Jürgen Schilling, BSc

Design und Implementierung von kontaktlosen System-in-Package Authentifizierungstags

MASTERARBEIT

zur Erlangung des akademischen Grades

Diplom-Ingenieur

Masterstudium Telematik

eingereicht an der

Technischen Universität Graz

Betreuer

Ass. Prof. Dipl.-Ing. Dr. techn. Christian Steger
Dipl.-Ing. Dr. techn. Norbert Druml (Infineon Technologies Austria AG)

Institut für Technische Informatik
Technische Universität Graz

Graz, Oktober 2015

EIDESSTATTLICHE ERKLÄRUNG

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 Masterarbeit identisch.

Datum

Unterschrift

Kurzfassung

RFID-Tags sind heutzutage weit verbreitet. Aktuelle Smartphones verfügen über eine NFC-Funktionalität, die es erlaubt, solche Tags auszulesen und, je nach Art, auch zu beschreiben.
Das SCAD Projekt (System-in-Package Contactless Authentication Devices) stellt miniaturisierte Lösungen für kontaktlose Authentifizierungen vor. Verschiedene RFID-Chips werden gemeinsam mit einer HF-Antenne in ein embedded Wafer Level Ball Grid Array (*eWLB*) Gehäuse integriert (*Coil-on-Embedding*). Zusätzlich werden Kondensatoren für eine bessere HF-Kopplungscharakteristik hinzugefügt. Als RFID-Chips kommen dabei drei verschiedene Typen von reinen Speichern und ein CIPURSE Chip zum Einsatz.
Mehrere verschiedene Gehäusedesigns wurden für jeden Chip Typ entwickelt um verschiedene Designentscheidungen (z.B. ein- oder zweilagige Spulen, zusätzliche Ferriteinlage für verbesserte Kopplungscharakteristik, Größe des Gehäuses) zu evaluieren und zu beurteilen.
Verglichen mit dem aktuellen Stand der Technik soll SCAD eine bessere HF-Kopplungscharakteristik ermöglichen als vergleichbare Coil-on-Chip Lösungen. Dies ermöglicht ein einfacheres Auslesen der Tags mit NFC-fähigen Smartphones.
Bedingt durch die kleinen Gehäusedimensionen von 3x3 mm und 5x5 mm können diese Tags außerdem in verschiedene Produkte wie Schmuck, Konsumgüter etc. integriert werden.
Im Zuge dieses Projektes wurden außerdem eine Android App und eine PC-basierte Demo entwickelt. Diese Demos sollen die Funktionsweise sowie mögliche Einsatzgebiete der Tags zeigen.

Schlüsselwörter: Kontaktlose System-in-Package Authentifizierungstags, SCAD, eWLB, Coil-on-Embedding, RFID, NFC, CIPURSE

Abstract

RFID tags are widely spread and current smartphones are equipped with NFC functionality to read and depending on the type of the tag to write information on the tag.
The SCAD project (System-in-Package Contactless Authentication Devices) aims to introduce miniaturized contactless authentication solutions. Several RFID chips are integrated into embedded Wafer Level Ball Grid Array (eWLB) packages together with HF antennas (*Coil-on-Embedding*) as well as capacitors for improving HF coupling characteristics. Three different types of memory ICs and one CIPURSE IC are used.
Several package designs are developed for each RFID chip with the aim to evaluate various design decisions (e.g.: one or two layers of coils, integration of a ferrite layer for improved coupling characteristics, size of the package).
Compared to state-of-art, SCAD will give better HF coupling characteristics than Coil-on-Chip approaches which will also enable a verification of authenticity of SCAD-tagged products through NFC enabled smartphones. Thanks to the small sized packages of 3x3 mm and 5x5 mm, SCAD enables integration into various types of products (such as jewelry, casings, consumable materials, etc.).
During this project also an Android application and a PC based demo are developed to communicate with the authentication chip and demonstrate possible fields of application.

Keywords: System-in-Package Contactless Authentication Devices, SCAD, eWLB, Coil-on-Embedding, RFID, NFC, CIPURSE, System-in-Package

Danksagung

Diese Masterarbeit wurde im Sommersemester 2015 bei der Infineon Technologies Austria AG in Kooperation mit dem Institut für Technische Informatik der TU Graz durchgeführt.

Zu Beginn möchte ich mich bei all jenen bedanken, die zum Gelingen dieser Arbeit beigetragen haben. Insbesondere möchte ich mich bei Herrn Dipl.-Ing. Dr. techn. Norbert Druml und Herrn Dipl.-Ing. Dr. techn. Walther Pachler bedanken, die mir in allen Belangen unter die Arme gegriffen haben und mir bei technischen Fragen jederzeit mit Rat und Tat zur Seite standen. Ein besonderer Dank gilt auch Herrn Ass. Prof. Dipl.-Ing. Dr. techn. Christian Steger, der mich auf universitärer Seite unterstützt hat.

Mein Dank gilt insbesondere meinen engsten Freunden, die mich jederzeit tatkräftig unterstützt haben und damit einen wertvollen Beitrag zu dieser Arbeit geleistet haben.

Zum Schluss möchte ich natürlich noch meinen Eltern ganz herzlich danken, die mir mein Studium ermöglicht haben. Ohne sie hätte ich es nicht bis hier her geschafft.

Graz, im Oktober 2015 Jürgen Schilling

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

SiP System-in-Package

CoC Coil-on-Chip

CoM Coil-on-Module

CoE Coil-on-Embedding

LF Low Frequency

HF High Frequency

UHF Ultra High Frequency

NFC Near Field Communication

RFID Radio Frequency Identification

IC Integrated Circuit

GUI Graphical User Interface

eWLB embedded Wafer Level Ball Grid Array

AES Advanced Encryption Standard

HFSS High Frequency Structural Simulator

ADS Advanced Design System

FEM Finite-Elemente-Method

MoM Method-of-Moments

SCAD System-in-Package Contactless Authentication Devices

RDL Redistribution Layer

HG High Gain

DPA Differential Power Analysis

DFA Differential Fault Analysis

Kapitel 1

Einleitung

Diese Masterarbeit ist im Zuge des SCAD Innovationsprojektes bei der Infineon Technologies Austria AG [IFA] im Sommersemester 2015 am Institut für Technische Informatik [ITI] der TU Graz [TUG] durchgeführt worden.

Durch dieses Projekt soll eine neue, verkleinerte Bauform für RFID[1]-Tags eingeführt werden. Diese Tags sollen robust gegenüber äußeren Einflüssen, aber trotzdem günstig in der Herstellung sein. Es soll einfach möglich sein zusätzliche Bauteile wie etwa Kondensatoren in den Tag zu integrieren, wodurch sie an spezielle Anforderungen im gewünschten Einsatzgebiet angepasst werden können und somit die möglichen Anwendungsgebiete erweitert werden.

Zusätzlich sollen sie so klein wie möglich gestaltet werden, aber trotz kompakter Bauweise eine akzeptable Reichweite aufweisen können.

Eine mögliche Anwendung wäre den Chip in ein hochpreisiges Produkt, wie etwa einen Ring, zu integrieren. Dadurch besteht dann die Möglichkeit, den Chip mit einem handelsüblichen Smartphone mit NFC[2]-Funktion auszulesen und die Echtheit des Rings zu verifizieren. Damit würden Fälschungen deutlich erschwert werden. Der schematische Aufbau eines solchen Szenarios ist in Abbildung 1.1 dargestellt.

1.1 Motivation

Kontaktlose RFID-Tags finden immer weitere Verbreitung im alltäglichen Leben. Lesegeräte um diese auszulesen werden immer häufiger auch in Smartphones eingebaut. Die möglichen Anwendungen erstrecken sich dabei von einfachen kontaktlosen Speichern, über elektronische Fahrscheine bis hin zu Zutrittskontrolle.

Je kleiner diese Tags werden, desto einfacher ist es, sie in diversen Gebrauchsgegenständen zu integrieren. Damit wäre es zum Einen möglich lediglich zusätzliche Informationen zu übertragen oder aber auch die Echtheit von Gegenständen zu überprüfen um Produktfälschungen zu erkennen. Statistiken der internationalen Handelskammer bezüglich des Handels mit Produktfälschungen (siehe Tabelle 1.1) zeigen, dass sich der Umsatz von gefälschten Produkten zwischen 2008 und 2015 voraussichtlich verdreifachen wird.

[1] Radio Frequency Identification
[2] Near Field Communication

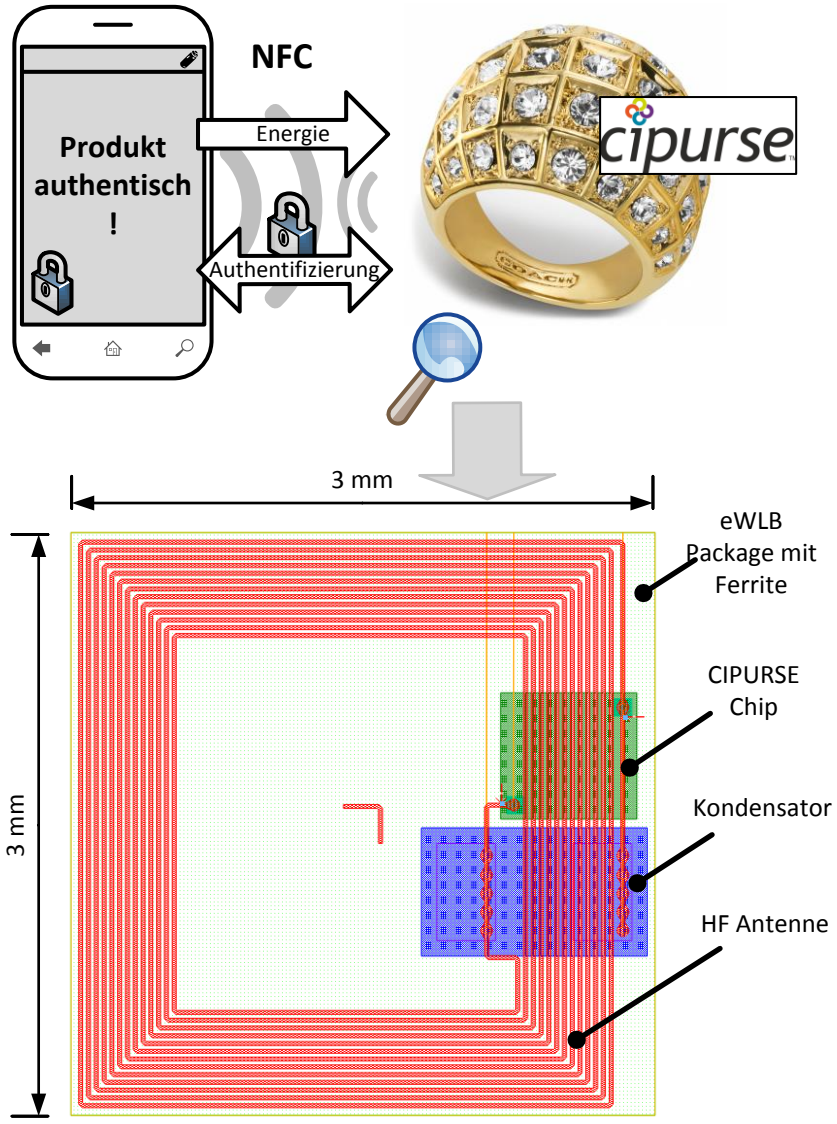


Abbildung 1.1: Mögliche Anwendung der Authentifizierungslösung

Um solche Fälschungen zu erkennen sind gut ausgebildete und erfahrene Leute notwendig, welche die Produkte auf ihre Echtheit hin überprüfen müssen. Dieser Aufwand könnte verringert werden, in dem z.b. fälschungssichere RFID-Tags in die Produkte integriert werden, um die Echtheit bei Bedarf mit einfachen Mitteln überprüfen zu können.

Gegenwärtig verfügbare Transponder weisen dahingehend allerdings Nachteile auf. Kleine Transponder haben aufgrund ihrer Größe nur eine sehr geringe Reichweite, während Transponder im ID-1 Format eine gute Reichweite aufweisen, dabei aber relativ groß sind.

	Internationaler Handel gefälschter Produkte	**Produzierte und konsumierte gefälschte Produkte**	**Total**
2008	285 Mrd. € - 360 Mrd. €	140 Mrd. € - 215 Mrd. €	425 Mrd. € - 575 Mrd. €
2015	770 Mrd. € - 960 Mrd. €	370 Mrd. € - 570 Mrd. €	1.140 Mrd. € - 1.530 Mrd. €

Tabelle 1.1: Schätzung des Gesamtwertes von gefälschten und nachgeahmten Produkten in den Jahren 2008 und 2015 [ICC]

Zusätzlich fehlen den meisten verfügbaren Transpondern Sicherheitsfunktionen, wodurch sie für den Einsatz in sicherheitsrelevanten Bereichen grundsätzlich nicht geeignet sind. Den kleinsten Bauformen fehlt außerdem die Möglichkeit, neben dem IC[3] und der Antenne, weitere Bauteile zu integrieren, weshalb die möglichen Einsatzgebiete weiter einschränkt sind. Der größte Teil eines solchen Tags ist die Antenne. Während die eigentlichen ICs in Größenordnungen von $1/2mm^2$ bis ca. $2mm^2$ erhältlich sind, kommt die Antenne eines ID-1 RFID-Tags auf rund 85,60 mm x 53,98 mm. Die Miniaturisierung eines RFID-Tags gelingt daher am schnellsten über eine Verkleinerung der Antenne, wodurch sich die nutzbare Reichweite verringert. Deshalb muss bei einer Verkleinerung immer die geforderte Mindestreichweite beachtet werden.

1.2 Ziele der Arbeit

Ziel dieser Masterarbeit ist es, funktionsfähige Prototypen von miniaturisierten RFID-Tags mit verschiedene Typen von ICs zu entwickeln, sowie Demonstratoren auszuarbeiten um die Funktion der Prototypen sowie mögliche Einsatzgebiete zu demonstrieren. Diese Tags sollen folgende Eigenschaften erfüllen:

- Robust gegenüber äußeren Einflüssen
- Integration von zusätzlichen Bauelementen wie Kondensatoren
- Sicheres Speichern und Auslesen von Informationen
- Gutes Ansprechverhalten
- Verschiedene Transpondergrößen von 3x3mm und 5x5mm
- Gewährleistung der Datenintegrität

Zudem soll evaluiert werden, inwieweit sich solche Miniaturisierungen bei den gegebenen Anforderungen realisieren lassen und mit welchen Problemen hierbei gerechnet werden muss.

[3] Integrated Circuit

1.3 Gliederung

Diese Arbeit ist in folgende Abschnitte gegliedert:

In Kapitel 2 werden zuerst die Grundlagen zu RFID gezeigt. Danach werden aktuelle Ansätze und alternative Bauformen vorgestellt. Desweiteren unterscheidet dieses Kapitel zwischen theoretischen Lösungen bzw. grundlegenden Konzepten (Abschnitt 2.2) sowie bereits verfügbaren kommerziellen Produkten (Abschnitt 2.3). Am Ende erhält man eine Gesamtübersicht der gezeigten Varianten.
Unter Abschnitt 2.4 wird die im Zuge dieses Projektes verwendete Fertigungstechnik vorgestellt sowie ihre Verwendung verdeutlicht.

Im Kapitel 3 bekommt man vorab einen Überblick über den Ablauf des Projektes. Anschließend werden die Designparameter festgelegt sowie die verwendeten ICs vorgestellt. Zum Schluss des Kapitels bekommt man eine Übersicht von allen Varianten sowie den Designs der Demonstratoren.

In Kapitel 4 werden die Packages sowie die Simulationen gezeigt. Darin wird in Abschnitt 4.1 das verwendete Tool vorgestellt, welches für die Implementierung sowie die 2D-Simulationen verwendet wird, sowie unter Abschnitt 4.2 das Tool für die 3D-Simulationen. Danach werden die Packages und die dazugehörigen Simulationen gezeigt. Dieser Abschnitt ist nach den jeweils verwendeten ICs gegliedert. Darüberhinaus werden die Ergebnisse der 3D-Simulationen auf unterschiedlichen Untergrundmaterialien gezeigt. Am Ende wird noch die Implementierung der Demonstratoren dargestellt.

In Kapitel 5 werden die Ergebnisse der gefertigten Bauelemente vorgestellt sowie Probleme aufgezeigt, welche sich während der Laufzeit des Projektes ergeben haben.

Am Ende wird in Kapitel 6 noch einmal eine Zusammenfassung sowie ein Ausblick auf zusätzliche Möglichkeiten der Erweiterung der vorgestellten Tags gegeben.

Den Abschluss bildet das Literaturverzeichnis.

