graz University of Technology
Graz, Austria
{norbert.druml, manuel.menghin, steger, rweiss}@tugraz.at

Andreas Genser, Holger Bock and
Josef Haid
Design Center Graz
Infineon Technologies Austria AG
Graz, Austria
{andreas.genser, holger.bock, josef.haid}@infineon.com

***Abstract*—Many near field communication (NFC)-based reader / smart card applications are operated at a maximum magnetic field strength to increase the smart card's operational stability. However, a maximum magnetic field strength is worthwhile only in situations of high smart card power requirements (e.g., performing cryptographic operations) or long distance communications. As a result, electrical power is wasted, which limits the run-time of mobile battery-operated reader devices.**

Here we present an adaptive field strength scaling (AFSS) methodology. The strength of the reader's emitted magnetic field is modified depending on the instantaneous power consumption requirements of the smart card. When the smart card consumes less power, the magnetic field strength is reduced. Whereas when it consumes more power, the magnetic field strength is increased. Thus, the power consumption of the reader / smart card system as a whole is optimized while preserving the smart card's operational stability.

In this work, we present the design and implementation of two different AFSS approaches. A reader / smart card hardware emulation platform is used to prove the AFSS technique's feasibility and proper functionality. Experimental tests demonstrate that the energy consumption of the AFSS enhanced reader / smart card system can be reduced by up to 54% compared to current commonly used approaches. Furthermore, we show that the smart card's stability is preserved if the AFSS technique is applied.

I. Introduction

A smart card system, as depicted in Fig. 1, consists of a reader device and the smart card itself. The reader generates a magnetic field, which is used to power the smart card and for communication purposes. The transferred power to the smart card is very limited and depends on several system characteristics, e.g., antenna designs, smart card placement within the magnetic field, antenna output gain. Communication between reader and smart card is performed by means of magnetic field modulations. A permanent and sufficient power supply is uncertain. As a consequence, many near field communication (NFC)-based applications are designed to operate the reader at a maximum possible magnetic field strength, even if a lower field strength would suffice. If the electrical power provided by the reader's magnetic field is higher than the smart card's power consumption, the smart card's integrated capacitor stores the excessive electrical power. However, if the voltage across the capacitor exceeds a certain level, the smart card's shunt regulator (in Fig. 1 represented by a Zener diode) dissipates the excessive electrical power to prevent electric surges. This approach to using a maximum possible field strength increases the smart card's operational stability but electrical power is wasted at the same time. This power wastage results in a reduced run-time of mobile battery-operated readers. This run-time limiting issue is of eminent importance because of the increasing number of NFC enabled smart phones and the increasing availability of NFC-based applications, e.g., payment, ticketing, e-passports.

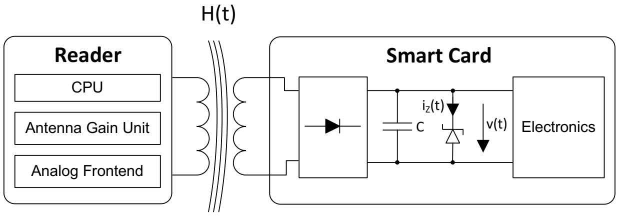


Fig. 1. Principle of a reader / smart card system. The reader generates a magnetic field for power supply and communication purposes. The induced electrical current is rectified and afterwards buffered within the capacitor C. A Zener diode prevents the electronics from electric surges.

According to Fig. 1, the reader generates a magnetic field $H(t)$ that is used for communication and power supply purposes. The strength of the magnetic field can be varied by the antenna gain unit. The magnetic field induces a variable electrical current in the smart card. This electrical current is rectified and the electrical charges are then buffered within the capacitor C. Depending on the smart card's power consumption, the charge level of the capacitor changes. If the smart card's current consumption is lower than the induced

We would like to thank the Austrian Federal Ministry for Transport, Innovation, and Technology, which funded the project META[:SEC:] under the FIT-IT contract 829586.

978-0-7695-4798-5/12 $26.00 © 2012 IEEE
DOI 10.1109/DSD.2012.20

current by the magnetic field, then the capacitor's charge level increases. If this behavior is left unchecked, the smart card's electronics may be damaged by a power surge caused by excessive supply voltage. This problem is solved by adding a shunt regulator, in the form of a Zener diode, that limits the supplied voltage $v(t)$ by bleeding off any excessive electrical charges. An improvement to save electrical power at a reader / smart card system abstraction level would be to adapt the strength of the emitted magnetic field to the instantaneous power requirements of the smart card. If the smart card consumes a high amount of electrical power (e.g., during cryptographic operations), the reader increases the magnetic field strength. Otherwise, during idle times and low power consuming periods, the reader decreases the magnetic field strength to save electrical power. Thus, the reader / smart card system's power consumption is optimized, the run-time of battery-operated readers is prolonged, and the operational stability of the smart card is preserved.

This paper makes the following contributions:

- It proposes a novel reader / smart card system operational technique, called adaptive field strength scaling (AFSS).
- AFSS optimizes the reader's power consumption and preserves the smart card's operational stability simultaneously. This is achieved by adapting the strength of the magnetic field dynamically according to the instantaneous power consumption requirements of the smart card.
- A hardware emulation approach is used to prove the feasibility and proper functionality of the proposed AFSS methodology.

II. Related Work

A. Power Analysis

Power analysis techniques are performed to determine the power consumption of electric circuits. Analyses can either be conducted *measurement-based* or *estimation-based*. Estimation-based analyses are conducted *simulation-based* or *hardware accelerated*. To speed-up the time-intense simulation algorithms, the hardware accelerated approach can be used. In [1], hardware performance counters are used to estimate the power consumption of the target device by means of a dedicated power model. Coburn et al. presented in [2] the *Power Emulation* technique. Power Emulation integrates the design-under-test as well as a power model into an FPGA. By means of this technique, the design-under-test's power consumption can be estimated cycle accurately at register-transfer level. Thus, power bugs can be found during a hardware's design stage and can be corrected before the tape-out.

B. Power Aware Approaches in RFID and NFC

In [3] and [4], the authors propose novel power optimized reader architectures. In [5], the electrical power, which is available to a smart card, is estimated depending on certain coupling factors. Then, these results are compared to various cryptographic power requirements. Thus, estimates can be conducted to test if a certain cryptographic algorithm can be feasibly implemented. A power-aware smart card design is presented by [6]. An adiabatic circuit design is used to minimize the power consumption. Further power optimization methods have been proposed in the field of RFID protocols. In [7], the authors present a novel power optimized RFID inventory estimation algorithm. An automatic power stepping algorithm is presented by [8], which estimates the number of available RFID tags by increasing the reader's power output gain continuously. Thus, the reader is able to save up to 60% of its power consumption.

C. Supply Voltage Analysis and Management

Supply voltage analysis describes techniques to determine the supply voltage of electric circuits. Analysis and management of a circuit's supply voltage is of importance, because a high amount of simultaneously switching transistors draws a lot of current from the capacitor and that can cause hazardous supply voltage variations. Proposed methodologies can be subdivided into design-time and run-time approaches. In [9], the authors highlight the problem of voltage variations in microprocessor systems. They also demonstrate a way to simulate and control such voltage variations by modeling the power supply network. A smart card power supply network model has been presented by the authors in [10], which is used in simulations to detect hazardous supply voltage drops. Using a semi-asynchronous architecture [11] or adding decoupling capacitors [12] are further design-time techniques to reduce voltage variations. During run-time, analog-to-digital converters [13] and voltage comparators [14] can be used for analysis purposes. In [15], the authors compare signatures of the running program with hazardous signatures to counteract voltage emergencies. Another way to resolve voltage drops has been presented by [16]. On-die circuits are used to inject electrical current into nodes that are affected by hazardous voltage variations.

III. Adaptive Field Strength Scaling

Adaptive field strength scaling (AFSS) is a methodology to adapt the strength of the magnetic field, which is generated by the reader, according to the smart card's instantaneous power consumption. Figure 2 illustrates this principle. The *H-Field Static* curve represents current approaches of generating a magnetic field of maximum strength. The *H-Field Adapted* curve represents the novel AFSS approach. During the smart card's high power consuming periods (e.g., performing cryptographic operations), the reader increases the magnetic field strength. Otherwise, during the smart card's idle times and low power consuming periods, the reader decreases the magnetic field strength to save electrical power. This paper presents two different AFSS approaches:

- Magnetic field strength scaling decisions are based upon a *smart card request power model*. Each smart card request provokes a specific smart card power consumption. The magnetic field is adapted to optimize the power consumption for the currently processed request. This approach can be implemented in software.

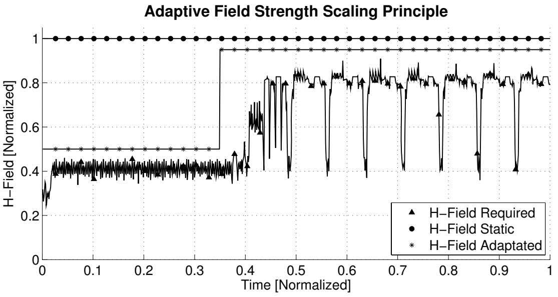


Fig. 2. Principle of the Adaptive Field Strength Scaling methodology. The magnetic field that is generated by the reader is adapted to the instantaneous power consumption of the smart card. During the smart card's high power consumption periods, the magnetic field strength is increased, otherwise it is decreased. Thus, electrical power can be saved compared to traditional static magnetic field strength approaches.

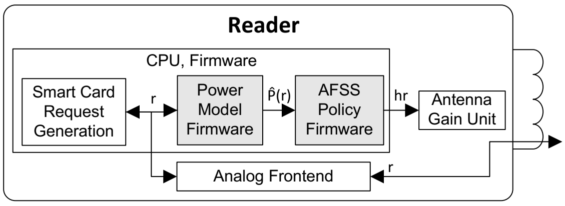


Fig. 3. Principle of the reader AFSS request-based approach. A smart card request r is generated and passed to the power model firmware. A power value $\widehat{P}(r)$ is estimated, which is needed by the smart card to process the request r properly. Based on this information, the AFSS policy firmware signals the antenna gain unit by means of a message hr to adapt the magnetic field strength.

- The smart card evaluates its *instantaneous power consumption* and supply voltage level. The reader is notified to modify the magnetic field strength. The reader / smart card system's power consumption is optimized very precisely. This approach requires hardware modifications at reader and smart card side.

In the following paragraph both approaches will be described.

A. Request-Based AFSS

Many types of contactless NFC applications (e.g., payment, e-passport) provoke a distinct smart card power consumption profile. This knowledge is exploited by a *request-based smart card power model*. Each request that is sent from the reader to the smart card has a specific smart card power consumption value assigned, e.g., authentication requests that use cryptographic calculations provoke a higher smart card power consumption than reading out an identification number. These power values are obtained from a smart card power model characterization process. During this process, the requests are issued on the target smart card and power consumption measurements are performed. Most applications (ticketing, payment, etc.) always use the same type of smart card, which reduces the effort needed for the characterization process. Here we present two implementations of the request-based AFSS technique, whether the power model is implemented in the reader or in the smart card. All AFSS implementations can be done within software, no costly hardware modifications are needed at all.

1) Reader: In this approach, the reader firmware implements the *request-based smart card power model*. Thus, the reader knows which kind of request r changes the smart card's power profile significantly. Fig. 3 depicts the reader's AFSS architecture. The reader's application generates a smart card request r. This request r is forwarded to the power model firmware. The *request-based smart card power model* provides an estimated smart card power consumption $\widehat{P}(r)$ that is provoked by the specific request r, according to (1). If additional information regarding the smart card's internal system states $\mathbf{x}$ (e.g., usage of a cryptographic core) or the reader / smart card system's coupling factor k are given (physical characteristics, distance, etc.), the resulting power requirement $\widehat{P}(r)$ can be calculated more precisely.

$$\widehat{P}(r) = f(r, \mathbf{x}, k) \tag{1}$$

The AFSS policy firmware then decides if the magnetic field strength needs to be adapted and forwards a corresponding magnet field adaptation request hr to the antenna gain unit:

- The magnetic field strength is decreased if a smart card request r is sent to the smart card that provokes a low smart card power consumption, e.g., basic calculations.
- The magnetic field strength is increased if a smart card request r is sent to the smart card that provokes a high smart card power consumption, e.g., cryptography operations.

2) Smart Card: In this approach, the *request-based smart card power model* is implemented by the smart card, instead of the reader. Fig. 4 illustrates the presented approach. The reader's application generates a smart card request r. This request is transmitted to the smart card by means of magnetic field modulation. The smart card's application forwards the request to the power model firmware. Then the smart card's power requirement $\widehat{P}(r)$ for processing this specific request r is estimated according to (2). Additional crucial information can be available to the smart card, e.g., internal system states $\mathbf{x}$ (e.g., usage of a cryptographic core), supply voltage $v(t)$, the Zener diode's state (conducting, blocking), or more detailed smart card request power states. Thus, the required electrical

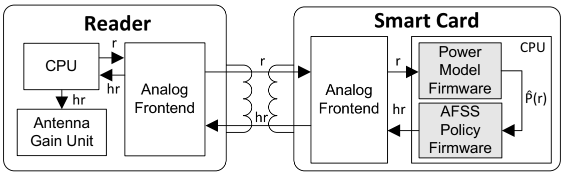


Fig. 4. Principle of the smart card AFSS request-based approach. A smart card request r is generated by the reader and is transmitted to the smart card. The smart card forwards r to the power model firmware and estimates the needed power $\widehat{P}(r)$ to execute the request properly. Then the AFSS policy firmware checks if a magnetic field strength adaptation is needed and sends a message hr to the reader. The reader evaluates this message hr and modifies the magnetic field strength accordingly.

power $\widehat{P}(r)$ can be estimated precisely. This smart card-based approach enables finer magnetic field strength adaptations than the reader-based approach.

$$\widehat{P}(r) = f(r, \mathbf{x}, k, v(t), ZenerDiodeState) \tag{2}$$

The power consumption estimate $\widehat{P}(r)$ is then forwarded to the AFSS policy firmware, which decides whether the magnetic field strength suffices, needs to be increased to meet the new power requirement or decreased to save electrical energy. If a magnetic field adaptation is required, then a corresponding magnetic field adaptation message hr is transmitted to the reader. The reader receives this message hr and adapts the magnetic field strength with the help of the antenna gain unit. The advantage of this smart card-based approach is that the reader does not need to know the physical characteristics of the smart card it is communicating with. As a drawback, transmitting magnetic field adaptation messages to the reader slows down the reaction time and decreases the system's maximum data transmission rate.

B. Instantaneous Power Consumption-Based AFSS

This AFSS approach enables precise magnetic field adaptations. Magnetic field adaptation decisions can be performed without any smart card power models, knowledge about coupling factors, etc. Both smart card and reader are enhanced with hardware AFSS units. This hardware-based approach ensures a speed up for the AFSS technique. No slow software interactions are needed at all. The smart card's AFSS unit monitors crucial internal stability parameters, e.g., the electronics' supply voltage $v(t)$. If a modification of the magnetic field strength is needed, then a dedicated high priority magnetic field adaptation messages hr is sent from the smart card to the reader. The reader's AFSS unit monitors the incoming data stream. If a magnetic field adaptation message is recognized, then the antenna gain unit is immediately signaled to change the field strength accordingly. In the following paragraphs the hardware enhancements of smart card and reader are described.

1) Reader: The architecture of the proposed AFSS enhanced reader is depicted in Fig. 5. The received data stream r, hr from the smart card is forwarded through the analog frontend, which is responsible for demodulation purposes, to the AFSS unit. The AFSS unit monitors the data stream and is triggered by specific, high priority magnetic field adaptation messages hr. If a magnetic field adaptation message hr is detected, then the reader's output gain is modified with the help of the antenna gain unit. The antenna gain modification is performed by selecting the dedicated resistor in the antenna output circuit. The whole procedure of adapting the magnetic field strength is accomplished without the need of any slow software interactions. Thus, a minimum delay is achieved, which makes the AFSS approach feasible.

2) Smart Card: Fig. 6 illustrates the equivalent circuit of the proposed AFSS enhanced smart card. The smart card's analog frontend is responsible to rectify the electrical current that is induced by the magnetic field. Correspondingly, a supply voltage $v_i(t)$ is provided to the smart card. Capacitor C buffers the provided electrical charges. The Zener diode prevents electric surges, which may disrupt the smart card's electronics, by bleeding off any excessive electrical charges. The voltage level of $v(t)$, which supplies the rest of the chip, is crucial for a proper smart card functionality:

- If $v(t)$ drops below the threshold V_{Low}, then the smart card's operational stability is lost. The smart card's electronics is reset by a reset circuit. Safety precautions (e.g., deactivating the smart card's clock) should be performed to prevent hazardous drops below V_{Low}.
- If $v(t)$ reaches the threshold V_Z, then the Zener diode acts as a perfect wire and bleeds off any excessive electrical charges.

The AFSS unit's purpose is to monitor the voltage $v(t)$ and to control it within the range of $V_{Low} < v(t) < V_Z$ by means of the AFSS methodology. By controlling $v(t)$ within the upper V_Z and lower V_{Low} boundaries, less electrical power is wasted and the smart card's operational stability is preserved at the same time. Fig. 7 depicts the basic architecture of the AFSS unit, which implements three main functionalities:

- The Zener diode is monitored to derive the charge level of the capacitor C. Two states can be evaluated: The voltage across the capacitor C equals V_Z (the Zener diode conducts) or the voltage level is below V_Z (the Zener diode blocks).
- Two voltage comparators check the voltage $v(t)$ against reference voltage levels V_{REF1} and V_{REF2}. The more voltage comparators are implemented, the finer the $v(t)$ analysis and magnetic field adaptations are.

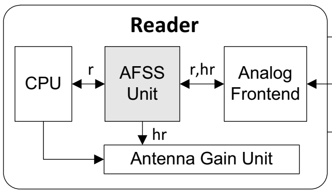


Fig. 5. Architecture of the AFSS unit enhanced reader. The received data r , hr from the smart card is monitored within the AFSS unit. If a field adaptation message hr is detected, then the AFSS unit signals the antenna gain unit to modify the magnetic field strength accordingly. No slow software interactions are needed.

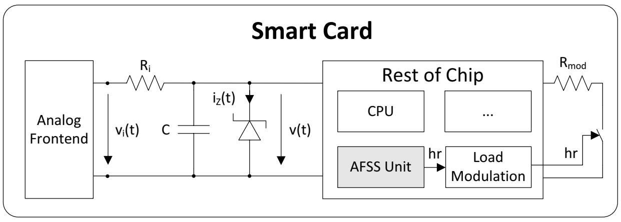


Fig. 6. Equivalent circuit of the AFSS enhanced smart card. The AFSS unit monitors the smart card's stability parameters and uses the load modulation unit to transmit high priority magnetic field change messages hr to the reader.

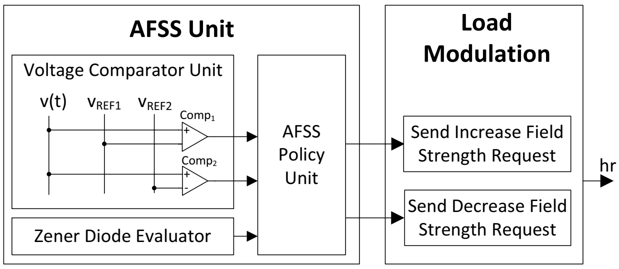


Fig. 7. The results of the voltage comparator and the Zener diode evaluator units are forwarded to the AFSS policy unit. Based on the provided information, the AFSS policy unit signals the load modulation unit if a magnetic field increase or decrease message should be sent.

- An AFSS policy unit implements the logic when magnetic field adaptations should be requested. Magnetic field adaptation decisions are based upon the policy presented in Fig. 8. If $v(t)$ drops below a threshold V_{REF1}, then the magnetic field should be increased. Otherwise, if the Zener diode conducts or $v(t)$ is above V_{REF2}, then the magnetic field should be reduced to save electrical power.

The AFSS unit is directly connected to the smart card's load modulation unit, which is responsible for any data transfers from the smart card to the reader. Thus, any slow software interactions are avoided. The load modulation unit handles incoming magnetic field adaptation notifications with highest priority. Therefore, magnetic field adaptation messages are sent to the reader with a minimum delay.

IV. Hardware Emulation Platform

All experiments are performed with the help of a hardware emulation platform, which is similar to an approach described in [17]. The hardware emulation platform's architecture is depicted in Fig. 9. It supports cycle accurate power and supply voltage analyses in real time. Smart card, power estimation and supply voltage estimation units are synthesized into an FPGA. The value of supply voltage $v_i(t)$, which is embossed by the magnetic field, as well as the smart card requests r are provided to the smart card. During the processing of the requests r, the smart card's internal system states $\mathbf{x}$ change. The power estimation unit monitors these states and estimates the dissipated power according to (3). Each smart card system state x_i is a corresponding power dissipation value c_i assigned. Vectors $\mathbf{x}$ and $\mathbf{c^T}$ are then formed. The linear combination of $\mathbf{x}$ and $\mathbf{c^T}$ plus c_0, which defines the leakage power dissipation, results in the total power estimate $\widehat{P}(\mathbf{x})$. A time dependency is finally introduced by $\widehat{P}(\mathbf{x}(t))$, because system states may change at any clock cycle. A power characterization process is needed to determine the parameters c_0, $\mathbf{c^T}$ and $\mathbf{x}$. The difference between estimated and real power consumption is defined by ϵ, according to (4). The average estimation error is as high as 8.4%.

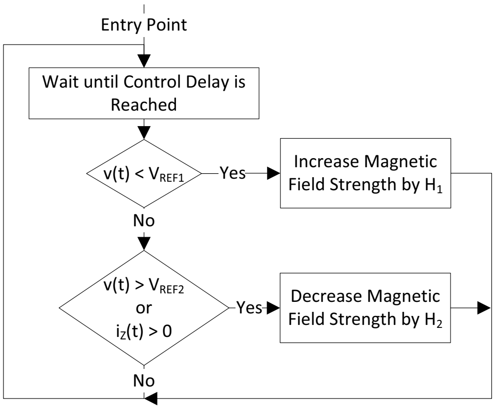

Entry Point
Wait until Control Delay is Reached
v(t) < V_{REF1}
Yes
Increase Magnetic Field Strength by H_1
No
v(t) > V_{REF2} or $i_Z(t)$ > 0
Yes
Decrease Magnetic Field Strength by H_2
No

Fig. 8. AFSS policy: If $v(t)$ drops below a threshold V_{REF1}, then the magnetic field should be increased. Otherwise, if the Zener diode conducts or $v(t)$ is above V_{REF2}, then the magnetic field should be reduced to save electrical power.

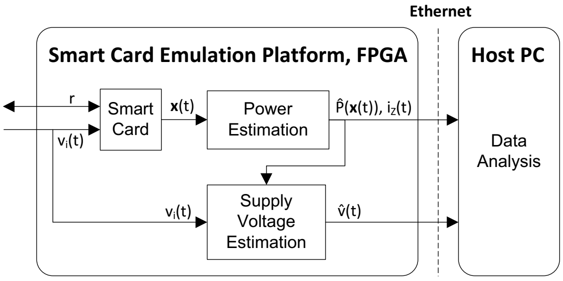


Fig. 9. Hardware emulation platform that is used to evaluate the novel AFSS approaches. The estimates of power and supply voltage estimation units are sent over Ethernet to a host PC for further data analysis tasks. Average estimation errors of 8.4% and 2% are caused respectively.

$$\widehat{P}(\mathbf{x}) = \widehat{P}_{stat} + \widehat{P}_{dyn} = c_0 + \sum_{i=1}^{n} c_i \cdot x_i = c_0 + \mathbf{c^T} \cdot \mathbf{x} \quad (3)$$

$$P(\mathbf{x}) = \widehat{P}(\mathbf{x}) + \epsilon \quad (4)$$

The power estimates $\widehat{P}(\mathbf{x}(t))$ are then forwarded to the supply voltage estimation unit. This unit implements an electrical charge-based model of the smart card's power supply network, similar to [10] and [18]. The smart card's supply voltage is estimated according to (5). The average estimation error is given by ϵ, which is as high as 2%.

$$\widehat{v}(t) = v(t) + \epsilon = \frac{Q_C(t)}{C} + \epsilon \quad (5)$$

All relevant data is then sent over Ethernet to the host PC for further analysis tasks.

