Dipl.-Ing. Manuel Josef Menghin, Bakk.techn.

Power Optimization Techniques for Near Field Communication 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

Near Field Communication (NFC) ist eine Verbindungstechnologie, die den Datentransfer über geringe Distanzen erlaubt. Radio-frequency identification (RFID) ist die zugrunde liegende Technologie, die zusätzlich eine drahtlose Energieübertragung von RFID-Lesegeräten zu Transpondern (z.B. Smart Cards) erlaubt. NFC spezifiziert die zu verwendenden Kommunikationsprotokolle und Formate für den Datenaustausch nach existierenden Normen. Das Ziel dieser resultierenden Spezifikationsarchitektur ist es, die Interoperabilität zwischen NFC-fähigen Geräten zu gewährleisten. Diese Interoperabilität treibt die Integration von NFC in mobilen Geräten, wie zum Beispiel dem Smartphone voran. Die Anzahl ausgelieferter Geräte mit NFC wird auf bis zu 1,2 Milliarden im Jahr 2017 geschätzt. Die NFC-Integration führt jedoch zu einem erhöhten Energieverbrauch dieser Geräte, der durch die Verwendung der drahtlosen Energieübertragung noch weiter erhöht wird. Schlussfolgernd ergibt sich, dass zur Reduktion dieses Energieverbrauchs das Gesamtsystem bestehend aus dem NFC-Lesegerät (z.B. Smartphone), dem Kanal zur drahtlosen Energieübertragung und dem Transponder (z.B. Bezahlkarte) betrachtet werden muss.

Der Beitrag dieser Arbeit liegt in der Erforschung neuer Methoden zur Leistungsoptimierung basierend auf der Adaptierung der magnetischen Feldstärke. Ergänzend wurde ein Werkzeug zur Entwicklung von NFC-Systemen vorgeschlagen und implementiert, um diese Methoden sowohl anwenden, als auch die Anforderungen an den Energieverbrauch während der Entwicklung solcher Systeme verifizieren zu können. Die Adaptierung der magnetischen Feldstärke zielt auf eine Reduktion des drahtlosen Energietransfers auf das nötige Minium zur Versorgung des Transponders ab. Die erste Implementierung skaliert das magnetische Feld einmalig während der Phase des drahtlosen Verbindungsaufbaus. Der Einfluss auf den Leistungsverbrauch wurde hierbei anhand einer Fallstudie evaluiert. Die zweite Implementierung erweitert die Erste mit der Funktion der periodischen Nachskalierung während des gesamten Kommunikationsprozesses. Zwei weitere Fallstudien untersuchen sowohl die Anwendbarkeit der Adaptierung der magnetischen Feldstärke für Systeme mit mehreren Transpondern im Feld als auch den Einfluss von Sicherheitsmethoden auf den Leistungsverbrauch von NFC-Systemen. Das ergänzende Werkzeug zur Entwicklung von NFC-Systemen basiert auf Entwurfsmustern (Patterns) für Methoden zur Leistungsoptimierung und einem Verifikations-Framework das Werkzeuge wie SystemC Simulationen und Hardware in the Loop (HiL) Messungen unterstützt.

Abstract

Near Field Communication (NFC) is a short range connectivity technology that enables a contactless exchange of data. The underlying technology of Radio-frequency identification (RFID) allows a wireless power transfer to the transponder (e.g., smart card). NFC also specifies the communication protocols and data exchange formats based on existing standards. This specification architecture aims for interoperability between NFC enabled devices. This interoperability is one main driver for integrating NFC into handsets like smart phones. The number of shipped handsets is predicted to hit the 1.2 billion mark in 2017. Unfortunately, the integration of NFC leads to increased energy consumption, especially when the feature of wireless power transfer, as for instance in accessing a payment card, is used. Undeniably, this reduction of the energy consumption is a matter of consideration for the whole system, consisting of the NFC-Reader (e.g., smart phone), the wireless communication channel, and the transponder (e.g., payment card).

This work contributes to research into power optimization techniques based on adapting the magnetic field strength. Additionally, a development toolbox for NFC-Systems to apply these techniques including the verification of the power requirements across the development phases has been proposed and implemented. The principle of magnetic field strength scaling aims to reduce the wireless power transfer from the NFC-Reader to the transponder to a minimum. The first implementation presented scales the field once during the phase of wireless connection establishment. The impact to the NFC-Systems power consumption is evaluated via a case study. The second implementation extends the first one with the feature of periodic rescaling during the whole communication process. Two additional case studies investigate the application of field strength scaling for multi-transponder applications, and the impact of security methods on the power consumption of NFC-Systems. The additional development toolbox consists of patterns for power-management, and a power verification framework supporting common verification tools like SystemC simulations and Hardware in the Loop (HiL) measurements across the development phases.

Acknowledgements

"Nothing can grow without a fertile ground ..."

I would like to thank my parent's support for so many years. Without them I would never have been able to get where I am now. The guidance and support of Professor Reinhold Weiss at the Institute for Technical Informatics was very important to finish my thesis - many thanks to you.
I also want to thank the Austrian Federal Ministry of Transport, Innovation and Technology for the funded project called META[:SEC:], which is the basis of my thesis. No project can succeed without leadership, and therefore I want to thank Christian Steger, Josef Haid, Holger Bock and also Thomas Ruprechter. Likewise many thanks to our two project partners Infineon Technologies Austria AG and Enso Detego GmbH for their support and valuable cooperation. Just as many thanks to my students for their important contribution.
I want to thank my teammate Norbert Druml, who was essential to accomplish the project tasks of META[:SEC:]. Additionally, I want to thank my working colleagues Johannes Grinschgl, Armin Krieg, Christoper Preschern, and Andreas Genser for their valuable comments and support. Last but not least I also would like to thank Silvia Reiter and Engelbert Meissl which helped me on all administrative matters.
Finally, I want to thank my dear Yvonne for her patience and support over the last years. Thank you!

Graz, June 2014 Manuel Menghin

Extended Abstract

Near Field Communication (NFC) is a short-range wireless connectivity technology based on inductive coupling. The working principle is "touch to communicate", which means that bringing NFC enabled devices in proximity to each other is enough to establish a connection. A pairing procedure, as in Bluetooth, is not required. The transmission range is about 10cm, and the operation frequency is 13.56MHz. NFC is not only a transmission technology, it also specifies the communication protocols and data exchange formats based on existing standards to provide interoperability. Through this interoperability, it is an obvious step to integrate NFC into everyday handsets like smart phones. According to market studies 50% of smart phones will be equipped with NFC hardware by 2015, which opens up new possibilities for mobile applications. A prominent application is wireless payment, which is predicted to be the preferred method of payment by 2020. The number of NFC handsets will rise over the years and is projected to hit the 1.2 billion mark by 2017. Unfortunately, integrating NFC into handsets also increases the handsets energy consumption. NFC is not only an interface for exchanging data, it is also possible to transfer energy to the communication partner called the transponder. For example, reading such a transponder using a smart phone increases the average power consumption of the smart phone by 107% during the communication process[1]. Reducing this energy consumption is a matter of considering the whole system, consisting of the NFC-Reader (e.g., smart phone), the wireless communication channel, and the transponder (e.g., payment card) to optimize this wireless power transfer. Therefore, the project called META[:SEC:][2] was started to investigate NFC-Systems. The project's research fields cover fault-awareness and power-awareness of NFC-Systems. In the field of power-awareness, the impact of NFC to the system's energy consumption is investigated to find proper optimization techniques. These techniques should be suitable for application in the development of an NFC-System. This means that the link between the proposed optimization techniques and the development process is of importance. Furthermore, the application of optimization techniques can take place in different phases of development and should also cover optimizations for software and hardware. The investigated development is shown in Figure 1. The development begins with an idea / specification of an NFC-System. The next step is to develop the NFC-System and optimize it to fulfill the specification. This step requires a development process, optimization techniques, and a development toolbox supporting this process. The development process is based on Model Driven Architecture (MDA), which uses models to design the system starting with use cases and requirements and transforms them into architecture, design and the implementation. Finally the development is finished resulting in an power optimized NFC-System.

[1] *Menghin et al., Using field strength scaling to save energy in mobile HF-band RFID-systems*, EURASIP Journal on Embedded Systems Volume 2013

[2] *Mobile Energy-efficient Trustworthy Authentication Systems with Elliptic Curve based SECurity*, col-

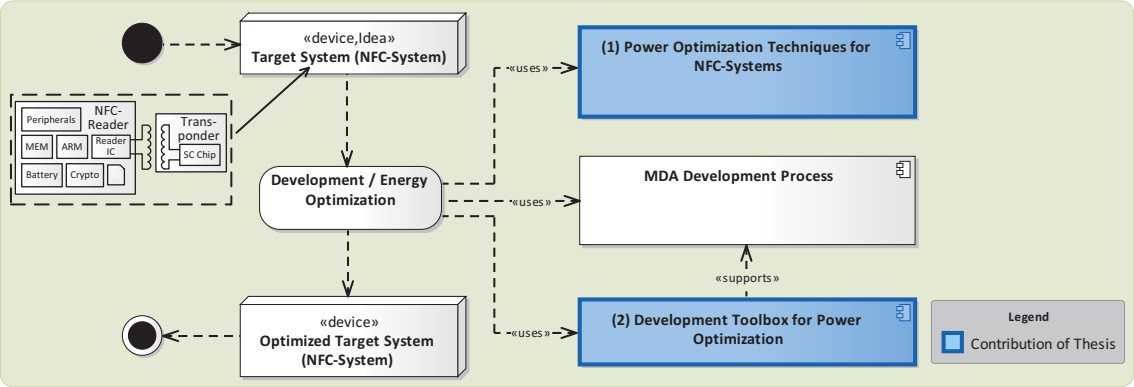


Figure 1: Overview of the steps required to develop an NFC-System, and the for development and power optimization.

This thesis contributes (1) a power optimization technique in two complementary implementations and the (2) development toolbox to apply and verify these optimization techniques across the development phases. The proposed optimization technique in this work is based on magnetic field strength scaling. The magnetic field strength provided by the NFC-Reader is commonly static and designed to provide enough power for the transponder at maximum transmission range. This leads to a waste of energy on the NFC-Reader side for smaller distances to the transponder. The idea is now to dynamically scale down the field strength in order to reduce this wastage of energy. The communication with the transponder can be separated into a detection phase and the actual communication, i.e. reading the data from the digital business card. In the first implementation, the scaling is done once during detection phase. Measurements show that this implementation is able to save up to 26 % energy on an actual NFC-System[3]. This implementation has the benefit of being simple and effective, but is not able to dynamically rescale on changes of distance between NFC-Reader and transponder. The second implementation deals with this disadvantage by allowing dynamic field strength scaling during the actual communication[4]. In a case study the technique of magnetic field strength scaling for multiple transponders has been evaluated. The experimental results show that magnetic field strength scaling is suitable, and for ten transponders stacked together an energy saving of up to 34 % is obtained[5]. This magnetic field strength technique has been explored and evaluated for the reader and transponder side in another work[6]. Magnetic field strength scaling depends on the power consumption of the transponder, which depends also on the usage of security in

laborative research project of the Graz University of Technology, Infineon Austria AG and Enso Detego GmbH. Funded by the Austrian Federal Ministry for Transport, Innovation, and Technology under the FIT-IT contract FFG 829586.

[3] *Menghin et al., The PTF-Determinator: A run-time method used to save energy in NFC-Systems*, Fourth International EURASIP Workshop on RFID Technology 2012

[4] *Menghin et al., NFC-DynFS: A way to realize dynamic field strength scaling during communication*, 5th International Workshop on Near Field Communication (NFC) 2013

[5] *Menghin et al., Energy Efficiency by Using Field Strength Scaling for Multi-Transponder Applications*, 12th International Conference on Telecommunications - ConTEL 2013

[6] *Druml et al., Adaptive Field Strength Scaling - A Power Optimization Technique for Contactless Reader / Smart Card Systems*, 15th Euromicro Conference on Digital System Design 2012

NFC-Systems. Therefore, a case study using an implementation of a secure NFC-Bridge to embedded systems has been created. In this case study, the energy consumption of different variants and strengths of security have been measured. The result of this evaluation shows, that by selecting the right variant, according to the measurement results, for the specified use case, up to 55 % of the energy can be saved on the NFC-Reader side[7]. Proposing these power optimization techniques without describing them in a usable structure is not enough. To find the right technique, a developer needs to know the context, the problem and needs to understand the consequences of applying this technique to the system. Therefore, the optimization technique of magnetic field strength scaling has been described as a pattern. A pattern is a systematic solution to a reoccurring problem. The pattern form has been extended to describe solutions for power optimization techniques[8]. Furthermore, applying techniques without verifying that the power requirements are now fulfilled can lead to costly redesigns. MDA is already well established in functional verification but not yet suited for power verification. Therefore, the MDA based development process used has to support power verification from the development stage where the technique has been applied all the way down to the implementation. The tools used and the experience of applying optimization techniques has been used to propose and implement a development framework for NFC-Systems. The framework integrates power verification techniques based on common tools like SystemC and hardware in the loop measurements across the development phases into one MDA-Tool. This set of techniques in the form of patterns and the development framework serves as a toolbox for the developer to reduce the development time and costs.

There are still open topics for future projects. One topic is improving the way patterns are used to apply power optimization techniques. This also includes additional extensions of the development process to apply these design patterns. Also the pattern portfolio has to be increased, to provide a workable selection. Another topic is creating support for IP-Core reuse in the proposed development process extension. IP-Core reuse is very important at present in achieving the development of new products in a shorter time. Another very important research topic is to investigate the NFC-System's influence on our lives and especially on our privacy. Industry and governments aim to include NFC in nearly every device and some of them are carried with us. Security is only a tool to restrict access to our private data, but does this really mean that our privacy is maintained?

[7] *Menghin et al., PtNBridge - A Power-Aware and Trustworthy Near Field Communication Bridge to Embedded Systems*, 16th Euromicro Conference on Digital System Design 2013

[8] *Menghin et al., Introduction of design patterns for power-management in embedded systems*, 18th European Conference on Pattern Languages of Programs 2013

Contents

List of Figures

List of Tables

Glossary

Pattern
A *pattern* is a systematic solution for an occurring problem within a given context. In distinction to a specific solution design patterns are no finished designs or implementations, and can also be described as formalized best practices.

Development Process
A *development process* is a structured set of activities to develop a product. This structure depends on the used development model. Example activities are design, implementation, and testing. These activities can have a relation to each other, like implementation requires the completion of the design.

NFC-Reader
An *NFC-Reader* is an electronic NFC-enabled device and is in this thesis configured in Reader/writer mode. This mode allows to communicate with transponders. The NFC-Reader sends a request to the transponder and waits for the response.

Power Optimization
A *power optimization* means reducing the power consumption of the component or system while preserving the functionality of the system. This can be achieved by using tools or techniques. An example technique is voltage scaling to reduce the power consumption of digital circuits.

Power Verification
Power verification is the evaluation whether the system complies to given power-requirements. This evaluation can be performed formally or via tools on different phases of the development. Two example tools are simulation and measurement.

Smart Card
A *smart card* is a credit-card sized card including an integrated circuit. The integrated circuit can be a pure state-machine or an embedded system. The interface of this card can be contactbased or contactless, like NFC.

Transponder
A *transponder* is an electronic device, which is able to respond to an incoming request. An example transponder is a contactless smart card, which listens to request from the NFC-Reader and answers with the appropriate response.

List of Abbreviations

AADL	Architecture Analysis & Design Language
AES	Advanced Encryption Standard
ARM	Advanced RISC Machines
CIM	Computational Independent Model
CPU	Central Processing Unit
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
FPGA	Field Programmable Gate Array
HiL	Hardware in the Loop
IC	Integrated Circuit
IP-Core	Intellectual Property Core
LLCP	Logical Link Control Protocol
MARTE	Modeling and Analysis of Real-time and Embedded systems
MDA	Model Driven Architecture
MDD	Model Driven Development
META[:SEC:]	Mobile Energy-efficient Trustworthy Authentication Systems with Elliptic Curve based SECurity
NDEF	NFC Data Exchange Format
NFC	Near Field Communication
NIST	National Institute of Standards and Technology
PIM	Platform Independent Model
PSM	Platform Specific Model
RFID	Radio-frequency identification
RSA	Rivest, Shamir and Adleman
RTD	Record Type Definition
SoC	System on Chip
UART	Universal Asynchronous Receiver Transmitter
UID	Unique identifier
VHDL	Very High Speed Integrated Circuit Hardware Description Language

Chapter 1

Introduction

This chapter is separated into seven sections. The first and second sections briefly describe NFC in relation to the potential market development over the next few years and the considered target system. Furthermore, challenges in the topics of energy, security and development are shown. In Section 1.4, the research project called META[:SEC:] is introduced. The final two sections describe the problem definition and the contribution of this thesis.

1.1 NFC and its Market Development

In 2004 the NFC Forum was established. The idea of NFC is to enable touch based interactions between devices, e.g., in consumer electronics. Interactions are realized by using the technology of Radio Frequency Identification (RFID) at a carrier frequency of 13.56MHz. Establishing a connection only requires bringing both communication partners, which can be an NFC-Reader (e.g., smart phone) and a transponder (e.g., payment card), into transmission range. No pairing like in Bluetooth is required. The claim of "touch based interaction" is justified through the limited transmission range of 10cm. The current mandatory supported transmission speed of NFC is 106kBit/s [12]. NFC also specifies communication protocols and data exchange formats to provide interoperability. The

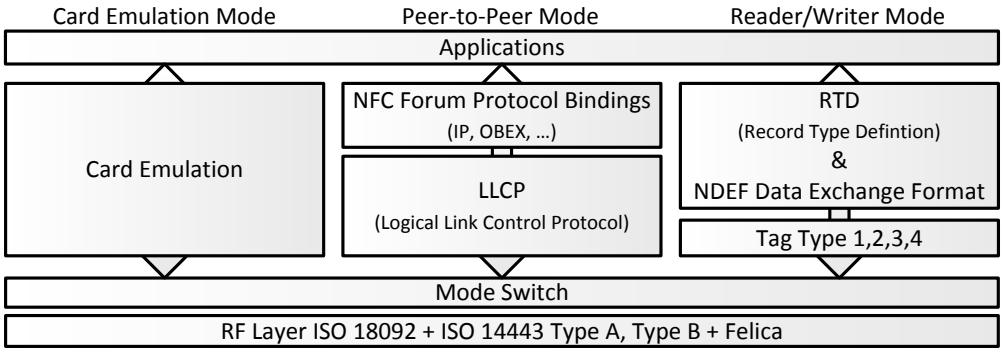


Figure 1.1: The NFC Forum Specification Architecture showing the used RFID technologies, the communication protocols and data exchange formats (adapted from [1]).

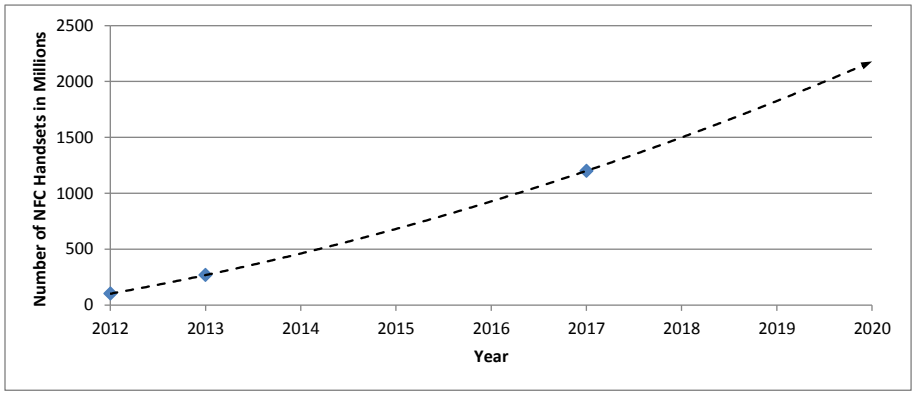


Figure 1.2: Trend estimation for the number of NFC handsets up to 2020 based on the study of [2].

specification architecture of NFC, shown in Figure 1.1, also supports different modes of communication. The reader/writer mode is used when communicating from an NFC-Reader to a transponder such as a payment card. In the card emulation mode an NFC-Reader behaves like a passive transponder. An example for this mode is using the NFC enabled smart phone as a payment card. The peer-to-peer mode enables a direct data exchange between two NFC-Readers. The NFC specification architecture is nowadays a driver to integrate NFC into everyday handsets like smart phones. Market studies predict that 50% of smart phones will be equipped with NFC hardware by 2015 [13]. The number of shipped NFC handsets is predicted to hit the 1.2 billion mark by 2017 as shown in Figure 1.2 [2]. In the year 2020 applications like wireless payment are predicted to be the preferred method of payment [14].

1.2 Definition of Target System

Before describing the emerging challenges in the domain of NFC, the target system considered in this thesis has to be defined. Figure 1.3 shows this target system and its

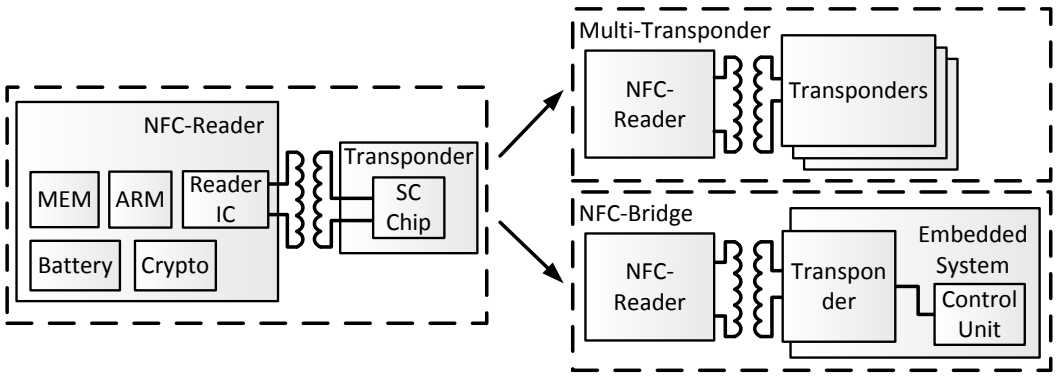


Figure 1.3: The target system considered for the power optimization techniques and the two variants of multi-transponder and NFC-Bridge.

variants. The base system consists of an NFC-Reader, the wireless communication path and a transponder. Two system variants are also investigated in this thesis. The first one consists of multiple transponders in range. An example is an access terminal as NFC-Reader and a briefcase with the access card and other transponders in it. The second variant is the NFC-Bridge. This bridge interlinks the wireless interface of NFC with another contact based interface, like UART. With this interlink an NFC-Reader is able to access an embedded system for control, configuration and monitoring. A scenario could be a smart meter equipped with this NFC-Bridge and a smart phone with an application to monitor the energy consumption of the household.

1.3 Motivation

1.3.1 Challenge of Saving Energy

The integration of NFC into handsets has the drawback of increasing the handset's energy consumption. The target system, as described in Section 1.2, can be a resource constraint, especially when the NFC-Reader is mobile, as in the case of a smart phone. Figure 1.4 shows the energy trace of such a smart phone reading a transponder using NFC (Reader/writer mode). During the reading process the average power consumption of the NFC-Reader increases by up to 107% [6]. One reason for this increase is the wireless power transfer to the transponder. This indicates that the energy consumption of the NFC-Reader depends on the consumption of the transponder, and concludes that reducing the energy consumption means considering the whole NFC-System.

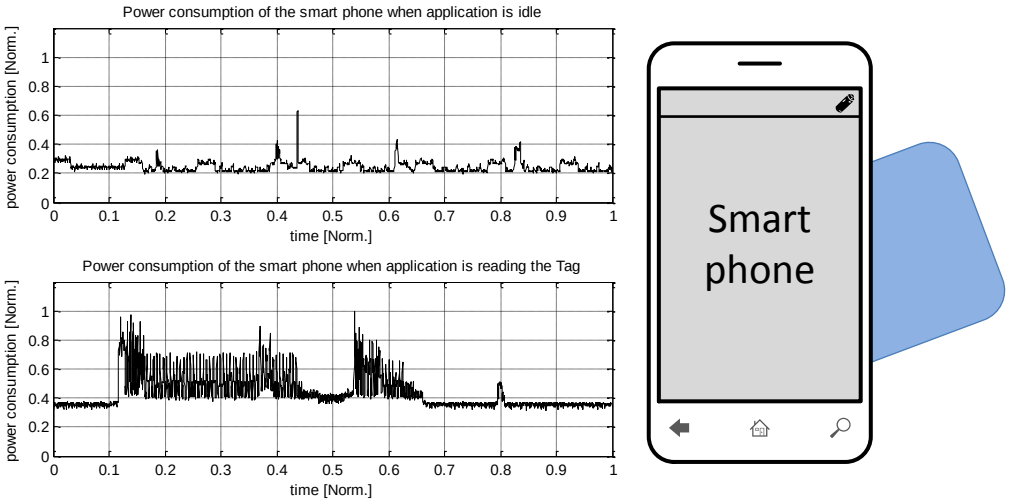


Figure 1.4: Power consumption of the smart phone (NFC-Reader) whilst reading a transponder over NFC, and the consumption when idle.

1.3.2 Security Needs Energy

Using NFC-Systems, as described in Section 1.2, for applications like wireless payment, it is mandatory to add security. The user of such systems trusts in its security. The violation

of this trust leads to the rejection of these systems by this user. To preserve the trust all weak spots have to be secure enough to prevent attackers from gaining unauthorized access to the system. Possible targets for attack can be the NFC-Reader, the wireless transmission channel, and the transponder. To secure the wireless transmission encryption algorithms like Elliptic Curve Diffie-Hellman (ECDH) for the key-exchange and Advanced Encryption Standard (AES) for the data encryption can be used. Unfortunately, the usage of such algorithms leads to an increased energy consumption. Figure 1.5 shows the power consumption of ECDH and AES. ECDH is executed first to securely exchange the secret key between two parties and consumes energy before any sensitive data is even transferred. As a second step the sensitive data is transferred encrypted by using AES and the secret key. This encryption leads to an increased average power consumption and time during the transmission. Finding a trade off between this power consumption and level of security is needed if the resources are a constraint in the NFC-System.

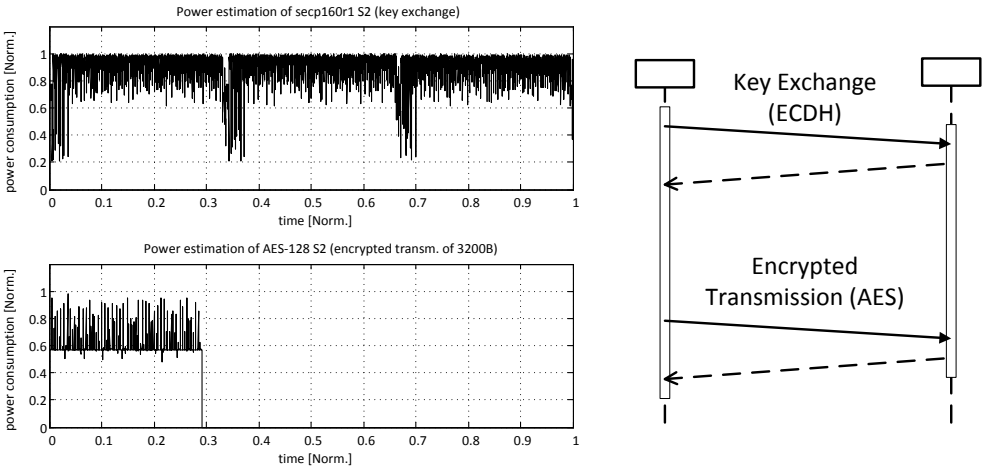


Figure 1.5: Abstract from the power estimation results of the key exchange (ECDH) and encrypted data transmission (AES) (adapted from [3]).

1.3.3 Challenge to Develop Power Optimized Systems

The developer of NFC-Systems, as described in Section 1.2, needs to include power optimization techniques in case of a violation of power-requirements (e.g., the system consumes too much energy). This inclusion can be divided into two steps. First, the developer has to find a suitable power optimization technique to remedy this violation. Second, the developer has to verify that the integrated optimization technique ensures that all requirements are now fulfilled.

Finding suitable power optimization techniques requires knowledge of the context and energy problem. There are several general guidelines available on how to implement optimization techniques as described in [15]. This leaves a gap between this guideline and the actual implementation. A more specific solution for a certain context and problem reduces the effort of integrating these techniques and reduces the risk of making mistakes. The principle of patterns is a possible solution to fill this gap, but as yet are not well established in the field of power-management for embedded systems. After finding a solution

and the integration of the solution into the design, the developer has to verify if the energy requirements are now fulfilled.

This verification of the energy requirements should be done in an early development phase to avoid costly redesigns. Therefore, verification techniques like simulation (63%), modeling (36%), virtual prototyping (32%), and graphical system design (31%) win on importance [16]. The inclusion of these verification techniques into the development process is important in order to force the developer to verify the system across the development phases. Adapting the Model Driven Architecture (MDA) is one possible approach, which uses model-based views on the system to develop. The Computational Independent Model (CIM) describes the use cases and (power-)requirements, the Platform Independent Model (PIM) consists of the design, and the Platform Specific Model (PSM) consists of the platform specific design and implementation. The MDA verification of the power requirements can now be done between the transitions of the development phases (model-based views). The power-verification tools are available for various levels of abstractions (e.g., SystemC transaction-level model, VHDL design), but due to the missing integration of these tools into MDA and the development process, this verification has to be done manually in a time consuming step. For this reason developers skip the verification in early development phases at the risk of costly redesigns.

1.4 The META[:SEC:]-Project

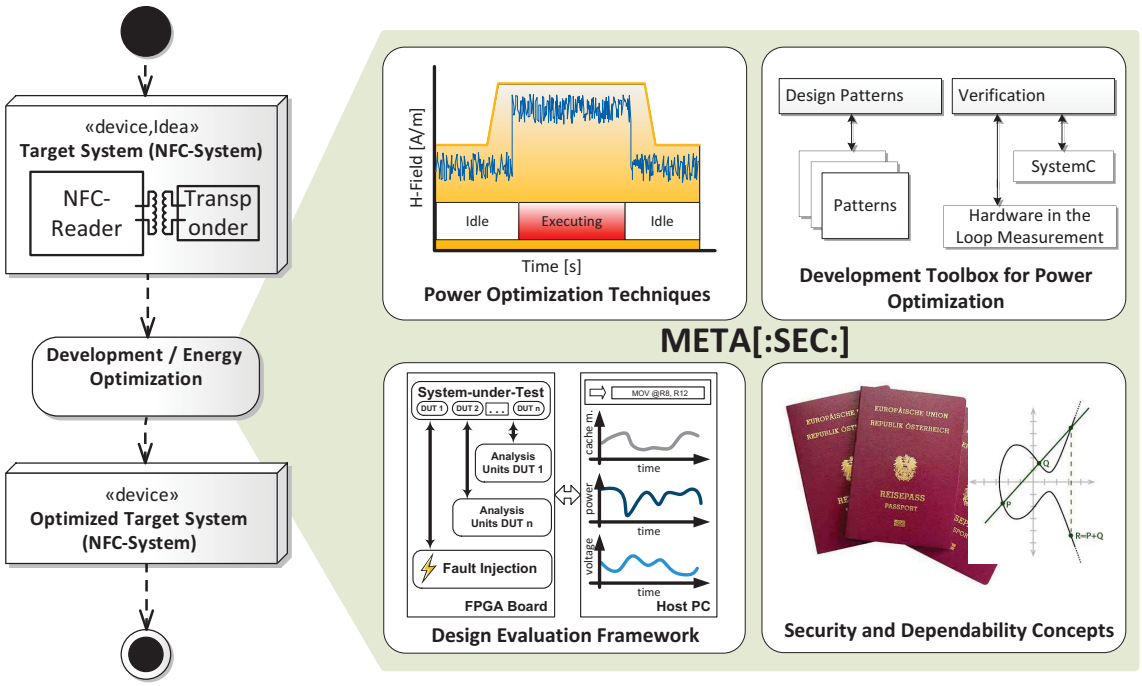


Figure 1.6: Flow to develop and optimize NFC-Systems and the four related topics of the META[:SEC:]-Project based on [4].

The project called META[:SEC:] was started to investigate RFID-Systems in four topics. One topic is dedicated to finding novel system based power optimization techniques.

There is particular focus on magnetic field strength scaling. The magnetic field provided by the RFID-Reader is used to supply the transponder. The required field strength depends on the physical relationship, e.g., the distance between the RFID-Reader and the transponder. The proposed optimization technique now tries to dynamically scale the field strength to save energy and to prolong the battery lifetime of the reader/transponder system. The focus of two other topics lie on power and fault aware hardware/software partitioning at the time of design, which involves defining/establishing a development toolbox for power optimization, and the creation of a design evaluation framework. This toolbox should be suitable to aid the developer in finding power optimization techniques (e.g., through using design patterns), and to verify power requirements across the development phases to perform the hardware/software partitioning. The design and evaluation framework is based on an emulation based tool to explore the design of a whole RFID-Systems. The fourth topic is concerned with the investigation, optimization and implementation of security applications, like the ePassport read by a customs officer. One goal is the evaluation of ECC for authentication and key exchange in the context of RFID-Systems. These four topics aim to solve issues in developing energy optimized RFID-Systems [4].

1.5 Problem Definition

The target systems of this thesis are NFC-Systems, which use RFID as technology. Therefore, the problem statement and the contribution is related to NFC. The following open issues in the context of NFC-Systems can be identified:

- New system based optimization techniques for mobile NFC-Systems are needed to reduce the energy consumption and prolong the battery lifetime of mobile systems.
- Using magnetic field strength scaling to optimize the energy consumption of NFC-Systems has been sparsely investigated.
- Publications regarding the relation between energy consumption and security exist, but further evaluations are needed in the context of optimization techniques and NFC-Systems.
- Patterns are well established in software development, but using patterns to describe solutions for power-management of embedded systems has been scarcely researched.
- Power verification tools for embedded systems exist but their integration into MDA and the development process is still a topic of research.

1.6 Contribution of this Thesis

The contribution of this work is based on topics of the research project META[:SEC:], which are shown in Figure 1.7. This thesis contributes in (1) power optimization techniques for NFC-Systems based on the topics of magnetic field strength scaling, and the power evaluation of security algorithms. The second contribution is (2) the development toolbox to apply and verify these optimization techniques across the development phases with the goal to realize power aware hardware/software partitioning at the time of design.

1. **Power optimization technique for NFC-Systems in two complementary implementations.** The optimization technique that has been contributed focuses on the idea of magnetic field strength scaling, with the goal of reducing the energy consumption of the NFC-System as defined in Figure 1.3. This technique is shown in two implementations. The first one scales the field strength once during detection phase. The second implementation extends the first one and allows dynamic field strength scaling during the whole communication. A case study has been created to show that magnetic field strength scaling can be used for multi-transponder applications. The field strength scaling technique depends on the transponder's energy consumption. This energy consumption also depends on the use of security. This consumption has been measured in a case study with different variants and strength of security, and energy optimized variants have been proposed for NFC-Bridges.

2. **Development toolbox for power optimization in NFC-Systems.** The two implementations of the contributed optimization techniques are used to mine patterns for power-management. Therefore, the pattern form had to be extended to be able to express these techniques. In addition, a proof of concept of power verification framework across the development phases has been implemented. This framework uses existing tools like SystemC and hardware in the loop measurements and enables verification across the MDA development process.

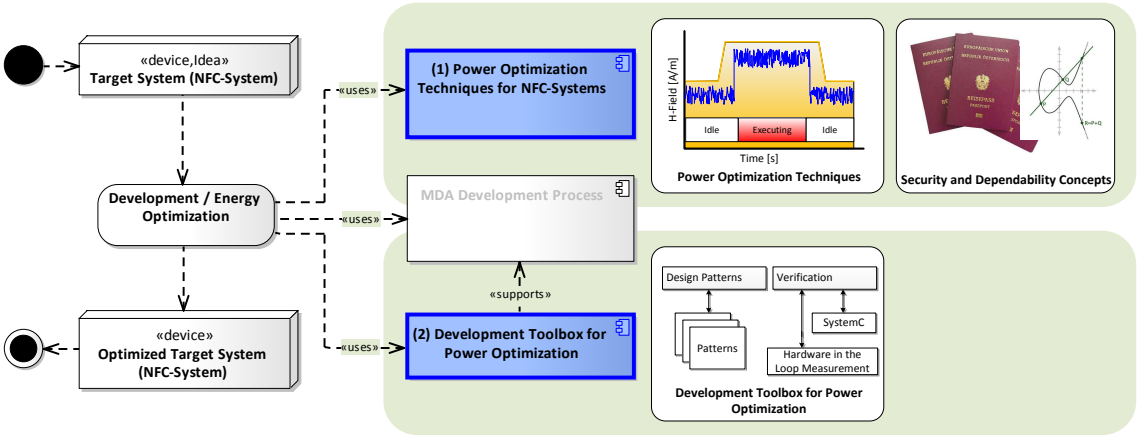


Figure 1.7: Link between the META[:SEC:]-Project and the contribution of this thesis [4].

1.7 Structure of the Work

This thesis is separated into six chapters. In Chapter 2 the related work and the difference to this thesis is presented. Chapter 3 gives an overview of the research done in terms of the optimization techniques, and Chapter 4 presents the development toolbox for power optimization. The experimental results are shown in Chapter 5. The conclusion and future work of this thesis is presented in Chapter 6. The final Chapter 7 presents the related publications made during the research.

Chapter 2

Related Work

This chapter describes the related work in four sections. The first section shows existing work on power optimization techniques for the domain of NFC. Additionally, publications regarding security and its impact on energy consumption are shown. The second section regards using design patterns for power optimization. Existing tools for power optimization and verification and works regarding power optimized development by using MDA are discussed in the third section. The final section presents the thesis difference to the related work. The description of the related work is done in respect to the NFC target system as defined in Section 1.2.

2.1 Power Optimization Techniques For NFC

2.1.1 System Based Power Optimization

Power optimization is often performed by optimizing single components of the system. This can lead to success, but for further improvement the whole system has to be considered. An example is NFC in reader/writer-mode, where the NFC-Reader wirelessly transfers the power to the passive transponder. Without regulating this power transfer in the NFC-System, energy will be wasted. The first step needed to develop new optimization techniques is to explore the system. Unsal et al. make a layer-by-layer survey of this system and use the results to develop power optimization techniques. This work focuses on real-time systems, but can also be applied to others [17]. Exploring the system and optimization on higher abstractions like the network layer (e.g., power aware routing strategy) is shown in the work of [18]. For such abstract views, generalized power-management architecture like the observer-controller can be used [15]. This architecture observes internal states, and controls defined parameters in the system, like the wireless power transfer in NFC. The algorithm for the observer-controller has to be implemented with the goal of saving energy.

This generalized power-management architectures can also be used for the domain NFC. A technique for energy provisioning on the network layer for systems based on RFID (underlying technology of NFC) is shown by [19]. They observe the information acquired from the investigated multi-transponder multi-reader system and control this system with the goal of saving execution time and energy. This provisioning service is similar to the observer-controller architecture. Such optimizations are important for mobile battery

powered RFID-Readers [20]. The implementation of such an architecture in complex systems is a challenge due to the difficulty of finding the correct internal states to observe and to control the system. One possible approach for such complex systems is the Cinder operating system. This operating system is designed for smart phones. The underlying model used to optimize the power consumption can be extended to include consumptions like the wireless power transfer in NFC [21].

2.1.2 Power Optimization through Controlling the NFC Power Transfer

It has already been discussed that one way to power optimize the system is to optimize the wireless power transfer (see Chapter 1). In terms of using the observer-controller architecture one solution can be to observe the power-consumption of the transponder and control the transfered power on the NFC-Reader side. To design an algorithm to save energy, two considerations have to be made. To know how the wireless power transfer works is the first consideration. A description based on a two-port model of this power transfer is shown by [22]. With this model the maximum power transfer efficiency can be evaluated. Another work by [23] shows the equations for the relation between the transmission distance and the transferred power from the NFC-Reader. The power transfer is based on inductive coupling, which implies that the NFC-Reader uses a magnetic field for this transfer. The field strength decreases with the power of three in relation to the distance of the NFC-Reader [24]. To ensure a certain transmission distance this field strength provided by the NFC-Reader is set to the minimum strength needed to supply a transponder at this distance. For example RFID-Readers according to ISO 14443 have to provide a static magnetic field between 1.5 and 7.5 A/m [25]. The required field strength of the transponder is lower, which concludes that for smaller distances this transponder will be oversupplied. The work of [26] scales the power transfer in UHF-RFID (uses electromagnetic field for power and data transmission) to save energy in an application to detect transponders in transmission range. They were able to reduce the energy consumption of the RFID-Reader by up to 60% in this application. The wireless power transfer also depends on the misalignment of the NFC-Reader and transponder, which is the second consideration to be made. Models like the one of Kyriaki Fotopoulou et al. can be used to consider this misalignment. This equation based model is restricted to circular shaped coils for a single NFC-Reader and transponder [27]. Multiple transponders mutually influence the power transfer. The work of [28] investigates this mutual influence from one RFID-Reader using a carrier-frequency of 13.56MHz, as used in NFC, to two transponders, and presents equations to calculate the power transfer in this environment.

2.1.3 Security requirements in NFC

The lower layers of the NFC standards do not demand the integration of security. As some applications, like wireless payment or access control, have to be secure, this means that security has to be introduced on the application level. An unencrypted and unauthenticated wireless transmission can lead to loss of privacy and data integrity. In the work of Haselsteiner et al. threats like eavesdropping and countermeasures like RSA and AES are discussed [29]. Unfortunately, encrypting the wireless communication is not sufficient to secure the whole system. Sensitive data can be stored in secure elements, like

the Subscriber Identity Module (SIM) card of the smart phone. The application has to communicate with this element, to retrieve this required data. If this communication is not secured, an attacker has additional weak spots (attack vectors) to exploit the system [30]. Before communication partners exchange sensitive information, an authentication should be done. The work of [31] presents an approach for mutual authentication in the domain of wireless sensor networks, with the benefit that both partners know that they are communicating with the correct one. Digital signatures are a way of proving authenticity. The usability of such digital signatures in the domain of RFID-Systems is shown by [32]. Before sensitive data can be encrypted, both communication partners have to know the same secret key. The exchange of such a key can be done by using asymmetric encryption based on ECC. In the work of Aigner et al. a co-processor for smart cards is presented and evaluated in terms of its performance (clock cycles) [33]. The work of Alrimeih et al. compares ECC in timing and performance with different levels of security [34]. ECC can also be used on an 8-bit AVR-based RISC processor as shown by [35]. The integration of security occurs on multiple layers of abstractions. Encryption/decryption can be done by a co-processor in hardware (required security algorithms), but the security policy is application dependent [36].

Integrating security means providing the appropriate security for the targeted application. It is essential to choose the required level of security, particularly in resource constrained systems. In the National Institute of Standards and Technology (NIST) publication of Barker et al. recommended levels are described as well as how long they will be secure enough for. A security strength of less than 80 bits is no longer recommended in 2014 by the NIST, while strengths of 112 bits are acceptable till 2030 [37]. Also in the work of Ravi et al. the need to choose the ”right” security is discussed. Using co-processors and other hardware can counter the resource constraints, such as power, of embedded systems [38]. The work of Eisenbarth et al. shows a survey of symmetric and asymmetric ciphers for embedded systems in terms of their performance [39]. Internal communication buses also have to be secured particularly in secure elements. These secure structures have to be as lightweight as possible. The publication of [40] shows an implementation of a trusted sensor in respect to optimization to fulfill resource constraints. A solution for secure transmission over a bus by using a simple XOR is shown by [41].

2.1.4 Role of Security in the Power Optimization of Embedded Systems

As addressed in the former section, considering resource constraints such as power is important when adding security. The work from [42] discuss this importance, and presents new security mechanisms by considering the energy costs of the design. To know the ”energy costs” of a security algorithm evaluations and measurements have to be made in advance. Wander et al. [43] made measurements of public-key cryptography, like RSA and ECC, for wireless sensor networks, and compared the energy results of the different algorithms. They achieved 4.2 times the number of key exchange operations with ECC 160 compared to RSA 1024. Another work from Trakadas et al. is dedicated to measuring authentication and key exchange algorithms on wireless sensor networks, and concludes that ECC is the most power saving algorithm [44]. There are several surveys on encryption algorithms, like the one from [45] which shows evaluations on ECC in terms of its power-consumption on 8-bit platforms, and the work from [46] showing an investigation of the

power-consumption from symmetric cryptography like DES and AES. These surveys can be used to consider security in the process of developing new power optimization techniques for embedded systems.

2.2 Patterns for Power Optimization

Optimizing a system and proposing solutions for specific problems and domains is done in a lot of publications. Also design patterns describe solutions, but the difference is that they present a reusable solution to an occurring problem. They are based on specific solutions for one common problem and describe the general solution to solve them all (also called mining of patterns). The work of [47] describes what makes out a design pattern in nine different characteristics. Design patterns can be mined for different levels of abstractions. One of them is conceptual patterns, which describe solutions for system structures consisting of hardware and software [48]. This shows that design patterns are not restricted to software, and can also be used for hardware designs.

Hardware Intellectual Properties (IP), which are reusable hardware components, are common in hardware development. The work of [49] presents a solution for translating these IPs into design patterns for hardware. They translate the hardware description of the IP to a more general system description language called SystemC. [50] show how aspect-oriented programming (AOP), SystemC and design patterns in combination can be used to verify system designs.

Design patterns also exist to provide solutions for resource-management for e.g., memory, CPU [51]. The work from [52] presents design patterns for small memory systems. One resource is power, which is also of importance for embedded systems. There are publications regarding the emerging power overhead when using specific design patterns [53]. A solution proposed by [54] is to define power profiles for each design artifact (design pattern). These power profiles can be used to evaluate the power consumption when using the design pattern's solution. There is also a publication from [55] where a design pattern is used reduce the power-consumption of the system. There are also other works about design patterns for power-management, like the one of [56], which provides the solution of using the power gating of wires to save energy.

2.3 Power Optimization for Embedded Systems in MDA

2.3.1 Power Requirements and Verification in MDA

An approach for designing embedded systems is Model Driven Architecture (MDA). This approach uses three model-based views of the embedded system. The first one is the Computional Independent Model (CIM) showing the use cases and requirements, the second one is the Platform Independent Model (PIM) used for the design, and the third is the Platform Specific Model (PSM) for the platform specific design. This structured approach separates the development into three different levels of abstraction based on these views, but with the advantage that the transitions are defined and the abstractions remain connected to each other. This helps the developer to keep track, for example, of which part of the design is needed for a certain requirement. MDA can be used to design complete systems consisting of hardware and software. The work of [57] presents how model-based

approaches like MDA and SystemC can be combined in a System on Chip (SoC) design. [58] show how to integrate other system- and hardware description languages, like SpecC and ImpulseC, into the approach of MDA. An important part of developing systems is the verification of the design to find out if the requirements are met for a certain test case. MDA uses UML for it's models and diagrams and one type is the sequence diagram, which is a graphical description of an execution order. This sequence diagram is suitable for describing a certain test case to verify the requirements [59]. Design space exploration is used to explore the possibilities to design a system. The integration of such tools such as a simulation is shown by from [60]. Another work by [61] shows how to integrate hardware in the loop measurements into the MDA approach. Both simulation and and hardware in the loop measurement open the path to verify even non-functional requirements like power.

To describe such non-functional requirements, notations in UML are required. [62] present Modeling and Analysis of Real-time and Embedded systems (MARTE) to describe such non-functional requirements. The work of [63] focused on how to model and analyze non-functional properties in Model Driven Development (MDD). An MDA framework to include and verify non-functional requirements is presented by [64]. One non-functional requirement is power. In the work of Dhouib et al. a language used to perform power estimations in MDA called AADL (Architecture Analysis & Design Language) is proposed [65]. [66] also discuss how the combination of estimation tools and MDA can be used to create power-aware systems.

2.3.2 Power Evaluation and Verification Tools

To power optimize an embedded system tools are needed to verify its design or implementation. This should already be part of an early design stage. Possible tools are simulations, emulations, or hardware in the loop measurements. The SystemC framework has been extended by [67] to evaluate the power consumption by simulation of the design. SystemC is also used by [68] to perform power simulations. [69] developed a tool called PK tool to separate the functional design from the power state machine required for power simulations. This makes it possible to add a power description to every model without changing the functional design. A way of using power state machines has been described by [15]. These state machines can be used as MARTE extension to describe power profiles [9]. The DIPLODOCUS tool from [70] based on TTool is a toolkit for UML and SysML to be able to simulate and formally verify SoC models by these power state machines. A power-emulation tool for SoC'S is described in [11]. The benefit lies in the emulation time compared to simulation time. In the work of [11] the evaluation of AES 128 took 17.2h in simulation and only 13.5μs in emulation. A drawback of the emulation technique is the requirement of a time consuming power characterization before it can be used. Hardware in the loop measurements require real hardware. They are the last step in the verification process, or used to characterize hardware components that have already been implemented for a new system under design. An example is provided by [71] who used the measured power values to create a power model to evaluate software.

2.4 Conclusion and Difference to Related Work

Power optimization techniques exist in several abstraction levels. One more general approach is the observer-controller mechanism. In the domain of NFC, several component based power optimization techniques are used. The wireless power transfer is identified as a viable point to save power. There are approaches to make the power transfer more efficient. Other investigations are made in terms of considering and optimizing the power consumption of the security algorithms used. Patterns to describe solutions for occurring problems is well established in software development. Mining patterns for hardware wins on importance, and approaches exist to translate harware IPs into SystemC and to use these in mining design patterns. A rather new field is using design patterns for power management in embedded systems. There are some analogical approaches to describe solutions for power-management for a common problem rather than only describing a specific solution. The importance of verifying power requirements throughout the development process is also identified in several publications. There are several works on how to consider non-functional requirements in the development with the MDA approach. Possible solutions for the integration of simulation and hardware in the loop measurement into MDA have been published. The thesis contribution differentiates the following points:

- **System-based power optimization technique and implementations for NFC-Systems.** There are several solutions for embedded systems, RFID, and smart cards which propose component based optimizations, like optimizing the power consumption of the smart card or optimizing the wireless power transfer itself. This thesis proposes a system based approach in respect to this related work for NFC.
- **Consider the wireless power transfer used in NFC (uses inductive coupling) in the design of the thesis power optimization technique.** There is related work on the optimization of the wireless power transfer for the underlying technology of NFC. Also a publication exists for UHF RFID, which take the wireless power transfer (uses electromagnetic field) into account. This thesis proposes an approach to consider the power transfer used in NFC in respect to the existing work.
- **Using patterns to create a development toolbox for power optimization.** Several publications exist regarding patterns for software, hardware, and dealing with non-functional requirements like memory in the design. The thesis differentiates by extending the pattern's form and mining patterns for power-management in embedded systems as part of a development toolbox.
- **Integration of power verification across the design phases as part of a development toolbox for power optimization.** Several publications and tools exists for verification and design space exploration. In this thesis existing tools are integrated into the MDA approach to provide a power verification toolbox across the development phases.

Chapter 3

Power Optimization Techniques

This chapter presents the thesis contribution to power optimization techniques for NFC-Systems. In the first section the wireless power transmission model and its underlying equations are described. The next two sections describe the proposed technique of magnetic field strength scaling and the two complementary implementations. Section 3.4 shows a case study that applies this technique for multi-transponder applications. Another case study addressing power evaluation and optimization of security in NFC-Systems (NFC-Bridge variant) is shown in Section 3.5.

3.1 Wireless Power Transmission Model

Designing and implementing new power optimizations techniques requires a model of the system. In our case the optimization technique should consider the whole NFC-System including the wireless power transmission from the NFC-Reader to the transponder. Conclusively to develop this model, replacement circuits and equations have to be chosen for this power transmission, which can be subdivided into four parts as shown in Figure 3.1.

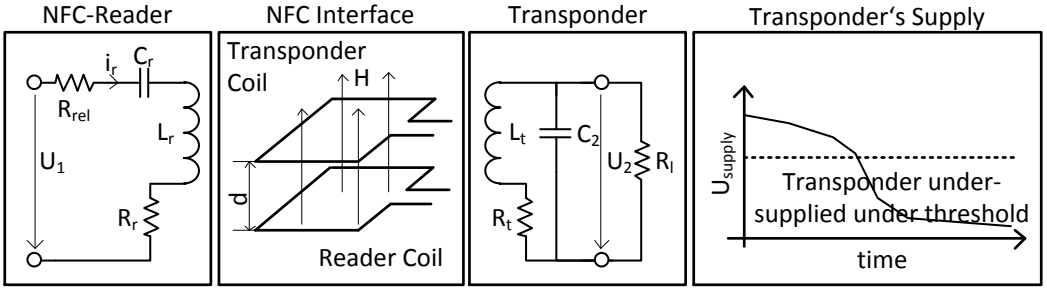


Figure 3.1: Overview of the wireless power transmission based on inductive coupling as used in NFC (adapted from [5]).

The first part is described by the mathematical equation (3.1) and the replacement circuit shown in Figure 3.1, and represents the control of the wireless power transfer by the NFC-Reader. The transmission power, represented by the current i_r over the NFC-Readers coil, is controlled by the resistance R_{rel} in series to this coil (C_r, L_r, and R_r). The amplitude of the carrier U_1 remains constant (frequency is 13.56MHz). Increasing R_{rel}

reduces the power transfer and conclusively the overall power consumption ($P = i_r \cdot U_1$) of the NFC-Reader decreases. The resulting current i_r not only depends on R_{rel}, but also on the coils impedance Z_c which consists of C_r,L_r, and R_r according to the replacement circuit used. Through the mutual inductance, the impedance of L_r depends on the physical orientation and distance of the NFC-Readers coil to the transponders coil. (3.1).

$$i_r = \frac{U_1}{Z_c + R_{\text{rel}}} \tag{3.1}$$

The second part is described by equation (3.2) representing the wireless power transmission over inductive coupling (magnetic field H) to the transponder. This equation uses i_r as input parameter and is valid as approximation for two rectangular-shaped and coaxial oriented coils based on the law of Biot-Savart [25].

$$H = \frac{i_r \cdot N_r \cdot a_r \cdot b_r}{4 \cdot \pi \cdot \sqrt{(\frac{a_r}{2})^2 + (\frac{b_r}{2})^2 + d^2}} \cdot (\frac{1}{(\frac{a_r}{2})^2 + d^2} + \frac{1}{(\frac{b_r}{2})^2 + d^2}) \tag{3.2}$$

The required parameters are the NFC-Readers coil diameters a_r and b_r, the number of windings N_r and the distance d to the transponder coil (shown in Figure 3.2).