Kapitel 2

Stand der Technik und Grundlagen

In diesem Kapitel erhält man zuerst einen Überblick von den Grundlagen der RFID Technik. Darauffolgend werden einige Ansätze vorgestellt, wie RFID-Tags aufgebaut sein können und wie eine Miniaturisierung erreicht werden kann. Unter Abschnitt 2.2 erfolgt eine Vorstellung über grundsätzliche Ansätze, wie solche Miniatursysteme aussehen können. Der nachfolgende Abschnitt 2.3 behandelt fertige Lösungen, welche sich zum Zeitpunkt der Erstellung dieser Arbeit bereits im Handel befanden. Es werden in diesem Kapitel Systeme im LF[1]-, HF[2]- und UHF[3]-Bereich gezeigt. Um eine bessere Vergleichbarkeit mit SCAD[4] zu ermöglichen, wird jedoch lediglich auf Systeme im HF-Bereich genauer eingegangen.

2.1 Grundlagen RFID

RFID steht für Radio Frequency Identification und bedeutet *Identifizierung mithilfe von elektromagnetischen Wellen*. Grundsätzlich besteht ein RFID-System aus einem Transponder und einem Lesegerät [Fin03]. Der Transponder befindet sich auf dem zu identifizierenden Objekt, welcher vom Lesegerät kontaktlos gelesen und je nach Anwendung auch beschrieben werden kann. Der Transponder selbst besteht in der Regel aus einem IC und einer Antenne, auch Koppelelement genannt, welche gemeinsam auf ein Trägermaterial aufgebracht werden. Der IC beinhaltet den Speicher, die Energieverwaltung sowie etwaige Zusatzfunktionen wie etwa eine Verschlüsselung. An diesem wird dann die Antenne angeschlossen.

Passive Transponder

Die meisten Transponder beziehen die Energie die sie benötigen direkt aus dem Feld des Lesegerätes. Solche Transponder bezeichnet man als *passiv*. Sie verfügen über keinerlei zusätzliche Energiequelle und beziehen die gesamte Energie, welche sie für die Funktionen

[1] Low Frequency
[2] High Frequency
[3] Ultra High Frequency
[4] System-in-Package Contactless Authentication Devices

des ICs sowie für die Kommunikation benötigen, aus dem Feld des Lesegerätes (Abbildung 2.1). Die Reichweite des Systems ist somit auf jene Distanz begrenzt, in der das Erregerfeld noch genug Spannung in die Transponderantenne induzieren kann um den IC mit genügend Energie zu versorgen sowie diese Versorgung stabil zu halten. Diese Transponder können aufgrund dieser einfachen Bauweise, unter Berücksichtigung des verbauten ICs, äußerst kostengünstig produziert werden.

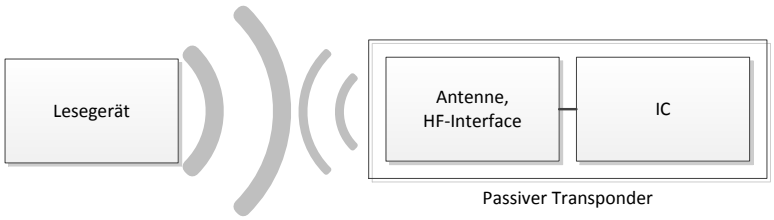


Abbildung 2.1: Schematische Darstellung eines passiven Transponders

Aktive Transponder

Transponder mit einer integrierten zusätzlichen Energiequelle, wie etwa Stützbatterien, werden als *aktive* Transponder bezeichnet (Abbildung 2.2). Der IC des Transponders wird von dieser Energiequelle gespeist und es ist daher nicht mehr notwendig, diese Energie aus dem Erregerfeld zu beziehen. Die Reichweite eines solchen Systems ist damit größer als bei passiven Transpondern bzw. das Erregerfeld kann bei gleicher Reichweite schwächer sein. Allerdings sind auch diese Transponder nicht in der Lage ein eigenes Feld aufzubauen. Die Kommunikation mit dem Lesegerät erfolgt somit wie bei passiven Systemen im HF-Bereich über das Feld des Lesegerätes mittels Lastmodulation. Solche Systeme werden gelegentlich auch als *semi-passiv* oder *semi-aktiv* bezeichnet, da die Kommunikation nach wie vor über das Erregerfeld des Lesegerätes erfolgt und die zusätzliche Energiequelle des Transponders darauf keinen Einfluss hat und lediglich der Versorgung des ICs dient.

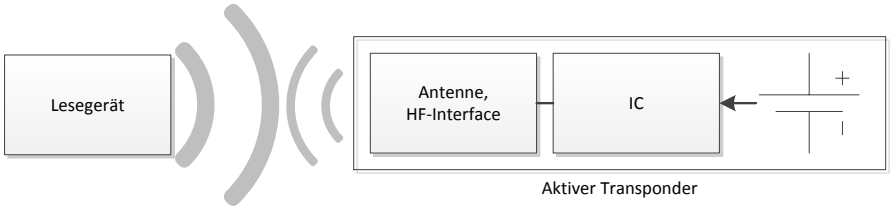


Abbildung 2.2: Schematische Darstellung eines aktiven Transponders

2.1.1 Funktionsweise von RFID-Systemen

Die Funktionsweise von RFID-Systemen lässt sich wie folgt vereinfacht beschreiben: Das Lesegerät erzeugt ein magnetisches Feld (bei induktiver Kopplung im Nahfeld), in welches ein Transponder eingebracht wird. Dadurch durchströmt dieses Wechselfeld die Antenne (das Koppelelement) des Transponders und induziert eine Spannung. Der bei geschlossener Spule fließende Strom versorgt den IC des Transponders und aktiviert ihn. Der Transponder selbst verfügt über einen Schwingkreis, dessen Resonanzfrequenz mit der Sendefrequenz des Lesegerätes übereinstimmt, wodurch es bei Parallelschwingkreisen durch Resonanz zu einer Stromüberhöhung kommt. Diese Anpassung des Transponders an die Resonanzfrequenz kann bei einigen Typen zusätzlich über einen externen *Tuning Kondensator* angepasst werden. Über Modulation des Erregerfeldes kann das Lesegerät Daten und Befehle an den Transponder übermitteln. Dieser wertet die gesendeten Daten und Befehle aus. Der Transponder erzeugt selbst kein Feld, sondern überträgt die Antwort durch Beeinflussung des Erregerfeldes. Das geschieht etwa durch an- oder abkoppeln eines Lastwiderstandes (Lastmodulation), welcher die Impedanz des Transponders verändert und das Erregerfeld beeinflusst, was wiederum vom Lesegerät detektiert werden kann.

2.1.2 Klassifizierung von RFID-Systemen

RFID-Systeme können anhand der Betriebsfrequenz, der Kopplungsart sowie der Reichweite unterschieden werden. Folgende Unterscheidungen sind möglich:

Close Coupling

Unter *close coupling* versteht man Systeme mit einer Reichweite von bis zu einem Zentimeter. Die Kopplung solcher Systeme erfolgt beispielsweise über ein elektrisches Feld. Der Transponder muss dazu in das Lesegerät eingebracht werden. Wird die Kopplung über ein elektrisches Feld erreicht, wie in Abschnitt 2.2.4, hat dies den Vorteil, dass die Betriebsfrequenz keinen Einfluss hat und eine Anpassung daher nicht nötig ist.

Remote Coupling

Unter *remote coupling* fallen Systeme mit einer Reichweite von bis zu einem Meter. Diese basieren auf einer magnetischen Kopplung zwischen Transponder und Lesegerät. Hierbei kommen Frequenzbereiche von LF bis HF zum Einsatz. Allgemein bekannt sind dabei zum Beispiel SmartCards, welche bei einer Resonanzfrequenz von 13,56 MHz operieren.

Long-Range Systems

Dabei handelt es sich um Systeme mit einer Reichweite über einem Meter sowie einer Betriebsfrequenz im UHF Bereich. Sie werden als *long-range systems* bezeichnet. Diese nutzen elektromagnetische Wellen zwischen Lesegerät und Transponder. Die Antennen werden als Dipole ausgeführt. Die Kommunikation vom Transponder zum Lesegerät erfolgt hierbei über das *backscatter*-Verfahren. Passive Transponder erreichen eine Reichweite von einigen Metern, aktive sogar bis zu 15 Meter.

Zusammenfassung

Die Reichweite hängt zusammenfassend von mehreren Faktoren ab:

- Betriebsfrequenz
- Größe und Art der Antenne (gerichtet, ungerichtet)
- Art des Objektes (elektrisch leitfähig oder nicht elektrisch leitfähig)
- Leistung des Lesegerätes
- Verwendung von Stützbatterien bei aktiven Transpondern

2.1.3 Physikalisches Funktionsprinzip

In Abbildung 2.3 ist ein Ersatzschaltbild eines RFID-Systems dargestellt. Auf der linken Seite befindet sich das Lesegerät mit der als L_{reader} bezeichneten Antenne, auf der rechten Seite der Transponder mit der als $L_{transponder}$ bezeichneten Antenne sowie der Tuning Kapazität C_{cap}. Ein Strom $i_1(t)$, der durch die Antenne des Lesegerätes fließt, hat ein magnetisches Feld zur Folge. Der allgemeine Zusammenhang zwischen dem Strom I, der Anzahl der Windungen N sowie des Radius R einer runden Spule, wie sie in RFID-Systemen verwendet wird, ist in [Fin03] beschrieben. Im Abstand x von der Spule, entlang der Spulenachse, kann die Feldstärke H mit Gleichung 2.1 berechnet werden und vereinfacht sich im Mittelpunkt der Spule ($x = 0$) wie in Gleichung 2.2 gezeigt. Für eine rechteckige Spule mit den Seitenlängen a und b berechnet sich die Feldstärke, ähnlich wie zuvor, nach Gleichung 2.3.

$$H = \frac{I \cdot N \cdot R^2}{2 \cdot \sqrt{(R^2 + x^2)^3}} \tag{2.1}$$

$$H = \frac{I \cdot N}{2 \cdot R} \tag{2.2}$$

$$H = \frac{I \cdot N \cdot a \cdot b}{4 \cdot \pi \cdot \sqrt{(\frac{a}{2})^2 + \frac{b}{2} + x^2}} \cdot \left(\frac{1}{(\frac{a}{2})^2 + x^2} + \frac{1}{(\frac{b}{2})^2 + x^2} \right) \tag{2.3}$$

Wird nun eine Leiterschleife, wie die Antenne eines RFID-Transponders, in dieses Feld eingebracht, wird eine Spannung induziert. Dabei muss man zwischen der Selbstinduktion in der Transponderantenne (Gleichung 2.4) und der Gegeninduktivität durch die Erregerspule (Gleichung 2.5) unterscheiden.

$$u_s(t) = L_2 \cdot \frac{di_2}{dt} \tag{2.4}$$

$$u_g(t) = M \cdot \frac{di_1}{dt} \tag{2.5}$$

Zusammengefasst ergibt sich daraus die induzierte Spannung (Gleichung 2.6). Die Gegeninduktivität M mit den Teilflüssen Φ_{12} und Φ_{21} kann mit Gleichung 2.7 berechnet werden.

$$u_2(t) = u_g(t) - u_s(t) = M \cdot \frac{di_1}{dt} - L_2 \cdot \frac{di_2}{dt} \tag{2.6}$$

$$M_{12} = \frac{\Phi_{12}}{i_2} = M_{21} = M \tag{2.7}$$

Diese Spannung $u_2(t)$ wiederum hat einen Strom $i_2(t)$ zur Folge, welcher den IC des Transponders versorgt. Durch Lastmodulation des ICs kann man den Strom $i_2(t)$ auf der Transponderseite beeinflussen.

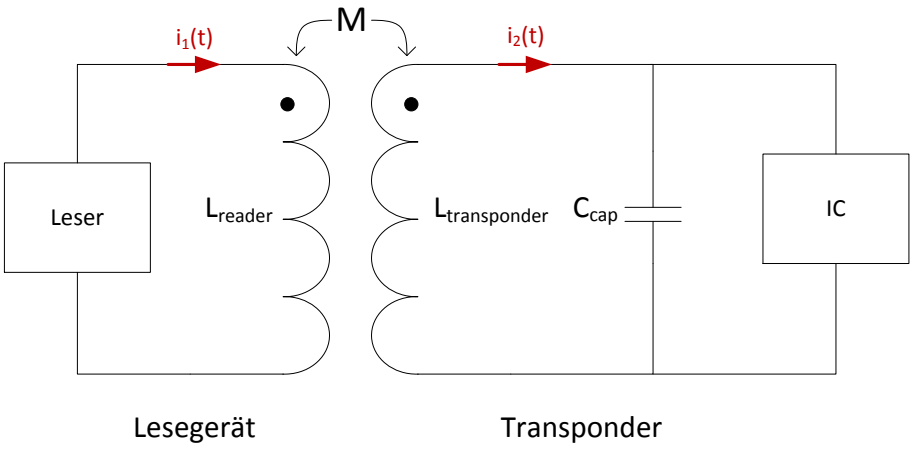


Abbildung 2.3: Ersatzschaltbild eines RFID-Systems

Resonanz

Wie in Abbildung 2.3 ersichtlich ist, besteht der Transponder aus einer als Spule ausgeführten Antenne, einem optionalen Tuning Kondensator sowie dem IC. Dieser IC kann elektrisch als ohmsch-kapazitiv angesehen werden, d.h. er besitzt eine Eigenkapazität C_{IC} sowie einen Wirkwiderstand. Somit bildet der Transponder einen Schwingkreis aus $L_{transponder}$, C_{cap} und dem IC. In einem Schwingkreis wird die Energie immer abwechselnd im elektrischen Feld des Kondensators und im magnetischen Feld der Spule gespeichert, sie pendelt (schwingt) dauernd zwischen diesen Bauteilen.

Durch Verluste in den nicht idealen Bauteilen sowie ohmschen Lasten im Schwingkreis wird die Schwingung allerdings gedämpft und klingt ohne Zuführung von Energie von außen mit der Zeit ab.

Die Berechnung der Resonanzfrequenz eines idealen Schwingkreises kann mit Gleichung 2.8 erfolgen.

$$f_{res} = \frac{1}{2 \cdot \pi \cdot \sqrt{L_{transponder} \cdot (C_{cap} + C_{IC})}} \tag{2.8}$$

Bei einem Parallelschwingkreis kommt es bei einer Resonanz zu einer Stromüberhöhung, was bei passiv betriebenen Transpondern erwünscht ist. Die genaue Abstimmung auf die Resonanzfrequenz hat somit eine große Relevanz. Die hier besprochene Anpassung kann mittels des Tuning Kondensators vorgenommen werden. Dieser dient einerseits dazu Toleranzen auszugleichen, andererseits aber auch, um die Gesamtkapazität des Schwingkreises zu beeinflussen und somit bei kleinen Transpondern die benötigte Anzahl an Windungen der Spule zu begrenzen. Die exakte Anpassung an eine vorgegebene Resonanzfrequenz ist aufgrund von Bauteil- sowie Fertigungstoleranzen allerdings sehr schwierig. Oft ist es nur möglich, sich der gewünschten Resonanzfrequenz anzunähern und die verbleibende Abweichung in Kauf zu nehmen.

2.2 Transponderarten und theoretische Ansätze

Jeder RFID-Transponder besteht immer aus einem IC sowie einem Koppelelement. Als Koppelelement dient in der Regel eine Antenne. Sie kann jedoch auf verschiedene Art und Weise ausgeführt sein und hat nicht nur einen starken Einfluss auf die finale Größe des gesamten Transponders, sondern auch auf sein Verhalten.

2.2.1 ID-1 Format

In der ISO/IEC 7810 [ISO13c] werden vier Formate für Identitätsdokumente festgelegt. Eines davon ist das 85,60 mm x 53,98 mm große ID-1 Format, umgangssprachlich auch „Scheckkartenformat“ genannt. Mit RFID-Funktionalität ausgestattet, werden solche Karten häufig als kontaktlose Zugangskarten verwendet.
Die ISO/IEC 14443-1 [ISO13a] spezifiziert hierbei die physikalische Charakteristik und ISO/IEC 14443-4 [ISO13b] das Übertragungsprotokoll für solche Identitätskarten. Sie arbeiten mittels induktiver Kopplung im HF-Bereich bei 13,56 MHz. Aufgrund der großen Antenne ist eine Lesereichweite von ca. 1 m möglich [Fin03]. Der Chip wird dabei mit der Antenne verlötet und zwischen PVC Folien eingeschweißt. Abbildung 2.4 zeigt den Aufbau einer solchen Karte schematisch. Dieses Format eignet sich aufgrund der Maße und des Aufbaus nicht für eine Integration in kleine Objekte. Transponder in diesem Format bieten jedoch eine gute Lesereichweite und sind im alltäglichen Gebrauch leicht ohne technische Hilfsmittel handhabbar.