V. Experimental Results

This chapter presents the results of magnetic field strength experiments. All experiments execute the same benchmark, which is divided into two subsequent parts. During the first part, the reader requests the smart card to perform some security relevant and high power consuming SHA calculations. After these calculations are finished, the second part starts. The reader requests the smart card to allocate a string array

TABLE I
DESCRIPTION OF THE USED FIGURE PARAMETERS

Parameter	Description
$\widehat{P}(t)$	The estimated power consumption of the smart card's electronics.
$v_i(t)$	Supply voltage, which is generated by the magnetic field and rectified by the smart card's analog fronted.
$\widehat{v}(t)$	Estimated supply voltage, which is applied to the smart card's electronics.
V_T	Supply voltage threshold (1 V). To guarantee a proper working smart card, $v(t)$ should not be below this threshold longer than a specific amount of time t_{Low}.
V_Z	Zener diode's threshold voltage (2.5 V).
$\widehat{P_Z}(t)$	Estimated power dissipation of the Zener diode. The higher this value, the higher the power wastage of the smart card / reader system.

and to perform Quicksort on it. Both benchmark parts, SHA and Quicksort, are taken from the MiBench benchmarking suite [19] for reproducibility purposes. Table I elucidates the variable names used in this chapter's figures.

The mathematical background of the presented results is defined as follows: The reader transfers electrical power to the smart card according to (6). The amount of transferred power $P_{SmartCard}(t)$, which is usable by the smart card, depends on the coupling factor k. According to (7) and (8), $P_{SmartCard}$ can be split up into the electrical power $P_Z(t)$, which is wasted by the Zener diode, and $P(t)$, which is dissipated by the rest of the smart card.

$$P_{Reader}(t) = P_{SmartCard}(t) \cdot k \tag{6}$$

$$P_{Reader}(t) \sim P_Z(t) + P(t) \tag{7}$$

$$P_{Reader}(t) \sim i_Z(t) \cdot V_Z + P(t) \tag{8}$$

A. Maximum Field Strength

Fig. 10 depicts the smart card's behavior of current reader / smart card system approaches. The reader emits a magnetic field at the highest possible magnetic field strength. As a consequence, the magnetic field embosses a high rectified supply voltage level $v_i(t)$ of 4 V. In this benchmark, the electronics' supply voltage $\widehat{v}(t)$ never drops below the crucial threshold V_T. This method guarantees the smart card a high amount of operational stability. However, a high amount of electrical power is needed to upkeep the magnetic field, which limits the run-time of mobile battery-operated reader devices. During the smart card's low power consuming periods, $\widehat{v}(t)$ reaches the Zener diodes threshold V_Z. Therefore, the Zener diode conducts and bleeds off the excessive electrical current $i_Z(t)$ to prevent electric surges. Electrical power is wasted.

B. Insufficient Field Strength

Fig. 11 illustrates the smart card's behavior if a magnetic field of insufficient strength is generated by the reader. The magnetic field provokes a supply voltage $v_i(t)$ of only 2.5 V. As a consequence, the smart card electronics' supply voltage $\widehat{v}(t)$ drops continuously below the threshold V_T of 1 V during the execution of the SHA benchmark. The smart card's operational stability is compromised. Voltage drop countermeasures, e.g., deactivating the smart card CPU's clock, have to be conducted to improve the smart card's stability during these magnetic field and supply voltage starvation periods. Because of the magnetic field starvation, $\widehat{v}(t)$ never reaches the Zener diode's voltage threshold V_Z of 2.5 V. Therefore, the diode's electrical current $i_Z(t)$ stays zero and no electrical power $\widehat{P_Z}(t)$ is wasted.

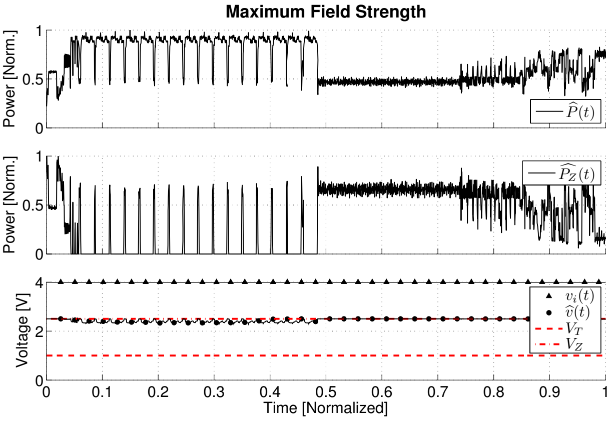


Fig. 10. This figure illustrates the smart card behavior of current RFID and NFC application approaches. A maximum magnetic field is generated to guarantee a high smart card operational stability. No hazardous $\widehat{v}(t)$ voltage drops below V_T are recognizable during this benchmark. $\widehat{P_Z}(t)$ represents the amount of electrical power that is wasted by the Zener diode.

C. Request-Based AFSS, Reader

Fig. 12 depicts the smart card's behavior if a reader implemented *request-based AFSS* technique is applied. The power model enables the reader to estimate the amount of electrical

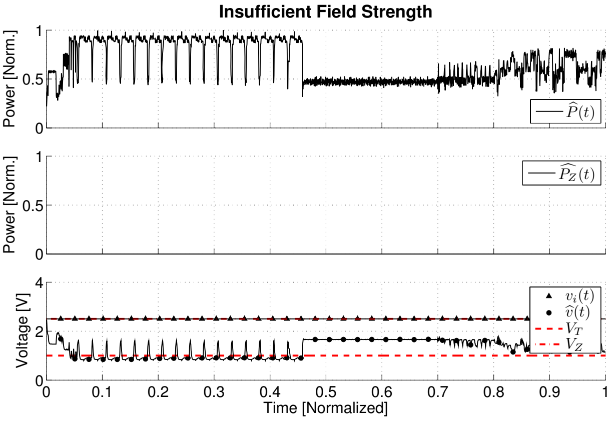


Fig. 11. This figure depicts the smart card behavior during a period of low magnetic field supply. The supply voltage $v_i(t)$ that is embossed by the magnetic field is only as high as 2.5 V. $\widehat{v}(t)$ drops hazardously below the threshold V_T and provokes smart card instabilities. Due to supply starvation, $\widehat{P_Z}(t)$ stays zero. Thus, no electrical power is wasted.

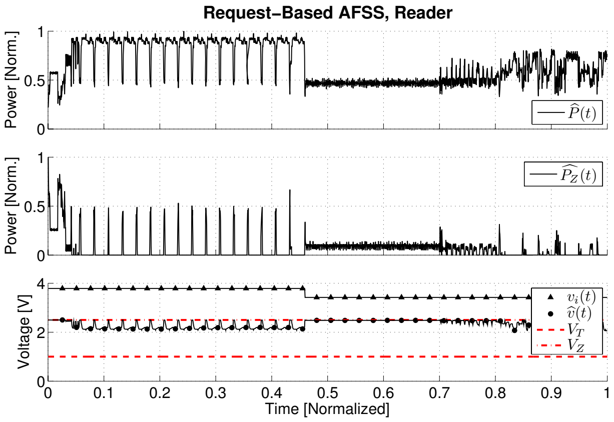


Fig. 12. This figure depicts the smart card behavior while using the reader implemented *request-based AFSS* technique. The reader increases the magnetic field during the processing of the SHA smart card request. Voltage $v_i(t)$ changes correspondingly. No $\widehat{v}(t)$ drops below the crucial threshold V_Z are detectable. During the low power consuming period, the magnetic field is reduced. The Zener diode's power dissipation $\widehat{P}_Z(t)$ is minimized. Thus, the reader / smart card system wastes only little electrical power.

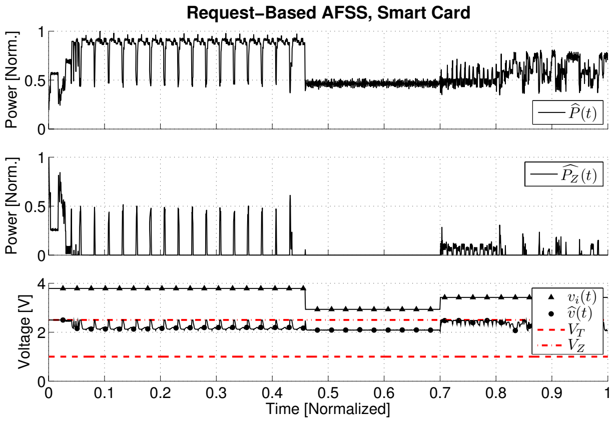


Fig. 13. This figure shows the smart card behavior while using the smart card implemented *request-based AFSS* technique. The reader is requested to increase the magnetic field during the processing of the SHA benchmark. Voltage $v_i(t)$ changes correspondingly. No $\widehat{v}(t)$ drops below the crucial threshold V_T are detectable. During the low power consuming period, the magnetic field is reduced. The Zener diode's power dissipation $\widehat{P}_Z(t)$ is minimized. Thus, the reader / smart card system wastes only little electrical power.

power needed by the smart card to execute the specific smart card request r properly. During the high power consuming SHA benchmark, the reader increases the magnetic field strength. As a result, $v_i(t)$ equals 3.9 V. During the Quicksort benchmark, the magnetic field is reduced. Less electrical power $\widehat{P}_Z(t)$ is wasted than during the maximum field strength approach. Furthermore, the crucial supply voltage $\widehat{v}(t)$ does not drop below the hazardous threshold V_T. The smart card's stability is preserved.

D. Request-Based AFSS, Smart Card

Fig. 13 depicts the smart card's behavior if a smart card implemented *request-based AFSS* technique is applied. Finer magnetic field adaptations can be performed because of a more detailed smart card power model, e.g., the coupling factor k, which may change at any time, can be estimated more precisely. During the high power consuming SHA benchmark, the reader is requested to increase the magnetic field strength. As a result, $v_i(t)$ equals 3.9 V. During the low power consuming string allocation period, the magnetic field strength is reduced and $v_i(t)$ decreases to 3 V. Afterwards, the magnetic field strength is increased again to execute the Quicksort benchmark properly. Only little electrical power is wasted by the reader / smart card system, $\widehat{P}_Z(t)$ is minimized. Furthermore, the crucial supply voltage $\widehat{v}(t)$ does not drop below the hazardous threshold V_T. The smart card's stability is preserved.

E. Instantaneous Power Consumption-Based AFSS

Here we highlight the test results of an *AFSS instantaneous power consumption* improved reader / smart card system. The tested AFSS implementation supports three different magnetic field strengths as well as magnetic field change rates of up to 10 kHz. Given a recent NFC reader / smart card system with a data rate of 848 kBit / s, the magnetic field change requests of 8-Bit length would lower the systems' data rate in worst case by 9.5%. Fig. 14 illustrates the smart card's behavior during the benchmark. The smart card's AFSS policy unit constantly monitors the smart card's supply voltage $\widehat{v}(t)$. If a magnetic field adaptation is requested, then a corresponding $v_i(t)$ change is detectable. Supply voltage $\widehat{v}(t)$ stays above the hazardous threshold V_T, thus the smart card's stability is preserved. Furthermore, the Zener diode's power dissipation $\widehat{P}_Z(t)$ stays zero.

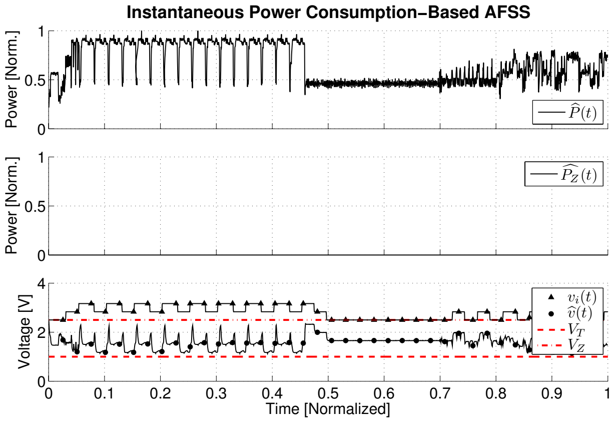


Fig. 14. Smart card behavior of the *Instantaneous Power Consumption-Based AFSS* implementation. The smart card constantly evaluates crucial parameters like $\widehat{v}(t)$, $i_Z(t)$, etc. and requests magnetic field adaptations if necessary. $\widehat{P}_Z$ is minimized while preserving the smart card's operational stability at the same time.

TABLE II
READER / SMART CARD ENERGY SAVED COMPARISON

Magnetic Field Approach	Energy Saved [%]
Maximum Field Strength	0.0
Request-Based AFSS, Reader	22.0
Request-Based AFSS, Smart Card	25.0
Instant. Power Consumption-Based AFSS	41.9

TABLE III
BENCHMARKS FOR INSTANTANEOUS POWER CONSUMPTION-BASED AFSS COMPARED TO MAXIMUM FIELD STRENGTH

Benchmark	Energy Saved [%]
AES	35.3
BasicMath	51.7
FFT	54.0
Stringsearch	46.7

F. Comparison of Energy Usage

Table II illustrates the amount of electrical energy saved by the reader / smart system while performing the presented benchmark and using the AFSS technique. The results are compared to the commonly used approach to supplying a maximum possible magnetic field strength. Table III presents further energy saving comparisons of the instantaneous power consumption-based AFSS technique during the execution of various benchmarks. Up to 54 % of the electrical energy can be saved compared to a maximum field strength approach.

VI. CONCLUSION

The number of mobile battery-operated NFC readers is increasing drastically, because of the propagation of NFC enhanced smart phones. Most of the NFC-based applications use a maximum magnetic field strength. The higher the magnetic field strength, the higher the smart card's operational stability, the higher the reader's power consumption. However, a maximum magnetic field strength is not always required and it wastes the reader's electrical power. As a consequence, the run time of mobile battery-operated readers is reduced unnecessarily.

This paper presents an adaptive field strength scaling (AFSS) methodology. The magnetic field strength is adapted to the smart card's instantaneous power consumption requirements to save electrical power. During the smart card's low power consuming periods, the magnetic field is reduced. Otherwise, during the smart card's high power consuming periods, the magnetic field is increased. We present two different AFSS strategies. The *request-based* AFSS is a coarse grained solution, which is implementable in software. It can be integrated either in the reader or the smart card. *Instantaneous Power Consumption-Based AFSS* represents the second proposed AFSS strategy. Hardware modifications are performed on reader and on smart card for a fast and fine grained AFSS implementation.

A reader / smart card hardware emulation environment is used to implement and prove the proper functionality of the AFSS methodology. Reproducible benchmarks are executed for testing purposes. The results show, that using the AFSS technique reduces the reader / smart system's energy consumption by up to 54% and preserves the smart card's operational stability simultaneously.

ACKNOWLEDGMENTS

We would like to thank our industrial partners Infineon Technologies Austria AG as well as Enso Detego GmbH for their support.

REFERENCES

[1] R. Joseph and M. Martonosi, "Run-Time Power Estimation in High Performance Microprocessors," in *International Symposium on Low Power Electronics and Design*, 2001.

[2] J. Coburn, S. Ravi, and A. Raghunathan, "Power Emulation: A New Paradigm for Power Estimation," in *Design Automation Conference*, 2005.

[3] L. Hua, W. Hong-jun, S. Zhen, L. Qing-hua, and X. Wei, "Low-power UHF Handheld RFID Reader Design and Optimization," in *World Congress on Intelligent Control and Automation*, 2010.

[4] G. Shu-qin, W. Jin-hui, Z. Lei, H. Li-gang, and W. Wu-chen, "A Low-power Active RFID Portable Reader System," in *Annual IEEE Systems Conference*, 2008.

[5] T. Lohmann, M. Schneider, C. Ruland, H. li gang, and W. Wu-chen, "Analysis of Power Constraints for Cryptographic Algorithms in Mid-Cost RFID Tags," in *Lecture Notes in Computer Science*, vol. 3928, 2006.

[6] R. Tessier, D. Jasinski, A. Maheshwari, A. Natarajan, W. Xu, and W. Burleson, "An Energy-Aware Active Smart Card," in *IEEE Transactions on Very Large Scale Integration Systems*, vol. 13, 2005.

[7] T. Li, S. Wu, S. Chen, and M. Yang, "Energy Efficient Algorithms for the RFID Estimation Problem," in *INFOCOM*, 2010.

[8] X. Xu, L. Gu, J. Wang, and G. Xing, "Negotiate Power and Performance in the Reality of RFID Systems," in *IEEE International Conference on Pervasive Computing and Communications*, 2010.

[9] E. Grochowski, D. Ayers, and V. Tiwari, "Microarchitectural simulation and control of di/dt-induced power supply voltage variation," in *Symposium on High Performance Computer Architecture*, 2002.

[10] M. Wendt, C. Grumer, C. Steger, and R. Weiss, "System Level Power Profile Analysis and Optimization for Smart Cards and Mobile Devices," in *ACM Symposium on Applied Computing*, 2008.

[11] M. Badaroglu, K. Tiri, S. Donnay, P. Wambacq, I. Verbauwhede, G. Gielen, and H. De Man, "Clock Tree Optimization in Synchronous CMOS Digital Circuits for Substrate Noise Reduction Using Folding of Supply Current Transients," in *Design Automation Conference*, 2002.

[12] H. Su, S. Sapatnekar, and S. Nassif, "An algorithm for optimal decoupling capacitor sizing and placement for standard cell layouts," in *International Symposium on Physical Design*, April 2002.

[13] E. Alon, V. Stojanovic, and M. Horowitz, "Circuits and Techniques for High-Resolution Measurement of On-Chip Power Supply Noise," in *IEEE Journal of Solid-State Circuits*, vol. 40, 2005.

[14] T. Nakura, M. Ikeda, and K. Asada, "Preliminary Experiments for Power Supply Noise Reduction using Stubs," in *Asia-Pacific Conference on Advanced System Integrated Circuits*, 2004.

[15] V. Reddi, M. Gupta, G. Holloway, G. Wei, M. Smith, and D. Brooks, "Voltage Emergency Prediction Using Signatures to Reduce Operating Margins," in *IEEE International Symposium on High Performance Computer Architecture*, 2009.

[16] M. Holtz, S. Narasimhan, and S. Bhunia, "On-Die CMOS Voltage Droop Detection and Dynamic Compensation," in *ACM Great Lakes Symposium on VLSI*, 2008.

[17] A. Genser, C. Bachmann, J. Haid, C. Steger, and R. Weiss, "Supply Voltage Emulation Platform for DVFS Voltage Drop Compensation Explorations," in *IEEE International Symposium on Performance Analysis of Systems and Software*, 2011.

[18] K. Finkenzeller, *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification*, 2nd ed. John Wiley & Sons, 2003.

[19] M. R. Guthaus, J. S. Ringenberg, D. Ernst, T. M. Austin, T. Mudge, and R. B. Brown, "MiBench: A free, commercially representative embedded benchmark suite," in *IEEE International Workshop on Workload Characterization*, 2001.

Hardware/Software Co-Design of Elliptic-Curve Cryptography for Resource-Constrained Applications

Andrea Höller, Norbert Druml,
Christian Kreiner and Christian Steger
Institute of Technical Informatics
Graz University of Technology, Austria
{andrea.hoeller, norbert.druml,
christian.kreiner, steger}@tugraz.at

Tomaz Felicijan
Infineon Technologies Austria
Design Center Graz, Austria
tomaz.felicijan@infineon.com

ABSTRACT

ECC is an asymmetric encryption providing a comparably high cryptographic strength in relation to the key sizes employed. This makes ECC attractive for resource-constrained systems. While pure hardware solutions usually offer a good performance and a low power consumption, they are inflexible and typically lead to a high area.

Here, we show a flexible design approach using a 163-bit GF(2m) elliptic curve and an 8-bit processor. We propose improvements to state-of-the-art software algorithms and present innovative hardware/software codesign variants. The proposed implementation offers highly competitive performance in terms of performance and area.

Keywords

Elliptic Curve Cryptography, RFID, Hardware/Software Co-Design, Embedded Systems

1. INTRODUCTION

Radio Frequency Identification (RFID) is a popular technology when it comes to automatically identify people and goods wirelessly. In contrast to simple ID transmission applications, security relevant applications require cryptographic-based authentication. Public-key cryptography provides a simpler key management than symmetric cryptography, since no secret key is required on the readers side [20]. Thus, public-key cryptography is more reasonable in open-loop applications. Compared to conventional public-key algorithms like RSA, ECC can achieve the same level of security with shorter key sizes. However, since the resources of an RFID tag are extremely limited, the implementation of ECC on such tags is a challenging task.

To achieve a reasonable computation time, previous implementations of ECC on RFID mainly base on pure hardware solutions. However, development teams need flexible systems to react quickly on changing demands of the market. Flexibility can be achieved by using a lightweight microprocessor.

We present several options of partitioning hardware and software to offer a good runtime performance. The main contributions of this paper are:

- It proposes an algorithm for binary field multiplication in software that achieves a good performance with low storage requirements.
- It introduces a novel method of hardware/software codesign of ECC by presenting a small hardware extension that significantly speeds up the software implementation.
- It offers approaches for further hardware extensions like instruction set extensions and a coprocessor for binary multiplication.

2. THE RFID-TAG ARCHITECTURE

The target application of the presented ECC architectures are RFID tags which can range from a low-capability device (e.g. for pet identification) to a powerful contactless smartcard (e.g. for biometric passports). The modules of a typical tag IC are an analog front end, a digital control unit and a Non-Volatile Memory (typically realized as EEPROM). The area of RFID tag ICs range between 0.25 and 10 mm^2 [12].

2.1 The Microprocessor

To realize the control unit an 8-bit proprietary processor offering a reduced instruction set for RFID is used. Compared to hardwired state machines, the programmable framework supports a more efficient development of RFID products. Since the processor is very small (~2.5 kGE) and energy-efficient (average power consumption between 11.6μW/MHz and 26μW/MHz), the processor is ideally suitable for resource-constrained applications.

The processor is based on the Harvard architecture with separate pathways for instructions and data and can be classified as a load-and-store architecture. The processor features 16 general purpose registers (GPRs) and 30 instructions. All basic instructions of a microprocessor like binary operations, addition, subroutine functions, and branch-conditions are supported. Although there is a shift-left instruction, there is no shift-right functionality. Furthermore, the processor does not feature a multiplication operation. All instructions, can be executed within one clock cycle, except memory accesses to ROM, which require two cycles.

Primarily, the processor was designed for RFID communication protocols according to ISO/IEC 15603 or ISO/IEC 14443. However, it can also be used for more advanced calculations as shown in this paper.

3. ECC DESIGN DECISIONS

Designing an ECC-based system involves decisions on the following hierarchical levels: Security protocol, elliptic curve arithmetic and field arithmetic including field operations. Our design decisions on each of these levels are outlined in the next two sections. Since the field operation multiplication accounts for the majority of runtime, the remainder of this paper focuses on proposals for effective multiplication implementation methods.

3.1 Security Protocol and Elliptic Curve Arithmetic

Our implementation establishes an one-way authentication of RFID tags and is based on the work of Bock et al. [5]. A challenge-response protocol requiring one point multiplication on the tag realizes the authentication. A Montgomery multiplication operating on projective coordinates including several protections against side channel attacks establishes the point multiplication as presented in [5].

3.2 Field Arithmetic

Standards define elliptic curves over prime fields *GF(p)* or binary fields *GF*(2^m) [6]. The hardware support of processors offering a multiplier, favours the usage of prime fields [10, 22, 6]. However, it has been demonstrated that software-based ECC can achieve better performance using binary fields [19]. Since our processor does not feature a hardware multiplier and the usage of binary fields eases further hardware accelerations [6], we use binary fields *GF*(2^m) in polynomial base representation.

The parameter size m is 163, thus one element is stored in 21 words. Throughout this document $A[i]$ refers to the i^{th} word of an array representing the binary vector representation of an polynomial $a(z)$. Whereby $A[0]$ stores the lower and $A[20]$ stores the higher coefficients.

Note, the protocol and point multiplication do not require an inversion operation. Thus, to compute the Montgomery multiplication the following field operations are required: addition, reduction, squaring and multiplication.

3.2.1 Addition

This operation only requires a word-wise XOR (binary addition) of both addends.

3.2.2 Reduction

Modulo reduction $c(z)=c_d(z) \bmod f(z)$ reduces the output of a field multiplication $c_d(z)$ with a field size of $(2m-1)$ to a size of m using a irreducible polynomial $f(z)=z^m+r(z)$. Basically, the reduction algorithm goes through all coefficients c_j of $c_d(z)$ that have to be reduced and adds $z^j r(z)$ to $c_d(z)$, if the coefficient is one. The elliptic curve parameters we use define an irreducible polynomial where two 8-bit words are needed to store $r(z)$.