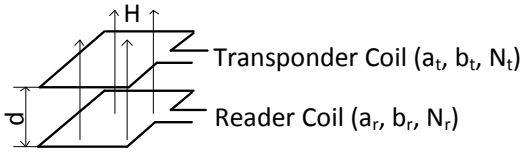


Figure 3.2: Considered coaxial orientation of coils (obtained from [6]).

The third part is described by equation (3.3) representing the transformation of the magnetic field strength H to the voltage U_2 available to supply the transponder. The inductivity of the transponders coil L_t and C_2 build a resonance circuit tuned to the frequency of 13.56MHz to improve the energy transmission. Further required parameters to calculate the output voltage are the transponder's coil diameters a_t and b_t, the number of windings N_t, the coil's resistance R_t, and the transponder's load represented by R_l. This equation is only valid for rectangular-shaped receiver coils as described in [25].

$$U_2 = \frac{\omega \cdot \mu_0 \cdot H \cdot N_t \cdot a_t \cdot b_t}{\sqrt{(\frac{\omega \cdot L_t}{R_l} + \omega \cdot R_t \cdot C_2)^2 + (1 - \omega^2 \cdot L_t \cdot C_2 + \frac{R_t}{R_l})^2}} \tag{3.3}$$

The fourth part describes the power supply of the transponder's digital circuit. The resulting resistance of the power supply and the digital circuit is represented by R_l. It is common, that the transponder uses a shunt resistance to regulate the input current and conclusively the supply voltage. The input voltage U_2 is rectified to the supply voltage U_{supply}. If the supply voltage drops below a certain threshold, the digital circuit of the transponder is under supplied and is powered down. In Figure 3.3 a plot of the impact from the transmission distance d to the voltage supply U_{supply} (result of simulation) is shown. Different values for the parameter of the transmission power represented by i_r are shown as comparison. The plot shows that U_{supply} decreases with a higher value of d and

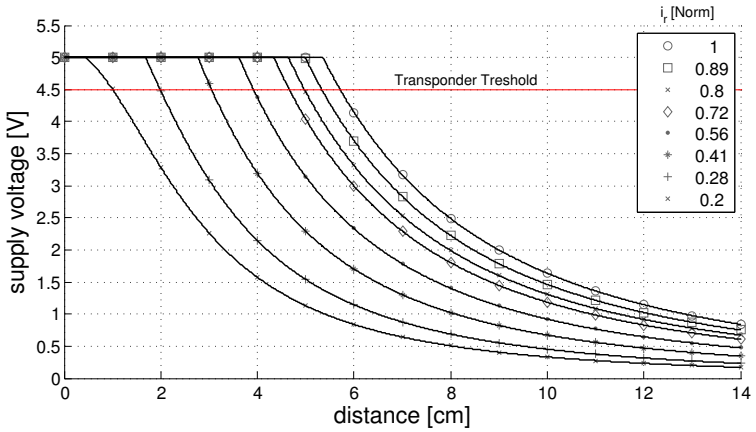


Figure 3.3: Relation of the transmission distance d to the supply voltage u_2 of the transponder (obtained from [6]).

a lower i_r (parameter). A proper supply to the transponder (above the threshold) is only achieved with a certain level of i_r within a certain transmission distance d.

These parts are used to include the wireless power transmission in the model of the NFC-System by using the system description language SystemC. The top level module diagram of the model is shown in Figure 3.4. The first module is the NFC-Reader with its required functional implementation and the described first part of the wireless power transfer. The wireless power transmission module implements part two and a feedback response (e.g., to model the mutual inductance) for the first part. The transponder module consists of the functional implementation and part three and four of the wireless power transmission. The data transmission module is used to model the data transmission between NFC-Reader and transponder. This SystemC model is used to simulate and verify power optimized designs. Derived models are created through additional requirements and variants of the investigated system as shown in Section 1.2 (e.g., NFC-Bridge).

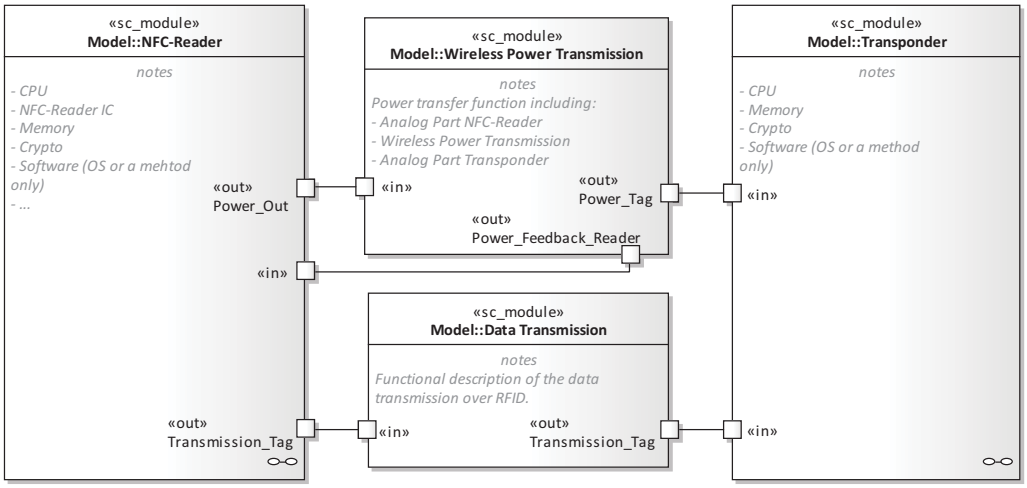


Figure 3.4: Top level view of the SystemC model from the NFC-System.

3.2 First Implementation: Initial Field Strength Scaling (FSS)

As previously mentioned the idea of magnetic field strength scaling as an optimization technique is to reduce the magnetic field strength dynamically to the minimum required strength to supply the transponder. Figure 3.5 illustrates this basic idea.

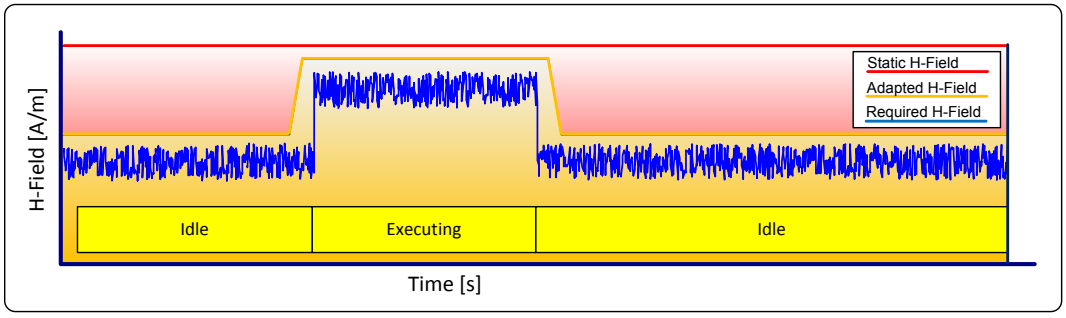


Figure 3.5: Basic idea behind magnetic field strength scaling for NFC-Systems by adapting the provided field strength of the NFC-Reader over time to just ensure a proper supply to the transponder (adapted from [4]).

The first implementation uses the transponder detection phase to properly scale the magnetic field strength (as shown in Figure 3.6). If the NFC-Reader detects a transponder in range, it sends a simple request (e.g., REQA) and an anti-collision (required to communicate in a multi-transponder environment) command to establish a connection. The response to this anti-collision command is the unique identifier (UID) of the transponder. After the NFC-Reader is aware of all transponders in range it can select and establish a connection to one. All other transponders in range will not answer commands sent until they are selected. During this detection phase, data between NFC-Reader and transponder is exchanged. This data exchange during the detection phase is used as one part for the first implementation of the magnetic field strength scaling technique [7].

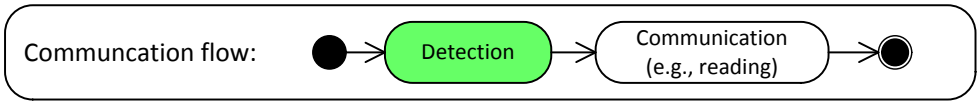


Figure 3.6: Basic communication flow between NFC-Reader and transponder showing in which phase (filled) the magnetic field strength scaling is executed for the first implementation.

The algorithm used is based on the observer-controller technique from [15]. The observed parameter is the distance between the NFC-Reader and transponder and the controlled process value is the magnetic field strength (H-Field) on NFC-Reader side. The distance parameter cannot be directly be measured during runtime. However, one known parameter during runtime is the resistance R_{rel} which controls the current wireless power transfer and conclusively influences the transponders ability to respond through a proper supply. Acquiring two values of R_{rel} at the transition from a proper supply to an undersupply of the transponder is sufficient to determine the distance and to control the magnetic field strength to properly supply the transponder.

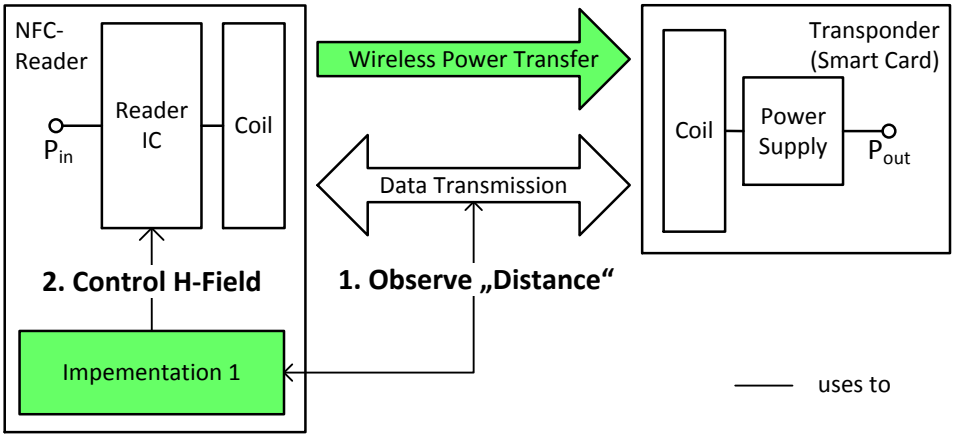


Figure 3.7: Architecture used for implementation 1 of the magnetic field strength scaling technique (adapted from [7]).

One disadvantage of this approach is that the field strength has to be altered multiple times to find this point of transition. This is not a problem during the detection phase except for the additional timing overhead, but is not possible during the actual communication because of the requirement of maintaining the transponders proper supply during this phase. This also implies that changes in distance between the NFC-Reader and transponder during the communication phase may lead to an undersupply or oversupply of the transponder [7]. The experimental results from this implementation are shown in Section 5.3.

3.3 Second Implementation: Dynamic Field Strength Scaling (DynFS)

This second implementation extends the first one to deal with the issue of not being able to scale the field strength during the communication phase. Scaling during the communication phase aims to avoid an undersupply or oversupply of the transponder when e.g., the distance between NFC-Reader and transponder changes. This implementation is able to rescale the field strength during all phases (shown in Figure 3.8).

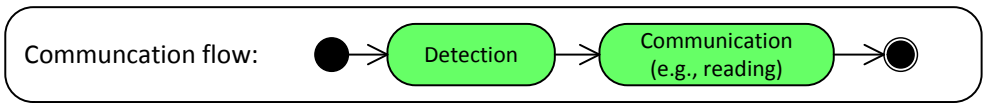


Figure 3.8: Basic communication flow between NFC-Reader and transponder showing in which phase (filled) the magnetic field strength scaling is executed for the second implementation.

The solution is split into two parts. In the first part, distance changes between NFC-Reader and transponder are detected. Such changes occur occur, for example, through pushing the access card (transponder) towards the terminal (NFC-Reader). The approach

of sweeping through the possible field strength values as in implementation 1 would result in an increased timing overhead and potential loss of connection. Therefore, this part of the solution observes the electrical current i_r over the NFC-Reader's coil. The value of this current depends on the distance between the NFC-Reader and transponder as described in Section 3.1. This dependence can be used to control the field strength by R_{rel} when a change in distance is detected. The second part deals with scaling the magnetic field strength when the transponder's power consumption changes. In our case we assume that such changes occur only when requests (e.g., reading data from the transponder) are sent from the NFC-Reader to the transponder. These requests are observed to control the magnetic field strength in advance. These two parts of the solution are combined in an observer-controller architecture to dynamically scale the field strength for both changes in distance and power consumption of the transponder across the detection and communication phase as shown in Figure 3.9 [5].

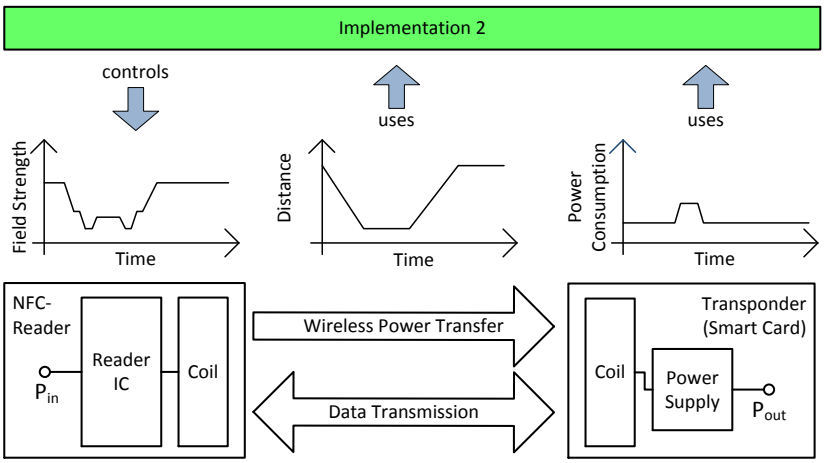


Figure 3.9: Concept used for implementation 2 of the magnetic field strength scaling technique (adapted from [5]).

One drawback of this implementation is that the dependencies of the NFC-System between i_r, the transponder's power consumption and the required field strength have to be known. One approach to obtain these dependencies is to characterize the system using a predefined procedure and to provide the results as lookup table. The experimental results from this implementation are shown in Section 5.4.

3.4 Case Study: Field Strength Scaling for Multi-Transponder Applications

Both implementations that have been described do not support multi-transponder applications, like holding a briefcase with an access card (tranponder) and other transponders against an access terminal (NFC-Reader) to gain access to a building. Multiple transponders in range of one NFC-Reader influence the wireless power transfer and the power consumption of a certain transponder depends on whether it is selected or not. The field strength scaling implementation has to be extended to deal with these occasions. The

implementation for this multi-transponder case study is based on the first implementation and extends the detection phase for multiple transponders (as shown in Figure 3.10).

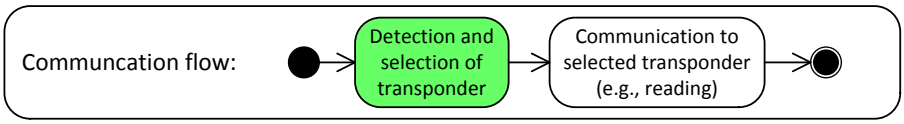


Figure 3.10: Basic communication flow between NFC-Reader to multiple transponders showing in which phase (filled) the magnetic field strength scaling is executed.

The detection phase extension, as shown in Figure 3.11, is capable of evaluating the required field strength to communicate with a certain transponder (e.g., the access card). As in the first implementation the transition (two values of R_{rel}) is determined to proper supply the desired transponder. The proper supply of the rest of the transponders is ignored by the algorithm to reduce the energy consumption to minimum [8].

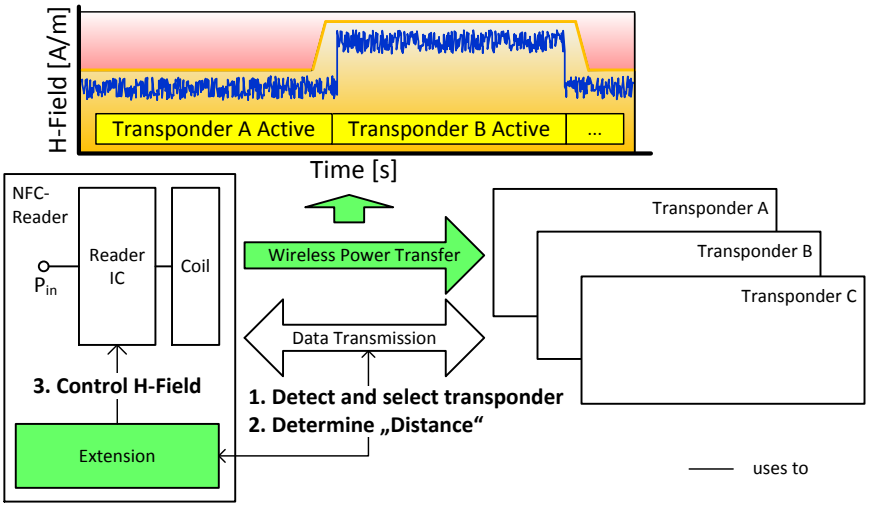


Figure 3.11: Architecture of the NFC-System used for the case study of magnetic field strength scaling for multiple transponders (adapted from [8]).

This case study uses this extension during the transponder detection phase and evaluates its behavior in terms of power consumption, stability and liabilities of using magnetic field strength scaling in a multi-transponder environment. The experimental results from this implementation are shown in Section 5.5.

3.5 Case Study: Power Optimization for Secure NFC-Bridges

The impact of the proposed implementations of the magnetic field strength scaling technique depends on the power consumption of the transponder. A greater power consumption requires a higher field strength to supply the transponder at the same distance. One part, which has an impact on the power consumption is security. Therefore, a case study has been made using an implementation of the NFC-Systems variant called NFC-Bridge

as described in Section 1.2. The reason for using such an NFC-Bridge for evaluation is that it combines all aspects of exposed communication like the wireless data transmission, the contact based communication, and bridging of data to an embedded system. As shown in Figure 3.12, three exposed paths of communication A,B, and C were identified [3].

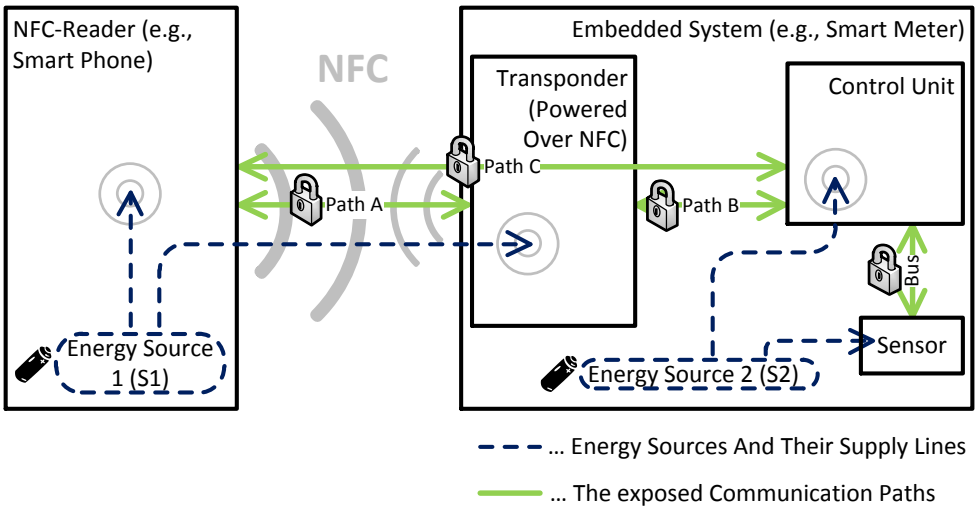


Figure 3.12: Overview of the investigated system, the exposed communication paths (Path A, B, C), and the two energy sources S1 and S2 including their dependencies on what they supply (obtained from [3]).

These paths are secured by using asymmetric cryptography (ECDH) for the key exchange and symmetric cryptography (AES) to encrypt the data transmission. The choices of ECC and AES were taken according to the related work as described in Section 2.1. The security implementations are evaluated in terms of their power consumption of both energy sources of the smart phone and the embedded system. Details of the results of the evaluation are shown in Section 5.6.

Chapter 4

Development Toolbox for Power Optimization

This chapter describes the contribution of this thesis in creating a development toolbox to power optimize NFC-Systems (as shown in Figure 4.1). This toolbox consists of mined patterns of the proposed specific solutions of optimization technique to make them applicable for a developer and to provide the necessary verification tools to develop power optimized NFC-Systems. The first part of this toolbox consists of a set of patterns which use an extended pattern form for power-management to provide solutions for power optimization problems that occur. In Section 4.1.2 an example is given in the form of an abstract from the *Energy Valve* pattern (based on magnetic field strength scaling). The second part describes the developed power verification framework for NFC-Systems. This framework aids the developer across the development phases of MDA by using commonly used simulation tools for the design, and the hardware-in-the-loop tools for the implementation. This framework integrates these tools into the verification phases of MDA and has been developed to reduce the development time and costs.

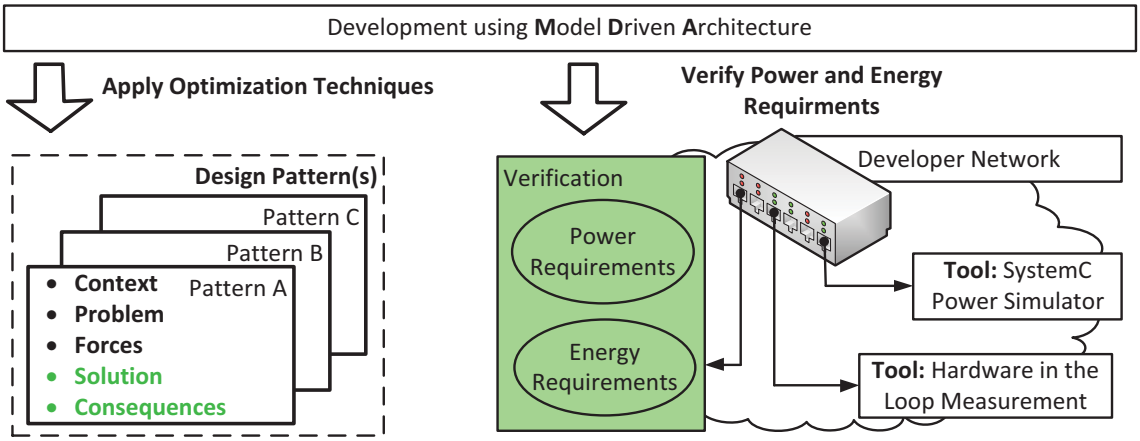


Figure 4.1: Overview of the proposed development toolbox consisting of a set of power-management patterns, and the integration of power verification tools into MDA.

4.1 Patterns for Power-Management in NFC-Systems

The purpose of patterns is to describe a systematic solution for a occurring problems. The use of patterns is well established in software design. However, as presented in Section 2 patterns for power-management in embedded systems are scarcely available. The contribution of this thesis is separated into two parts. First, the forum of the pattern is extended to improve the description of the problem, solution, and consequences for power-management patterns. The second part is dedicated to mining patterns with this extended form for the proposed solutions based on magnetic field strength scaling. An example is given by describing parts of the *Energy Valve* pattern in this section.

4.1.1 Extension of the Pattern Form for Power-Management

The form of the pattern includes the sections "Context", the occurring "Problem" which should be solved by this solution, the "Solution" itself, and the "Consequences" of applying this pattern. The common description has proven to be sufficient for most domains as for software design. In case of power-management the problem to solve arises by not fulfilling a certain power requirement. The designer requires a quantitative statement, like "How much energy in percent can be saved by applying the patterns solution?" Therefore, the extension shown in [10] is proposed as a contribution to this thesis. The basic structure, based on [51], and is extended in four parts.

- **Extension of the dynamics section:** The dynamics section describes the functional behavior of the design patterns solution. The proposed extension appends the power behavior in form of a power profile called MARTE [9]. The structure of this power profile is shown in Figure 4.2 and consists of instances of *HwPowerConfiguration*, which describe the system configuration with and without using the patterns solution, instances of *HwComponent* which describe the power consumption of the systems components, and instances of *PowerStateMachine* which are power state machines used for more complex power descriptions of one specific component. The power behavior is domain specific and requires input parameters. These required input parameters are stated in an object indicated by the stereotype *Parameters*.

- **First extension of the consequences section:** The appended power profile in combination with a power mode diagram in the consequences section allows the calculation of the energy consumption with (guard "with $< patternName >$") and without (guard "without $< patternName >$") using the patterns solution.

- **Second extension of the consequences section:** Using the pattern has benefits and also liabilities in terms of the power consumption. These can be calculated with the energy results of the power mode diagram and by using equation (4.1). The saved energy E_{saved} is calculated by subtracting $E_{solution}$ (with the patterns solution) from $E_{original}$ (without using the patterns solution). This may also lead to a liability if E_{saved} becomes negative.

$$E_{saved} = E_{original} - E_{solution} \tag{4.1}$$

- **Third extension of the consequences section:** To get a rough estimation of the pattern's impact on the energy consumption, domain specific values and references to specific solutions are added to the consequences section (tagged with "Known impact to energy consumption").

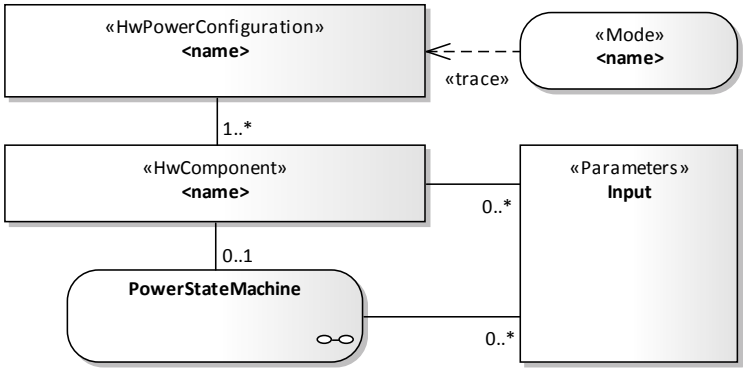


Figure 4.2: Component diagram showing the structure of the power profile and the power modes based on [9] (obtained from [10]).

4.1.2 Energy Valve - Pattern for Magnetic Field Strength Scaling

One mined design pattern for power-management as a contribution to this thesis is *Energy Valve*. This pattern describes the solution of magnetic field strength scaling in a more general form to cover problems occurring in power-management. In terms of the NFC-System the "Provider" is the NFC-Reader, the "Consumer"' is the transponder and the "lossy path" is the wireless power transfer over NFC. Only abstracts of this design pattern are shown in this section, however the complete version is described in [10].

Context of the Pattern

The context section describes the dedicated environment of this design pattern. In case of *Energy Valve* this section is written as follows: *"The system consists of a provider and a consumer, where the provided energy of the attached consumer can be controlled during the communication between the provider and the consumer to reduce the energy consumption of the provider. The provider can only transfer energy over a lossy path and has a communication channel available to the consumer."* [10].

Problem to solve

The problem section describes the occurring problem, which is in this case the power constraints, and is written as follows: *"Through the limitation of the available energy the transferred energy to the consumer should be the same as the needed one. The rest of the transferred energy is lost (sink). The provider does not know how much energy the consumer needs. How can the provider get the information how much energy needs to be transferred?"* [10].

Power Profile

The appended power profile (Figure 4.3) in the dynamics section of *Energy Valve* describes the overall power behaviors of the system required to calculate the system's consumed energy with and without using this pattern. Some profiles like the one of the consumer can be described as static values (NFP_Power). Other more complex behaviors require power state machines. The required input parameters are stated in the *Input* object. These parameters are the maximum transmission power P_{trans_max} from the provider, the consumer's power consumption $P_{consumer}$ and the lost power P_{lossy_path} over the lossy path. In the case of the NFC-System this power loss can be calculated by the equations described in Section 3.1.

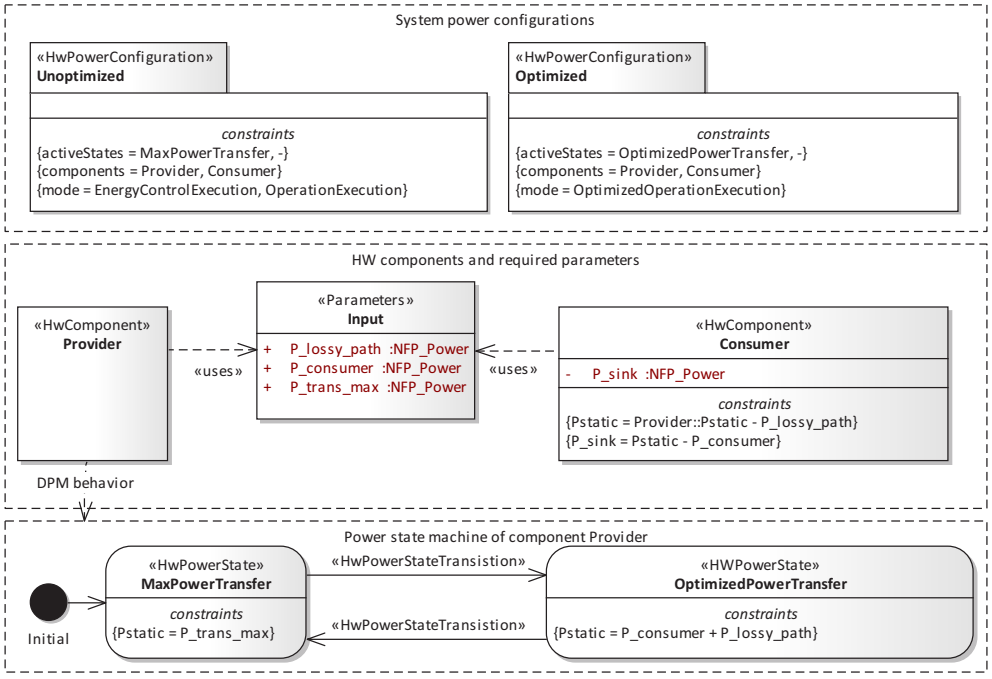


Figure 4.3: Power profile needed to evaluate the *Energy Valve* pattern's impact to the energy consumption of the system under design (obtained from [10]).

Consequences

The three extensions of the consequence section are adding a power mode diagram (example shown in Figure 4.4), defining the benefits and liabilities to the energy consumption, and describing a known impact from a specific domain. In case of *Energy Valve* these extensions are described as follows:

- "**Benefit on energy consumption.** The pattern is able to reduce the energy consumption of the system, even the components themselves are energy-optimized. The saved energy E_{saved} through the usage of the *Energy Valve* pattern can be evaluated using the power state diagram as shown in Fig. 4.4 following the path with the guard "without EnergyValve" to evaluate $E_{original}$, and "with EnergyValve"

to evaluate $E_{solution}$. The diagram uses the power profile described in Fig. 4.3 as basis. t_{setup} is the time needed for the energy control. $t_{operation}$ is the time needed for the actual operation. $E_{original} - E_{solution}$ defines the resulting benefit."[10].

- "**Liability on energy consumption.** The design of the pattern includes an overhead through the state "EnergyControlExecution" as shown in Fig. 4.4. This effects the consumed energy of the system." [10].

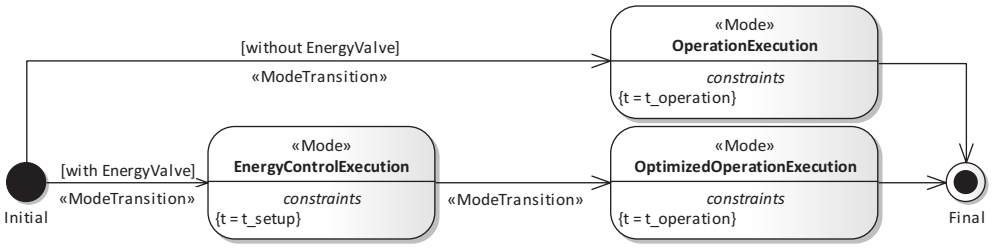


Figure 4.4: The power mode diagram with and without using the pattern's solution (obtained from [10]).

In some cases a rough estimation of the solution's impact is sufficient to decide if this design pattern is suitable. The impact of a related domain specific solution to the power consumption is described for *Energy Valve* as follows: *"**Domain - NFC.** Saved Energy is 43.87% as shown by [7]"* [10].

4.2 Power Verification Framework for NFC-Systems

In this section the developed power verification framework for NFC-Systems is presented. This framework allows verifications across the development phases of the MDA approach (see Section 1.3.3) and consists of three abstraction layers (as shown in Figure 4.5).

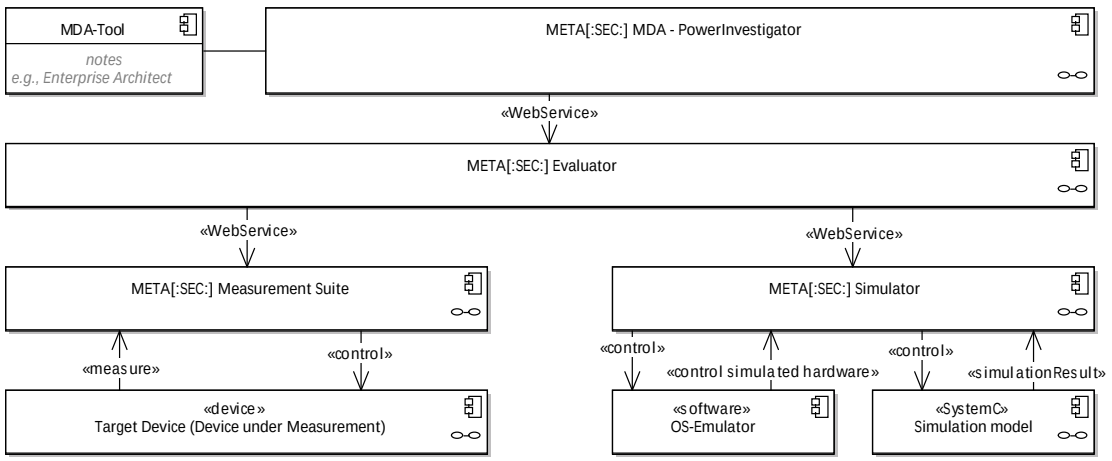


Figure 4.5: Architecture of the developed tool to verify power requirements of designs and implementations from NFC-Systems.

The first layer consists of the simulator (META[:SEC:] Simulator) and the measurement tool (META[:SEC:] Measurement Suite). The measurement tool is able to control the device under measurement and measures the power consumption during the execution. The simulator interconnects an OS-Emulator and the simulated hardware modeled in SystemC, controls both, and acquires the power trace from the simulation (power state machines). The second layer combines both measurement and simulation into one tool called META[:SEC:] Evaluator. The user of this tool can select between simulation and measurement and gets a common power trace as a result. The user interface is shown in Figure 4.6.

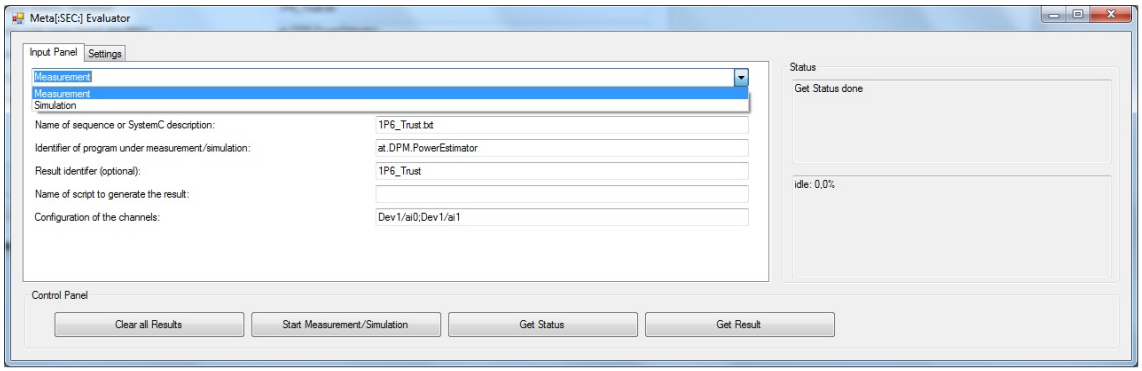


Figure 4.6: Graphical user interface of the evaluation tool called META[:SEC:] Evaluator.

The third layer interconnects a model based development tool (e.g., Enterprise Architect) with the META[:SEC:] Evaluator. This allows a direct verification of power requirements in the development tool itself. Therefore, one or multiple use cases (sequences to execute) and the refined power requirements to verify are selected. At the next step, the META[:SEC:] MDA-PowerInvestigator has all the required information to call the META[:SEC:] Evaluator to perform either a simulation or measurement. The graphical menu is shown in Figure 4.7.

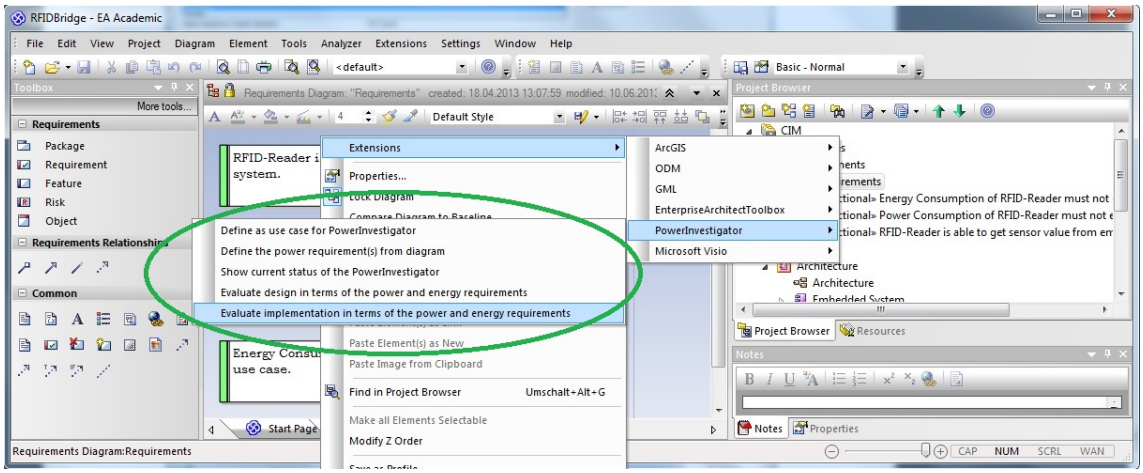


Figure 4.7: Graphical user menu of the META[:SEC:] MDA-PowerInvestigator integrated into the commercial tool Enterprise Architect.

The next two subsections give a more detailed architecture description of the two verifications based on a simulation using SystemC and an OS-Emulator, and hardware in the loop measurement of a real target device.

4.2.1 Verification by Simulation (SystemC)

The architecture of the simulation is shown in Figure 4.8. The software implementation is deployed on the OS-Emulator, which is controlled by the META[:SEC:] Simulator. The deployed implementation uses an interface with the simulated hardware modeled in SystemC. The simulation model itself is deployed into a simulation framework for SystemC. The simulation provides power traces of the NFC-System, which are converted to a common format to be processed by the META[:SEC:] Evaluator.

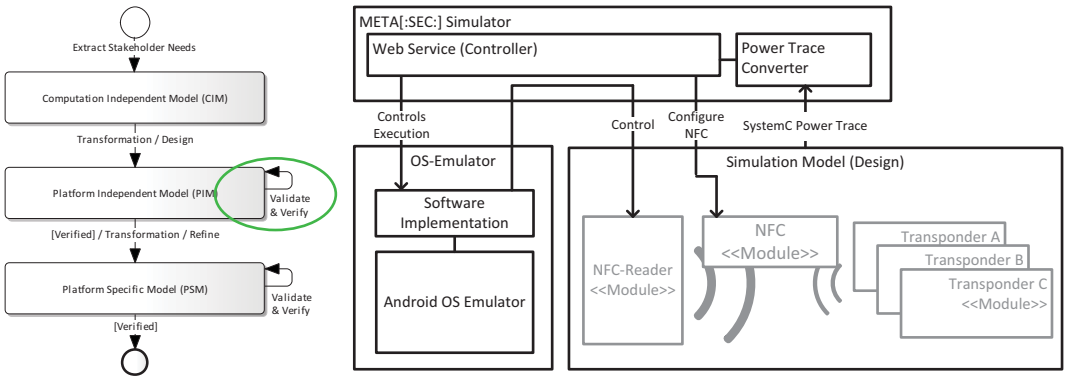


Figure 4.8: Architecture of the verification by simulation.

4.2.2 Verification by Measurement

The architecture of the hardware in the loop measurement is shown in Figure 4.9. The software is deployed onto a development board, which is attached to a state of the art NFC-Reader. The transponder(s) are programmable to be able to deploy their own firmware. The power is measured directly on the hardware and the values are converted to the common format to be processed by the META[:SEC:] Evaluator.

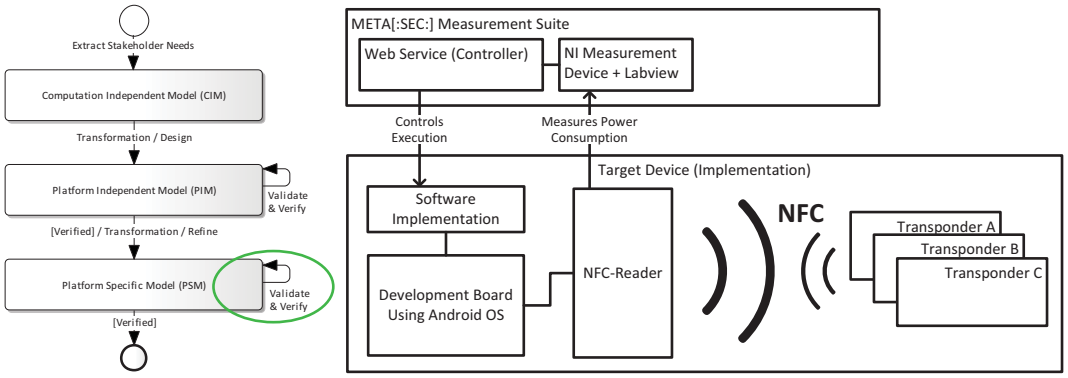


Figure 4.9: Architecture of the verification by measurement (adapted from [8]).

Chapter 5

Experimental Results

The following chapter shows an abstract of the experimental results from the two implementations based on the proposed power optimization technique, and the case studies performed divided into seven sections. The first section defines the simulation used and measurement setup, and the second section describes the applied use cases. The third and fourth section are dedicated to presenting the results of the two implementations of magnetic field strength scaling as presented in Section 3.2 and 3.3. The fifth part presents the results of the case study of magnetic field strength scaling for multi-transponder applications (as described in Section 3.4). In part six the results of the case study for power optimized and secure NFC-Bridges from Section 3.5 are shown. Part seven concludes the results with an evaluation of the overall impact of the magnetic field strength scaling technique to the system's energy consumption for different application scenarios.

5.1 Simulation and Measurement Setup

To obtain the experimental results the power verification toolbox for NFC-Systems, as described in Section 4.2, has been used. The setup for the simulation is described in Table 5.1. This setup is used to evaluate the design of the first and second implementation of the magnetic field strength scaling technique.

Component	**Description**
OS-Emulator	Android 2.3.4 (ARM as platform)
Simulation Model	SystemC version 2.2
NFC-Reader	SystemC transaction layer module of a Duali DE-620
Wireless Power Transfer	SystemC transaction layer module based on the equations described in Section 3.1 and characterizations of a real NFC-System
Transponder	SystemC transaction layer module of a Type 2 transponder based on ISO/IEC 14443A

Table 5.1: Setup used for the simulation based on the verification toolbox for NFC-Systems.

The measurement setup is described in Table 5.2. The measurement is used to verify

both implementations of the magnetic field strength scaling technique and also in an adapted form for the two case studies. The measurement is dedicated to verifying the proposed implementations according to their energy consumption and also to characterize the power behavior of a hardware module like the NFC-Reader to create the power model for the simulation. A picture of the measurement setup is shown in Figure 5.1.

Component	**Description**
Measurement Device	NI PXI-1042Q
Development Board	Beagleboard-xM (ARM) with Android 2.3.4
NFC-Reader	Duali DE-620
Transponder	Type 2 transponder based on ISO/IEC 14443A

Table 5.2: Used setup for the measurement based on the verification toolbox for NFC-Systems.

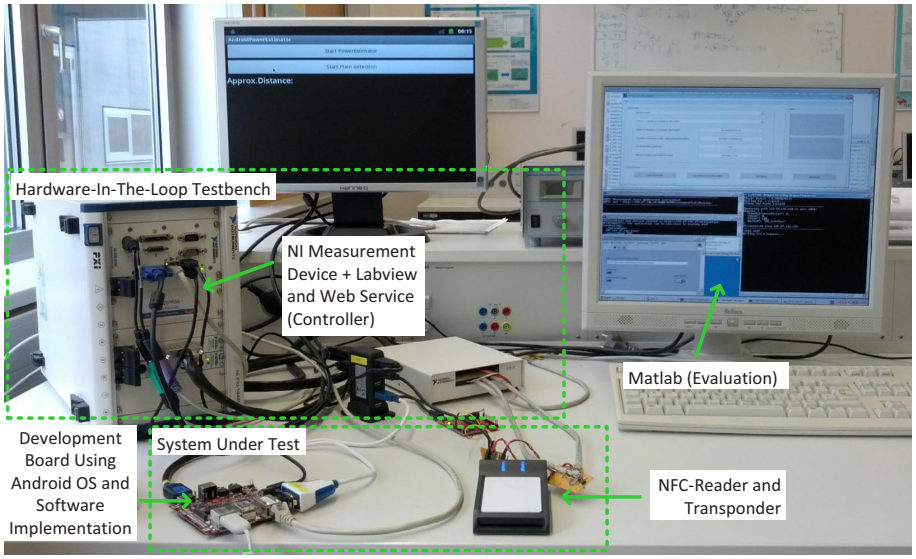


Figure 5.1: Picture and description of the setup used for the hardware in the loop measurement based on the verification toolbox for NFC-Systems (adapted from [8]).

5.2 Common Evaluation Use Case

To be able to compare the results of both implementations for magnetic field strength scaling and the case study for multi-transponder applications, a common use case has been defined as part of the simulation and measurement setup. This use case is shown in Figure 5.2. This use case describes reading data from a transponder by using the NFC-Reader after this transponder has been detected. In the multi-transponder environment the transponder detection is extended by selecting the desired transponder.

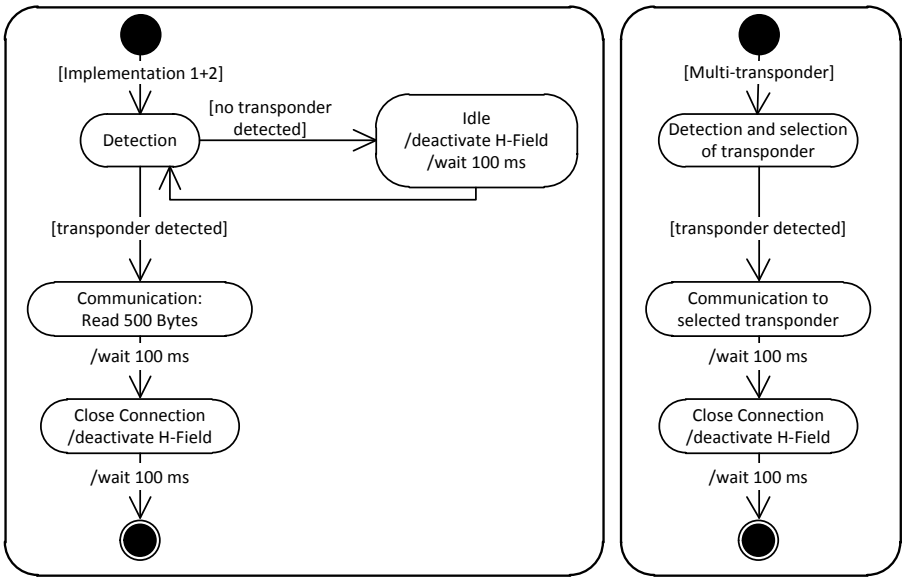


Figure 5.2: Two flow diagrams showing the two common use cases for the implementations based on magnetic field strength scaling (use case on the left), and the case study for multi-transponder applications (use case on the right) (adapted from [6]).

5.3 First Implementation: Initial Field Strength Scaling (FSS)

This section presents the experimental results of [7] from the first implementation based on magnetic field strength scaling as described in Section 3.2. This implementation has been simulated and measured on real hardware. The setup used and use case are described in Section 5.1 and 5.2. The results are presented in two parts consisting of an abstract of the results for the simulation and measurement and a summary of all experimental results including a conclusion.

5.3.1 Abstract of the Results for the Simulation and Measurement

The left part of Figure 5.3 presents an abstract result of the simulation with and without using the power optimization technique. Anticipating the summary result, up to 80% energy on NFC-Reader side could be saved at close distance. This should emphasize the potential of this implementation to save energy. The impact depends on the distance between the NFC-Reader to the transponder and the ability to change the provided power to be transferred on NFC-Reader side. In the case of the first implementation the dominant part of the overhead (timing) is situated in the detection phase as can be seen in the leftmost part of the plots. The measurement result on real hardware (right part of the figure), which has only limited abilities to change this power transfer, is not currently able to achieve such a reduction in energy, but it proves nevertheless that this technique is already able to save energy in real NFC-Systems [7].

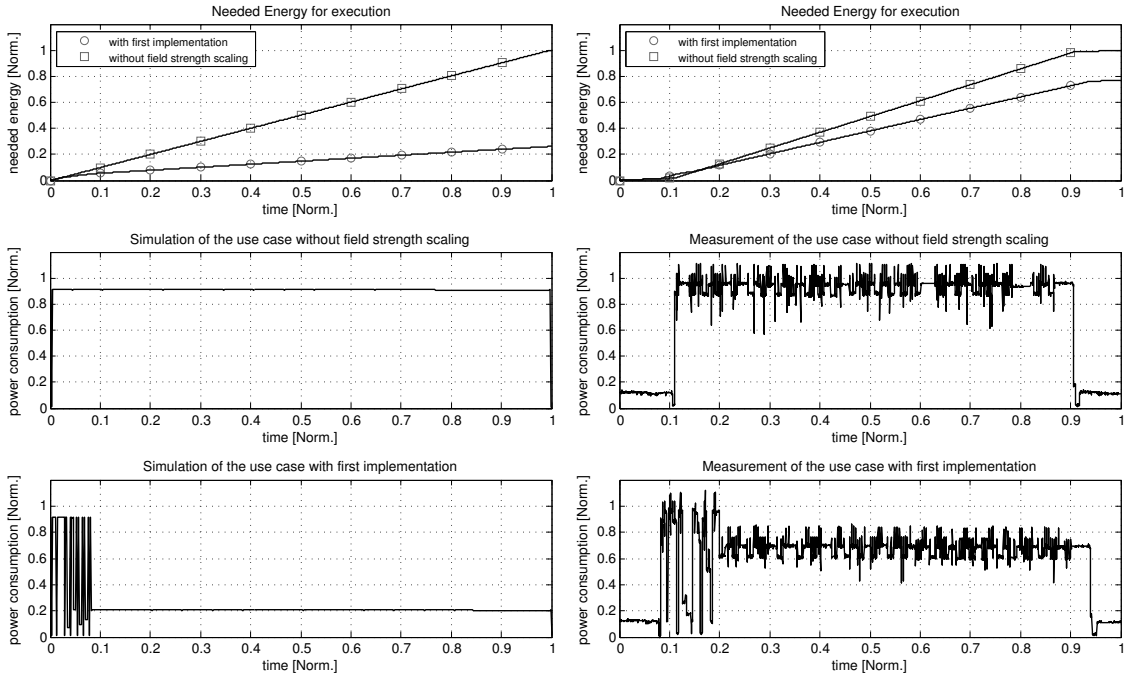


Figure 5.3: Simulation (left) and measurement (right) results for the first implementation based on magnetic field strength scaling (adapted from [7]).

5.3.2 Summary

The summarized results are shown in Table 5.3. It shows the results of the simulation and measurement with and without using the implemented optimization technique. The distances are altered in simulation to show the potential, and one result is shown of the measurement for comparison and feasibility on real NFC-Systems [6]. In measurement 26% could be saved at a distance of ∼4cm compared to the same NFC-System without using this implementation of magnetic field strength scaling [7].

Type	**Distance [cm]**	**Energy with impl. 1 [Norm.]**	**Energy without FSS [Norm.]**	**Energy saved [%]**
Simulation	0-1	0.20	1.00	80
Simulation	1-2	0.26	1.00	74
Simulation	2-3	0.39	1.00	61
Simulation	3-4	0.67	1.00	33
Measurement	~ 4	0.74	1.00	26

Table 5.3: Summarized results from the evaluation of the first implementation by using magnetic field strength scaling (adapted from [8]).

5.4 Second Implementation: Dynamic Field Strength Scaling (DynFS)

In this section the results for the simulation and measurement of the second implementation based on magnetic field strength scaling as described in Section 3.3 and published in [5] are shown. The setup and use case for both simulation and measurement are described in Section 5.1 and 5.2. The description is divided into two parts. First an abstract of the results are presented and discussed, and second a summary of the results is given.