Um kontaktloses Bezahlen zu ermöglichen, werden Bank- oder Kreditkarten zusätzlich mit einem kontaktlosen Interface ausgestattet[5]. Die zusätzlich benötigte Antenne lässt sich sehr einfach im bestehenden Kartendesign integrieren.

[5] `http://www.maestrocard.com/at/privatkunden/innovation_kontaktlos.html`

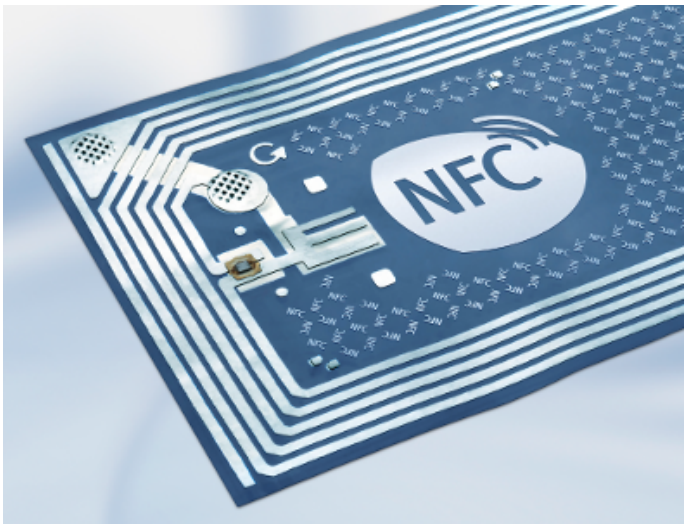


Abbildung 2.4: Aufbau einer ID-1 Karte (©Infineon Technologies AG, www.infineon.com)

2.2.2 Booster-Antennen zur Reichweitenvergrößerung

Booster-Antennen können verwendet werden um die Reichweite von Tags mit integrierter Antenne (vgl. hierzu Abschnitt 2.2.3) zu erweitern. Sie konzentrieren das magnetische Feld auf eine kleinere Fläche. In [PBHH13] wird ein solches System dargestellt. Dabei wird ein unter $1mm^2$ großer HF-Transponder mit einer Resonanzfrequenz von 13,56 MHz verwendet. Dieser hat eine Lesereichweite von rund 2mm. Verwendet man nun zusätzlich eine externe Antenne, wie zum Beispiel in [PBHH13] gezeigt wird, kann die Lesereichweite erheblich gesteigert werden, im gezeigten Fall von 2mm auf rund 1m. Somit kann unter Beibehaltung der kompakten Bauweise des Transponders bei Bedarf die Reichweite erhöht werden.

CoM[6] Systeme wie unter Abschnitt 2.2.5 nützen dieses Verfahren. Es kann damit aber auch die Reichweite anderer miniaturisierter RFID-Transponder, falls notwendig, erweitert werden.

Gedruckte Antennen und Ferrit

Antennen für RFID-Tags als auch für Booster-Antennen können auf verschiedene Arten hergestellt werden. Eine Möglichkeit ist es sie gleich auf das Trägermaterial zu drucken. Um Antennen in metallischen Umgebungen einsetzen zu können, wird in der Regel Ferrit eingesetzt, welche den Tag vom metallischen Untergrund abschirmt. Ein Verfahren welches beide Eigenschaften kombiniert, wird in [PGB+14b] gezeigt. Dabei druckt man eine Antenne mit Silbertinte direkt auf Ferrit und Fotopapier. Die so erzeugten Antennen sind nicht nur sehr dünn (ca. $100\mu m$) sondern schirmen bei Verwendung von Ferrit die Antenne auch vom eventuell vorhandenen metallischen Untergrund ab.

Um diese Eigenschaft zu demonstrieren, wird dafür im vorgestellten Fall eine Kupferschicht unter der Antennen angebracht.

[6] Coil-on-Module

Ohne Ferrit muss ein vertikaler Abstand von rund 1,4 cm zwischen Kupfer und Antenne eingehalten werden, um die Interferenzen zu minimieren und den Chip auslesen zu können. Mit Ferrit kann diese Lücke kleiner sein oder ganz entfallen.

Eine alternative Möglichkeit, um Batterien mit konventionellen Antennen und Ferrit zu markieren, wird in [JK15] gezeigt.

Wie allerdings in [GNSW11] dargestellt wird, erkauft man sich diese Schirmung mit einer höheren minimalen Feldstärke, es ist daher mit Ferrit eine höhere magnetische Feldstärke notwendig, damit der Chip funktioniert.

2.2.3 Coil-on-Chip

Bei CoC[7] Systemen wird die Antenne direkt als oberste Schicht auf den Chip gepackt. Die Spule wird dabei direkt als Silizium oder Kupferlage auf den Isolator der Chipoberseite aufgebracht und mittels Durchkontaktierungen durch den Isolator mit den Anschlüssen des ICs verbunden. Die Fertigungsschritte sind in Abbildung 2.5 anhand einer zweilagigen Spule zu sehen.

Zuerst wird eine Schicht Dielektrikum aufgebracht, wobei die Anschlusspads des Chips freigelassen werden. Danach wird die erste Verteilungsschicht aufgebracht, welche mit den Chippads verbunden sind. Danach folgt eine weitere Dielektrikumsschicht sowie die zweite Verteilungsschicht. Zum Abschluss wird nochmals eine Dielektrikumsschicht als oberste Lage aufgebracht.

Der fertige Tag hat somit lediglich die Abmessungen des Chips. Die Abmessungen des ICs sind somit maßgeblich entscheidend für die maximal mögliche Größe der Antenne. Da diese in der Regel sehr gering sind, ist somit auch die Antenne sehr klein, was zu einer sehr geringen maximalen Lesedistanz führt, oder aber ein sehr starkes magnetisches Feld des Lesegerätes erfordert. Zusätzlich stört die metallische Beschaffenheit des ICs das Feld und schwächt es zusätzlich, die Antenne selbst hat aufgrund des Fertigungsprozesses ebenfalls einen höheren ohmschen Widerstand als konventionelle Antennen.

Solche Tags können somit nur sehr schwer von integrierten mobilen Lesern mit geringer Feldstärke, wie zum Beispiel Smartphones, ausgelesen werden. Selbst wenn das Lesegerät des Smartphones ein ausreichend großes magnetisches Feld aufbauen kann, muss trotzdem etwa die Position der Spule im Smartphone bekannt sein und der Tag direkt darauf abgelegt werden, um eine Kommunikation zu ermöglichen.

Dual-Band Chip

Die Reichweite von UHF-Tags ist im Vergleich zu ähnlichen HF-Tags größer. Um also die Reichweite von sehr kleinen Tags zu steigern, kann man daher etwa vom HF-Band in das UHF-Band wechseln. Um die Kompatibilität mit den weit verbreiteten HF-Systemen nicht zu verlieren, können beide Systeme auf einem Chip untergebracht werden. In [PGB+14c] wird ein solcher Chip mit zwei Antennen vorgestellt. Er verfügt auf einer Fläche von $1,32mm^2$ sowohl über eine HF-Antenne für 13,56 MHz als auch eine UHF-Antenne für 868 MHz.

[7] Coil-on-Chip

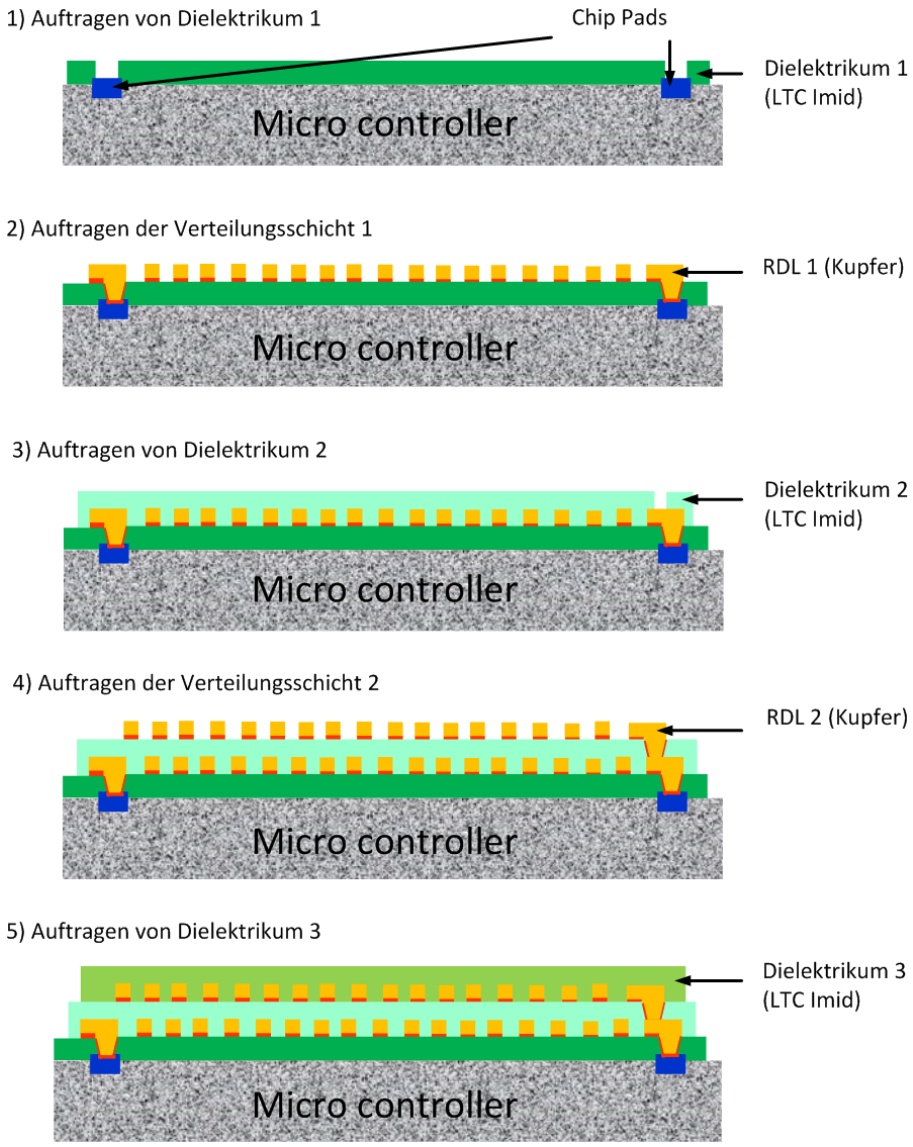


Abbildung 2.5: Coil-on-Chip Fertigungsprozess aus [Pac15]

Mit dieser Dual-Band Lösung werden Lesereichweiten von 2,5mm im HF, sowie 4,4mm im UHF-Betrieb erreicht.

2.2.4 Ansätze mit kapazitiver Kopplung

Zusätzlich zur weit verbreiteten induktiven Kopplung kann die Energie und Informationsübertragung auch kapazitiv erfolgen, wie unter Abschnitt 2.1.2 bereits dargestellt wurde. Als Koppelelement dienen hierbei Elektroden und keine Antennen. Die Übertragung der benötigten Energie von einem System zum anderen erfolgt dabei durch die gegenseitige elektrische Kapazität.

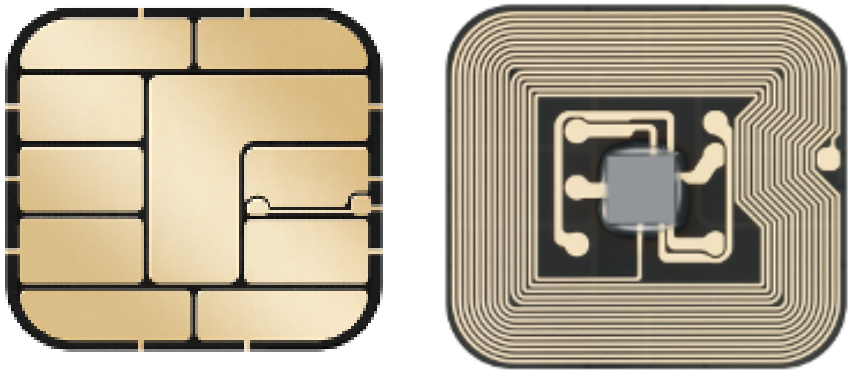
Allerdings sinkt diese elektrische Kapazität mit steigendem Abstand, wodurch eine erfolgreiche Kommunikation nur bei sehr geringer Distanz möglich ist. Eine Anpassung auf eine bestimmte Resonanzfrequenz ist nicht notwendig, außerdem haben metallische Oberflächen keinen so großen Einfluss wie bei induktiver Kopplung.
Diese können somit ohne Anpassung auch auf Metall eingesetzt werden.

Ein solcher Tag erhält eine zusätzliche Metallschicht als oberste Chiplage, diese dient als eine Elektrode des Kondensators. Das Chipsubstrat selbst dient als zweite Elektrode. Um den Tag auszulesen, muss er zwischen den beiden Elektroden des Lesegerätes platziert werden. Dieser nötige Aufbau schränkt die Anwendungsgebiete allerdings erheblich ein.

Da auf diese Art nur wenig Energie übertragen werden kann, sind nur geringe Lesereichweiten möglich wie in [PGB+14a] gezeigt wird. Beispielsweise sind beim gezeigten $1mm^2$ großen Tag bei niedrigen Frequenzen (HF 13,56 MHz) rund $200\mu m$ und bei höheren Frequenzen (UHF 868 MHz) rund $400\mu m$ möglich.

2.2.5 Coil-on-Module

Bei herkömmlichen Dual-Interface Karten wie zum Beispiel Bankkarten mit integrierter RFID-Funktion ist zusätzlich zur kontaktlosen eine kontaktbehaftete Kommunikation möglich. Das Modul benötigt somit zusätzlich zu den Anschlüssen für die Antenne noch jene für die kontaktbasierte Kommunikation. Diese doppelte Ausführung führt allerdings zu mechanischer Beanspruchung an der Lötstellen der Antenne. CoM basierte Module haben deshalb auf der Vorderseite die Pads für die kontaktbasierte Kommunikation wie in Abbildung 2.6a dargestellt und auf der Rückseite eine integrierte Antenne, dargestellt in Abbildung 2.6b.



(a) Vorderseite (b) Rückseite

Abbildung 2.6: Coil-on-Module (©Infineon Technologies AG, www.infineon.com)

Weiters kann man hier den eigentlichen IC in der Mitte deutlich erkennen. In Kombination mit einer herkömmlichen Antenne im ID-1 Format als Booster-Antenne, wie in Abbildung 2.7 dargestellt, ergibt sich eine Kopplung der beiden Antennen und ein Wegfall der Lötverbindung zur Antenne. Dieses System ist somit mechanisch robuster sowie einfacher und billiger zu fertigen.

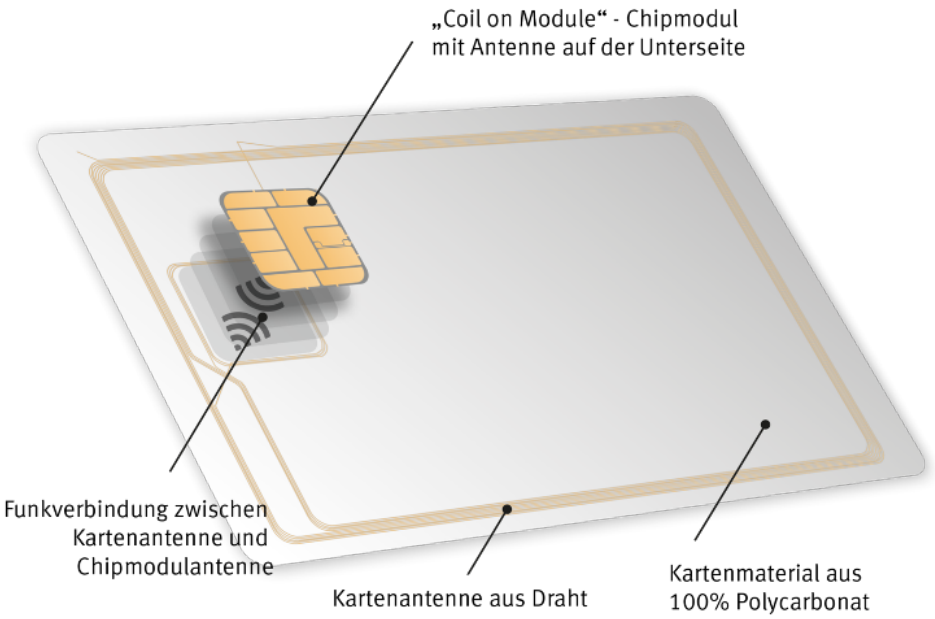


Abbildung 2.7: Coil-on-Module kombiniert mit einer ID-1 Karte (©Infineon Technologies AG, www.infineon.com)

2.2.6 Implantierbare Tags

Zusätzlich zum starren Aufbau gibt es auch flexible Antennen wie in [LRT08] gezeigt wird. Hierbei wird ein RFID-Chip in ein Silizium Gehäuse verbaut und mit einer Schicht aus Parylene bedeckt. Auf dieser Kunststoffschicht wird eine Antenne aufgebracht. Am Ende wird der gesamte Tag mit Parylene versiegelt. Mit diesem Ansatz ist es auch möglich, zusätzliche Bauteile in den Transponder zu integrieren. Parylene sind resistent gegen organische Medien und somit wäre es möglich einen solchen Tag zu implantieren. Bei einer Frequenz von 125 kHz erreicht der rund $1mm^2$ große Chip mit seiner 2x2cm großen Antenne eine Lesereichweite von bis zu 4mm.