For acceleration, we use two lookup tables (LUTs) to store precalculated additions of shifted $r(z)$. They require 288 bytes in total. Since shifts $z^j r(z)$, where $j \geq 8$, can be achieved with array indexing, the reduction can be calculated without shifts during runtime.

3.2.3 Squaring

Squaring can be achieved by inserting zeros between two consecutive bits, as described in [6]. To square the element A, every nibble of the lower words ($A[0]$ to $A[10]$) is expanded to a 21-word element with a 16-byte LUT.

The expansion of the remaining words of A would result in words, which have to be reduced afterwards. However, we take into advantage that when squaring an element, every second bit is zero and implemented an interleaved reduction similar to the standard reduction. We use two 32-byte LUTs to reduce the number of shifts and additions during runtime.

3.2.4 Multiplication

The runtime of the binary field multiplication represents the main factor for the overall performance. Thus, below we will describe novel methods to accelerate the binary field multiplication.

```
Input: $a(z)$ and $b(z)$ of degree at most $m-1$
Output: $c(z) = a(z) \cdot b(z)$ of degree at most $2m-2$
Compute all $B_u = u(z) \cdot b(z)$ where $deg\{u(z)\} < w$
for $k \leftarrow (8/w)$ downto 0 do
    for $j \leftarrow 0$ to 20 do
        $u = (u_{w-1}, ..., u_1, u_0)$, where $u_i$ is bit $(wk+i)$ of $A[j]$
        for $i \leftarrow 0$ to 20  $C[i+j] \leftarrow C[i+j] \oplus B_u[i]$
    end for
    if $(k \neq 0)$ $C \leftarrow C \cdot z^w$
end for
```

Figure 1: Left-to-right binary field multiplication. Adapted from [6].

3.3 Enhanced Binary Field Multiplication Algorithm

A well-known approach for the binary field multiplication is the *left-to-right (l-t-r) comb* method as shown in Fig. 1. The algorithm calculates $C = A \cdot B$ by processing w bits of every word of A at a time and requires precalculation of multiples of B. The choice of w comes with a trade-off between memory requirements and performance. In general, the number of precalculated elements equals $2^w - 1$. For example, if *w=2* the products $B_1 = B$, $B_2 = 2_d \cdot B$, $B_3 = 3_d \cdot B$ are precalcuated and stored. Note that $B_0 = 0 \cdot B$ does not need to be stored, since it is always zero.

To accelerate the calculation, the window size could be increased to *w=4*. However, this would require the storage of 15 elements requiring 315 byte RAM, which is often not suitable for a resource-constrained device like an RFID tag. To achieve a good performance with low storage requirement, we propose a novel enhancement of the *l-t-r comb* method. The idea is to perform fewer precalculations and calculate more during runtime by ignoring the last term of $u(z)$ in the precalculation phase. Only these $B_u = u'(z) \cdot b(z)$, satisfying $deg\{u(z)\} < w$ and $u'(z) = \{u_{w-1}z^{w-1} + ... + u_2z^2 + u_1z\}$ are determined and stored. Put simply, only these B_u, where u is even, are considered for precalculation. Additionally, $B_1 = B$ is stored. This reduces the number of stored elements to 2^{w-1}. For example, choosing a window size of *w=4*, requires only eight elements (168 bytes) to be stored in RAM.

The enhanced algorithm is shown in Fig. 2. The precalculation procedure can be designed to reduce the number of required shift operations by combining already calculated elements. If *w=4* the outer loop has to be executed two times. If the processed nibble u of A is even, it is only necessary to add the corresponding B_u to the accumulator C. If u is odd, u' is determined by setting the last bit of u to zero. Thereafter, B_u is read from RAM and additionally B_1 is added to C. In simple terms, if for example $u = 7_d$, then $B_7 = 7_d \cdot B$ is calculated as follows: $B_7 = 6_d \cdot B + B$. The term $B_6 = 6 \cdot B$ is determined by reading B_6 from RAM. Thus, only the additional addition of B_1 is calculated during runtime.

3.4 Binary Field Multiplication using Virtual Addressing

Here we explore an innovative small-footprint hardware extension approach to speed up the multiplication by reducing the number of pointer calculations and memory accesses. Typically, dedicated coprocessors or instruction set extensions accelerate ECC. We propose to use the idea of virtual addressing to design a hardware accelerator.

Many procedures needed for the calculation of ECC access memory consecutively and hence require many pointer calculations. Loop unfolding can reduce the number of pointer calculations, but involve a large increase of code size.

Virtual addressing allows to use static coded addresses (virtual addresses), without increasing the code size significantly. This can be achieved by inserting a virtual address logic be-

```
**Input**: $a(z)$ and $b(z)$ of degree at most $m-1$
**Output**: $c(z) = a(z) \cdot b(z)$ of degree at most $2m-2$
$B_1 \leftarrow B$; $B_2 \leftarrow B \cdot z; B_4 \leftarrow B_2 \cdot z; B_8 \leftarrow B_4 \cdot z; B_6 \leftarrow B_4 \oplus B_2;$
$B_{10} \leftarrow B_8 \oplus B_2$; $B_{12} \leftarrow B_8 \oplus B_4; B_{14} \leftarrow B_{12} \oplus B_2$
for $k \leftarrow 1$ downto $0$ do
    for $j \leftarrow 0$ to $20$ do
        if $(k = 1)$ $u = (A[j] \gg 4))$ else $u = A[j]$
        if bit 0 of $u$ is set and $u \neq 1$ then
            for $i \leftarrow 0$ to $20$ do
                $u' = u' \& 0x0E$
                $C[i+j] \leftarrow C[i+j] \oplus B'_u[i] \oplus B_1[i]$
            end for
        else if $u \neq 0$ then
            for $i \leftarrow 0$ to $20$ $C[i+j] \leftarrow C[i+j] \oplus B_u[i]$
        end if
    end for
    if$(k \neq 0)$ $C \leftarrow C \cdot z^4$
end for
```

Figure 2: *Enhanced left-to-right comb* multiplication with windowsize $w = 4$.

tween the processor and the external RAM as shown in Fig. 3. Whenever the microprocessor accesses an address in a virtual address range, the virtual address logic translates the address into a physical address. The microprocessor can influence the address mapping by setting configuration parameters. This is achieved by writing the desired value of the parameter to a predefined address. Registers within the virtual address logic store the parameters.

The basic idea of virtual addressing can be illustrated with the acceleration of a binary addition *A=A+B*. A straightforward implementation would keep the addresses of *A[0]* and *B[0]* in registers. After loading, XORing and storing the words, the address registers would be increased to process the next words. These pointer additions can be outsourced to hardware by using two 21-byte virtual elements VE_A and VE_B. Parameters called par_A and par_B could indicate to which physical addresses the virtual elements should point. For example, if par_A is one, then VE_A points to the first 21-byte of the RAM, if par_A is two, then VE_A points to the second 21-byte, and so on.

In the following, we show how virtual addressing can be used to speed up the *l-t-r comb* multiplication. We illustrate the approach by using a word size of *W=8*, a window size of *w=4* and 13 available GPRs. However, the method could also be adapted for other conditions.

3.4.1 Virtual Address Logic

The virtual addressing concept includes one 22-byte virtual element. For the address mapping five parameters are used. The determination of u and calculation of the start address of B_u (see Fig. 1) can be outsourced to the virtual addressing logic by using two parameters: *element* and *addr_mode*. The parameter *element* is set to the processed word of A and *addr_mode* defines which bits are used to determine u as shown in Equation 1. Thus, u indicates which window is currently processed.

$$u = \begin{cases} element[7:4] & \text{when } addr\_mode = 0 \\ element[3:0] & \text{when } addr\_mode = 1 \end{cases} \tag{1}$$

To achieve a shifting of B_u, the parameters *neg_offset* and *offset* are used according to Equation 2.

$$VE[i] \xrightarrow[\text{maps to}]{} B_u[i + \text{offset} - \text{neg\_offset}], i = \{0, 1, ..., 21\} \tag{2}$$

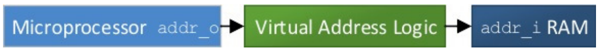


Figure 3: Principle of virtual addressing.

Furthermore, there is a parameter *shiftC* to shift the accumulator C as shown in Equation 3.

$$C[i] \xrightarrow[\text{maps to}]{} C[i + \text{shiftC}], i = \{0, 1, ..., 40\} \tag{3}$$

3.4.2 Binary Field Multiplication Algorithm

Fig. 5 shows the proposed algorithm to implement a *l-t-r comb* multiplication using the virtual addressing features. First, the required multiples of B are precalculated and stored in RAM. To keep the address logic simple, we assume that all B_u elements are stored subsequently in RAM. The virtual addressing mechanism does not influence the precalculation step.

The processing of the first window starts by setting the parameter *addr_mode* to zero. Then, the algorithm has to go through all words of A and adds the corresponding B_u to C. The determination of u depending on the currently processed word of A is outsourced to the virtual addressing logic by setting the parameter *element* to the currently processed word of A. This causes a mapping of the virtual element to the currently required B_u.

These additions represent the most expensive part of the multiplication, since the high number of required word-wise additions (see Fig. 6). Nearly all words of C, which are affected during one addition, are manipulated again by the successive addition. Using virtual addressing it is possible to perform the operations on these bytes of C, which are altered most frequently, with registers: Instead of loading values from memory and storing the altered content back to the same position, all operations which target these addresses are performed with predefined registers.

The algorithm using the virtual addressing contains two subroutines implementing successive word-wise additions with the virtual element. It is possible to jump to every single word-wise addition. For example, to process $A[0]$, all word-wise additions of the first subroutine are executed. The virtual addressing logic is configured so that $VE[0]$ points to $B_u[0]$, $VE[1]$ points to $B_u[1]$ and so on.

When processing $A[1]$, $C[0]$ is not affected (see Fig. 6). Thus the algorithm jumps into the second word-wise addition of the first subroutine. Then, 20 word-wise additions are preformed starting with the addition of $VE[1]$ to $C[1]$. Now it is required to add $B_u[0]$ to $C[1]$. Thus, the parameter *neg_offset* is set to one before calling the subroutine. This causes the virtual address logic to map $VE[1]$ to $B_u[0]$, $VE[2]$ to $B_u[1]$ and so on. The last word-wise addition is realized with the second subroutine by calling *ADD_B2_1* and setting the parameter *offset* to 9. This causes that $VE[12]$ points to *B_u[12-neg_offset+offset]=B_u[20]*. Thus, $B_u[20]$ is added to $C[21]$.

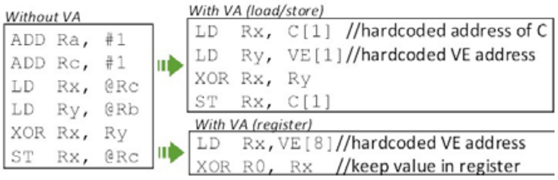
The remaining words of A are processed in a similar way. The pattern of processing the first and second half of A is very similar as shown in Fig. 6. The processing of the words *A[10]* to *A[20]* can use the same code of the implementation realizing the processing of *A[0]* to *A[9]*, when shifting the accumulator C. This is realized by setting the parameter *shiftC* before performing the remaining additions.

After processing the first window, the parameter *addr_mode* is set to one to process the second window of every word of A, and the whole procedure is repeated.

3.4.3 Advantages of Virtual Addressing

As stated above, the word-wise additions represent the most time-consuming task of the binary field multiplication, since they are executed very often. As shown in Fig. 6, 882 such word-wise additions are required (for processing both windows). A straight forward assembler implementation of a word-wise addition would require six instructions as shown in Fig. 4. Outsourcing the pointer calculations to hardware reduces the number of required instructions to four.

Additionally, the approach also reduces the number of memory accesses. By storing some intermediate results in 13



Without VA

```
ADD Ra, #1
ADD Rc, #1
LD  Rx, @Rc
LD  Ry, @Rb
XOR Rx, Ry
ST  Rx, @Rc
```

With VA (load/store)

```
LD  Rx, C[1]  //hardcoded address of C
LD  Ry, VE[1]//hardcoded VE address
XOR Rx, Ry
ST  Rx, C[1]
```

With VA (register)

```
LD  Rx,VE[8]//hardcoded VE address
XOR R0, Rx    //keep value in register
```

Figure 4: Assembler implementation of a word-wise addition with/without virtual addressing.

```
Precalcuate all $B_u$
$A_{ptr}$ ← address of $A[0]$
ADDR_MODE ← 0
call PROCESS_WINDOW
ADDR_MODE ← 1
call PROCESS_WINDOW
return

PROCESS_WINDOW:
 Reset all registers
 SHIFTC ← 0
 for $k \leftarrow 0$ to 9 do call MULT_LOOP
 Store and load registers from/to $C$                ▷ see Fig. 6
 SHIFTC ← 10
 for $k \leftarrow 0$ to 10 do call MULT_LOOP
 return

MULT_LOOP:
 ELEMENT ← value stored in $A_{ptr}$
 $A_{ptr} \leftarrow A_{ptr} + 1$
 NEG_OFFSET ← k
 call ADD_B1_[$k$]
 if $k \neq 0$ then
   OFFSET ← 9
   call ADD_B2_[$k$]
 return

ADD_B1_0: $C[0] \leftarrow C[0] \oplus VE[0]$          ▷ Subroutine 1
ADD_B1_1: $C[1] \leftarrow C[1] \oplus VE[1]$
...
ADD_B1_7: $C[7] \leftarrow C[7] \oplus VE[7]$
ADD_B1_8: $R0 \leftarrow R0 \oplus VE[8]$
ADD_B1_9: $R1 \leftarrow R1 \oplus VE[9]$
...
ADD_B1_20: $R12 \leftarrow R12 \oplus VE[20]$
return

ADD_B2_10: $C[30] \leftarrow C[30] \oplus VE[21]$     ▷ Subroutine 2
ADD_B2_9: $C[29] \leftarrow C[29] \oplus VE[20]$
...
ADD_B2_1: $C[21] \leftarrow C[21] \oplus VE[12]$
OFFSET ← 0
return
```

Figure 5: Algorithm implementing the *l-t-r comb* method using virtual addressing.

GPRs, it is possible to eliminate the need of memory accesses for 538 word-wise additions. This means that only two instruction are required.

Consequently, this saves about 2,100 instructions per multiplication while introducing a small overhead of about 100 instructions for setting the parameters for virtual addressing (see Fig. 5). The principles of virtual addressing could also be adapted to speed up other cryptographic algorithms.

3.5 Instruction Set Extension

A well-known approach to accelerate a software implementation is to expand the microprocessor to support specific instructions. We examined two additional instructions, which lead to a significant performance improvement: a shift-right instruction and an instruction to load a value from RAM and XOR it with a register. Both operations are executed during one clock cycle. These extensions accelerate ECC and other cryptographic algorithms like AES as well.

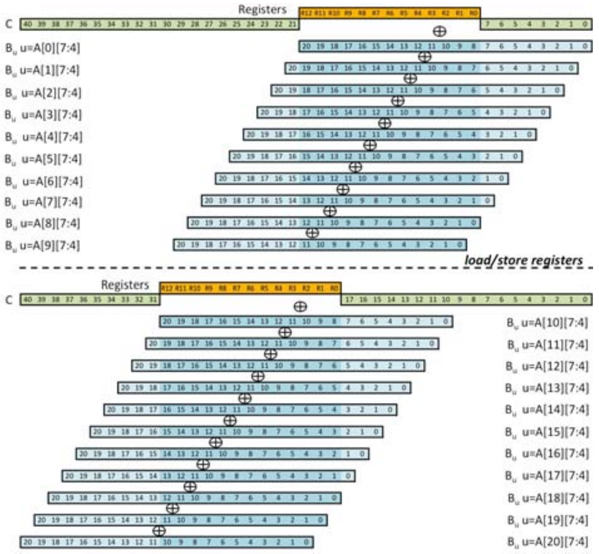


Figure 6: Illustration of additions stated in Fig. 5 for processing the first window. To process the second window, the bits [3:0] of the currently processed A are used to determine u.

3.6 Lightweight Coprocessor for Binary Field Multiplication

Next, we present a low-cost coprocessor for outsourcing the whole field multiplication and reduction to hardware.

3.6.1 Coprocessor Design

To keep the communication overhead low, the coprocessor directly communicates with the RAM via Direct Memory Access. The coprocessor first reads two factors from RAM, then performs a multiplication, and finally stores the result back to the RAM. The addresses of the two factors and the result are provided from the microprocessor. During the calculation of the coprocessor, the microprocessor pauses.

Typical ECC coprocessors in literature have relative high area requirements, since they offer partial multiplications with high bitlengths (i.e. *mxm*-bit [18] or *mx1*-bit [14]). In general, a *mxn*-bit binary multiplier requires *m·n* AND and *(m-1)·(n-1)* XOR gates.

We propose to use a 4*x*8-bit multiplier and calculate an 8*x*8-bit multiplication in two cycles with seven additional XOR gatters (see Fig. 7). The used multiplication algorithm executes about 440 8*x*8 bit multiplications. Hence, one multiplication takes about 440 cycles longer using a 4*x*8-bit multiplier. However, compared to a conventional 8*x*8-bit multiplier this saves the area of 32 AND and 21 XOR gatters.

3.6.2 Binary Field Multiplication and Reduction

The coprocessor features an own control logic to calculate the binary field multiplication and reduction. The availability of additional hardware influences the choice of the multiplication algorithm. If partial hardware multiplication is supported, it is proposed to use Comba's method [9].

The difference to the *l-t-r* multiplication is the order in which the partial products are generated. Comba's method determines each word of the result C at a time proposed in literature and includes two nested loops: the first one calculates the words $C[20]$ to $C[40]$ and the second one determines the words $C[0]$ to $C[19]$. Only one store operation is required for every word of the result. This order of calculation favours an interleaved reduction. This means that the higher words, which would require a reduction, are not stored in the accumulator. They are directly reduced, which

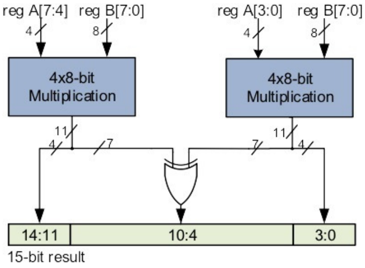


Figure 7: Construction of an 8x8-bit multiplication with a 4x8-bit multiplication.

is implemented in hardware requiring only 13 XOR-gatters. For more information about Comba's method, we refer to [9] and [6].

4. RESULTS

The previously presented methods have been implemented and simulated. The software implementations were coded in assembler and the hardware accelerators were implemented at Register Transfer Level using the SystemVerilog language. For area comparison the variants were synthesized in standard 220nm CMOS technology. The result of the synthesis represented the space needed for the standard cell area. To take place and route into account assumed 20% were added to the cell area.

4.1 Comparison of Implementation Variants

Table 1 summarizes the performance and area requirements of the previously presented methods. Note that the given areas do not include the microprocessor.

Table 1 illustrates that the binary field multiplication is the most time-consuming field operation and thus is the determining factor for the overall performance. It accounts for about 80% of the execution time without hardware accelerators. The low-area hardware extensions lead to significant performance improvements of the field multiplication.

Compared to the standard *l-t-r comb* method with a windowsize of *w=4*, the *enhanced l-t-r comb* method with a windowsize of *w=4* requires 148 bytes less RAM. However, it requires 105 bytes more RAM than the standard *l-t-r comb* method with a windowsize of *w=2*, while decreasing the execution time by 25%.

The next implemented variant is a combination of the virtual addressing (VA) concept described above and the *enhanced l-t-r comb* algorithm. Therefore, only slight adaptations of the algorithm shown in Figure 5 were required. Adding the virtual address logic causes a small additional area overhead (est. +1kGE), but the performance further improves by 26%.

The two additional instructions lead to a negligible area overhead and improve the computation performance even further by 27% to 5.1 MCycles.

The coprocessor offers the best performance/area trade-off. Since the availability of additional hardware features changed the choice of the field multiplication algorithm, no precomputation is required any more. This approach reduced the size of the required RAM to almost a half. Furthermore, the coprocessor lowered the ROM storage requirement by a factor of 3.5. This is due to the outsourcing of the multiplication logic to dedicated hardware. Hence, no software code for the field multiplication is neccessary any more. We determined the area of the coprocessor with synthesis, which reported 1.41 kGE combinational and 0.64 kGE non-combinational area. We assumed 20% additional area for routing overhead, which leads to a area-footprint 2.13 kGE. Additionally, VA logic for field addition was used (est. 0.3kGE). In sum, the area reduction due to lower storage requirements, was larger than the additional introduced area of the coprocessor. As a consequence this solution requires the smallest area-footprint. In addition, due to the usage of dedicated hardware to calculate the field multiplication, the performance of the coprocessor variant stands far above the previous partitioning methods. Compared to the fastest pure software approach a speed up of 3.5 was reached.

The results show that hardware extensions can almost always accelerate the execution time at the expense of area. An exception is the coprocessor variant. Due to the algorithmic change, this solution offers both the fastest runtime and the smallest area.

5. RELATED WORK

In resent years, many authors showed that RFID is ready for hardware-based ECC. The most notable implementations were presented by Batina et al. [3], Hein et al. [11], Kumar et al. [15], Lee et al. [16], Wolkersdorfer et al. [23], and Bock et al. [5]. They mainly use binary fields, require between 10.4 and 23.8 kGE area, and consume between 32.4 and 500 $\mu W/MHz$ of power.

In terms of ECC on 8-bit microprocessors, also much research has been done. Most publications target Wireless Sensor Networks (WSNs) and use the ATmega128 [2] processor. Malan et al. investigated the feasibility of ECC over binary fields in WSNs [17]. However, their implementation was quite slow, requiring about 2,510 MCycles per authentication. Guara et al. showed in [10] that ECC offers significant performance advantages compared to RSA on 8-bit architectures. Yan and Shi proposed a sophisticated inversion algorithm to speed up the ECC calculation [24]. Seo et al. [19] proposed an approach to reduce the number of memory accesses, which was then implemented assembly-optimized in [13]. Wenger et al. built in [22] a low-area processor (6.5 kGE) for RFID applications and presented AES, Grøstl, and ECC implementations.

Several papers describe how to accelerate software-based ECC with dedicated hardware like a coprocessor (e.g., [1, 14, 4]) or instruction set extensions (e.g., [20, 7, 9, 8]).

The presented ECC hardware/software architecture compares favourably with works described in the literature. Table 2 highlights different 8-bit ECC implementations. The implementations over prime fields exploit the ATmega128's hardware multiplier. Guara et al. [10] reached considerable performance results. However, they used a non-adjacent form method for point multiplication. Wenger et al. [22] presented a clone of the ATmega128 targeting resource- constrained RFID tags. The silicon-footprint of their proposed processor is 6.5 kGE, which is almost two times larger than the processor we used. Our approach requires comparable memory resources, but achieves better performance results. The ECC calculations presented in [21] and [13] were also performed over binary fields and could not take advantage of the hardware multiplier. The implementation of Kargl et al. [13] is comparable to ours, since they use a similar field and point multiplication method. By fully utilizing the 32 registers available on the ATmega128, they reduced the number of memory accesses and reached a runtime of 6.1 MCycles. Thus, the execution time is faster than our pure software approach, but requires significantly more ROM. Furthermore, we had only half as many GPRs at our disposal.

By using our presented hardware extensions, we achieve a notable runtime performance, small memory requirements, and maintain a high level of flexibility.

6. CONCLUSION

ECC is well suited for security related resource-limited applications. However, current smart card and RFID tag solutions often focus on pure inflexible hardware ECC designs. We offer design proposals for implementing ECC using a lightweight 8-bit RFID processor. An effective enhancement of a state-of-the art software-based binary field multiplication algorithm is presented. Furthermore, a novel ECC

Table 1: Area and performance comparison of implementation variants

Implementation	*Code Size (ROM)*		*RAM*		*Ext.*	***Area***	*Binary Field Operations [Cycles]*				***Mont. Mult.***
Variant	*[Byte]*	*[kGE]*	*[Byte]*	*[kGE]*	*[kGE]*	***[kGE]***	*Add.*	*Squar.*	*Red.*	*Mult.*	***[MCycles]***
L-t-r mult. w=2	3,205	3.41	318	4.1	-	**7.51**	150	1,560	580	9,750	**12.1**
Enh. l-t-r mult. w=4	3,123	3.32	423	5.46	-	**8.92**	150	1,560	580	7,640	**9.4**
Enh. l-t-r mult. w=4 & VA	3,840	4.09	423	5.46	1	**10.55**	90	1,540	580	5,280	**7.0**
Enh. l-t-r mult. w=4 VA & ISE	3,594	3.83	423	5.46	1	**10.29**	75	1,070	500	3,820	**5.1**
Coprocessor & ISE	1,023	1.09	214	2.76	2.43	**6.18**	75	1,070	-	1,830	**2.8**

Table 2: Comparison to 8-bit ECC implementations available in literature

Implementation	*GF*	*ROM*	*RAM*	*Runtime*
Variant		*[kByte]*	*[Byte]*	*[MCycles]*
Guara et al.[10]	p_{160}	3.6	280	6.48
Wenger et al.[22]				
Slowest version	p_{160}	3.86	384	35.1
Fastest version	p_{160}	7.76	384	13.0
Szczechowiak et al.[21]	2^{163}	32.4	1741	16.0
Kargl et al [13]	2^{167}	11	>588	6.1
Our implementation				
Pure software	2^{163}	3.05	423	9.7
VA and ISE	2^{163}	3.51	423	5.1
Coprocessor	2^{163}	1.02	214	2.8

hardware/software partitioning approach using virtual addressing is introduced. Additional hardware/software partitioning variants are outlined and evaluated.