5.4.1 Abstract of the Results for the Simulation and Measurement

In this abstract result the distance (physical relation factor) between the NFC-Reader and the transponder has been decreased during the use case of reading the transponder. This decrease simulates the user in pushing the transponder against the NFC-Reader. The ab-

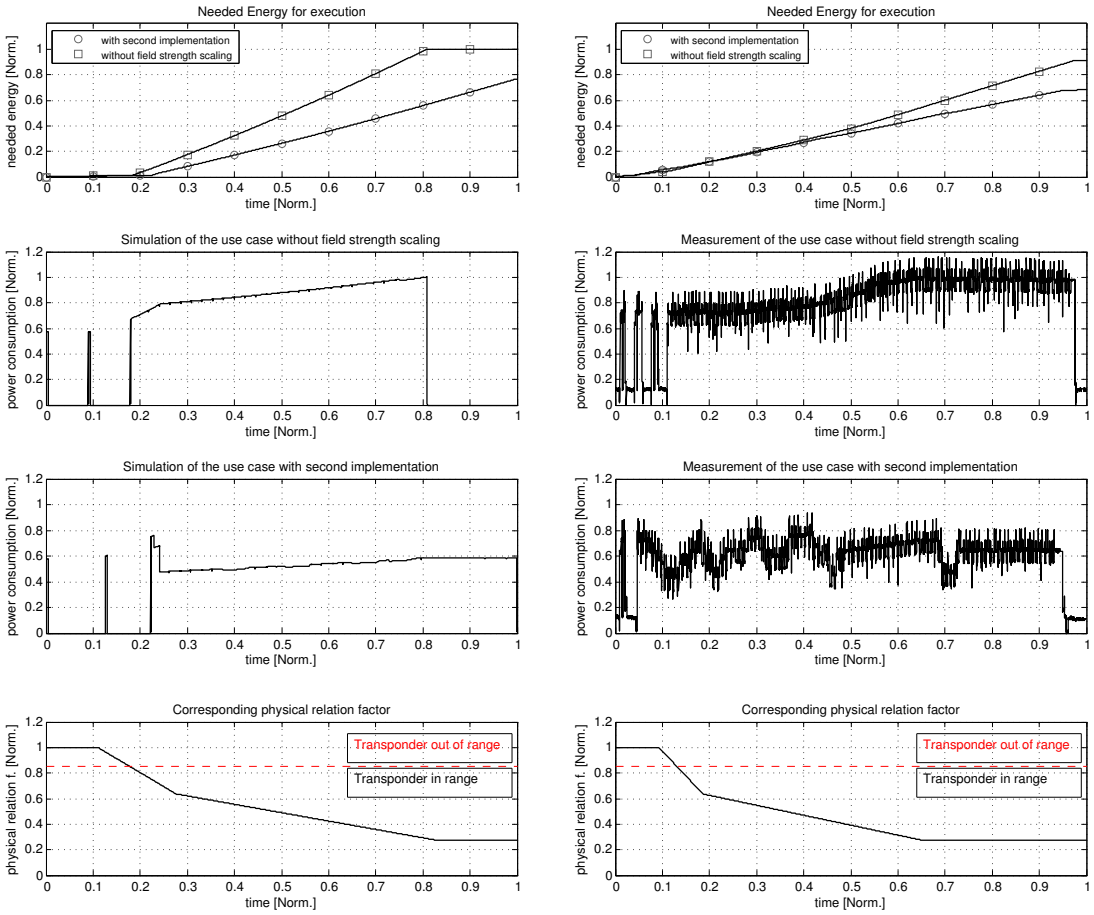


Figure 5.4: Simulation (left) and measurement (right) results for the second implementation based on magnetic field strength scaling. The physical relation factor represents the distance between NFC-Reader and transponder (adapted from [5]).

stract simulation result is shown in the left part of Figure 5.4. After the detection of the transponder the magnetic field strength is periodically rescaled. If this rescaling process was not performed the transponder would be oversupplied which results in a wastage of energy. This rescaling can be seen in the first part (between time 0.2 to 0.3). The right side of Figure 5.4 shows the behavior of the same use case on real hardware. Also here periodic rescaling occurs without undersupply of the transponder, which would lead to a connection loss and a resulting termination of the reading process. Compared to the results without using the second implementation based on field strength scaling, the execution time (overhead) is higher during the reading process through the periodic rescaling procedure, but the energy consumed is nevertheless reduced through the beneficial effect of the reduced power consumption [5].

5.4.2 Summary

A summary of the results is shown in Table 5.4. Conclusively, the results of the simulation and measurement comply to each other. In simulation 23% and in measurement 26% energy could be saved. The divergence of the results is too small to make reasonable statements [5].

Type	**Distance**	**Energy with impl. 2 [Norm.]**	**Energy without FSS [Norm.]**	**Energy saved [%]**
Simulation	decreasing	0.77	1.00	23
Measurement	decreasing	0.73	0.98	26

Table 5.4: Summarized results from the second implementation by using magnetic field strength scaling (adapted from [5]).

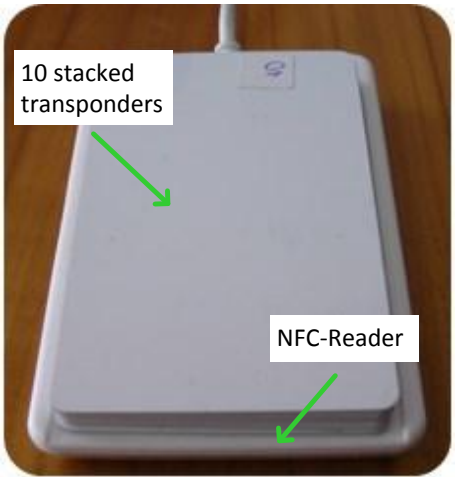
5.5 Case Study of using Magnetic Field Strength Scaling for Multi-Transponder Applications

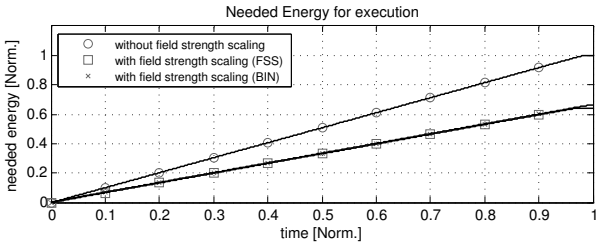
This case study uses the measurement setup as described in Section 5.1 with changes. As NFC-Reader an ACS ACR122U is used. Also multiple transponders are needed for this measurement. The NFC-Reader, the transponders used and an abstract from the results are shown in Figure 5.5. The results cover the two implemented methods FSS and BIN, which are based on the principle described in Section 3.4. FSS uses gradual scaling of field strength and BIN uses a binary quadratic search through the field strengths. For

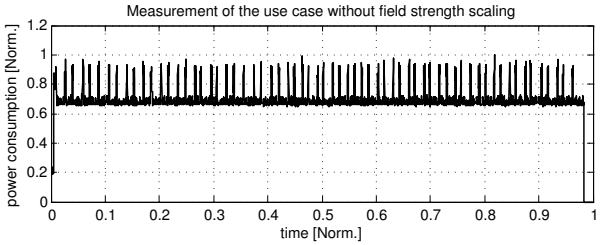
Algorithm	**Energy with FSS / BIN [Norm.]**	**Energy without FSS / BIN [Norm.]**	**Energy saved [%]**
Measurement (FSS)	0.66	1.00	34
Measurement (BIN)	0.68	1.00	32

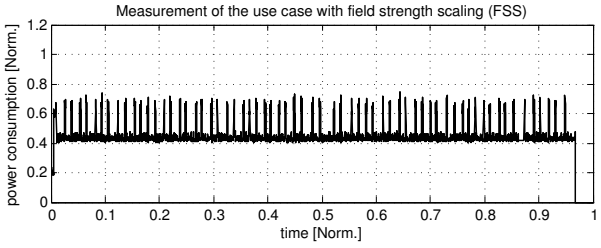
Table 5.5: Summarized results from the case study of using magnetic field strength scaling for multi-transponder applications (adapted from [8]).

this abstract result ten transponders are stacked together and the use case is selecting and reading data from a specific transponder (as described in Section 5.2). The results show that energy can be saved in this use case compared to the approach without using field strength scaling. A summarized result is shown in Table 5.5. On the NFC-Reader side up to 34% energy could be saved for this use case by using FSS. The impact of energy saving and the choice of which of the methods FSS and BIN are more efficient depends on several parameters like the number of transponders and their physical relationship to each other. Nevertheless, this result proves that magnetic field strength scaling can also be used in multi-transponder applications to save energy on NFC-Reader side [8].









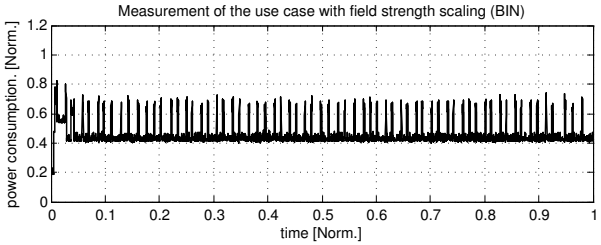


Figure 5.5: Extended measurement setup (left) and result (right) for the case study of using magnetic field strength scaling for multi-transponder applications (adapted from [8]).

5.6 Case Study regarding Power Optimization for Secure NFC-Bridges

In this case study an extended version of the measurement path as presented in Section 5.1 has been used. For this extension the NFC-Reader is replaced by an Android smart phone (Nexus S), and the power consumption is directly measured at the clamps of the battery by using an NI-DAQ 6009 (sampling rate 1kS) measurement device. For the case study a reference implementation of a smart meter deployed on a Spartan III FPGA prototyping board is used. A more detailed description and listing of results is given in [3]. The presented parts of the case study are split into two parts. First, two security strategies called variant 1 (V1) and variant 2 (V2), as shown in Figure 5.6 and described in Section 3.5, are evaluated for different strength of security. These variants also cover the case of an unauthorized (the NFC-Bridge blocks unauthorized users after the key exchange) access to the NFC-Bridge. The second part presents the proof of concept implementation by securing a sensor readout from the smart meter reference implementation over the NFC-Bridge [11].

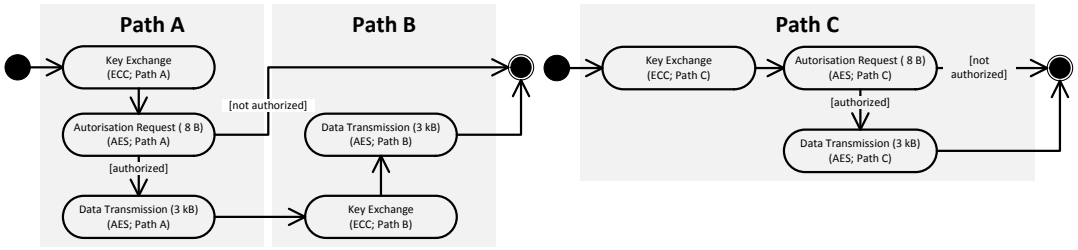


Figure 5.6: Flow diagram of the security strategies called variant 1 (V1) on the left and variant 2 (V2) on the right describing, what paths and encryption are used for authorized and unauthorized access (obtained from [11]).

Table 5.6 presents selected results from the case study. This table presents the measured energy consumptions $E_{V1,2}$ of the two different variants V1 and V2 in the case of an authorized or not authorized user trying to read out data. These variants are measured for different strength of security $S_{V1,2}$ (defined by $S_{CryptA,B,C}$ and $S_{KeyA,B,C}$). The energy consumed for V2 is 55% lower than for V1 by using secp224r1 for the key exchange and AES-128 for the data encryption [11].

$S_{CryptA,B,C}$ / $S_{KeyA,B,C}$	E_{V1} [Norm.]	E_{V1} (unauth.) [Norm.]	E_{V2} [Norm.]	E_{V2} (unauth.) [Norm.]	$S_{V1,2}$
AES-128 / secp160r1	0.7	0.15	0.29	0.14	80
AES-128 / secp192r1	0.86	0.23	0.37	0.23	96
AES-128 / secp224r1	1	0.28	0.45	0.31	112

Table 5.6: Results of the evaluation of both variants V1 and V2 in case of authorized and unauthorized access for different strength of security (adapted from [11]).

In Figure 5.7 a picture from the proof of concept implementation is shown. It consists of an Android smart phone (Android 4.2) including an application to securely read out the

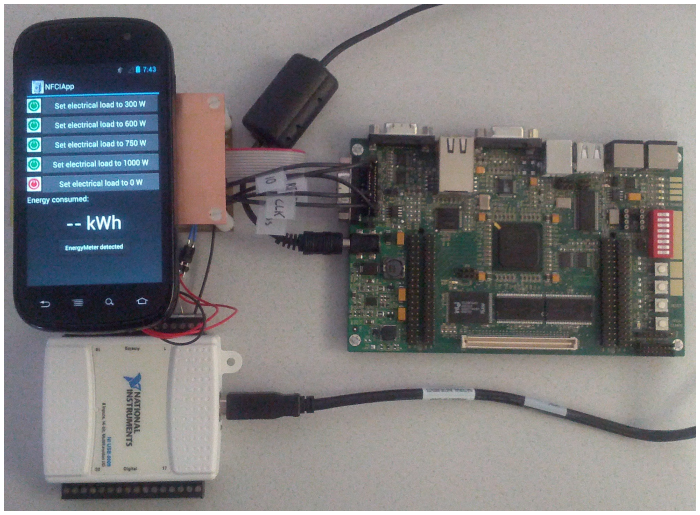


Figure 5.7: Proof of concept of the proposed secure NFC-Bridge system called PtNBridge including the smart meter reference implementation (obtained from [11]).

sensor value from the smart meter, such as in this case the consumed energy, the NFC-Bridge, and the reference implementation of the smart meter deployed on the Spartan 3 FPGA board. The encryptions used are AES-128 and ECC (secp160r1). Also the internal bus system of the smart meter is encrypted to make attacks like differential power analysis more difficult to apply [11].

5.7 Impact on Energy Consumption when using Magnetic Field Strength Scaling

Proposing a technique without thinking about the impact on real application scenarios is insufficient. Therefore, a rough evaluation of the impact to the battery lifetime of a mobile NFC-Reader for three application scenarios has been made.

- **Exchanging business cards.** In this scenario digital business cards on NFC enabled transponders are read.
- **Ticketing.** Using NFC enabled transponders as tickets to replace the printed versions win on importance and are already used. One scenario is that the ticket inspector uses a mobile NFC-Reader to check, if the tickets of the guests are valid. In this scenario a lot of transponders are read in a period of time.
- **NFC-Bridge.** The third scenario is using NFC as a gateway to embedded systems. The scenario's distinctiveness lies in the prolonged communication to the NFC-Bridge to exchange data.

This evaluation defines the energy resource of the NFC-Reader (battery) to be 20kJ. The remaining capacity after 12 hours of operation is presented in Figure 5.8. The relation between an active communication over NFC and idle state of the NFC-Reader is drawn on the x-axes. As the figure presents, the impact of using magnetic field strength scaling

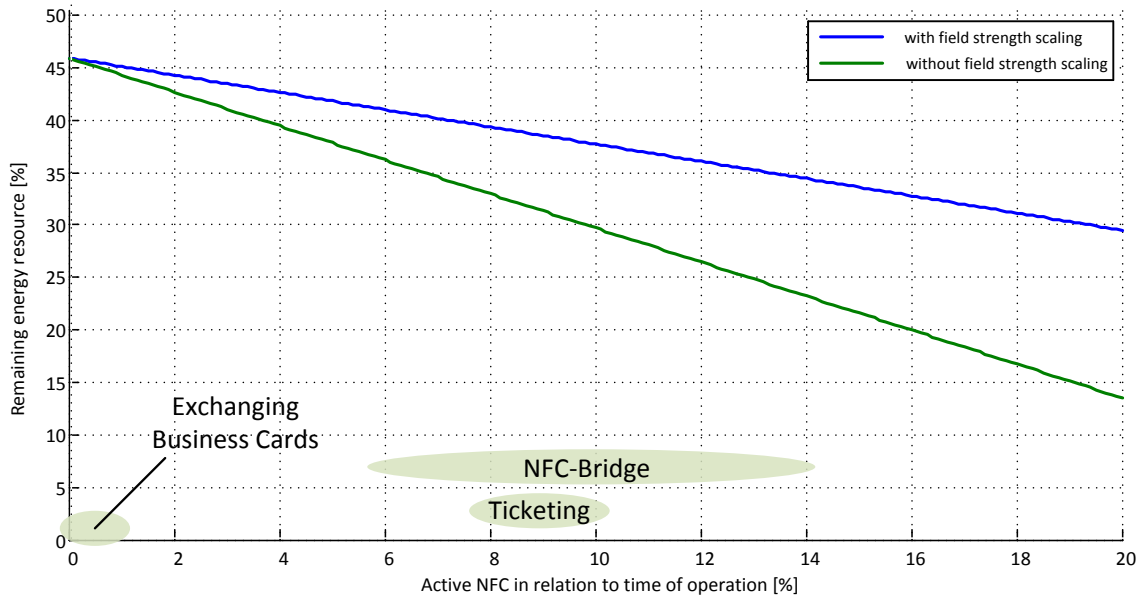


Figure 5.8: Impact to the NFC-Reader's energy resource (e.g., battery) with and without using field strength scaling for different application scenarios.

to the energy consumption of the NFC-Reader is quite low for the scenario of exchanging business cards. However, the impact becomes significant for the ticketing or NFC-Bridge scenario through the high frequency of reading tickets and the prolonged time needed for the data exchange. Conclusively, magnetic field strength scaling can prolong the battery lifetime of the mobile NFC-Reader depending on the application scenarios.

Chapter 6

Conclusion and Future Work

6.1 Conclusion

NFC is designed for interoperability which is achieved by its specification architecture of the underlying RFID standards, supported communication protocols and data exchange formats. Also the capacity for touch based interaction makes NFC ideal for applications such as wireless payment. Therefore, the integration of NFC into everyday handsets like smart phones is driven by the market, and it is predicted that about 50 % of all smart phones will feature NFC by 2015 [13]. However, mobile NFC handsets like smart phones have a limited energy resource (battery driven), and NFC further increases the handsets energy drain. Measurements taken showed that the average power consumption of a smart phone rises by 107 % during an NFC communication. The cause of this burden on the power consumption is not only restricted to the NFC enabled smart phone itself, rather than the complete system including the wireless power transfer and the transponder. This thesis deals with this liability in two complementary contributions.

The first contribution is dedicated to proposing and implementing power optimization techniques, and performing case studies related to the energy liabilities of NFC-Systems. The two implementations of the power optimization technique are based on the principle of magnetic field strength scaling. The first implementation scales the field strength once at the transponder detection phase and is able to reduce the energy consumption by up to 26 % (shown by measurement). This implementation lacks the feature to rescale this field strength during the communication, which can result in an oversupply or undersupply of the transponder. The second implementation deals with this lack with an approach that features periodic rescaling during the communication. Furthermore, a case study has been made to prove that the magnetic field strength scaling technique can also be used in multi-transponder applications. The measurement results show that up to 34 % of energy can be saved in such a multi-transponder environment (ten transponders stacked together). An additional case study aims to evaluate the impact of security to the power consumption of the NFC-System. Security is essential for applications like NFC-Bridges (gateway to embedded systems). Therefore, different security strategies for NFC-Bridges have been evaluated by measurement. An energy divergence of 55 % can be determined by using different strategies for a certain use case and the same strength of security.

Proposing an optimization technique and its implementations without a toolbox to ap-

ply them is not sufficient. Therefore, the second contribution lies in the toolbox consisting of a set of patterns for power management and a framework for power verification throughout the development process. The pattern's form has been extended to be able to describe a systematic solution for an occurring problem in the domain of power-management. This extension consists of multiple parts such as defined power profiles based on MARTE, and power-mode diagrams to describe the impact with and without using the patterns solution. One pattern example called *Energy Valve* is presented in this thesis for clarification. The proposed and implemented power verification framework for NFC-Systems enables the verification of the power and energy requirements before and after applying optimization techniques (e.g., by using the proposed design patterns). Also the verification across the development phases, such as the verification of the design by simulation, is supported. This combination of design patterns for power management and the verification framework aims to reduce development time and costs.

6.2 Future Work

This thesis contributes to power optimization techniques for NFC, in the form of implementations for magnetic field strength scaling and a development toolbox for power optimization. There are still open topics remaining in the field of power optimization for NFC-Systems and NFC in general. Three of them are described in this section.

One topic is design patterns for power-management. An extension to the patterns structure and an example pattern called *Energy Valve* has been published. Additionally, there is ongoing work to mine additional design patterns to create a set of power-management patterns. This work should be continued to create a comprehensive portfolio of such patterns for power-management. Also a survey to develop and optimize an NFC-System by applying these patterns should be made to improve the applicability of these mined patterns. This also leads to an important topic of extending the development process and the framework contributed by this thesis for a barrier-free application of such design patterns for the development and optimization of NFC-Systems.

The second topic regards IP-Core reuse. Existing hardware IP-Cores are used or bought from other companies when a new product or a derivative needs to be developed. This reduces the development time and can also reduce costs. The current contributed verification framework does not support such a feature of verifying NFC-Systems under development by IP-Cores reuse. Such a feature requires a common interface for multiple development phases for functional and non-functional verification. For example this IP-Core may have a power characterization on a very detailed level. The rest of the design is not capable of such a level of detail.

The third topic is related to the influence of NFC-Systems on our lives and especially to our privacy. As described in the introduction, the number of shipped NFC-handsets is rising through the interoperability benefit of NFC. But this also means more persons or machines can access NFC compatible devices, such as the private access card in our wallet. Work has been undertaken in terms of security for NFC-Systems as part of this thesis. This does not include surveys regarding the impact to our privacy. Can everyone track where we are going, or is it possible for unknown parties to obtain sensitive data we don't want to share? We have to be aware of these when we push forward with NFC.

Chapter 7

Publications

This chapter presents the publications related to this thesis. An overview is given in Figure 7.1. The publications are grouped into the contributions of this thesis. The comprehensive overview of this contribution and the content of these publications is given in Chapters 3 and 4. The publications are added to give a more detailed description of the contribution, the related work for the specific topic and the experimental results.

Publication 1: Menghin et al., *Using field strength scaling to save energy in mobile HF-band RFID-systems*, EURASIP Journal on Embedded Systems 2013.
Publication 2: Menghin et al., *The PTF-Determinator: A run-time method used to save energy in NFC-Systems*, 2012 Fourth International EURASIP Workshop on RFID Technology, Turin, Italy.
Publication 3: Menghin et al., *NFC-DynFS: A way to realize dynamic field strength scaling during communication*, 2013 5th International Workshop on Near Field Communication (NFC), Zurich, Switzerland.
Publication 4: Menghin et al., *Energy Efficiency by Using Field Strength Scaling for Multi-Transponder Applications*, 12th International Conference on Telecommunications - ConTEL 2013, Zagreb, Croatia.
Publication 5: Druml et al., *Adaptive Field Strength Scaling - A Power Optimization Technique for Contactless Reader / Smart Card Systems*, 2012 15th Euromicro Conference on Digital System Design, Izmir, Turkey.
Publication 6: Menghin et al., *PtNBridge - A Power-Aware and Trustworthy Near Field Communication Bridge to Embedded Systems*, 2013 16th Euromicro Conference on Digital System Design, Santander, Spain.
Publication 7: Menghin et al., *Introduction of design patterns for power-management in embedded systems*, 18th European Conference on Pattern Languages of Programs, Irsee, Bavaria.
Publication 8: Menghin et al., *Development Framework for Model Driven Architecture to Accomplish Power-Aware Embedded Systems*, 2014 17th Euromicro Conference on Digital System Design (Under Review).

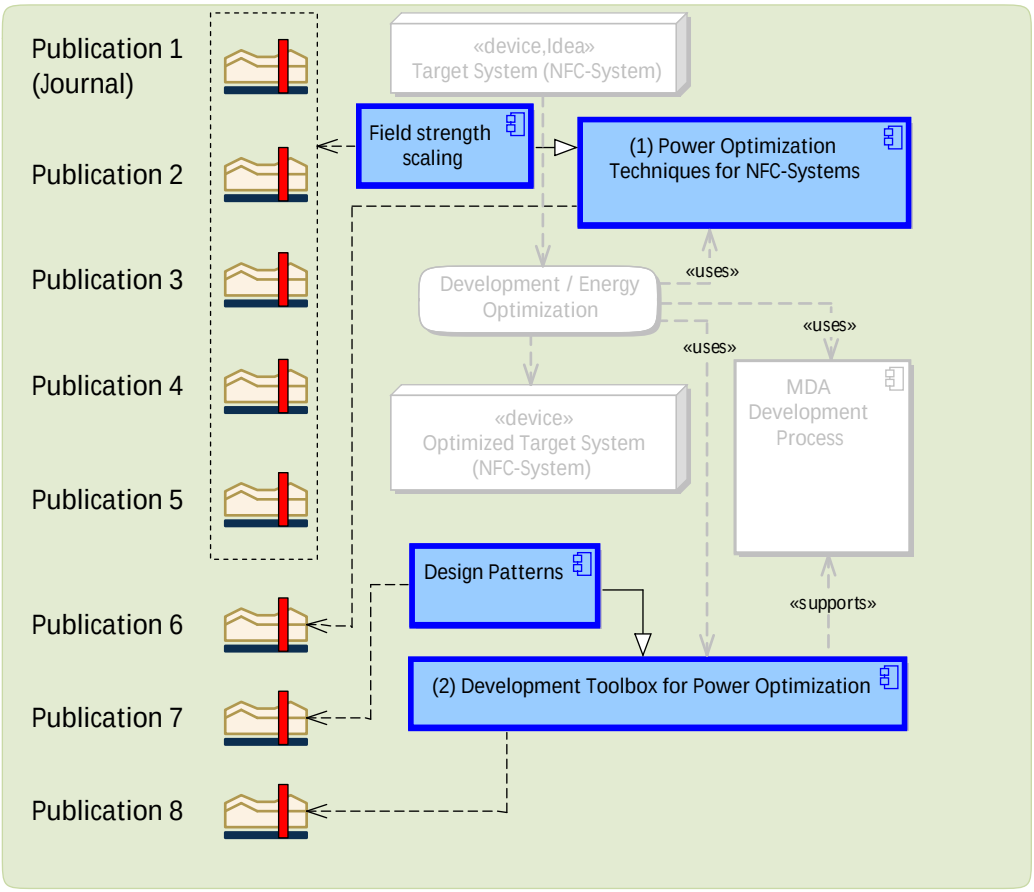


Figure 7.1: Overview showing the publications and their relation to the contribution of this thesis.

The first group deals with the optimization technique of magnetic field strength scaling and the related case study. The two implementations of the technique are presented in *Publication 2 and 3*. *Publication 5* presents the exploration and evaluation performed regarding magnetic field strength scaling for the reader and transponder side. *Publication 4* is the case study performed regarding the applicability of field strength scaling in multi-transponder environments. The journal *Publication 1* summarizes the research into magnetic field strength scaling. The case studies performed to investigate the impact of security to the energy consumption of NFC-Systems is presented in *Publication 6*. The second group deals with the topic of the development toolbox. *Publication 7* introduces design patterns for power management as part of this toolbox. The *Publication 8* continues with the work in terms of integrating the verification framework that has already been implemented into an MDA based development processes.

Menghin *et al. EURASIP Journal on Embedded Systems* 2013, **2013**:4
http://jes.eurasipjournals.com/content/2013/1/4

EURASIP Journal on Embedded Systems
a SpringerOpen Journal

RESEARCH Open Access

Using field strength scaling to save energy in mobile HF-band RFID-systems

Manuel Menghin[1*], Norbert Druml[1], Christian Steger[1], Reinhold Weiss[1], Holger Bock[2] and Josef Haid[2]

Abstract

Radio frequency identification (RFID) is a technology enabling a contactless exchange of data. This technology features the possibility to wirelessly transfer power to the transponder (opponent). HF-RFID is used in mobile devices like smart phones and shows potential for applications like payment, identification, etc. Unfortunately, the needed functionality increases the battery drain of the device. As a countermeasure, power-management techniques are implemented. However, these techniques commonly do not consider the whole system, which also consists of the communication to the transponder, to prevent wasting energy. One cross-system technique of reducing the wasted energy is magnetic field strength scaling, which regulates the power transfer to the transponder. This article shows three investigations made, regarding field strength scaling to prevent this wastage of energy. The results of one investigation, how to use field strength scaling at card detection phase in form of the PTF-Determinator method, is described in detail. This method determines the Power Transfer Function (PTF) during run-time and scales the provided power accordingly to save energy. As a case study the PTF-Determinator is integrated in an application to read digital business cards. The resulting power consumption and timing has been evaluated by simulation and measurement of a development platform for mobile phones. Furthermore, the impact of field strength scaling to the energy consumption of a state of the art NFC-enhanced smart phone has been analyzed. The results of the case study shows that up to 26% less transmission energy (energy drain of NFC) is needed, if field strength scaling is applied (proofen by measurement). According to this result a smart phone's battery drain (energy drain of the whole system) can be decreased by up to 13% by using field strength scaling for this case study.

Keywords: RFID, NFC, Power consumption, Magnetic field strength scaling, Power transfer, Power-management

1 Introduction

HF-band radio frequency identification (RFID) is a wireless form of communication. One feature of this wireless communication form is the possibility to transfer power from the reader (sender) to the transponder (receiver). There are many standards using this communication form. One of them is near field communication (NFC). An exemplary application of NFC is using it in mobile devices like smart phones, which opens a wide set of applications like payment, identification, and ticketing. Unfortunately, NFC increases the battery drain, because of the additional power-consumption needed by the reader during communication. Minimizing this consumption is the goal of the power-management algorithms implemented in software and hardware. These algorithms commonly focus on one component and do not consider the whole system.

The considered target system consists of multiple components as shown in Figure 1. The mobile RFID-Reader includes a battery, which can only provide a limited amount of energy. The reader also has to power the Reader-IC needed for the RFID communication. The transponder has no own power source and is powered over RF. This wireless power transfer includes losses (more power has to be provided by the reader to satisfy the power requirements of the transponder). This discussed RFID communication (HF-Band) is based on inductive coupling where an alternating magnetic field is used to transfer the data and the power to the transponder.

The reader is able to control this transferred power by scaling the strength of the magnetic field. In most cases, the provided power by the reader is set to a maximum value to ensure the transponder's proper supply at an

*Correspondence: manuel.menghin@tugraz.at
[1]Graz University of Technology, Graz, Austria
Full list of author information is available at the end of the article

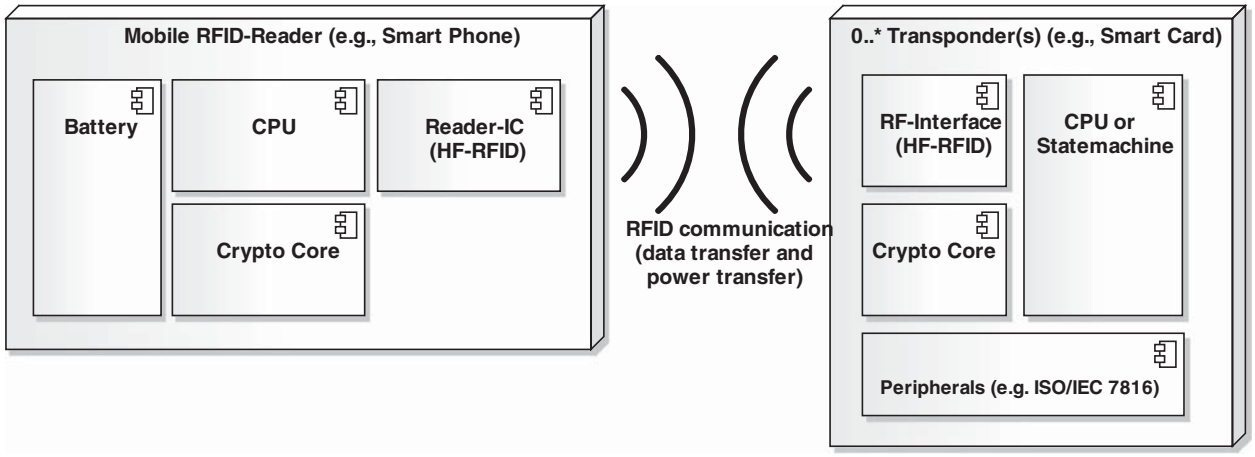


Figure 1 Target system. This component model describes the target system considered in this article. Basically, it consists of the battery-powered HF-RFID reader and zero to multiple transponder(s). The case study of this article considers the case of one reader connected to one transponder.

expected transmission distance (about 5–10 cm) regardless of the transponder-type. This provided power output is in most cases (e.g., closer distance) too high and leads to an oversupply of the transponder. To give an example, the power consumption of a state-of-the-art smart phone with NFC has been measured, which is shown in Section 5.4 in detail. The result shows that the smart phone needs 50% more power when NFC is activated but no transponder is in range compared to the consumption without NFC. However, if a transponder is read over NFC, then the device consumes up to 107% more power. This shows that reducing the power consumption of NFC plays a relevant role in decreasing the battery drain of the RFID-Reader (e.g., smart phone). One way to achieve that is the dynamic configuration of the magnetic field strength by the reader during run-time. To perform this dynamic configuration, the reader has to know, which field strength is currently needed to supply the transponder properly. The investigations made to realize this dynamic configuration can be divided into three parts:

- The first investigation regards dynamic field strength scaling during card detection phase. The challenge lies in gathering the needed parameters (e.g., distance between reader and transponder) to evaluate the power transfer function (PTF) after a transponder has been detected. Based on the PTF knowledge, the reader is able to properly scale the magnetic field strength. Additional methods to prevent a wastage of energy can be implemented based on the knowledge of the PTF, which will be discussed later on [1].
- During the phase of RFID communication, the distance between reader and transponder can change (user typically moves the transponder in the direction to the reader), which results in a changing PTF. Furthermore, different operations, like reading data from the transponder or performing an encryption, lead to a change of the transponder's power requirements. The adaption of the magnetic field strength during communication is important, to preserve a proper supply for the transponder at all time [2].
- The RFID technology is able to read multiple transponders in range. Multiple transponders in the magnetic field influence the PTF, which also depends on the states of these transponders (e.g., selected and active or deselected). These dependencies occur because different transponder states provoke different power consumption requirements. With this knowledge, the PTF can be redetermined and the consumed energy can be reduced by a proper field strength scaling algorithm.

The contribution of this article consists of three parts:

- Three investigations of magnetic field strength scaling in HF-Band RFID-Systems to create a power-aware system are presented.
- The investigation how to use field strength scaling during card detection phase in form of the novel PTF-Determinator method is described in detail in [1] (see Figure 2).
- A case study using the PTF-Determinator in an application of reading digital business cards (including a feature to restrict the maximum transmission distance) is shown [1].

The remainder of this article is split into five main parts. The first part can be found in Section 2, which shows the related work and highlights the contribution. The second part shows the three investigations to realize magnetic field strength scaling. As third part, which can be found in Section 4, the PTF-Determinator and its integration into

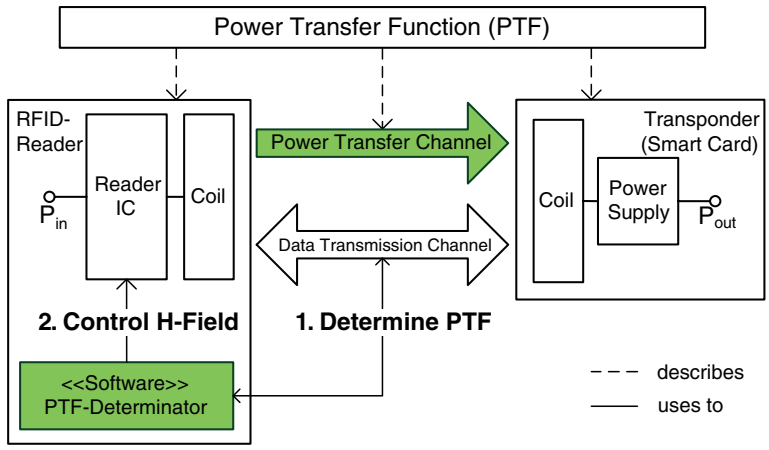


Figure 2 The proposed first step towards field strength scaling using the PTF-Determinator and the integration into the NFC system.

the RFID-System is shown in detail. The case study is presented in the fourth part in Section 5. The fifth part in Section 6 finally concludes this article.

2 Related work

This section is split into four parts. The first part deals with the state-of-the-art possibilities to acquire the physical relation factor (simplified the distance between reader and transponder). The second part shows investigations regarding the influence of the transponder's operation to it's power requirements. In addition, the related work regarding multiple transponders is shown in part three. In the fourth part, known system-based power-management concepts including reader and transponder are shown.

2.1 Acquisition of the physical relation factor

One consideration regards acquiring the physical relation, like the distance between the reader and the transponder coil, and other dynamic parameters, during run-time. An approach is to find a known parameter that describes this physical relation. Cheng et al. [3] show that there is a relation between the provided power of the reader and the distance to the transponder. The analysis has been concluded by altering the signal strength of the reader and checking if the transponder has enough power to be active. Another approach is distance bounding, which uses the delay between the request and the response as known parameter to calculate the physical distance between reader and transponder to detect relaying attacks [4]. To use this information to determine the PTF, the parameter has to be measured during run-time. Furthermore, transmission characteristics (e.g., coil dimensions) have to be included into the determination. These characteristics depend on the system's setup (e.g., different types of transponders). Xu et al. [5] use power stepping to detect different positioned transponders (distance to the reader). This consideration does not include the physical principles of the power transfer but leads to a evaluation of a parameter, which is similar to a distance value, during run-time. Another method measures the voltage on transponder side and to use it for the PTF determination [6].

2.2 Power requirements of the passive transponder

Another fact to consider is that the transponder is only passively powered by the reader [7]. This means that the transponder cannot respond, if the provided power drops under a certain threshold. Furthermore, the power consumption of the transponder itself depends on the currently executed operation, which influences the level of needed power [8]. Power-consuming operations are especially encryptions/decryptions [9]. Mercier et al. [10] show the relation between the provided power and the consumption of the circuit. To consider this in the determination of the PTF, the transponder has to be in a state that is aware of its power consumption. The last point of consideration is the transmission of the data (response), which is realized through load modulation on transponder side. The influence on the modulation is similar to the power consumption of the transponder [11]. One possibility to acquire the power consumption of the transponder during run-time is using the principle of using power estimation units directly on the transponder. This information can be transferred to the reader afterwards [12].

2.3 Influence of multiple transponders on the PTF

Multiple transponders in RF field influence the power consumption of the RFID-System, and a PTF used for one transponder is not enough to describe this environment. Collisions for example influence the power consumption of the total system. The reader sends a request and gets the response from the transponders. These messages can

collide and have to be detected. There is a protocol included in the detection algorithm to deal with this challenge. Most of the publications made in this topic are dealing with the question, how to optimize or avoid these collisions. Kamineni et al. [13] are using the power level information on transponder side to avoid collisions by defined delays according this power level. Other published approaches deal with the avoidance of collisions to increase the performance of the system [14,15].

2.4 System-based power-management for RFID

Liu and Tong [16] describe energy provisioning services. They show that knowing the system can lead to optimization possibilities. Their concept focuses on a multi-tag multi-reader application but it can be adapted to the challenge of field strength scaling. This knowledge can be used to optimize the system in terms of power consumption and stability. This should especially be considered in combination with mobile readers [17]. The challenge is to manage the distributed information and the calculation among the system for power-optimization. The Cinder operating system is an example how such optimizations can be done. This approach is designed for smart phones but the model can be extended to include externally powered devices as well [18].

3 Investigations made for field strength scaling

This section describes the three investigations made to use magnetic field strength scaling in RFID-Systems as mentioned in Section 1. These investigations are separated according to the overview of the RFID communication flow and the dependencies to the PTF as shown in Figure 3. The reader should know the PTF at each point in time to react on changes. The first investigation regards the determination of the PTF during card detection phase. The second investigation deals with the dependencies to the currently executed operation invoked by the reader and sent to the transponder (e.g., read block), and the changing physical relation factor (distance) of the transponder. The third investigation regards the influence of the multiple transponders in range to the PTF.

3.1 Field strength scaling during card detection phase

If a transponder gets in range, the reader is able to establish the communication by sending the request (e.g., REQA) and an anti-collision command (needed for multi-transponder communications). The transponder answers to this anti-collision command with its unique identification number (UID). This procedure is followed by a selection command, which elevates the transponder to the ready state. During this card detection phase, data are already exchanged between the reader and the transponder. If this phase is modified to determine the PTF, the reader would be able to scale the magnetic field strength accordingly before the communication process begins (e.g., reading a digital business card). The challenge of this approach is getting the information needed for the determination during this phase (a detailed description is given in Section 4) [1]. One issue, which is not covered by this approach, is the changing physical relation factor during communication. An initial magnetic field scale can lead to an oversupply or to an undersupply of the transponder during the communication process.

3.2 Dynamic field strength scaling during communication

This approach deals with the issue of dynamically scaling the field strength during communication. A scenario can scaling the field while reading the data of a digital business card. Thus, this method avoids an oversupply or undersupply by inappropriate scaling. The challenge of this approach can be split into two parts. The first part is detecting changes of the physical relation factor (distance) during communication. These changes occur by pulling the transponder from or pushing it towards the reader, which can be a scenario (e.g., access card is held by the user against the reader). Redeterming the PTF using the same method as in the card detection would result in a considerable communication overhead. This redetermination has to be made fast enough to react on the change of the physical relation factor. Thus, another way has to be found to detect the changes like finding an easy to acquire equivalent parameter to the physical relation factor on reader side. The second part concerns the fact that different transponder commands demand different transponder power requirements, e.g., reading a memory-block versus performing cryptographic operations. This also has to lead to a redetermination of the PTF and to a proper scaling [2].

3.3 Field strength scaling for multiple transponders

The two described ways of accomplishment do not consider multiple transponders in range. The usage of multiple transponders with one reader is not restricted to logistic applications, like reading tagged packets. An example of other applications is a briefcase, with multiple access cards. These transponders influence the PTF in two ways. First, each transponder has a different physical relation factor (distance to the reader). The transponders cannot be on the same position. The PTF depends on the currently selected transponder. Second, the instantaneous power consumption of a transponder influences the PTF of all other transponders. Therefore, the reader has to be aware of the presence of all transponders and their states to properly scale the magnetic field to avoid an oversupply or undersupply. Furthermore, a policy has to be defined how to interact with the transponders. The transponders, which are not selected, can either get a proper supply to remain in their states, or the policy allows the undersupply

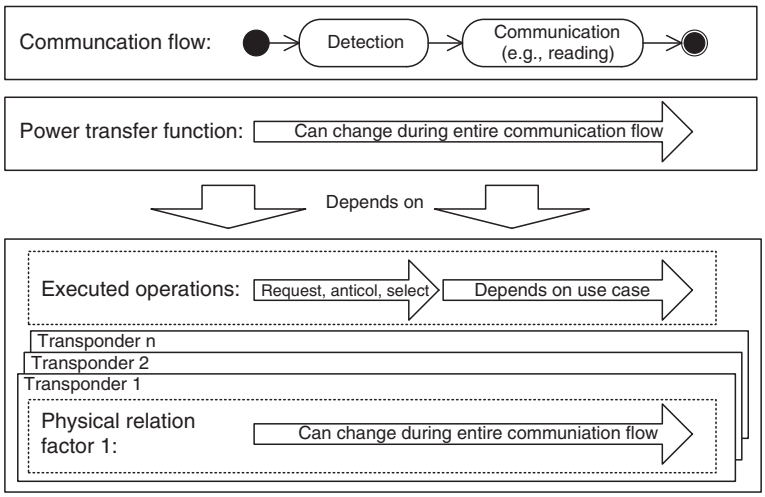


Figure 3 Overview of the dependencies of the PTF during communication. This figure gives an overview of the dependencies during communication regarding the PTF. The upper part visualizes the communication flow. The lower two parts are the dependencies of the PTF during the communication.

of those deselected transponders to save energy with the disadvantage of a loss of connection to them.

4 Method - Field strength scaling during card detection in detail

In this Section, the investigation of field strength scaling during card detection phase and the used method called PTF-Determinator is shown. The challenge to determine the PTF in the card detection phase is to collect the needed information during this phase and to pass this information to the reader side. With the determined PTF, the field strength can dynamically be scaled. To realize the above described steps, the RFID-System has to be defined and examined. For examination, the target system is reduced to one reader and one transponder. The RFID communication channel between them is split into two main parts. The first part is the power transmission path. It describes how the provided power, which can be altered by the reader, is transferred to the transponder. The second part is the communication channel used to exchange data between reader and transponder. The solution how to integrate the PTF-Determinator method into an existing RFID-System is shown in Figure 2.

At first, the needed electrical characteristics for the realization of the method are shown. The realization itself is split into four considerations. The first one deals with gathering the needed parameters from the reader and transponder. The second relates to the evaluation of the physical relation factor, which cannot be acquired directly. The third consideration deals with the integration of the method into the RFID-System's existing communication flow. The fourth consideration describes a library providing an interface to access the determined PTF. This library can be used for power-management methods.

4.1 Electrical characteristics

This section explains the used replacement circuit and equations for the method to calculate the PTF. The equations describe how the power is transferred from the Reader-IC to the supply of the transponder. The replacement circuit describes the connection between them, as shown in Figure 4. The calculation is split into four parts.

The first part describes the power control of the Reader-IC, which can be configured by a resistance (R_{rel}) serial to a constant voltage-source (U_1) as shown in Equation (1).

$$i_r = \frac{U_1}{Z_c + R_{\text{rel}}} \tag{1}$$

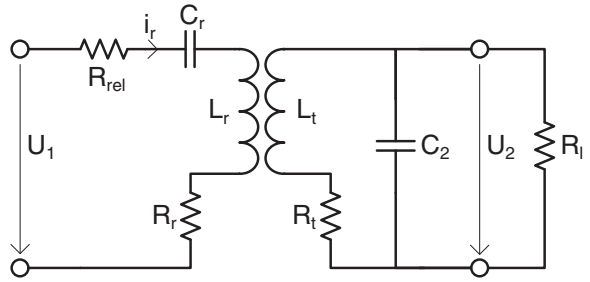


Figure 4 Replacement circuit of the power transfer over RFID. This replacement circuit describes the power transfer from the reader to the transponder without the voltage regulation on transponder-side, adapted from [19]. In this case, the input current i_r is scaled by the resistance R_{rel}. U_2 represents the supply voltage of the transponder.

Increasing the resistance causes a reduction of the overall power (decrease of i_r) consumption with the disadvantage of loosing transmission range [20]. The current i_r also depends on the configurable resistance R_{rel} and the input resistance Z_c of the circuit beyond. Z_c alters according to the inductive coupling between reader and transponder and is therefore not static.

The second part consists of the equation used to calculate the provided magnetic field H of the reader, which is provoked by the electrical current i_r. The considered orientation of the sender and receiver coil is shown in Figure 5.

Equation (2) can be used for rectangular-shaped sender coils and is based on the law of Biot-Savart. It is based on the physical principle of loose inductive coupling. The needed parameters are the dimensions a_r and b_r of the reader coil and the number of windings N_r. The distance to the coil can only be used if the coils are coaxial oriented [19].

$$H = \frac{i_r \cdot N_r \cdot a_r \cdot b_r}{4 \cdot \pi \cdot \sqrt{(\frac{a_r}{2})^2 + (\frac{b_r}{2})^2 + d^2}} \cdot \left(\frac{1}{(\frac{a_r}{2})^2 + d^2} + \frac{1}{(\frac{b_r}{2})^2 + d^2} \right) \quad (2)$$

The third part deals with the transformation of the magnetic field strength back to a voltage on transponder side (see Figure 4). A resonance circuit, consisting of a parallel capacitance and the coil's inductance, is used to amplify the received voltage. First of all the coupling coefficient k is calculated with Equations (3) and (4). The coefficient represents an abstract relation between reader and transponder and requires the magnetic field strength as input. Equation (5) calculates the resulting voltage on transponder-side. This is only valid for rectangular receiver coils. The needed input parameters are the dimensions a_t and b_t, the number of windings N_t, and the coil's inductance L_t [19].

$$M_{12} = \frac{\mu_0 \cdot H \cdot N_t \cdot a_t \cdot b_t}{i_r} \quad (3)$$

$$k = \frac{M_{12}}{\sqrt{L_r \cdot L_t}} \quad (4)$$

$$u_2 = \frac{w \cdot k \cdot \sqrt{L_r \cdot L_t} \cdot i_r}{\sqrt{(\frac{(w \cdot L_t)}{R_l} + w \cdot R_t \cdot C_2)^2 + (1 - w^2 \cdot L_t \cdot C_2 + \frac{R_t}{R_l})^2}} \quad (5)$$

The fourth part describes that the output voltage is limited by a Zener-diode to prevent the smart card's electronics from power surges. It is also necessary to provide a minimum voltage. If the supply drops below the minimum threshold voltage, the circuit is set to power down. Figure 6 shows an example of the relation between reader/transponder distance, and the supply voltage of the transponder (the power consumption of the transponder is considered static) for several reader power output levels.

4.2 Gathering needed parameters

As first consideration, the needed parameters have to be collected from the RFID-System. They are distributed between reader and transponder. Some of them are physical values, which have to be stored in digitalized form. Because of the system's variability during run-time (e.g., different transponders), the storage of all parameters in a single location is inappropriate. Table 1 depicts the number of parameters, their location, and their required space.

These parameters shall be provided on the described location shown in Figure 7. One approach is to store this data into a memory during the device's production phase

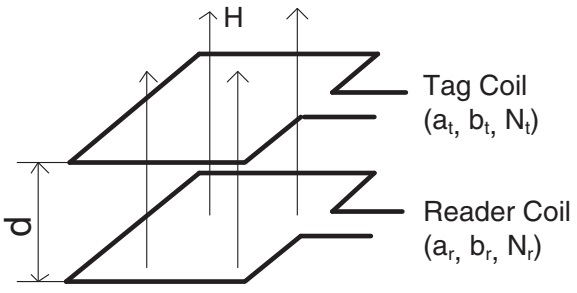


Figure 5 Considered coaxial orientation of coils. This figure visualizes the considered coaxial orientation of the reader to the transponder by using rectangular shaped sender and receiver coils.

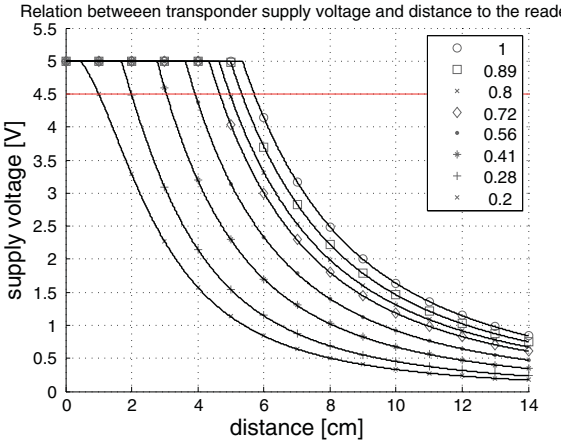


Figure 6 Relation to the supply voltage of the transponder. Plot of the relation between the supply voltage of the transponder to the distance between the reader and the transponder. The relation is shown using different input power levels as described in the legend. The two coils are oriented coaxial.

Table 1 Number of parameters needed for the PTF-Determinator including their location and needed space in bytes

Location	Number of parameters	Accuracy [b]	Space [B]
Mobile RFID-Reader	5	32	20
		8	5
Transponder	8	32	32
		8	8

The space is shown with different accuracies of the parameters.

(reader and transponder). The needed storage space is 32 byte on transponder-side if an accuracy of 32 bit is used. In practice, the needed storage can be decreased by adapting the resolution of the values according to the needed PTF accuracy requirements. An example is shown in Table 2 where the needed space is reduced to 8 bytes. These values have to be transferred to a central computation unit. This can either be the reader or the transponder. In this study, the reader has been chosen because of its advanced computational resources and a direct control of the needed input parameters for the PTF (parameter of provided power). This also means that the parameter-values from the transponder have to be transferred to the reader which can costly be in terms of time and power. For comparison, sending a ping request to the transponder requires 7-bit and results in a 2-byte response [19]. The request could be the same size but the response would be 16 times greater. If the bit length of the send values is reduced to 8 bits, which should be enough in practice, the bytes to sent can be four times greater.

4.3 Evaluation of the physical relation factor

The second consideration regards the physical relation factor, which is independent from the type of reader and transponder used. Furthermore, its value is unknown and has to be evaluated during run-time. It cannot directly be measured because of the lack of sensing mechanisms on both sides.

Table 2 Comparison of the saved energy for the RFID-transmission in percent between the method with and without an improved version of the PTF-Determinator from [1] in the simulation

Simulated distance (cm)	Energy with PTF (Norm.)	Energy no PTF (Norm.)	Energy saved (%)
0–1	0.202	1.000	79.78
1–2	0.263	1.000	73.75
2–3	0.391	1.000	60.92
3–4	0.674	1.000	32.59
4–5 $x > x_{max}$	0,072	1.000	92.78
5–6 $x > x_{-max}$	0,067	1.000	93.33

To solve this problem, the PTF described in Section 4.1 is used. The equations of the PTF described in Section 4.1 have to be transformed to determine the physical relation using the provided power by the reader and the corresponding supply voltage of the transponder as input parameters. The supply voltage is also unknown because of the lack of an integrated sensor at transponder side. To approximate this value the current power state of the transponder can be used. This means if the transponder is not responding, the supply voltage is too low for operation ($< U_t$). Otherwise, the transponder responds that the operation voltage is above the needed one ($> U_t$) as shown in Figure 6 (U_t is marked as red line). If the reader's provided power is altered until the transition from power down to idle state is reached, the value of the supply voltage from the transponder is slightly above U_t (see Figure 8).

The execution time needed for the approximation depends on the selected resolution of the power steps on reader-side. To use this method in practice, a balance between the power step resolution and the execution time needed for the algorithm has to be found. In case of ten steps this would also mean that four iterations have to be made with a successive approximation approach (2^n). This

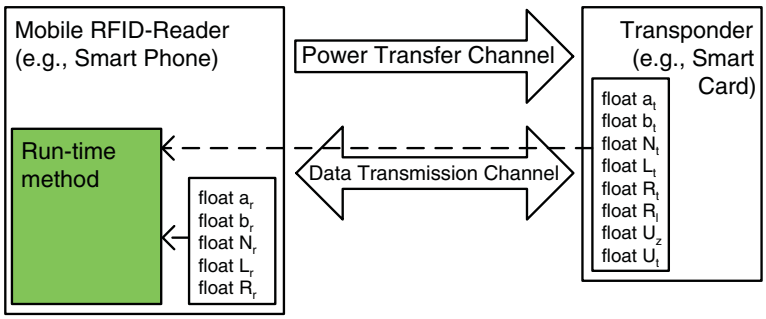


Figure 7 Distribution of the needed parameters. Distribution of the needed parameters to determine the PTF in the RFID-System and the possible paths to transfer them to a central location.