Zu erwähnen sind in diesem Zusammenhang noch Glastransponder mit gewickelter Antenne [Fin03]. Diese Tags werden seit längerer Zeit zum Beispiel bei der Identifikation von Tieren verwendet. Dabei wird die Antenne um einen Kern gewickelt und gemeinsam mit dem RFID-Chip in eine Glasröhre verbaut. Diese Glastransponder gibt es in verschiedenen Varianten mit Durchmessern von ca. 2-4mm und Längen von 8-30mm.

2.3 Kommerzielle Produkte

In diesem Abschnitt werden einige bereits kommerziell erhältliche miniaturisierte RFID-Tags vorgestellt. Dabei werden nur Tags mit integrierter Antenne berücksichtigt.

2.3.1 Maxell

Hitachi Maxell, Ltd. hat zwei miniaturisierte Transponder mit integrierter Antenne im Angebot.

CoC

Mit den ME-Y1001/ME-Y2000 Serien [Maxa] hat Maxell RFID-Tags in Coil-on-Chip Bauweise im Portfolio, welche mit 2,5x2,5mm sehr klein sind. Bedingt durch diese geringen Abmessungen beträgt die Kommunikationsdistanz nur rund 1-3mm je nach Position der Antenne. Zwar funken diese Tags auf der HF-Frequenz von 13,56 MHz, verwenden allerdings ein proprietäres Kommunikationsprotokoll. Dadurch soll sichergestellt werden, dass nur berechtige Lesegeräte mit den Tags kommunizieren können. Diese Baureihe unterstützt die Vergabe eines Passwortes als einzigen Schutz. Maxell bietet auch Booster-Antennen an, um die Reichweite der Tags auf 1cm bis 2cm zu steigern. Um den Speicherplatz zu erhöhen, könnten so einige CoC-Tags auf einer Booster-Antenne untergebracht werden.

Miniatur RFID-Tags

Zusätzlich zu den oben genannten CoC basierten Tags gibt es größere Tags, welche Ferrit als Antennensubstrat verwenden [Maxb], welches die Tags kompatibel mit Metalloberflächen macht. Diese gibt es in 2 Baugrößen: rund 10x3mm und 5x3mm (Abbildung 2.8), mit einer Höhe von 2,2mm sind sie allerdings sehr dick. Die Kommunikationsdistanz gibt Maxell mit <19mm beim 5x3mm auf Nichtmetall und <34mm beim 10x3mm auf Metall an.

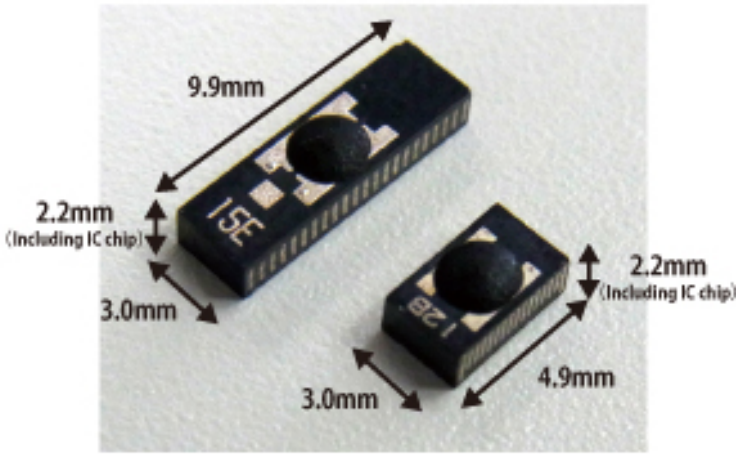


Abbildung 2.8: Maxell Miniatur RFID Tags (©Hitachi Maxell, Ltd., biz.maxell.com)

Standardmäßig verbaut Maxell hier I-CODE SLI ICs von NXP Semiconductors. Zur Absicherung der Daten können lediglich Passwörter verwendet werden.

2.3.2 Murata

Murata bietet mit der Magicstrap Serie ebenfalls kleine RFID-Tags an.

Magicstrap Single

Mit der HF-Single Serie [Murb] hat Murata mehrere Tags im HF- und UHF-Bereich im Angebot. Die beiden Tags im HF-Band sind 3,2x3,2mm groß und weisen je nach verbautem IC eine Lesereichweite von 12-15mm auf. Für das UHF-Band gibt es ebenfalls 2 Tags mit 3,2x1,6mm und 2,0x1,2mm Außenmaßen und einer Lesereichweite von 6-7mm.

Magicstrap Inlay

Zusätzlich zu den oben genannten kleinen Tags existiert noch ein größerer mit 8,3x8,3mm [Mura]. Dieser kann aufgrund seiner Größe und der damit verbundenen Lesereichweite von 25mm von Smartphones ausgelesen und beschrieben werden.

Sicherheit

Murata verbaut bei den oben genannten Produkten standardmäßig einen IC der NTAG Serie der Firma NXP Semiconductors. Wie viele andere Produkte unterstützen diese einen Passwortschutz für den Speicherinhalt. Zusätzlich bieten diese aber auch eine sogenannte *originality signature*. Diese basiert auf asymmetrischer Kryptografie und dient dazu, unbefugte Kopien von NTAG basierten Tags zu erkennen. Dazu wird während der Produktion die UID des IC mittels des privaten Schlüssels des Herstellers signiert und diese Signatur auf dem Tag gespeichert. Während der Verifikation wird dann diese Signatur zusammen mit der UID übertragen. Durch den dazugehörigen öffentlichen Schlüssel des Herstellers kann dann die Signatur des Tags entweder online oder offline überprüft werden.

Diese Funktion dient allerdings lediglich dazu, die Echtheit des Tags zu gewährleisten. Eine logische Verbindung des Tags mit dem Produkt existiert nicht, ebenso kann die Integrität der Daten bzw. der Kommunikation dadurch nicht gewährleistet werden.

2.4 eWLB-Technik

2.4.1 eWLB-Grundlagen

Unter eWLB[8] versteht man ein Packaging Verfahren für ICs, erstmals vorgestellt in [BMO+08]. Ihr zugrunde liegt das *Ball Grid Array*, eine Packaging Variante bei der die Anschlusspads auf der Unterseite von ICs mit Bällen aus Lötpaste versehen werden um sie damit auf Leiterplatten löten zu können. Diese Bälle sind dabei wesentlich größer als das darunter liegende Pad. Bei sehr kleinen ICs ist die zur Verfügung stehende Fläche gering.

[8] embedded Wafer Level Ball Grid Array

Da aber die Lötbälle eine gewisse Mindestgröße sowie einen Mindestabstand untereinander haben müssen (das *Ball Grid*) folgt daraus, dass nur so viele Anschlusspads möglich sind wie es das Ball Grid zulässt.

Um dennoch mehr Anschlusspads bei gleich großer Siliziumfläche unterbringen zu können wurde das embedded Wafer Level Ball Grid Array entwickelt. Dabei wird die zur Verfügung stehende Fläche mittels einer Vergussmasse (*mold compound*) vergrößert da Silizium als zusätzliche Fläche zu teuer wäre. So kann der eigentliche IC so klein wie möglich hergestellt werden.

Am Beginn der Herstellung werden die fertigen ICs aus dem Silizium Wafer gesägt bzw. aus ihrer Verpackung entnommen und in vorbestimmten Abständen mittels doppelseitigem Klebeband auf einen Metallträger (*Handlingwafer*) aufgeklebt, wobei die Anschlusspads des ICs nach unten zeigen müssen. Danach wird dieser Handlingwafer mit einer Vergussmasse versehen. Nach dem Aushärten wird der Metallträger wieder entfernt. Die Chipfläche wird als *Fan-In*, die Vergussmasse als *Fan-Out* bezeichnet wie in Abbildung 2.9 dargestellt ist.

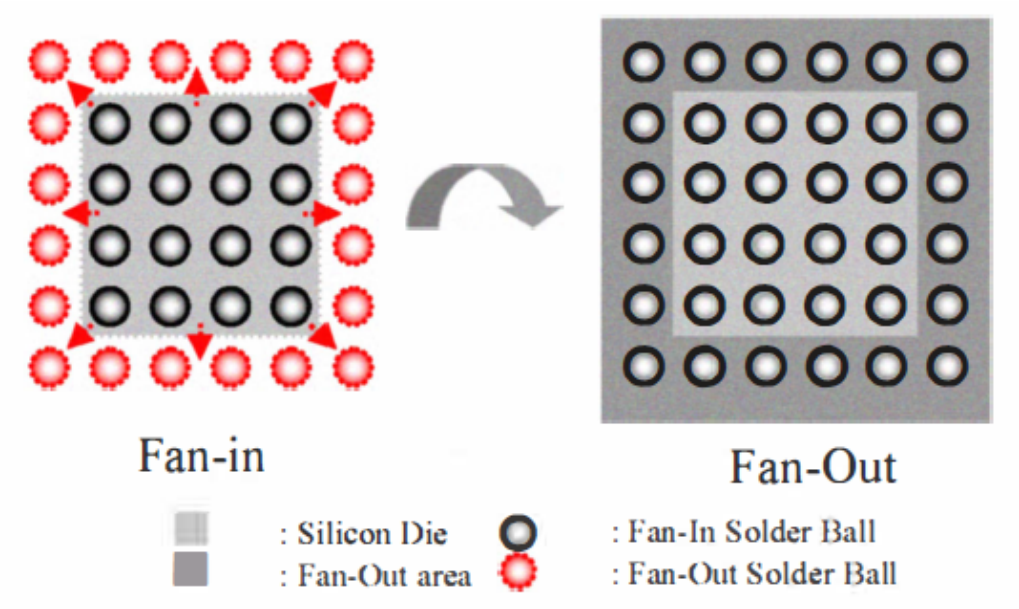


Abbildung 2.9: eWLB-Package aus [BMO+08]

Anschließend wird darauf eine Dielektrikumsschicht aufgebracht, wobei die Anschlusspads auf dem IC frei bleiben (Durchkontaktierungen zur nächsten Schicht). Darauf wird dann in Dünnschichttechnik die RDL[9] (Verteilungslage) aufgebracht, welche die Anschlusspads des ICs mit den Lötbällen verbindet.

Die Pads werden somit auf der gesamten Fläche neu verteilt. Nachdem eine weitere Dielektrikumsschicht als Isolator hinzugefügt wurde, können dann die Lötbälle angebracht werden. Ein Schnitt durch ein eWLB-Package ist in Abbildung 2.10 dargestellt. Zum Schluss werden die einzelnen Chips noch aus dem Handling Wafer gesägt (vereinzelt). Die einzelnen Schritte sind in Abbildung 2.11 grafisch dargestellt.

[9]Redistribution Layer

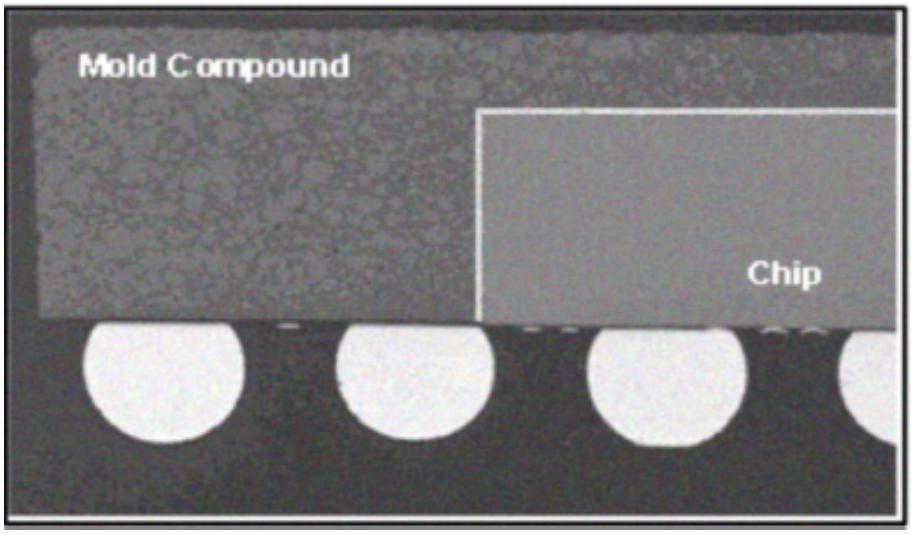


Abbildung 2.10: Schnitt durch ein eWLB-Package aus [BMO+08]

2.4.2 eWLB bei SCAD

Wie in Unterabschnitt 2.4.1 beschrieben, dient die RDL dazu, die Anschlusspads des ICs mit den Lötbällen auf der gesamten Package Fläche zu verbinden. Im Zuge des SCAD Projektes wird diese RDL dazu verwendet den IC mit einem Kondensator zu verbinden sowie als Antenne des RFID-System zu fungieren (CoE[10]).

Hierzu werden zuerst der IC, ein Kondensator sowie eine eventuell nötige Untertunnelung auf einem Handlingwafer platziert. Als Untertunnelung dient dabei ein metallisiertes Plättchen. Die exakte Ausrichtung der Bauteile untereinander spielt hierbei eine große Rolle. Da die Anschlusspads wie auch die Durchkontaktierungen durch die Dielektrikumsschicht nur eine sehr geringe Größe aufweisen, müssen die Positionen genau stimmen. Diese Bauteile werden dann mit einer gemeinsamen Vergussmasse versehen. Darauf wird mittels der RDL eine Antenne platziert. Als Antennensubstrat dient hier die Vergussmasse. Im Vergleich zum herkömmlichen eWLB-Fertigungsprozess aus Abbildung 2.11 wird das Aufbringen der Bälle aus Lot (Schritt 7) weggelassen sowie die oberste Dielektrikumsschicht vollständig, d.h. ohne die Durchkontaktierung für die Verbindung der Lötbälle mit der RDL, ausgeführt. Der gesamte Tag hat somit eine Dicke <1 mm.

Mehr zu den verwendeten ICs sowie den Designs folgt in den weiteren Kapiteln.

2.5 Gegenüberstellung der Bauarten

Am Ende dieses Kapitels werden die in den vorherigen Abschnitten vorgestellten Verfahren sowie Produkte nochmals gegenüber gestellt und verglichen.

In Tabelle 2.1 wird der in dieser Arbeit verwendete Fertigungsprozess mit den gezeigten Fertigungsverfahren verglichen. Gegenübergestellt werden dazu die Größe der Tags, ihre voraussichtlich erzielte Reichweite sowie ihre HF-Eigenschaften und ob das Verfahren eine Integration von zusätzlichen Bauteilen zulässt.