Our approaches is highly competitive regarding performance and area. The fastest variant requires about 0.2s@13.56MHz to calculate a challenge. This is about 4.6 times faster as the most similar solution using a microprocessor to calculate ECC on an RFID tag [22]. We showed that a software-based development of ECC is practical for applications, like brand protection, which are not very time critical.

Our future work includes an analysis of the proposed implementation methods in the light of side-channel attacks and power consumption.

Acknowledgment

We would like to thank our industrial partner Infineon Technologies Austria AG, especially all members of Infineon's PDC team for their great support and the Austrian Federal Ministry for Transport, Innovation, and Technology, which funded the project META[:SEC:] under the FIT-IT contract 829586.

7. REFERENCES

[1] H. Aigner, H. Bock, M. Hütter, and J. Wolkerstorfer. A low-cost ECC coprocessor for smartcards. *CHES*, 2004.

[2] Atmel Corp. *8-bit Microcontroller with 128K Bytes In-System Programmable Flash: ATmega 128*, 2004.

[3] Batina et al. Hardware architectures for public key cryptography. *Integration, the VLSI journal*, 2003.

[4] G. Bertoni, L. Breveglieri, and M. Venturi. Power aware design of an elliptic curve coprocessor for 8 bit platforms. In *PerCom*. IEEE, 2006.

[5] H. Bock, M. Braun, M. Dichtl, E. Hess, J. Heyszl, W. Kargl, H. Koroschetz, B. Meyer, and H. Seuschek. A Milestone Towards RFID Products Offering Asymmetric Authentication Based on Elliptic Curve Cryptography. *Invited talk at RFIDsec*, 2008.

[6] S. V. D.R. Hankerson and A. Menezes. *Guide to Elliptic Curve Cryptography*. 2004.

[7] W. Drescher, K. Bachmann, and G. Fettweis. VLSI architecture for datapath integration of arithmetic over GF(2m) on digital signal processors. In *Acoustics, Speech, and Signal Processing*, 1997.

[8] H. Eberle, A. Wander, N. Gura, S. Chang-Shantz, and V. Gupta. Architectural extensions for elliptic curve cryptography over $GF(2^m)$ on 8-bit microprocessors. *ASAP*, 2005.

[9] Großschädl et al. When Instruction Set Extensions Change Algorithm Design: A Study in Elliptic Curve Cryptography. 2005.

[10] Gura et al. Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs. *CHES*, 2004.

[11] D. Hein, J. Wolkerstorfer, and N. Felber. ECC is Ready for RFID–A Proof in Silicon. In *Selected Areas in Cryptography*, 2009.

[12] U. Kaiser, C. Paar, J. Pelzl, D. Rappe, W. Schindler, A. Weimarskirch, and T. Wollinger. Auswahlkriterien fuer kryptographische Algorithmen bei Low-Cost-RFID-Systemen, 2005.

[13] A. Kargl, S. Pyka, and H. Seuschek. Fast arithmetic on ATmega128 for elliptic curve cryptography. *context of the SMEPP project*, 2008.

[14] Koschuch et al. Hardware/software co-design of elliptic curve cryptography on an 8051 microcontroller. *CHES*, 2006.

[15] S. Kumar and C. Paar. Are standards compliant elliptic curve cryptosystems feasible on RFID? In *Workshop on RFID Security*, 2006.

[16] Lee et al. Elliptic-curve-based security processor for RFID. *IEEE Transactions on Computers*, 2008.

[17] D. Malan, M. Welsh, and M. Smith. A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography. In *Sensor and Ad Hoc Communications and Networks*, 2004.

[18] S. Okada, N. Torii, K. Itoh, and M. Takenaka. Implementation of elliptic curve cryptographic coprocessor over $GF(2^m)$ on an FPGA. In *CHES*, 2000.

[19] S. Seo, H. Dong-Guk, H. Kim, and H. Seokhie. TinyECCK: Efficient Elliptic Curve Cryptography Implementation over $GF(2^m)$ on 8-Bit MICAz Mote. *IEICE transactions on information and systems*, 2008.

[20] Z. Shi and H. Yan. Software implementations of elliptic curve cryptography. *International Journal of Network Security*, 2008.

[21] Szczechowiak et al. NanoECC: Testing the limits of elliptic curve cryptography in sensor networks. *WSNs*, 2008.

[22] E. Wenger, T. Baier, and J. Feichtner. JAAVR: Introducing the Next Generation of Security-enabled RFID Tags. *Euromicro Conference on DSD*, 2012.

[23] J. Wolkerstorfer. Scaling ECC Hardware to a Minimum, 2005. Slides of a talk given at Workshop CRASH 2005, Leuven.

[24] H. Yan and Z. Shi. Studying software implementations of elliptic curve cryptography. In *Information Technology: New Generations*, 2006.

A Flexible and Lightweight ECC-Based Authentication Solution for Resource Constrained Systems

Norbert Druml, Manuel Menghin, Christian Steger,
and Reinhold Weiss
Institute for Technical Informatics
Graz University of Technology
Graz, Austria
{norbert.druml, manuel.menghin, steger, rweiss}@tugraz.at

Holger Bock and
Josef Haid
Design Center Graz
Infineon Technologies Austria AG
Graz, Austria
{holger.bock, josef.haid}@infineon.com

***Abstract*—RFID-based and NFC-based applications can be found, apart from others, in security critical application fields, such as payment or access control. For this purpose, Elliptic-Curve Cryptography (ECC) is commonly used hardware integrated in resource constrained applications in order to provide authenticity and data integrity. On the one hand, specialized crypto hardware approaches provide good performance and consume low power. On the other hand, they often lack flexibility, caused, for example, by hardware integrated protocols and cryptographic parameters.**

Here we present a flexible and lightweight ECC-based authentication solution that takes into account resource constrained systems. This technique permits to shift parts of the computational intense ECC calculations from the resource constrained device to the authentication terminal. By employing a security controller with a small multi-purpose hardware acceleration core, high computation speed is achieved and a maximum level of flexibility is maintained at the same time.

We demonstrate the feasible implementation of the proposed technique by means of an Android-based reader / smart card system, which represent a prime example of contemporary power-constrained and performance-constrained embedded systems. An ECC-based authentication can be carried out on average within 25 ms and checked against a back-end server within 66 ms in a secured manner. Thus, a secured and flexible one-way authentication system is given that shows high performance. This solution can be utilized in a wide variety of application fields, such as anti-counterfeiting, where flexibility and low chip prices are essential.

***Index Terms*—Elliptic-Curve Cryptography, Authentication, Resource Constrained System, Smart Card**

I. Introduction

Applications that feature Radio Frequency Identification (RFID) and Near Field Communication (NFC) can be found in our everyday life. Such RFID-based and NFC-based applications are used in the fields of, e.g., payment, transport, logistics, health care, and access control. Not to mention that the market value of RFID-based devices, applications, and services will increase from \$9.2 billion to \$30.4 billion between the years 2014 and 2024, according to a recently published market study (cf. [1]). Given these trends and due to the fact that RFID and NFC are contactless communication techniques, security is a crucial factor, particularly in application fields such as Industry 4.0. Industry 4.0 is a concept coined by the German government that promotes so-called smart factories. In these smart factories all devices, machines, and appliances will be interconnected, leading to cyber-physical systems. Authenticity and data integrity of all involved components and remote terminals must be protected all time. For this purpose, smart cards featuring security controllers and Elliptic-Curve Cryptography (ECC) are the device of choice in order to maintain secure system operation and to protect from malicious security attacks.

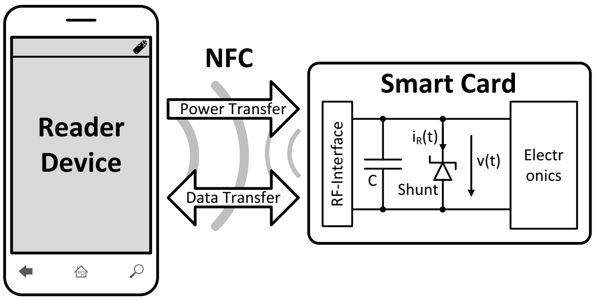


Fig. 1. A typical contactless reader / smart card system. The reader emits an alternating and modulated magnetic field that powers the smart card and through which contactless communication is also enabled.

Fig. 1 illustrates the basic setup of a contactless reader / smart card system. A reader emits an alternating and modulated magnetic field that powers the smart card and through which contactless communication is also enabled. Due to this inductive coupling, a smart card is very constrained in terms of available electrical power, chip size, and computational resources. During a smart card's peak power consumption or during low magnetic field supply periods, a smart card's supply voltage may drop hazardously below a certain threshold. Such hazardous voltage drops result in a loss of operational stability. This power sensitivity is stressed in Fig. 2. In this figure, a smart card executes a pure software encryption, which results in its supply voltage to drop hazardously below a threshold of 1 V. Given these vulnerabilities and constraints, flexible pure software solutions for complex cryptographic

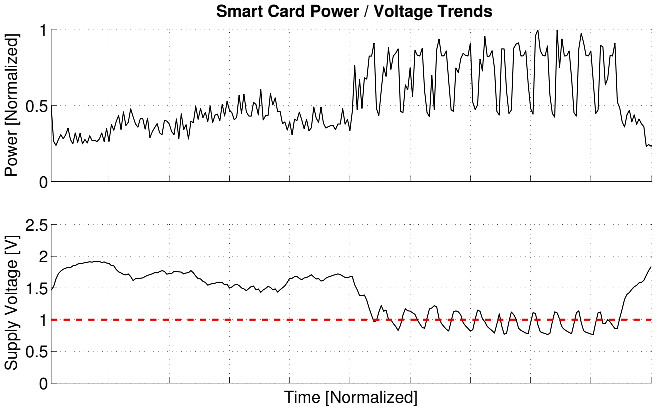


Fig. 2. This figure highlights the power constraints of contactless smart cards. Voltage drops are caused by a software-based cryptographic algorithm. The smart card's operational stability will be disturbed if these emergencies are not handled properly. Obtained with changes from [3].

operations are very difficult to implement without violating critical power or timing constraints. As a consequence, dedicated and specialized hardware crypto cores are commonly integrated into constrained embedded systems, such as smart card chips. This approach of highly specialized crypto cores can solve these power and timing issues. However, unwanted inflexibility can be introduced caused, for example, by hardware integrated protocols and cryptographic parameters. Yet, development teams require flexible and adaptable systems in order to react quickly to changing demands of the market.

This paper presents an innovative ECC-based authentication solution that takes into account the highlighted contactless smart card issues concerning flexibility and resource constraints. The presented approach is implemented by employing an optimized ECC-based authentication protocol, which is based on the work of [2]. This protocol permits to shift parts of the computational intense ECC calculations from a resource constrained embedded system, which is represented by a smart card, to the computational powerful reader device. At the same time, a maximum level of flexibility can be maintained. Furthermore, this paper evaluates the timing behavior of a secured datalink between an Android-based reader device and a back-end server system. The shown authentication solution can be utilized in a wide variety of resource constrained application fields, ranging from anti-counterfeiting, where chip prices play an important role, to industrial applications.

This paper makes the following contributions:

- It demonstrates the shifting of computational intense ECC calculations from a resource constrained embedded system to the computational powerful reader device while maintaining a maximum level of flexibility.
- It proves the feasible implementation and usage of the proposed techniques by means of an Android-based reader / smart card system and a back-end server.
- It evaluates the timing behavior of a secured wireless datalink between an Android-based reader device and an industrial back-end server system.

This paper is structured as follows. Section II gives a short introduction into the related work covering the topic of ECC-based software and hardware crypto implementations. In Section III our flexible authentication solution is presented. Followed by Section IV which demonstrates the feasible implementation of the presented authentication concept featuring a commonly used Android-based reader device and an industrial back-end server. Finally, our results are concluded and some details about our future work are given in Section V.

II. Related Work

A lot of research has been carried out in the field of asymmetric cryptography and embedded systems. In [4], Wander et al. showed that ECC can be feasibly implemented in resource constrained devices. Accordingly, significant amounts of electrical energy can be saved compared to RSA implementations of equivalent security level. In addition, ECC leads to improved computation times and reduced storage requirements as well as reduced communication overheads due to smaller key sizes. Batina et al. evaluated in [5] ECC for the usage in RFID-based identification protocols and demonstrated a feasible implementation. Further ECC-based protocols that targeted resource constrained applications were presented, for example, by the authors in [6] and [7]. In [8], the authors introduced an ECC-based authentication protocol that is particularly suitable for resource constrained embedded systems, such as contactlessly powered RFID tags. Bock et al. demonstrated in [2] that this ECC-based protocol can be feasibly implemented in an RFID tag chip. This ECC-tag chip featured 163-bit binary fields, was optimized for low energy consumption, and finished the computations that are required for an authentication procedure within 95 ms. In [9], Wenger et al. built a clone of the 8-bit ATMega128 running at 13.56 MHz and targeted resource constrained RFID applications. The authors also integrated hardware acceleration cores for faster cryptographic computations, such as ECC over prime fields, AES, and Grøstl. An ECC point multiplication was conducted within 13 MCycles while employing the secp160r1 curve. In [10], the authors evaluated cycle-accurate clones of the popular embedded processors 8-bit Atmel ATmega, 16-bit Texas Instruments MSP430, and 32-bit ARM Cortex-M0+ with regards to the resulting performance of software ECC implementations. While the MSP430 dissipates the least amount of power, the Cortex-MO+ provides the best performance, and the ATmega the highest improvement potential. In [11], the authors aimed at flexibility and presented a hardware support that featured five prime field-based NIST ECC curves. Optimized hardware/software co-design approaches were evaluated and proposed by the authors in [12] in order to accelerate ECC calculations for resource constrained applications. Further ECC implementations were presented, for example, by the authors in [13]–[15].

Summarizing, in the field of resource constrained secure systems it is particularly important to meet power and timing requirements and to maintain a high amount of flexibility at the same time. This paper provides an innovative contribution to the ongoing discussing in this important field of research.

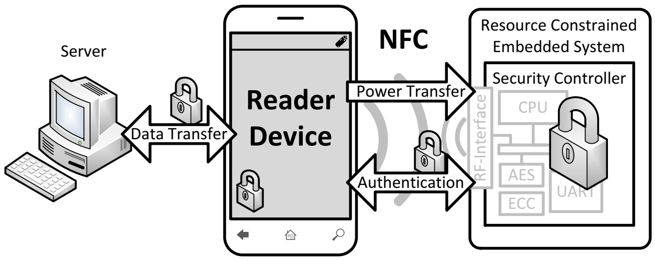


Fig. 3. Flexible ECC-based authentication system consisting of a back-end server, an NFC-enabled reader device, and a resource constrained embedded system.

III. Flexible Authentication Solution for Resource Constrained Systems

The concept of our presented flexible authentication system is shown in Fig. 3. It consists of a back-end server, a mobile NFC-enabled reader device, and the resource constrained embedded system whose authenticity is to verify.

In the following, the brand protection use case is employed as a motivational example. Given is a product, whose authenticity is to verify throughout the supply chain. For this purpose, the manufacturer equips the product with a security controller-based authentication chip similar to the one used in this work. The product's authenticity is checked with the help of a mobile reader device, such as an NFC-enabled smart phone, via an optimized lightweight authentication protocol. The gathered product's authentication information is then buffered on the mobile reader device. The reader then updates the back-end database with the buffered authentication information through a secured datalink as soon as wireless network coverage is given.

In this work, the resource constrained embedded system is represented by a contactless smart card. The following section describes in detail the individual components, concepts, as well as the authentication protocol that is used between reader and smart card. Note, due to disclosure policies, some security-related details are omitted and marked with *.

A. Back-end Server

For this work we used an industrial back-end server system running Windows 8. It features a relational database which is accessed through SQL. A Machine-to-Machine interface is provided by a Windows Communication Foundation (WCF)-based web service, which is run by the Internet Information Server (IIS). A secure connection from a reader device can be established through the HTTPS protocol by using Transport Layer Security (TLS) version 1.2, Elliptic Curve Cryptography, and RSA with the following configurations:

- Elliptic Curve Diffie-Hellman with Ephemeral keys (ECDHE) is used for the key exchange mechanism.
- Certificates are signed with the Rivest-Shamir-Adleman (RSA) algorithm. Note, the employed version of Microsoft's Internet Information Server did not support signatures signed with Elliptic Curve Digital Signature Algorithm (ECDSA).
- Symmetric message encryption is carried out with 256-bit Advanced Encryption Standard (AES) in Cipher Block Chaining (CBC) mode featuring Secure Hash Algorithm (SHA1) for message authentication.

Apart from the encrypted HTTPS interface, also an unencrypted interface is provided for the purpose of performance comparisons.

B. Reader Device

During this work, an NFC-enabled Samsung Galaxy i9300 S3 smart phone was used as reader device. This smart phone integrates an ARM Cortex-A9 quad-core with 1.4 GHz and runs the Android 4.3 operating system. A connection to the back-end server can either be established with unencrypted HTTP or encrypted HTTPS protocols through 3G/4G or WiFi communication networks. Open source cryptographic libraries, such as Spongy Castle, are used to carry out the ECC computations and signature checks of the one-way reader / smart card authentication protocol in order to verify the authenticity of the smart card.

The reader device acts as gateway between the server and the smart card. No direct interaction between server and smart card is given, which reduces the smart card's resource requirements in terms of performance and power supply. Note, in this work we assume that the reader device represents a secure entity.

C. Resource Constrained Embedded System

As an example for a typical power constrained and performance constrained embedded system, a contactless smart card was selected which features an Infineon security controller running at 30 MHz. The employed type of security controller implements a small processor (e.g., an Application Specific Instruction-set Processor (ASIP)) and a multipurpose hardware acceleration core that is optimized for long integer and polynomial modular multiplication. Thus, various calculation intense operations that are required, e.g., for ECC and RSA algorithms can be computed hardware accelerated. The used security controller provides a maximum level of flexibility by omitting highly specialized ECC or RSA crypto cores that integrate, for example, the protocol and only one type of security method (e.g., only secp192r1) in hardware. Furthermore, the security controller comes with a low area-footprint thanks to its small processor core. Due to this setup, application engineers can react quickly to changing market demands. For example, elliptic curves, calculations, and their special parameters can be changed easily due to the security controller's and its hardware accelerator's support of arbitrary ECC curves up to a bit-size of 521 bit. In addition, changes to the protocol can be easily handled by the small processor core. Apart from the small processor and the important flexible hardware acceleration core, the security controller also integrates crucial state-of-the-art side-channel countermeasures. Thanks to the security controller's low area consumption and low-power technology, it can be used in an optimal way for resource constrained applications.

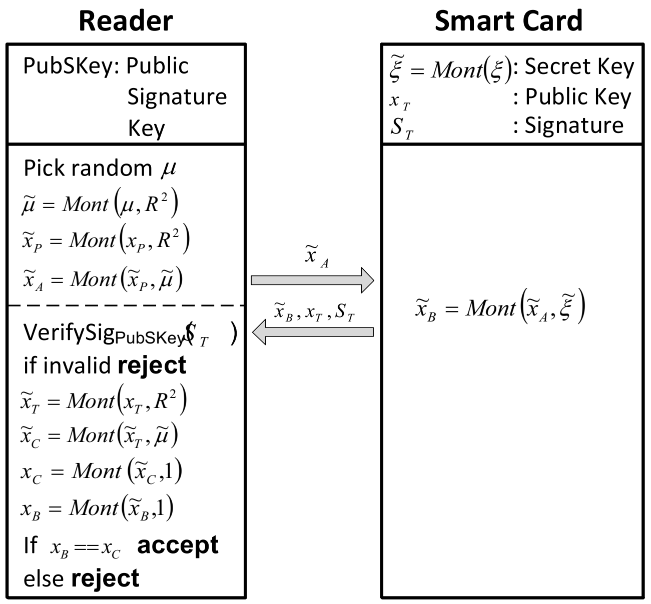

Reader
Smart Card
PubSKey: Public Signature Key
$\widetilde{\xi} = Mont(\xi)$: Secret Key
x_T : Public Key
S_T : Signature
Pick random μ
$\widetilde{\mu} = Mont(\mu, R^2)$
$\widetilde{x}_P = Mont(x_P, R^2)$
$\widetilde{x}_A = Mont(\widetilde{x}_P, \widetilde{\mu})$
$\widetilde{x}_A$
$\widetilde{x}_B, x_T, S_T$
$\widetilde{x}_B = Mont(\widetilde{x}_A, \widetilde{\xi})$
VerifySig$_{PubSKey}$(S_T)
if invalid reject
$\widetilde{x}_T = Mont(x_T, R^2)$
$\widetilde{x}_C = Mont(\widetilde{x}_T, \widetilde{\mu})$
$x_C = Mont(\widetilde{x}_C, 1)$
$x_B = Mont(\widetilde{x}_B, 1)$
If $x_B == x_C$ accept
else reject

Fig. 4. ECC-based one-way authentication protocol used between reader and smart card. Operating in the Montgomery Domain permits shifting computation effort from the smart card to the reader device. Obtained with changes from [2].

A security controller, as it is used in this work, can also support contact-based interfaces in addition to a concactless interface. Such a dual-interface approach can be employed, for example, as a secure contactless gateway to security critical embedded systems, as it is demonstrated in [16].

D. ECC-Based One-Way Authentication Protocol

Fig. 4 illustrates the concept of the one-way authentication protocol, which is based upon the authentication protocol presented in [2] and [8]. It is used between reader and the resource constrained embedded system, which is represented by the contactless smart card. The presented authentication protocol is based on the Diffie-Hellman key exchange, uses ECC over prime fields, and computes point multiplications with the help of Montgomery Domain transformations.

1) Requirements and Setup: Let E be an elliptic curve over GF(p) and let $P = (x_P, y_P)$ be a point on E with prime order $q \in \mathbb{N}$. During a setup phase, the smart card is initialized with a random private key $0 < \xi < q$, which is transformed into the Montgomery Domain $\widetilde{\xi}$. Additionally, the smart card is initialized with a certificate containing the public key x_T and its signature S_T, where x_T represents the x-coordinate of $T = \xi \cdot P$. The reader is configured with the public signature key $PubSKey$. No further public keys or private keys need to be initialized or stored on the reader.

2) Authentication Process: The process of authentication works as follows. The reader generates a random number $0 < \mu < q$ and transforms μ as well as the x-coordinate x_P of the point P into the Montgomery Domain $\widetilde{\mu}$ and $\widetilde{x}_P$ with the help of the Mongomery Reduction function $Mont()$. Then, the reader calculates the challenge $\widetilde{x}_A$ and sends it to the smart card. The smart card computes the response $\widetilde{x}_B$ with its pre-transformed secret $\widetilde{\xi}$. Afterwards, the smart card returns the computed response $\widetilde{x}_B$ and a certificate that contains the smart card's public key x_T and the public key's signature S_T. In a further step, the reader verifies the certificate through $VerifySig$ and transforms the smart card's public key x_T into the Montgomery Domain $\widetilde{x}_T$. Finally, the reader calculates $\widetilde{x}_C$ and transforms $\widetilde{x}_C$ back to the original domain x_C. If x_C equals x_B, a one-way authentication is completed successfully.

3) Security: The security of this protocol is based on the Elliptic Curve Diffie Hellman Problem. If an attacker receives the challenge $A = \mu \cdot P$, he has to return a valid response B with the signed public key $T = \xi \cdot P$. The attacker only knows A and T, but not the crucial parameters μ and ξ. Therefore, the attacker can only calculate a valid response $B = \xi \cdot (\mu \cdot P)$ if and only if he solves the Elliptic Curve Diffie Hellman Problem.