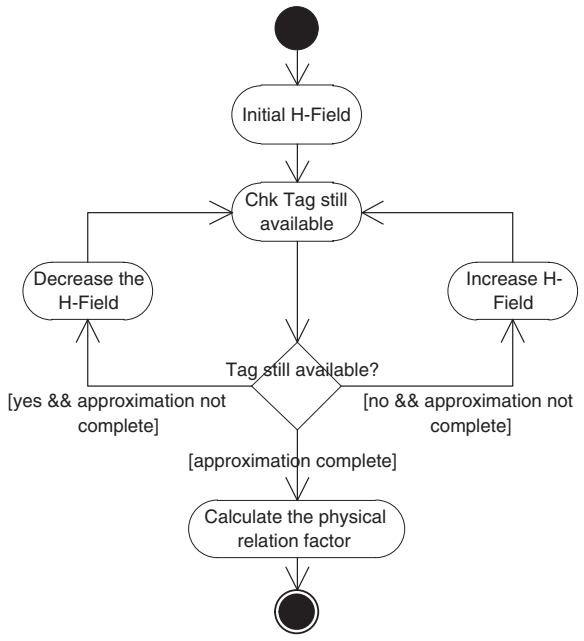


Figure 8 Used algorithm to approximate the physical relation factor between the reader and transponder needed for the determination of the PTF based on the ability to scale the magnetic field strength on reader side.

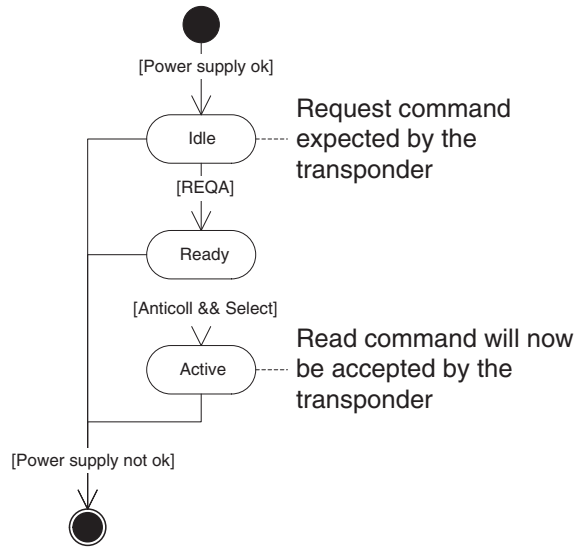


Figure 9 Simplified version of the state machine, adapted from [21], used to establish a connection between the reader and the transponder invoked by the reader (reader talks first).

leads to a longer time needed for the whole execution and an increase of needed energy compared to a simple card detection phase. To keep this overhead as small as possible the operation to proof if the transponder is responding (state "Chk Tag still available" as shown in Figure 8) should only invoke a small response and computation-effort for the transponder, which would otherwise lower the benefit of field strength scaling to save energy. In this approach, the request command (REQA) to the transponder can be used.

4.4 PTF-Determinator flow integration

The third consideration deals with the inclusion of the PTF-Determinator into the existing communication flow of reader and transponder. The transponder supports different states, which influence the accepted commands from the transponder (see Figure 9).

When the transponder receives enough power it switches to idle state. In this state, a request from the reader is expected. After the request is issued it is possible to select the card by sending an anti-collision command followed by a select command with the appropriate UID. After this procedure, the transponder enables extended commands like reading values from the memory. This read command is needed by the PTF-Determinator. If the power supply drops below a certain threshold (e.g., by exceeding the maximum transmission distance between reader and transponder) the state is set back to power down. To return to the active state the navigation through the state-machine of the transponder by sending a request (e.g., REQA) and select command has to be redone.

The integration of the PTF-Determinator method into the existing flow is split into three parts. The first part is executing the approximation algorithm as shown in Figure 8, but without calculating the physical relation factor. This approximation does not need any parameter information of the transponder, only a specified command to call. This can be REQA, which leads to a response which can be used to find out if the transponder is available or not. The second part is gathering the needed parameters from the transponder as shown in Figure 7, which needs to select the card to enable the command for reading. The third part is responsible for calculating the physical relation factor based on the gathered information from the other two parts. All needed information is now available to determine the PTF.

As last step of integration, it has to be defined, in which communication phase the PTF-Determinator is executed. As a first approach the method is included into the card detection phase. If a new transponder has been detected, the algorithm begins to determine the PTF, as described in the last paragraph, and is locked for operation until the method is finished. After that, the transponder is set to ready state and the wanted operations can be executed. Thanks to this approach, the knowledge of the PTF can be used after the card detection phase. Unfortunately, the time needed for this card detection phase increases.

Furthermore, changes to the PTF after this phase cannot be detected.

4.5 PTF library integration

The last consideration is to provide the determined PTF in form of a library, which can be used for power-management methods. This library is integrated on reader-side. It provides an application interface, which can be used to build a control loop to regulate the provided power of the reader according to the calculation result of the PTF. Furthermore, additional functions are provided by the interface to increase the optimization-possibilities (e.g., getting the current value of the physical relation factor to prevent long and power consuming transmission ranges). This design also makes it possible to integrate this as a hardware component to decrease the calculation time and to be more power efficient.

5 Case study

This section describes how the contributed method is implemented and tested. The overview is split into four parts. The first part describes the case study. In the second part, the simulation of the case study and the results are shown. In the third part, the implementation is deployed on real hardware and the measurement results are depicted. The fourth part consists of a measurement of a state-of-the-art mobile NFC-device (smart phone) and the comparison to the results of part two and three to evaluate the benefit to a mobile system.

5.1 Description of the case study

In this case study, the PTF-Determinator is implemented in an RFID-System. Furthermore, a feature to restrict the maximum transmission distance $x_{\max}$ between reader and transponder is implemented. When the limit is reached, the system automatically cuts off the power transfer to the transponder to save energy. As a use case the process of reading digital business cards is used. The flow diagram of the use case is shown in Figure 10.

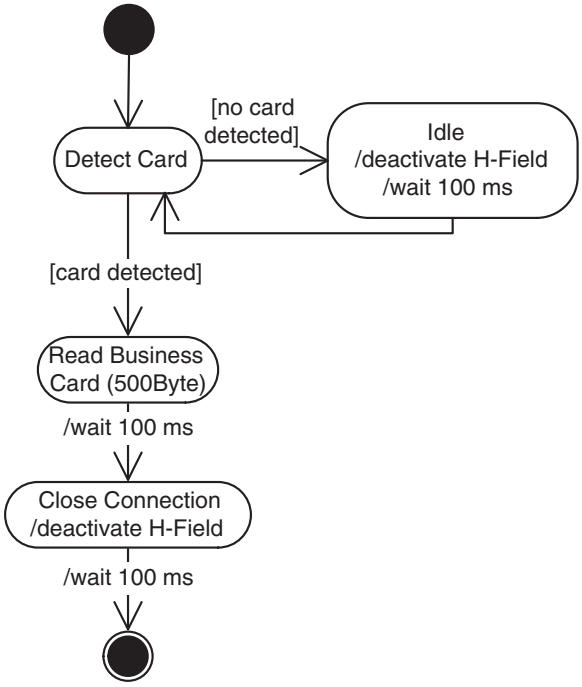


Figure 10 This flow diagram shows the use case of reading a digital business card using NFC. This use case is needed for the case study.

5.2 Simulation results

In the first phase, the PTF-Determinator is designed, implemented, and tested using a simulation model for an NFC-System consisting of reader and transponder. The program is an Android application running on an emulator and includes the functionality described in Section 5.1. The SystemC simulation model is based on the target NFC-System but the possible values for R_{rel} have been modified to show the potential of the method to approximate the physical relation factor over the whole transmission range. The original target hardware has limited possibilities to alter the value R_{rel}. The used simulation model features the possibility to provide the current power consumption of its components and the whole system. The model is implemented on transaction layer and is therefore not cycle accurate. The power values are based on the measurement results of the target NFC-Reader and transponder.

The simulation procedure is configured to step through different distances between reader and transponder. The simulator assumes that the two coils are oriented coaxial. The procedure is designed to wait until the execution of the PTF-Determinator with the described use case is finished before the next simulation with another distance is invoked. To deliver realistic results, the use case for reading digital business cards is used.

Figure 11 shows the comparison of the physical and the approximated relation factor of the method between the reader and the transponder. The steps of the approximation depend on the resolution of the R_{rel} (see Section 4.1). With the modified hardware (more possible values for R_{rel}), the physical relation factor can be approximated over the whole transmission range.

In Figure 12, the power consumption is shown when detecting a transponder with and without the PTF-Determinator. The case of $x > x_{\max}$ is shown in Figure 13. The power increase of the central processing unit is simulated using a simple power state machine on reader side. The result shows that the effectiveness of the PTF-evaluation depends on the time relation between

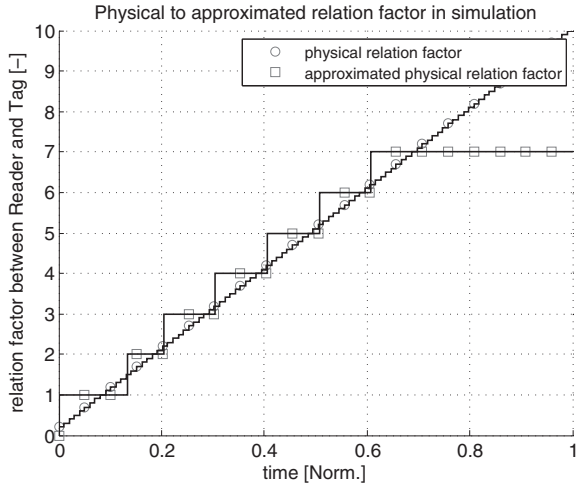


Figure 11 Result of simulation physical relation factor. This plot is generated by simulation, which shows the comparison of the physical relation factor and the approximated distance of the PTF-Determinator between reader and transponder.

the execution of PTF-Determinator and the use case. Figure 13 shows the result of the simulation in case of the physical relation factor $x > x_{\max}$. If this case occurs, the PTF-Determinator invokes a forced cut-off in the power transfer on reader side to the transponder. With this method an energy wastage is prohibited. A comparison of the saved energy in relation to the simulated distance d between reader and transponder is shown in Table 2.

The saved transmission energy (energy needed by the Reader-IC for the power transfer to the transponder) is as high as 80% in close distance. Thus, this approach offers a lot of potential in saving energy. This result depends on the use case and can only be achieved by adapting the hardware and no further influence is given by the environment. The benefit of saving energy decreases if the physical relation increases because the transmission power has to be increased to provide enough power for the transponder. If the physical relation factor x is higher than $x_{\max}$, then the power supply is cut off as described.

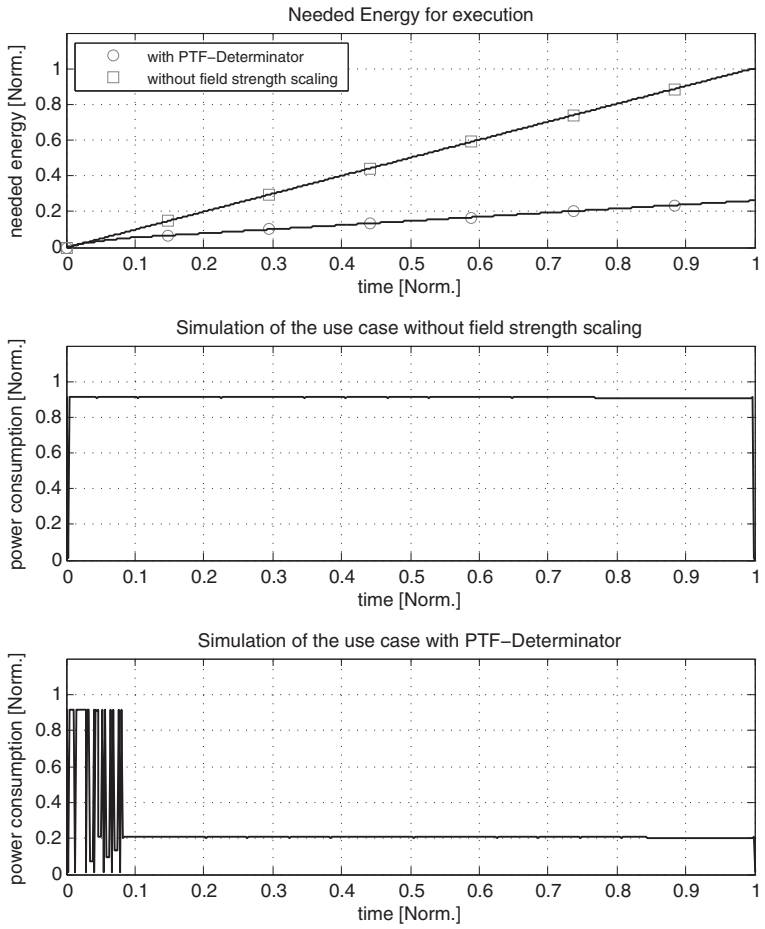


Figure 12 Result of simulation $x < x_{\max}$. The plot shows the simulation result, with the use case described in Figure 10, with and without an improved version of the PTF-Determinator from [1] under the condition $x < x_{\max}$.

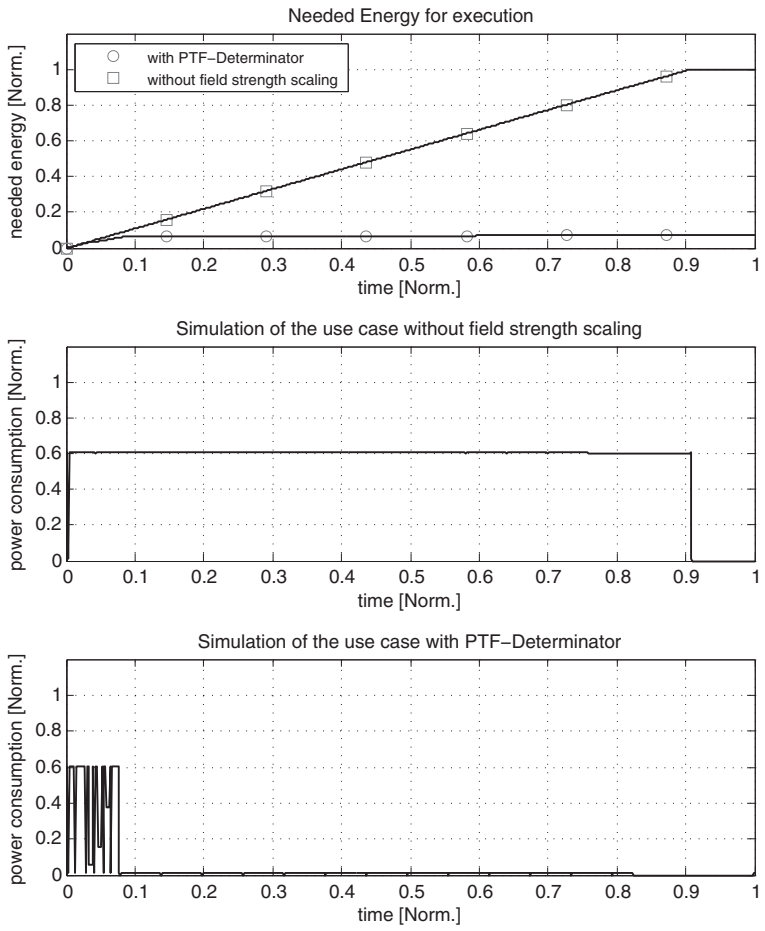


Figure 13 Result of simulation $x > x_{max}$. The plot shows the simulation result, with the use case described in Figure 10, with and without an improved version of the PTF-Determinator from [1] under the condition $x > x_{max}$.

This leads to a power saving of 93% with the disadvantage of loosing connectivity to the transponder. To reestablish a communication, the transponder's current physical relation factor has to be below the maximum allowed physical relation factor.

5.3 Measurement results

In the second phase, the PTF-Determinator is implemented and tested on real hardware. Power consumption measurements are conducted for verification purposes. The program is the same used during the simulation and includes the functionality described in Section 5.1. The used set-up is shown in Figure 14 and described in Table 3. To verify the method and compare the resulting power consumption of the simulation and a real environment behavior, the method is deployed and tested on a target NFC-System. To get the needed measurement data, the hardware is placed into a hardware-in-the-loop measurement suite. The suite is configured to acquire the power consumption of the whole system while the program under test is executed. For comparison, the use case of reading a digital business card without the PTF-Determinator is also measured. The physical relation between reader and transponder is altered to validate the functionality of the program and to evaluate its influence on its power consumption.

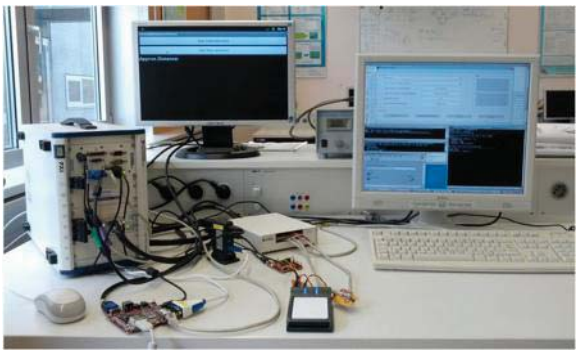


Figure 14 Setup used for the measurement of the use case. It consists of the development board, the RFID-Reader, the measurement device from National Instruments and an evaluation software in Matlab.

Table 3 The setup used for the power measurement needed for the case study

Program language	Java
Development board	Beagleboard
Operating system	Android 2.3.4
NFC-Reader	USB-Reader connected to the development board
Measurement device	Hardware-in-the-loop Measurement-suite

Figure 15 shows the power consumption of the NFC-System with and without the PTF-Determinator. In Figure 16, the power consumption of the NFC-System is shown when physical relation factor $x > x_{\max}$. This leads to cutting off the power supply of the transponder. This cut-off prevents the energy waste invoked by the power loss in the reader circuit and the loosely coupled power transfer to the transponder. The measurement results also show that the influence of the physical relation factor on the consumed energy, invoked by the influence of the reader and transponder coil, has to be considered. The execution of the PTF-Determinator results in a small overhead as shown in Figures 15 and 16.

In Table 4, a comparison between the simple card detection and the usage of the PTF-Determinator is made. It includes the needed energy of the whole procedure. The needed energy is compared and the saved energy can be evaluated when using the PTF-Determinator instead of the simple card detection. The approximation of the physical relationship is limited on the real hardware, because only few steps to scale the magnetic field are supported. However, it can be shown that the needed energy for the power transmission is 26% lower when considering the execution of the PTF-Determinator in case of $x <= x_{\max}$. The needed energy in case of $x > x_{\max}$ for the power transmission is about 75% lower compared to the use case without PTF-Determinator.

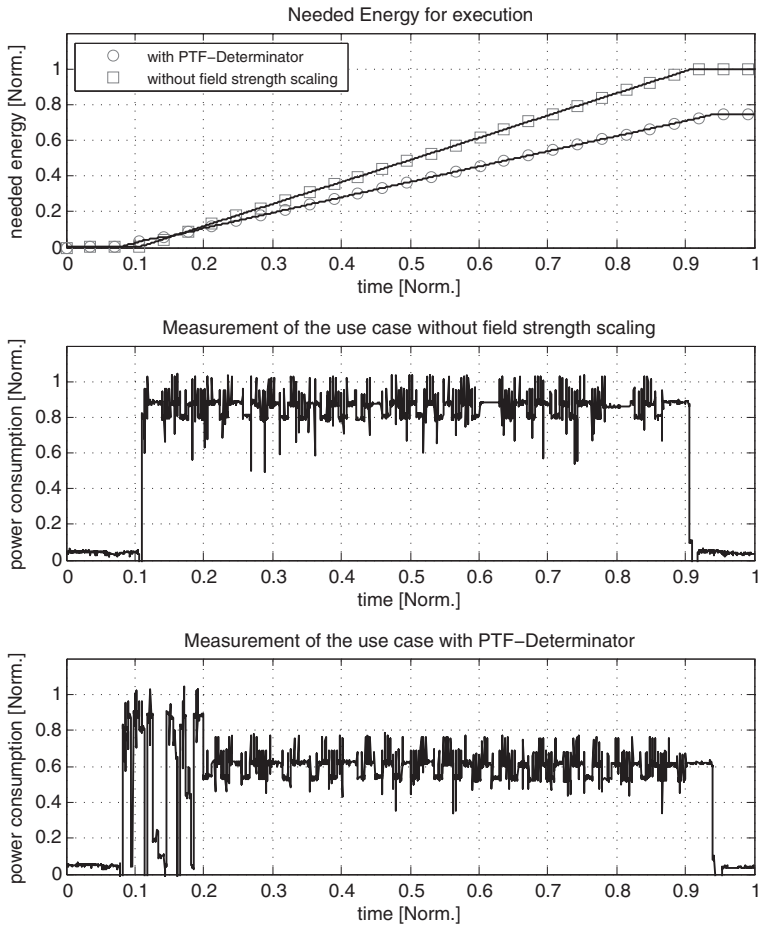


Figure 15 Result of the measurement $x < x_{\max}$. The plot shows the measurement result, with the use case described in Figure 10, with and without an improved version of the PTF-Determinator from [1] under the condition $x < x_{\max}$.

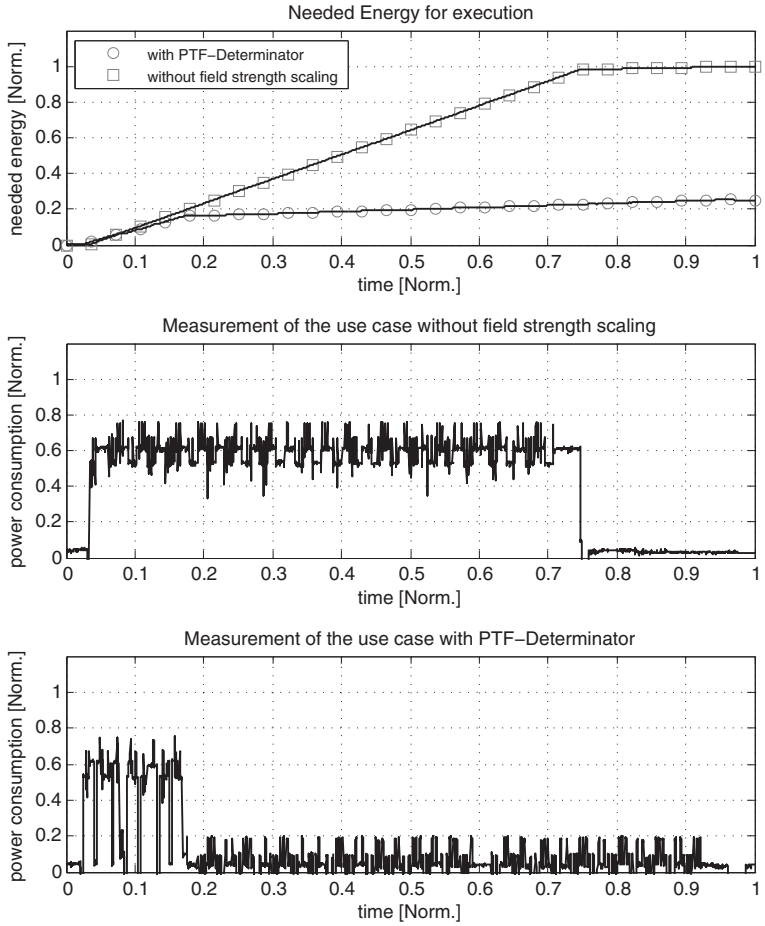


Figure 16 Result of the measurement $x > x_{max}$. The plot shows the measurement result, with the use case described in Figure 10, with and without an improved version of the PTF-Determinator from [1] under the condition $x > x_{max}$.

5.4 Comparison to an NFC-enhanced smart phone

In this section, a power measurement of a state-of-the-art smart phone is done. The idea is to get results, how field strength scaling is influencing the power consumption of such a device. The power consumption is measured directly at the battery source and therefore includes all components (e.g., display and processor). The measurement setup is listed in Table 5. The results of the simulation in Section 5.2 and the measurement in Section 5.3 can then be combined with this measurement to one result to get an approximation of the possible power reduction using field strength scaling on a state-of-the-art smart phone.

To achieve the evaluation goal, the power consumptions of the different smart phone states concerning the Reader-IC (RFID) (e.g., "reading the tag" or "RFID is powering the transponder") are extracted from the power measurement. The power consumption of the smart phone during the state idle and reading the transponder (tag) is shown in Figure 17. It can be seen that there is a significant

Table 4 Comparison of the saved energy for the RFID-Transmission in percent between the method with and without an improved version of the PTF-Determinator from [1] in the measurement

Physical	Energy with PTF (Norm.)	Energy without PTF (Norm.)	Energy saved (%)
$x <= x_{max}$	0.745	1.000	25.51
$x > x_{max}$	0.251	1.000	74.88

Table 5 The measurement setup for the acquisition of the smart phone's power consumption including the devices used for the measurement

Smart phone	Samsung Nexus S
Operating system	Android 2.3.4
Application	NFC TagInfo from NFC Research Hagenberg
Measurement device	PXI NI 6221 using DAQ SignalExpress
Transponder	Infineon Tag Type 2 (2kB)

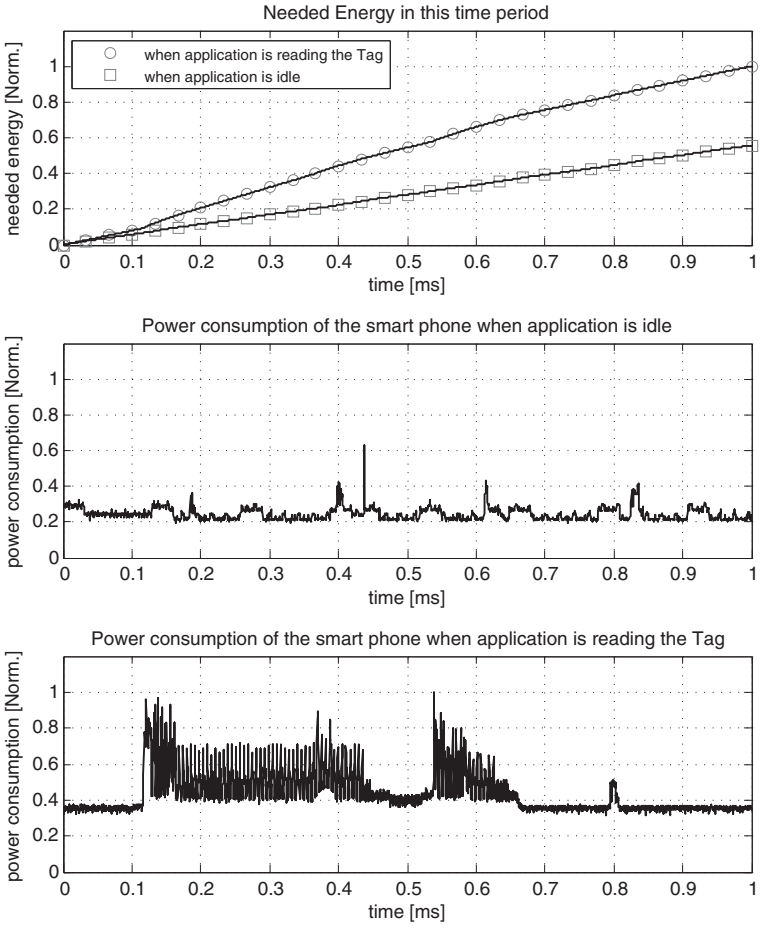


Figure 17 Power consumption of the state-of-the-art smart phone with NFC. This figure shows the power consumption during the execution of the application described in the measurement setup (see Table 3). The figure is divided into three plots, showing the energy consumption as well as the power consumptions in idle state and during the smart phone's reading process of the transponder.

smart phone power consumption rise during the process of reading the transponder. Table 6 shows this different power consumptions of the smart phone.

The extraction shows that during the reading process of the transponder the power consumption increases up to 107% compared to the idle state power consumption. Furthermore, the state while the transponder is powered by the Reader-IC without executing any operation consumes 50% more power. The presented numbers show that reducing this power consumption has potential of saving energy in the whole system (smart phone).

Table 6 Results of the state-of-the-art smart phone's measurement are presented in form of its power consumptions during different states

State	Consumed power [%]
NFC is on but no transponder in range	100
Transponder is powered over NFC	150
Transponder is powered over NFC and reading operations are performed	207

These results of a state-of-the-art smart phone are now used to scale the results (E_{unscaled}) of Sections 5.2 and 5.3 to get an approximation of the expectable results (E_{scaled}) of field strength scaling on a state-of-the-art smart phone using Equation 6.

$$E_{\text{scaled}} = 100 - \frac{(100 - E_{\text{unscaled}}) \cdot 1,07 + 100}{207} \cdot 100 \quad (6)$$

Theses combined results (transmission power saving and the power states of the art smart phone) show that approximately 41% of the energy can be saved compared to simulation with a modified hardware and 13% can be expected in a real environment without changing the hardware. In case of $x > x_{\max}$ the approximated saved energy is as high as 48% in simulation and 39% in a real environment.

6 Conclusion

The additional energy consumption by using RFID in mobile system is a challenging task. This article shows that magnetic field strength scaling in HF-Band RFID-Systems is a good way to reduce this energy wastage. The three investigations made are a way to deal with the challenges of the dynamic behavior during communication like the changing physical relation factor (e.g., the user is moving the transponder towards the reader). This study has also shown that the integration of the run-time method to determine the PTF on reader side is feasible. The energy saving potential of the presented PTF-Determinator, using the PTF to scale down the magnetic field strength, is shown by simulation and is verified through measurement. In simulation using a improved hardware model (more suitable steps to scale the magnetic field strength are included) up to 80% less transmission energy is needed. In the measurement, using existing hardware, the energy needed by the transmission is reduced by 26% compared to a simple card-detection method. Thus, a state-of-the-art NFC smart phone featuring our proposed method would reduce the battery drain by up to 13%. The implemented feature to set a maximum physical relation factor, by cutting off the power supply to avoid energy-consuming transactions, has been proven by measurement to reduce the transmission energy by up to 75%. This results into a reduction of 39% less battery drain of a state-of-the-art smart phone.

The combination of simulation and verification through measurement in one tool chain has proven to be a good way for developing power-aware systems. The simulation gives the opportunity of reconfiguring the hardware (design hardware and software together) to evaluate the potential of ideas like magnetic field strength scaling.

In future work, the proposed PTF-Determinator method shall be improved, focusing on optimizing the approximation of the physical relation factor. Furthermore, the other investigations made regarding the dynamic field strength scaling during communication and the usage in an environment with multiple transponders will be verified by simulation and measurement.

Competing interests
The authors declare that they have no competing interests.

Acknowledgements
We would like to thank our industrial partners Infineon Technologies Austria AG as well as Enso Detego GmbH for their support. Furthermore, 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 FFG 829586.

Author details
[1]Graz University of Technology, Graz, Austria. [2]Infineon Technologies Austria AG, Graz, Austria.

Received: 30 October 2012 Accepted: 18 March 2013
Published: 16 April 2013

References

1. M Menghin, N Druml, C Steger, R Weiss, J Haid, H Bock, in *Fourth International EURASIP Workshop on RFID Technology (EURASIP RFID) 2012*. The PTF-Determinator: a run-time method used to save energy in NFC-Systems (Turin, 2012), pp. 92–98
2. M Menghin, N Druml, C Steger, R Weiss, J Haid, H Bock, in *5th International Workshop on Near Field Communication (NFC 2013)*. NFC-DynFS: a way to realize dynamic field strength scaling during communication (Zurich, 2013), pp. 1–6
3. D Cheng, Z Wang, Q Zhou, in *4th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM'08)*. Analysis of distance of RFID systems working under 13.56 MHz (Dalian, 2008), pp. 1–3
4. J Clulow, GP Hancke, MG Kuhn, T Moore, in *Third European conference on Security and Privacy in Ad-Hoc and Sensor Networks (ESAS'06)*. So, near and yet so far: distance-bounding attacks in wireless networks (Springer, New York, 2006), pp. 83–97
5. X Xu, L Gu, J Wang, G Xing, in *IEEE International Conference on Pervasive Computing and Communications (PerCom 2010)*. Negotiate power and performance in the reality of RFID systems (Mannheim, 2010), pp. 88–97
6. Wireless Power Consortium. System Description Wireless Power Transfer, Vol. I, Part 1, (2011), p. 32. http://www.wirelesspowerconsortium.com/downloads/wireless-power-specification-part-1.html. Accessed 11 April 2013
7. M Wendt, M Grumer, C Steger, R Weiss, U Neffe, A Muehlberger, in *Proceedings of the 2008 ACM Symposium on Applied Computing (SAC'08)*. System level power profile analysis and optimization for smart cards and mobile devices (ACM, New York, 2008), pp. 1884–1888. doi:10.1145/1363686.1364144
8. A Genser, C Bachmann, C Steger, R Weiss, J Haid, in *IEEE Asia Pacific Conference on Circuits and Systems (APCCAS 2010)*. Estimation-based run-time power profile flattening for RF-powered smart card systems, (Kuala Lumpur, 2010), pp. 1187–1190
9. T Lohmann, M Schneider, C Ruland, in *Smart Card Research and Advanced Applications, vol. 3928 of Lecture Notes in Computer Science*, ed. by J Domingo-Ferrer, J Posegga, and D Schreckling. Analysis of power constraints for cryptographic algorithms in mid-cost RFID tags (Springer, Berlin, 2006), pp. 278–288. doi:10.1007/1173344720
10. J Mercier, C Dufaza, M Lisart, in *Proceedings of the 2007 International Symposium on Low Power Electronics and Design (ISLPED'07)*. Signoff power methodology for contactless smartcards (ACM, New York, 2007), pp. 407–410. doi:10.1145/100000
11. E Rolf, V Nilsson. Near field communication (NFC) for mobile phones (Master's Thesis, Lund University, 2006), p. 25. http://www.es.lth.se/teorel/Publications/TEAT-5000-series/TEAT-5082.pdf. Accessed 11 April 2013
12. N Druml, M Menghin, C Steger, R Weiss, A Genser, J Haid, in *15th Euromicro Conference on Digital System Design (DSD 2012)*. Adaptive field strength scaling—a power optimization technique for contactless reader/ smart card systems (Izmir, 2012), pp. 616–623
13. N Kamineni, X Li, in *International Conference on Computing Communication and Networking Technologies (ICCCNT 2010)*. Analysis of anti-collision multi-tag identification algorithms in passive RFID systems (Karur, 2010), pp. 1–8
14. DF Tseng, ZC Lin, Anti-collision algorithm with the aid of interference cancellation and tag set partitioning in radio-frequency identification systems. IET Commun. **3**, 143–150 (2009)
15. K Wu, Y Liu, in *Second International Conference on Future Networks (ICFN'10)*. A new energy-aware scheme for RFID system based on ALOHA (Sanya, Hainan, 2010), pp. 149–152
16. J Liu, W Tong, in *IEEE International Conference on Cloud Computing and Intelligence Systems (CCIS 2011)*. Dynamic share energy provisioning service for one-hop multiple RFID tags identification system, (Beijing, 2011), pp. 342–347
17. J Haid, W Kargl, T Leutgeb, D Scheiblhofer, in *Proceedings of Telecommunications and Mobile Computing Graz Series (TCMC 2005)*. Power management for RF-powered vs. battery-powered devices, (Graz, 2005)

18. A Roy, SM Rumble, R Stutsman, P Levis, D Mazières, N Zeldovich, in *Proceedings of the sixth conference on Computer systems, (EuroSys'11)*. Energy management in mobile devices with the cinder operating system (ACM, New York, 2011), pp. 139–152. doi:10.1145/1966445.1966459
19. K Finkenzeller, *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification*, 2nd edn. (Wiley, New York, 2003)
20. X Xu, L Gu, J Wang, G Xing, SC Cheung, Read more with less: an adaptive approach to energy-efficient RFID systems. IEEE J. Sel. Areas Commun. **29**(8), 1684–1697 (2011)
21. W Rankl, W Effing, *Smart Card Handbook: Physical and Electrical Properties*, 3rd edn. (Wiley, New York, 2003)

doi:10.1186/1687-3963-2013-4
Cite this article as: Menghin *et al.*: **Using field strength scaling to save energy in mobile HF-band RFID-systems.** *EURASIP Journal on Embedded Systems* 2013 **2013**:4.

2012 Fourth International EURASIP Workshop on RFID Technology

The PTF-Determinator: A run-time method used to save energy in NFC-Systems

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

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

***Abstract* - Near Field Communication (NFC) in mobile devices like smart phones shows potential for applications like payment, identification, etc. Unfortunately the needed functionality increases the battery drain of the device. As a countermeasure power-management techniques are implemented. However, these techniques commonly don't control the power transfer to the tag to prevent wasting energy.**

To adapt this transfer during run-time the properties of the reader, tag and the physical relation between them are needed. This paper proposes a method called PTF-Determinator. It determines the Power Transfer Function (PTF) during run-time and scales the provided power transfer accordingly to save energy.

As a case study the PTF-Determinator is integrated into the tag-detection algorithm. Investigations are made regarding the power consumptions and timings through simulation and measurement on a development platform for mobile phones. The results show that 12% of the energy can be saved on average.

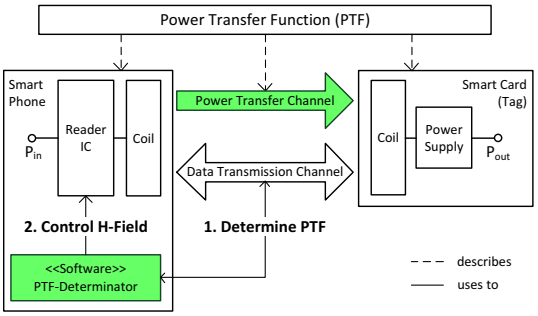


FIGURE 1 - PROPOSED PTF-DETERMINATOR AND THE INTEGRATION INTO THE NEAR FIELD COMMUNICATION SYSTEM

I. INTRODUCTION

Mobile devices like smart phones featuring a Near Field Communication (NFC) interface open a wide set of applications like payment, identification and ticketing. The integration of NFC increases the battery drain because of the additional power-consumption through the needed reader when active. Minimizing the consumption is the goal of the power-management algorithms implemented in software and hardware. These algorithms commonly focus on one component and not the whole system. In our case the component is the NFC-reader, which has to transfer power to the tag (see Figure 1). Currently the reader is able to scale the magnetic field strength during run-time, but has no access to information about the connected tag or the power transmission path between them. Therefore, the field strength is configured statically. In most cases the power output is set to a maximum value to ensure the expected (about 5-10 cm) transmission distance regardless of the tag-type. This power output produces losses in the antenna circuit. A dynamic configuration of the magnetic field strength during run-time reduces this losses and this waste of energy.

The challenge to perform the dynamic configuration is to collect the needed information during run-time and to determine the power transfer function (PTF) on the reader side. With the determined PTF the field strength can be dynamically scaled. To realize the above described steps the NFC-system has to be defined and examined. The scoped system consists of one reader and one tag. The wireless communication channel between them can be split into two main parts. The first part deals with the power transmission path. It describes how the provided power, which can be altered by the reader, is transfered to the tag. The physical principle of the power transmission is inductive coupling (see Figure 2). This can be represented through the the PTF. Several parameters for the PTF are needed for determination. These are the reader characteristics, and coil properties, the parameters needed to calculate the inductive coupling (e.g. physical relationship between the two coils), as well as the parameters of the tag's coil and power supply. The second part deals with the data-transfer path. This path can be used to obtain information about the available tag if enough power is provided by the power-transfer path. These both parts are available for realizing a dynamical approach to reduce the power consumption. The contribution of this paper consists of two parts:

- Introduction of the novel PTF-Determinator method, which determines the PTF during run-time and scales the magnetic field strength based on the result to save energy (see Figure 1).
- Implementation of the presented PTF-Determinator in a reader device and add a feature to set a maximum physical relation factor to avoid energy consuming transmissions, which are not necessary

The paper is split into five main parts. The first part describes the electrical characteristics used for this approach (see Section II.). As second part, which can be found in Section III., the method is shown in detail and how it is integrated into the system. The third part can be found in Section IV., which shows the related work and highlights our contribution. For evaluation the fourth part in Section V. presents experimental results when using this method. The fifth part in Section VI. finally concludes this work

II. ELECTRICAL CHARACTERISTICS

This Section explains the used replacement circuit and equations for the method to calculate the PTF. The equations describe how the power is transferred from the Reader-IC to the supply of the tag and the replacement circuit describes the connection between them, as shown in Figure 2. The calculation is split into four parts.

The first part describes the power control of the NFC-Reader, which can be configured by a resistance (R_{rel}) serial to a constant voltage-source (U_1). This is shown in Equation 1.

$$i_r = \frac{U_1}{Z_c + R_{rel}} \tag{1}$$

Increasing the resistance leads to a reduction of the overall power (decrease of i_r) consumption with the disadvantage of loosing transmission range [1]. The current i_r also depends on the configurable resistance R_{rel} and the input resistance Z_c of the circuit beyond. Z_c alters with the inductive coupling between reader and tag and is

978-0-7695-4813-5/12 $26.00 © 2012 IEEE
DOI 10.1109/RFID.2012.12

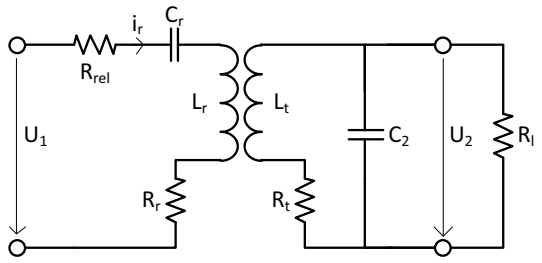


FIGURE 2 - REPLACEMENT CIRCUIT TO DESCRIBE THE POWER TRANSFER FROM THE READER TO THE TAG WITHOUT THE VOLTAGE REGULATION ON TAG- SIDE, ADAPTED FROM [2]

therefore not static. The second part consists of the equation used to calculate the provided magnetic field H of the reader, which is provoked by the electrical current i_r. The considered orientation of the sender and receiver coil is shown in Figure 3.

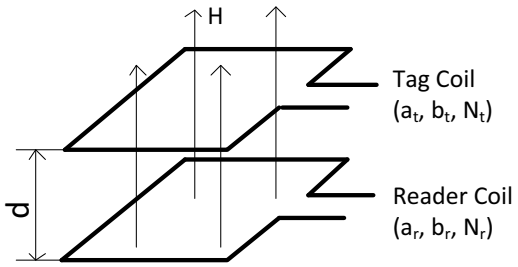


FIGURE 3 - CONSIDERED COAXIAL ORIENTATION BY USING RECTANGULAR SHAPED SENDER AND RECEIVER COILS

Equation 2 can be used for rectangular shaped sending coils and is based on the law of Biot-Savart. It is based on the physical principle of loose inductive coupling. The needed parameters are the dimensions a_r and b_r of the reader coil and the number of windings N_r. The distance to the coil can only be used when the coils are coaxial oriented [2].

$$H = \frac{i_r \cdot N_r \cdot a_r \cdot b_r}{4 \cdot \pi \cdot \sqrt{(\frac{a_r}{2})^2 + (\frac{b_r}{2})^2 + d^2}} \cdot (\frac{1}{(\frac{a_r}{2})^2 + d^2} + \frac{1}{(\frac{b_r}{2})^2 + d^2}) \quad (2)$$

The third part deals with the transformation of the magnetic field strength back to a voltage on tag side (see Figure 2). A resonance circuit, consisting of a parallel capacitance and the coils inductance, is used to amplify the received voltage. First of all the coupling coefficient is calculated with Equation 3 and 4. The coefficient represents an abstract relation between reader and tag and requires the magnetic field strength as input. Equation 5 calculates the resulting voltage on tag-side. This is only valid for a rectangular receiver coils. The needed parameters are the dimensions a_t and b_t, the number of windings N_t, and the coil's inductance L_t [2].

$$M_{12} = \frac{\mu_0 \cdot H \cdot N_t \cdot a_t \cdot b_t}{i_r} \quad (3)$$

$$k = \frac{M_{12}}{\sqrt{L_r \cdot L_t}} \quad (4)$$

$$u_2 = \frac{w \cdot k \cdot \sqrt{L_r \cdot L_t} \cdot i_r}{\sqrt{(\frac{(w \cdot L_t)}{R_l} + w \cdot R_t \cdot C_2)^2 + (1 - w^2 \cdot L_t \cdot C_2 + \frac{R_t}{R_l})^2}} \quad (5)$$

The fourth part describes that the output voltage is limited by a Zener-diode. The reason is the power supply of the tag which needs a certain operation voltage. It is also necessary to provide a minimum voltage. If the supply exceeds the minimum threshold voltage the circuit is set to power down. Figure 4 shows an example of the relation between the the distance between the reader and the tag and the supply voltage of the tag (the power consumption of the tag is considered static). Multiple power outputs are shown to visualize the dependency between the power output and the transmission distance.

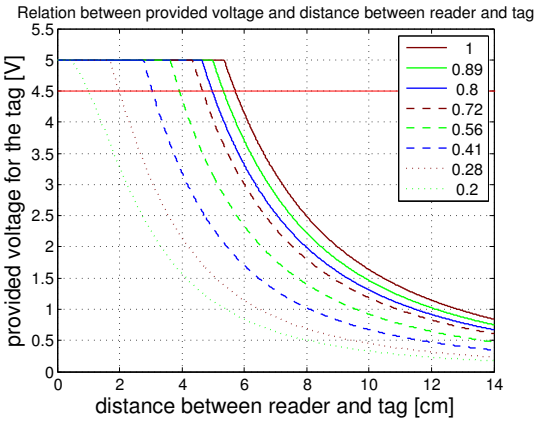


FIGURE 4 - RELATION BETWEEN THE SUPPLY VOLTAGE OF THE TAG AND THE DISTANCE TO THE READER USING. THE RELATION IS SHOWN USING DIFFERENT INPUT POWER LEVELS AS DESCRIBED IN THE LEGEND. THE TWO COILS ARE ORIENTED COAXIAL.

III. METHOD

In this Section the method is shown how to realize this PTF-Determinator. The realization is split into four considerations to be made. The first one deals with gathering the needed parameters from the reader and tag. The second relates to the evaluation of the physical relation factor, which can not be acquired directly. The third consideration deals with the integration of the method into the NFC-System's existing communication flow. The fourth consideration describes a library providing an interface to access the determined PTF. This library can be used can be used for power management methods.

3.1 Gathering needed parameters

As first consideration the needed parameters have to be collected from the NFC-System which are distributed between reader and tag. Some of them are physical values which have to be stored in digitalized form. Because of the system's variability during run-time (e.g. different tags), the storage of all parameters in a single location is inappropriate. Table 1 depicts the number of parameters, their location, and their required space.

These parameters shall be provided on the described location (see Figure 5). One approach is to store this data into a memory during the device's production phase (reader and tag). The needed storage space is 32 byte on tag-side if an accuracy of 32 bit is used. In practice the needed storage can be decreased by adapting the resolution of the values according to the needed PTF accuracy requirements. An example is shown in Table 1 where the needed space is reduced to 8 bytes.

location	number of parameters	accuracy [b]	space [B]
Mobile Reader	5	32	20
		8	5
Tag	8	32	32
		8	8

TABLE 1 - NUMBER OF PARAMETERS NEEDED FOR THE PTF-DETERMINATOR INCLUDING THEIR LOCATION AND NEEDED SPACE IN BYTES. THE SPACE IS SHOWN WITH DIFFERENT ACCURACIES OF THE PARAMETERS.

These values have to be transferred to a central processing unit. This can either be the reader or the tag. In this case the reader has been chosen because of its advanced computational resources and a direct control of the needed input parameters for the PTF (parameter of provided power). This also means that the parameter-values from the tag have to be transfered to the reader which can be costly in terms of time and power. For comparison, sending ping request to the tag requires 7 bit and results in a 2 byte response [2]. The request could be the same size but the response would be 16 times greater. If the bit length of the sent values is reduced to eight bits which should be enough in practice, the bytes to sent can be four times greater.

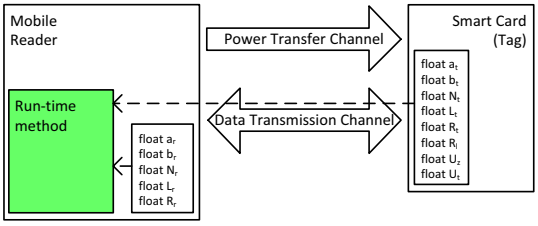


FIGURE 5 - DISTRIBUTION OF THE NEEDED PARAMETERS AND TRANSFER TO A CENTRAL PROCESSING UNIT

3.2 Evaluation of the physical relation factor

The second consideration regards the physical relation factor, which is independent from the type of reader and tag used. Furthermore, its value is unknown and has to be evaluated during run-time. It can not be directly measured because of the lack of sensing mechanisms on both sides.

To solve this problem the PTF described in Section II. is used. The equations described in Section II. have to be transformed to determine the physical relation using the power provided by the reader and the corresponding output voltage as input parameters. The output voltage is also unknown because of the lack of an integrated sensor at tag side. To approximate this value the current power state of the tag can be used. This means if the tag is not responding the supply voltage is too low for operation ($< U_t$) and if the tag responds the operation voltage is above the needed one ($> U_t$). If the reader's provided power is altered until the transition from power down to idle state is reached, the value of the supply voltage from the tag is slightly above U_t (see Figure 6). The approximation depends on the resolution of the power steps. To use this method in practice, a balance between power step resolution and the needed time of the algorithm has to be found. In case of ten steps this would also mean that four iterations have to be made with a successive approximation approach. This leads to a longer time needed for calculation and more needed energy compared to a simple card-detection. To keep this overhead as small as possible the operation to proof if the tag is responding should only invoke a small response and computation-effort for the tag. The request command to the tag can be used. To improve the approximation the tag

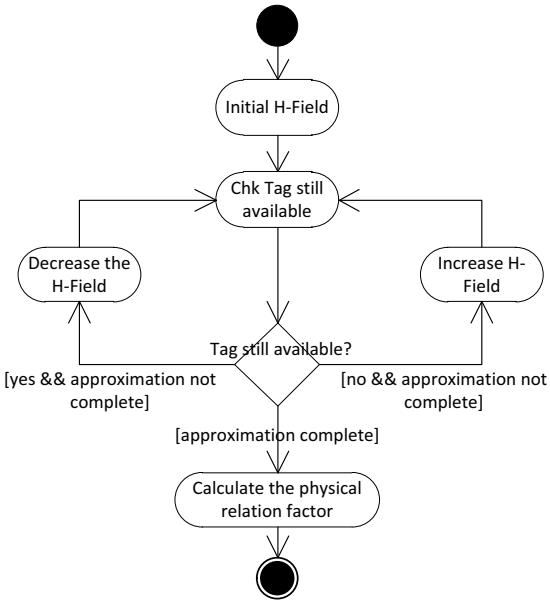


FIGURE 6 - USED ALGORITHM TO APPROXIMATE THE DISTANCE BETWEEN THE READER AND TAG

can provide information about the power consumption when sending this command.

3.3 PTF-Determinator flow integration

The third consideration deals with the inclusion of the PTF-Determinator into the existing communication flow of reader and tag. The tag has different states, which influence the provided functionality (see Figure 7).

When the tag gets enough power it switches to idle state. In this state a request from the reader is expected . All other commands are ignored. After the request is issued it is possible to select the card by sending a anti-collision- followed by a select-command with the appropriate unique identifier (UID). After this procedure, the tag enables extended commands like reading values from the memory. This command is needed by a part of PTF-Determinator. If the power supply drops below a certain threshold (e.g. through exceeding the maximum transmission distance between reader and tag) the state is set back to power down. To get back to the active state the navigation through the state-machine of the tag by sending a request and select has to be redone. To integrate the method into the existing flow, it is split into three parts. The first part is executing the approximation algorithm as shown in Figure 6 but without calculating the physical relation factor. This approximation does not need any parameter information of the tag, only a specified command to call. This can be REQA, which leads to a response which can be used to find out if the tag is available or not. The second part is gathering the needed parameters from the tag as shown in Figure 5, which needs to select the card to enable the command for reading. The third part is responsible for calculating the physical relation factor based on the gathered information from the other two parts. All needed information is now available to determine the PTF.

As last step of integration it has to be defined in which communication phase the PTF-Determinator is executed. As first approach the method is included into the card detection phase. If a new tag has been detected, the algorithm begins to determine the power transfer function, as described in the last paragraph, and is locked for operation until the method is finished. After that, the tag is set to ready state

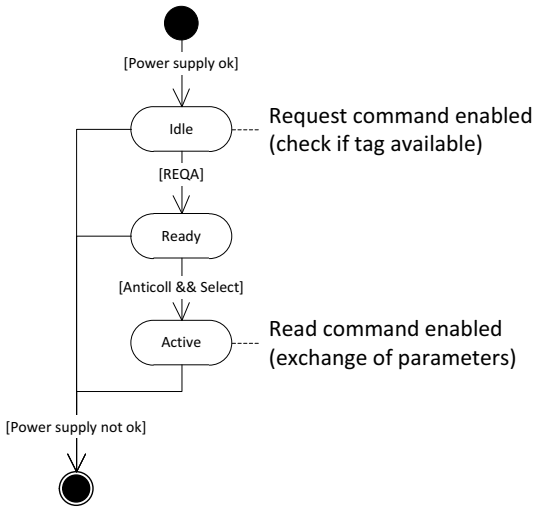


FIGURE 7 - SIMPLIFIED STATE MACHINE ADAPTED FROM [3] USED TO ESTABLISH A CONNECTION BETWEEN THE READER AND THE TAG INVOKED BY THE READER (READER TALKS FIRST)

and the wanted operations can be executed. Thanks to this approach, the knowledge of the PTF can be used in an early stage. Unfortunately the time needed to set-up the connection to the tag is also increased. Furthermore, changes after the set-up can not be detected. Another possibility is to periodically update the power transfer function while being connected to the tag. It has to be considered that this may be very costly in time and power consumption terms. Furthermore, the designed algorithm influences the power state of the tag and it may be necessary to reestablish the connection to the tag and restore the state.