[10] Coil-on-Embedding

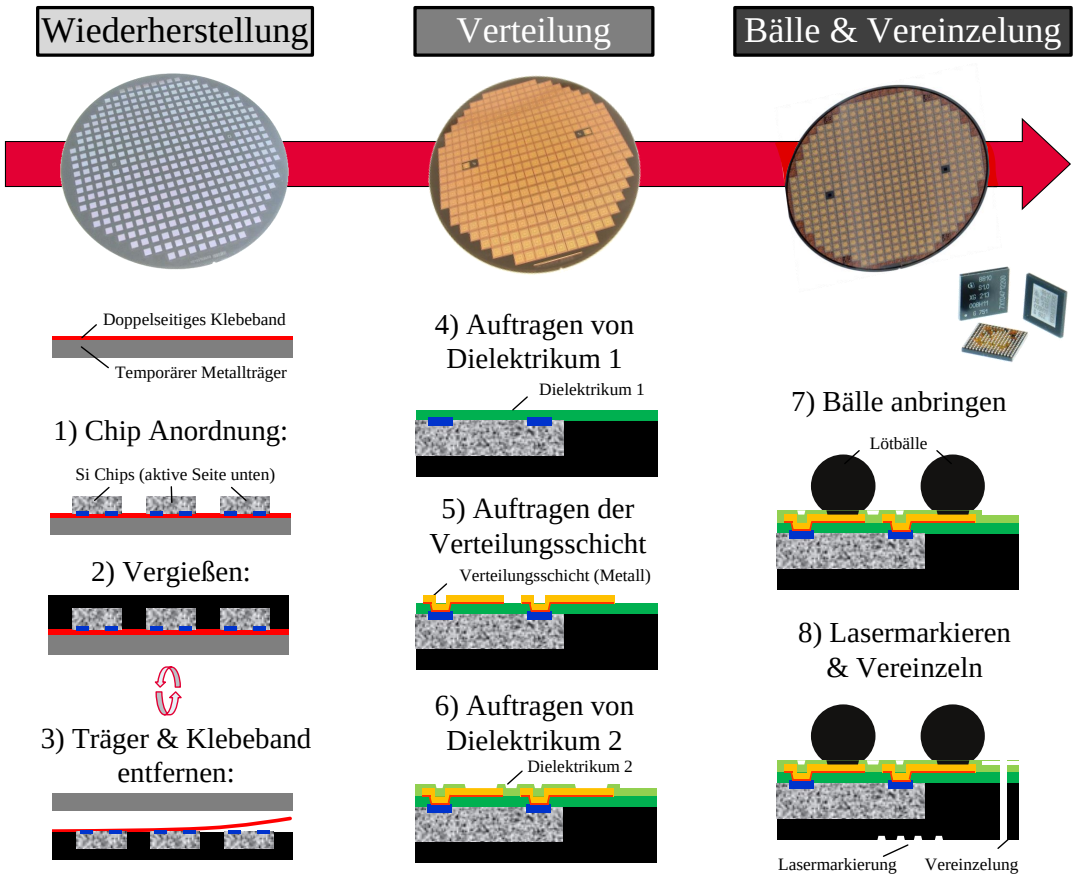


Abbildung 2.11: eWLB-Fertigungsprozess aus [Pac15]

In Tabelle 2.2 werden die in dieser Arbeit vorgestellten Tags mit bereits erhältlichen Produkten hinsichtlich ihrer Größe, Reichweite, eventuell vorhandenen Sicherheitsfunktionen sowie ihrer Nutzbarkeit in metallischen Umgebungen verglichen.

Hierbei wird ein einfacher Passwortschutz von Speicherbereichen nicht als Sicherheitsfunktion gewertet. Diese werden in Tabelle 2.2 mittels * gekennzeichnet.

	Größe	**Kommunikations-reichweite**	**Zusätzliche Komponenten**	**HF-Eigenschaften**
ID-1	--	++	✓	+
CoC	++	-	X	--
Kapazitive Kopplung	++	--	X	o
CoM	o	o	X	o
Parylene Tag	-	o	✓	+
eWLB	**+**	**o**	✓	**++**

Tabelle 2.1: Vergleich von eWLB mit den vorgestellten Fertigungsprozessen

	Größe	**Kommunikations-reichweite**	**Metallische Umgebungen**	**Sicherheits-funktionen**
Maxell CoC	+	o	X	X
Maxell Mini	o	+	✓	X
Murata Single	+	+	X	✓*
Murata Inlay	o	+	X	✓*
SCAD	**+**	**o**	✓	✓

Tabelle 2.2: Vergleich von SCAD-Tags mit bereits kommerziell verfügbaren Produkten

Kapitel 3

Konzept und Design

Das vorliegende Kapitel stellt den Projektablauf vor. Es beinhaltet die Definitionen der Anforderungen an die verschiedenen SiP[1], sowie die Überführung in die Designparameter. Anschließend werden die verwendeten RFID-ICs, sowie einige ihrer Eigenschaften vorgestellt. Am Ende dieses Kapitels werden die Designs der Android App sowie der PC-Demo gezeigt.

3.1 Projektablauf

Der Projektablauf gliedert sich in folgende Punkte:

- Einarbeitung in die Entwicklungswerkzeuge
- Festlegung der Designkriterien
- Auswahl der ICs
- Entwicklung der Designs mittels ADS[2]
- Simulation der Designs mittels ADS
- Analyse und Simulation des Verhaltens der Designs auf unterschiedlichen Grundmaterialien
- Vorbereitung und Übergabe der fertigen Varianten an die Fertigung
- Erstellen eines Demonstrators um die Funktionalität der Tags zu demonstrieren
- Verifizierung und Messung der gefertigten Tags
- Erstellung der Dokumentation sowie Präsentation

[1] System-in-Package
[2] Advanced Design System

Zu Beginn erfolgt eine Literaturrecherche, um den aktuellen Stand der Technik festzustellen und ähnliche Projekte und Produkte aufzuzeigen. Danach erfolgt die obligatorische Einarbeitung in die benötigten Entwicklungswerkzeuge wie ADS (siehe Kapitel 4.1) oder HFSS[3] (siehe Kapitel 4.2). Basierend auf den Ergebnissen der Literaturrecherche, sowie den Vorgaben seitens des Projektes, werden die Designparameter sowie die Ziele festgelegt. Mit diesen Informationen können die ICs ausgewählt werden, welche die zuvor festgelegten Parameter erfüllen. Nun können die unterschiedlichen Designs implementiert, sowie mit multiplen Simulationen formal verifiziert werden. Mit Hilfe dieser Resultate werden mit der Fertigung vorab etwaige Probleme und Verbesserungsvorschläge besprochen und die Änderungen in die Designs eingepflegt. Wenn die Entwürfe korrekt sind, werden sie an die Fertigung übergeben. Sobald dann die fertigen Prototypen vorliegen, werden diese vermessen und auf korrekte Funktion getestet. Zudem werden parallel Demos, entwickelt um die Funktionsweise der Prototypen zu zeigen.

Durch die gelegentliche, zeitliche Überlappung der oben genannten Punkte, wird in Abbildung 3.1 eine schematische Darstellung des Ablaufs gezeigt.

3.2 Anforderungsdefinition

In Kapitel 1 wird in Abbildung 1.1 ein prädestiniertes Einsatzszenario dargestellt. Dieses Szenario zeigt ein Smartphone, welches mit einem Tag kommuniziert um einen Authentifizierungsprozess durchzuführen. Betrachtet man dieses Beispiel lassen sich folgende Anforderungen an die Tags ableiten:

- Sie müssen **robust** gegenüber äußeren Einflüssen sein, da es sich bei den Objekten um Gegenstände des täglichen Gebrauchs handelt und diese diversen Einwirkungen wie Staub, Wasser, etc. ausgesetzt werden.
- Sie müssen auf **metallischen Oberflächen** funktionieren. Da Edelmetalle elektrisch leitfähige Materialien sind, müssen die Tags von diesen Materialien mit geeigneten Mitteln, wie etwa integrierten Ferriteinlagen, abgeschirmt werden.
- Es muss möglich sein zusätzliche **Bauelemente** zu **integrieren**, um auf geänderte Umstände, wie etwa andere ICs, spezielle Einsatzgebiete etc., reagieren zu können.
- Die Kommunikation muss **gesichert** sein, um einerseits die Integrität der Daten auf dem Tag zu schützen und andererseits die Authentifizierung des Tags zu ermöglichen.
- Sie müssen über ein gutes **Ansprechverhalten** verfügen, damit sie mit einem Smartphone ausgelesen werden können. Dies setzt einen geringen Energiebedarf des IC voraus.
- Die **Größe** soll variiert werden, da auf größeren Objekten größere Tags zum Einsatz kommen können, welche über eine höhere Reichweite verfügen oder bei gleicher Reichweite einen IC mit höheren Energiebedarf beinhalten können.
- Sie müssen **flach** genug sein um die Oberflächen jener Objekte, auf denen sie eingesetzt werden, möglichst wenig zu beeinflussen.

[3] High Frequency Structural Simulator

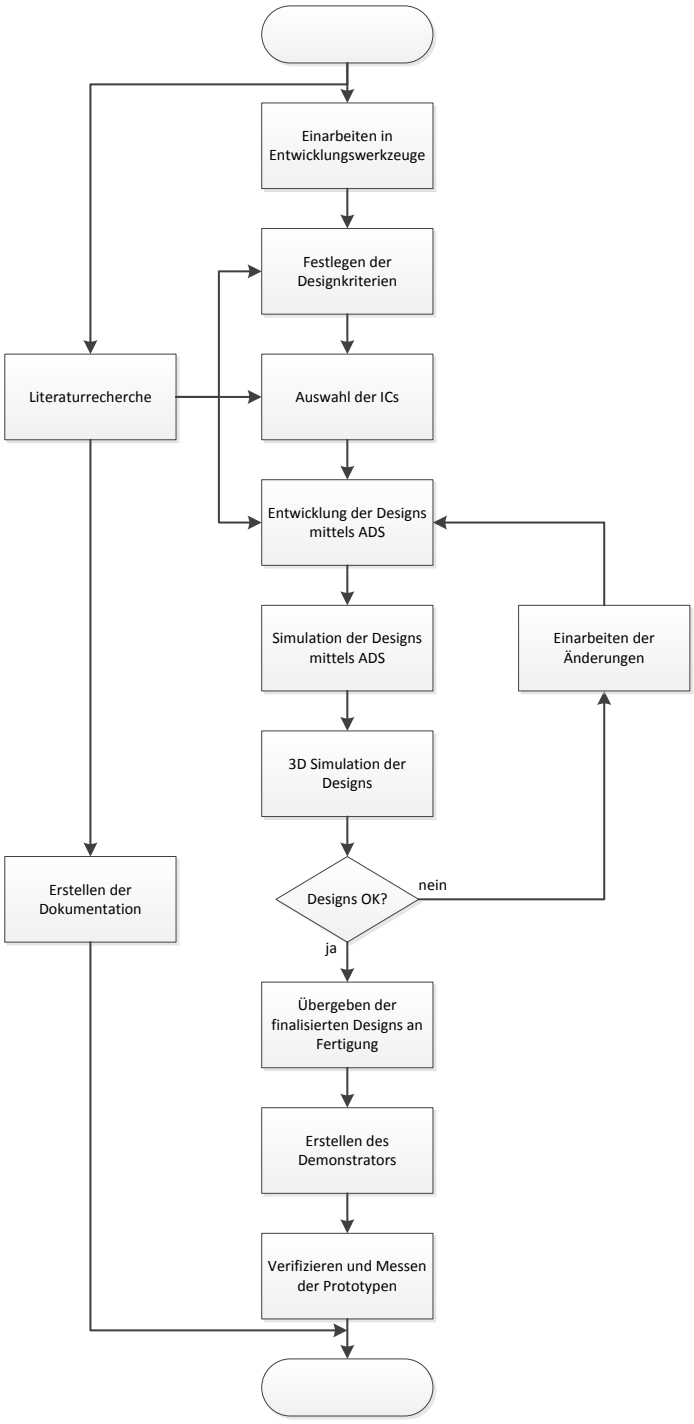


Abbildung 3.1: Schematischer Ablauf des Projektes

3.3 Designparameter

Um verschiedene Aspekte im Bezug auf Funktionalität, Anpassung der Spule und Größe des fertigen Packages zu beleuchten, werden unterschiedliche Designs erstellt. Diese Designs können mittels eines flexiblen Fertigungsprozesses leicht umgesetzt werden.

Im Allgemeinen beziehen sich diese Varianten auf:

1. *Hinzufügen eines Kondensators*: Es wird ein zusätzlicher Kondensator C_{Cap} mit einer Nominalkapazität von 100 pF hinzugefügt, um die benötigte Anzahl an Windungen für die Anpassung an 13,56 MHz klein zu halten. Sollte der IC selbst bereits über eine ausreichend hohe Eigenkapazität verfügen, kann dieser zusätzliche Kondensator entfallen. In Summe soll die Gesamtkapazität des Tags ungefähr 100 pF betragen.

   Dieser zusätzliche Kondensator wird mit den beiden Chippads und der Spule parallel verschalten, wie das Ersatzschaltbild in Abbildung 3.2 zeigt. Hierbei wird die Eigenkapazität der Chips als C_{Chip} und die zusätzliche Kapazität durch den diskreten Kondensator als C_{Cap} bezeichnet. Die Spule selbst wird durch ihre Induktivität L_A sowie ihren elektrischen Widerstand R_A der Windungen abstrahiert. Die Spule bildet mit den Kapazitäten somit einen Parallelschwingkreis.

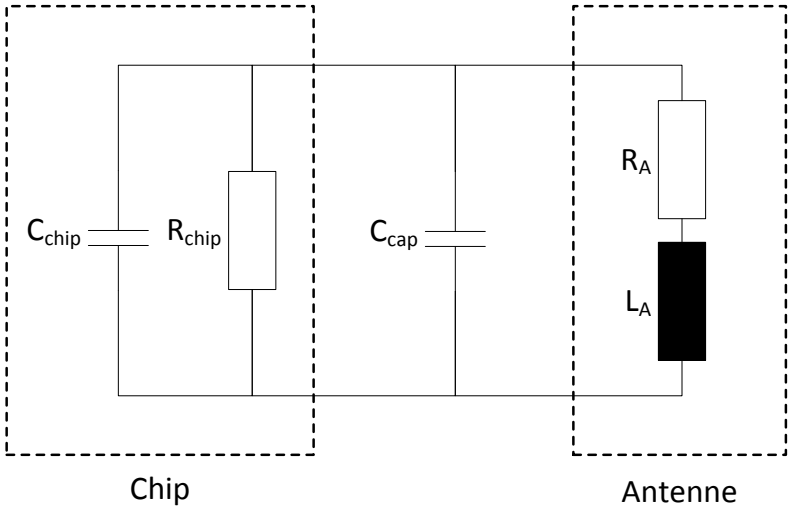


Abbildung 3.2: Ersatzschaltbild der Tags

2. *Anzahl der Spulenlagen*: Wenn auf den zusätzlichen Kondensator verzichtet wird und nur die Eigenkapazität des ICs zur Verfügung steht, ist eine höhere Anzahl an Windungen notwendig, um trotzdem die erforderliche Anpassung an 13,56 MHz zu erreichen. Bei größeren Packages kann der zur Verfügung stehende Platz ausreichend sein um die Spule trotzdem auf einer Lage unterzubringen. Bei kleineren Packages kann es jedoch notwendig sein, die Spule auf mehrere Lagen aufzuteilen.

3. *Variation der Spulenbreite*: Die Breite der Spule beträgt standardmäßig 20μm. Diese Spulenbreite wird bei einigen Varianten auf 40μm verdoppelt.

   Der ohmsche Widerstand des Leiters errechnet sich aus dem spezifischen Widerstand ρ, sowie der Länge l und dem Querschnitt A der Spule.

$$R = \rho \cdot \frac{l}{A} \tag{3.1}$$

$$Q = \frac{X}{R} \tag{3.2}$$

   Der spezifische Widerstand ρ, die Länge l sowie die Dicke mit 8 μm sind bei beiden Varianten aufgrund des selben Fertigungsprozesses und der selben Fertigungsparameter gleich. Es ergibt sich somit nach Gleichung 3.1 bei breiterer Spule ein größerer Querschnitt und damit ein geringerer ohmscher Widerstand.

   Die Güte Q wird somit nach Gleichung 3.2 bei kleinerem ohmschen Widerstand größer. Varianten mit breiter Spule werden deshalb mit dem Zusatz HG[4] versehen.

4. *Hinzufügen einer Ferritlage*: Mit einer Ferriteinlage kann die Anpassung ebenfalls verbessert werden und die Anzahl der benötigten Windungen sinkt. Außerdem schirmt diese zusätzliche Ferritlage den Tag vor dem Untergrund ab und somit funktioniert der Tag dann auch auf metallischen Oberflächen.

5. *Dummyspulen*: Um die gefertigten Spulen besser vermessen zu können, sehen einige Designs keine Verbindung zwischen Spule und Chippads vor, die Dielektrikumsschicht hat keine Durchkontaktierungen. Damit können an der Spule Messungen ohne elektrischen Einfluss der ansonsten damit verbundenen Bauteile darunter vorgenommen werden. Diese Varianten verfügen außerdem über Kontaktflächen der Spule nach außen. Die oberste Dielektrikumsschicht hat somi Löcher, um Zugang zur Spulenlage zu erhalten.

6. *Variation der Windungsanzahl*: Da die Bauteile sowie die Fertigung mit Toleranzen behaftet sind und die Simulationen von idealen Werten ausgehen, gibt es zusätzlich noch Varianten bei denen die Anzahl der ausgeführten Windungen von der Anzahl der berechneten Windungen nach oben und unten abweicht. Dadurch erhöht sich die Chance, dass diese Toleranzen ausgeglichen werden und eine dieser Variationen eine sehr gute Anpassung an die gewünschte Resonanzfrequenz aufweist. Während die Reduzierung der Windungsanzahl in der Regel kein Problem darstellt, ist eine Erhöhung aufgrund begrenzter räumlicher Reserven auf der selben Lage nicht immer möglich ohne eine weitere Spulenlage hinzufügen zu müssen.