4) Implementation and Performance Aspects: The basic and simplified implementation of this protocol is outlined in Listing 1 and Listing 2, according to [17] and [18]. Let $R > p$ and $gcd(R, p) = 1$. p is chosen to be odd. p' is defined according to (1). R is chosen, according to (2), in a way to ease the division of Listing 2. While W represents the W-bit architecture, t represents the number of W-bit words in order to store one element within an array. Thanks to this Montgomery approach, the modular multiplication can be carried out efficiently without explicitly conducting the costly modular reduction step.

$$p' = -p^{-1} \ mod \ R \tag{1}$$

$$R = 2^{W \cdot t} \tag{2}$$

The employed one-way authentication protocol offers the following performance and resource advantages for constrained embedded systems:

- The global computation effort is reduced due to the fact that only x-coordinates are used during the ECC

Listing 1. Montgomery-Based Calculation of $c = a \cdot b \bmod p$, cf. [17], [18]

```
$\widetilde{a} = Mont(a, R^2)$
$\widetilde{b} = Mont(b, R^2)$
$\widetilde{c} = Mont(\widetilde{a}, \widetilde{b})$
$c = Mont(\widetilde{c}, 1)$
return c
```

Listing 2. Basic Montgomery Reduction* $c = Mont(a, b)$, cf. [17], [18]

```
$z = a \cdot b$
$c = [z + (z \cdot p' \ mod \ R) \cdot p]/R$
if $c \geq p$ then
    $c = c - p$
endif
return c
```

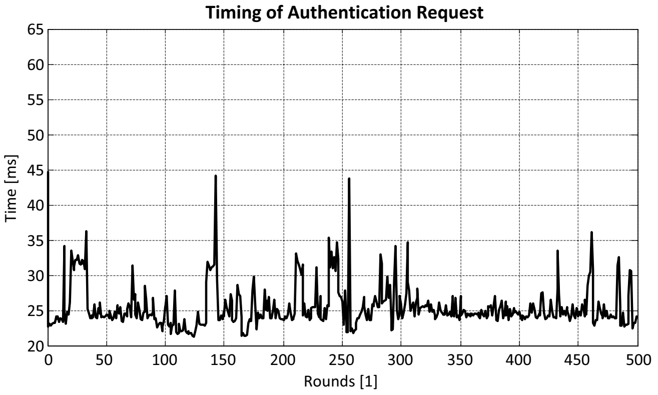


Fig. 5. This figure shows the required time for sending the authentication challenge from reader to smart card and waiting for the response. Note, an NFC data rate of 106 kBit/s is used. Timing spikes are caused by the Android operating system.

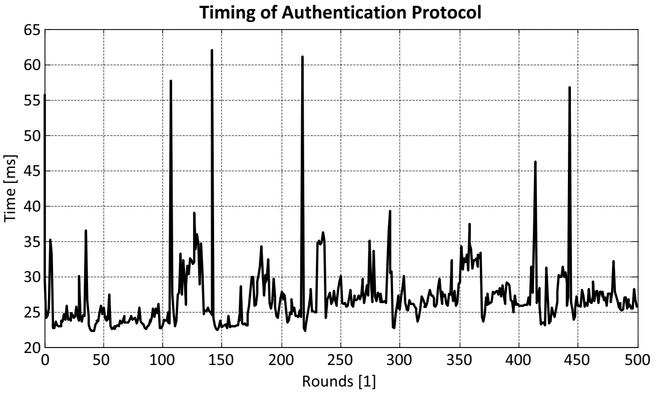


Fig. 6. This figure shows the required time for processing the ECC-based authentication protocol without signature verification. Note, an NFC data rate of 106 kBit/s is used. Timing spikes are caused by the Android operating system.

calculations.

- The reader sends and receives values which are part of the Montgomery Domain. This approach permits to shift computational effort from the resource constrained embedded system to the reader device.
- The resource constrained embedded system uses pre-transformed values and operates in the Montgomery Domain only. Therefore, the smart card reduces its computational effort through calling $Mont()$ only once.

The simplified Montgomery Reduction function* $Mont()$, which is given by Listing 2, can be carried out in the smart card's security controller by performing only seven hardware accelerated integer arithmetic operations.

IV. Results

The following section presents several results that we gained from benchmarking the back-end server connection as well as the ECC-based one-way authentication between reader and smart card. First, the timing of the one-way authentication request between reader and smart card is measured. Second, the total timing behavior of the one-way authentication protocol is analyzed. Third, a timing comparison of the conducted benchmarks is made. The final analysis evaluates the timing behavior of both the back-end HTTP and HTTPS server connections.

A. ECC-Based One-Way Authentication Request

The NIST secp192r1 ECC curve was used for benchmarking the ECC-based one-way authentication request between reader and smart card. This benchmark aims at evaluating the timing behavior of the authentication request only, which is sent from reader to smart card and is processed there. The measured total time value t, which is defined by (3), consists of the following timing components:

- A delay t_{OS1} that is caused by the Android operating system for sending the request from the application through the software stack to the reader's NFC chip. A second delay t_{OS2} is caused for transferring the smart card's response from the reader's NFC chip through the software stack to the application.
- Delays t_{REQ} and t_{RSP} are caused by transmitting the request and response on the contactless NFC data link. During the following tests, NFC is configured for the lowest possible data transmission speed of 106 kBit/s.
- t_{SC} defines the calculation time needed by the smart card in order to fetch the authentication request and to carry out the ECC calculations.

$$t = t_{OS1} + t_{REQ} + t_{SC} + t_{RSP} + t_{OS2} \tag{3}$$

Fig. 5 illustrates the timing behavior of the authentication request benchmark, which was executed 500 times. The average consumed time t is as low as 24.9 ms. Note, the non-deterministic timing spikes are caused by the Android operating system, which is represented by t_{OS}.

B. ECC-Based One-Way Authentication Protocol

Again, the NIST secp192r1 ECC curve was used for this benchmark. This benchmark aims at evaluating the complete timing behavior of the ECC-based one-way authentication protocol between reader and smart card. The timing of the signature verification $VerifySig$ was excluded in order to permit valid timing comparisons. In addition to t_{OS1}, t_{REQ}, t_{SC}, t_{RSP}, and t_{OS2} the measured total time value t, which is defined by (4), consists also of the following timing components:

- $t_{Prot.1}$ and $t_{Prot.2}$ define the time that is required by the smart phone to process the ECC-based authentication algorithms. This includes the initialization as well as the final verification.

$$t = t_{Prot.1} + t_{OS1} + t_{REQ} + t_{SC} + t_{RSP} + t_{OS2} + t_{Prot.2} \tag{4}$$

Fig. 6 depicts the timing behavior while performing the ECC-based one-way authentication protocol 500 times. The average required time t to process the protocol is as low as 26.2 ms. Although, the reader performs the calculation

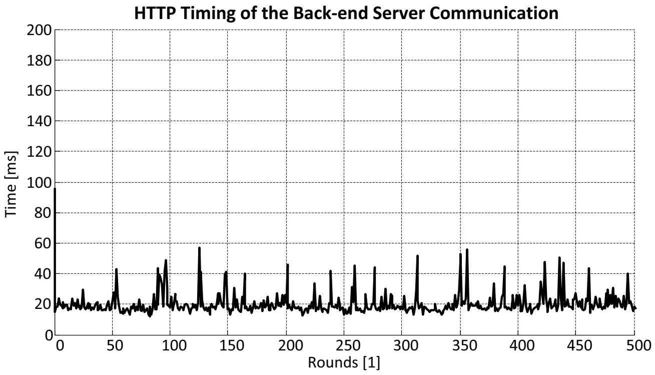


Fig. 7. This figure shows the timing behavior of an unencrypted HTTP connection between the reader device and the industrial back-end server during the process of a user's authentication check.

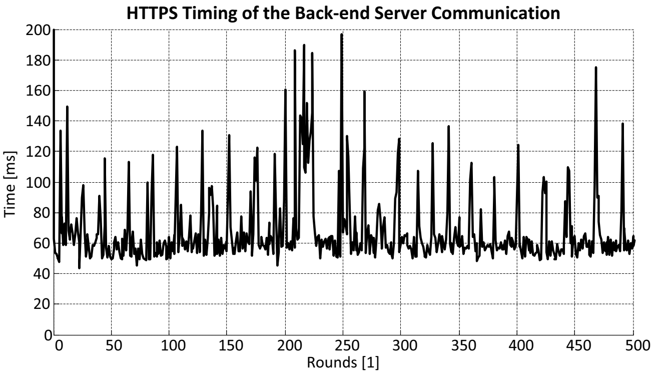


Fig. 8. This figure shows the timing behavior of an encrypted HTTP connection between the reader device and the industrial back-end server during the process of a user's authentication check.

intense authentication checks, the average benchmark's execution time t increases by only 5.2% compared to the previously carried out authentication request benchmark. Again, the non-deterministic timing spikes are caused by the Android operating system. However, these worst case execution time spikes are now approximately 35% higher. This behavior can be explained by the reader's and therefore Android's increased computation effort.

C. Comparison of the Authentication Benchmark Results

Table I gives a comparison of various evaluations of the one-way authentication protocol between reader and smart card. This table presents in addition to the previously presented average authentication request timing (24.9 ms) and the authentication protocol timing (26.2 ms) also the average timing result for reading out the smart card's ECC parameters. This timing value describes the time needed between sending the read request to the smart card and receiving the ECC parameters from the smart card. It is as high as 24.3 ms and involves only memory accesses of the smart card but no time-intense ECC calculations. If this timing result is compared with the authentication request benchmark result, it can be concluded that the smart card finishes the implemented Montgomery Reduction $Mont()$ very quickly*.

Another benchmark was carried out in order to deduce the estimated timing overhead caused by the Android operating system. For this purpose, a Windows 7 PC with external NFC-reader was employed to reproduce the authentication request benchmark. Again, the time between sending the request from the application and receiving the response was measured. An average required time of approximately 15 ms was measured. If this timing result is compared with the Android-based authentication request measurement, it can be concluded that the Android-based reader causes a timing overhead of approximately 10 ms.

TABLE I
READER / SMART CARD AUTHENTICATION PROTOCOL TIMING

Benchmark	Average Time [ms]
Authentication Request (Android 4.3)	24.9
Authentication Protocol (Android 4.3)	26.2
Reading ECC Parameters (Android 4.3)	24.3
Authentication Request (Windows 7)	15

These results outline that an Android-based reader device as well as the contactless NFC communication link (set to 106 kBit/s in the presented benchmarks) cause significant delays. If a time-critical application is given, engineers need to be aware of this performance degradation.

D. Back-end Server Communication

The following benchmark evaluates the timing behavior of an authentication check against a back-end server through a wireless communication channel. This benchmark represents the typical use-case of a brand's authentication check or a user's access control check. The benchmark is executed 500 times for both the unencrypted HTTP and the encrypted HTTPS approach over a WiFi channel. The HTTPS method uses ECDHE for key exchange, RSA for certificate signing, symmetric message authentication through 256-bit AES in CBC mode, and SHA1 for message authentication. While Fig. 7 illustrates the timing of the HTTP implementation, Fig. 8 shows the timing of the HTTPS implementation. The comparison of both techniques outlines the significant higher time requirements of the HTTPS technique. As shown in Table II, the average time requirement of the HTTPS method is as high as 66.3 ms, which is approximately 3.3 times higher than the timing of the unencrypted HTTP method. Timing spikes are caused in this benchmarks by several factors: Android operating system running on the smart phone, the complex wireless 3G/4G/Wifi channel, and a complex Windows 8 server architecture which runs a web service based on the

TABLE II
READER / BACK-END SERVER PROTOCOL TIMING OVER WIFI

Protocol	Average Time [ms]
HTTP	20.3
HTTPS	66.3

Windows Communication Foundation. According to Fig. 7 and Fig. 8, the worst case timing of the HTTPS method is approximately two times higher.

E. Conclusion of the Benchmark Results

The benchmark results demonstrate that the authenticity of a resource constrained embedded system, such as a smart card, can be verified efficiently if the whole authentication system is aware of the given constraints. Furthermore, we showed that a contactless smart card's authenticity can be checked against an industrial server back-end system through a secured wireless connection in approximately 90 ms on average. Thus, high authentication performance can be provided although a low NFC data transmission speed (106 kBit/s) and a standard Android-based smart phone were employed.

V. Conclusion

The RFID and NFC technologies can be found in important security-critical application fields, such as payment and access control. In these application fields, state-of-the-art approaches of Elliptic-Curve Cryptography typically employ specialized hardware accelerators that speed-up calculations and save power, but may introduce inflexibility. Yet, flexibility is a crucial factor in order to adapt quickly to changing demands of the markets.

This paper presents a flexible and lightweight ECC-based authentication solution that takes into account resource constrained systems. The employed authentication technique permits a shifting of computational intense ECC calculations from the resource constrained device to the computational powerful authentication terminal. At the same time, high performance and a maximum level of flexibility is maintained by employing a smart card security controller chip with a small multi-purpose hardware acceleration core. We showed the feasible implementation of the proposed technique in a contactless, resource constrained, and Android-based reader / smart card system. In addition, the reader device was connected to an industrial back-end server in a secured manner. We demonstrated that the authenticity of a contactless smart card can be verified against the back-end server within 90 ms on average. Furthermore, we showed that the one-way authentication protocol between reader and smart card can be processed within only 26 ms on average. Thus, a secured, flexible, and lightweight one-way authentication system is given that shows high performance and takes into account resource constrained devices.

Our future work concerns the fault attack-based evaluation of the implemented authentication solution. In addition, we are evaluating further system-level power optimization techniques in order to prolong the reader's battery lifetime and to reduce the smart card's power consumption.

Acknowledgments

We would like to thank the Austrian Federal Ministry for Transport, Innovation, and Technology, which funded the project META[:SEC:] under the FIT-IT contract 829586. Furthermore, we would like to thank our industrial partners Infineon Technologies Austria AG as well as Enso Detego GmbH for their support.

References

[1] R. Das. RFID 2014 to 2024: The Trends, Markets and Money. online. http://www.idtechex.com/, visited 2014-03-18.

[2] H. Bock, M. Braun, M. Dichtl, J. Heyszl, E. Hess, W. Kargl, H. Koroschetz, B. Meyer, and H. Seuschek, "A Milestone Towards RFID Products Offering Asymmetric Authentication Based on Elliptic Curve Cryptography," in *Workshop on RFID Security and Privacy (RFIDSec)*, July 2008.

[3] N. Druml, M. Menghin, D. Kroisleitner, C. Steger, R. Weiss, A. Krieg, H. Bock, and J. Haid, "Emulation-Based Fault Effect Analysis for Resource Constrained, Secure, and Dependable Systems," in *Euromicro Conference on Digital System Design (DSD)*, September 2013, pp. 337–344.

[4] A. Wander, N. Gura, H. Eberle, V. Gupta, and S. Shantz, "Energy analysis of public-key cryptography for wireless sensor networks," in *Third IEEE International Conference on Pervasive Computing and Communications (PerCom)*, March 2005, pp. 324–328.

[5] L. Batina, J. Guajardo, T. Kerins, N. Mentens, P. Tuyls, and I. Verbauwhede, "Public-Key Cryptography for RFID-Tags," in *Pervasive Computing and Communications Workshops, 2007. PerCom Workshops '07. Fifth Annual IEEE International Conference on*, March 2007, pp. 217–222.

[6] S. Ahamed, F. Rahman, and E. Hoque, "ERAP: ECC Based RFID Authentication Protocol," in *Future Trends of Distributed Computing Systems, 2008. FTDCS '08. 12th IEEE International Workshop on*, October 2008, pp. 219–225.

[7] G. Godor, N. Giczi, and S. Imre, "Elliptic curve cryptography based mutual authentication protocol for low computational capacity RFID systems - performance analysis by simulations," in *Wireless Communications, Networking and Information Security (WCNIS), 2010 IEEE International Conference on*, June 2010, pp. 650–657.

[8] B. Michael, H. Erwin, and M. Bernd, "Using Elliptic Curves on RFID Tags," *International Journal of Computer Science and Network Security*, vol. 8, no. 2, pp. 1–9, February 2008.

[9] E. Wenger and J. Grossschadl, "An 8-bit AVR-Based Elliptic Curve Cryptographic RISC Processor for the Internet of Things," in *45th Annual IEEE/ACM International Symposium on Microarchitecture Workshops (MICROW)*, December 2012, pp. 39–46.

[10] E. Wenger, T. Unterluggauer, and M. Werner, "8/16/32 Shades of Elliptic Curve Cryptography on Embedded Processors," in *Progress in Cryptology INDOCRYPT 2013*, ser. Lecture Notes in Computer Science. Springer International Publishing, 2013, vol. 8250, pp. 244–261.

[11] H. Alrimeih and D. Rakhmatov, "Fast and Flexible Hardware Support for ECC Over Multiple Standard Prime Fields," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, no. 99, pp. 1–14, 2014.

[12] Authors omitted for blinded review, "Title omitted for blinded review," in *51th ACM / EDAC / IEEE Design Automation Conference (DAC)*, June 2014, forthcoming.

[13] H. Aigner, H. Bock, M. Hütter, and J. Wolkerstorfer, "A Low-Cost ECC Coprocessor for Smartcards," in *Cryptographic Hardware and Embedded Systems (CHES)*, ser. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2004, vol. 3156, pp. 107–118.

[14] D. Hein, J. Wolkerstorfer, and N. Felber, "ECC Is Ready for RFID A Proof in Silicon," in *Selected Areas in Cryptography*, ser. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2009, vol. 5381, pp. 401–413.

[15] T. Plos, M. Hutter, M. Feldhofer, M. Stiglic, and F. Cavaliere, "Security-Enabled Near-Field Communication Tag With Flexible Architecture Supporting Asymmetric Cryptography," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 21, no. 11, pp. 1965–1974, November 2013.

[16] N. Druml, M. Menghin, C. Steger, H. Bock, and J. Haid, "A secure zero-energy NFC solution for everyday electronic devices," *e & i Elektrotechnik und Informationstechnik*, vol. 130, no. 7, pp. 224–229, November 2013.

[17] D. Hankerson, A. J. Menezes, and S. Vanstone, *Guide to Elliptic Curve Cryptography*. Springer Professional Computing, 2004.

[18] J. Guajardo, S. Kumar, C. Paar, and J. Pelzl, "Efficient Software-Implementation of Finite Fields with Applications to Cryptography," *Acta Applicandae Mathematica*, vol. 93, no. 1-3, pp. 3–32, 2006.

2012 IEEE 8th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)

NIZE - A Near Field Communication Interface Enabling Zero Energy Standby for Everyday Electronic Devices

Norbert Druml, Manuel Menghin, Rejhan Basagic,
Christian Steger and Reinhold Weiss
Institute for Technical Informatics
Graz University of Technology
Graz, Austria
{norbert.druml, manuel.menghin, steger, rweiss}@tugraz.at
rejhan.basagic@student.tugraz.at

Holger Bock and
Josef Haid
Design Center Graz
Infineon Technologies Austria AG
Graz, Austria
{holger.bock, josef.haid}@infineon.com

***Abstract*—Standby power consumption of electric devices is a growing waste of energy. Between 5% and 14% of the residential electrical power consumption is caused by devices being in standby mode. Depending on the device type, more than 50% of standby power consumption could be saved by applying state-of-the-art power management techniques. By implementing a zero energy standby design and outsourcing power consuming user interfaces, even more electrical power can be saved.**

Here we present a novel Near Field Communication (NFC) interfacing method for everyday electronic devices. By implementing this interface, the target device can be shut down during idle times. Thus, standby power consumption is eliminated completely. If user interaction is requested, NFC provides the electrical energy to switch on the target device's power supply and to start the device. Furthermore, any control, status, and maintenance information can be transmitted over NFC. By outsourcing high power dissipating and unoptimized user interfaces (touch screens, WiFi, etc.) to the power optimized NFC reader, further energy savings are possible also during running state.

This paper demonstrates the implementation and integration of this novel interfacing technique into common consumer electronics. Two implementation approaches are presented. A simple, energy harvesting-based approach illustrates the basic working principle. The second, more sophisticated approach, enables also authentication, encrypted data transfer, user interface outsourcing, configuration and control tasks, etc. A proof of concept is demonstrated by means of an access control terminal.

***Index Terms*—Zero Energy Standby, NFC, RFID**

I. Introduction

According to [1]–[3], between 5% and 14% of the residential electrical power consumption is caused by devices being in standby mode. More than 50% of this power waste could be saved by applying state-of-the-art power management techniques, as the authors highlight in [1]. McGarry outlines in [4] the environmental impact of this standby power waste. It was evaluated in the U.S. that the electrical energy wasted in this fashion corresponds to the emission of 27 millions tons of carbon dioxide for coal based electrical power plants. Governmental directives, like the 1 W plan or the Japanese standby proposal, mark important milestones for a global energy consumption reduction objective.

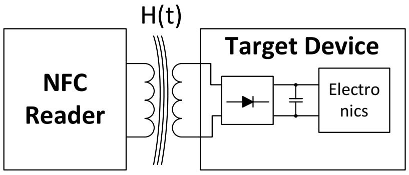


Fig. 1. Principle of a contactlessly and passively powered NFC system: The reader generates a magnetic field, which is used to power the target hardware and for communication purposes.

To design a device with ultra low or even suppressed standby power consumption, the Near Field Communication (NFC) technology can be used. Figure 1 illustrates the basic working principle of NFC systems. A reader device emits a magnetic field, which is used for communication purposes and to transmit electrical power to the target device. This approach enables the implementation of an innovative communication paradigm. Instead of waiting and polling for user activity within a power consuming standby state, the target device can be switched off completely. Only on demand, if the user wants to interact with the device, the target device is powered up by means of RF/NFC transmitted electrical power. Because of the high availability and propagation of NFC enhanced smart phones (e.g., Samsung's Nexus S) as well as the growing popularity of NFC and RFID-based applications, NFC is a suitable technology to be integrated into everyday electronic devices. Nowadays, NFC and RFID technologies can already be found in many application areas, e.g., ticketing [5], payment [6], logistic [7], system management [8], wireless sensor networks [9], [10]. However, the potential of NFC to design and implement zero energy standby devices has not been identified to its full extent so far.

We would like to thank the Austrian Federal Ministry for Transport, Innovation, and Technology, which funded the project META[:SEC:] under the FIT-IT contract 829586.

978-1-4673-1430-5/12/$31.00 ©2012 IEEE

This paper makes the following contributions:

- It introduces an innovative **N**ear field communication **I**nterface enabling **Z**ero **E**nergy standby (NIZE) for everyday electronic devices.
- It proposes a methodology of user interface outsourcing to improve a device's usability and to reduce a device's power consumption even more.
- Two implementation approaches, NIZE and Simple NIZE (SNIZE), as well as a proof of concept are presented. Standardized interfaces, protocols, and cheap electronic components are used to integrate and to operate NIZE.

II. Related Work

A lot of research has been conducted to reduce the standby power consumption of electronic devices. Approaches to reduce standby power consumption are feasible at any abstraction level. In [1], [4], [11], and [12], important power saving concepts are outlined, like power-gating, high voltage start-up, frequency reduction, etc. In [13], the authors decreased the standby power consumption of a flat TV by the factor of 800 down to 1.12 mW. They implemented an innovative power saving concept and maintained the TV's most important remote control capabilities at the same time. The authors of [14] presented a smart power unit dissipating only 300 nW during standby and 1.29 mW during active state. It features a wake-up radio allowing an activation of the actual target hardware on demand. Furthermore, this power unit features several energy harvesting units to charge the internal Li-Ion battery. In [15], a zero power remote control system is presented. 915 MHz-based RFID technology is used to transmit control information to the receiver. As a drawback, the transferred electrical energy does not suffice to control a power switch. A battery powered relay is proposed to solve this power switching issue. A similar 915 MHz-based RF wake-up approach, used in the field of wireless sensor networks, has been described by [16]. Another zero power standby system with an appropriate remote control has been proposed by the authors in [17]. Light should be used as energy transportation medium to power up and control the standby system. In [18], the authors developed a power socket featuring a photovoltaic array supplying the appliances. The appliances' electrical power supply is switched on / off by a sensor, which detects the user approaching. If the plug is switched on and enough luminance is given, standby power consumption of the whole system can be reduced to 0 W.

The outlined related work is admittedly trend-setting, it shows however one or more of the following three drawbacks: it is either complex in terms of used components (e.g., photovoltaic arrays), or represents only theoretical approaches, or lacks in energy provision for power switches.