3.4 Power transfer function library integration

The last consideration is to provide the determined PTF in form of a library, which can be used for power-management methods. This library is integrated on reader-side. It provides an interface for the application, which can be used to build a control loop to regulate the provided power of the reader according to the calculation result of the PTF. Furthermore, additional functions are provided by the interface to increase the optimization-possibilities (e.g. getting the current value of physical relation factor to prevent unwanted transmission ranges). This design also makes it possible to integrate this as a hardware component to decrease the calculation time and to be more power efficient.

IV. RELATED WORK

This Section is split into three parts. The first part deals with the state-of-the-art possibilities to acquire the physical relation factor. The second part shows investigations regarding the influence of the passive tag's power requirements. In the third and last part known system based concepts including reader and tag are shown.

4.1 Acquisition of the physical relation factor during run-time

One consideration regards acquiring the physical relation like the distance between the two coils and other dynamic parameters during run-time. An approach is to find a known parameter that describes this physical relation. Cheng Da et al. shows that there is a relation between the sent power of the reader and the distance to the tag. The analysis has been concluded by altering the signal strength of the reader and checking if the tag has enough power to be active [4]. Another approach is distance bounding, which uses the delay between the request and the response as known parameter to calculate the physical distance between reader and tag to detect relaying attacks [5]. To use this information to determine the PTF, the parameter has to be measured during run-time. Furthermore, transmission characteristics (e.g. coil dimensions) have to be included into the determination. These characteristics depend on the system's setup which also depend on the set-up of the system (e.g. different types of tags). Xunteng Xu et al. uses power stepping to detect different positioned tags (distance to the reader) in its environment [6]. This consideration does not include the physical principles of the power transfer but leads to a evaluation of a parameter, close to the distance, during run-time. Another method is through sensing the voltage on tag side and to use it for determination of the power transfer function [7].

4.2 Power requirements of the passive tag

Another fact which has to be considered is that the tag is passive and it's supply depends on the provided supply from the reader [8]. This means that the tag cannot respond if the provided power falls under the threshold. Furthermore the power consumption of the tag itself depends on the current executed operation which influences the level of needed power [9]. Power consuming operations are especially encryptions/ decryptions [10]. Julien Mercier et al. show the relation between the provided power and the consumption of the circuit [11]. To consider this in the determination of the PTF the tag has to be in a state that is aware of its power consumption. The last point of consideration is the transmission of the data (response), which is realized through ohmic load modulation on tag side. The influence on the modulation is similar to the power consumption of the tag [12].

4.3 System based power-management for NFC

Jianhua Liu et al. describe energy provisioning services. They show that knowing the system can lead to optimization possibilities. Their concept focuses on multi-tag multi-reader application but it can be adapted to this problem [13]. This knowledge can be used to optimize the system in terms of power consumption and stability. This should be especially considered in combination with mobile readers [14]. The challenge is to manage the distributed information and the calculation among the system for power-optimization and usability. The Cinder operating system is an example how such optimizations can be done by including the whole system. This approach is designed for smart phones but the model can be extended to include external powered devices as well [15].

V. EXPERIMENTAL RESULTS

This Section gives an overview over the the practical work, describing how the contributed method is implemented and tested. The overview is split into three parts. The first part describes the implementation and how it was done. In the second part the simulation of the case study is described and the results are shown. In the third part the implementation is deployed on real hardware and the measurement results are shown.

5.1 Case Study: Limiting the physical relation factor

In this case study the PTF-Determinator is implemented on reader-side in the card detection phase. The result of the method is used to scale the magnetic field strength according to the determined PTF. Furthermore, the result is used to limit the physical relation factor x_{max} between reader and tag. When the limit is reached, the system automatically cuts off the power transfer to the tag to save energy. The power consumption and timings are examined in two phases of development. In the first phase, the design is run on a simulation model. In the second phase the design is implemented and deployed on real hardware and measured for verifications in terms of the power consumption and the timing.

5.2 Simulation of the PTF-Determinator

In the first phase the PTF-Determinator is designed, implemented and tested using a simulation model for a NFC-System consisting of reader and tag. The program is based on C++ and includes the functionality described in Section 5.1. The SystemC simulation model is based on the target NFC-System but the possible values for R_{rel} have been modified to show the possibility of the method to approximate the physical relation factor over the whole transmission range. The original target hardware has limited possibilities to alter the value R_{rel}.

The used simulation model has the possibility to provide the current power consumption of its components and the whole system. The model is implemented on transaction layer and is therefore not cycle accurate. The power values are based on measurement results of the target NFC-reader and tag.

The simulation procedure is configured to step through different distances between reader and tag. The simulator assumes that the two coils are oriented coaxial. The procedure is designed to wait until the execution of the PTF-Determinator is finished before the next step is invoked. To deliver more realistic results, a certain time is waited after the detection, which represents the transaction process.

Figure 8 shows the comparison of the physical and the approximated relation factor of the method between the reader and the tag. The steps of the approximation depend on the resolution of the R_{rel} (see Section II.). With the modified hardware (more possible values for R_{rel}) the physical relation factor can be approximated over the whole transmission range.

In Figure 9 the power consumption is shown when detecting a tag with and without the PTF-evaluation. The case of $x > x_{max}$ is shown in Figure 10. The power increase of the central processing unit is simulated with a 10% on reader side while executing the method. The result shows that the effectiveness of the PTF-evaluation depends on the time needed for the data exchange between the reader and the tag. If this time is is smaller then the evaluation time the overhead gets to great to save energy.

Figure 10 shows the result of the simulation in case of the physical relation factor $x > x_{max}$. This leads to a forced cut-off in the power transfer on reader side to the tag. With this method a energy wastage is prohibited.

A comparison of the saved energy in relation to the simulated distance d between reader and tag is shown in Table 2. The saving decreases if the physical relation increases because the transmission power has to be increased to provide enough power for the tag. If the physical relation factor x is higher than x_{max}, then the power supply is cut off to prevent a waste of energy. This leads to a power saving of 44% with the disadvantage of loosing connectivity to the tag. To reestablish a communication, the tag's curent physical realtion factor has to be below the maximum allowed physical relation factor.

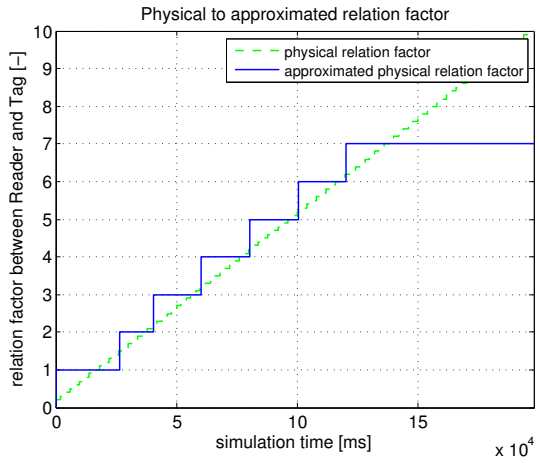


FIGURE 8 - RESULT OF SIMULATION, WHICH SHOWS THE COMPARISON BETWEEN THE PHYSICAL AND THE APPROXIMATED DISTANCE OF THE PTF-DETERMINATOR BETWEEN READER AND TAG

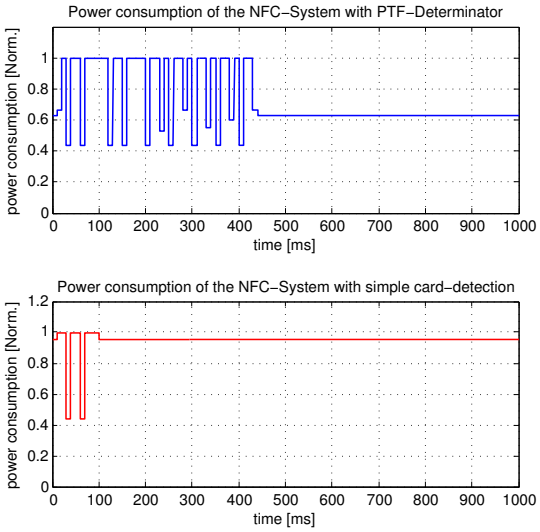


FIGURE 9 - RESULT OF SIMULATION, WHICH SHOWS THE DETECTION OF THE TAG WITH AND WITHOUT THE PTF EVALUATION IN CASE $x < x_{max}$

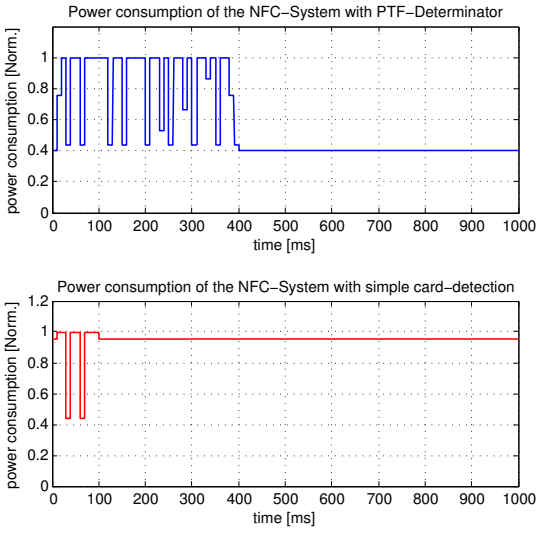


FIGURE 10 - RESULT OF SIMULATION, WHICH SHOWS THE DETECTION OF THE TAG WITH AND WITHOUT THE PTF EVALUATION IN CASE $x > x_{max}$

Simulated distance [cm]	Energy with PTF [Norm.]	Energy no PTF [Norm.]	Energy saved [%]
0-1	0,561	1.000	43.87
1-2	0.663	1.000	33.71
2-3	0.682	1.000	31.79
3-4	0.753	1.000	24.71
4-5 $x > x_{max}$	0.558	1.000	44.17
5-6 $x > x_{max}$	0.558	1.000	44.17

TABLE 2 - COMPARISON OF THE SAVED ENERGY IN PERCENT BETWEEN THE METHOD WITH AND WITHOUT PTF EVALUATION IN THE SIMULATION

5.3 Measurement of the PTF-Determinator

In the second phase the PTF-Determinator is implemented and tested on real hardware. Power consumption measurements are conducted for verification purposes. The program is based on Java and includes the functionality described in Section 5.1. The used set-up is described in Table 3.

Program language	Java
Development board	Beagleboard
Operating system	Android 2.3.4
NFC-Reader	USB-Reader connected to the development board
Measurement device	hardware-in-the-loop measurement-suite

TABLE 3 - SET-UP FOR THE MEASUREMENT

To verify the method and compare the resulting power consumption of the simulation and a real environment behavior, the method is deployed and tested on a target NFC-System. To get the needed measurement data, the hardware is placed into a hardware-in-the-loop measurement suite. The suite is configured to acquire the power consumption of the whole system while the program under test is executed. For comparison a simple card-detection is also implemented and measured. The physical relation between reader and tag is altered to validate the functionality of the program and to evaluate its influence on it's power consumption. The measurement window is set to 5000 ms.

Figure 11 shows the power consumption of the NFC-System with and without the PTF-Determinator. The time needed by the method is about four times higher than the simple card detection. Using the PTF-Determinator the power consumption is about 25 % lower compared to a simple detection algorithm.

In Figure 12, the power consumption of the NFC-System is shown when physical relation factor $x > x_{max}$. This leads to cutting off the power supply of the tag. This cut-off prevents the energy waste invoked by the power loss in the reader circuit and the loose coupled power transfer to the tag. The power consumption is about 50 % lower relative to the simple detection algorithm when the execution time of the PTF-Determinator itself is not considered. To consider is that the operator has to put the tag closer to the reader to reenable the communication which also consumes energy.

The measurement results also show that the influence of the physical relation factor on the consumed energy, invoked by the influence of the reader and tag coil, has to be considered. If the tag is brought closer to the reader, the coupling rises and the needed energy declines. Results show an average decrease of about 13% of the needed energy by closer distances. The execution of the PTF-Determinator results in a time-overhead. Measurements show that the algorithm takes about four times longer than a simple detection.

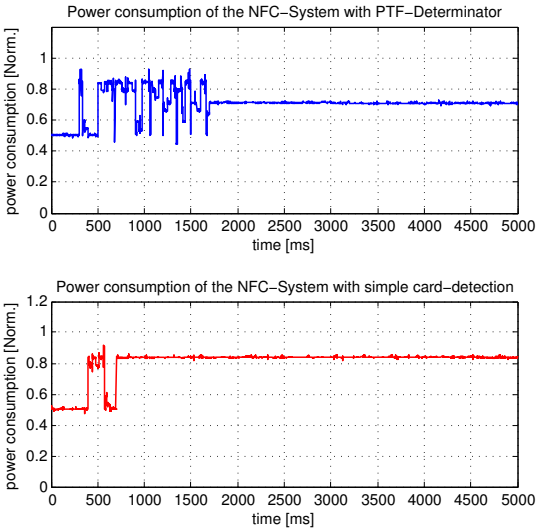


FIGURE 11 - RESULT OF THE POWER CONSUMPTION MEASUREMENT WITH THE CONDITION PHYSICAL RELATIVE FACTOR $x < x_{max}$

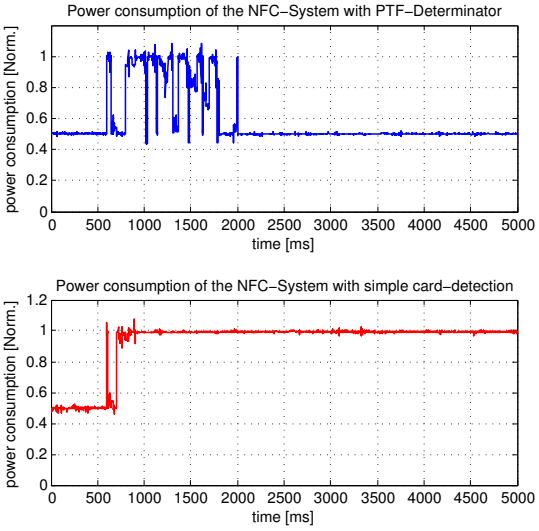


FIGURE 12 - RESULT OF THE MEASUREMENT OF THE POWER CONSUMPTION WITH THE CONDITION PHYSICAL RELATIVE FACTOR $x > x_{max}$

In Table 4, a comparison between the simple detection and usage of the PTF-Determinator is made. It includes the the needed energy of the whole procedure. The needed energies are compared and the saved energy can be evaluated when using the PTF-Determinator instead of the simple card detection. The approximation of the physical relationship is limited on the real hardware. The limitation regards the number of possible steps to scale the magnetic field strength which have been expanded in the simulation which is not possible on real hardware. But it can be shown that the needed energy is 12 % lower when considering the execution of the PTF-Determinator in case of

Physical condition	Energy with PTF [Norm.]	Energy no PTF [Norm.]	Energy saved [%]
$x <= x_{max}$	0.763	0.870	12.29
$x > x_{max}$	0.634	1.000	36.68

TABLE 4 - COMPARISON OF THE SAVED ENERGY IN PERCENT BETWEEN THE METHOD WITH AND WITHOUT PTF EVALUATION IN THE MEASUREMENT

$x <= x_{max}$. An effect can also be seen that a decrease of the physical relation factor leads also to a decrease of the needed energy with a simple card detection. This effect can be explained through the better coupling between reader and tag which has the effect of a more efficient power transmission between them (less losses in the power transmission path). This effect can also be explained through the effect of untuning of the reader coil through inserting the tags coil into the field.

VI. CONCLUSION

This work has shown that the integration of the run-time method to determine the Power Transfer Function (PTF) on reader side is feasible. The energy saving potential by the presented PTF-Determinator, using the PTF to scale down the magnetic field strength, is shown by simulation and verified through measurement. 12% of the energy can be saved in average compared to a simple card-detection method. The implemented feature to set a maximum physical relation factor, by cutting off the power supply to avoid energy consuming transactions, has proven to reduce the energy wastage by up to 40%.

The simulation of the model has given a good estimation of the power consumption to expect on the real target system. Simulation is a good way to test and optimize such a method as the PTF-Determinator before measurement. It also gives the opportunity to reconfigure the hardware (design hardware and software together) to fit the run-time method to optimize the power-consumption even more.

The hardware-in-the-loop measurement has proven to be a good choice to verify the simulated results. By integrating a complete measurable NFC-System, the results can be compared to the simulation and misleadings can easier be detected.

In future work this method shall be improved, focusing on optimizing the approximation of the physical relation factor. Furthermore, this method will be integrated into the communication flow to send periodical updates to react on the dynamic relation between reader and tag while in range (e.g. operator holds the tag in his hand and gets closer to the reader).

ACKNOWLEDGMENTS

We would like to thank our industrial partners Infineon Technologies Austria GmbH as well as Enso Detego GmbH for their support. Furthermore, 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 FFG 829586.

REFERENCES

[1] Xunteng Xu, Lin Gu, Jianping Wang, Guoliang Xing, and Shing-Chi Cheung. Read more with less: An adaptive approach to energy-efficient rfid systems. *Selected Areas in Communications, IEEE Journal on*, 29(8):1684 –1697, september 2011.

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

[3] Wolfgang Rankl and Wolfgang Effing. *Smart Card Handbook: Physical and Electrical Properties*. John Wiley & Sons, Inc., 3 edition, 2003.

[4] Da Cheng, Zhong Wang, and Quan Zhou. Analysis of distance of rfid systems working under 13.56mhz. In *Wireless Communications, Networking and Mobile Computing, 2008. WiCOM '08. 4th International Conference on*, pages 1 –3, oct. 2008.

[5] Jolyon Clulow, Gerhard P. Hancke, Markus G. Kuhn, and Tyler Moore. So near and yet so far: Distance-bounding attacks in wireless networks. In *In Security and Privacy in Ad-hoc and Sensor Networks*, pages 83–97. Springer, 2006.

[6] Xunteng Xu, Lin Gu, Jianping Wang, and Guoliang Xing. Negotiate power and performance in the reality of rfid systems. In *Pervasive Computing and Communications (PerCom), 2010 IEEE International Conference on*, pages 88 –97, 29 2010-april 2 2010.

[7] Wireless Power Consortium. Power receiver design requirements. In *System Description Wireless Power Transfer*, page 32, 2011.

[8] M. Wendt, M. Grumer, C. Steger, R. Weiss, U. Neffe, and A. Muehlberger. System level power profile analysis and optimization for smart cards and mobile devices. In *Proceedings of the 2008 ACM symposium on Applied computing*, SAC '08, pages 1884–1888, New York, NY, USA, 2008. ACM.

[9] A. Genser, C. Bachmann, C. Steger, R. Weiss, and J. Haid. Estimation-based run-time power profile flattening for rf-powered smart card systems. In *Circuits and Systems (APCCAS), 2010 IEEE Asia Pacific Conference on*, pages 1187 –1190, dec. 2010.

[10] Tobias Lohmann, Matthias Schneider, and Christoph Ruland. Analysis of power constraints for cryptographic algorithms in mid-cost rfid tags. In Josep Domingo-Ferrer, Joachim Posegga, and Daniel Schreckling, editors, *Smart Card Research and Advanced Applications*, volume 3928 of *Lecture Notes in Computer Science*, pages 278–288. Springer Berlin / Heidelberg, 2006. 10.1007/1173344720.

[11] Julien Mercier, Christian Dufaza, and Mathieu Lisart. Signoff power methodology for contactless smartcards. In *Proceedings of the 2007 international symposium on Low power electronics and design*, ISLPED '07, pages 407–410, New York, NY, USA, 2007. ACM.

[12] Erik Rolf and Viktor Nilsson. Near Field Communication (NFC) for Mobile Phones. In *Near Field Communication (NFC) for Mobile Phones*, page 25, 2006.

[13] Jianhua Liu and Weiqin Tong. Dynamic share energy provisioning service for one-hop multiple rfid tags identification system. In *Cloud Computing and Intelligence Systems (CCIS), 2011 IEEE International Conference on*, pages 342 –347, sept. 2011.

[14] Josef Haid, Walter Kargl, Thomas Leutgeb, and Dietmar Scheiblhofer. Power management for rf-powered vs. battery-powered devices, 2005.

[15] Arjun Roy, Stephen M. Rumble, Ryan Stutsman, Philip Levis, David Mazières, and Nickolai Zeldovich. Energy management in mobile devices with the cinder operating system. In *Proceedings of the sixth conference on Computer systems*, EuroSys '11, pages 139–152, New York, NY, USA, 2011. ACM.

NFC-DynFS: A way to realize dynamic field strength scaling during communication

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

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

***Abstract*—Near Field Communication (NFC) shows potential in multiple areas like payment, identification, transport, etc. To enable these features to a larger group of users, NFC-capability is nowadays integrated in mobile devices like smart phones. This integration unfortunately leads to an increase of the device's battery drain because the transponder is powered by the provided magnetic field of the mobile device. To decrease this drain, power-management techniques like magnetic field strength scaling are used. Through this scaling the power transfer can be reduced to the transponder's required level.**

The challenge of this technique is to dynamically adapt the magnetic field strength to physical relation changes of the transponder even during communication. Without this adaption, scaling down the field can lead to the transponder's undersupply or energy is wasted through oversupply. This paper proposes a method, named NFC-DynFS, to realize this adaption and to proper scale the magnetic field strength.

In a case study a system, to read digital business cards using NFC-DynFS, is simulated and implemented on real hardware. The power consumption results are evaluated and compared to implementations without NFC-DynFS. Furthermore, possible undersupplies of the transponder are investigated. It can be shown that, compared to implementations without field strength scaling, approximately 26% of the energy can be saved and an undersupply of the transponder can be avoided, until the reader's power transmission limit is reached.

I. Introduction

Near Field Communication (NFC) is a form of communication, which allows to transmit data at short distance without complicate pairing mechanisms. The transmission partners consisting of reader and transponder are brought close together to establish the connection. NFC can be used in several areas like payment or identification. To make these areas available to a large group of users, NFC is integrated into mobile devices like smart phones. Examples would be reading smart posters or digital business cards.

Unfortunately this integration also leads to an increasing battery drain of the mobile device. This drain is a result of the integrated Reader-IC to enable NFC. This Reader-IC generates a magnetic field to communicate and to transfer power to the transponder. The strength of this field is often set to a maximum allowed value to provide an expected transmission range regardless of the transponder-type. New methods have been proposed to scale this magnetic field relative to the physical relation factor to reduce the energy wastage [1]. The term of physical relation factor is used in this publication to describe the indirect relation of the coupling between reader and transponder. The more the relation factor rises the lesser the coupling gets. If the relation factor is constant, a lower field strength leads to a lower power consumption. Currently, these methods of field strength scaling [1] [2] don't consider the dynamic behavior of this relation factor during communication. This dynamic behavior occurs because the transponder is typically held by the user towards the reader, which leads to changes in position and distance over time. Furthermore, the power-consumption of the transponder changes depending on the operation and the state (e.g., en- decryption of data).

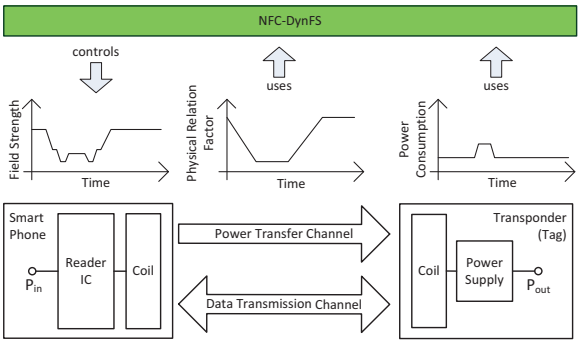


Fig. 1. Concept of the NFC-DynFS showing what parameters over time are used and what variable is controlled to reduce the power consumption of the system without risking an undersupply of the transponder.

In this paper the following contributions are made:

- A novel method called NFC-DynFS is proposed which enables the control of the magnetic field strength using the physical relation and transponder's power consumption over time as parameters (see Figure 1), to save energy during communication.
- The proposed method is also designed to avoid an undersupply of the transponder, which may happen through an increase of the physical relation factor (transponder is pulled away from the reader) or transponder's power consumption, until the limit of the possible power transmission capability of the reader is reached.

This paper is divided into four sections. In the first section the method and basic principles of NFC-DynFS are described. The second section gives an overview of the related work. In

Section three the results of the case study are shown, which are divided into the simulation part and the measurement on real hardware. The fourth section presents the conclusion of this work.

II. Method

This section describes how the issue of dynamic field strength scaling during communication is solved and the method called NFC-DynFS is designed. The description consists of three paragraphs. The first paragraph deals with the question how to scale the magnetic field strength according to changes of the physical relation factor during communication. The second paragraph focuses on the fact that during an operation (e.g., read) of the transponder, its power consumption rises and may lead to an undersupply. The design of the solution is described in the third paragraph.

A. Scaling according to changes of the physical relation factor

First of all the term physical relation factor has to be defined. The relation factor describes the indirect coupling relation between reader and transponder. This relation factor depends on the physical configuration between reader and the transponder but also on other parameters. An overview of the considered transmission path and circuits are shown in Figure 2. The physical configuration can be simplified to the parameter of distance between the reader and the transponder, when they are in a coaxial orientation to each other. One of those other parameters are the coil's properties which influence the coupling. In a controlled environment (simulation or measurement in a laboratory) this physical relation factor can be calculated, but if a system in a real environment is considered only parts like the coils properties are known and some parts like the physical configuration are hard to measure during communication.

A measurement of this physical relation factor is not necessarily needed. The approach of this paper is to find the needed minimal magnetic field strength on reader side without risking an undersupply of the transponder when the physical relation factor changes. This threshold marks a certain relation factor which can be reached with the provided field strength of the reader. The physical relation factor is still unknown but an equivalent field strength value has been found, which is enough for scaling according to changes of the physical relation factor.

This behavior can be explained by taking a closer look at the equation to calculate the inductive coupling between the reader and the transponder, which represents a part of the physical relation factor.

$$H = \frac{i_r \cdot N_r \cdot a_r \cdot b_r}{4 \cdot \pi \cdot \sqrt{(\frac{a_r}{2})^2 + (\frac{b_r}{2})^2 + d^2}} \cdot \left(\frac{1}{(\frac{a_r}{2})^2 + d^2} + \frac{1}{(\frac{b_r}{2})^2 + d^2}\right) \tag{1}$$

The Equation 1 shows the dependency of the magnetic field strength on transponder side to the supplied current of the reader, based on the law of Biot-Savart for rectangular shaped coils. The parameters N_r, a_r, b_r describe the physical properties of the reader coil consisting of the number of windings and the size of the coil. d represents the distance between the reader and the transponder coil under the assumption of a coaxial orientation.

$$M_{12} = \frac{\mu_0 \cdot H \cdot N_t \cdot a_t \cdot b_t}{i_r} \tag{2}$$

Equation 2 is needed for the calculation of the mutual inductance M_{12} according to the magnetic field strength on transponder side. N_t, a_t, and b_t represent the transponders parameters. The transformation of the provided input current to the output voltage is described in Equation 3 [3].

$$u_2 = \frac{w \cdot M_{12} \cdot i_r}{\sqrt{(\frac{(w \cdot L_t)}{R_l} + w \cdot R_t \cdot C_2)^2 + (1 - w^2 \cdot L_t \cdot C_2 + \frac{R_t}{R_l})^2}} \tag{3}$$

Under the assumption of a transponder's constant load and distance to the reader the Equations 1 to 3 show, that a certain input current i_r relates directly to the supply voltage on transponder-side. If the supply voltage drops under the needed threshold, the point of an undersupply is reached. This minimal i_r leads to the described minimum field strength on reader side.

Another aspect has not been considered in the equations above. The impedance on reader side is not constant, it alters because of the transponders dynamic load. Thus, only if the load remains constant the considerations are valid. This is achieved by measuring i_r when no or a defined operation is executed.

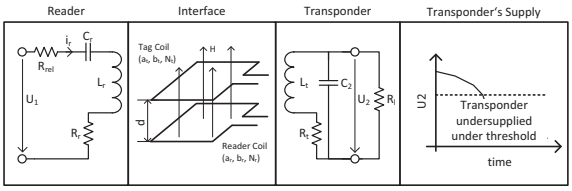


Fig. 2. Overview of the transmission path to describe the physical relation factor and the power transfer from the reader to the transponder and the possible undersupply (adapted from [3]).

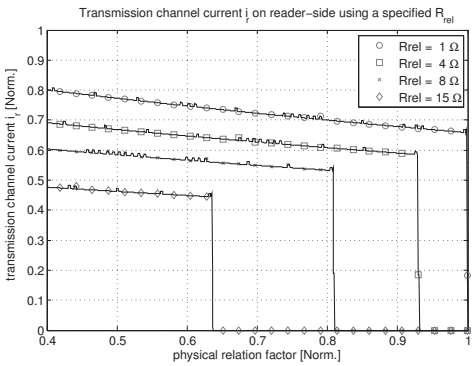


Fig. 3. Simulation of the provided field strength of the reader, represented by the transmission current i_r, simulated with different values of the digital controllable resistance R_{rel}, in relation to the physical relation factor.

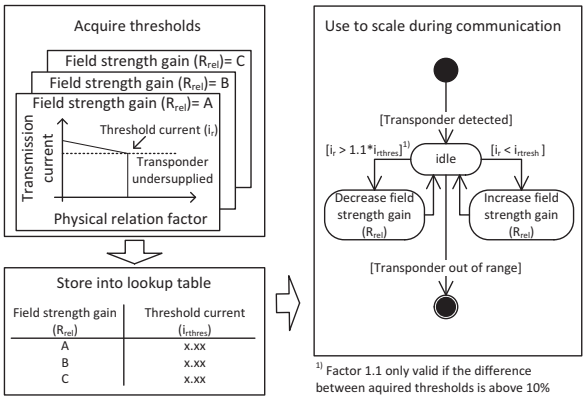


Fig. 4. Flow of the acquisition from the needed data to its usage to scale the magnetic field strength according to changes of the physical relation factor.

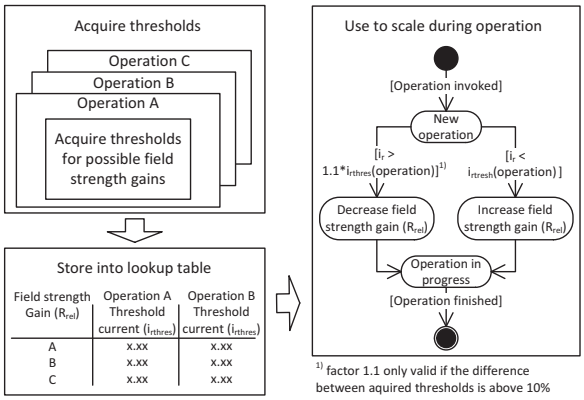


Fig. 5. Flow of the acquisition of the needed data to it's usage to scale the magnetic field strength according to called operations (e.g. read).

As next step the approach has to be made usable in practice. Readers commonly do not allow a infinite scaling of the field strength. They use a digital controllable resistance on the transmission channel for scaling (see Figure 2). The threshold, represented by i_r, is now evaluated for the possible field strength steps by increasing the physical relation factor until the transponder's undersupply. A simulation of this procedure is shown in Figure 3. The used procedure sets R_{rel} to a certain value and increases the physical relation until the transponder is not responding anymore. This point is indicated through setting the field strength to zero. The magnetic field strength is represented by transmission current i_r of the reader which is direct proportional to the field strength and can be directly measured.

With this threshold-values the supplied power value of the reader can be scaled. The scaling procedure is nothing more but increasing the magnetic field strength, when the supplied power falls under the threshold, and decreasing the power when the field strength rises above the difference between the lesser threshold and the current one (see Figure 4).

B. Transponder's power consumption changes

This paragraph deals with the question how to scale the magnetic field strength according to a change in the power consumption of the transponder through an invoked operation. Unfortunately this change has no practically measurable influence on the power consumption on reader side. Therefore, another approach has been found to relay the information, of an invoked operation and an upcoming change in the power consumption, to the reader.

To simplify this issue whole operations like reading, writing, or authenticating are considered. The operation calls are triggered by the reader and so the scaling process can be made in advance to avoid the expected undersupply (scale before execution).

The challenge is to know the proper scale to avoid an undersupply of the transponder. This approach uses the same flow, as used to scale according the physical relation factor, to avoid an undersupply. The investigated operation is executed periodically by increasing the physical relation factor until the transponder is undersupplied (does not respond anymore). This procedure has to be done slowly enough because the transponder implements countermeasures to compensate undersupplies for a short time which would influence the result.

The behavior of the change in the needed minimal magnetic field strength can be explained through Equation 3, which shows the influence of the load (simplified in one variable R_l) to the transponder's supply voltage. If the voltage drops under a certain threshold the transponder is undersupplied.

The resulting operation-thresholds can be used as lookup table before executing an operation. The scaling procedure is the same as in the case of the physical relation factor except the inclusion of the parameter of the operation. The magnetic field strength is increased, when the supplied power is under the operation-threshold, and is decreased when the power rises above the difference between the lesser operation-threshold and the current one, as shown in Figure 5.

C. Distribution of the needed components for NFC-DynFS

The described parts have to be integrated into the NFC-System as shown in Figure 6. The integration is designed in a way to avoid changes in the functional implementation of the system. The components of the design are the

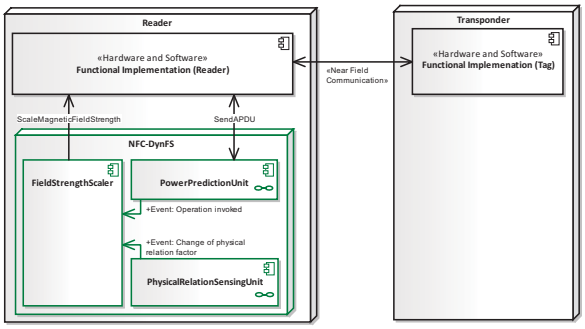


Fig. 6. Component model of the NFC-DynFS describing where the components are distributed and how they are connected.

FieldStrengthScaler, the PowerPredictionUnit and the PhysicalRelationSensingUnit. The FieldStrengthScaler is the core unit which receives events from the other two components. The first event is called by the PowerPredictionUnit, when an operation (reading, writing,authentication of the transponder) is invoked. Therefore, all operations to send to the transponder are relayed through the PowerPredictionUnit to invoke the operation-event. The second event is called by the component PhysicalRelationSensingUnit, when a change of the magnetic field strength occurs. This component periodically measures the transmission current i_r representing the magnetic field strength. The main component FieldStrengthScaler uses this events and the threshold values to properly scale the magnetic field strength. The acquisition of these threshold values are described in the two sections above (see Figure 4 and 5).

III. Related Work

In this Section a three part overview of the related work is given. The first part relates to publications regarding the wireless power transfer from the reader to the transponder and the way to evaluate and control it. The second part shows possible ways to predict the transponder's power consumption, which is needed as a control parameter for the power transfer. The third part describes general power management strategies for reader/transponder systems.

A. Wireless power transfer and control

One aspect to create a power-aware reader/transponder system is to determine the Power Transfer Function (PTF). Through this PTF the provided power for the transponder can be calculated using the needed power. To determine this PTF two steps have to be made. The first step is getting the coil's properties responsible for the transformation from the electric current into a magnetic field. This coil includes a matching network to provide an effective transformation. Michael Roland et al. describe an automatic matching algorithm for coils [4]. This algorithm measures and calculates the properties needed to perform the first step. The second step deals with the wireless transfer which uses the physical principle of inductive coupling. Cheng Da et al. show the relation between the maximum reading distance to the transponder and the reader's sending power [5]. Rolf et al. mathematically describe the transfer function which is needed for the PTF. The function shows that the magnetic field strength is decaying in distance by the power of three. This function also can be brought into relation with the maximum possible reading distance because the provided power of the reader falls below the transponder's needed power [6]. Esko Strömmer et al. also examined the power transmission from reader to transponder and concluded that the maximum provided power is as high as about 100mW [7]. This provided power is not always needed by the transponder and can be controlled by altering the magnetic field strength, which is shown by Xunteng Xu et al. [1].

B. Prediction of the transponder's consumed power

A needed control parameter for the power transfer is the power prediction of the transponder. Clemens Moser et al. show a power management algorithm through prediction of the future consumption over a certain time interval [8]. This algorithm is a possible solution to get the current and future power consumption without the need of measurement during communication. To perform this prediction a characterization is needed described by Bachmann et al. [9]. To get a power profile of a component like a cryptographic core an estimation can be made through estimation of the logic-gates which is described by Lohmann et al [10]. These characterization-methods can be used during design phase and can be used to to acquire the needed data needed for NFC-DynFS.

C. Power management strategies for reader/ transponder systems

System based power management strategies have more potential to save energy because the whole system is considered instead of only one component. The problem is how to consider all components in the algorithm and where to draw the line in complexity. F. Menichelli et al. describe a system level view exploration technique to create power-aware systems. They use a template for the top-view of the system and analyze the specific design and implementation in terms of their power-awareness [11]. Through this approach a power-aware configuration can be found and used for the system. Another publication written by Chatterjee et al. shows that putting the system into a more abstract level by defining selected states eases the design of a power management unit and leads to a more energy efficient behavior [12].

IV. Experimental Results

A. Case study: Power-aware design and implementation of a system reading digital business cards

To evaluate NFC-DynFS in terms of the overall power consumption and the avoidance of a transponder's undersupply, a

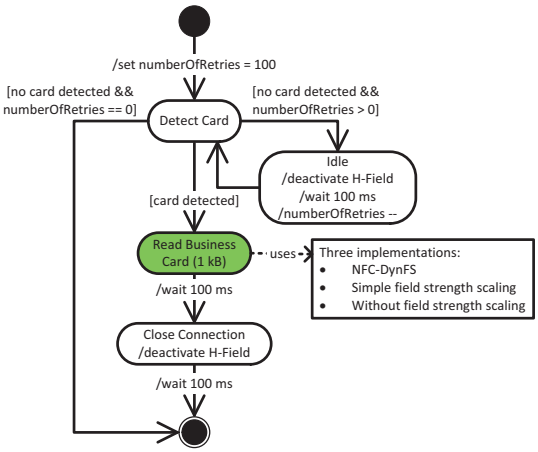


Fig. 7. Flow diagram of the use case. The state "Reading Business Card" uses three implementations to evaluate the efficiency of NFC-DynFS.

use case to read digital business cards is selected. This use case consists of a simple card detection mechanism and a reading procedure (see Figure 7). The reading procedure uses three different implementations for comparison. The first implementation includes NFC-DynFS. The second implementation uses a simple field strength scaling algorithm (scales only once at the detection of the card). The third implementation does not use field strength scaling. These three implementations are simulated, executed, and measured on real hardware.

B. Simulation

The first evaluation was made by simulating the system. The simulation environment is a SystemC-Model consisting of reader and transponder. This model is capable of calculating the power consumption of the reader regarding to the physical relation factor, the field strength, and the executed operation (e.g., read). The SystemC-Model is connected to a operating system emulation platform for Android. The result of the simulation is shown in Figure 8.

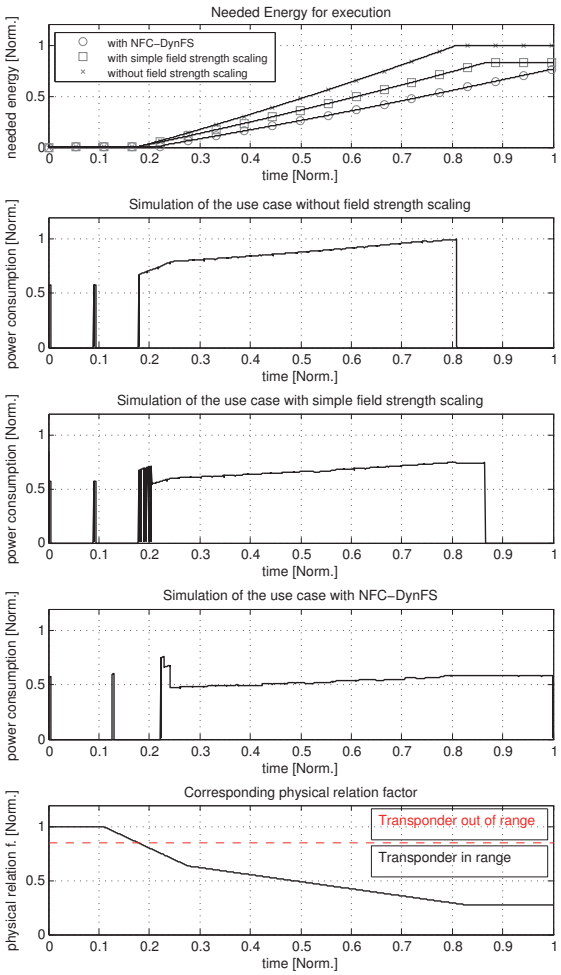


Fig. 8. Simulation result of the use case divided into the three implementations. The plot at the bottom shows the physical relation factor, which behaves like slowly pushing the transponder towards the reader.

Implementation	Needed Energy [Norm.]	Notes
without field strength scaling	1.00	oversupplied
with simple field strength scaling	0.82	oversupplied
with NFC-DynFS	0.77	-

TABLE I
COMPARISON REGARDING THE NEEDED ENERGY OF THE THREE IMPLEMENTATIONS IN SIMULATION.

First of all, the functionality of NFC-DynFS is evaluated. This can be shown in the first plot of Figure 8. The field is scaled down when the physical relation factor decreases. Without scaling, the power consumption would rise, which leads to an oversupply of the transponder and to a waste of energy.

The second aspect is the power consumption compared to the implementations. The implementation with the simple field strength scaling consumes more power than needed by the transponder. This behavior occurs through initial scale where the physical relation factor is high. The first implementation using NFC-DynFS provokes the lowest power consumption. The last implementation without any field strength scaling consumes the most power.

The third aspect deals with the needed energy (shown in Table I). NFC-DynFS increases the execution time but needs 23% less energy than an implementation without any field strength scaling.

C. Measurement on real hardware

To prove that NFC-DynFS works on real hardware, the three implementations are deployed on an existing NFC-System using the Android operating system. The system is placed into a hardware in the loop measurement suite [2]. The physical relation factor is approximated through the lack of an automatic change. The result is shown in Figure 9.

The first evaluation goal is to prove that NFC-DynFS works on real hardware. NFC-DynFS is able to scale the field strength properly to save energy. The simple field strength scaling algorithm oversupplies the transponder, because it scales at a time where the physical relation factor is high.

The second aspect regards the power consumption. NFC-DynFS needs less power than the implementation without field strength scaling. The simple field strength scaling is not able to properly scale the field strength and needs more energy than without field strength scaling.

The third aspect deals with the needed energy on real hardware (see Table II), which also corresponds to the sim-

Implementation	Needed Energy [Norm.]	Notes
without field strength scaling	0.98	oversupplied
with simple field strength scaling	1.00	oversupplied
with NFC-DynFS	0.73	-

TABLE II
COMPARISON REGARDING THE NEEDED ENERGY OF THE THREE IMPLEMENTATIONS ON REAL HARDWARE.

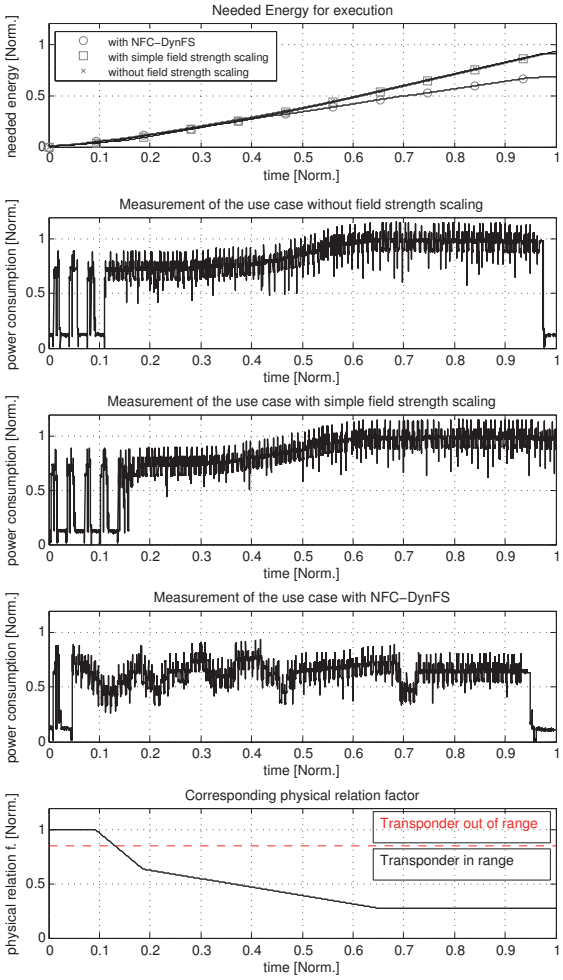


Fig. 9. Measurement result of the use case divided into the three implementations. The plot at the bottom shows the physical relation factor, which behaves like slowly pushing the transponder towards the reader.

ulated results. The saved energy is as high as 26%. Real hardware is more complex than in simulation leading to a slight divergence, which can be seen in the needed enegery for the simple field strength scaling.

V. Conclusion

The results show that dynamic field strength scaling during communication has a more efficient behavior in practice than the other implementations. A single field strength scale at the transponder's detection can lead to an undersupply or to a wastage of energy when the field strength is scaled too high. The NFC-DynFS is able to avoid this undersupply by scaling the field strength, using events invoked by changes in the physical relation factor and called operations. NFC-DynFS is also able to avoid oversupplies of the transponder by scaling down. These changes used for the events occur through the dynamic behavior during communication. In general the transponder is held against the reader by a person. This person pushes the transponder against the reader and therefore the physical relation factor is not static at all.

Methods have been shown in Figure 4 and 5 to acquire the data needed for NFC-DynFS to work, which are practically usable in real systems. These methods can be applied by either initially acquiring the information using an algorithm in the live system or through acquisition and storage of the needed information during the production process.

In the presented case study, NFC-DynFS has proven to be a good way to save energy. An algorithm without field strength scaling, transfers too much power to the transponder when the transponder is close to the reader. On a real NFC-System an energy reduction of 26% has been verified by measurement.

Acknowledgment

We would like to thank our industrial partners Infineon Technologies Austria AG as well as Enso Detego GmbH for their support. Furthermore, 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 FFG 829586.

References

[1] X. Xu, L. Gu, J. Wang, G. Xing, and S.-C. Cheung, "Read more with less: An adaptive approach to energy-efficient rfid systems," *Selected Areas in Communications, IEEE Journal on*, vol. 29, no. 8, pp. 1684 –1697, september 2011.

[2] M. Menghin, N. Druml, C. Steger, R. Weiss, J. Haid, and H. Bock, "The ptf-determinator: A run-time method used to save energy in nfc-systems," in *Eurasip Workshop RFID 2012*, 2012.

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

[4] M. Roland, H. Witschnig, E. Merlin, and C. Saminger, "Automatic impedance matching for 13.56 mhz nfc antennas," in *Communication Systems, Networks and Digital Signal Processing, 2008. CNSDSP 2008. 6th International Symposium on*, july 2008, pp. 288 –291.

[5] D. Cheng, Z. Wang, and Q. Zhou, "Analysis of distance of rfid systems working under 13.56mhz," in *Wireless Communications, Networking and Mobile Computing, 2008. WiCOM '08. 4th International Conference on*, oct. 2008, pp. 1 –3.

[6] E. Rolf and V. Nilsson, "Near Field Communication (NFC) for Mobile Phones," in *Near Field Communication (NFC) for Mobile Phones*, 2006, p. 25.

[7] E. Strommer, M. Jurvansuu, T. Tuikka, A. Ylisaukko-oja, H. Rapakko, and J. Vesterinen, "Nfc-enabled wireless charging," in *Near Field Communication (NFC), 2012 4th International Workshop on*, march 2012, pp. 36 –41.

[8] C. Moser, L. Thiele, D. Brunelli, and L. Benini, "Adaptive power management for environmentally powered systems," *Computers, IEEE Transactions on*, vol. 59, no. 4, pp. 478 –491, april 2010.

[9] C. Bachmann, A. Genser, C. Steger, R. Weiss, and J. Haid, "Automated power characterization for run-time power emulation of soc designs," in *Digital System Design: Architectures, Methods and Tools (DSD), 2010 13th Euromicro Conference on*, sept. 2010, pp. 587 –594.

[10] T. Lohmann, M. Schneider, and C. Ruland, "Analysis of power constraints for cryptographic algorithms in mid-cost rfid tags," in *Smart Card Research and Advanced Applications*, ser. Lecture Notes in Computer Science, J. Domingo-Ferrer, J. Posegga, and D. Schreckling, Eds. Springer Berlin / Heidelberg, 2006, vol. 3928, pp. 278–288, 10.1007/1173344720.

[11] O. Unsal and I. Koren, "System-level power-aware design techniques in real-time systems," *Proceedings of the IEEE*, vol. 91, no. 7, pp. 1055 –1069, july 2003.

[12] S. Chatterjee, S. Roy, and S. Bandyopadhyay, "Hop-efficient and power-optimized routing strategy in a decentralized mesh network using directional antenna," in *Parallel and Distributed Computing, 2006. ISPDC '06. The Fifth International Symposium on*, july 2006, pp. 155 –160.

Energy Efficiency by Using Field Strength Scaling for Multi-Transponder Applications

Manuel Menghin*, Norbert Druml*, Bernhard Kipperer*, Christian Steger*, Reinhold Weiss*,
Holger Bock† and Josef Haid†
*Institute for Technical Informatics,
Graz University of Technology, Graz, Austria
Email: {manuel.menghin, norbert.druml, steger, rweiss}@tugraz.at, kippy@sbox.tugraz.at
†Design Center Graz,
Infineon Technologies Austria AG, Graz, Austria
Email: {holger.bock, josef.haid}@infineon.com

***Abstract*—The rising demand for Near Field Communication (NFC), which uses the RFID technology, drives the market to deliver up to 500 million devices in 2014. The applications for RFID spread from simple identification to wireless gateways for embedded systems. The integration of this RFID-Reader in smart phones are an example for mobile RFID-Systems. Unfortunately, this integration leads to a decreased smart phones battery life, through the increased power consumption.**

To decrease this consumption, power management techniques like magnetic field strength scaling have been proposed. This technique adapts the amount of transferred power to the requirements of the transponder. This technique does not consider multiple transponders in transmission range. Therefore, this paper proposes an adapted version of the reader's transponder-detection process using magnetic field strength scaling to reduce the reader's battery drain. The adapted version has been implemented by two novel methods.

These two methods have been experimentally verified by a case study. The potential of needing less battery drain is evaluated and compared to different possible implementations. In this case study, the battery drain needed by the RFID-Reader can be reduced by up to 34% using magnetic field strength scaling for multiple transponders.

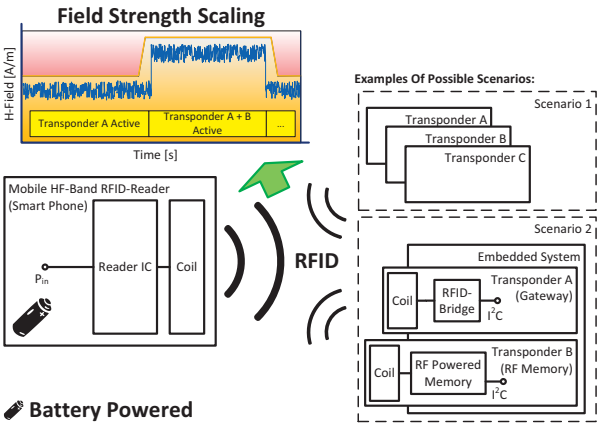


Fig. 1. This illustration shows the idea of using magnetic field strength scaling for multiple transponders in two possible scenarios, to reduce the battery drain of the mobile RFID-Reader.

I. Introduction

HF-Band Radio Frequency Identification (RFID) is a wireless form of communication using inductive coupling to transfer data and also power to a receiver (transponder). Mainly used for identification purposes, RFID also shows potential to supply whole embedded systems with power using an RFID-Reader (transmitter). This enables applications like RF harvesting memory-chips, which can be read and written via RFID without needing a wired power supply. These memories can be directly integrated into the circuit of an embedded system. Additionally, they also provide a contact based interface like Inter-Integrated Circuit (I^2C), for a wired exchange of data with the embedded system [1]. Also applications like RF powered gateways, used for the exchange of data between the RFID-Reader and the embedded system directly by bridging the communication to common interfaces like I^2C or Serial Peripheral Interface (SPI), are possible. Another application is using the RF-Channel as pure energy source without transferring any data at all. The advantage of all these applications can also be described as adding a common wireless interface (e.g., Near Field Communication) to any imaginable device (embedded system) to transfer data and power over one channel.

To increase the flexibility of those systems, RFID-Readers can be used in mobile devices like smart phones. However, the battery drain on these mobile devices rises through the additional power consumption. To reduce this drain, power management techniques are integrated in the devices. Most of these techniques are component based like making the Reader-IC more energy efficient. To consider is that the power consumption of the mobile RFID-Reader depends not only on the efficiency of single components, it depends on the efficiency of the whole system including the transponders. Proposed solutions like magnetic field strength scaling can be used for system based power management techniques [2]. In this technique, the magnetic field strength is scaled on the reader's side to adapt the power transfer to the transponders requirements. The scaling is based on the power transmission depending on the current physical relation factor, which also

12th International Conference on Telecommunications - ConTEL 2013
ISBN: 978-953-184-180-1, June 26-28, 2013, Zagreb, Croatia

involves the distance, between transponder and the RFID-Reader. If this factor decreases, more power is transfered to the transponder but the requirements of the transponder remain the same. This leads to an oversupply and to a unnecessary battery drain of the RFID-Reader. Scaling the magnetic field strength avoids that oversupply.

The increasing amount of applications lead to an environment with multiple transponders in transmission range of the RFID-Reader. Present scenarios are payment systems using an additional transponder in form of a sticker for security reasons or a briefcase with multiple wireless identification and payment cards in it (Scenario 1 as shown in Figure 1). Another scenario is a RFID-Gateway used for communication, and a RF-powered memory for identification and tracking integrated into one embedded system (Scenario 2 as shown in Figure 1).

Unfortunately, magnetic field strength scaling is not designed for multiple transponders in range. On the other hand, the transponder-detection process on reader-side is designed to communicate to a certain transponder but does not consider the power transfer, which is required to expand power management techniques like magnetic field strength scaling for multiple transponders. To combine those two, following contributions are made in this paper:

- Two methods of dynamic field strength scaling for practical use in a multi transponder environment labeled as FSS and BIN have been developed (as shown in Fig. 1). Their goal is to reduce the battery drain of the mobile HF-Band RFID-Reader.
- The impact to the power consumption of the two methods have been evaluated by measurement in a case study of reading up to ten transponders in transmission range.