7. *Packagegröße*: Die Packages werden in 3x3 und 5x5 mm Kantenlänge designt, um die Auswirkungen der unterschiedlich großen Spulen zu untersuchen. So ermöglichen die größeren Packages etwa eine einfachere Anpassung der Windungsanzahl, wie unter Punkt 6 bereits erklärt wurde.

[4] High Gain

Tabelle 3.1 zeigt eine Gesamtübersicht aller erstellten Designs. Darin finden sich neben den verbauten ICs auch die finale Packagegröße. Außerdem zeigt die Tabelle ob im jeweiligen Design ein zusätzlicher Kondensator oder Ferrit verbaut wird, bzw. ob die Spule als HG mit 40 μm Windungsbreite ausgeführt wird.

Die Designnummer findet sich auch auf den fertigen Packages, wodurch eine Identifizierung erleichtert wird.

Design-nummer	**Chip**	**Größe**	**Konden-sator**	**Ferrit**	**Spule**
1	my-d Vicinity	3x3mm	x	x	20μm, einlagig
2	my-d Vicinity	3x3mm	x	✓	20μm, einlagig
3	my-d Vicinity	5x5mm	x	x	40μm, einlagig
4	my-d Vicinity	5x5mm	x	✓	40μm, einlagig
5	my-d Proximity	3x3mm	✓	x	20μm, einlagig
6	my-d Proximity	5x5mm	✓	x	40μm, einlagig
7	CIPURSE Move	3x3mm	✓	✓	20μm, einlagig
7m	CIPURSE Move	3x3mm	✓	✓	20μm, einlagig, -2 Windungen
8	CIPURSE Move	5x5mm	✓	x	40μm, einlagig
9	CIPURSE Move	5x5mm	✓	x	20μm, einlagig
9m	CIPURSE Move	5x5mm	✓	x	20μm, einlagig, -2 Windungen
9p	CIPURSE Move	5x5mm	✓	x	20μm, einlagig, +2 Windungen
10	CIPURSE Move	3x3mm	✓	x	20μm, einlagig
11	CIPURSE Move	5x5mm	✓	✓	40μm, einlagig
12	CIPURSE Move	5x5mm	x	x	20μm, zweilagig
13	my-d Move	3x3mm	✓	x	20μm, einlagig
14	my-d Move	5x5mm	✓	x	40μm, einlagig
A	my-d Vicinity	3x3mm	x	x	20μm, einlagig, Dummy
A1	my-d Vicinity	3x3mm	x	✓	20μm, einlagig, Dummy
B	my-d Vicinity	5x5mm	x	x	40μm, einlagig, Dummy
B1	my-d Vicinity	5x5mm	x	✓	40μm, einlagig, Dummy
C	CIPURSE Move	5x5mm	x	x	20μm, zweilagig, Dummy

Tabelle 3.1: Übersicht der erstellten Designvarianten sortiert nach Designnummer

3.4 Chipauswahl

Im Zuge dieses Projektes wurden verschiedene Chiptypen verwendet. Diese wurden aufgrund ihrer Verfügbarkeit sowie ihres Energiebedarfes ausgewählt. Zu den verwendeten Typen zählen drei reine Speicherchips sowie ein CIPURSE[5] Move IC. Die verschiedenen ICs unterscheiden sich hinsichtlich Interface, Speichergröße, Strombedarf und Funktionalität. Eine Gegenüberstellung der verwendeten ICs wird in Tabelle 3.2 gezeigt.

Chip	**Interface**	**Nutzbarer Speicher (Byte)**	**Datenrate (kBit/s)**	**Eigenkapazität (pF)**	**Sonstiges**
my-d Vicinity	ISO 18000-3	224	26,48	97	Zähler, Seriennummer
my-d Proximity	ISO 14443-3, NFC	4072	106/848	17	NFC, Seriennummer
my-d Move	ISO 14443-3, NFC	128	106/848	17	NFC, Zähler, Passwortschutz, Seriennummer
CIPURSE Move	ISO 14443-3, NFC	256	n.A.	17	CIPURSE-Architektur, AES 128 Bit

Tabelle 3.2: Aufstellung und Vergleich der verwendeten ICs

3.4.1 my-d Vicinity

Der my-d Vicinity [Vic] ist ein reiner Speicher IC mit einer Speicherkapazität von 288 Byte. Dieser ist aufgeteilt in 224 Byte Nutzdaten und 64 Byte Verwaltungsdaten. Diese können über ein ISO/IEC 18000-3 Mode 1 Interface angesprochen werden. Die Datenübertragungsrate beträgt laut Datenblatt 26,48 kBit/s. Jeder Chip enthält eine eindeutige Seriennummer sowie einen 16 Bit breiten Zähler. Zusätzlich besitzt er, im Gegensatz zu den übrigen ICs, eine hohe Eigenkapazität von 97 pF. Man kann daher auf einen externen Kondensator verzichten, erkauft sich das aber mit einem flächenmäßig größeren IC. Die empfohlenen Einsatzgebiete dieses ICs umfassen beispielsweise Objektidentifizierung, wie sie etwa bei Verleihservices oder in der Logistik benötigt werden. Abgesehen von der Möglichkeit individuelle Speicherbereiche zu sperren, verfügt dieser IC über keine weiteren Sicherheitsfunktionen und dient somit lediglich als kontaktloser Speicher für einfache und unkritische Anwendungen.

3.4.2 my-d Proximity

Der my-d Proximity [Pro] ist ein intelligenter Speicher mit einer Speicherkapazität von 5120 Byte. Dieser ist aufgeteilt in 4072 Byte Nutzdaten und 1048 Byte Verwaltungsdaten.

[5] ©OSPT Alliance [OSP]

Er besitzt den größten nutzbaren Speicher dieses Projektes.
Der IC kann über ein ISO/IEC 14443-3 Type A bzw. NFC Type 2 Tag Interface angesprochen werden, die Datenübertragungsrate zum Tag beträgt 106 kBit/s und zum Leser 848 kBit/s. Jeder Chip enthält eine eindeutige Seriennummer sowie einen 16 Bit breiten Zähler. Als Sicherheitsfunktion ist, wie bei reinen Speicher-ICs üblich, nur das individuelle Sperren von Speicherbereichen vorgesehen. Sie können z.b. als Smart Poster eingesetzt werden oder als Hilfsmittel zur Kopplung von Bluetooth Geräten dienen.

3.4.3 my-d Move

Der my-d Move [Mov] ist ein intelligenter Speicher mit einer Speicherkapazität von 152 Byte. Dieser ist aufgeteilt in 128 Byte Nutzdaten und 24 Byte Verwaltungsdaten. Damit hat dieser IC das kleinste Speichervolumen der verwendeten Speicher-ICs. Er kann über ein ISO/IEC 14443-3 Type A bzw. NFC Type 2 Tag Interface angesprochen werden, die Datenübertragungsrate zum Tag beträgt 106 kBit/s und zum Leser 848 kBit/s. Jeder Chip enthält eine eindeutige Seriennummer sowie einen 16 Bit breiten Zähler. Als Sicherheitsfunktion kann zusätzlich ein Passwort für Schreib- bzw. Lesezugriffe gesetzt werden. Gerätekopplung sowie Smart Poster zählen auch hier zu den empfohlenen Anwendungsgebieten.

3.4.4 CIPURSE Move

Im Gegensatz zu den in den Unterabschnitten 3.4.1, 3.4.2 und 3.4.3 genannten ICs unterstützt der CIPURSE Move [Cip] den offenen CIPURSE Sicherheitsstandard der OSPT [OSP] für sichere Bezahlung des Beförderungsentgeldes (*transit fare collection*). Dies beinhaltet unter anderem:

- Erweiterte Sicherheitsfunktionen
- Unterstützung von multiplen Applikationen und Formfaktoren
- Kompatibilität mit Legacy Systemen

Der IC kann über ISO/IEC 14443-3 Type A, 14443-4 sowie NFC Type 4 Tag Interface angesprochen werden. Es stehen 256 Byte Speicher für Nutzdaten zur Verfügung. Der CIPURSE Move kann im öffentlichen Verkehr für Einmalfahrkarten verwendet werden. Er unterstützt dabei aber lediglich eine CIPURSE spezifische Anwendung pro IC, d.h. ein Tag kann nur für eine Aufgabe konfiguriert werden.

Mittels einer 3-Wege Authentifizierung kann wechselseitig die Identität beider Teilnehmer (Tag sowie Lesegerät) festgestellt werden. Um die Integrität der Daten während der Kommunikation zu gewährleisten, wird diese mittels 128 Bit AES-MAC gesichert. Dazu können kryptografische Schlüssel für symmetrische Verschlüsselungsverfahren hinterlegt werden.

Der IC ist außerdem resistent gegen DPA[6] und DFA[7]. Damit zählt der CIPURSE Move nicht mehr zu den reinen Speichern und bietet sich aufgrund seiner Funktionen für sicherheitsrelevante Anwendungen an.

[6] Differential Power Analysis
[7] Differential Fault Analysis

Allerdings benötigt dieser IC aufgrund seiner erweiterten Funktionalität mehr Energie als die ansonsten verwendeten reinen Speicher. Dies bedeutet, dass Tags mit diesem IC ein stärkeres Feld benötigen bzw. eine geringe Reichweite aufweisen.

3.5 Demos

In diesem Abschnitt werden die Designs von zwei verschiedenen Demonstratoren vorgestellt, welche Funktionalität der Tags sowie mögliche Anwendungsgebiete zeigen. Diese Designs beziehen sich zum einen auf eine Android basierte Smartphone App (Unterabschnitt 3.5.1) und zum anderen auf eine PC-basierte Variante (Unterabschnitt 3.5.2).

3.5.1 Android Applikation

Wie bereits in der Einleitung erwähnt wurde, wäre die Authentizitätsprüfung von Wertgegenständen ein mögliches Einsatzgebiet der Tags. Da dies mit einem handelsüblichen Smartphone mit NFC-Funktion möglich ist, wird eine App benötigt, um die Authentifizierung mit einem CIPURSE Tag durchzuführen. Diese App soll auf Android basierten Smartphones laufen. Wenn ein Gegenstand mit CIPURSE Tag an das Gerät gehalten wird, soll die Authentifizierung des Tags durchgeführt und das Ergebnis auf dem Display angezeigt werden wie in Abbildung 3.3 schematisch dargestellt ist.

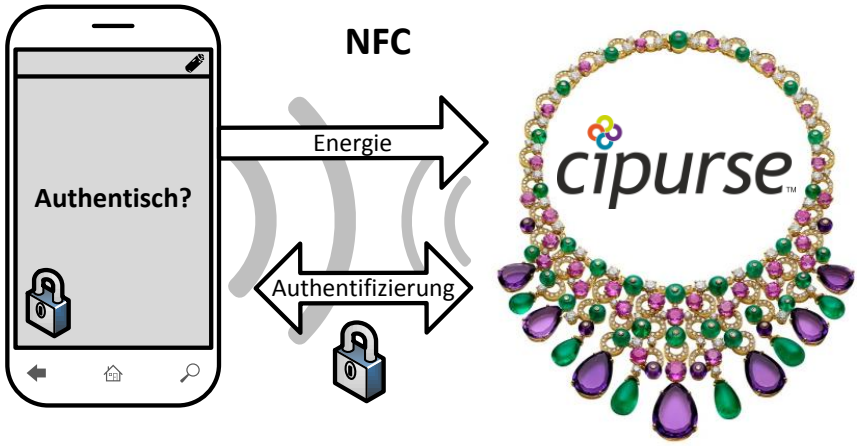


Abbildung 3.3: Design der Android Demo

Klassendiagramm

Die Android App wird in drei Teile aufgeteilt (siehe Klassendiagramm in Abbildung 3.4):

- **MainActivity**: In dieser Klasse wird die GUI realisiert werden und die benötigten Initialisierungen des Kommunikationskanals durchgeführt.

- **CommsChannel**: In dieser Klasse wird der Kommunikationskanal zum Tag abgebildet. Hierzu gehören etwa das Übertragen der Daten, das Empfangen der Antwort und das Öffnen bzw. Schließen des Kanals.
- **CommandLibraryDemo**: Hier wird der Demonstrationsalgorithmus implementiert. Dazu zählen etwa das Auswählen der richtigen Applikation auf dem Tag, das Herstellen eines sicheren Kommunikationskanals mittels gegenseitiger Authentifizierung, sowie das Auslesen der Daten vom Tag. Außerdem befinden sich in dieser Klasse die Fehlerbehandlung sowie das Logging.

Im Klassendiagramm sind CIPURSE spezifische Methoden sowie Bibliotheken nicht aufgeführt. Diese Bibliotheken umfassen dabei etwa die verwendete AES Implementierung, die Übertragung der Kommandos zum Tag, die Rückübermittlung der Antwort, sowie administrative Methoden um den Tag zu konfigurieren.

Die GUI soll so minimalistisch wie möglich gestaltet werden. Dazu gehört ein automatischer Start des Authentifizierungsvorganges sobald ein Tag in die Nähe des Smartphones gebracht und erkannt wird. Ebenfalls Teil der App ist ein Popup ob die Authentifizierung dieses Tags erfolgreich war oder fehlgeschlagen ist.

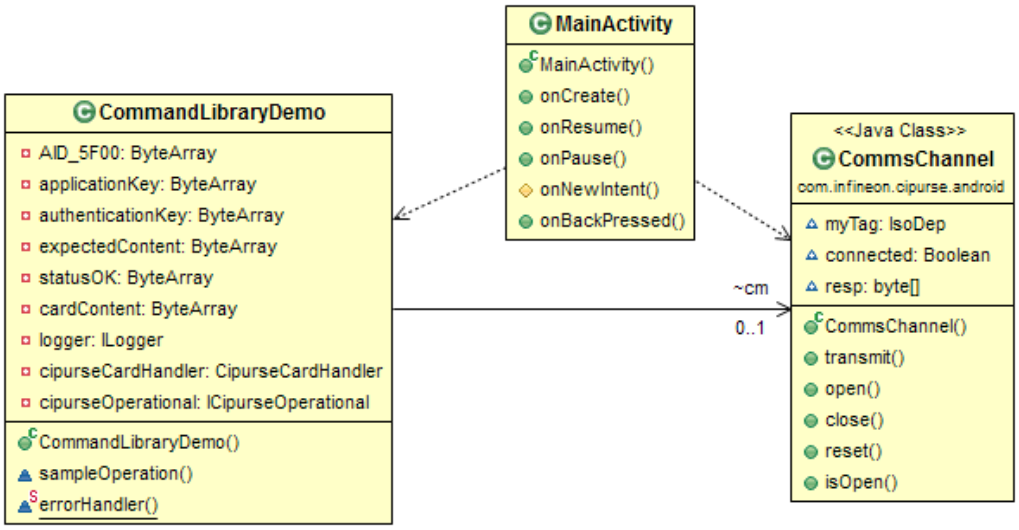


Abbildung 3.4: Klassendiagramm der Android Demo

3.5.2 PC-Demo: Zugangskontrolle

Um ein weiteres mögliches Einsatzgebiet der Tags zu zeigen, wird eine PC-basierte Demo entwickelt. Diese zeigt einen einfachen Anwendungsfall für die Authentifizierungslösung.

Es soll ein handelsübliches Schloss mit einer elektrischen Aufschließsperre erweitert werden. Diese Sperre soll von einem PC aus manuell, sowie automatisch gelöst bzw. geschlossen werden können. Einer der beiden zum Schloss gehörenden Schlüssel soll dabei mit einem CIPURSE Tag versehen werden. Das Schloss soll nur dann mechanisch aufschließbar sein, wenn ein Schlüssel mit CIPURSE Tag verwendet wird und dieser über die benötigten Software Schlüssel und Berechtigungen verfügt.

Eine schematische Übersicht aller Komponenten ist unter Abbildung 3.5 zu sehen. Abbildung 3.5a stellt hierbei die Systemansicht der Demo dar und verdeutlicht das grundsätzliche Konzept. In Abbildung 3.5b werden die grundlegenden elektronischen Komponenten aufgezeigt, welche für das Ansteuern der Verriegelung nötig sind. Der Schalter $S1$ soll vom PC aus mittels Relais geschaltet werden können. Der Schalter $S2$ dient der Überbrückung von $S1$ und ermöglicht eine manuelle Betätigung zu Testzwecken. Die Diode $D1$ fungiert als Freilaufdiode und leitet den Strom des Hubmagneten beim Abschalten ab.