III. Simple NIZE (SNIZE)

The system architecture of SNIZE is depicted in Figure 2. It consists of a NFC enhanced reader device (e.g., a NFC enabled smart phone like Samsung's Nexus S) and the target device. The target device itself consists of the energy harvesting analog front end and power supply control circuitry as well as the Rest of the Target Device (RoTD). The RoTD represents the actual appliance the user wants to interact with, e.g., payment station, access control terminal, microwave oven, washing machine. If the user wants to start the RoTD, then the reader emits a magnetic field $H(t)$ according to the NFC standard. This magnetic field is used to transfer electrical power to the target device by inducing a varying electrical voltage in the target device's antenna coil. The transferred electrical power is forwarded by the target device's analog front end to a power supply control unit. After enough electrical energy was transferred from the reader to the smart card, this power supply control unit is able to switch on the target device's power supply. From this moment on, the target device uses its own power supply and does not rely any more on RF-transmitted electrical power. Now, the RoTD is able to perform its designated tasks. If the RoTD finished all tasks, it signals the power supply control unit to break the connection to the power supply. Thus, no electrical power can be wasted during idle times. Because the SNIZE-based target device features only a RF-based energy harvesting architecture, it is impossible to exchange data between reader and RoTD.

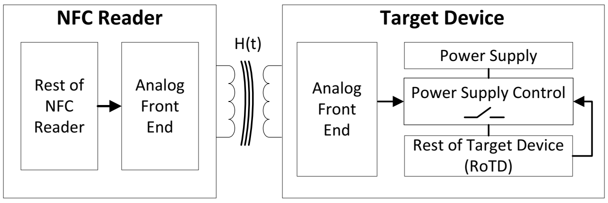


Fig. 2. Architecture of the proposed SNIZE interface. If the user wants to start the target device, the NFC compliant reader (e.g., NFC enhanced smart phone) emits a magnetic field. The transferred electrical power is used in the target device to switch on its own power supply. During idle times, the power supply is switched off by the target device itself. No electrical power is wasted.

Figure 3 illustrates the target device's internal state transitions. During idle state the RoTD is not supplied. If the user wants to start the RoTD (i.e., running state), the target device's power supply control unit uses the reader emitted RF-power to switch on the target device's power supply. After the RoTD finished the processing of its tasks, it changes back to idle state by switching off its power supply.

A. Analog Front End

The target device's analog front end is depicted in Figure 4. A varying magnetic field $H(t)$, which is emitted by the reader device and is fulfilling the requirements of the RFID / NFC standard, induces a varying electrical voltage within the antenna circuit. After rectification, the electrical charges are buffered within the capacitor C. A Zener diode limits the supplied voltage and prevents the adjacent electronics from electrical surges. The resulting supply voltage $v(t)$ is forwarded to the power supply control unit. The value of $v(t)$ is set by the charge level $Q_C(t)$ of the capacitor C. In turn, $Q_C(t)$ will be increased by the induced voltage from the

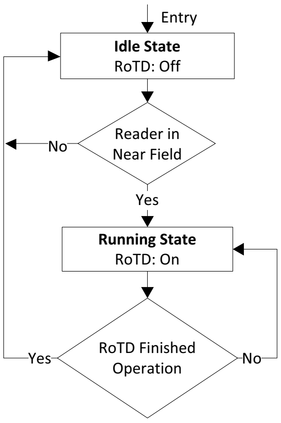


Fig. 3. State transitions of the SNIZE target device. During idle state no power is dissipated. The transition to running state is performed by supplying a magnetic field. Transition back to idle state is performed if the RoTD's task is finished.

magnetic field and $Q_C(t)$ will be decreased when the adjacent electronics consumes power.

B. Power Supply Control

This unit represents a small electrical circuit that controls the target device's power supply. Figure 5 illustrates the simplified architecture. A control logic decides when to activate or deactivate the switch S, which connects the RoTD with the power supply. Figure 6 depicts the control flow of the integrated logic. Applying a magnetic field results in the supply voltage $v(t)$. If $v(t)$ reaches a certain threshold (a charge pump can be optionally used for higher voltage requirements), switch S is closed. As a consequence, the RoTD is supplied and is switched on. The RoTD stays connected to the power supply until it signals the control logic that it finished its designated tasks and entered the idle state. Thus, no power can be dissipated during idle state.

C. Rest of Target Device (RoTD)

The RoTD represents the actual appliance the user wants to interact with, e.g., access control terminal, payment station, microwave oven.

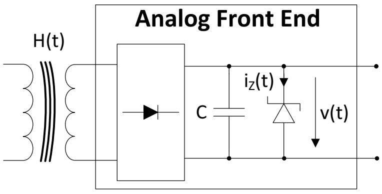


Fig. 4. Simplified schematic of the target device's analog front end unit. The induced electrical voltage is rectified. Afterwards the electrical charges are buffered within the capacitor C. A Zener diode prevents the adjacent electronics from electrical surges.

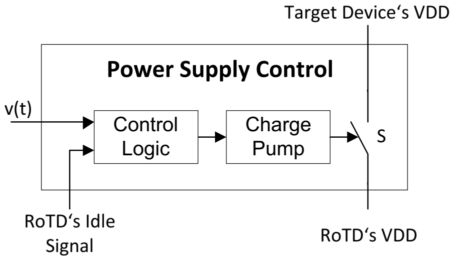


Fig. 5. Simplified architecture of the power supply control unit. The control unit decides based on its both inputs whether the switch S should be closed or opened. A charge pump can be optionally used for higher voltage requirements.

D. Feasible Use Cases

SNIZE can be feasibly integrated into appliances that wait or poll for user activity in a power consuming standby state. A SNIZE enhanced appliance stays unpowered during idle times and is activated on demand by the reader device. No data communication between reader / appliance takes place, which keeps the SNIZE integration effort low. Example use cases are monitors, charging devices, access controls, cooking and microwave ovens, door openers, etc.

IV. NIZE

NIZE represents a more sophisticated implementation of the presented interface methodology, thus enabling an electronic device to dissipate zero energy during standby. NIZE's basic system architecture is depicted in Figure 7. It consists of a NFC enabled reader and the target device. The reader device features a software stack for communication, service provision, and GUI related tasks. The target device itself consists of interfacing chips, a RF energy harvesting analog front end,

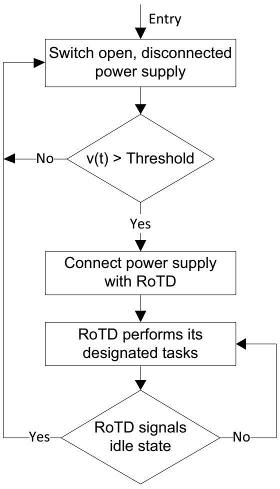

Entry
Switch open, disconnected power supply
v(t) > Threshold
No
Yes
Connect power supply with RoTD
RoTD performs its designated tasks
RoTD signals idle state
Yes
No

Fig. 6. Flow chart of the power supply control unit. If $v(t)$ reaches a specific threshold, switch S is closed and RoTD is powered. After RoTD finished all tasks and entered idle state, it signals the control unit to open switch S. Thus, no power can be dissipated during idle times.

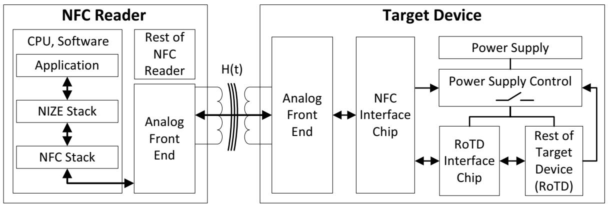


Fig. 7. Architecture of the proposed NIZE method. The reader emits a magnetic field which powers the target device's NFC interface chip. The NFC interface chip forwards electrical energy to the power supply control unit to switches on the target device's power supply. Then the RoTD is able to communicate with the reader device and performs its designated tasks.

a power supply control unit, and the RoTD which represents the actual appliance the user wants to interact with. In the following section every system component will be described in detail.

A. NFC Reader

Figure 7 illustrates the reader's architecture by means of a NFC enabled smart phone. No reader-based hardware modifications are needed at all to support NIZE-based communication with the target device. Upon the NFC software stack, a NIZE stack is implemented. It handles all NIZE specific tasks like:

- Basic target device handling within the near field, e.g., detection, termination, magnetic field strength modifications.
- Support of a hardware abstraction in form of a generic command language for common devices.
- Determining target device specific services and providing them to the application and the user, e.g., communication, graphical user interface specifications, authentication, encryption, event handling, monitoring, control.

The application is responsible to present to the user, in an appropriate way, all the services provided by the target device. Examples of such service can be drawing the graphical user interface or handling RoTD event notifications. Furthermore, any user input data is transmitted by the NIZE and NFC stacks to the target device.

B. Target Device

The architecture of the target device is illustrated in Figure 7. It consists of a RF energy harvesting analog front end, NFC- and RoTD interface chips, power supply control unit, as well as the RoTD that represents the actual appliance the user wants to interact with. Figure 8 depicts the target device's internal state transitions. Initially, the target device is in idle state, i.e., all target device components are switched off and no standby power can be dissipated. If the user wants to interact with the RoTD, the reader application activates the magnetic field. Electrical power is transferred to the target device. As a consequence, the target device's NFC interface chip is powered contactlessly and communication between reader and NFC interface chip starts. During this initial communication phase basic identification and authentication checks are performed. If this procedure succeeded, electrical power is forwarded to the power supply control unit, which switches on the target device's power supply. Now, the target device is in a running state and the RoTD performs its designated tasks. If the NFC reader leaves the target device's near field and the RoTD finished all tasks, the RoTD signals the power supply control unit to disconnect the target device's supply. As a consequence, the target device returns to idle state and no standby power is dissipated.

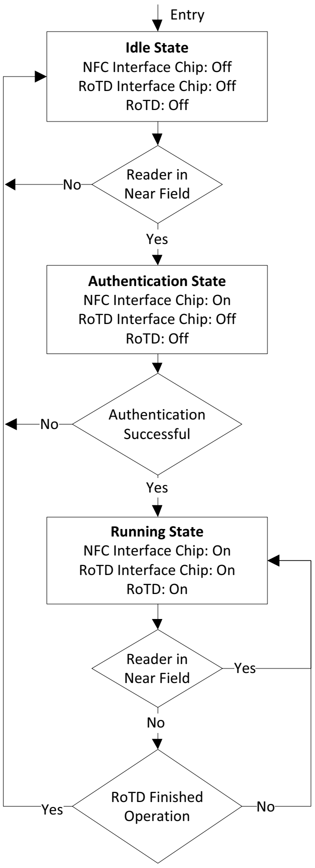


Fig. 8. State transitions of the NIZE enhanced target device. During idle state no power is dissipated. The transition to running state is performed by supplying a magnetic field and conducting the authentication successfully. Transition back to idle state is performed if the reader device leaves the near field and the RoTD's tasks are finished.

C. Target Device - NFC Interface Chip

The NFC interface chip implements the interconnection between reader device and target device's RoTD interface chip. An ultra low power smart card-based security chip is used as NFC interface chip. Figure 9 depicts the basic architecture of this interface chip. It is powered contactlessly and passively by the reader's emitted magnetic field. Data transfer to the reader is done by means of load modulation. During target device's idle state, when the user is not interacting with the RoTD, this

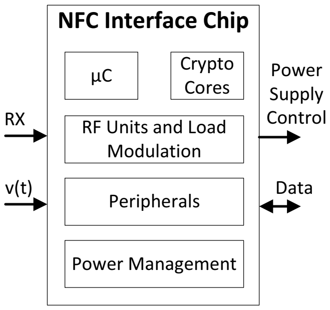


Fig. 9. Architecture of the ultra low power smart-card based security chip, which is used as NFC interface chip. Load modulation is used to transmit data to the NFC reader.

NFC interface chip does not dissipate any electrical standby power. Thus, a zero energy communication interface is given. If the reader device starts interacting with the NFC interface chip and the initial identification / authentication procedure succeeded, available electrical power from the magnetic field is forwarded to the target device's power supply control unit. The power supply control unit then connects the RoTD with the target device's power supply. During the target device's running state any received data is forwarded transparently to the RoTD interface chip. Optionally, any data transfer can be encrypted / decrypted, thanks to the integrated cryptographic cores.

D. Target Device - RoTD Interface Chip

Because the NFC interface chip is designed for a very limited RF-based power budget, its peripheral and computational resources are very limited. Therefore, a RoTD interface chip is used, which is powered by the target device's supply. This interface chip implements all RoTD specific tasks:

- Hardware abstraction between NIZE interface and RoTD hardware by supporting a generic command language for common devices.
- Storing RoTD specific data, e.g., graphical user interface specifications.
- Basic RoTD communication using SPI, I^2C, UART, GPIO interfaces, etc.
- Configuring the RoTD with user supplied data.
- Monitoring and controlling the RoTD's functionality.
- Forwarding relevant event and status information to the NFC reader.

E. Hardware Abstraction / Generic Command Language Concept

An essential concept of the NIZE interface is the hardware abstraction by supporting a generic command language. This approach makes the NFC interface chip and the NIZE software stack independent from the actually interfaced RoTD hardware. To integrate NIZE into a new RoTD hardware, only a few hardware dependent components within the reader's application and the RoTD interface chip's firmware need to be adopted.

F. User Interface Outsourcing Concept

There is an ongoing trend to integrate LCD-, touchscreen-, WiFi-based user interfaces in any suitable electronic device. To keep an appliance's bill of materials as low as possible, these user interface solutions are often implemented halfheartedly, difficult to use, or power dissipative. NIZE encourages the removal of a RoTD's dispensable user interface. Instead, the user interface is moved to reader side. This approach grants the following benefits:

- Electrical power consumption can be reduced by removing RoTD's power dissipative user interface and displaying it on the power optimized reader device. If practical, high power consuming wireless communication interfaces like WiFi can be replaced by NFC too.
- A smart phone featuring NFC used as reader device improves the display quality of the user interface (e.g., colorful and high resolution displays, modern user input controls). Thus, an appliance's usability is increased.
- Bill of materials decreases by removing RoTD's user interface hardware components.

This user interface outsourcing concept is implemented by taking advantage of the generic command language. A specification of the RoTD's GUI layout and functionality can be saved within the RoTD interface chip. After the initial identification and authentication procedure, this GUI specification is transmitted to the reader. The reader's application interprets this specification data and paints it accordingly.

V. NIZE Proof of Concept

NIZE can be practically integrated into appliances that wait / poll for user activity (e.g., access control terminal, sensor systems, payment terminals) or into appliances featuring a push-to-wakeup concept (e.g., monitors, charging devices, microwave and cooking ovens, washing machines, logistic applications). Instead of letting the appliance wait or poll for user activity in a power consuming standby state, the NFC enabled reader powers up the device only on demand. Applying this approach results in a zero energy standby appliance. In the presented proof of concept, we enhance a contactless card-based access control terminal with NIZE. Table I illustrates the hardware configuration used for this proof of concept.

Figure 10 illustrates the use case's control flow. The encrypted access card authentication information is saved on the smart phone. Initially, the access control terminal (RoTD) is switched off (idle state) and no standby power is dissipated. The user activates the smart phone's NFC functionality and moves the smart phone to the NIZE enhanced access control terminal (target device). The emitted magnetic field powers

TABLE I
Proof of Concept Hardware Configuration

Schematic	Used Hardware
NFC Reader	Samsung Nexus S
NFC Interface chip	Infineon Prototype Chip (undisclosed)
RoTD Interface chip	TI MSP430G2553IN20

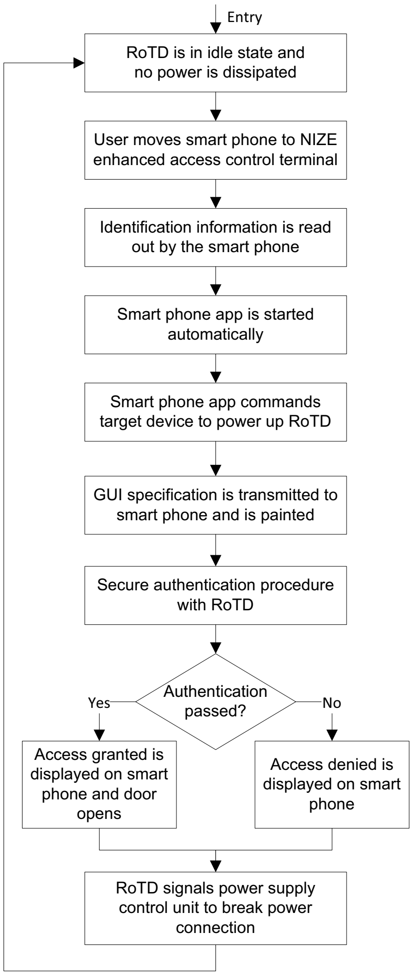

Entry
RoTD is in idle state and no power is dissipated
User moves smart phone to NIZE enhanced access control terminal
Identification information is read out by the smart phone
Smart phone app is started automatically
Smart phone app commands target device to power up RoTD
GUI specification is transmitted to smart phone and is painted
Secure authentication procedure with RoTD
Authentication passed?
Yes
No
Access granted is displayed on smart phone and door opens
Access denied is displayed on smart phone
RoTD signals power supply control unit to break power connection

Fig. 10. Flow chart of the NIZE enhanced access control terminal.

up the target device's NFC interface chip. Then the smart phone starts the NFC communication and reads out basic identification information. Based on this information, the smart phone starts automatically the according NIZE application. The NIZE application tells the target device's NFC interface chip to activate the power switch to power up the RoTD, the access control terminal. User interface specification data is transmitted from the target device to the smart phone application, which paints a graphical user interface accordingly. Then, the secure authentication procedure between smart phone and access control terminal starts. If the authentication succeeded, the access control terminal opens the door. Furthermore, an appropriate message is displayed on the smart phone (e.g., access granted, access denied). After the door closed, the RoTD returns to the zero energy idle state by disconnecting its power supply.

Figure 12 depicts the NIZE prototype assembly. The NFC reader, in form of a smart phone, displays the message box 'Access Granted', after the user authentication was conducted successfully. Figure 11 outlines the standby power savings achieved with the NIZE enhanced access control terminal. The original terminal's card reader hardware solely consumed on average 0.49 W if magnetic field and a card detection polling duty cycle of 10% were activated. In contrast, the NIZE enhanced access control terminal elimates standby power consumption.

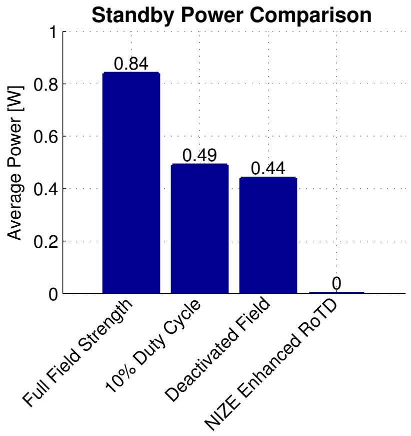


Fig. 11. The original access terminal's RF interface consumed at least 0.44 W during standby. The NIZE enhanced version eliminates standby power consumption.

VI. Conclusion

Standby power consumption of electronic devices is a waste of energy that needs to be reduced. A major milestone of this objective was the introduction of several governmental standby power guidances, such as the 1 W plan, Japanese standby proposal, etc.

This paper presents the innovative interfacing concept NIZE for everyday electronic devices enabling zero energy standby. It uses the NFC technology and is especially suitable for appliances that wait / poll for user activity (e.g., access control terminal, sensor systems, payment terminals) or for appliances featuring a push-to-wakeup concept (e.g., monitors, charging devices, microwave and cooking ovens, washing machines, logistic applications). NIZE also features user interface outsourcing to the NFC-based reader device (e.g., smart phone) to improve the appliance's usability and to reduce its power consumption also during running state. Authentication, encrypted data transfers, configuring, monitoring, and control are some further features to note. We exemplified the feasible integration of NIZE by means of an access control terminal and eliminated its standby power consumption.

Acknowledgments

We would like to thank our industrial partners Infineon Technologies Austria AG as well as Enso Detego GmbH for their support.

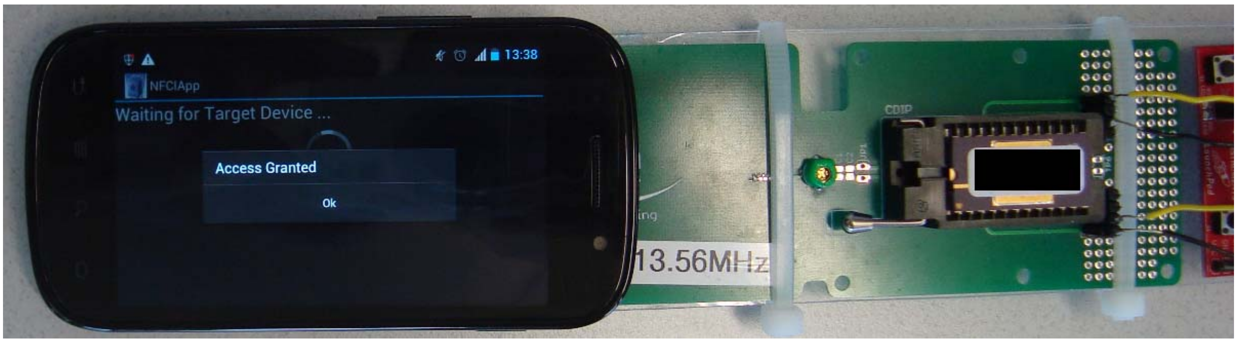


Fig. 12. This picture shows the NIZE prototype assembly. The NFC reader (Samsung's Nexus S) is put upon the target device's antenna circuit. It powers the target device's NFC interface chip and communicates with the access control terminal (RoTD).

REFERENCES

[1] A. Chakraborty and A. Pfaelzer, "An overview of standby power management in electrical and electronic power devices and appliances to improve the overall energy efficiency in creating a green world," in *Journal of Renewable and Sustainable Energy*, vol. 3, 2011.

[2] K. Clement, I. Pardon, and J. Driesen, "Standby Power Consumption in Belgium," in *International Conference on Electrical Power Quality and Utilisation*, 2007.

[3] A. Meier, "A worldwide review of standby power use in homes," *Lawrence Berkeley National Laboratory*, 2001.

[4] L. Mcgarry, "The Standby Power Challenge," in *International IEEE Conference on the Asian Green Electronics (AGEC)*, 2004.

[5] R. Widmann, S. Grunberger, B. Stadlmann, and J. Langer, "System Integration of NFC Ticketing into an Existing Public Transport Infrastructure," in *International Workshop on Near Field Communication (NFC)*, 2012.

[6] I. Lacmanovic, B. Radulovic, and D. Lacmanovic, "Contactless payment systems based on RFID technology," in *International Convention on Information and Communication Technology, Electronics and Microelectronics*, 2010.

[7] T. Jinrong and C. Haiquan, "Manufacturing logistics management Using RFID: Dynamic and case study," in *International Conference on Computer Application and System Modeling*, 2010.

[8] F. Kamoun, "RFID system management: state-of-the art and open research issues," *IEEE Transactions on Network and Service Management*, vol. 6, no. 3, 2009.

[9] E. Stroemmer, M. Hillukkala, and A. Ylisaukko-oja, "Ultra-low Power Sensors with Near Field Communication for Mobile Applications," in *Wireless Sensor and Actor Networks*, ser. IFIP International Federation for Information Processing. Springer Boston, 2007, vol. 248.

[10] D. Brenk, J. Essel, J. Heidrich, and R. Weigel, "Ultra low-power techniques for sensor-enhanced RFID tags," in *International Microwave Workshop on Wireless Sensing, Local Positioning, and RFID*, 2009.

[11] V. Tiwari, R. Donnelly, S. Malik, and R. Gonaalea, "Dynamic Power Management for Microprocessors: A Case Study," in *International Conference on VLSI Design*, 1997.

[12] B. Calhoun, D. Daly, N. Verma, D. Finchelstein, D. Wentzloff, A. Wang, S.-H. Cho, and A. Chandrakasan, "Design considerations for ultra-low energy wireless microsensor nodes," *IEEE Transactions on Computers*, vol. 54, no. 6, 2005.

[13] C. Deppe and G. Sauerlander, "Realizing standby operation of a television with zero energy consumption: Options and issues of the ultimate energy saving standby mode on the example of a recent flat TV model," in *European Conference on Power Electronics and Applications*, 2009.