The rest of this paper is divided into four sections. In Section II the related work is described. Section III shows the method used to realize the contributed methodology. The case study and the experimental results are shown in Section IV. The conclusion of this publication is presented in Section V.

II. Related Work

This section is divided into four topics. The first topic shows works regarding the wireless power transfer. The second topic deals with the possibilities and considerations controlling this wireless power transfer. The third topic summarizes system based power management techniques and their application in embedded systems. In the fourth topic, approaches for energy efficient anti-collision procedures are described.

A. Power transfer using the RF-Interface in RFID-Systems

Wireless power transfer in HF-Band RFID-Systems is a common approach to power passive transponders by an RFID-Reader. Esko Stroemmer et al. show the potential of wireless power transfer in inductive coupled RFID-Systems [3]. Unfortunately, the available power on transponder side is constrained through the loosely coupled transponder, the regulations and standards for RFID. Narijun et al. describe these power constraints through a reference implementation of the RF-harvesting component of the transponder using UHF [4]. The publication from Jung-Hyun Cho et al. shows the structure of a hybrid transceiver (active or passive) for HF-Band RFID and the available power on transceiver side [5]. It can be shown that it is possible to power even sensors with the available power but they have to be designed power efficient. Another approach to RF harvesting and powering sensors is shown by Andreas Loftier et al. by charging the transponder over RF. After the charging process, the transponder can temporarily operate without any external supply at all [6].

B. Controlling the power transfer using the RF-Interface in multi-transponder environments

Controlling the power transfer from the reader to the transponder is a way to find new system based power management techniques. Two considerations are made for this way. The first consideration deals with the power transfer to the transponder. The work of Meysam Zargham et al. describes the problem of the power transfer in a two-port notation. Through their approach, the effectiveness of the power transfer can be investigated in design phase [7]. In another publication from Cheng Da et al. the relation between the transmission distance and the sending power of the reader is shown [8]. Rolf et al. showed, that the magnetic field strength, provided by the reader, on transponder-side decreases in distance with the power of three [9]. This shows that a appropriate scaling of the field strength for the appropriate distance can decrease the oversupply of the transponder(s). This scaling technique is also used by Xunteng Xu et al. [10] and also shown in [2]. The second consideration has to be made in terms of the misalignment of the transponder. This means that the transponder is not perfectly aligned to the reader. Kyriaki Fotopoulou et al. present a complete misalignment model for circular shaped and inductive coupled coils. Their publication gives an overview of the parameters needed to model the power transfer to a single transponder including misalignment [11].

The power transfer changes, when two or more transponders are in transmission range of the reader. Witschnig et al. investigated the power transfer behavior from one reader to two transponders. Their mathematical approach is suitable for modeling the power transfer to multi-transponder environments [12]. A technique using the power transfer function to reduce the power consumption in the transponder-detection procedure is shown by Pierre-Henri Thevenon et al. [13]. The existing publications show that a lot of investigations are made to transfer as much power as possible to the transponders, but without considering the consumption on the reader side. In security applications, the power consumption of the transponder remains the same regardless of the current operation and can be expressed as a constant current source and a shunt resistance as described by [14]. This means the power consumption depends on the physical relation between transponder and RFID-Reader, and the magnetic field strength of the RFID-Reader.

C. System based power management techniques for embedded systems

To reduce the power consumption in HF-Band RFID-Systems, the whole system should be considered. One way of accomplishment is described by F. Menichelli et al. by using a system level exploration technique. They apply this technique on the systems architecture to create a power-aware system [15]. Chatterjee et al. also shows that bringing the system into a more abstract form can be used to optimize the power consumption [16]. To implement these system based power management techniques, observer-controller architectures can be used as described by Luca Benini et al. [17].

D. Increasing the energy efficiency of transponder-detection procedures in RFID-Systems

A main part of communication establishment with multiple transponders is the anti-collision process. There are several publications which try to increase the efficiency of this process in terms of power and time. Several approaches evaluate the protocol level to make anti-collision protocols more efficient like integrating location-awareness described by Su Haoru et al. [18] or divide-and-conquer technique by Jeong Geun Kim [19]. Furthermore, analytic approaches using performance analysis methods on state-diagrams are presented by Mohammed Berhea et al. [20]. Feng Zhou et al. evaluate the power consumption needed for the different implementations of the anti-collision protocols for UHF-Band RFID Systems. They show evaluation approaches for the protocol level down to the circuit level [21].

III. Method

The section is divided into four parts. In the first part, the used terms, formulas, and general considerations are described. The second part shows the first proposed method called FSS. In the third part the second method BIN is described. The last part describes how these two methods are integrated into the RFID-System.

A. Definitions and used formulas

The solution to the challenge of magnetic field strength scaling in multi transponder environments is solved analytically. To understand the approach, the used terms and formulas have been described in this section.

- t_U ... This is an abstract time unit, which describes the smallest amount of time used in the analytic approach. The value of this time factor can be matched to the investigated system by measurement (measuring the average time of execution).
- t_{SET} ... Every method discussed in this paper has to set the field strength used during transmission at least once. The two contributed methods however are based on the principle of field strength scaling and therefore may even set the field multiple times during their execution. To cover the resulting delay that influences the energy consumption, t_{SET} is introduced which describes the amount of time required to set the field strength once. By definition one single field strength setting operation takes t_U time.
- t_{FIND} ... In order to communicate with a certain transponder, independently of how many targets are actually in transmission range at that time, the transmission module of the reader has to acquire its full UID (unique identifier). This process can be repeated (n_{TL}) until either all transponders have been inspected or the wanted one was successfully found. If only one transponder is reached with the current field strength, its UID is returned. Whenever collisions occur because more than one target answers, a SDD (Single Device Detection) has to be executed that represents a kind of binary search. It requires several steps to return one full UID.
- t_{READ} ... In order to demonstrate the correct behavior of all algorithms discussed in this document, an amount of 1 kB has to be read from the specified transponder after it was successfully reached. This process takes approximately 80 time units (acquired by measurement) and is independent of the algorithm used. All approaches rely on the exact same commands and the transmission rate is never changed. Only the used field strength and therefore the momentary power consumption of each read cycle is set by the algorithm during a transponder's discovery. The value of t_{READ} therefore is constant and can be written as $t_{READ} = 80 \cdot t_U$.

The main goal of the analytic approach is to minimize the energy consumption. Equation 1 describes how the energy consumption is calculated through the time factors and the average power consumption P_i during this time.

$$E = P_i \cdot (t_{SET} + t_{FIND} + t_{READ}) \tag{1}$$

To solve this equation, the average values for the time factors, and power consumptions of the operations have to be defined according the current magnetic field strength. This has been done by measurement using a reference transaction reading 1 kB of data from one transponder. The results are shown in Table I and Fig. 2. This measurement consists of a power and timing analysis of a ACS ACR122U RFID-Reader.

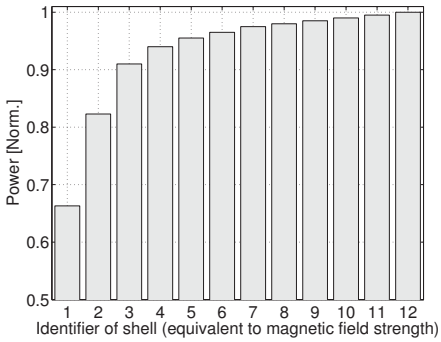


Fig. 2. Average power consumption of the measured HF-RFID-Reader according to the selected shell (magnetic field strength) for one transponder

TABLE I
FACTORS FOR THE ANALYTIC APPROACH RELATING TO THE TIME UNIT t_U BASED ON THE TIMING ANALYSIS OF THE MEASURED RFID-READER

	value
t_{SET}	t_U
t_{FIND}	$t_{FIND} = 1.2 \cdot n_{TL} \cdot t_U$
t_{READ}	$80 \cdot t_U$

B. Analytic evaluation of the standard transponder-detection

As next step the standard transponder-detection procedure, which is labeled CONST, is analytically evaluated (best, average, and worst case behavior as shown in Equation 2 to 10) in terms of their energy consumption. $P_i = P_{MAX}$, because the field strength is always set to maximum.

- Best case ... In this case the wanted transponder is the first one found by the transponder-detection procedure ($n_{TL} = 1$)

$$t_{FIND} = 1.2 \cdot t_U \quad (2)$$

$$t = t_{SET} + t_{FIND} + t_{READ} = 82.2 \cdot t_U \quad (3)$$

$$E = P_{MAX} \cdot 82.2 \cdot t_U \quad (4)$$

- Average Case ... For this case it is assumed that after listing half of the transponders, the wanted one is found ($n_{TL} = \frac{n}{2}$).

$$t_{FIND} = 1.2 \cdot \frac{n}{2} \cdot t_U = 0.6 \cdot n \cdot t_U \quad (5)$$

$$t = t_{SET} + t_{FIND} + t_{READ} = (0.6 \cdot n + 81) \cdot t_U \quad (6)$$

$$E = P_{MAX} \cdot (0.6 \cdot n + 81) \cdot t_U \quad (7)$$

- Worst case ... The wanted transponder is only found after all the others have been inspected ($n_{TL} = n$).

$$t_{FIND} = 1.2 \cdot n \cdot t_U \quad (8)$$

$$t = t_{SET} + t_{FIND} + t_{READ} = (1.2 \cdot n + 81) \cdot t_U \quad (9)$$

$$E = P_{MAX} \cdot (1.2 \cdot n + 81) \cdot t_U \quad (10)$$

An overview of the analytic results from CONST is shown in Table II.

To understand the basic principle of the following proposed methods, it is essential to know the concept of field strength scaling in terms of multi transponder environments. The different possible field strengths are described as "shells". In each shell a set of transponders can be detected. The detection is possible if the shell provides enough field strength to proper supply the transponder. Therefore, each transponder can be mapped to a certain shell as shown in Fig. 3.

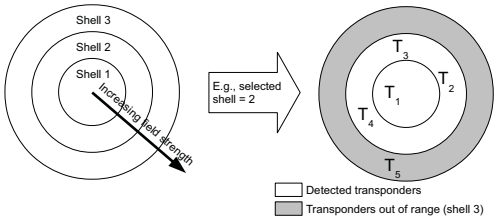


Fig. 3. Description of the perspective of using shells to describe the methods of FSS and BIN and an example of the selection of one specific shell with the resulting detection of the transponders

C. Method FSS: gradually scaling of field strength

The aim of this proposed method is to prevent two issues. First, a lot of energy is wasted in cases where a small amount of the field strength would be sufficient to reach a certain transponder. Second the more transponders that can possibly be reached, the bigger becomes the shift of the resulting resonance frequency and the effective energy transmission gets lower [12].

To prevent said issues, the field strength (shell) is dynamically scaled to consume a power of $P = P_i$. In the last shell, the power consumption is equivalent to the one of the CONST algorithm, which always uses the maximum field strength. FSS simply scales the field strength gradually until the wanted transponder can be found or the maximum output power is reached.

A disadvantage of the FSS algorithm however is the fact that it may have to step through multiple field strengths, in the worst case all n of them, which leads to an increased overhead, depending on the number of times the algorithm has to switch to another field strength. The results of the analytic evaluation of FSS is shown in Table III. P_i is set to shell 1 for the best case, shell 2 for the average case, and to shell $P_I = P_{MAX}$ for the worst case.

D. Method BIN: executing a binary quadratic search through the field strengths

FSS strictly scales the field strength from the lowest to the highest shell, which is not optimal, if for example the wanted transponder is in the last shell. BIN handles these scenarios more efficiently. This is achieved with a quadratic binary search through the available field strengths. Given that the field strengths do not grow linearly, which was already shown in Fig. 2, a commonly used linear binary search would be very inefficient. Therefore, an optimized quadratically binary search was designed for use with BIN. The algorithm handles

TABLE II
ENERGY CONSUMPTION OF THE DIFFERENT CASES OF THE CONST METHOD (BASIC ANTI-COLLISION PROCEDURE)

	Energy
Best Case	$P_{MAX} \cdot 82.2 \cdot t_U$
Average Case	$P_{MAX} \cdot (0.6 \cdot n + 81) \cdot t_U$
Worst Case	$P_{MAX} \cdot (1.2 \cdot n + 81) \cdot t_U$

TABLE III
ENERGY CONSUMPTION OF THE DIFFERENT CASES OF THE PROPOSED FSS METHOD

	Energy
Best Case	$P_{MAX} \cdot 54.50 \cdot t_U$
Average Case	$P_{MAX} \cdot (0.45 \cdot n + 67.33) \cdot t_U$
Worst Case	$P_{MAX} \cdot (1.2 \cdot n + 103.4) \cdot t_U$

ConTEL 2013, ISBN: 978-953-184-180-1

TABLE IV
ENERGY CONSUMPTION OF THE DIFFERENT CASES OF THE PROPOSED BIN METHOD

	Energy
Best Case	$P_{MAX} \cdot 56.31 \cdot t_U$
Average Case	$P_{MAX} \cdot (0.49 \cdot n + 69.93) \cdot t_U$
Worst Case	$P_{MAX} \cdot (1.2 \cdot n + 89.29) \cdot t_U$

the field strengths as a sorted list, starts with a field strength close to the mean one, tests whether the wanted transponder can be detected with this field strength (shell) or not, and recursively continues in the lower or upper half of the list to look for another field strength that can detect the transponder. Table IV shows a summary of the different cases of the BIN algorithm. P_i is set to shell 2 for the best and average case (starting shell), and to shell $P_i = P_{MAX}$ for the worst case.

E. Comparison of the proposed methods

The comparison of the two proposed methods FSS and BIN to the standard implementation CONST is shown in Fig. 4. For a more general view, the results are shown in relation to the transponders in range (in field). FSS performs very well energy wise in the best as well as the average case, being the most efficient of all the algorithms. In the worst case FSS is not the best but rather the worst choice of all, caused by the fact that all field strength scaling operations are necessary and a lot of time is wasted while searching for a transponder that can only be found in the last step. BIN is a bit less efficient than FSS in the best case but still much better than CONST. In the average case BIN performs better than CONST but worse than FSS, given its complex internal logic. In the worst case, BIN is the second best choice and can abort an inconclusive search much faster than FSS. Therefore, overall BIN is a good choice, given that it performs nearly as good as FSS in the best and even much better than FSS in the worst case. CONST, the standard approach, always using the maximum field strength naturally leads to a lot of unnecessary energy waste. CONST however offers an otherwise unmatched performance in worst case scenarios. No other algorithm can abort an inconclusive search that fast. Nevertheless, CONST does perform very badly in scenarios with many transponders close to each other, whereas the other algorithms, trough their incrementally increased or step-wise set field strengths usually do not have any problems finding most or all of the transponders.

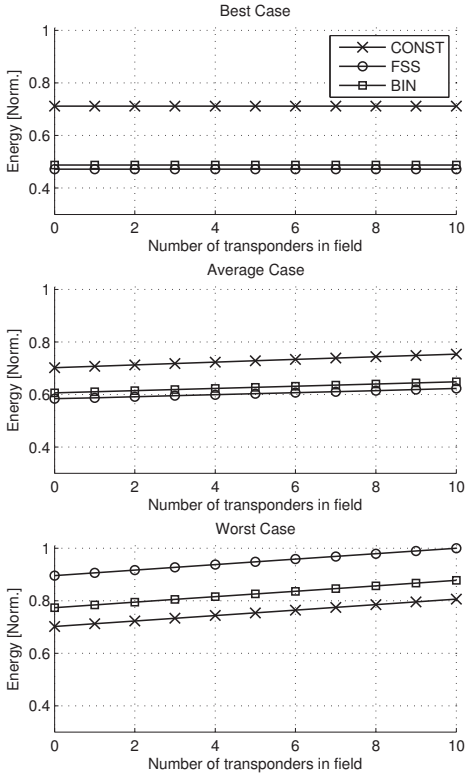


Fig. 4. Overview over the needed energy consumptions, based on the analytic results from Table II to IV, of the different implementations in relation to the number of transponders

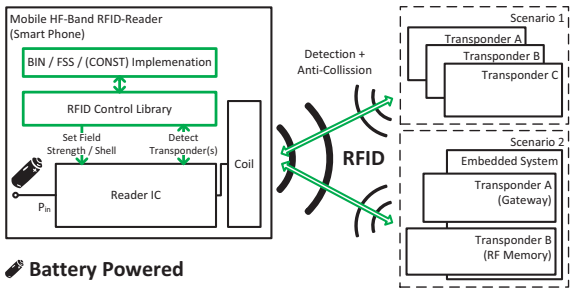


Fig. 5. Deployment model of the multi transponder environment using the proposed methods FSS and BIN

F. Deployment into the multi transponder environment

The proposed methods are implemented and deployed into the multi transponder environment as shown in Figure 5. An advantage of the proposed methods is that they only need to observe and control the RFID-Reader. The transponders don't have to be modified. The only needed functionality of the transponders is their ability to respond. The current implementation is based on a software approach, which is enough to implement a proof of concept. The software consists of a library to control the field strength and a detection of the transponder(s) and the library of the three implementations FSS, BIN and CONST.

IV. EXPERIMENTAL RESULTS

This section shows the results of the case study of supplying up to ten transponders at once using the proposed methods (BIN and FSS). This case study is done using real hardware. The proposed methods are deployed on the System Under Test (SUT) consisting of a HF-Band RFID-Reader combined with a development board using Android as operating system, and the smart cards. The power consumptions are measured

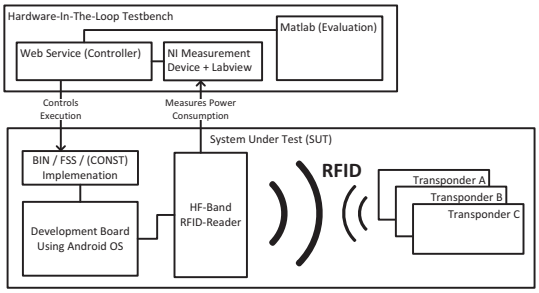


Fig. 6. This component model shows the measurement setup used for the case study, consisting of the hardware-in-the-loop testbench and the SUT (Android development board and a HF-Band RFID-Reader).

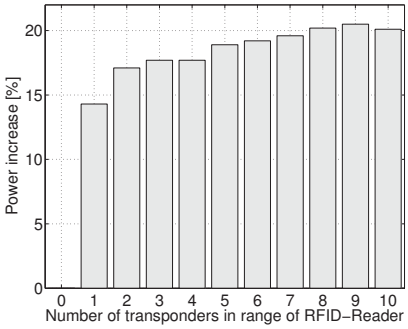


Fig. 7. Measured RFID-Reader's power consumption impact of n transponders in transmission range, relative to zero transponders

through a hardware-in-the-loop testbench using Labview for measurement and Matlab for evaluation (see Fig. 6). To compare the results to the standard implementation, the CONST (simple anti-collision procedure) method is also deployed on the SUT. The measurement setup consists of the components described in Table V. The case study is split into two parts. The first part concerns the influence to the RFID-Readers's power consumption, through multiple (0-10) transponders in transmission range. The second part shows how the proposed methods behave in terms of their energy consumption on a real embedded system.

A. Influence of n transponders to the RFID-Reader's power consumption

In this section the influence of multiple transponders to the power consumption of the reader is evaluated. In this evaluation one to ten transponders are brought into the transmission range of the RFID-Reader. The measurement setup remains the same as shown in Fig. 6. The results are shown in Figure 7. The measurement shows, that there is an impact on the power consumption, but it is not that high. It also shrinks with the increasing amount of transponders in the field. This behavior can be explained through the influence of the multiple transponders to the coupling factor and to the resulting resonance frequency. The power transfer rises when another transponder is brought into the field because the resonance frequency of a single tag is commonly tuned to a higher resonance frequency to prevent a to great detuning effect in multi tag scenarios [12]. For more tags the detuning effect becomes greater and the power increase get lower.

B. Measurement of the energy consumption of FSS and BIN

In this case study ten transponders, directly stacked upon each other, are positioned on the surface of the reader. The goal of this setup is to show how multiple of transponders, which are here up to ten, interact, especially when being that close to each other. The transponders were labeled T_1 to T_{10}. The algorithms FSS and BIN were tested against each other in ten iterations, changing the transponder to supply (field strength is scaled accordingly to provide a proper supply for

TABLE V
MEASUREMENT SETUP OF THE CASE STUDY

Measurement Device	NI PXI-1042Q
Development Board	BeagleBoard-xM
RFID-Reader	ACS ACR122U
Transponders	Type 2 Tags based on ISO/IEC 14443A

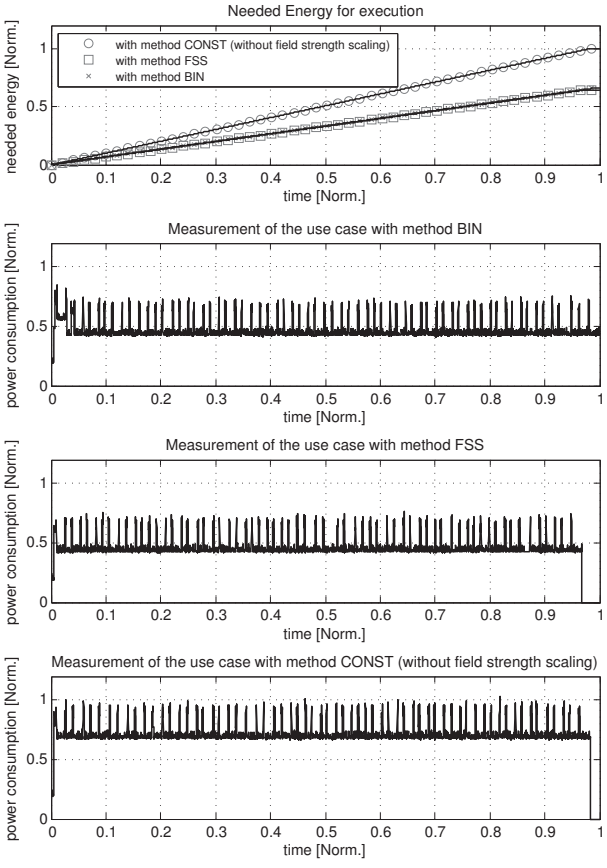


Fig. 8. Comparison of the energy consumptions over time of the algorithms BIN and FSS to CONST in a ten transponder environment

TABLE VI
COMPARISON OF THE ENERGY CONSUMPTIONS OF THE ALGORITHMS BIN AND FSS TO CONST IN A TEN TRANSPONDER ENVIRONMENT

	Energy Consumption [%]
Method BIN	68.13
Method FSS	65.53
Method CONST (without field strength scaling)	100

this transponder regardless of the others) from T_1 up to T_{10}. Fig. 8 shows a comparison of all algorithms when searching for the wanted transponder T_9. FSS and BIN are more energy efficient than the standard approach of CONST. This scenario explains the advantage of the field strength scaling principle, as both optimized algorithms are able to successfully read from the transponder with a lower field strength, whereas CONST always operates with the maximum amount. In Table VI the associated total energy consumptions are presented. Up to 34% of the RFID-Reader's energy can be saved, when using the proposed methods. The result depends on parameters like the amount of transponders in range and the physical relation, but shows the potential of field strength scaling for multiple transponders and proofs it on real hardware.

V. CONCLUSION

Properly supplying the transponder(s) using a HF-Band RFID-Reader does not always mean to provide as much power (magnetic field strength) as possible. The needed field strength depends on parameters, like the physical relation factor (e.g., distance and orientation) between RFID-Reader and transponder. Oversupplying the transponder leads to a unneeded power consumption of the RFID-Reader. Therefore, field strength scaling during runtime can be used to reduce the power consumption of the RFID-Reader. This principle of magnetic field strength scaling for one transponder is already known, but we showed that this can be also used for multiple transponders. The challenge here is that all transponders have their own physical relation factor, and also interfere with each other.

The proposed methods FSS and BIN are a way to deal with this challenge and use the transponder detection phase to find out, which field strength is needed to properly supply the transponders. We evaluated the methods in a case study with up to ten transponders. In this case study we were able to save up to 34% of the RFID-Reader's energy. This saviour can be especially important for mobile RFID-Readers to prolong their life.

ACKNOWLEDGMENT

We would like to thank our industrial partners Infineon Technologies Austria AG as well as Enso Detego GmbH for their support. Furthermore, 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 FFG 829586.

REFERENCES

[1] STMicroelectronics, "Datasheet - 16-bit EEPROM with password protection, dual interface & energy harvesting: 400 kHz IC bus & ISO 15693 RF protocol at 13.56 MHz - Doc ID 018932 Rev 8," June 2012.
[2] 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 *RFID Technology (EURASIP RFID), 2012 Fourth International EURASIP Workshop on*, sept. 2012.
[3] E. Strommer, M. Jurvansuu, T. Tuikka, A. Ylisaukko-oja, H. Rapakko, and J. Vesterinen, "NFC-Enabled Wireless Charging," in *Near Field Communication (NFC), 2012 4th International Workshop on*, 2012.
[4] N. Cho, S.-J. Song, J.-Y. Lee, S. Kim, S. Kim, and H.-J. Yoo, "A 8- mu;W, 0.3-mm2 RF-powered transponder with temperature sensor for wireless environmental monitoring," in *Circuits and Systems, 2005. ISCAS 2005. IEEE International Symposium on*, may 2005.
[5] J.-H. Cho, P. Cole, and S. Kim, "An NFC transceiver using an inductive powered receiver for passive, active, RW and RFID modes," in *SoC Design Conference (ISOCC), 2009 International*, nov. 2009.
[6] A. Loeffler, U. Wissendheit, H. Gerhaeuser, and D. Kuznetsova, "Inductively-Charged and Temporarily Self-Sufficient Operating Sensor Using Standard RFID-HF-Technology," *RFID Systems and Technologies (RFID SysTech), 2009 5th European Workshop on*, june 2009.
[7] M. Zargham and P. Gulak, "Maximum Achievable Efficiency in Near-Field Coupled Power-Transfer Systems," *Biomedical Circuits and Systems, IEEE Transactions on*, vol. 6, no. 3, june 2012.
[8] D. Cheng, Z. Wang, and Q. Zhou, "Analysis of distance of rfid systems working under 13.56mhz," in *Wireless Communications, Networking and Mobile Computing, 2008. WiCOM '08. 4th International Conference on*, oct. 2008, pp. 1 –3.
[9] E. Rolf and V. Nilsson, "Near Field Communication (NFC) for Mobile Phones," in *Near Field Communication (NFC) for Mobile Phones*, 2006.
[10] X. Xu, L. Gu, J. Wang, G. Xing, and S.-C. Cheung, "Read more with less: An adaptive approach to energy-efficient rfid systems," *Selected Areas in Communications, IEEE Journal on*, vol. 29, no. 8, pp. 1684 –1697, september 2011.
[11] K. Fotopoulou and B. Flynn, "Wireless Power Transfer in Loosely Coupled Links: Coil Misalignment Model," *Magnetics, IEEE Transactions on*, vol. 47, no. 2, feb. 2011.
[12] H. Witschnig and E. Merlin, "Modeling of Multilabel Scenarios of 13.56 MHz RFID Systems," in *Microwave Conference, 2008. EuMC 2008. 38th European*, oct. 2008.
[13] P.-H. Thevenon, O. Savry, and S. Tedjini, "Minimization of energy consumption in passive HF contactless and RFID systems," in *Software, Telecommunications and Computer Networks (SoftCOM), 2011 19th International Conference on*, sept. 2011.
[14] M. Gebhart, J. Bruckbauer, and M. Gossar, "Chip impedance characterization for contactless proximity personal cards," in *Communication Systems Networks and Digital Signal Processing (CSNDSP), 2010 7th International Symposium on*, 2010, pp. 826–830.
[15] O. Unsal and I. Koren, "System-level power-aware design techniques in real-time systems," *Proceedings of the IEEE*, vol. 91, no. 7, pp. 1055 – 1069, july 2003.
[16] S. Chatterjee, S. Roy, and S. Bandyopadhyay, "Hop-efficient and power-optimized routing strategy in a decentralized mesh network using directional antenna," in *Parallel and Distributed Computing, 2006. ISPDC '06. The Fifth International Symposium on*, july 2006, pp. 155 –160.
[17] L. Benini, A. Bogliolo, and G. De Micheli, "A survey of design techniques for system-level dynamic power management," *Very Large Scale Integration (VLSI) Systems, IEEE Transactions on*, vol. 8, no. 3, june 2000.
[18] S. Haoru, D. Ko, and S. An, "Power-aware location-based anti-collision protocol for RFID-sensor networks," in *Ubiquitous and Future Networks, 2009. ICUFN 2009. First International Conference on*, june 2009.
[19] J. G. Kim, "A Divide-and-Conquer Technique for Throughput Enhancement of RFID Anti-collision Protocol," *Communications Letters, IEEE*, vol. 12, no. 6, june 2008.
[20] M. Berhea, C. Chen, and Q. Wu, "Protocol-level performance analysis for anti-collision protocols in RFID systems," in *Circuits and Systems, 2008. ISCAS 2008. IEEE International Symposium on*, may 2008.
[21] F. Zhou, C. Chen, D. Jin, C. Huang, and H. Min, "Evaluating and Optimizing Power Consumption of Anti-Collision Protocols for Applications in RFID Systems," in *Low Power Electronics and Design, 2004. ISLPED '04. Proceedings of the 2004 International Symposium on*, aug. 2004.

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.

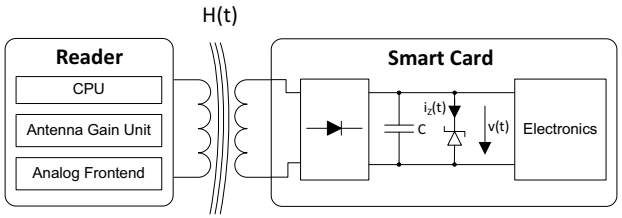


Fig. 1. Principle of a reader / smart card system. The reader generates a magnetic field for power supply and communication purposes. The induced electrical current is rectified and afterwards buffered within the capacitor C. A Zener diode prevents the electronics from electric surges.

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.

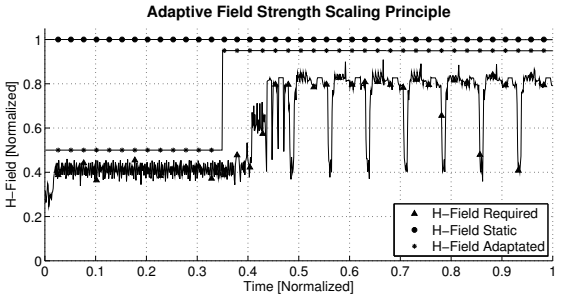


Fig. 2. Principle of the Adaptive Field Strength Scaling methodology. The magnetic field that is generated by the reader is adapted to the instantaneous power consumption of the smart card. During the smart card's high power consumption periods, the magnetic field strength is increased, otherwise it is decreased. Thus, electrical power can be saved compared to traditional static magnetic field strength approaches.

- 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

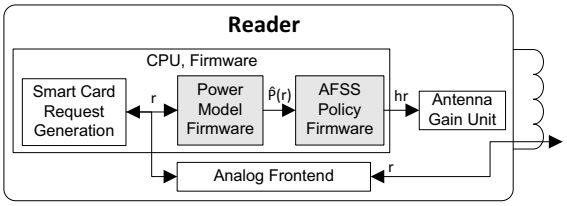


Fig. 3. Principle of the reader AFSS request-based approach. A smart card request r is generated and passed to the power model firmware. A power value $\widehat{P}(r)$ is estimated, which is needed by the smart card to process the request r properly. Based on this information, the AFSS policy firmware signals the antenna gain unit by means of a message hr to adapt the magnetic field strength.

the 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

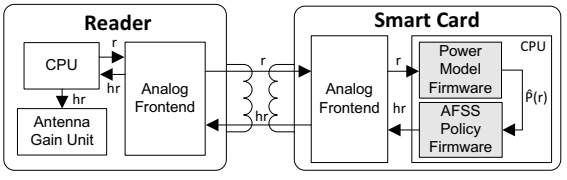


Fig. 4. Principle of the smart card AFSS request-based approach. A smart card request r is generated by the reader and is transmitted to the smart card. The smart card forwards r to the power model firmware and estimates the needed power $\widehat{P}(r)$ to execute the request properly. Then the AFSS 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.

$$\widehat{P}(r) = f(r, \mathbf{x}, k, v(t), ZenerDiodeState) \quad (2)$$

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.

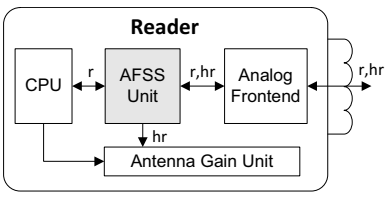


Fig. 5. Architecture of the AFSS unit enhanced reader. The received data r, hr from the smart card is monitored within the AFSS unit. If a field adaptation message hr is detected, then the AFSS unit signals the antenna gain unit to modify the magnetic field strength accordingly. No slow software interactions are needed.

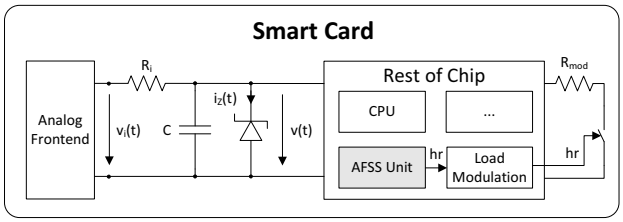


Fig. 6. Equivalent circuit of the AFSS enhanced smart card. The AFSS unit monitors the smart card's stability parameters and uses the load modulation unit to transmit high priority magnetic field change messages hr to the reader.

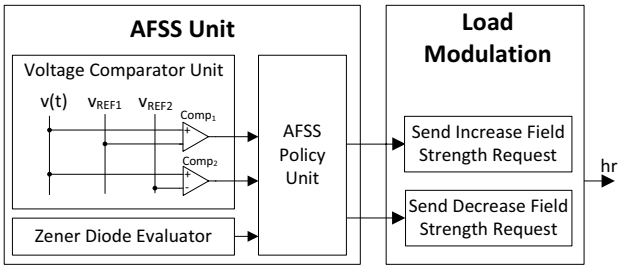


Fig. 7. The results of the voltage comparator and the Zener diode evaluator units are forwarded to the AFSS policy unit. Based on the provided information, the AFSS policy unit signals the load modulation unit if a magnetic field increase or decrease message should be sent.

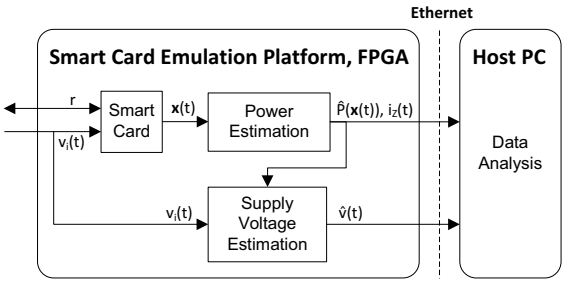


Fig. 9. Hardware emulation platform that is used to evaluate the novel AFSS approaches. The estimates of power and supply voltage estimation units are sent over Ethernet to a host PC for further data analysis tasks. Average estimation errors of 8.4% and 2% are caused respectively.

- 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

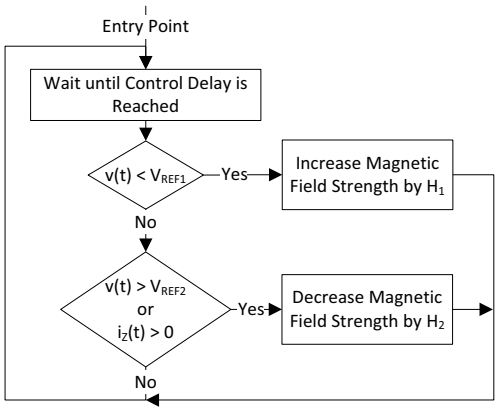


Fig. 8. AFSS policy: If $v(t)$ drops below a threshold V_{REF1}, then the magnetic field should be increased. Otherwise, if the Zener diode conducts or $v(t)$ is above V_{REF2}, then the magnetic field should be reduced to save electrical power.

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%.

$$\widehat{P}(\mathbf{x}) = \widehat{P}_{stat} + \widehat{P}_{dyn} = c_0 + \sum_{i=1}^{n} c_i \cdot x_i = c_0 + \mathbf{c^T} \cdot \mathbf{x} \quad (3)$$

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

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

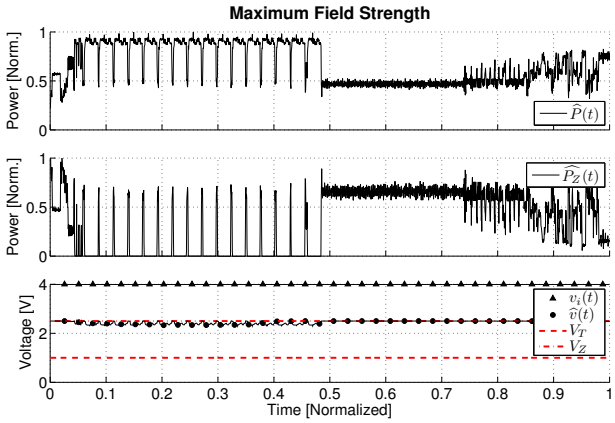


Fig. 10. This figure illustrates the smart card behavior of current RFID and NFC application approaches. A maximum magnetic field is generated to guarantee a high smart card operational stability. No hazardous $\widehat{v}(t)$ voltage drops below V_T are recognizable during this benchmark. $\widehat{P_Z}(t)$ represents the amount of electrical power that is wasted by the Zener diode.

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.

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

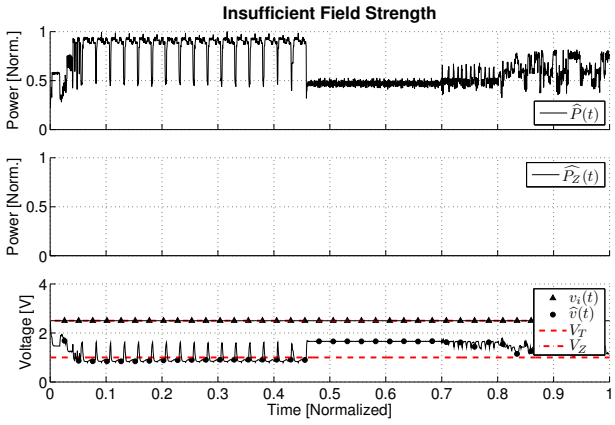


Fig. 11. This figure depicts the smart card behavior during a period of low magnetic field supply. The supply voltage $v_i(t)$ that is embossed by the magnetic field is only as high as 2.5 V. $\widehat{v}(t)$ drops hazardously below the threshold V_T and provokes smart card instabilities. Due to supply starvation, $\widehat{P_Z}(t)$ stays zero. Thus, no electrical power is wasted.

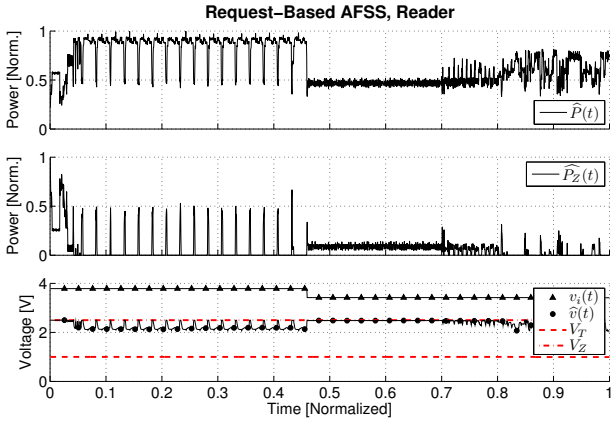


Fig. 12. This figure depicts the smart card behavior while using the reader implemented *request-based AFSS* technique. The reader increases the magnetic field during the processing of the SHA smart card request. Voltage $v_i(t)$ changes correspondingly. No $\widehat{v}(t)$ drops below the crucial threshold 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.

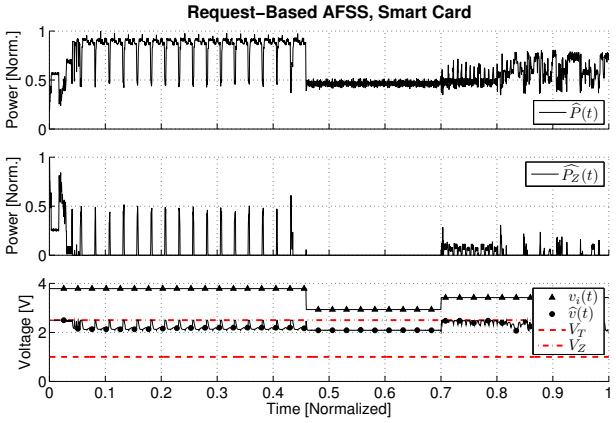


Fig. 13. This figure shows the smart card behavior while using the smart card implemented *request-based AFSS* technique. The reader is requested to increase the magnetic field during the processing of the SHA benchmark. Voltage $v_i(t)$ changes correspondingly. No $\widehat{v}(t)$ drops below the crucial 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.

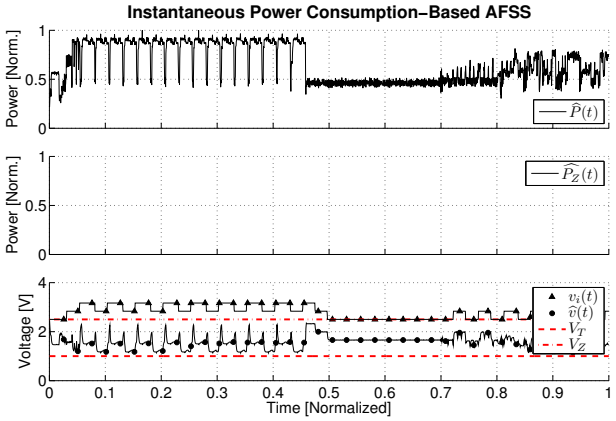


Fig. 14. Smart card behavior of the *Instantaneous Power Consumption-Based AFSS* implementation. The smart card constantly evaluates crucial parameters like $\widehat{v}(t)$, $i_Z(t)$, etc. and requests magnetic field adaptations if necessary. $\widehat{P}_Z$ is minimized while preserving the smart card's 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.

2013 16th Euromicro Conference on Digital System Design

PtNBridge - A Power-Aware and Trustworthy Near Field Communication Bridge to Embedded Systems

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

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

***Abstract*—More than 500 million Near Field Communication (NFC) devices will be delivered in 2014. This technology enables a lot of application fields like using it for bridges to embedded systems (e.g., smart meters). With this wireless bridge the user can interact with the embedded system using an off-the-shelf NFC-enabled smart phone. The user of such a bridge also trusts in the system's security. Furthermore, this security should not lead to an excessive battery drain of the smart phone nor the embedded system. This publication deals with these concerns and shows a method called PtNBridge. The method secures the whole communication path from the smart phone application to the accessed module in the embedded system (e.g., power sensor of the smart meter). To take account of the energy consumption, the PtNBridge has been analyzed and optimized to avoid an excessive battery drain. Two variants of the PtNBridge have been implemented, which aim for two different goals of power-aware security.**

***Keywords*-RFID, energy management, security, embedded system**

I. Introduction

Near Field Communication (NFC) is a technology which enables an easy to use wireless communication over short distances (<10cm). Other benefits are the short time to establish a connection, and the ability to wirelessly transfer data and power. These benefits enable a lot of innovative use cases. One of them is wirelessly interacting with other embedded systems (e.g., smart meters). This interaction will be called NFC-Bridge in this paper. There are several publications about this topic like NIZE from Druml et al. [1], which proposes an NFC Interface enabling zero energy standby for electronic devices. The benefit of using NFC-Bridges is that common NFC-enabled smart phones can be used as an interface to control, configure, or monitor the embedded system. Adding complex physical user interfaces directly into an embedded system is not needed anymore. An exemplary use case is displaying the currently consumed energy of a household or even a graphical representation of the daily consumption per hour by simply holding your smart phone in front of the smart meter.

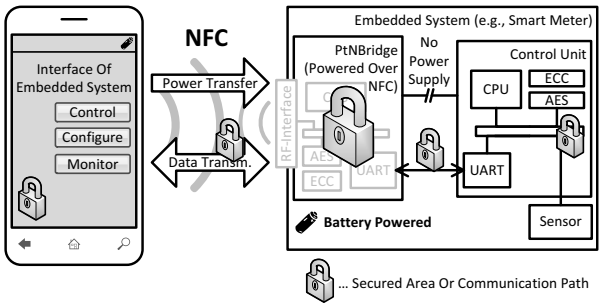


Figure 1. Integration of the proposed PtNBridge method in an exemplary embedded system (smart meter). It shows the proposed secured communication paths, and the energy sources of the system (battery in the embedded system and in the smart phone).

Unfortunately, this NFC-Bridge opens new security related attack vectors to the system. These new vectors are the smart phone application itself, the NFC communication, the communication to the embedded system, and the bus to the attached sensor. Concepts to secure the NFC communication, and also strategies to encrypt buses in embedded systems exist. However, securing the whole communication path is commonly not considered. The user trusts in the security of the system. If this trust is violated, the NFC-Bridge is not usable for commercial products. Additionally, a secure NFC-Bridge which excessively drains the battery of the smart phone or the embedded system has no practical use. This additional battery drain occurs through the calculation of the cryptographic algorithms and the used level of security (longer keys need more time to calculate).

Another special issue occurs through the power transfer of NFC. The NFC-Bridge itself can be powered over NFC, which has the benefit that the embedded system does not need to provide the energy for the bridge (for applications, where the capacity of the battery of the embedded system is very limited). Unfortunately, this power transfer is very lossy

`/13 $26.00 © 2013 IEEE
DOI 10.1109/DSD.2013.102

(inductive coupling over the air over several centimeters). This means that cryptographic operations executed on the wirelessly powered NFC-Bridge can be very energy consuming for the energy source of the smart phone.

Therefore, a NFC-Bridge is needed, which can secure the whole communication path from the smart phone application to the accessed module of the embedded system. Additionally, this bridge should be designed power-aware to avoid an excessive battery drain (overview is shown in Figure 1). This work makes following contributions:

- It presents two variants of the method called PtNBridge, which is an NFC-Bridge that secures the whole communication using Elliptic Curve Cryptography (ECC) and AES to satisfy the trust of the user.
- The additional energy drain of using security for NFC-Bridges for the embedded system and the smart phone has been evaluated and optimized in the design of the PtNBridge.
- The two variants of the PtNBridge, using the results of the energy evaluation, have been implemented on real hardware in form of a case study (reference implementation of a smart meter on an FPGA).

II. Related Work

The related work is split into three parts. The first part deals with the security concepts for NFC and RFID. The second part shows the existing concepts regarding security for embedded systems. The third part emphasizes the relevance of power-aware security.

A. Security concepts for NFC and RFID

NFC has the drawback that the wireless communication is not natively encrypted, and therefore can be recorded or even manipulated. Therefore, security is needed to prevent this. Haselsteiner et al. talk about these threats like eavesdropping and data corruption and the possible countermeasures like using RSA and AES. They also present a simple and fast key agreement mechanism [2]. The threats are not only restricted to the wireless communication path. Madlmayr et al. describe that some NFC applications need to communicate with a secure element (e.g., Sim card of the smart phone). If this path is not secured, the attacker has another vulnerable vector to access the system [3]. Another security concept is the mutual authentication. In some cases both parties need to know, if their opponent is authorized. Chi-Huan et al. present an approach for a mutual authentication system for wireless sensor networks, where the wireless communication is only used as a bridge [4]. O'Neill et al. show how digital signatures can be used in RFID-Systems [5]. Another important factor, when talking about security, is the used encryption algorithm. ECC is suitable to exchange keys (smaller key size by providing the same level of security). Aigner et al. present an ECC coprocessor for smart cards and evaluate its performance in terms of clock cycles [6].

B. Security concepts for embedded systems

When talking about security in embedded systems, we have to consider, what level of security makes sense. Barker et al. present in a NIST (National Institute of Standards and Technology) publication the recommended security strength and how long it will be secure. They propose that the strength of 80 is the absolute minimum and the strength of 112 will be secure till 2030 [7]. Another aspect is that security can be deployed on several levels of abstractions. Hwang et al. show how embedded systems can be secured using these different abstraction levels (from protocol down to the circuit level) [8]. Embedded systems are commonly limited in their resources (e.g., energy, computation power). Ravi et al. talk about choosing the "right" security to implement in embedded systems [9]. Eisenbarth et. al made a survey of Lightweight-Cryptography implementations in terms of performance and hardware [10]. Poktonjak et al. show a way to create trusted sensors in hardware via simple structures to respect those resource constraints [11]. The authors of [12] use an XOR to secure transmissions over buses. Also in the sector of embedded systems, ECC is interesting. Wenger et al. present an ECC implementation for an 8-bit AVR-based RISC processor [13]. Alrimeih et al. compared ECC in timing and performance with different levels of security [14].

C. Power-aware security concepts and evaluations

When talking about mobile embedded systems and NFC, power-awareness is essential. Caviglione et al. describe that green aware security is important, because security should not be an energy waster in the system [15]. To deal with power-awareness, power-evaluations are needed. Wander et al. talk about the energy consumption of public-key cryptography for embedded systems and compare the results [16]. Trakadas et al. present the resulting overheads in timing and power for different security algorithms [17]. Bertoni et al. evaluate ECC in terms of the power-consumption in wireless sensor networks [18]. Jiang et al. made a measurement-based analysis of the power consumption for different encryption algorithms [19]. With these evaluations, the "right" security for the power-aware NFC-Bridge can be chosen.

III. Method

This section describes the PtNBridge. It is divided into five parts. The first part shows the general concept and the description of the investigated system. In the parts two to four, the evaluation of the possible security algorithms in terms of timing, consumed energy and security strength is shown. The fifth part shows the final result of the evaluation.

A. Concept

Before the concept can be designed, the investigated system has to be defined (as shown in Fig. 2). In our case, we investigated a system consisting of a mobile NFC-Reader

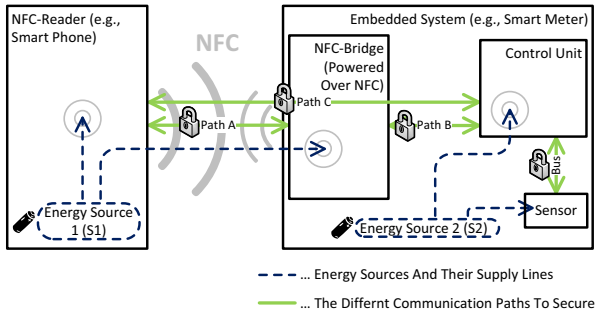


Figure 2. Overview of the investigated system, the possible path's to secure the communication (Path A, B, C and Bus), and the energy sources including the mapping, what they supply.

(e.g., smart phone) and a battery powered embedded system (e.g., smart meter). These are connected using an NFC-Bridge. The energy source 1 (S1) supplies the NFC-Reader and the NFC-Bridge. The energy source 2 (S2) supplies the embedded system and the sensor, but not the NFC-Bridge electronics. The communication paths to be secure are divided into Path A, Path B, Path C and Bus. The communication is separated into two variants. Variant 1 (V1) encrypts the data from the NFC-Reader to the NFC-Bridge (Path A), and separately encrypts the data from the NFC-Bridge to the embedded system (Path B). In variant 2 (V2) the NFC-Bridge is transparent and the data is encrypted between the NFC-Reader and the embedded system (Path C). The benefit of variant 1 is that the embedded system can remain idle until an authorized communication occurs (NFC-Bridge is able to block unauthorized access). The encryption on the sensor (Bus) is considered separately.

As next step, the security algorithms to investigate have to be selected. These are separated into the algorithm to perform a key exchange and the one to encrypt the data. The selection is based on the definition of the security strength described by [7]. The selected algorithms are ECC for the key exchange and AES for the encryption of data. The security strength 80 to 112 are investigated by altering the domain parameters for ECC.

The bus encryption is important to secure the whole

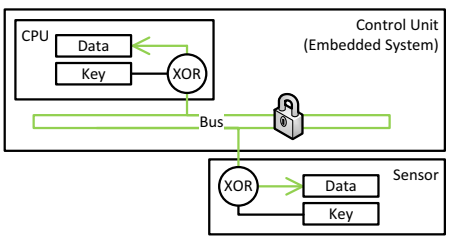


Figure 3. Proposed bus encryption algorithm adapted from [12] using an XOR and a private key to encrypt the data between sensor and CPU.

communication path. Through the computation limitations of the components (e.g., the sensor), encryptions like ECC and AES create a too large overhead. Therefore, the approach described in [12] by using an XOR to encrypt the plain data using a secret key (as shown in Fig. 3) is applied. The following list provides an overview of the used variants and encryptions of this paper:

- **Encryptions.** ECC is done with the curves secp160r1, secp192r1, and secp224r1. The data is encrypted using an AES-128. The bus encryption is done using an XOR.
- **Variant 1 (V1).** Separate key exchange (ECC) and encryption (AES) between the NFC-Reader and the NFC-Bridge as well as between the NFC-Bridge and the embedded system (Path A and B).
- **Variant 2 (V2).** One key exchange (ECC) and encryption (AES) between the NFC-Reader and the embedded system (Path C).

B. Evaluation of timing and consumed energy

As next steps the two variants and encryptions are evaluated in timing, their energy consumption, and the security strength. The purpose from the evaluation is to answer two questions. The first one is how much more energy is consumed when using encryption with a higher strength of security. The second question is about the difference between the two proposed variants (V1 and V2) in terms of their energy consumption.

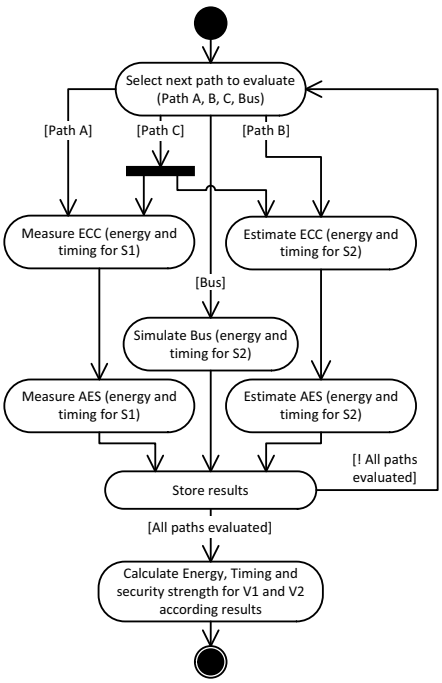


Figure 4. Used evaluation flow to get the consumed energy, timings and security strength for the proposed variants (V1 and V2).