Klassendiagramm

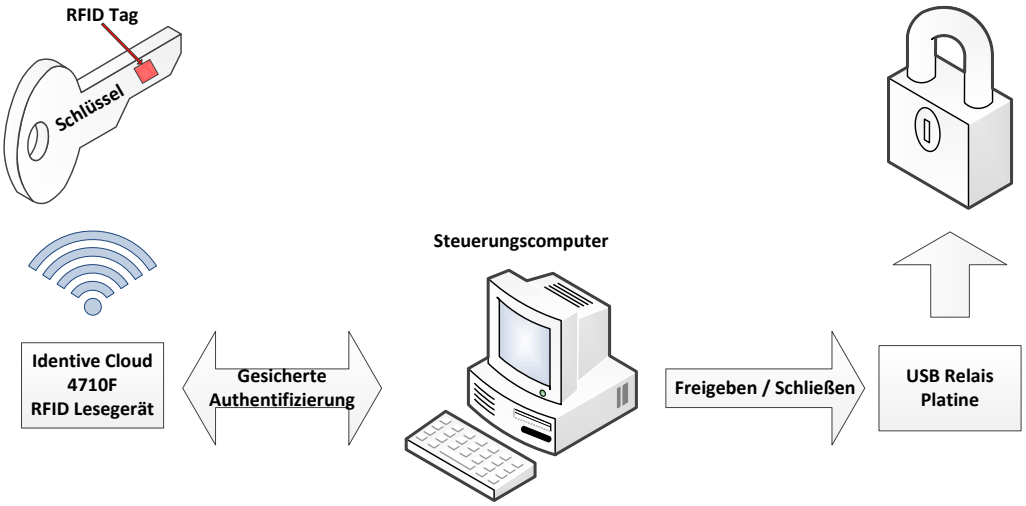
Die PC-Demo besteht aus einer Klasse sowie zwei Enumerationen (siehe Klassendiagramm in Abbildung 3.6). In der ersten Enumeration wird der Status der Zugangssteuerung abgebildet. Als Zustand gelten folgende Parameter:

- **noCard**: Es wurde kein Tag erkannt bzw. es befindet sich kein Tag in Reichweite des Lesegerätes.
- **notAllowed**: Es wurde ein Tag erkannt, dieser hat jedoch keine gültige Zutrittsberechtigung.
- **Success**: Es wurde ein Tag erkannt und dieser besitzt eine gültige Zutrittsberechtigung.
- **Init**: Initialer Zustand. Dieser wird eingenommen sobald das System aktiviert ist und noch kein Tag erkannt wurde.
- **Override**: Die Türsteuerung wurde manuell ausgelöst. Dazu gehören das manuelle Schließen sowie das manuelle Öffnen der Tür. Die manuelle Öffnung soll außerdem mit einem Timer versehen werden, sodass sich die Tür nach einer vorgegebenen Zeitspanne wieder automatisch verriegelt.

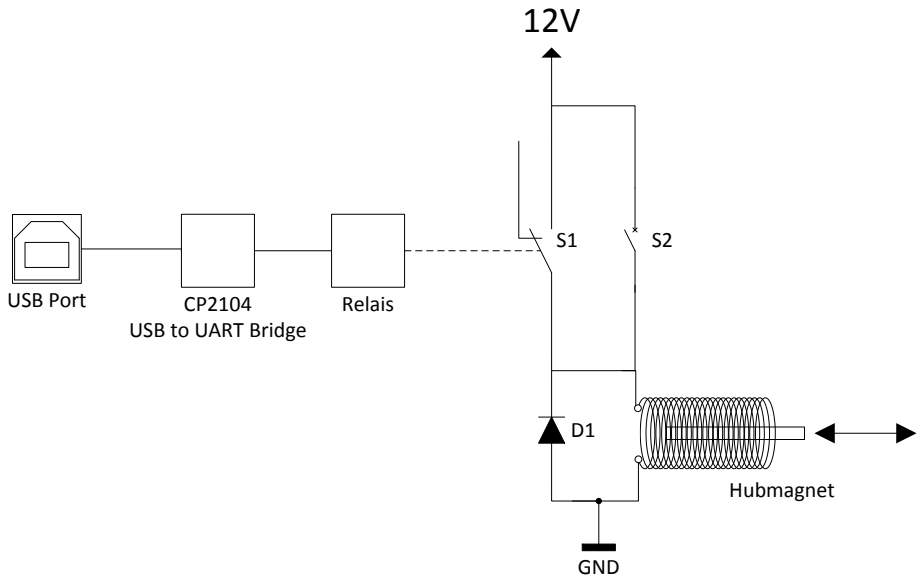
Die zweite Enumeration dient zur Abbildung des Türstatus. Diese kennt zwei Zustände: **open** (geöffnet) oder **closed** (verriegelt). In der Hauptklasse wird die Zugangskontrolle implementiert. Diese umfasst neben Möglichkeiten zum Öffnen und Verriegeln der Tür eine Methode, um einen Tag in Reichweite auszulesen und dessen Zutrittsberechtigung festzustellen.

Der aktuelle Türzustand sowie der Status der Zugangssteuerung soll grafisch angezeigt werden. Ein Mockup der GUI ist in Abbildung 3.7 zu sehen. Die GUI soll folgende Komponenten beinhalten:

- Ein Textfeld um **Benachrichtigungen** des Systems anzuzeigen.
- Ein **Logo**.
- Eine Schaltfläche zum **manuellen Öffnen** der Tür.
- Eine Schaltfläche zum **manuellen Verriegeln** der Tür.
- Ein Textfeld, um den **Türstatus** inklusive farblicher Hervorhebung anzuzeigen.



(a) Systemansicht



(b) Schematische Darstellung der elektronischen Komponenten

Abbildung 3.5: Design der PC-Demo

- Ein Textfeld, um den **Status der Zugangsteuerung** auch farblich hervorgehoben anzuzeigen.
- Ein Textfeld, um Systemmeldungen wie etwa Timer, Status der Authentifizierung etc. anzuzeigen.

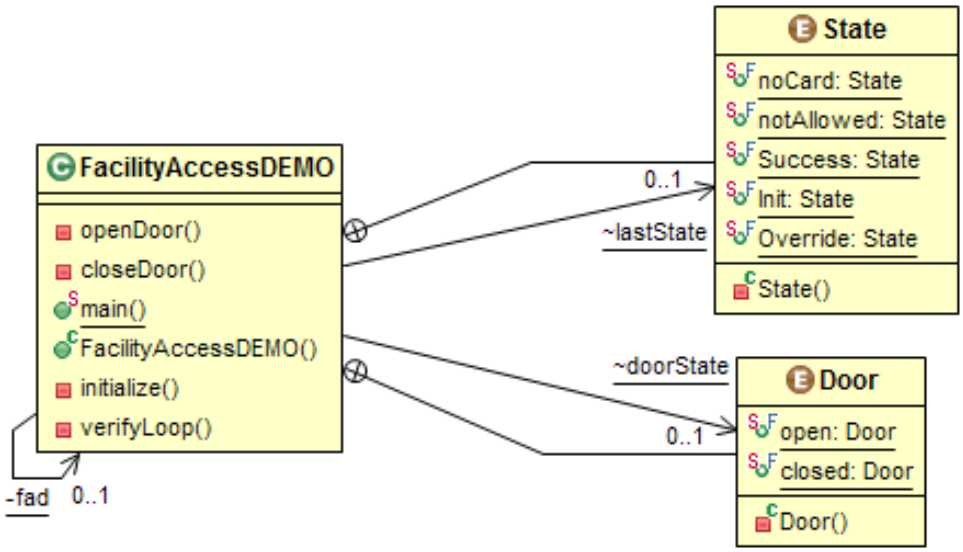


Abbildung 3.6: Klassendiagramm der PC-Demo

Abbildung 3.7: Mockup der GUI der PC-Demo

Kapitel 4

Implementierung

In diesem Kapitel werden zuerst die verwendeten Programme vorgestellt, die zur Implementierung der Designs sowie zu deren Simulation verwendet wurden. Danach werden die fertigen Packages gezeigt und die Simulationsergebnisse präsentiert. Anschließend werden 3D-Simulationen der Tags auf unterschiedlichen Untergrundmaterialien gezeigt und analysiert. Das Ende des Kapitels zeigt die Implementierungen der Android App sowie der PC-Demo.

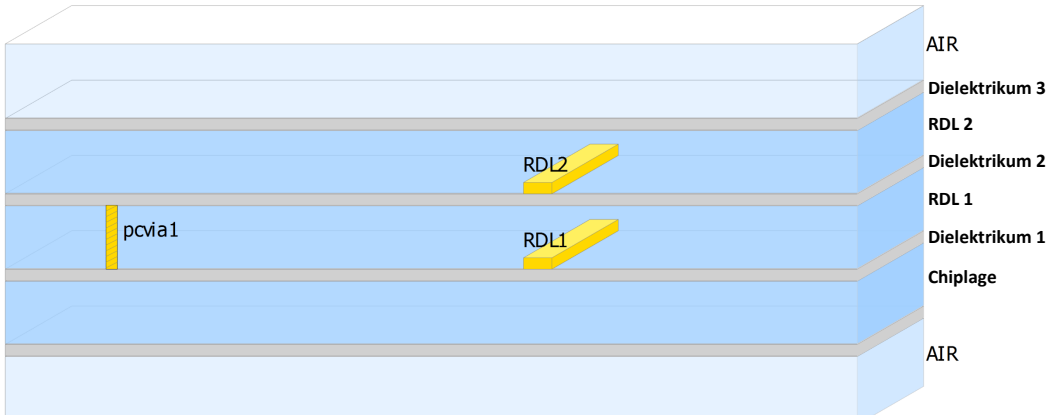
4.1 Advanced Design System

Die Designs sowie die 2D-Simulationen wurden mit Hilfe des Advanced Design System von Keysight [ADS] erstellt.

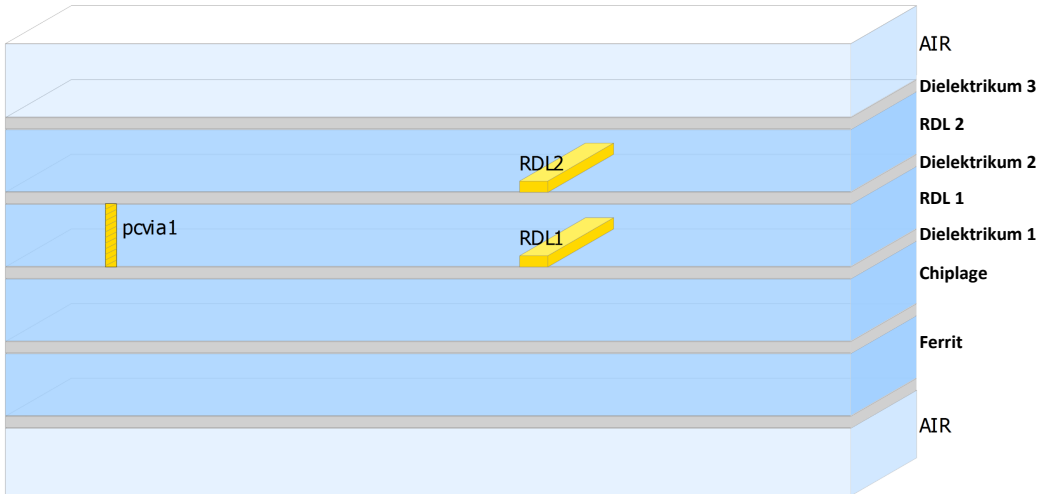
Ein Querschnitt durch die beiden hier verwendeten Substrate stellt Abbildung 4.1 dar. Die Substrate bestehen aus folgenden Lagen:

1. Ferrit
2. Chiplage: Dort befinden sich die ICs, Kondensatoren etc.
3. Dielektrikum 1: Erste Dielektrikumsschicht zwischen RDL 1 und Chiplage
4. RDL 1: Erste Antennenlage
5. Dielektrikum 2: Zweite Dielektrikumsschicht zwischen erster und zweiter Antennenlage
6. RDL 2: Zweite Antennenlage
7. Dielektrikum 3: Abschließende Dielektrikumsschicht, kapselt die oberste Antennenlage von der Umgebung ab

Diese beiden Substrate unterscheiden sich nur dadurch, dass bei Abbildung 4.1b eine zusätzliche Ferritschicht eingefügt wurde. Die gezeigten Abbildungen sind nicht maßstabsgetreu, die einzelnen RDL Schichten sind wesentlich dünner als die Chiplage. Die Verbindung durch die Dielektrika wurde mittels Durchkontaktierungen hergestellt. Bei einlagigen Designs entfällt naturgemäß RDL 2 sowie Dielektrikum 3.



(a) Substrat ohne Ferrit



(b) Substrat mit Ferrit

Abbildung 4.1: Für Entwurf und Simulation verwendete Substrate

4.1.1 Simulator

Für die Simulation wurde ein Schema, wie es unter Abbildung 4.2 dargestellt ist, verwendet. Der IC wird dabei in grün, der Kondensator in blau und die Spule in rot dargestellt. Mit C_{chip} wird die Eigenkapazität des IC bezeichnet. Diese liegt bei dem gezeigten IC bei 17 pF. Die zusätzliche Kapazität des Kondensators wird als C_{cap} bezeichnet und liegt immer bei 100 pF. Am Ende dient noch ein 50Ω Widerstand zur Terminierung.

Sämtliche Bauteile wurden hierbei als ideal angesehen, etwaige Streuungen der Eigenkapazitäten der ICs sowie die Toleranz der Kondensatoren fanden bei den Simulationen keine Berücksichtigung.

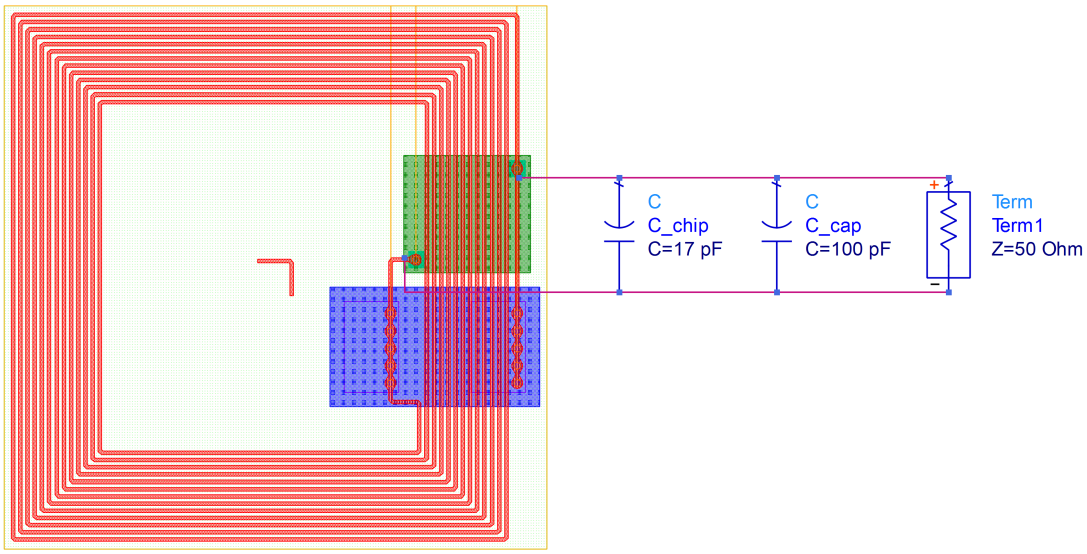


Abbildung 4.2: Schematische Darstellung der Simulation in ADS

Die Simulationen selbst wurden auf einem Computercluster ausgeführt, da lokale Rechner eine zu geringe Rechenleistung aufwiesen sowie über zu wenig Arbeitsspeicher verfügten. Ein Screenshot eines solchen Simulationsdurchlaufes ist in Abbildung 4.3 zu sehen.

Method-of-Moments

Dieser Simulator basiert auf der Momentenmethode (MoM[1]) und ist ein numerisches Berechnungsverfahren zur Lösung von linearen, partiellen Differentialgleichungen. Da hierbei nur die Randbedingungen und nicht alle Werte im Raum berechnet werden müssen, ist dieses Verfahren relativ schnell und effizient. Dies gilt hauptsächlich bei Objekten mit kleinem Oberflächen/Volumen Verhältnis. Dabei wird ein Gitter, das *mesh*, auf die Oberfläche des zu simulierenden Objektes gelegt und somit in Zellen unterteilt. Die Feinheit dieses Gitters bzw. die Größe der Zellen hat großen Einfluss auf die Simulationsgenauigkeit. Je kleiner die Zellen, desto exakter die Lösung, desto höher aber auch der Rechenaufwand. Das Substrat wird bei dieser Methode als unendlich ausgedehnt betrachtet. Da 3D-Objekte dadurch schichtweise simuliert werden, spricht man hier von einem 2.5D-Simulator.