[14] M. Magno, S. Marinkovic, D. Brunelli, E. Popovici, B. O'Flynn, and L. Benini, "Smart Power Unit with Ultra Low Power Radio Trigger Capabilities for Wireless Sensor Networks," in *Design, Automation and Test in Europe Conference and Exhibition*, 2012.

[15] L. Chen, Z. Wang, C. Jia, F. Li, W. Hao, B. Xiao, C. Zhang, and Z. Wang, "A RF Remote-Control Transceiver with Zero-Standby Power Based on RFID Technology," in *Asia Pacific Conference on Postgraduate Research in Microelectronics and Electronics*, 2010.

[16] P. Kolinko and L. Larson, "Passive RF Receiver Design for Wireless Sensor Networks," in *International Microwave Symposium*, 2007.

[17] S. Siwamogsatham, P. Rattanawan, M. Kitjaroen, P. Songtung, P. Pongpaibool, and K. Navanugraha, "Smartly saving energy with a zero power consumption standby system," in *Technology Management in the Energy Smart World (PICMET)*, 2011.

[18] C.-H. Tsai, Y.-W. Bai, C.-A. Chu, C.-Y. Chung, and M.-B. Lin, "Design and implementation of a socket with zero standby power using a photovoltaic array," in *IEEE Transactions on Consumer Electronics*, vol. 56, no. 4, 2010.

ORIGINALARBEITEN

Elektrotechnik & Informationstechnik (2013) 130/7: 224–229. DOI 10.1007/s00502-013-0153-1

A secure zero-energy NFC solution for everyday electronic devices

N. Druml, M. Menghin, C. Steger OVE, IEEE, H. Bock, J. Haid

Standby power consumption of electric devices is a major issue. It accounts for 5 % to 14 % of the total residential power consumption. However, applying state-of-the-art power management techniques can reduce this waste of energy drastically.

In this paper we present an innovative and secure Near Field Communication (NFC) Interface technique for everyday electronic devices. By integrating this field-powered and secure communication interface, a target device can be switched off during standby. If user interaction is requested, NFC provides the electrical energy to switch on the target device's power supply and to start the device. Thus, standby power consumption of an NFC enhanced device is eliminated completely. Besides standby power management, our interface features cryptography, innovative hardware abstraction and user interface concepts, and it enables configuration, monitor, and control tasks of the target device.

Keywords: zero-energy standby; secure wireless interface; RFID; NFC

Eine sichere Null-Energie-NFC-Lösung für elektronische Geräte.

Der Standby-Leistungsverbrauch elektronischer Geräte markiert ein stetig wachsendes Problem. Dieser beträgt zwischen 5 % und 14 % des gesamten häuslichen Leistungsverbrauchs. Durch Implementierung und Anwendung von Power Management-Techniken ist es jedoch möglich, diese Energieverschwendung fast zur Gänze zu beseitigen.

In dieser Arbeit präsentieren wir eine auf Near Field Communication (NFC) basierende sichere Schnittstellentechnik, die in jeglichen elektronischen Geräten integrierbar ist. Dank dieser Funkschnittstelle kann ein Gerät während der Standby-Zeit komplett abgeschaltet werden. Falls ein Benutzer mit dem Gerät interagieren möchte, wird die von NFC bereitgestellte elektrische Energie verwendet, um das Gerät wieder einzuschalten. Somit kann der Standby-Leistungsverbrauch eines Gerätes unterdrückt werden. Neben Power Management, unterstützt die Schnittstelle Kryptographie, als auch innovative Hardwareabstraktions- und Userinterfacekonzepte. Ferner bietet die Schnittstelle Funktionen zur Konfiguration, Beobachtung und Steuerung eines elektronischen Gerätes an.

Schlüsselwörter: Null-Energie-Standby; verschlüsselte Funkschnittstelle; RFID; NFC

Received July 30, 2013, accepted September 20, 2013, published online November 6, 2013

1. Introduction

According to recent analyses, between 5 % and 14 % of the residential electrical power consumption is caused by devices being in standby mode [2]. In 2004, McGarry outlined that the standby power consumption waste of the US corresponds to the emission of 27 million tons of carbon dioxide for coal-based electrical power plants. More than 50 % of this power consumption waste could be saved by applying state-of-the-art power management techniques [5]. Furthermore, directives, like IEA's One-Watt Initiative or the Japanese standby proposal, mark important milestones for a global energy consumption reduction objective.

To achieve an ultra-low power or even zero-energy standby approach, the Near Field Communication (NFC) technology can be used. A typical NFC system consists of a reader device (e.g., smart phone, tablet) and a transponder. The reader emits a magnetic field, which is used to power the transponder and to communicate with it by means of inductive coupling. This approach can be used to facilitate an innovative communication and power saving paradigm: a target device (e.g., access control terminal, payment terminal) does not wait or poll for user activity anymore, instead it is switched off completely. Only on demand when the user wants to interact with the target device, it is powered up with electrical power provided by NFC. Thanks to the high availability of NFC enhanced smart phones and very cheap transponder chips, NFC is a suitable technology to be integrated into everyday electronic devices.

This paper makes the following contributions:

- It introduces a secure and trustworthy NFC Interface technique, which is based on Druml et al. [3], for everyday electronic devices enabling the zero-energy paradigm.
- It demonstrates the usage of innovative concepts like user interface outsourcing and hardware description languages in the field of everyday electronic devices.
- It exemplifies the feasible integration of the NFC Interface by means of an industrial smart meter case-study.

Druml, Norbert, Institute for Technical Informatics, Graz University of Technology, Inffeldgasse 16, 8010 Graz, Austria (E-mail: Norbert.druml@tugraz.at); **Menghin, Manuel,** Institute for Technical Informatics, Graz University of Technology, Inffeldgasse 16, 8010 Graz, Austria (E-mail: manuel.menghin@tugraz.at); **Steger, Christian,** Institute for Technical Informatics, Graz University of Technology, Inffeldgasse 16, 8010 Graz, Austria (E-mail: steger@tugraz.at); **Bock, Holger,** Design Center Graz, Infineon Technologies Austria AG, Babenbergerstraße 10, 8010 Graz, Austria (E-mail: holger.bock@infineon.com); **Haid, Josef,** Design Center Graz, Infineon Technologies Austria AG, Babenbergerstraße 10, 8010 Graz, Austria (E-mail: josef.haid@infineon.com)

1.1 Related work

Standby power consumption reduction of electronic devices is a major research field. Power saving techniques (e.g., power-gating, high voltage start-up, frequency reduction) have been outlined by various authors [2, 7]. A zero-energy standby approach can be achieved, e.g., by harvesting RF supplied energy and forwarding it to a power switch to activated the target appliance. NFC can be used to harvest adequate amounts of power for controlling power switches and for powering additional security related circuitry, as demonstrated, e.g., by the authors of [3]. Magno et al. presented a smart ultra-low power plug unit dissipating only 300 nW during standby and 1.29 mW during active state [4]. A wake-up radio is featured to activate the actual target hardware on demand. In addition, energy harvesting units are used to charge an internal Li-Ion battery. A power socket was presented by Cheng-Hung Tsai et al., which features a photovoltaic array to supply the appliances. The electrical power supply of the appliances is switched on/off by a sensor which detects the user approaching. If enough luminance is given and the plug is switched on, the standby power consumption of the whole system can be reduced to 0 W [8]. A zero-energy standby approach was presented by Siwamogsatham et al. [6]. They proposed light as an energy transfer medium to control power switches. As a drawback, the limited amount of transferred electrical power can be noted. NFC Tag chips have been shipped recently, which feature field detection functionality for adjacent electronics. An output pin is used to signal if a magnetic field is present or not. An electronic device can use this pin, e.g., as an interrupt source to be woken out of its standby state. This functionality of waking up hardware from standby if a magnetic field is sensed was demonstrated, e.g., by means of a wireless charging prototype. Thus, the standby power consumption was eliminated.

Summarizing, several ultra-low power or even zero-power standby solutions were presented in the past. However, the following drawbacks for everyday electronic devices can be identified: proprietary and complex components are used (e.g., photovoltaic arrays) or energy provision is lacking for a feasible power switch control. Furthermore, security concerns are supported only to some extent or are neglected completely, which limits an industrial application of such approaches.

2. Secure zero-energy NFC Interface solution

The architecture of an NFC Interface enhanced system is depicted by Fig. 1. It consists of an NFC reader (e.g., NFC-enabled smart phone or tablet) and a target device. The reader consists of the NFC Interface software stack as well as the NFC chip and its analog frontend. The target device comprises an analog frontend, a passively powered NFC Interface chip, power supply and dedicated control unit, the rest of the target device (RoTD) and its optional interface chip. The RoTD represents the actual appliance the user wants to interact with (e.g., access control terminal, payment terminal). The basic conceptual idea of the presented interface solution is as follows: during standby, the appliance is disconnected from its power supply. Only on demand, if the user wants to interact with the RoTD, electrical power is transferred from the reader to the target device to switch on its power supply. After the RoTD finished its designated tasks, it goes back into standby and its power supply is switched off. Therefore, no electrical power can be wasted during standby. Besides standby power management, the presented interface solution is used for monitoring, control, configuration, authentication, secure data transfer, etc. In the following, each component, the realized conceptual ideas, and a typical flow of operation are described in detail.

2.1 NFC reader

As reader device, any commercially available NFC-enabled device can be used, e.g., Android-based NFC-enabled smart phones or tablets. No hardware modifications are required at all to communicate with an NFC Interface enhanced target device. The only extension needed is the NFC Interface specific software stack, which is built upon Android's NFC stack. This NFC Interface software stack provides several services to the application layer:

- It provides functionalities to handle the target device within the near field, e.g., device detection, setup and termination of the communication, data transfer, event handling, or adaptation of the magnetic field strength to save electrical energy.
- It offers cryptographic functionalities for secure data transfer and elliptic curve-based (ECC) signature and key exchange algorithms. In addition, it features a performance-optimized and power-optimized authentication protocol, which is based on the work of Bock et al. [1]. Depending on the chosen security strength, elliptic curve algorithms can be computed within a three-digit milliseconds time period.
- It supports an XML-based hardware description language. With the help of this hardware description language, a target device can define its provided functionalities and graphical user interface specifications. This specification is then interpreted to access the

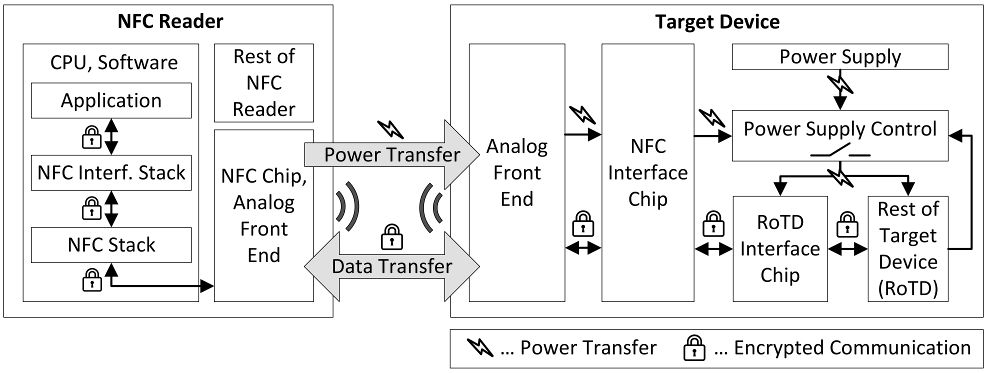


Fig. 1. Architecture of the secure zero-energy NFC Interface solution for everyday electronic devices. Obtained with changes from Druml et al. [3]

target device's functionalities and to paint the graphical user interface accordingly.

The application is built upon the NFC Interface stack. It is responsible to present to the user all services and functionalities, which are provided by the target device and which are defined by its hardware description. In addition, any user input data is forwarded to the NFC Interface stack to be transmitted to the target device.

2.2 Target device – analog frontend

The target device's analog frontend consists of an NFC compliant antenna circuitry. A varying magnetic field, which is emitted by the reader, induces a varying electrical voltage within the antenna. Thus, electrical power is transferred contactlessly from the reader to the target device. After a voltage rectification, electrical energy is buffered by a capacitor. A shunt resistor prevents the adjacent electronics from power surges and reduces security-related side channel footprints. The transferred electrical power is used to operate the NFC Interface chip and to control the power supply control unit. Data is exchanged between the reader and the target device by means of amplitude shift keying and load modulation.

2.3 Target device – NFC Interface chip

The NFC Interface chip provides the NFC-based interconnection between reader device and target device. For this purpose, an ultra-low power security controller is used, which features hardware accelerated state-of-the-art cryptography (e.g., elliptic curve cryptography, advanced encryption standard). Since the NFC Interface chip is powered contactlessly and passively by the magnetic field, it does not dissipate any electrical power of the target device and is switched off during idle times when no magnetic field is present. Thus, a zero-energy communication interface is given. When the reader starts interacting with the NFC Interface chip and the initial authentication procedure succeeds, the chip forwards electrical power from the magnetic field to the target device's power supply control unit. The power supply control unit then connects the RoTD with its power supply. During running state, the NFC Interface chip forwards the received data transparently to the RoTD and its optional RoTD interface chip via a serial communication interface (e.g., GPIO, UART, I^2C).

Implementing cryptography algorithms feasibly in hardware and software requires additional resources and, as a consequence, also additional electrical energy. Performance approximations can be given of the NFC Interface chip. Depending on the chosen security strength, elliptic curve Diffie-Hellman (ECDH) and elliptic curve digital signature algorithm (ECDSA) are computed within high two-digit milliseconds and low three-digit milliseconds time period ranges by the NFC Interface chip. The featured computational-optimized ECC-based authentication protocol can be handled even faster because it shifts parts of the computational complexity from the target device to the reader, as outlined in [1].

2.4 Target device – power supply control

If a magnetic field is supplied to the target device and the initial authentication succeeds, then the NFC Interface chip forwards electrical energy to the power supply control unit with the help of an activate signal. Figure 2 depicts the power supply control unit's simplified architecture. This unit implements a small electrical circuitry that controls the target device's power supply based on the NFC Interface chip's activate signal and the RoTD's idle signal. If activate goes high, switch *S* is closed and the RoTD is connected to its power supply. The RoTD stays connected to its power supply until it signals the control unit that it finished its operation and entered the idle state. Therefore, no electrical power is dissipated by the RoTD during idle state.

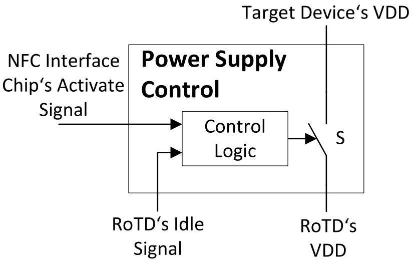


Fig. 2. Power supply control unit, obtained with changes from Druml et al. [3]

2.5 Target device – rest of target device (RoTD)

The RoTD represents the actual appliance/device the user wants to interact with. Appliances that can be feasibly enhanced with our secure NFC Interface solution

- wait or poll for user activity (e.g., payment terminals, access control terminals, door opening systems, electronic devices with remote control interfaces),
- feature a push-to-wakeup concept (e.g., charging device, monitors, microwave and cooking ovens, logistic applications), or
- shall support a zero-energy/passively powered communication interface for tasks like monitoring, control, configuration, etc. (e.g., passively powered sensor systems, smart meters).

2.6 Target device – RoTD Interface chip

The NFC Interface chip is designed to operate during a very limited RF-based power supply. As a consequence, its peripheral and computational resources are limited as well. If the chip's provided resources do not suffice, an optional RoTD Interface chip can be used. This interface chip is powered actively by the target device and is therefore not constrained in terms of power supply and computational resources. For example, tasks of an RoTD Interface chip can be:

- Support for more sophisticated and high speed communication interfaces (e.g., USB, Ethernet).
- Control of the RoTD's functionalities.
- Monitoring of the RoTD's integrity.
- Extending the target device's cryptographic features.
- Extending the features of the hardware description and hardware abstraction technique.

2.7 Flow of operation

A typical NFC Interface's flow of operation is presented by Fig. 3. Initially the target device is in idle state, RoTD and interface chips are switched off, and the reader's magnetic field is deactivated. The target device does not dissipate any standby power. If the user wants to interact with the target device, the reader activates its magnetic field and electrical power is transferred to the target device. Now, the NFC Interface chip is powered passively, the target device's hardware description is submitted to the reader, and the target device enters the authentication state. If the authentication succeeds, the power supply control unit switches on the target device's power supply. Now, the target device is in running state and the RoTD performs its designated tasks. If the NFC reader leaves the target device's near field and the RoTD finished all of its tasks, the RoTD

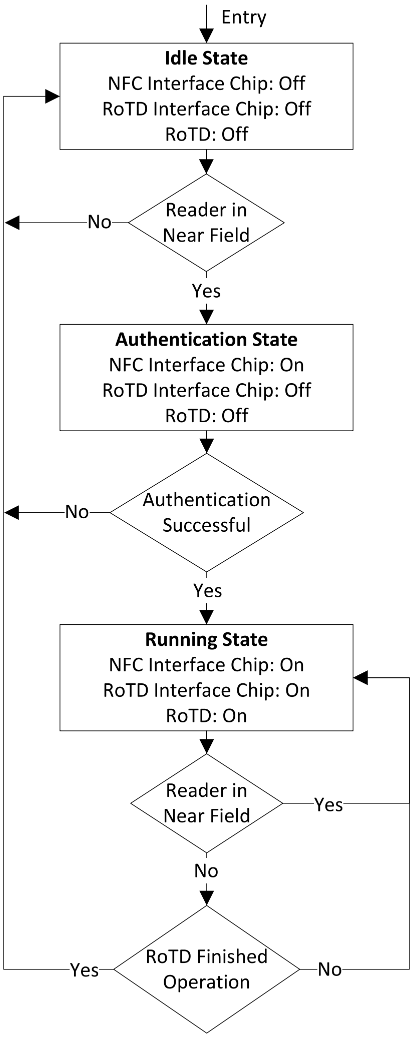


Fig. 3. A typical NFC Interface's flow of operation, obtained with changes from Druml et al. [3]

signals the power supply control unit to switch off the supply. As a consequence, the target device returns to idle state and no standby power is dissipated.

If an RoTD is given, which needs a significant amount of time to startup, an alternative early startup approach can be carried out to speed up the whole flow of operation. During this procedure, the RoTD is started asynchronously as soon as a magnetic field is sensed or a dedicated command is received from the reader. While performing this early-startup approach, the NFC Interface chip acts like a firewall and restricts any data transfers to the RoTD until the authentication procedure finishes successfully. With the help of this early startup approach and the usage of hardware accelerated cryptography, the amount of delay until the RoTD is accessible can be minimized. Thus, a proper user experience can be maintained.

2.8 Hardware description concept

The NFC Interface solution can be feasibly integrated into any electronic device. As a consequence, a high variability of different target device functionalities shall be supported by the reader device's application. Therefore, our interface solution features a target device hardware description approach: the target device specifies its provided functionalities and GUI representation by means of an XML-based notation. The target device's specification is saved within the NFC Interface chip's non-volatile memory. When the user wants to interact with the target device and the magnetic field is switched on, this functional specification is transmitted to the reader device. Note, the specification data can be read out by the reader device without powering up the RoTD, the actual appliance. The reader device's application and NFC Interface software stack interpret this specification and present it in an appropriate way to the user. Therefore, various functionalities (e.g., user interface, event handling, monitoring, control, configuration), which differ from device type to device type, can be supported by only one application. This approach grants a maximum of flexibility while keeping the overhead costs low within the target device.

2.9 User interface outsourcing concept

There is an ongoing trend to provide everyday electronic devices with all kinds of user interfaces (e.g., touch screens, LCD displays, LEDs, Wi-Fi) which may waste a significant amount of power. In addition, these interfaces are often implemented halfheartedly and difficult to use, because of time-to-market and cost pressures. The presented NFC Interface-based hardware description concept enables the innovative user interface outsourcing paradigm: the target device dispenses with power dissipating and clumsy user interface. The user interface is moved to the reader, i.e. smart phone or tablet. Thus, the target device's bill of materials and power consumption are reduced. Furthermore, state-of-the-art, power-aware, and smart phone-based user interface elements can be featured.

2.10 Internet connectivity concept

Given the fact that NFC-enabled smart phones and tablets feature internet access, innovative system architectures are realizable which may encompass a server, reader, and the target device. Thus, any kind of data transfer (e.g., status or configuration data) between the target device and a server can be supported without the need for a dedicated costly peripheral on the target device itself. For example, if the target device requires maintenance work due to a broken hardware component, a maintenance request along with an exact component specification can be transmitted to a dedicated service provider. As a further example of application, software and firmware updates for reader application and components of the target device can be issued during the entire product's life time.

3. Example of application

Figure 4 illustrates our NFC Interface technology demonstrator. This demonstrator consists of an NFC-enabled Android smart phone, the NFC Interface along with its very cheap (two-digit cent range for high order volumes) NFC Interface chip and its designated analog frontend, as well as an RoTD implemented on TI's MSP430 LaunchPad Experimeter Board. As RoTD case-study, a simplified functional simulation of a smart meter was chosen. In this case-study, the zero-energy secure communication interface can be used, e.g., for residential power consumption analyses, status checks, or configuration purposes. Thanks to the passively powered NFC Interface, no electrical power is wasted during its standby time. Furthermore, the smart phone's internet connectivity enables further innovative applications: e.g., cryptographically signed energy consumption reports could be transmitted encrypted to the electricity supplier, which would reduce the electricity supplier's and the customer's time expenditures.

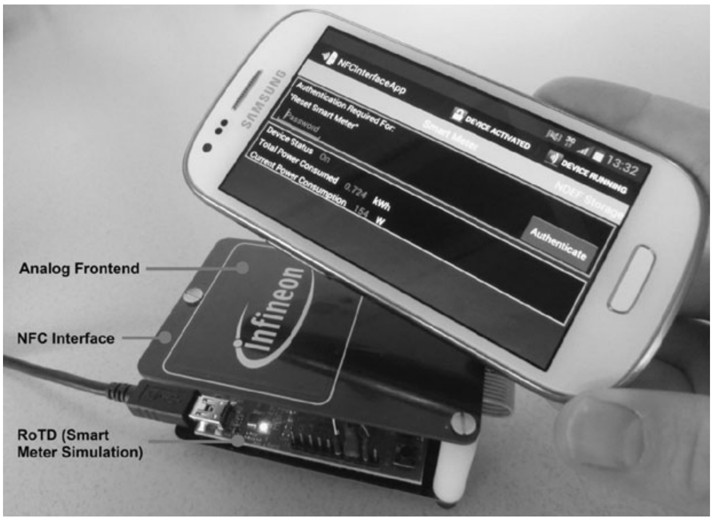


Fig. 4. NFC Interface demonstrator with a smart meter target device simulation

4. Conclusion

Standby power consumption of electronic devices is a waste of energy that needs to be reduced. A major milestone in reducing standby power was the introduction of several standby power guidances, such as the One-Watt Initiative, Japanese standby proposal, etc.

This paper presents an innovative NFC-based secure interface concept for everyday electronic devices, which enables the zero-energy paradigm. It is especially suitable for appliances that wait / poll for user activity (e.g., access control terminal), for appliances featuring a push-to-wakeup concept, or for appliances requiring a passively powered communication interface. Besides standby power management, the NFC Interface features state-of-the-art cryptography, innovative hardware abstraction and user interface concepts, and it enables configuration, monitor, and control tasks of the NFC Interface enhanced target device. We exemplified the feasible integration of the NFC Interface by means of a smart meter case-study.

Acknowledgements

We would like to thank the Austrian Federal Ministry for Transport, Innovation, and Technology which funded the project META[:SEC:] under the FIT-IT contract 829586. Furthermore, we would like to thank our industrial partners Infineon Technologies Austria AG as well as Enso Detego GmbH for their support.