For the evaluation measurements, power estimations and simulations have been made for the different communication paths and encryptions. The procedure is shown in Fig. 4. The used methods for evaluation are described in the following enlistment:

- **Measurement.** For the NFC-Reader, an Android smart phone has been used. The cryptographic library called Spongycastle is used. The data acquisition is done with a NI-DAQ 6009. The power consumption from the NFC-Reader is directly measured at the battery (sampling rate 1kS). The measurement uses a hardware in the loop measurement tool, which controls the Android application and acquires the power consumption. These results are used for evaluation of Path A and C.
- **Power Estimation.** A Spartan III FPGA Board is used. As CPU, a modified version of a Leon 3 (30 Mhz) with integrated Power Estimation Units (PEU) is synthesized, which uses a power characterization approach similar to [20]. For the cryptography a native C library is used. The results are needed to evaluate Path B and C.
- **Simulation.** Modelsim is used to get the timing. The simulation is needed for non power characterized hardware implementations like the bus encryption.

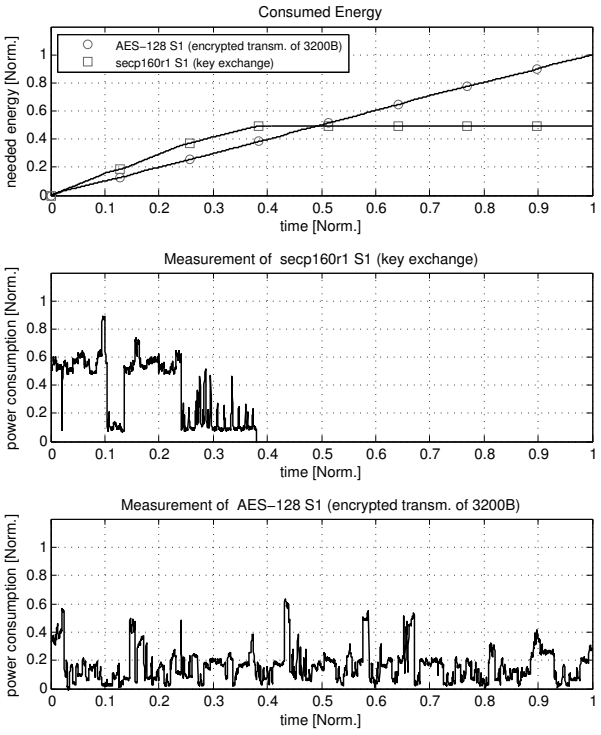


Figure 5. Abstract from the measurement results of the key exchange (ECC) and encrypted data transmission (AES) from the NFC-Reader to the NFC-Bridge (for S1).

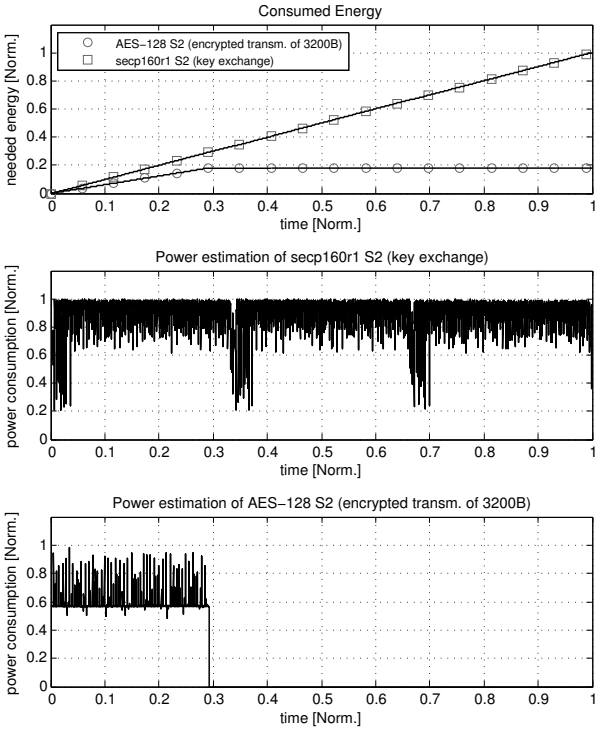


Figure 6. Abstract from the power estimation results of the key exchange (ECC) and encrypted data transmission (AES) from the NFC-Bridge to the embedded system (for S2).

An abstract of the result from the measurement is shown in Fig. 5. It shows that the timing and energy behavior of the used cryptographic library (Spongycastle). The transmission of 1 kByte of encrypted data to the NFC-Bridge needs 1.5 times less energy than the key exchange.

The power estimation (Fig. 6) shows, the timing and energy behavior of the cryptographic library (native C) on the embedded system. The transmission of 1 kByte of encrypted data to the NFC-Bridge needs 18 times less energy than the key exchange. A direct comparison of the timings of the power estimation and the measurement does not make sense, because the NFC-Reader uses a different cryptographic library compared to the embedded system, which uses a native C library. Additionally the NFC-Reader uses an operating system, which generates an additional overhead. The results of the measurement, power estimation and simulation are now used to evaluate the proposed two variants V1 and V2. Following shortcuts are used in the evaluation:

- **V1:** Investigated variant 1 (described in Fig. 7).
- **V2:** Investigated variant 2 (described in Fig. 8).
- **S1:** Energy source of NFC-Reader and NFC-Bridge.
- **S2:** Energy source of the embedded system.

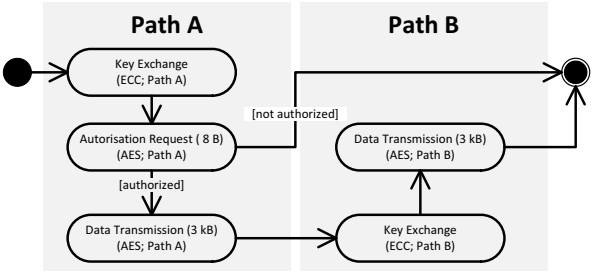


Figure 7. Flow diagram of the proposed variant 1 (V1) describing, what paths and encryptions are used for authorized and unauthorized access.

C. Evaluation of variant 1 (V1)

The flow diagram for V1 is shown in Fig. 7. The flow includes checks if the sender is authorized to send data to the embedded system. In case of an authorized access, the key exchange using ECC is done twice (Path A and B). The data encryption uses AES and transmits 3kB. This transmission is also done twice (relaying of data from path A to path B). If the sender is not authorized to send data, the key exchange is only done once (path A) and only a small amount of encrypted data (8 Bytes) are transmitted using path A. The timing of V1 is calculated using (1) to (3).

$$T_{PathA} = T_{KeyA} + T_{CryptTXA} + T_{CryptRXA} \quad (1)$$

$$T_{PathB} = T_{KeyB} + T_{CryptTXB} + T_{CryptRXB} \quad (2)$$

$$T_{V1} = T_{PathA} + T_{PathB} + T_{Sensor} \quad (3)$$

The timing of V1 (T_{V1}) consist of the key exchange and encryption from path A and path B. Additionally the needed time from the sensor (bus encryption) is added. As next step, the energy consumption of V1 is calculated using (4) to (8).

$$E_{PathA} = E_{KeyExchA} + E_{CryptTXA} + E_{CryptRXA} \quad (4)$$

$$E_{PathBS1} = E_{KeyBS1} + E_{CryptTXBS1} + E_{CryptRXBS1} \quad (5)$$

$$E_{PathBS2} = E_{KeyBS2} + E_{CryptTXBS2} + E_{CryptRXBS2} \quad (6)$$

$$E_{V1S1} = E_{PathA} + E_{PathBS1} + E_{IdleS1} \quad (7)$$

$$E_{V1S2} = E_{IdleS2} + E_{PathBS2} + E_{Sensor} \quad (8)$$

The energy consumption of V1 is divided into two results for each energy source (E_{V1S1} and E_{V1S2}). This equations include the idle energy, while waiting until the cryptographic operation of the opponent is complete (E_{IdleS1} and E_{IdleS2}). For example the encryption of path A has the greatest impact to S1 (E_{PathA}), while the embedded system remains idle during that time and consumes only a small amount of energy (E_{IdleS2}). At last the security strength of V1 is calculated using (9).

$$S_{V1} = min(S_{KeyA}, S_{CryptA}, S_{KeyB}, S_{CryptB}) \quad (9)$$

Table I
RESULTS OF THE EVALUATION OF VARIANT 1 (V1)

S_{CryptA} S_{KeyA}	S_{CryptB} S_{KeyB}	T_{V1} [Norm.]	E_{V1} (S1/S2) [Norm.]	S_{V1}
AES-128 secp160r1	AES-128 secp160r1	0.77	0.7 / 0.014	80
AES-128 secp192r1	AES-128 secp192r1	0.87	0.86 / 0.021	96
AES-128 secp224r1	AES-128 secp224r1	1	1 / 0.029	112

Table II
RESULTS OF THE EVALUATION OF VARIANT 1 (V1), WHEN SENDER (E.G., SMART PHONE) IS NOT AUTHORIZED

S_{CryptA} S_{KeyA}	T_{V1} [Norm.]	E_{V1} (S1/S2) [Norm.]	S_{V1}
AES-128 secp160r1	0.1	0.15 / 0.00062	80
AES-128 secp192r1	0.12	0.23 / 0.00074	96
AES-128 secp224r1	0.14	0.28 / 0.00087	112

The security strength S_{V1} is defined through their weakest encryption.

The results for V1 is shown in Table I. In Table II the consumed energy and timing of V1 is shown, when the sender (e.g., smart phone) is not authorized to use the NFC-Bridge.

Following answers to the two questions can be given:

- When an authorized user uses the NFC-Bridge, elevating the strength of security from 80 to 112 leads to an increase of 43 % of the energy consumption for S1, and 107 % of the energy consumption for S2.
- When a non authorized user uses the NFC-Bridge, elevating the strength of security from 80 to 112 leads to an increase of 87 % of the energy consumption for S1 and 40 % of the energy consumption for S2.
- A non authorized access to the system needs 21 % energy from S1, and 4.4 % energy from S2 compared to the needed energy for an authorized access (security strenght of 80).

D. Evaluation of variant 2 (V2)

The next step of the evaluation focuses on V2 (Fig. 8). The major change to the equations is that the key exchange and

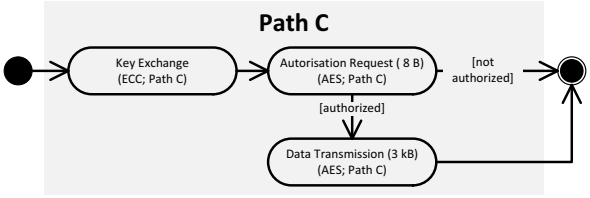


Figure 8. Flow diagram of the proposed variant 2 (V2) describing, what paths and encryptions are used for authorized and unauthorized access.

Table III
RESULTS OF THE EVALUATION OF VARIANT 2 (V2)

S_{CryptC} S_{KeyC}	T_{V2} [Norm.]	E_{V2} (S1/S2) [Norm.]	S_{V2}
AES-128 secp160r1	0.35	0.29 / 0.012	80
AES-128 secp192r1	0.44	0.37 / 0.018	96
AES-128 secp224r1	0.54	0.45 / 0.026	112

Table IV
RESULTS FROM THE EVALUATION OF VARIANT 2 (V2), WHEN SENDER (E.G., SMART PHONE) IS NOT AUTHORIZED

S_{CryptC} S_{KeyC}	T_{V2} [Norm.]	E_{V2} (S1/S2) [Norm.]	S_{V2}
AES-128 secp160r1	0.17	0.14 / 0.0098	80
AES-128 secp192r1	0.26	0.23 / 0.016	96
AES-128 secp224r1	0.36	0.31 / 0.024	112

the encrypted data transmission is only done once using path C. The authorization is now done by the embedded system. This means that the embedded system also has to wake up, even when the sender is not authorized. The evaluation of the timing is done by using (10) and (11).

$$T_{PathC} = T_{KeyC} + T_{CryptTXC} + T_{CryptRXC} \quad (10)$$

$$T_{V2} = T_{PathC} + T_{Sensor} \quad (11)$$

The evaluation of the energy consumption is similar, to the timing, with the difference of calculating the energy for S1 and S2 as shown in (12) to (15).

$$E_{PathCS1} = E_{KeyCS1} + E_{CryptTXCS1} + E_{CryptRXCS1} \quad (12)$$

$$E_{PathCS2} = E_{KeyCS2} + E_{CryptTXCS2} + E_{CryptRXCS2} \quad (13)$$

$$E_{V2S1} = E_{PathC} + E_{PathCS1} + E_{IdleS1} \quad (14)$$

$$E_{V2S2} = E_{IdleS2} + E_{PathCS2} + E_{Sensor} \quad (15)$$

The strength of security now depends on one key exchange (S_{KeyC}) and data encryption (S_{CryptC}) as shown in (16).

$$S_{V2} = min(S_{KeyC}, S_{CryptC}) \quad (16)$$

The results from the evaluation of V2 are shown in Table III under the condition of an authorized access. The results for an unauthorized access are shown in Table IV.

Following answers to the two questions can be given:

- In V2, in case of an authorized user access, elevating the strength of security from 80 to 112 leads to an increase of 55 % of the energy consumption for S1, and 117 % of the energy consumption for S2.
- When a non authorized user tries to access using V2, elevating the strength of security from 80 to 112 leads to an increase of 121 % of the energy consumption for S1, and 145 % of the energy consumption for S2.
- A non authorized access to the system needs 48 % energy from S1, and 82 % energy from S2 compared to the needed via an authorized access (security strenght of 80 and V2).

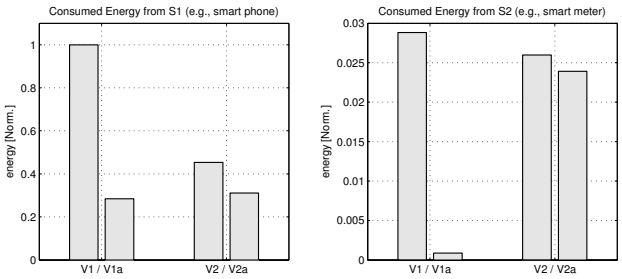


Figure 9. Result from the evaluation of the energy consumption separated to the two energy sources S1 and S2 for both variants V1 and V2. Both variants are split into an authorized (V1, V2), and non authorized access (V1a, V2a).

E. Comparison of both variants (V1 and V2)

To get an overview of the benefits from both variants, a comparison is shown in Fig. 9. This comparison shows that variant 1 (V1) is suitable, when the goal of the NFC-Bridge is to keep the energy consumption of the source of the embedded system (S2) as low as possible, when an unauthorized access occurs. If the overall energy consumption for an authorized access should be kept low, variant 2 (V2) is a better solution.

IV. CASE STUDY

To find out if the proposed PtNBridge method works in practice, a case study using it to interact with a smart meter is made. The implementation of the PtNBridge supports the two described variants. The implementation is shown in Fig. 10. The smart meter is a reference implementation on an FPGA-Board. To deploy the needed hardware changes

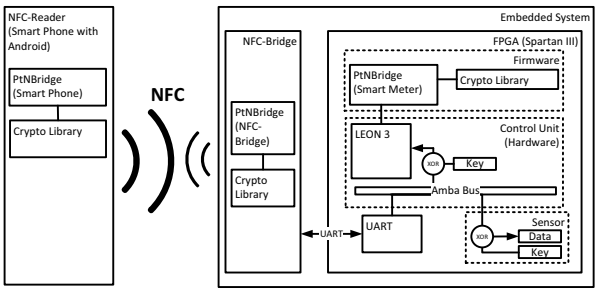


Figure 10. This component model of the implementation of the PtNBridge shows how the proposed solution is deployed into the existing NFC-Bridge system.

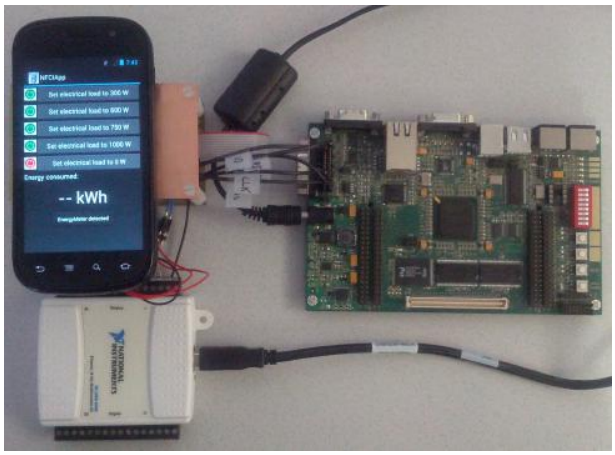


Figure 11. Picture of the prototype built for the case study of using the PtNBridge to interact with a reference implementation of a smart meter.

(XOR bus encryption) a Spartan III FPGA-Board is used. The processor is the Leon 3 with a clock frequency of 30 MHz (the same has been used for the evaluation). This processor is not a low power variant, but is open source and can be modified to create the security modifications for the smart meter reference implementation. As NFC-Reader an Android based Smart Phone (Android 4.2) is used. The sensor module (energy sensor of the smart meter) is a simple counter. The needed cryptography for the NFC-Reader and the embedded system (FPGA) is realized using software based cryptographic libraries. The NFC-Bridge also supports a hardware implementation of the needed cryptographic functions. The user interface on the smart phone is an Android application. It periodically fetches the sensor value and displays it. All the communication paths are encrypted using AES and ECC with the curve secp160r1. A picture of the prototype and the used measurement setup is shown in Fig. 11. The existing NFC-Bridge has been modified to support the two variants to secure the system.

V. Conclusion

NFC-Bridges can ease our lives. As shown in the case study, we can read the daily energy consumption of the household by simply holding the smart phone against the smart meter. Without the integration of security, those applications will not be used because trust is lost. To gain this trust, we have to secure the whole communication path and not only parts of it. Furthermore, these applications become useless, if the smart phone needs to be recharged, after a few interactions with NFC-Bridges.

This publication shows that it is possible to secure the whole communication path using ECC and AES and an XOR approach. Using security, without considering the power consumption, can lead to a great energy drain. In our case the most energy hungry variant needed 3.5 times more energy compared to the lowest. The power-considerations can be split into three factors. The first factor is the strength of security. The more strength, the better is the system secured, but the more energy is consumed. The second factor is the used variant to secure the whole communication. We showed two variants, which provide the same level of security. In our evaluation variant 1 needed 141% more energy than variant 2. The third factor is the importance to know the goal of saving energy. If the goal is to block unauthorized users from wasting energy from the embedded system, the proposed variant 2 can save up to 96% energy compared to variant 1 (for our setup).

In the future work, we plan to combine both proposed variants 1 and 2, to create an even more power-aware and secure system. Furthermore, the security strength of 80 is nowadays not sufficient anymore. Therefore, we plan to use stronger algorithms.

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, 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 *Wireless and Mobile Computing, Networking and Communications (WiMob), 2012 IEEE 8th International Conference on*, 2012, pp. 261–267.

[2] E. Haselsteiner and K. Breitfus, “Security in near field communication (nfc) strengths and weaknesses,” *Semiconductors*, vol. 11, no. 71, 2006.

[3] G. Madlmayr, J. Langer, C. Kantner, and J. Scharinger, “Nfc devices: Security and privacy,” in *Availability, Reliability and Security, 2008. ARES 08. Third International Conference on*, 2008, pp. 642–647.

[4] C.-H. Jiang, H.-L. Li, Y.-J. Huang, and W.-C. Lin, “Mutual authentication architecture in wireless sensor networks,” in *Microelectronics and Electronics (PrimeAsia), 2010 Asia Pacific Conference on Postgraduate Research in*, 2010, pp. 291–294.

[5] M. O”Neill and M. J. B. Robshaw, “Low-cost digital signature architecture suitable for radio frequency identification tags,” *Computers Digital Techniques, IET*, vol. 4, no. 1, pp. 14–26, 2009.

[6] H. Aigner, H. Bock, M. Hütter, and J. Wolkerstorfer, “A low-cost ecc coprocessor for smartcards,” in *Cryptographic Hardware and Embedded Systems - CHES 2004*, ser. Lecture Notes in Computer Science, M. Joye and J.-J. Quisquater, Eds. Springer Berlin Heidelberg, 2004, vol. 3156, pp. 107–118.

[7] W. B. W. P. Elaine Barker, William Barker and M. Smid, in *Recommendation for Key Management Ű Part 1: General(Revision 3)*, 2012.

[8] D. Hwang, P. Schaumont, K. Tiri, and I. Verbauwhede, "Securing embedded systems," *Security Privacy, IEEE*, vol. 4, no. 2, pp. 40–49, 2006.

[9] S. Ravi, A. Raghunathan, P. Kocher, and S. Hattangady, "Security in embedded systems: Design challenges," *ACM Trans. Embed. Comput. Syst.*, vol. 3, no. 3, pp. 461–491, Aug. 2004. [Online]. Available: http://doi.acm.org/10.1145/1015047.1015049

[10] T. Eisenbarth and S. Kumar, "A survey of lightweight-cryptography implementations," *Design Test of Computers, IEEE*, vol. 24, no. 6, pp. 522–533, 2007.

[11] M. Potkonjak, S. Meguerdichian, and J. Wong, "Trusted sensors and remote sensing," in *Sensors, 2010 IEEE*, 2010, pp. 1104–1107.

[12] J. Yang, L. Gao, and Y. Zhang, "Improving memory encryption performance in secure processors," *Computers, IEEE Transactions on*, vol. 54, no. 5, pp. 630–640, 2005.

[13] E. Wenger and J. Grossschädl, "An 8-bit AVR-Based Elliptic Curve Cryptographic RISC Processor for the Internet of Things," in *Microarchitecture Workshops (MICROW), 2012 45th Annual IEEE/ACM International Symposium on*, 2012, pp. 39–46.

[14] H. Alrimeih and D. Rakhmatov, "Security-performance tradeoffs in embedded systems using flexible ecc hardware," *Design Test of Computers, IEEE*, vol. 24, no. 6, pp. 556–569, 2007.

[15] L. Caviglione, A. Merlo, and M. Migliardi, "What is green security?" in *Information Assurance and Security (IAS), 2011 7th International Conference on*, 2011, pp. 366–371.

[16] A. Wander, N. Gura, H. Eberle, V. Gupta, and S. Shantz, "Energy analysis of public-key cryptography for wireless sensor networks," in *Pervasive Computing and Communications, 2005. PerCom 2005. Third IEEE International Conference on*, 2005, pp. 324–328.

[17] P. Trakadas, T. Zahariadis, H. C. Leligou, S. Voliotis, and K. Papadopoulos, "Analyzing energy and time overhead of security mechanisms in wireless sensor networks," in *Systems, Signals and Image Processing, 2008. IWSSIP 2008. 15th International Conference on*, 2008, pp. 137–140.

[18] G. Bertoni, L. Breveglieri, and M. Venturi, "Power aware design of an elliptic curve coprocessor for 8 bit platforms," in *Pervasive Computing and Communications Workshops, 2006. PerCom Workshops 2006. Fourth Annual IEEE International Conference on*, 2006, pp. 5 pp.–341.

[19] W. Jiang, Z. Guo, Y. Ma, and N. Sang, "Research on cryptographic algorithms for embedded real-time systems: A perspective of measurement-based analysis," in *High Performance Computing and Communication 2012 IEEE 9th International Conference on Embedded Software and Systems (HPCC-ICESS), 2012 IEEE 14th International Conference on*, 2012, pp. 1495–1501.

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

Introduction of design pattern(s) for power-management in embedded systems

MANUEL MENGHIN and NORBERT DRUML and CHRISTOPHER PRESCHERN and CHRISTIAN STEGER and REINHOLD WEISS, Graz University of Technology

HOLGER BOCK and JOSEF HAID, Infineon Technologies Austria AG

Resource management is important because of the rising diversity and the resource constraints, like energy, of embedded systems. Energy-constraints are especially challenging in mobile systems like smart phones. A solution to deal with these constraints are power-management techniques that are often only general design principles. Consequently, implementation is often done by experts only. One common approach is to optimize hardware and software until the energy-constraints are fulfilled. This leads to resulting solutions working only for one specific use case. So why shouldn't we mine and use design patterns for power-management in embedded systems from these individual solutions. In contribution, we extended the dynamics and consequence section of the pattern structure to be able to describe the impact to the power consumption. We used the extended structure and mined an example pattern called *Energy Valve* as a start for mining others.

Categories and Subject Descriptors: Software and its engineering [**Software organization and properties**]: Contextual software domains—*Power management*; Software and its engineering [**Software creation and management**]: Software development process management—*Design patterns*

Additional Key Words and Phrases: Hardware design, resource management

ACM Reference Format:

Menghin, M. and Druml, N. and Preschern, C. and Steger, C. and Weiss, R. and Bock, H. and Haid, J. 2013. Introduction of design pattern(s) for power-management in embedded systems. ACM Trans. Appl. Percept. 2, 3, Article 1 (May 2013), 12 pages. DOI = 10.1145/0000000.0000000 http://doi.acm.org/10.1145/0000000.0000000

1. INTRODUCTION

In the last years the number of embedded systems as part of huge decentralized networks grew. Examples are smart phones, small sensors, or wireless identification cards, as interconnected nodes. As presented by [Sangiovanni-Vincentelli 2012], these embedded systems will become even smaller and he predicts that the number of these systems will rise to over 1000 per person by the year 2025. The desire to pack more and more functionality into one embedded system under the pressure of costs makes this to a great challenge for the designers of such systems. Additionally, these designers also have to consider the constrained resources of the embedded system in their design. An example is the constraint of available energy in mobile battery driven systems. Therefore, they have to be energy efficient or at

DOI 10.1145/0000000.0000000 http://doi.acm.org/10.1145/0000000.0000000

least efficient enough to satisfy the user's expectancy of a certain time before the mobile system needs to recharge. One concrete example is a smart phone with enabled Near Field Communication (NFC). With NFC you are able to pay, or to use your phone to get information from a NFC-Tag like a smart poster. To deal with this energy-constraint, power-management techniques are implemented. Some of them are custom solutions, which are designed and implemented after the actual implementation to "fix" a violation of energy requirements. There are several general design principles available, how to implement power-management in embedded systems like the one of [Benini et al. 2000].

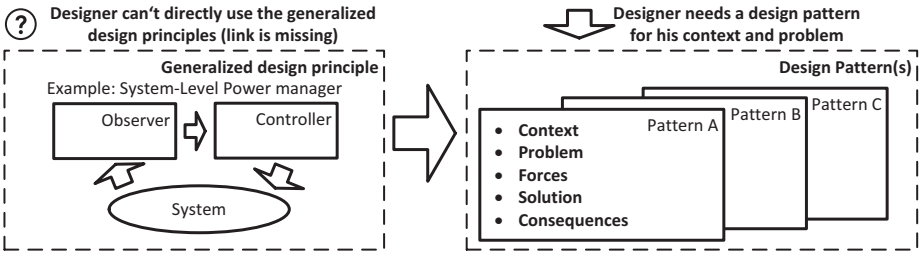


Fig. 1. This figure shows the concept of using the generalized design principles for power-management, like from [Benini et al. 2000], as basis for design patterns of embedded systems. The design patterns are proposed to be the missing link between the general principles, and the usable design for a specific context and problem.

The problem is, that the designer needs to know the consequences in terms of the energy consumption according to a certain context and problem (as shown in Fig. 1). This specific form has to be like a tool to find a certain solution to a problem. It also should not be too general, because then the effort to integrate them into the design is too great, and the risk of making mistakes through the additional design effort rises. Nevertheless, general design principles should not be underestimated, because they are basis for design patterns to specific problems. Therefore, this paper makes following contribution:

—We extended dynamics and consequences section of the pattern structure described in [Kircher and Jain 2004] to be able to express the impact to the energy consumption when using the pattern.

—We present the $Energy\ Valve$ pattern as an example power-management pattern.

2. RELATED WORK

This section gives a four part overview of the related work to this topic. In the first part, it is described how power-management is currently applied to the design. The second part gives an overview how patterns are used to design systems. In the third part known publications are shown, which aim for design patterns for hardware. In the fourth part existing works of using design patterns for power-management are presented.

2.1 Applying power-management to the system's design

There are several techniques to deal with the challenge of system based power-management. For example, [Unsal and Koren 2003] describe system-level power-aware design techniques. One design technique is voltage and frequency scaling, which can be used to decrease the power consumption of SoC's (System on Chip). Another approach by [Chatterjee et al. 2006] focuses on an evaluation strategy to create a power-aware design. In this approach the power-consumption of the system is transformed into the abstract form of power-states to analyze the behavior of the design. An additional approach to optimize the system, is to create a power profile of the system for analysis. The work of [Arpinen et al.

2012] present an extension of Modeling and Analysis of Real-time and Embedded systems (MARTE) for dynamic power management. The proposed extended profile consists of power states, mapped to their hardware components and grouped into power configurations. There are also design recommendations for power-management, like published by [Benini et al. 2000]. Other techniques to aim for a power-aware design are shown by [Bachmann et al. 2010] and [Druml et al. 2012b], which describe the flow how to analyze a system's power-consumption with characterization techniques and to optimize the system using an emulation of the characterized system. These publications are all aiming to transfer the experience in terms of power-management like design patterns.

2.2 The usage of patterns in designing systems

Patterns provide a solution to a certain context and problem. The difference to standard publications is, that a pattern is written to match a certain structure as presented by [Winn and Calder 2002]. They propose nine different characteristics, which make out a pattern. Another paper also supports the statement that patterns are a way to effectively pass designing experiences to other engineers, which is a key factor in effective engineering. In [Kircher and Jain 2004], the usage of patterns for resource management is shown, which is similar to the challenge of power-management, because power is system's resource. The patterns also apply to different levels of abstraction and also can be used for hardware designs as shown by [Grone 2006]. Another work from [Weir and Noble 2004] present software design patterns for constraint hardware, for example a small memory.

2.3 Patterns considering the hardware design in the system

Design patterns are not restricted to software applications, they can also be used in hardware design. [Rincon et al. 2005] show, that hardware IP's (Intellectual Property; stands for a reusable hardware component) are effective but are also specific for one implementation and platform. They show a way, how to translate these IP's into a design pattern for hardware, for example into a description usable for SystemC, which is a commonly used hardware description language. Also [Damasevicius et al. 2003] propose a design pattern to create a wrapper to convert hardware IP's to hardware design patterns. These patterns can then be used to generate specific hardware IP's, which fit for the desired design as shown by [Meng et al. 2008]. Furthermore, a way to solve interoperability between SystemC, and the formal description of the design is shown by [Charest et al. 2004]. This also leads to a more efficient verification of such designs using design patterns as shown by [Déharbe and Medeiros 2006] using SystemC. The pattern itself is already verified and for that only the other parts of the design have to be verified. Another aspect by [Damasevicius and Stuikys 2004] shows, that using design patterns to create IP cores can be very effective. They also presented, that the power overhead using design patterns can be significant, like up to 600% more power consumption as shown by he paper. Therefore, this disadavantage has to be considered, when dealing with non-functional properties of the system.

2.4 Using design patterns for system based power-management

The possible drawback of design patterns in terms of performance loss is also investigated by [Mani et al. 2011]. They emphasis the need of considering the overhead, when using design patterns for power-management. [Sahin et al. 2012] map the power-profile to design artifacts (patterns) to investigate the power consumption in the usage of design patterns and to decide if the beneficial effect is greater than the overhead. The paper from [Damaševičius et al. 2003] shows the benefit of using design patterns, that the power-consumption can be reduced through the optimized design itself, including the resulting overhead through using the pattern. A practical example is the power gating of wires as design-pattern-like description to use it to save power in SoC's as shown by [Heyrman et al. 2010]. This is a good example of a hardware pattern to reduce the power consumption.

3. EXTENSION TO THE PATTERN STRUCTURE FOR POWER-MANAGEMENT

The used pattern structure is the based on [Kircher and Jain 2004], and addresses four questions.

(1) *How do i get the pattern's benefits and liabilities related to the energy consumption?*
This information is added to the consequences section. The benefits can be found under the key term "Benefit on energy consumption". To quantify the benefit, the energy consumption without ($E_{original}$) and with ($E_{solution}$) using the pattern's solution has to be evaluated. The benefit is the subtraction of these energy values as shown in (1).

$$E_{saved} = E_{solution} - E_{original} \tag{1}$$

The liabilities to energy consumption are described under "Liability on energy consumption". A liability example is the emerging overhead by implementing the needed algorithms for power-management. The user of this pattern should be informed about this form of liabilities.

(2) *How do i evaluate energy consumption of the system?*
This is addressed by defining the resulting power profile according the pattern's solution. This profile is based on the work of [Arpinen et al. 2012]. They extended MARTE for modeling dynamic power management. In this work the power state machine, the hardware components and the hardware power configuration is included in the power profile. This power profile is separated into the described components in the structure section of the pattern as shown in Figure 2. Some of the used parameters in this profile are not defined and need input by the user of the pattern. They are summarized in a separate block of the stereotype "Parameters" called "Input". A description is given how to get the values of these parameters. After providing the values of these parameters, the power profile is complete. There is another question to be answered.

(3) *How do i get energy consumption with and without the pattern's solution?*
The power modes with and without using the pattern's solution are added to the consequences section. The modes are shown in a state diagram including the paths with and without using the pattern, which are indicated using guards "with $< patternName >$" and "without $< patternName >$". They can be used together with the complete power profile to get both energy consumptions.

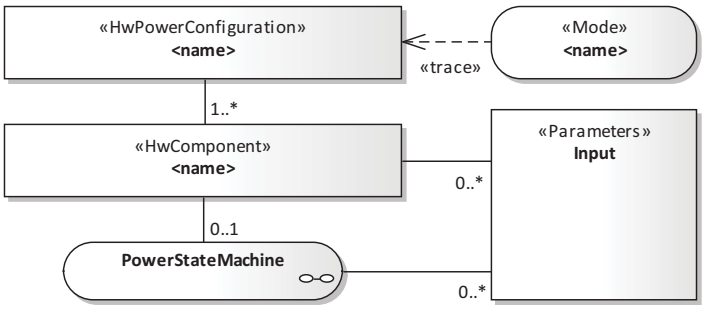


Fig. 2. This figure shows the structure of the power profile and the power modes based on [Arpinen et al. 2012].

(4) *How can i get the impact to the saved energy consumption, when i can't complete the power profile?*
Reference values for the impact to the energy consumption, including the reference with more detailed information, are given. The reference values are linked to a certain domain, like the usage of the design pattern for NFC. This is added to the consequences section and indicated by "Known impact to energy consumption".

4. THE ENERGY VALVE PATTERN

This pattern is written for the designer of an embedded system. The $Energy\ Valve$ Pattern can be used, when the transfered energy from a provider to a consumer over a lossy path should automatically be controlled to save energy on the side of the provider.

4.1 Example

Consider a system consisting of a NFC-enabled smart phone (provider), which is used to get information from a smart poster (consumer). This poster does not have any energy source. Therefore, the smart phone wirelessly transfers electrical energy to a poster. The smart phone is able to control the transferred energy to the poster. The wireless energy transmission is very lossy. The poster only needs a certain amount of energy to transmit the wanted information. The rest of the transferred energy is lost (sink). Because of the limited amount of available energy on the smart phone, this lost energy should be kept as small as possible.

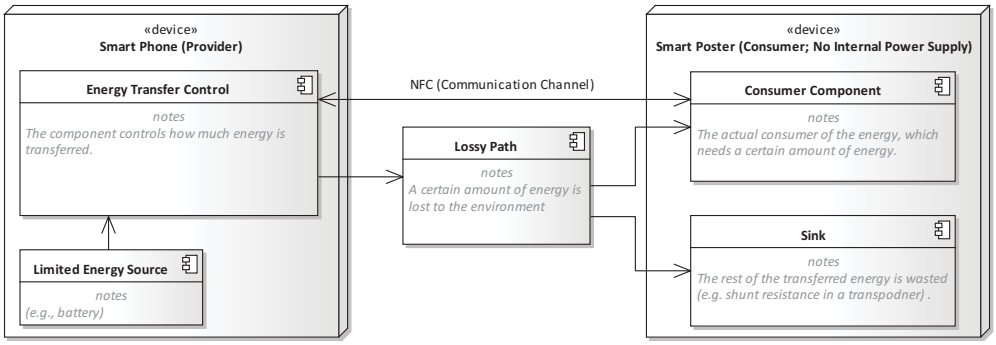


Fig. 3. This deployment diagram shows an example, where the $Energy\ Valve$ pattern can be used.

4.2 Context

The system consists of a provider and a consumer, where the provided energy of the attached consumer can be controlled during the communication between the provider and the consumer to reduce the energy consumption of the provider. The provider can only transfer energy over a lossy path and has a communication channel available to the consumer.

4.3 Problem

Through the limitation of the available energy the transferred energy to the consumer should be the same as the needed one. The rest of the transferred energy is lost (sink). The provider does not know how much energy the consumer needs. How can the provider get the information how much energy needs to be transfered? Following forces require resolution:

Simplicity. The solution must not be too complex, to avoid that the overhead is too big to save energy. The solution addresses operations with a certain level of complexity, because the simpler the operation gets the smaller the impact to the saved energy is.

Availability. The consumer's availability, like being properly supplied, should not be affected by the solution.

Transparency. The solution should be loosely coupled through a defined interface to the rest of the system.

Stability. The solution must not force the system into an unstable state, like an undersupply or an oscillating control loop.

Energy reduction. The solution should reduce the overall energy consumption.

4.4 Solution

Provide a control unit on the side of the energy provider, which uses the communication channel to the consumer as input to regulate the energy transfer over the lossy path. The control unit request the current state of the consumer, what operation the system wants to perform, and evaluates the correct amount of energy to transfer. This evaluation uses a specified rule set suitable for the specific domain. This evaluation is done before the actual operation of the system begins (setup phase).

4.5 Structure

The structure of the *Energy Valve* pattern including the components and their interrelationship is shown in Fig. 4:

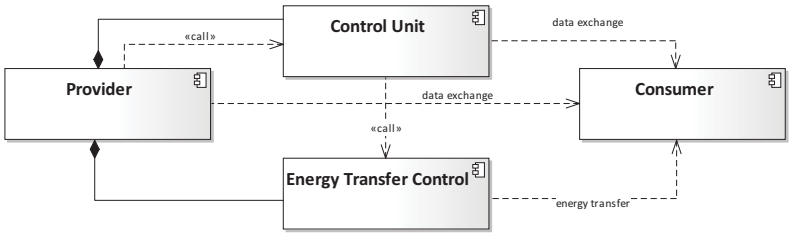


Fig. 4. This figure shows the interrelationship between the components.

The class-responsibility-collaboration (CRC) cards are shown in Fig. 5.

Component **Provider**	Collaborator
Responsibility • Provides the energy for the system • Provides information of the operation the system wants to perform	• Control Unit • Energy Transfer Control

Component **Consumer**	Collaborator
Responsibility • Consumes the transfered energy • Provides energy state for the control unit	• Control Unit

Component **Control Unit**	Collaborator
Responsibility • Evaluates the needed energy to be transferred • Controls the energy transfer control	• Energy Transfer Control

Component **Energy Transfer Control**	Collaborator
Responsibility • Sets the amount of power to transfer • Transfers the Power to the energy consumer	• Consumer

Fig. 5. This figure shows the CRC cards of the participants from the solution.

4.6 Dynamics

The interaction in the *Energy Valve* pattern is shown in Fig. 6.

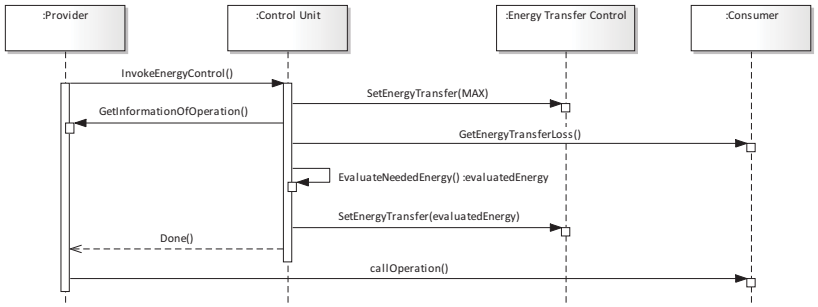


Fig. 6. This sequence diagram shows how the design pattern deals with the scenario.

Scenario. In the setup phase, the provider invokes the control unit. The control unit sets the energy transfer to the maximum to ensure that a communication is possible. The control unit now collects the required information of the operation to call, and the expected energy loss. The expected energy loss is estimated by using the communication path to the consumer. The information of the called operation and the expected energy loss are now evaluated by the control unit to get the necessary amount of energy to transfer. This value is then used to set the energy transfer. The control unit now signalizes, that the energy transfer is now scaled accordingly. The energy provider can now call the operation without wasting energy. The power profile related to the pattern's solution, structure and dynamics is shown in Fig. 7.

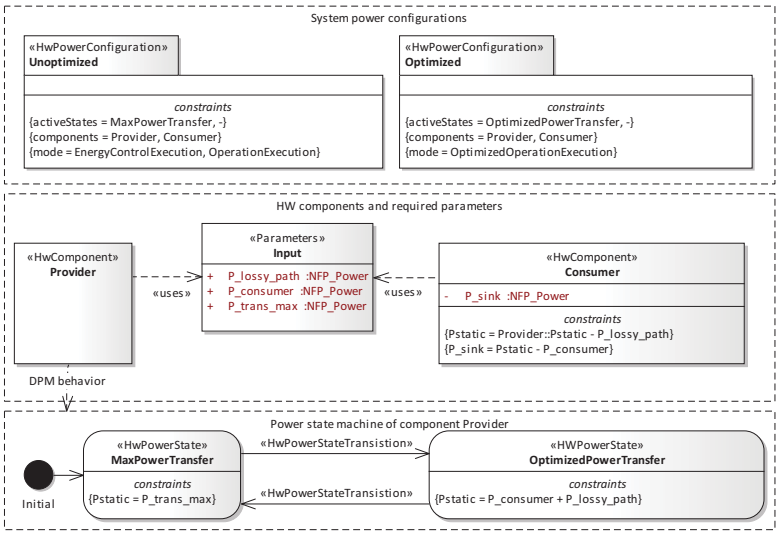


Fig. 7. This figure shows the power profile of the system needed to evaluate the pattern's impact to the energy consumption.

The power profile shows the needed system's profile to evaluate the energy consumption of the pattern's solution. The profile exists of one power state machine describing the possible states of the provider. The other components are described with one static power value. To complete the power profile several parameters are needed to be included. One parameter is the maximum transmission power (P_{trans_max}). Another is the power consumption of the consumer $P_{consumer}$. This power value does not include the consumption of the sink. The third parameter is P_{lossy_path}, which defines the lost power through the transmission path. This can be expressed through the transmission function, which is domain specific, like using Biot-Savar for NFC described in [Finkenzeller 2003].

4.7 Implementation

There are four steps involved in defining the $Energy\ Valve$ pattern:

(1) Implement a method for the control unit to get the energy consumption for the operation to call, according to known information. This information can be implemented using a power characterization method [Bachmann et al. 2010] during design phase and can be made available.
(2) Implement a method for the control unit to determine the energy transfer loss. A possible method is to scale down the transferred energy to a level, where the consumer stops to respond. Other ways to implement this, are measuring the energy consumption of the consumer and transferring this value to the control unit.
(3) Implement the evaluation procedure for the control unit. It calculates the needed energy transmission according the both described methods. It is also possible to add additional rules to increase the stability of the $Energy\ Valve$ pattern, like setting the energy transmission higher than needed, to avoid an undersupply invoked by possible distortions.
(4) Adapt the setup process of the energy producer to invoke the control unit before calling the actual operation. This should be done as transparent as possible to avoid influencing the functional implementation.

4.8 Example Resolved

Consider the example in which an NFC-System, like in Fig. 8, consumes too much energy and the designer has to find a way to counter that. All the components of the systems themselves are already energy-optimized. By using the $Energy\ Valve$ pattern the consumption can be further reduced. In this

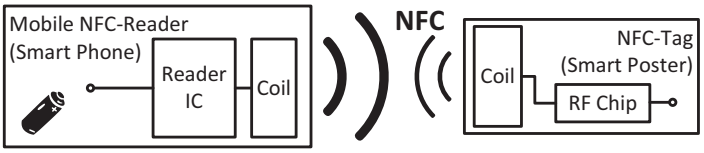


Fig. 8. This figure shows the basic structure of the NFC-System used in the example.

example the control unit is implemented in software. In this implementation, as shown in Algorithm 1, the algorithm uses binary search to adjust the energy transfer of the provider within a discrete scale between 0 up to the maximum power level. The search criteria is the visibility of the consumer. The binary search has the benefit of a reduced and constant search time. The software implementation uses the provided hardware interfaces consisting of an operation to communicate with the smart card (ChkTagAvailable()) and one to control the energy transfer (SetEnergyTransfer()). This energy transfer is controlled via the magnetic field strength of the provider.

ALGORITHM 1: Software part of the implementation of method GetEnergyTransferLoss()

```
fieldStrength = MAX;
SetEnergyTransfer(MAX);
for (stepSize=MAX; !tagfound && stepSize¿0 ; stepSize /= 2) {
  boolean tagFound = ChkTagAvailable();
  if (tagFound && (fieldStrength != 0)) {
    fieldStrength -= stepSize;
    SetEnergyTransfer(fieldStrength);
  } else if (!tagFound && fieldStrength != (numberOfPossibleFieldStrength - 1)) {
    fieldStrength += stepSize;
    SetEnergyTransfer(fieldStrength);
  }
}
```

4.9 Consequences

There are several **benefits** using the $Energy\ Valve$ pattern:

Reusability. The defined interface separates the power-management design from the rest.

Transparency. The pattern is decoupled from the functional implementation.

Stability. The pattern proposes a control sequence (InvokeEnergyControl()), that is executed once. This prevents instabilities.

Benefit on energy consumption. The pattern is able to reduce the energy consumption of the system, even the components themselves are energy-optimized. The saved energy E_{saved} through the usage of the $Energy\ Valve$ pattern can be evaluated using the power state diagram as shown in Fig. 9 following the path with the guard "without EnergyValve" to evaluate $E_{original}$ and "with EnergyValve" to evaluate $E_{solution}$. The diagram uses the power profile described in Fig. 7 as basis. t_{setup} is the time needed for the energy control. $t_{operation}$ is the time needed for the actual operation. $E_{original} - E_{solution}$ defines the resulting benefit.

There are some **liabilities** using the $Energy\ Valve$ pattern:

Dependence. The potential of reducing the energy-consumption through the pattern, depends on the lossy path and the operation to execute. If the provider has to set the energy-transfer to maximum to be able to communicate with the consumer, the potential of saving energy shrinks to zero.

The consumers availability. If more supply is needed during the communication the consumer can get under supplied.

Liability on energy consumption. The design of the pattern includes an overhead through the state "EnergyControlExecution" as shown in Fig. 9. This effects the consumed energy of the system.

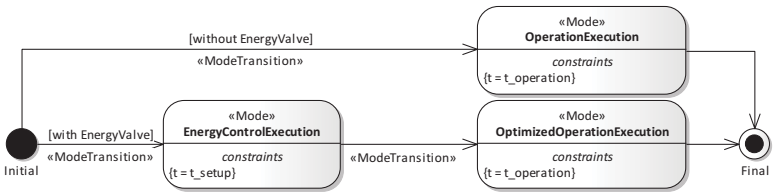


Fig. 9. This figure shows the power state diagram with and without using the pattern's solution.

There is a **known impact to the energy consumption**. The presented reference value for the saved energy can be used to get an approximation for the specified domain.

Domain - NFC. Saved Energy is 43.87% as shown by [Menghin et al. 2012]

4.10 Known Uses

The PTF-Determinator [Menghin et al. 2012]. This approach uses the pattern to reduce the overall energy consumption of an NFC-System consisting of one reader (energy provider) and one transponder (energy consumer). The communication channel is used to find out, if the consumer is properly supplied, through a response to a request, at a certain energy transfer.

Adaptive Field Strength Scaling [Druml et al. 2012a]. This approach also uses the pattern in NFC-Systems. The energy transfer loss is evaluated through a sensor on the consumer side and the information is sent back over the communication channel.

Component-aware dynamic voltage scaling [Hormann et al. 2011]. This approach uses an intelligent voltage converter (energy provider), which communicates to the consumers over a bus, to scale down the supply voltage to a minimum. The lossy path is in this case direct power lines and are in this approach ignored.

Energy-efficient RF source power control [Bicen and Akan 2012]. An RF-power is configured according to the backscatter communication of the passive sensor nodes (energy consumers). This is not a real time approach, but it works according to the principle of the $Energy\ Valve$ pattern.

Radiator. A real world example is the radiator control. The radiator is the energy provider and the person is the energy consumer. The ”communication channel” between the temperature sensor and the radiator control is used to scale the heat transfer (energy transfer) to the person.

5. CONCLUSION

Design patterns for power-management can support designers to use known solutions. The extension of the dynamics and consequences allows a selection of the pattern according to the known energy requirements. The separation of benefits and liabilities in terms of the energy consumption eases the evaluation if energy can be saved by using this design pattern. The included power profile and the power state diagram can be used to model the energy behavior of the system.

The example $Energy\ Valve$ pattern shows a practical example of using this extended structure. This pattern derives from the general design principle called observer-controller power-management technique from [Benini et al. 2000]. The power profile is suitable to estimate the energy consumption of the system. If this is not possible through lack of information, the domain-specific help to decide if this certain pattern is the right one to satisfy the requirements in embedded systems.

6. OUTLOOK

The presented $Energy\ Valve$ pattern is only the beginning. It is planned to mine more patterns for power-management. Furthermore, it is planned to group these pattens to a pattern system. An important future step will be presenting how these design patterns can be used in the design process. This includes how to search for matching patterns, iteratively use them for designing the power-management and how to use the resolved example for the implementation.

ACKNOWLEDGMENTS

We would like to thank our industrial partners Infineon Technologies Austria AG as well as Enso Detego GmbH for their support. Furthermore, 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 FFG 829586. We would also like to thank our shepherd Peter Sommerlad and the workshop group at Europlop 2013 who gave us valuable feedback on this paper.

REFERENCES

ARPINEN, T., SALMINEN, E., HMLINEN, T. D., AND HNNIKINEN, M. 2012. {MARTE} profile extension for modeling dynamic power management of embedded systems. *Journal of Systems Architecture 58,* 5, 209 – 219.

BACHMANN, C., GENSER, A., STEGER, C., WEISS, R., AND HAID, J. 2010. Automated Power Characterization for Run-Time Power Emulation of SoC Designs. In *Digital System Design: Architectures, Methods and Tools (DSD), 2010 13th Euromicro Conference on*. 587 –594.

BENINI, L., BOGLIOLO, A., AND DE MICHELI, G. 2000. A survey of design techniques for system-level dynamic power management. *Very Large Scale Integration (VLSI) Systems, IEEE Transactions on 8,* 3.

BICEN, A. AND AKAN, O. 2012. Energy-efficient rf source power control for opportunistic distributed sensing in wireless passive sensor networks. In *Computers and Communications (ISCC), 2012 IEEE Symposium on*. 000738 –000743.

CHAREST, L., ABOULHAMID, E., AND BOIS, G. 2004. Using design patterns for type unification and introspection in systemc. In *System-on-Chip for Real-Time Applications, 2004.Proceedings. 4th IEEE International Workshop on*. 45 – 50.

CHATTERJEE, S., ROY, S., AND BANDYOPADHYAY, S. 2006. Hop-efficient and power-optimized routing strategy in a decentralized mesh network using directional antenna. In *Parallel and Distributed Computing, 2006. ISPDC '06. The Fifth International Symposium on*. 155 –160.

DAMASEVICIUS, R., MAJAUSKAS, G., AND STUIKYS, V. 2003. Application of design patterns for hardware design. In *Design Automation Conference, 2003. Proceedings*. 48 – 53.

DAMASEVICIUS, R. AND STUIKYS, V. 2004. Application of uml for hardware design based on design process model. In *Proceedings of the 2004 Asia and South Pacific Design Automation Conference*. ASP-DAC '04. IEEE Press, Piscataway, NJ, USA, 244–249.

DAMAŠEVIČIUS, R., MAJAUSKAS, G., AND ŠTUIKYS, V. 2003. Application of design patterns for hardware design. In *Proceedings of the 40th annual Design Automation Conference*. DAC '03. ACM, New York, NY, USA, 48–53.

DÉHARBE, D. AND MEDEIROS, S. 2006. Aspect-oriented design in systemc: implementation and applications. In *Proceedings of the 19th annual symposium on Integrated circuits and systems design*. SBCCI '06. ACM, New York, NY, USA, 119–124.

DRUML, N., MENGHIN, M., STEGER, C., WEISS, R., GENSER, A., BOCK, H., AND HAID, J. 2012a. Adaptive field strength scaling: A power optimization technique for contactless reader / smart card systems. In *Digital System Design (DSD), 2012 15th Euromicro Conference on*. 616 –623.

DRUML, N., STEGER, C., WEISS, R., GENSER, A., AND HAID, J. 2012b. Estimation based power and supply voltage management for future rf-powered multi-core smart cards. In *Design, Automation Test in Europe Conference Exhibition (DATE), 2012*. 358 –363.

FINKENZELLER, K. 2003. *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification* 2 Ed. John Wiley & Sons, Inc., New York, NY, USA.

GRONE, B. 2006. Conceptual patterns. In *Engineering of Computer Based Systems, 2006. ECBS 2006. 13th Annual IEEE International Symposium and Workshop on*. 6 pp. –246.

HEYRMAN, K., PAPANIKOLAOU, A., CATTHOOR, F., VEELAERT, P., AND PHILIPS, W. 2010. Control for power gating of wires. *Very Large Scale Integration (VLSI) Systems, IEEE Transactions on 18,* 9, 1287 –1300.

HORMANN, L., GLATZ, P., STEGER, C., AND WEISS, R. 2011. Evaluation of component-aware dynamic voltage scaling for mobile devices and wireless sensor networks. In *World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2011 IEEE International Symposium on a*.

KIRCHER, M. AND JAIN, P. 2004. *Pattern-Oriented Software Architecture Volume 3: Patterns for Resource Management*. Wiley.

MANI, N., PETRIU, D., AND WOODSIDE, M. 2011. Studying the impact of design patterns on the performance analysis of service oriented architecture. In *Software Engineering and Advanced Applications (SEAA), 2011 37th EUROMICRO Conference on*. 12 –19.

MENG, Z., MINGLUN, G., AND XIAOSONG, H. 2008. Design method for parameterized ip generator using structural and creational design patterns. In *Anti-counterfeiting, Security and Identification, 2008. ASID 2008. 2nd International Conference on*. 378 –381.

MENGHIN, M., DRUML, N., STEGER, C., WEISS, R., BOCK, H., AND HAID, J. 2012. The PTF-Determinator: A Run-Time Method Used to Save Energy in NFC-Systems. In *RFID Technology (EURASIP RFID), 2012 Fourth International EURASIP Workshop on*.

RINCON, F., MOYA, F., BARBA, J., AND LOPEZ, J. 2005. Model reuse through hardware design patterns. In *Design, Automation and Test in Europe, 2005. Proceedings*. 324 – 329 Vol. 1.

SAHIN, C., CAYCI, F., GUTIERREZ, I., CLAUSE, J., KIAMILEV, F., POLLOCK, L., AND WINBLADH, K. 2012. Initial explorations on design pattern energy usage. In *Green and Sustainable Software (GREENS), 2012 First International Workshop on*. 55 –61.

SANGIOVANNI-VINCENTELLI, A. 2012. Cyber-Physical System Design Challenges and Solutions: Taming Dr. Frankenstein. *Nano-Tera/ARTIST Summer School on Embedded System Design 2012*.

UNSAL, O. AND KOREN, I. 2003. System-level power-aware design techniques in real-time systems. *Proceedings of the IEEE 91,* 7.

WEIR, C. AND NOBLE, J. 2004. *Thinking Small - The Processes for Creating Small Memory Software*.

WINN, T. AND CALDER, P. 2002. Is this a pattern? *Software, IEEE 19,* 1, 59 –66.

Development Framework for Model Driven Architecture to Accomplish Power-Aware Embedded Systems

– Omitted for blinded review. –

***Abstract*—Developing an embedded system today means integrating a bundle of features into a constrained and complex system. Examples are Near Field Communication (NFC) handsets like smart phones, which will hit the 1.2billion mark in 2017. Model Driven Architecture (MDA) is an approach to handle this complexity. Challenges in MDA are the verification of power-requirements across the development phases and to find the suitable abstraction for the power models for higher abstraction levels. Therefore, we propose a framework for MDA to support cross-verification of these requirements. We implemented this framework and made a case study of developing a power-aware NFC-System. The case study shows that the framework allows a power-verification with an accuracy of 10%.**

***Keywords*—System-level design, power system modeling, energy management, Radiofrequency identification**

I. Introduction

Embedded system design is increasing in complexity. One reason for this is the demand to integrate additional features such as NFC (Near Field Communication) for smart phones. In case of NFC the number of shipped handsets is predicted to hit the 1.2billion mark in 2017 [12]. Integrating this into an already complex system is a great challenge for developers. To deal with this challenges, techniques like simulation (63%), modeling (36%), virtual prototyping (32%), and graphical system design (31%) win on importance [5]. One approach for combining these techniques is Model Driven Architecture (MDA). MDA uses model-based views on the system like the Computional Independent Model (CIM) for use cases and requirements, the Platform Independent Model (PIM) for design, and the Platform Specific Model (PSM) for platform specific design (as shown in Fig. 1). These views enable a development with multiple levels of abstraction to make it easier to keep track of the system. Additionally, these levels of abstractions allow to condense the complex system to perform the verification of the system with assessable effort. For example, the NFC-System to investigate can be condensed to its main interface for a high level verification.

One important type of requirements for mobile embedded systems are non-functional ones for power and energy. Considering these requirements earlier in the development process the better avoids costly redesigns in a later development stage. The common approach to verify non-functional requirements is through the use of design and exploration tools. This can be done on several levels of abstraction (e.g., SystemC transaction-level model, VHDL design). This step is commonly done manually, and therefore time consuming. Additionally finding the right abstraction for this verification and obtaining the required power model is challenging. An example is obtaining the power model of a wireless power transmission for NFC-Systems for a high level model [15]. This power model has to be a compromise between accuracy and platform specific commitments. For these two reasons, this step is often skipped during the early development phases, and an evaluation is performed after the system has already been implemented. However, a late evaluation bears the risk of a major redesign. After the design is finished, about 38% of the development time is invested in simulation, testing, debugging, and prototyping, and at worst would be lost [5]. This publication demonstrates a framework for MDA which enable the verification of power-requirements during early design stages, and presents the implementation of the framework suitable to develop NFC-Systems. The following steps, as highlighted in Fig. 1, are presented:

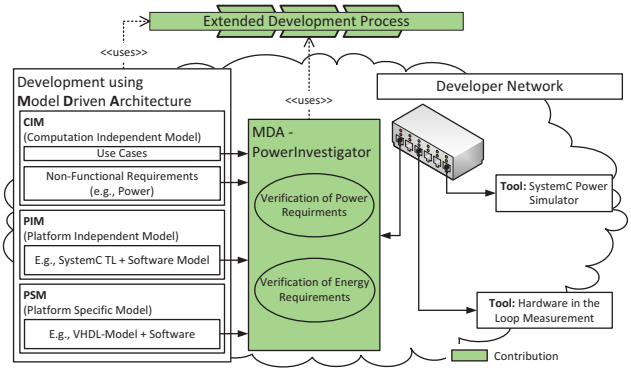


Fig. 1. Overview of the development using MDA, the proposed extension and the MDA-PowerInvestigator framework in order to realize power-aware embedded systems.

- We demonstrate the process extension required for the MDA framework to verify power and energy requirements across the development phases.
- In order to apply the proposed process, we implemented the framework called MDA-PowerInvestigator.
- In a case study we developed an NFC-System in order to investigate the accuracy and usability of the framework.

This paper is divided into four parts. Part one shows the work related to this topic. The second part describes the proposed development process and the implemented framework. The case study in part three evaluates the practical use. Part four concludes this work.

II. Related Work

A. Using MDA to develop embedded systems

Riccobene et al. demonstrate how MDA and SystemC can be combined to design System on Chips (SoCs) [19]. The approach of [11] shows the integration of SystemC, SpecC and ImpulseC into the MDA development process. Sequence diagrams, which graphically describe the execution order, can be used as input for verification [10]. An approach from [23] focuses on the topic of design space exploration in combination with MDA. An advantage of the model based approach emerges through combination with simulation. Chong et al. describe an approach for integrating hardware in the loop simulation into the MDA flow [6]. [18] shows model based approaches which either use System Modeling Language (SysML) to describe the functionality, or Modeling and Analysis of Real-time and Embedded systems (MARTE) in order to describe non-functional properties of the embedded system.

B. Non-functional requirements in MDA

It is possible to specify functional requirements of the system (CIM). Zhu et al. analyzed the usage of non-functional requirements in Model Driven Development (MDD) and emphasized the challenge of integrating the requirements into a single MDD paradigm [24]. Cortellessa et al. present a framework for MDA in order to include and verify non-functional requirements such as performance [8]. Verifying non-functional requirements is difficult during the early design stages. Dhouib et al. describe AADL (Architecture Analysis & Design Language) modeling of embedded systems used for power estimation in MDA [9]. Saadatmand et al. discuss how MDA and estimation tools can be combined to create power-aware systems [20].

C. Tools and models for power-evaluation

Power evaluation tools are needed to analyze the design or implementation of the system under development. Conti et al. propose an extension of the SystemC framework in order to evaluate the power consumption of the system [7]. Lorenz et al. show another approach for SystemC power-simulation [14]. The publication of [22] describes the PK tool, which defines a power state-machine for every module. Another approach from [2] describes a run-time power emulation of SoC. The result of the evaluation of a system can be used to characterize the power behavior of a system, but we need a represtation to describe the behavior according to this characterization. Especially for high level power evaluations, SystemC Transaction Level Models (TLM) are suiteable. In the work of [16] a methodology for power estimation on transaction level is presented, and the estimation errors are shown for different application scenarios. [13] demonstrate how to model DVFS architectures based on Network-on-Chip (NoC) in SystemC TLM, and achieved a relative error less than 4%. They also described the design of the used power unit. Article [1] shows an extension of MARTE for describing power profiles. This extension also uses power state machines, but uses the standardized form of MARTE. The tool from [3] called *DIPLODOCUS* based on *TTool*, which is a toolkit for UML and SysML, is able to simulate and formally verify SoC models by using power state machines.

The related work presented covers research fields needed for this work. However, it lacks in combining these to one process for power verification across the development phases.

III. Method

In this section the verification framework for MDA is presented, which is divided into the description of the development process extension and implementation called MDA-PowerInvestigator. Finally the verification setup for NFC-Systems using the implemented MDA-PowerInvestigator is presented.

A. Proposed development process extension

Our extended development process uses parts of the risk-driven iterative development process shown in [21] and integrates the concept of MDA into this process, as shown in Fig. 3. This process includes replacing the system model and design model with the PIM and the implementation model with the PSM. The requirements are part of the CIM. Our extension mainly focuses on the models used for MDA, and

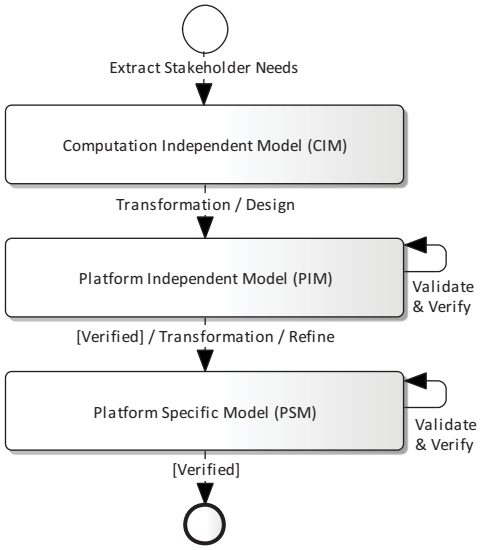


Fig. 3. Overview of the development process based on the risk-driven iterative development process shown by [21] and the MDA guideline.

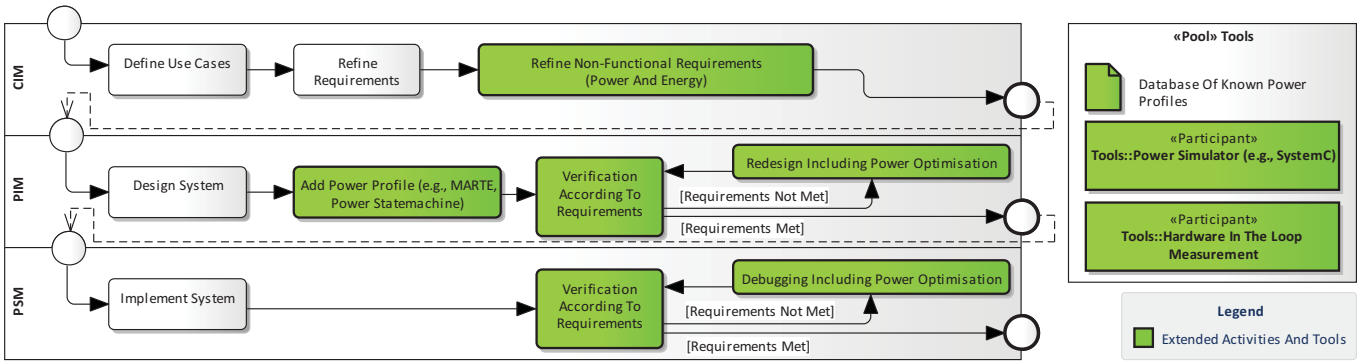


Fig. 2. Extended development process based on MDA focused on the verification of the requirements for power-awareness in the platform independent model (PIM) and platform specific model (PSM).

not on the structure of the development process. As shown in Fig. 2, the extended development process is separated into the three models.

Computation Independent Model (CIM): In this model, the use cases and requirements are defined. The use cases are extracted from the requirements of the stakeholder. Use cases are usage scenarios for the system, and can be defined as sequence diagrams. These use cases are applied in order to evaluate the power and energy consumption in the verifications of the PIM and PSM, which are then described in detail later on. The requirements are refined from these use cases. During this development phase, non-functional requirements for power and energy are also refined. These requirements are needed for verification in the PIM and PSM. Power requirements can be expressed through values and equations. This makes automatic checks possible in order to see whether this requirement has been fulfilled. Examples of these definitions are the maximum allowed power consumption for a certain use case. The CIM is then transformed into the PIM.

Platform Independent Model (PIM): In the PIM, the system is designed according to the use cases and requirements. Non-functional requirements need additional information in order to be verified. One solution is to add power profiles to the functional model. This can either be done using an extension of MARTE [1], or through the use of power state machines [4]. The data for these profiles can be provided by characterization methods such as [2]. These methods use already existing modules and perform a gate-level power simulation in order to characterize the entire module. Existing modules are used in many developments (e.g., a new product variant from an existing platform), so we can assume that power profiles are already available.

Once the power profile has been added, the non-functional requirement can be verified using a power simulator such as SystemC [17]. These used a multi-layer model, which returns cycle accurate power and energy-values according to the control signals of the functional model. The defined use cases represent the execution sequence, and are used for the simulation in order to get the power and energy consumption. This verification procedure allows multiple use cases. If the non-functional requirements are not met, a redesign with power optimizations has to be made. The PIM is considered as verified, when all requirements have been met. The PIM is then transformed into the PSM.

Platform Specific Model (PSM): The functional design is transformed into a platform specific implementation, and the power profiles are no longer needed. As in the PIM, the use cases and refined requirements are used for verification. The implemented system needs a test interface in order to execute the sequences for the use case. A hardware in the loop (HIL) measurement can be used to verify the implementation. In the case of a software implementation, an existing platform can be used for verification. Otherwise the implemented hardware has to be available and integrated into the HIL. If the hardware is not available yet, power emulation as described in [2] can be used in order to verify the non-functional properties. Power emulation combines the functional implementation and a power model in an FPGA in order to get the power-values. This approach requires a characterized hardware, and is therefore not as accurate for newly designed platforms. If the requirements have not been fulfilled, the implementation has to be debugged and the integrated power-management techniques can be further optimized. The development of the PSM is complete, when all requirements are verified.

B. The MDA-PowerInvestigator

In this section we will describe the implemented framework called MDA-PowerInvestigator, which use the proposed

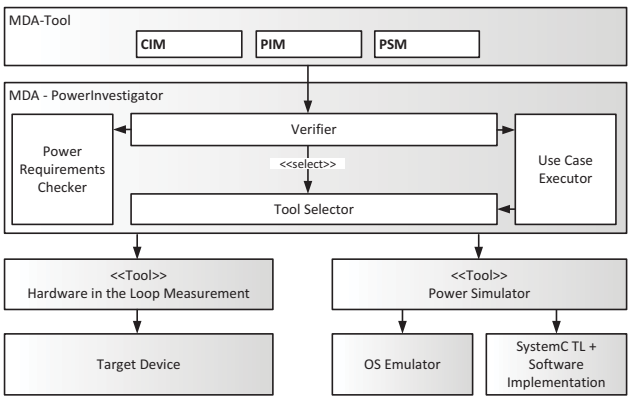


Fig. 4. Architecture of the proposed MDA-PowerInvestigator for the setup using MDA-Tool, HIL, and Power Simulator as tools for verification.

development process extension. This framework is designed to develop software for embedded systems for the domain of NFC (simulation model and hardware in the loop measurement is designed to verify NFC-Systems) The architecture of the framework is shown in Fig. 4. It utilizes the following existing tools:

- **MDA-Tool.** The software "Enterprise Architect" is used to create the CIM, PIM and PSM
- **Power Simulator.** Consists of the SystemC model of the target system using a power model and a connected Operating System (OS) Emulator
- **Hardware in the Loop Measurement.** Controls and monitors the target device (embedded system)

The MDA-Power-Investigator connects these tools in order to support the proposed development process. The toolchain is divided into the following main components:

Verifier: This component is responsible for the verification of the PIM and PSM, and does this in a three step execution. First, it selects the right tool according to the development phase (e.g., simulator for PIM). Secondly it invokes the *Use Case Executor* in order to get the power consumption of the use case. During the third step it uses the *Power Requirements Checker* to find out whether all of the power requirements have been met.

Tool Selector: The development phases require certain tools in order to verify the power-requirements. This component is able to setup and select the appropriate tool or a set of tools. It also provides a common interface to the *Use Case Executor* in order to control and monitor the design or implementation to be verified. This makes the results comprehensible across the development phases.

Use Case Executor: This component parses the sequence diagrams created in the MDA-Tool, and extracts the execution sequence. This type of diagram is a graphical representation of the execution sequence (An example is shown in Fig. 8. This sequence is then used to control the selected verification tool in order to acquire the power consumption. The components identifier and method calls used in the models have to be recognized by the selected tools. This means that there has to be a defined mapping between the identifier and the addressed component. In SystemC, every component and method has an identifier which is able to deal with this challenge. For the HIL, the mapping has to be defined according to the former used model. One solution is to insert the mapping table directly into the HIL in order to avoid changes to the target device and implementation to be verified.

Power Requirements Checker: The power consumptions have to be checked to see whether they fulfill the power-requirements. The concept of the power requirements check is shown in Fig. 5. This is done in two steps. First the provided requirements from the MDA-Tool are parsed, in order to acquire the essential data. It is also possible to store the requirements directly into a standardized format such as MARTE, which reduces the effort of parsing. In step two the power and energy consumptions are compared to the parsed requirements, and the results are returned to the *Verifier*.

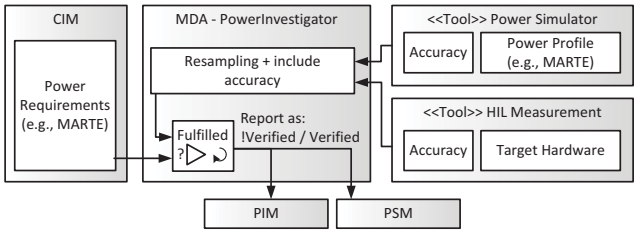


Fig. 5. Concept of the verification of the power requirements provided by the CIM and the reporting to the PIM or PSM as used in the MDA-Power-Investigator framework.

Considerations of comparability and accuracy: First of all there is a significant difference between simulation and measurement according the acquisition of power consumption (comparability). In simulation, the power consumption can be acquired on every clock cycle. The measurement however acquires the power consumption using a specified sampling rate. To get a comparable result, both tools should acquire the power consumption using the same sampling rate. The second consideration is the accuracy of the simulation in comparison to the measurement. The measured target system and SystemC model will differ depending on the model's level of detail and the used power model. In our approach the power models are characterized by measuring the target system through the use of a benchmark program. The average power values are then mapped in order to power states of the simulation model. The accuracy of the used models in comparison to the target system has to be known in order to be able to evaluate whether the target system requirements can be met during early design phases or not. In this work, three accuracies are calculated through the use of a benchmark program on the transaction-level (TL) simulation and target system:

- The calculation of the accuracy of the power consumption, represented by the maximum error E_{max}, is shown in (1) to (2). Input parameters are the results of the simulation P_{sim}, the measurement P_{meas}, which are acquired from all benchmarked transactions T.
- The accuracy of execution time is described by the maximum error of the simulation compared to the measurement. The calculation is similar to the power consumption.
- The accuracy of energy consumption is described and calculated using error propagation by adding the maximum error of time and power consumption.

$$E_{max} = \max(\{E(P_{meas}(T_i), P_{sim}(T_i)) : T_i = 1, ..., \#_T\}) \quad (1)$$

$$E(P_{meas}, P_{sim}) = \left| \frac{\frac{1}{\#_{P_{meas}}} \cdot \sum_{i=1}^{\#_{P_{meas}}} P_{meas}(i)}{\frac{1}{\#_{P_{sim}}} \cdot \sum_{i=1}^{\#_{P_{sim}}} P_{sim}(i)} \right| \cdot 100 \quad (2)$$

C. Usage of MDA-PowerInvestigator to verify NFC-Systems

The MDA-PowerInvestigator has been used to develop a verification framework for NFC-Systems (parts are shown in Fig. 6). Therefore, a setup of the simulation and measurement has to be established. The used MDA development tool is Enterprise Architect, which has been extended with an Addin

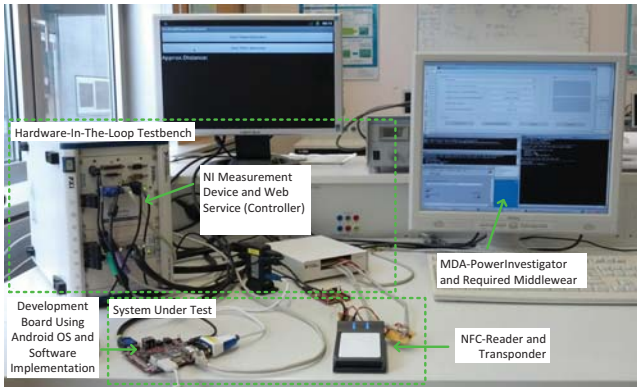


Fig. 6. Picture of the setup used to verify the developed implementation on real hardware. The hardware in the loop measurement setup is connected to the MDA-PowerInvestigator to verify the PSM according the use cases and requirements of the CIM.

as interface to the MDA-PowerInvestigator to verify the system under development.

Simulation: The simulator consists of the SystemC model and the underlying simulator and the connected OS-Emulator. The simulation model used power states to simulate the power consumption and is kept on transaction level. The OS-Emulator is used to simulate commonly used environments like the Android OS. The rest of the NFC-System is extended during the development and is not part of the framework.

Measurement: The measurement setup uses a measurement device from NI to acquire the power consumption of the NFC-System. The system under test uses a development board to represent commonly used environments like the Android OS. The part of the NFC-System beyond the NFC-Reader (e.g., NFC-Bridge) is extended during the development and is not part of the framework.

- Development Tool: Enterprise Architect
- OS-Emulator: Android 2.3.4 (ARM as platform)
- Simulation Model: SystemC version 2.2
- Measurement Device: NI PXI-1042Q
- Development Board: Beagleboard-xM (ARM) with Android 2.3.4

IV. Case Study

In the case study, a NFC-System is designed and implemented using the MDA-PowerInvestigator. The NFC-System should be able to read out sensor data from an embedded system. The architecture of the system is shown in Fig. 7. The system consists of a NFC-Reader for reading and visualizing the sensor data, a NFC-Bridge between the reader and the embedded system, and the embedded system with the sensor. The case study shows a software development for an existing target hardware. This target hardware consists of the following components:

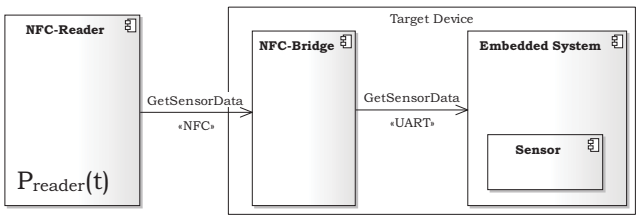


Fig. 7. Architecture of the embedded system used to design and implement the case study.

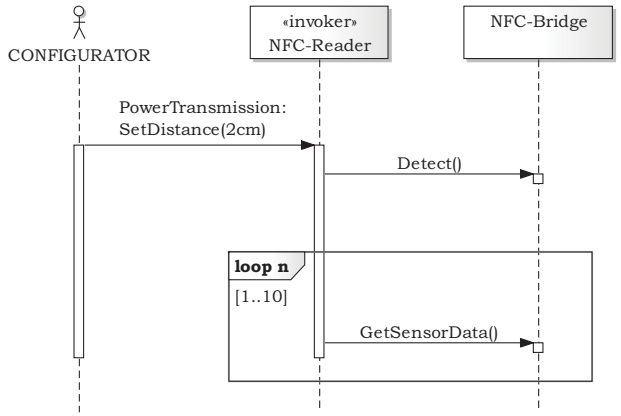


Fig. 8. Sequence diagram of the defined use case of the embedded system for designing the case study.

- NFC-Reader: ISO 14443 A/B DUALI DE-620
- NFC-Bridge: Modified ISO 14443 B Tag Type 2
- Embedded System: MSP-EXP430G2

The described system's use case for this case study is shown in Fig. 8. It focuses on the interaction between the NFC-Reader and the NFC-Bridge in order to read the sensor data. This use case also demonstrates a specific precondition (marked by the actor CONFIGURATOR) which is needed in order to evaluate the power consumption. It defines the condition of physical distance between the NFC-Reader and NFC-Bridge. The reader exclusively supplies the bridge over NFC. The greater the distance between them is the more power has to be provided by the reader to supply the bridge.

The power-requirement for the NFC-Reader is refined which restricts the energy consumption: "Energy Consumption of NFC-Reader must not exceed 5 J for use case."

A. Used simulation model and accuracy

The next step is to define the simulation. In this case study the TL simulation is designed in SystemC (as shown in Fig. 9), using the application protocol data unit (APDU) commands as transactions ($NFCReader\_IF$).The target hardware system already exists, therefore the power model uses the averaged power and time values from the characterization process of the existing hardware. The characterized average power and time values are used for the transactions. Every transaction

TABLE I. Accuracy of the used power simulation.

	Maximum Error E_{max} [%]
Power consumption	5.98
Time	4.01
Energy consumption	9.99

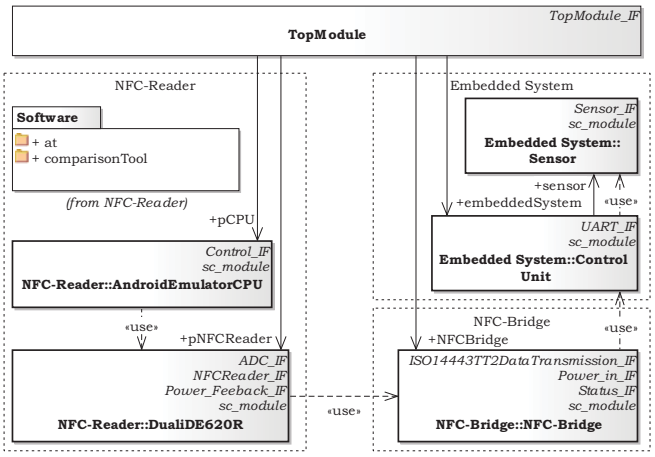


Fig. 9. Top level view of the TL SystemC Model used to develop the NFC-Bridge system.

has one power and time value. An exception is the used model for the domain specific power transfer over NFC. This power transfer depends on the physical distance d and uses the approximation equation (3) and (4) based on the law of Biot-Savart. Parameters such as the reader and bridge coils diameters a_r, b_r, a_t, and b_t, as well as the windings N_r and N_t are known. The unknown parameters are calculated using the results of the characterization under the condition of different distances d. The resulting power transfer is defined through the electrical current provided by the reader i_r and the output voltage u_2 on the bridge.

$$H = \frac{i_r \cdot N_r \cdot a_r \cdot b_r}{4 \cdot \pi \cdot \sqrt{(\frac{a_r}{2})^2 + (\frac{b_r}{2})^2 + d^2}} \cdot \left(\frac{1}{(\frac{a_r}{2})^2 + d^2} + \frac{1}{(\frac{b_r}{2})^2 + d^2}\right) \tag{3}$$

$$u_2 = \frac{\omega \cdot \mu_0 \cdot H \cdot N_t \cdot a_t \cdot b_t}{\sqrt{(\frac{\omega \cdot L_t}{R_l} + \omega \cdot R_t \cdot C_2)^2 + (1 - \omega^2 \cdot L_t \cdot C_2 + \frac{R_t}{R_l})^2}} \tag{4}$$

This TL simulation is now compared to the existing target hardware by using a benchmark program in order to get the accuracy of time, power, and energy as shown in Table I. Every module has its own power-statemachine with a defined interface to separate the power-behavior from the functional implementation. For the wireless power transfer an interface called $Power\_Feeback\_IF$ has been implemented to model the mutual inductance behavior based on equations (3) and (4). The module called $TopModule$ provides the interface $TopModule\_IF$ to interconnect with the MDA-PowerInvestigator framework. This interconnection is used to call the functional operation to perform (e.g., *Detect()*) and to acquire the power values of the modules during the operation. Also the configurations, like changing the distance between the NFC-Reader and the NFC-Bridge, are executed.

B. Verification of the unoptimized system

As a next step the functional part of the system is designed as PIM using the MDA-Tool. This is done using activity diagrams for every call shown in the use case, such as *Detect()*. The resulting software design is now converted into an executable using code generation tools, provided by the

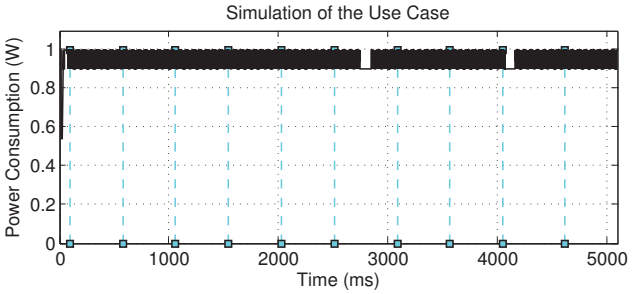


Fig. 10. Simulation result of the unoptimized system showing the power consumption $P_{reader}(t)$.

MDA-Tool. This executable is now deployed to the simulator and executed using the provided use case from Fig. 8. The power result is shown in Fig. 10. The indication lines shown by squares and cyan dotted lines separate the transactions like *Detect()* according the use case. This helps to identify time and power consuming transactions. The resulting energy consumption of the use case according to simulation is 4.89J, which would be sufficient without considering the accuracy of the simulation. When considering the error shown in Table I the energy consumption can be up to 5.38J, which violates the energy requirement.

C. Verification of the power-optimized system

The unoptimized system needs a power-management technique in order to fulfill the requirement. The system based

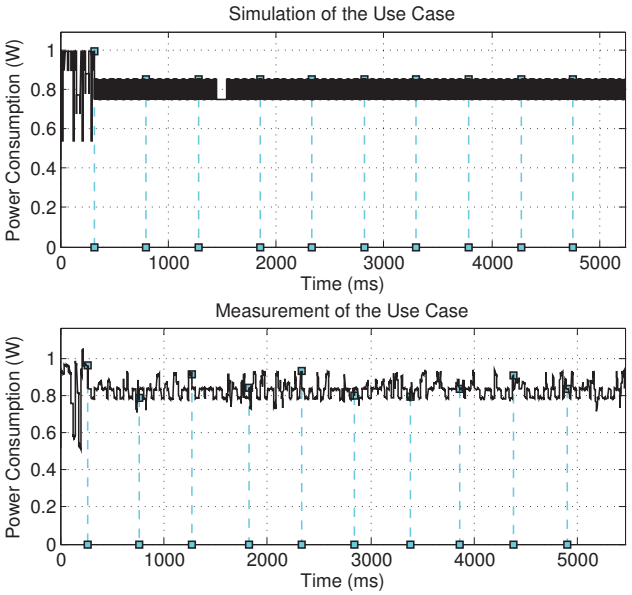


Fig. 11. Result of optimized system showing simulated and measured power consumption $P_{reader}(t)$.

TABLE II. RESULTS OF THE VERIFICATION TOOLS AND THE NEEDED VERIFICATION TIME OF THE POWER-OPTIMIZED SYSTEM.

	Energy Consumption [J]	**Average verification time [s]**
Simulation	4.29 ± 0.43	46.22
Measurement	4.55	5.46 (+50.76 setup t.)

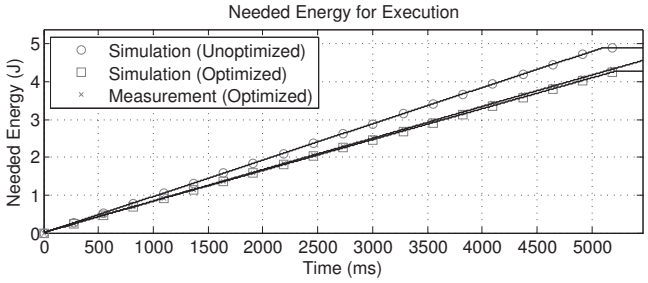


Fig. 12. Combined result of the developed system showing the NFC-Reader's energy consumption.

power management technique from [15] is used for the redesign. The verification is performed as described in Section IV-B. The result is shown in Fig. 11 and Table II. The requirement is now also fulfilled considering the worst-case accuracy scenarios.

As a further step, the software design of the PIM can be transformed into the PSM, which also has to be verified. This is done with the HIL. The result shows, that the power-requirement is fulfilled. The comparison with and without the optimization is shown in Fig. 12. The detected violation of the requirement in the PIM avoided a violation in the implementation. Without the verification of the PIM, a redesign would have been necessary after the implementation. The whole implementation and measurement would have been in vain, which involves increased time and development costs.

V. Conclusions

The MDA verification framework for power-requirements has proven to be a good way to design and implement embedded systems (as in our case software implementations for NFC-Systems). This framework obtains the use cases and requirements directly from the CIM, and offers a unified verification for the PIM and PSM. The MDA-PowerInvestigator shows how to integrate existing tools for power evaluation using the proposed MDA framework. The verification framework for the PIM supports SystemC TL simulation. For the case study the time needed for verification was 46s with 10% accuracy for the energy consumption. The verification of the PSI uses a HIL measurement. Both verification tools use a common interface in order to offer a comparable result. The case study shows, that the proposed process using the MDA-PowerInvestigator detects a violation of the power-requirement in the PIM design stage, which would otherwise only be detected after the measurement in the HIL.

VI. Acknowledgments

Omitted for blinded review.

References

[1] T. Arpinen, E. Salminen, T. D. Hmlinen, and M. Hnnikinen. {MARTE} profile extension for modeling dynamic power management of embedded systems. *Journal of Systems Architecture*, 2012.

[2] C. Bachmann, A. Genser, C. Steger, R. Weiss, and J. Haid. Automated Power Characterization for Run-Time Power Emulation of SoC Designs. In *DSD*, 2010.

[3] F. Ben Abdallah and L. Apvrille. Fast evaluation of power consumption of embedded systems using diplodocus. In *SEAA*, 2013.

[4] L. Benini, A. Bogliolo, and G. De Micheli. A survey of design techniques for system-level dynamic power management. *Very Large Scale Integration (VLSI) Systems, IEEE Transactions on*, 2000.

[5] D. Blaza and A. Wolfe. 2013 Embedded market study. 2013.

[6] S. Chong, C.-B. Wong, H. Jia, H. Pan, P. Moore, R. Kalawsky, and J. O'Brien. Model Driven System Engineering for vehicle system utilizing Model Driven Architecture approach and hardware-in-the-loop simulation. In *ICMA*, 2011.

[7] M. Conti. Extension of SystemC framework towards power analysis. In *FDL*, 2009.

[8] V. Cortellessa, A. Di Marco, and P. Inverardi. Non-Functional Modeling and Validation in Model-Driven Architecture. In *Software Architecture, 2007. The Working IEEE/IFIP Conference on*, 2007.

[9] S. Dhouib, E. Senn, J.-P. Diguet, J. Laurent, and D. Blouin. Model Driven High-Level Power Estimation of Embedded Operating Systems Communication Services. In *ICESS*, 2009.

[10] M. Hause and F. Thom. An Integrated MDA Approach with SysML and UML. In *Engineering of Complex Computer Systems, 2008. ICECCS 2008. 13th IEEE International Conference on*, 2008.

[11] G. Hu, S. Ren, and X. Wang. A Comparison of C/C++-based Software/Hardware Co-design Description Languages. In *ICYCS*, 2008.

[12] I. iSuppli. NFC-Enabled Handsets to Grow Nearly Tenfold from 2012 to 2017. http://www.isuppli.com/Mobile-and-Wireless-Communications/MarketWatch/pages/NFC-Enabled-Handsets-to-Grow-Nearly-Tenfold-from-2012-to-2017.aspx. [Online; 2014].

[13] H. Lebreton and P. Vivet. Power modeling in systemc at transaction level, application to a dvfs architecture. In *Symposium on VLSI, 2008. ISVLSI '08. IEEE Computer Society Annual*, pages 463–466, April 2008.

[14] D. Lorenz, P. Hartmann, K. Grttner, and W. Nebel. Non-invasive Power Simulation at System-Level with SystemC. In *Integrated Circuit and System Design. Power and Timing Modeling, Optimization and Simulation*. 2013.

[15] 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 *EURASIP RFID*, 2012.

[16] V. Narayanan, I.-C. Lin, and N. Dhanwada. A power estimation methodology for systemc transaction level models. In *Hardware/Software Codesign and System Synthesis, 2005. CODES+ISSS '05. Third IEEE/ACM/IFIP International Conference on*, pages 142–147, Sept 2005.

[17] U. Neffe, K. Rothbart, C. Steger, R. Weiss, E. Rieger, and A. Muhlberger. Energy estimation based on hierarchical bus models for power-aware smart cards. In *DATE*, 2004.

[18] R. Passerone et al. Metamodels in Europe: Languages, Tools, and Applications. *Design Test of Computers, IEEE*, 2009.

[19] E. Riccobene, P. Scandurra, A. Rosti, and S. Bocchio. A SoC design methodology involving a UML 2.0 profile for SystemC. In *Design, Automation and Test in Europe, 2005. Proceedings*, 2005.

[20] M. Saadatmand, A. Cicchetti, and M. Sjodin. A methodology for designing energy-aware secure embedded systems. In *SIES*, 2011.

[21] B. Selic. From Model-Driven Development to Model-Driven Engineering. In *ECRTS*, 2007.

[22] G. Vece. PK tool 2.0: a SystemC environment for high level power estimation. In *Electronics, Circuits and Systems*, 2005.

[23] J. Vidal, F. de Lamotte, G. Gogniat, J.-P. Diguet, and P. Soulard. IP reuse in an MDA MPSoPC co-design approach. In *ICM*, 2009.

[24] L. Zhu and Y. Liu. Model Driven Development with non-functional aspects. In *ICSE*, 2009.

Bibliography

[1] NFC Forum. NFC Forum Specification Architecture. http://nfc-forum.org/our-work/specifications-and-application-documents/specifications/. [Online; accessed 15-January-2014].

[2] IHS iSuppli. NFC-Enabled Handsets to Grow Nearly Tenfold from 2012 to 2017. http://www.isuppli.com/Mobile-and-Wireless-Communications/MarketWatch/pages/NFC-Enabled-Handsets-to-Grow-Nearly-Tenfold-from-2012-to-2017.aspx. [Online; accessed 04-March-2014].

[3] M. Menghin, N. Druml, M.T. Fioriello, C. Steger, R. Weiss, H. Bock, and J. Haid. PtNBridge – A Power-Aware and Trustworthy Near Field Communication Bridge to Embedded Systems. In *Digital System Design (DSD), 2013 Euromicro Conference on*, pages 907–914, 2013.

[4] Infineon Technologies Austria AG. Mobile Energy-efficient Trustworthy Authentication Systems with Elliptic Curve based SECurity, 2010. collaborative research project of the Graz University of Technology, Infineon Austria AG and Enso Detego GmbH. Funded by the Austrian Federal Ministry for Transport, Innovation, and Technology under the FIT-IT contract FFG 829586.

[5] M. Menghin, N. Druml, C. Steger, R. Weiss, R. Bock, and J. Haid. NFC-DynFS: A way to realize dynamic field strength scaling during communication. In *Near Field Communication (NFC), 2013 5th International Workshop on*, pages 1–6, 2013.

[6] 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*, 2013(1):1–16, 2013.

[7] 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 *RFID Technology (EURASIP RFID), 2012 Fourth International EURASIP Workshop on*, pages 92–98, 2012.

[8] M. Menghin, N. Druml, B. Kipperer, C. Steger, R. Weiss, H. Bock, and J. Haid. Energy efficiency by using field strength scaling for multi-transponder applications. In *Telecommunications (ConTEL), 2013 12th International Conference on*, pages 263–270, 2013.

[9] T. Arpinen, E. Salminen, T. D. Hämäläinen, and M. Hännikäinen. {MARTE} profile extension for modeling dynamic power management of embedded systems. *Journal of Systems Architecture*, 58(5):209 – 219, 2012.

[10] M. Menghin, N. Druml, C. Preschern, C. Steger, R. Weiss, H. Bock, and J. Haid. Introduction of design pattern(s) for power-management in embedded systems. In *19th European Conference on Pattern Languages of Programs, EuroPLoP (in press)*, pages 1–16, 2013.

[11] C. Bachmann, A. Genser, C. Steger, R. Weiss, and J. Haid. Automated Power Characterization for Run-Time Power Emulation of SoC Designs. In *Digital System Design: Architectures, Methods and Tools (DSD), 2010 13th Euromicro Conference on*, pages 587 –594, sept. 2010.

[12] NFC Forum. NFC Digital Protocol Technical Specification, DIGITAL 1.0, 2010.

[13] Koichi Tagawa. The Four Essential Keys to a Winning NFC Solution, 2013. Presentation at WIMA 2013 Monaco.

[14] Natt Garun. Study: By 2020, smartphones will replace cash and credit cards as the preferred payment method, sept 2013.

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

[16] David Blaza and Alex Wolfe. 2013 EMBEDDED MARKET STUDY, 2013.

[17] O.S. Unsal and I. Koren. System-level power-aware design techniques in real-time systems. *Proceedings of the IEEE*, 91(7), july 2003.

[18] S. Chatterjee, S. Roy, and S. Bandyopadhyay. Hop-Efficient and Power-Optimized Routing Strategy in a Decentralized Mesh Network Using Directional Antenna. In *Parallel and Distributed Computing, 2006. ISPDC '06. The Fifth International Symposium on*, pages 155 –160, 2006.

[19] J. Liu and W. Tong. Dynamic share energy provisioning service for one-hop multiple RFID tags identification system. In *Cloud Computing and Intelligence Systems (CCIS), 2011 IEEE International Conference on*, pages 342 –347, 2011.

[20] Josef Haid, Walter Kargl, Thomas Leutgeb, and Dietmar Scheiblhofer. Power management for rf-powered vs. battery-powered devices, 2005.

[21] Arjun Roy, Stephen M. Rumble, Ryan Stutsman, Philip Levis, David Mazières, and Nickolai Zeldovich. Energy management in mobile devices with the cinder operating system. In *Proceedings of the sixth conference on Computer systems*, EuroSys '11, pages 139–152, New York, NY, USA, 2011. ACM.

[22] M. Zargham and P.G. Gulak. Maximum Achievable Efficiency in Near-Field Coupled Power-Transfer Systems. *Biomedical Circuits and Systems, IEEE Transactions on*, 6(3), june 2012.

[23] D. Cheng, Z. Wang, and Q. Zhou. Analysis of Distance of RFID Systems Working under 13.56MHz. In *Wireless Communications, Networking and Mobile Computing, 2008. WiCOM'08. 4th International Conference on*, pages 1 –3, 2008.

[24] E. Rolf and V. Nilsson. Near Field Communication (NFC) for Mobile Phones. In *Near Field Communication (NFC) for Mobile Phones*, page 25, 2006.

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

[26] X. Xu, L. Gu, J. Wang, G. Xing, and S. Cheung. Read More with Less: An Adaptive Approach to Energy-Efficient RFID Systems. *Selected Areas in Communications, IEEE Journal on*, 29(8):1684 –1697, september 2011.

[27] K. Fotopoulou and B.W. Flynn. Wireless Power Transfer in Loosely Coupled Links: Coil Misalignment Model. *Magnetics, IEEE Transactions on*, 47(2), feb. 2011.

[28] H. Witschnig and E. Merlin. Modeling of Multilabel Scenarios of 13.56 MHz RFID Systems. In *Microwave Conference, 2008. EuMC 2008. 38th European*, pages 59 – 62, 2008.

[29] E. Haselsteiner and K. Breitfus. Security in Near Field Communication (NFC) Strengths and Weaknesses. *Semiconductors*, 11(71), 2006.

[30] G. Madlmayr, J. Langer, C. Kantner, and J. Scharinger. NFC Devices: Security and Privacy. In *Availability, Reliability and Security, 2008. ARES 08. Third International Conference on*, pages 642–647, 2008.

[31] Chi-Huan Jiang, Hung-Lin Li, Yu-Jung Huang, and Wei-Cheng Lin. Mutual authentication architecture in wireless sensor networks. In *Microelectronics and Electronics (PrimeAsia), 2010 Asia Pacific Conference on Postgraduate Research in*, pages 291–294, 2010.

[32] M. O"Neill and M. J B Robshaw. Low-cost digital signature architecture suitable for radio frequency identification tags. *Computers Digital Techniques, IET*, 4(1):14–26, 2009.

[33] H. Aigner, H. Bock, M. Hütter, and J. Wolkerstorfer. A Low-Cost ECC Coprocessor for Smartcards. In Marc Joye and Jean-Jacques Quisquater, editors, *Cryptographic Hardware and Embedded Systems - CHES 2004*, volume 3156 of *Lecture Notes in Computer Science*, pages 107–118. Springer Berlin Heidelberg, 2004.

[34] H. Alrimeih and D. Rakhmatov. Security-performance trade-offs in embedded systems using flexible ecc hardware. *Design Test of Computers, IEEE*, 24(6):556–569, 2007.

[35] E. Wenger and J. Grossschädl. An 8-bit AVR-Based Elliptic Curve Cryptographic RISC Processor for the Internet of Things. In *Microarchitecture Workshops (MICROW), 2012 45th Annual IEEE/ACM International Symposium on*, pages 39–46, 2012.

[36] D. Hwang, P. Schaumont, K. Tiri, and I. Verbauwhede. Securing embedded systems. *Security Privacy, IEEE*, 4(2):40–49, 2006.

[37] E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid. Recommendation for key management x96 part 1: General(revision 3). In *NIST Special Publication 800-57*, pages 1–147, 2012.

[38] S. Ravi, A. Raghunathan, P. Kocher, and S. Hattangady. Security in embedded systems: Design challenges. *ACM Trans. Embed. Comput. Syst.*, 3(3):461–491, August 2004.

[39] T. Eisenbarth and S. Kumar. A Survey of Lightweight-Cryptography Implementations. *Design Test of Computers, IEEE*, 24(6):522–533, 2007.

[40] M. Potkonjak, S. Meguerdichian, and J. L. Wong. Trusted sensors and remote sensing. In *Sensors, 2010 IEEE*, pages 1104–1107, 2010.

[41] Jun Yang, Lan Gao, and Youtao Zhang. Improving memory encryption performance in secure processors. *Computers, IEEE Transactions on*, 54(5):630–640, 2005.

[42] L. Caviglione, A. Merlo, and M. Migliardi. What is green security? In *Information Assurance and Security (IAS), 2011 7th International Conference on*, pages 366–371, 2011.

[43] A.S. Wander, N. Gura, H. Eberle, V. Gupta, and S.C. Shantz. Energy analysis of public-key cryptography for wireless sensor networks. In *Pervasive Computing and Communications, 2005. PerCom 2005. Third IEEE International Conference on*, pages 324–328, 2005.

[44] P. Trakadas, T. Zahariadis, H. C Leligou, S. Voliotis, and K. Papadopoulos. Analyzing energy and time overhead of security mechanisms in wireless sensor networks. In *Systems, Signals and Image Processing, 2008. IWSSIP 2008. 15th International Conference on*, pages 137–140, 2008.

[45] G. Bertoni, L. Breveglieri, and M. Venturi. Power aware design of an elliptic curve coprocessor for 8 bit platforms. In *Pervasive Computing and Communications Workshops, 2006. PerCom Workshops 2006. Fourth Annual IEEE International Conference on*, pages 5 pp.–341, 2006.

[46] Wei Jiang, Zhenlin Guo, Yue Ma, and Nan Sang. Research on cryptographic algorithms for embedded real-time systems: A perspective of measurement-based analysis. In *High Performance Computing and Communication 2012 IEEE 9th International Conference on Embedded Software and Systems (HPCC-ICESS), 2012 IEEE 14th International Conference on*, pages 1495–1501, 2012.

[47] T. Winn and P. Calder. Is this a pattern? *Software, IEEE*, 19(1):59 –66, jan/feb 2002.

[48] B. Grone. Conceptual patterns. In *Engineering of Computer Based Systems, 2006. ECBS 2006. 13th Annual IEEE International Symposium and Workshop on*, pages 6 pp. –246, march 2006.

[49] F. Rincon, F. Moya, J. Barba, and J.C. Lopez. Model reuse through hardware design patterns. In *Design, Automation and Test in Europe, 2005. Proceedings*, pages 324 – 329 Vol. 1, march 2005.

[50] David Déharbe and Sergio Medeiros. Aspect-oriented design in systemC: implementation and applications. In *Proceedings of the 19th annual symposium on Integrated circuits and systems design*, SBCCI '06, pages 119–124, New York, NY, USA, 2006. ACM.

[51] Michael Kircher and Prashant Jain. *Pattern-Oriented Software Architecture Volume 3: Patterns for Resource Management*. Wiley, June 2004.

[52] C. Weir and J. Noble. *Thinking Small - The Processes for Creating Small Memory Software*. Weir, C. and Noble, J., 2004.

[53] N. Mani, D.C. Petriu, and M. Woodside. Studying the impact of design patterns on the performance analysis of service oriented architecture. In *Software Engineering and Advanced Applications (SEAA), 2011 37th EUROMICRO Conference on*, pages 12 –19, 30 2011-sept. 2 2011.

[54] C. Sahin, F. Cayci, I.L.M. Gutierrez, J. Clause, F. Kiamilev, L. Pollock, and K. Winbladh. Initial explorations on design pattern energy usage. In *Green and Sustainable Software (GREENS), 2012 First International Workshop on*, pages 55 –61, june 2012.

[55] Robertas Damaševičius, Giedrius Majauskas, and Vytautas Štuikys. Application of design patterns for hardware design. In *Proceedings of the 40th annual Design Automation Conference*, DAC '03, pages 48–53, New York, NY, USA, 2003. ACM.

[56] K. Heyrman, A. Papanikolaou, F. Catthoor, P. Veelaert, and W. Philips. Control for power gating of wires. *Very Large Scale Integration (VLSI) Systems, IEEE Transactions on*, 18(9):1287 –1300, sept. 2010.

[57] E. Riccobene, P. Scandurra, A. Rosti, and S. Bocchio. A soc design methodology involving a uml 2.0 profile for systemc. In *Design, Automation and Test in Europe, 2005. Proceedings*, pages 704 – 709 Vol. 2, march 2005.

[58] Ge Hu, Shengbing Ren, and Xie Wang. A comparison of c/c++-based software/hardware co-design description languages. In *Young Computer Scientists, 2008. ICYCS 2008. The 9th International Conference for*, pages 1030 –1034, nov. 2008.

[59] M.C. Hause and F. Thom. An integrated mda approach with sysml and uml. In *Engineering of Complex Computer Systems, 2008. ICECCS 2008. 13th IEEE International Conference on*, pages 249 –254, 31 2008-april 3 2008.

[60] Ricardo Jorge Machado, Rita Suzana Pitangueira Maciel, Julia Rubin, and Goetz Botterweck, editors. *Model-Based Methodologies for Pervasive and Embedded Software, 8th International Workshop, MOMPES 2012, Essen, Germany, September 4, 2012. Revised Papers*, volume 7706 of *Lecture Notes in Computer Science*. Springer, 2013.

[61] Seng Chong, Chi-Biu Wong, Haibo Jia, Hongtao Pan, P. Moore, R. Kalawsky, and J. O'Brien. Model driven system engineering for vehicle system utilizing model driven architecture approach and hardware-in-the-loop simulation. In *Mechatronics and Automation (ICMA), 2011 International Conference on*, pages 1451 –1456, aug. 2011.

[62] R. Passerone et al. Metamodels in Europe: Languages, Tools, and Applications. *Design Test of Computers, IEEE*, 2009.

[63] Liming Zhu and Yan Liu. Model driven development with non-functional aspects. In *Aspect-Oriented Requirements Engineering and Architecture Design, 2009. EA '09. ICSE Workshop on*, pages 49 –54, may 2009.

[64] V. Cortellessa, A. Di Marco, and P. Inverardi. Non-functional modeling and validation in model-driven architecture. In *Software Architecture, 2007. WICSA '07. The Working IEEE/IFIP Conference on*, page 25, jan. 2007.

[65] S. Dhouib, E. Senn, J.-P. Diguet, J. Laurent, and D. Blouin. Model driven high-level power estimation of embedded operating systems communication services. In *Embedded Software and Systems, 2009. ICESS '09. International Conference on*, pages 475 –481, may 2009.

[66] M. Saadatmand, A. Cicchetti, and M. Sjodin. A methodology for designing energy-aware secure embedded systems. In *Industrial Embedded Systems (SIES), 2011 6th IEEE International Symposium on*, pages 87 –90, june 2011.

[67] M. Conti. Extension of SystemC framework towards power analysis. In *Specification & Design Languages, 2009*, 2009.

[68] Daniel Lorenz, Philipp A. Hartmann, Kim Grüttner, and Wolfgang Nebel. Non-invasive Power Simulation at System-Level with SystemC. In Jose. Ayala, Delong Shang, and Alex Yakovlev, editors, *Integrated Circuit and System Design. Power and Timing Modeling, Optimization and Simulation*, volume 7606. Springer Berlin Heidelberg, 2013.

[69] G.B. Vece. PK tool 2.0: a SystemC environment for high level power estimation. In *Electronics, Circuits and Systems, 2005*, 2005.

[70] F. Ben Abdallah and L. Apvrille. Fast Evaluation of Power Consumption of Embedded Systems Using DIPLODOCUS. In *SEAA*, 2013.

[71] MeuseN.O. Junior, Silvino Neto, Paulo Maciel, Ricardo Lima, Angelo Ribeiro, Raimundo Barreto, Eduardo Tavares, and Frederico Braga. Analyzing software performance and energy consumption of embedded systems by probabilistic modeling: An approach based on coloured petri nets. In Susanna Donatelli and P.S. Thiagarajan, editors, *Petri Nets and Other Models of Concurrency - ICATPN 2006*, volume 4024 of *Lecture Notes in Computer Science*, pages 261–281. Springer Berlin Heidelberg, 2006.