References

1. Bock, H., Braun, M., Dichtl, M., Hess, E., Heyszl, J., Kargl, W., Koroschetz, H., Meyer, B., Seuschek, H. (2008): A milestone towards RFID products offering asymmetric authentication based on elliptic curve cryptography. Invited talk at RFIDsec.
2. Chakraborty, A., Pfaelzer, A. (2011): An overview of standby power management in electrical and electronic power devices and appliances to improve the overall energy efficiency in creating a green world. Journal of Renewable and Sustainable Energy. American Institute of Physics, 3(2).
3. Druml, N., Menghin, M., Basagic, R., Steger, C., Weiss, R., Bock, H., Haid, J. (2012): NIZE – a near field communication interface enabling zero energy standby for everyday electronic devices. In Proceedings of the 8th international conference on wireless and mobile computing, networking and communications (WiMob) (pp. 261–267).
4. Magno, M., Marinkovic, S., Brunelli, D., Popovici, E., O'Flynn, B., Benini, L. (2012): Smart power unit with ultra low power radio trigger capabilities for wireless sensor networks. In Design, automation and test in Europe conference and exhibition (DATE) (pp. 75–80).
5. McGarry, L. (2004): The standby power challenge. In International IEEE conference on the Asian green electronics (AGEC) (pp. 56–62).
6. Siwamogsatham, S., Rattanawan, P., Kitjaroen, M., Songtung, P., Pongpaibool, P., Navanugraha, K. (2011): Smartly saving energy with a zero power consumption standby system. In Proceedings of PICMET'11: technology management in the energy smart world.
7. Tiwari, V., Donnelly, R., Malik, S., Gonaalea, R. (1997): Dynamic power management for microprocessors: a case study. In International conference on VLSI design (pp. 185–192).
8. Tsai, C.-H., Bai, Y.-W., Chu, C.-A., Chung, C.-Y., Lin, M.-B. (2010): Design and implementation of a socket with zero standby power using a photovoltaic array. IEEE Trans. Consum. Electron., 56(4), 2686–2693.

Authors

Norbert Druml

received his Master's degree in telematics from Graz University of Technology in 2011, focusing on microelectronics, embedded systems, and software development. Since 2011, he has been carrying out research for his doctoral thesis in the field of electrical engineering at the Institute for Technical Informatics at Graz University of Technology in collaboration with Infineon Technologies Austria AG and Enso Detego GmbH. His research interests include low-power hardware/software codesign and emulation-based design analysis techniques.

Manuel Menghin
received his Master's degree in telematics from Graz University of Technology in 2010, focusing on microelectronics and biomedical engineering. Since 2011, he has been a Ph.D. student in electrical engineering at the Institute for Technical Informatics at Graz University of Technology in collaboration with Infineon Technologies Austria AG and Enso Detego GmbH. His research interests include system-based concepts for power-awareness in embedded systems.

Christian Steger
received the Dipl.-Ing. degree (M.Sc.) 1990, and the Dr. techn. degree (Ph.D.) in electrical engineering from Graz University of Technology, Austria, in 1995, respectively. He is key researcher at the Virtual Vehicle Competence Center (ViF, COMET K2) in Graz, Austria. From 1989 to 1991 he was software trainer and consultant at SPC Computer Training GmbH., Vienna. Since 1992 he has been Assistant Professor at the Institute for Technical Informatics, Graz University of Technology. He heads the HW/SW codesign group at the Institute for Technical Informatics. His research interests include embedded systems, HW/SW codesign, HW/SW coverfication, SOC, power awareness, smart cards, UHF RFID systems, multi-DSPs.

Holger Bock
received his Master's degree in electrical engineering at the Graz University of Technology in 1994. From 1991 to 1998 he has been working on concepts, software and hardware development, especially on VLSI-Design for cryptographic co-processors for smart cards (DES, ECC) at the Institute for Applied Information Processing and Communications Technologies (IAIK). In December 1998 he joined the team at Infineon's development center in Graz as a core competence for security. Since beginning of 2001 he had been a member of the technology & innovations methodology team at Infineon's business group Chipcard & Security ICs, focusing on secure, especially DPA resistant, design methodologies for cryptographic hardware.

Josef Haid
received his Master's degree in telematics and a doctoral degree in electrical engineering both from Graz University of Technology, Austria, in the years 2001 and 2003, respectively. Presently, he is a senior staff engineer at Infineon Technologies in Graz, Austria and is responsible for specification of low-power contactless smart cards. His interests include advanced digital design and low power design of hardware and software.

Bibliography

[1] R. Kurzweil, *The Singularity Is Near: When Humans Transcend Biology.* The Viking Press, 2005.

[2] P. Berezin, "Human Intelligence And Economic Growth From 50,000 B.C. To The Singularity." online. http://blog.bcaresearch.com/human-intelligence-economic-growth-50000-bc-singularity, visited 2014-03-04.

[3] ITRS, "International Technology Roadmap for Semiconductors (2011 Edition)." online. http://www.itrs.net/Links/2011ITRS/Home2011.htm, visited 2014-01-14.

[4] S. Borkar, "Designing reliable systems from unreliable components: the challenges of transistor variability and degradation," *IEEE Micro*, vol. 25, no. 6, pp. 10–16, 2005.

[5] H. Foster, "The 2012 Wilson Research Group Functional Verification Study." online. http://blogs.mentor.com/verificationhorizons/blog/author/hfoster/, visited 2014-03-03.

[6] N. Druml, M. Menghin, C. Steger, R. Weiss, A. Genser, H. Bock, and J. Haid, "Emulation-Based Test and Verification of a Design's Functional, Performance, Power, and Supply Voltage Behavior," in *Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP)*, pp. 328–335, February 2013.

[7] N. Druml, M. Menghin, D. Kroisleitner, C. Steger, R. Weiss, A. Krieg, H. Bock, and J. Haid, "Emulation-Based Fault Effect Analysis for Resource Constrained, Secure, and Dependable Systems," in *Euromicro Conference on Digital System Design (DSD)*, pp. 337–344, September 2013.

[8] N. Druml, M. Menghin, D. Kroisleitner, C. Steger, R. Weiss, H. Bock, and J. Haid, "Emulation-based Design Evaluation of Reader/Smart Card Systems," in *International Symposium on Rapid System Prototyping (RSP)*, pp. 80–86, October 2013.

[9] N. Druml, M. Menghin, T. Rauter, C. Steger, R. Weiss, C. Bachmann, H. Bock, and J. Haid, "Power and Thermal Fault Effect Exploration Framework for Reader/Smart Card Designs," in *Euromicro Conference on Digital System Design (DSD)*, pp. 898–906, September 2013.

[10] N. Druml, A. Genser, J. Haid, C. Steger, and R. Weiss, "Estimation Based Power and Supply Voltage Management for Future RF-Powered Multi-Core Smart Cards," in

Design Automation and Test in Europe Conference and Exhibition (DATE), pp. 358–363, March 2012.

[11] M. Wendt, C. Grumer, C. Steger, R. Weiss, U. Neffe, and A. Muehlberger, "System Level Power Profile Analysis and Optimization for Smart Cards and Mobile Devices," in *ACM Symposium on Applied Computing*, pp. 118–121, November 2008.

[12] N. Druml, M. Menghin, C. Steger, R. Weiss, A. Genser, H. Bock, and J. Haid, "Adaptive Field Strength Scaling - A Power Optimization Technique for Contactless Reader / Smart Card Systems," in *Euromicro Conference on Digital System Design (DSD)*, pp. 616–623, September 2012.

[13] N. Druml, M. Menghin, C. Steger, R. Weiss, H. Bock, and J. Haid, "A Flexible and Lightweight ECC-Based Authentication Solution for Resource Constrained Systems," in *Euromicro Conference on Digital System Design (DSD) (under review)*, 2014.

[14] N. Druml, M. Menghin, R. Basagic, C. Steger, R. Weiss, H. Bock, and J. Haid, "NIZE - A Near Field Communication Interface Enabling Zero Energy Standby for Everyday Electronic Devices," in *International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pp. 261–267, October 2012.

[15] N. Druml, M. Menghin, C. Steger, H. Bock, and J. Haid, "A secure zero-energy NFC solution for everyday electronic devices," *e & i Elektrotechnik und Informationstechnik*, vol. 130, pp. 224–229, November 2013.

[16] Aeroflex Gaisler, "LEON3 Processor." online, February 2014. http://gaisler.com/index.php/products/processors/leon3.

[17] S. Borkar, "Design challenges of technology scaling," *IEEE Micro*, vol. 19, pp. 23–29, July 1999.

[18] R. Das, "RFID 2014 to 2024: The Trends, Markets and Money." online. http://www.idtechex.com/, visited 2014-03-18.

[19] L. Benini, D. Bertozzi, A. Bogliolo, F. Menichelli, and M. Olivieri, "MPARM: Exploring the Multi-Processor SoC Design Space with SystemC," *Journal of VLSI Signal Processing Systems*, vol. 41, pp. 169–182, Sept. 2005.

[20] C. Jalier, D. Lattard, and G. Sassatelli, "A flexible modeling and simulation framework for Design Space Exploration," in *International Symposium on System-on-Chip*, pp. 1–4, November 2008.

[21] C. Chang, K. Kuusilinna, B. Richards, A. Chen, N. Chan, R. Brodersen, and B. Nikolic, "Rapid Design and Analysis of Communication Systems Using the BEE Hardware Emulation Environment," in *IEEE International Workshop on Rapid Systems Prototyping*, pp. 148–154, June 2003.

[22] G. Ganapathy, R. Narayan, C. Jorden, M. Wang, and J. Nishimura, "Hardware Emulation for Functional Verification of K5," in *Design Automation Conference (DAC)*, pp. 315–318, June 1996.

[23] P. Del Valle, D. Atienza, I. Magan, J. Flores, E. Perez, J. Mendias, L. Benini, and G. De Micheli, "Architectural Exploration of MPSoC Designs Based on an FPGA Emulation Framework," in *Conference on Design of Circuits and Integrated Systems (DCIS)*, pp. 12–18, November 2006.

[24] X. Li and O. Hammami, "Multi-FPGA emulation of a 48-cores multiprocessor with NOC," in *3rd International Design and Test Workshop (IDT)*, pp. 205–208, December 2008.

[25] Kouadri-Mostefaoui, Abdellah-Medjadji, B. Senouci, and F. Petrot, "Large Scale On-Chip Networks : An Accurate Multi-FPGA Emulation Platform," in *EUROMICRO Conference on Digital System Design Architectures, Methods and Tools (DSD)*, pp. 3–9, September 2008.

[26] P. Meloni, S. Secchi, and L. Raffo, "An FPGA-Based Framework for Technology-Aware Prototyping of Multicore Embedded Architectures," *IEEE Embedded Systems Letters*, vol. 2, pp. 5–9, March 2010.

[27] N. Genko, D. Atienza, G. De Micheli, J. Mendias, R. Hermida, and F. Catthoor, "A complete network-on-chip emulation framework," in *Design, Automation and Test in Europe (DATE)*, pp. 246–251, March 2005.

[28] R. Bergamaschi, G. Han, A. Buyuktosunoglu, H. Patel, I. Nair, G. Dittmann, G. Janssen, N. Dhanwada, Z. Hu, P. Bose, and J. Darringer, "Exploring Power Management in Multi-Core Systems," in *Asia and South Pacific Design Automation Conference*, pp. 708–713, March 2008.

[29] R. Joseph and M. Martonosi, "Run-Time Power Estimation in High Performance Microprocessors," in *International Symposium on Low Power Electronics and Design*, pp. 135–140, August 2001.

[30] J. Coburn, S. Ravi, and A. Raghunathan, "Power Emulation: A New Paradigm for Power Estimation," in *Design Automation Conference*, pp. 700–705, June 2005.

[31] A. Genser, C. Bachmann, J. Haid, C. Steger, and R. Weiss, "An Emulation-Based Real-Time Power Profiling Unit for Embedded Software," in *International Symposium on Systems, Architectures, Modeling, and Simulation*, pp. 67–73, July 2009.

[32] C. Bachmann, A. Genser, J. Haid, C. Steger, and R. Weiss, "Automated Power Characterization for Run-Time Power Emulation of SoC Designs," in *13th Euromicro Conference on Digital System Design (DSD)*, pp. 587–594, September 2010.

[33] E. Grochowski, D. Ayers, and V. Tiwari, "Microarchitectural simulation and control of di/dt-induced power supply voltage variation," in *Eighth International Symposium on High-Performance Computer Architecture*, pp. 7–16, February 2002.

[34] M. Holtz, S. Narasimhan, and S. Bhunia, "On-Die CMOS Voltage Droop Detection and Dynamic Compensation," in *Proceedings of the 18th ACM Great Lakes symposium on VLSI*, pp. 35–40, May 2008.

[35] E. Alon, V. Stojanovic, and M. Horowitz, "Circuits and Techniques for High-Resolution Measurement of On-Chip Power Supply Noise," *IEEE Journal of Solid-State Circuits*, vol. 40, pp. 820–828, April 2005.

[36] T. Nakura, M. Ikeda, and K. Asada, "Preliminary Experiments for Power Supply Noise Reduction using Stubs," in *Asia-Pacific Conference on Advanced System Integrated Circuits*, pp. 286–289, August 2004.

[37] A. Genser, C. Bachmann, J. Haid, C. Steger, and R. Weiss, "Supply Voltage Emulation Platform for DVFS Voltage Drop Compensation Explorations," in *IEEE International Symposium on Performance Analysis of Systems and Software*, pp. 129–130, April 2011.

[38] L. Benini, A. Bogliolo, and G. De Micheli, "A survey of design techniques for system-level dynamic power management," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 8, pp. 299–316, June 2000.

[39] M. Badaroglu, K. Tiri, S. Donnay, P. Wambacq, I. Verbauwhede, G. Gielen, and H. De Man, "Clock Tree Optimization in Synchronous CMOS Digital Circuits for Substrate Noise Reduction Using Folding of Supply Current Transients," in *Design Automation Conference*, pp. 399–404, June 2002.

[40] V. Reddi, M. Gupta, G. Holloway, G. Wei, M. Smith, and D. Brooks, "Voltage Emergency Prediction Using Signatures to Reduce Operating Margins," in *International Symposium on High Performance Computer Architecture*, pp. 18–29, February 2009.

[41] J. Haid, W. Kargl, T. Leutgeb, and D. Scheiblhofer, "Power Management for RF-Powered vs. Battery-Powered Devices," 2005.

[42] P. Lall, "Tutorial: Temperature as an Input to Microelectronics-Reliability Models," *IEEE Transactions on Reliability*, vol. 45, pp. 3–9, March 1996.

[43] D. Atienza, G. De Micheli, L. Benini, J. Ayala, P. Del Valle, M. DeBole, and V. Narayanan, "Reliability-aware design for nanometer-scale devices," in *Asia and South Pacific Design Automation Conference (ASP-DAC)*, pp. 549–554, March 2008.

[44] D. Atienza, P. G. Del Valle, G. Paci, F. Poletti, L. Benini, G. D. Micheli, J. M. Mendias, and R. Hermida, "HW-SW emulation framework for temperature-aware design in MPSoCs," *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, vol. 12, pp. 26:1–26:26, May 2008.

[45] K. Skadron, M. R. Stan, K. Sankaranarayanan, W. Huang, S. Velusamy, and D. Tarjan, "Temperature-aware microarchitecture: Modeling and implementation," *ACM Transactions on Architecture and Code Optimization (TACO)*, vol. 1, pp. 94–125, March 2004.

[46] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," *IEEE Transactions on Dependable and Secure Computing*, vol. 1, pp. 11–33, Jan 2004.

[47] S. Ravi, A. Raghunathan, P. Kocher, and S. Hattangady, "Security in embedded systems: Design challenges," *ACM Transactions on Embedded Computing Systems (TECS)*, vol. 3, pp. 461–491, August 2004.

[48] P. Kocher, "Complexity and the challenges of securing SoCs," in *Design Automation Conference (DAC)*, pp. 328–331, June 2011.

[49] K. Rothbart, U. Neffe, C. Steger, R. Weiss, E. Rieger, and A. Muehlberger, "High level fault injection for attack simulation in smart cards," in *13th Asian Test Symposium (ATS)*, pp. 118–121, November 2004.

[50] C. Bolchini, A. Miele, and D. Sciuto, "Models and Injection Strategies in SystemC Specifications," in *11th EUROMICRO Conference on Digital System Design Architectures, Methods and Tools (DSD)*, pp. 88–95, September 2008.

[51] R. Shafik, P. Rosinger, and B. Al-Hashimi, "SystemC-Based Minimum Intrusive Fault Injection Technique with Improved Fault Representation," in *14th IEEE International On-Line Testing Symposium (IOLTS)*, pp. 99–104, July 2008.

[52] J. Arlat, M. Aguera, L. Amat, Y. Crouzet, J.-C. Fabre, J.-C. Laprie, E. Martins, and D. Powell, "Fault injection for dependability validation: a methodology and some applications," *IEEE Transactions on Software Engineering*, vol. 16, pp. 166–182, February 1990.

[53] E. Jenn, J. Arlat, M. Rimen, J. Ohlsson, and J. Karlsson, "Fault injection into VHDL models: the MEFISTO tool," in *International Symposium on Fault-Tolerant Computing, Digest of Papers*, pp. 66–75, June 1994.

[54] J. Grinschgl, A. Krieg, C. Steger, R. Weiss, H. Bock, J. Haid, T. Aichinger, and C. Ulbricht, "Case study on multiple fault dependability and security evaluations," *Microprocessors and Microsystems*, vol. 37, pp. 218–227, March 2013.

[55] M. Valderas, M. Garcia, R. Cardenal, C. Lopez Ongil, and L. Entrena, "Advanced Simulation and Emulation Techniques for Fault Injection," in *IEEE International Symposium on Industrial Electronics*, pp. 3339–3344, June 2007.

[56] J. Baraza, J. Gracia, D. Gil, and P. Gil, "Improvement of fault injection techniques based on VHDL code modification," in *IEEE International High-Level Design Validation and Test Workshop*, pp. 19–26, November 2005.

[57] L. Entrena, M. Garcia-Valderas, R. Fernandez-Cardenal, A. Lindoso, M. Portela, and C. Lopez-Ongil, "Soft Error Sensitivity Evaluation of Microprocessors by Multilevel Emulation-Based Fault Injection," *IEEE Transactions on Computers*, vol. 61, pp. 313–322, March 2012.

[58] A. Rahimi, L. Benini, and R. Gupta, "Analysis of instruction-level vulnerability to dynamic voltage and temperature variations," in *Design, Automation Test in Europe Conference Exhibition (DATE)*, pp. 1102–1105, March 2012.

[59] R. Leveugle, “Fault injection in VHDL descriptions and emulation,” in *IEEE International Symposium on Defect and Fault Tolerance in VLSI Systems*, pp. 414–419, October 2000.

[60] J.-M. Daveau, A. Blampey, G. Gasiot, J. Bulone, and P. Roche, “An Industrial Fault Injection Platform for Soft-Error Dependability Analysis and Hardening of Complex System-On-a-Chip,” in *IEEE International Reliability Physics Symposium*, pp. 212–220, April 2009.

[61] T. Kasper, D. Oswald, and C. Paar, “A Versatile Framework for Implementation Attacks on Cryptographic RFIDs and Embedded Devices,” in *Transactions on Computational Science X*, vol. 6340, pp. 100–130, Springer-Verlag, 2010.

[62] T. Plos, M. Aigner, T. Baier, M. Feldhofer, M. Hutter, T. Korak, and E. Wenger, “Semi-Passive RFID Development Platform for Implementing and Attacking Security Tags,” *International Journal of RFID Security and Cryptography*, vol. 1, pp. 16–24, 2012.

[63] J. Barton, E. Czeck, Z. Segall, and D. Siewiorek, “Fault injection experiments using FIAT,” *IEEE Transactions on Computers*, vol. 39, pp. 575–582, April 1990.

[64] G. Kanawati, N. Kanawati, and J. Abraham, “FERRARI: a tool for the validation of system dependability properties,” in *International Symposium on Fault-Tolerant Computing*, pp. 336–344, July 1992.

[65] S. Govindavajhala and A. Appel, “Using memory errors to attack a virtual machine,” in *Symposium on Security and Privacy*, pp. 154–165, May 2003.

[66] S. Mangard, E. Oswald, and T. Popp, *Power Analysis Attacks: Revealing the Secrets of Smart Cards.* Springer, 2007.

[67] A. Krieg, J. Grinschgl, C. Steger, R. Weiss, H. Bock, and J. Haid, “POWER-MODES: POWer-EmulatoR- and MOdel-Based DEpendability and Security Evaluations,” *ACM Transactions on Reconfigurable Technology and Systems (TRETS)*, vol. 5, pp. 19:1–19:21, December 2012.

[68] E. Haselsteiner and K. Breitfuss, “Security in Near Field Communication (NFC) - Strengths and Weaknesses,” in *Workshop on RFID Security (RFIDSec)*, pp. 1–10, July 2006.

[69] M. Hutter, J.-M. Schmidt, and T. Plos, “RFID and its Vulnerability to Faults,” in *International workshop on Cryptographic Hardware and Embedded Systems (CHES)*, pp. 363–379, August 2008.

[70] T. Korak, T. Plos, and M. Hutter, “Attacking an AES-Enabled NFC Tag: Implications from Design to a Real-World Scenario,” in *Constructive Side-Channel Analysis and Secure Design*, vol. 7275 of *Lecture Notes in Computer Science*, pp. 17–32, Springer Berlin Heidelberg, 2012.

[71] T. Korak and T. Plos, "Applying Remote Side-Channel Analysis Attacks on a Security-Enabled NFC Tag," in *Topics in Cryptology - CT-RSA 2013*, vol. 7779 of *Lecture Notes in Computer Science*, pp. 207–222, Springer Berlin Heidelberg, 2013.

[72] M. Feldhofer and J. Wolkerstorfer, "Strong Crypto for RFID Tags - A Comparison of Low-Power Hardware Implementations," in *IEEE International Symposium on Circuits and Systems (ISCAS)*, pp. 1839–1842, May 2007.

[73] M. Menghin, N. Druml, M. Fioriello, C. Steger, R. Weiss, H. Bock, and J. Haid, "PtNBridge - A Power-Aware and Trustworthy Near Field Communication Bridge to Embedded Systems," in *Euromicro Conference on Digital System Design (DSD)*, pp. 907–914, September 2013.

[74] D. Hankerson, A. J. Menezes, and S. Vanstone, *Guide to Elliptic Curve Cryptography*. Springer Professional Computing, 2004.

[75] E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid, "Recommendation for Key Management - Part 1: General (Revised)," in *NIST Special Publication*, 2006.

[76] National Security Agency, "The Case for Elliptic Curve Cryptography." online, February 2014. http://www.nsa.gov/business/programs/elliptic_curve.shtml3.

[77] H. Aigner, H. Bock, M. Hütter, and J. Wolkerstorfer, "A Low-Cost ECC Coprocessor for Smartcards," in *Cryptographic Hardware and Embedded Systems (CHES)*, vol. 3156 of *Lecture Notes in Computer Science*, pp. 107–118, Springer Berlin Heidelberg, August 2004.

[78] H. Bock, M. Braun, M. Dichtl, E. Hess, J. Heyszl, W. Kargl, H. Koroschetz, B. Meyer, and H. Seuschek, "A Milestone Towards RFID Products Offering Asymmetric Authentication Based on Elliptic Curve Cryptography," in *Invited talk at Workshop on RFID Security (RFIDSec)*, pp. 1–14, July 2008.

[79] J. Fan, K. Sakiyama, and I. Verbauwhede, "Elliptic curve cryptography on embedded multicore systems," *Design Automation for Embedded Systems*, vol. 12, no. 3, pp. 231–242, 2008.

[80] E. Wenger, T. Baier, and J. Feichtner, "JAAVR: Introducing the Next Generation of Security-Enabled RFID Tags," in *Euromicro Conference on Digital System Design (DSD)*, pp. 640–647, September 2012.

[81] E. Wenger, T. Unterluggauer, and M. Werner, "8/16/32 Shades of Elliptic Curve Cryptography on Embedded Processors," in *Progress in Cryptology - INDOCRYPT 2013*, vol. 8250 of *Lecture Notes in Computer Science*, pp. 244–261, Springer International Publishing, December 2013.

[82] J. Fan, X. Guo, E. De Mulder, P. Schaumont, B. Preneel, and I. Verbauwhede, "State-of-the-art of secure ECC implementations: a survey on known side-channel attacks and countermeasures," in *International Symposium on Hardware-Oriented Security and Trust (HOST)*, pp. 76–87, June 2010.

[83] R. Leveugle, “Early Analysis of Fault-based Attack Effects in Secure Circuits,” *IEEE Transactions on Computers*, vol. 56, pp. 1431–1434, October 2007.

[84] A. Krieg, C. Bachmann, J. Grinschgl, C. Steger, R. Weiss, and J. Haid, “Accelerating early design phase differential power analysis using power emulation techniques,” in *IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, pp. 81–86, June 2011.

[85] K. Finkenzeller, *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification.* John Wiley & Sons, 2nd ed., 2003.

[86] Infineon, “SLE 77CFX2400P - Short Product Overview.” online, February 2014. http://www.infineon.com.