[1] Method-of-Moments

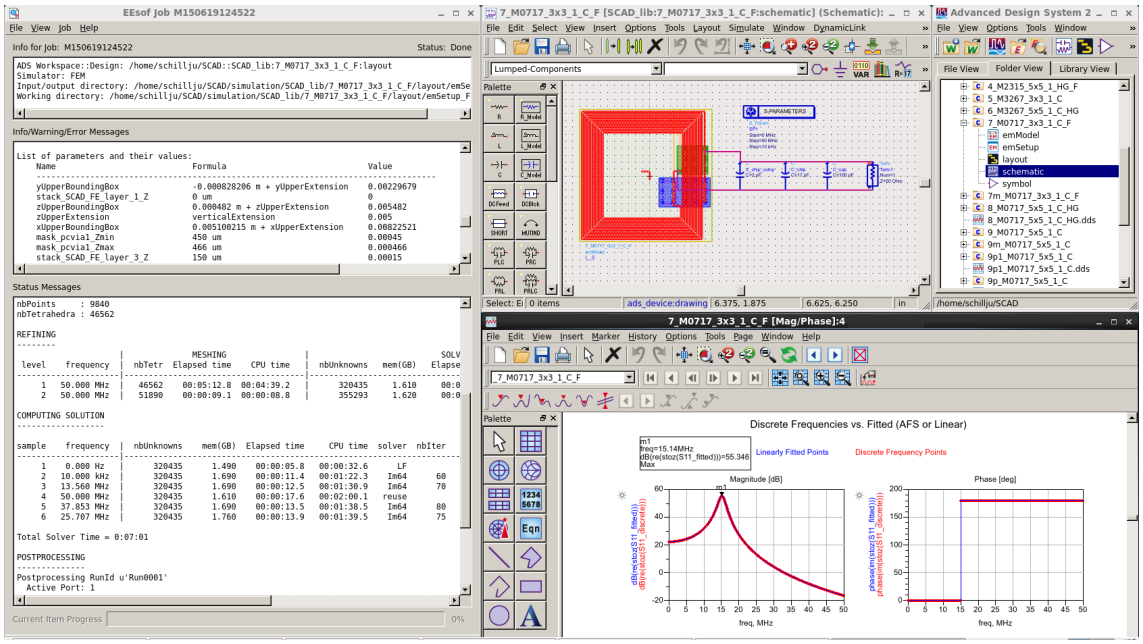


Abbildung 4.3: Screenshot einer FEM-Simulation in ADS

Finite-Element-Method

Der FEM[2]-Simulator basiert auf der Methode der finiten Elemente und ist ebenfalls ein numerisches Berechnungsverfahren zur Lösung von partiellen Differentialgleichungen. Es unterteilt das zu lösende Problem in endlich kleine Teile (daher *finite Elemente*). Je höher die Anzahl dieser Elemente, desto größer ist am Ende das zu lösende Gleichungssystem. Hierbei handelt es sich um einen 3D-Simulator, da ein echtes dreidimensionales Gitter zur Anwendung kommt. Dieses Volumengitter wird zusätzlich adaptiv verfeinert, sofern die Lösung es erfordert. Diese Methode kann auch zur Visualisierung von magnetischen Feldern genutzt werden.

Vergleich der Simulatoren

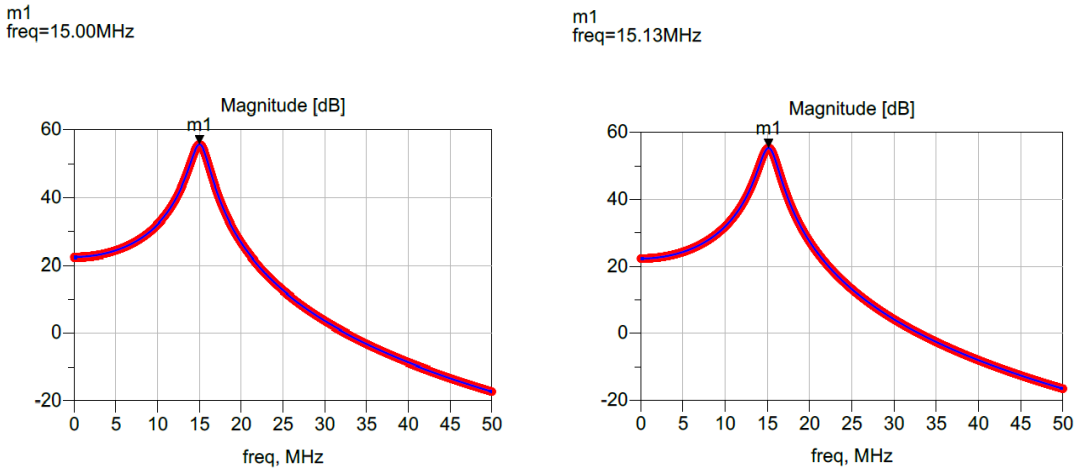
Ein Simulationsdurchlauf mittels ADS FEM benötigte, je nach Auslastung der Server, zwischen 5 und 90 Minuten. Bei Verwendung des ADS Momentum Simulators (MoM) sank die benötigte Rechenzeit, wiederum je nach Auslastung, auf 1 bis 30 Minuten.

Die Ergebnisse der beiden Simulatoren wichen allerdings bis zu rund 3,5 Prozent von einander ab, wie in Abbildung 4.4 ersichtlich ist.

4.2 Ansys HFSS

Für die 3D-Simulation der H-Feldverteilung wurde der HFSS von Ansys [HFS] verwendet. Die Simulationen wurden lokal erstellt und danach, wie vorher, auf einem Computercluster ausgeführt. Die Simulationszeit betrug zwischen 3 und 5 Stunden.

[2] Finite-Elemente-Method



(a) MoM-Simulator (b) FEM-Simulator

Abbildung 4.4: Vergleich der Simulationsergebnisse

In Abbildung 4.5 ist ein Screenshot einer fertigen Simulation des Design 9 zu sehen. Dieser Screenshot zeigt das Programm sowie einen Tag mit dazugehörender H-Feld Verteilung.

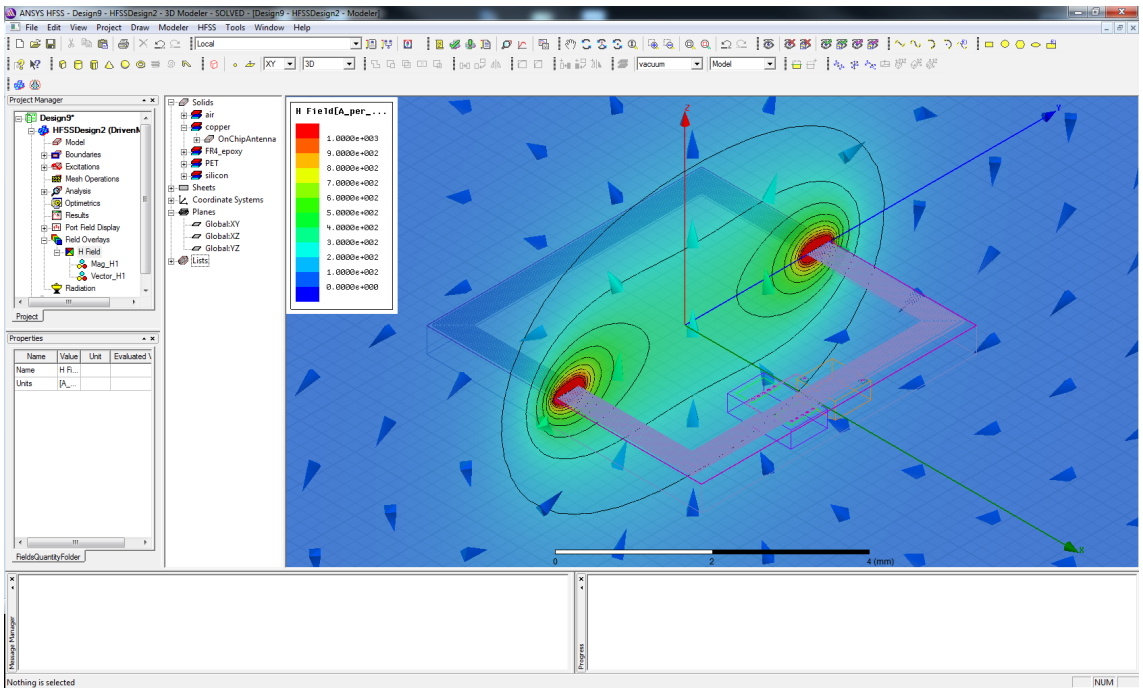


Abbildung 4.5: Ansys HFSS 3D-Simulation Screenshot

4.3 Antennendimensionierung

Zur Dimensionierung der Antennen stand ein Programm der Firma Infineon Technologies Austria AG zur Verfügung. Die Berechnungen erfolgten aufgrund folgender Parameter:

- Abmessungen des Packages
- Breite und Dicke der Leiterbahnen
- Leitfähigkeit des Leiterbahnenmaterials
- Abstand der Leiterbahnen untereinander
- Gesamtkapazität des Tags
- relative Permittivität des Grundmaterials

So konnte die benötigte Windungsanzahl, für eine Anpassung an die Resonanzfrequenz von 13,56 MHz, näherungsweise berechnet werden. Diese Berechnungen dienten als Grundlage für die Implementierung der Tags. Mit Hilfe der nachfolgenden Simulationen wurden diese Berechnungen anschließend verfeinert und die Antennen entsprechend den Simulationen angepasst.

4.4 Packageaufbau und Simulationsergebnisse

4.4.1 my-d Vicinity

Die Designs 1 bis 4, sowie die Dummies A bis B1, beinhalten den my-d Vicinity IC. Dieser verfügt, wie bereits unter Abschnitt 3.4.1 erwähnt, über eine hohe Eigenkapazität von 97 pF. Dadurch ist es bei diesen Designs nicht nötig einen zusätzlichen Kondensator zu verbauen.

Design 1 (Abbildung 4.10a) stellt eine unangepasste Form dar. Die Spule enthält also nicht die Anzahl an Windungen, die nötig wäre, um auf die erforderliche Resonanzfrequenz von 13,56 MHz zu kommen. Dies ist der Größe des Packages sowie der Kapazität des Chips geschuldet. Bei einer Packagegröße von 3x3 mm und 97 pF wären rund 20 Windungen nötig. Platzbedingt sind hier auf einer Lage aber nur 18 möglich. Abbildung 4.6 zeigt die Simulation dieses Designs. Es ist ersichtlich, dass die zu erwartende Resonanzfrequenz bei etwa 15,56 MHz und damit rund 2 MHz über dem Optimum liegen wird.

Design 2 (Abbildung 4.10b) enthält zusätzlich eine Ferritlage, wodurch sich die Anzahl der nötigen Windungen auf 16 verringert. Die Simulation ist in Abbildung 4.7 zu sehen.

Design 3 (Abbildung 4.10c) ist das 5x5 mm große Äquivalent zu Design 1, enthält aber die mit 40 μm doppelt so breite Spule. Dies ist aufgrund der Packagegröße von 5x5 mm möglich. Bezüglich der Anzahl der Windungen, bzw. der nicht angepassten Resonanzfrequenz, verhält es sich hier wie bei Design 1. Die Simulation ist in Abbildung 4.8 zu sehen.

Design 4 (Abbildung 4.10d) ist das 5x5 mm große Äquivalent zu Design 2, enthält aber wieder die doppelt so breite Spule und die Ferritlage. Die Simulation ist in Abbildung 4.9 zu sehen.

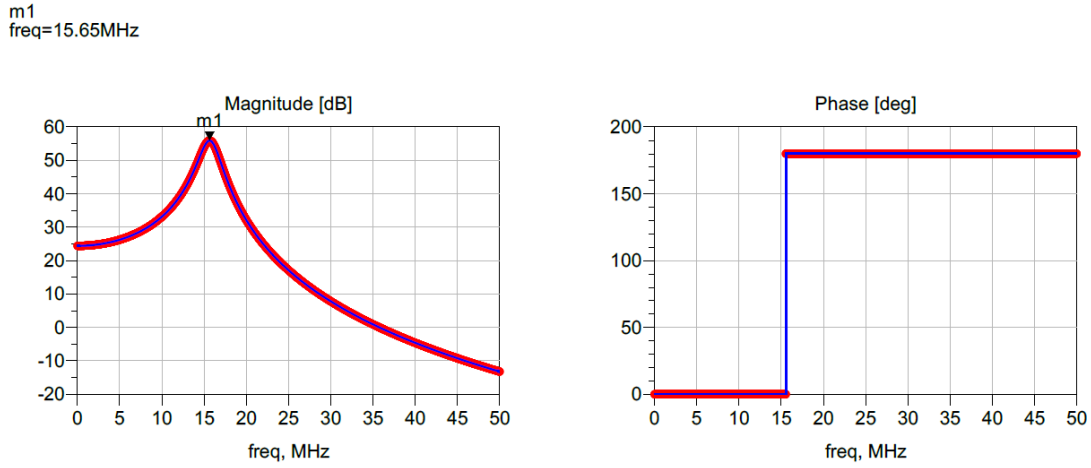


Abbildung 4.6: Simulation des Design 1

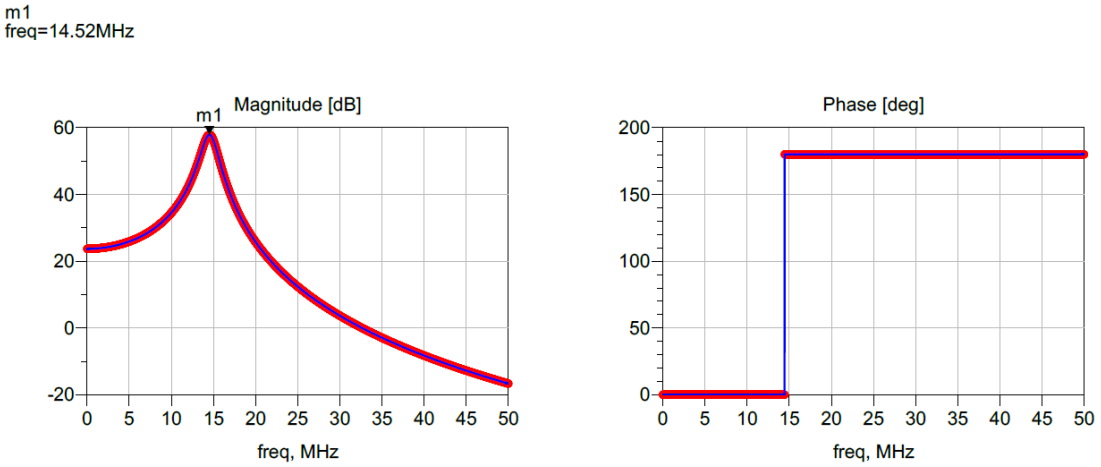


Abbildung 4.7: Simulation des Design 2

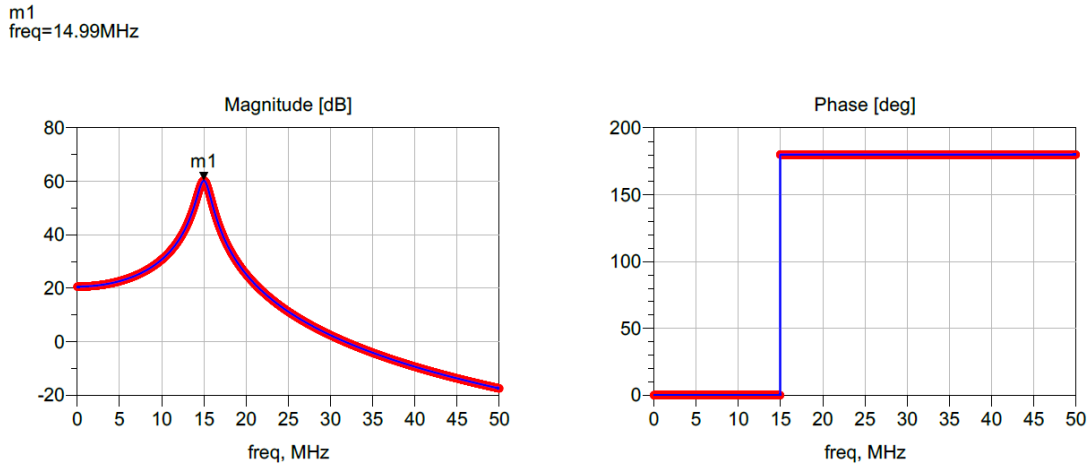


Abbildung 4.8: Simulation des Design 3

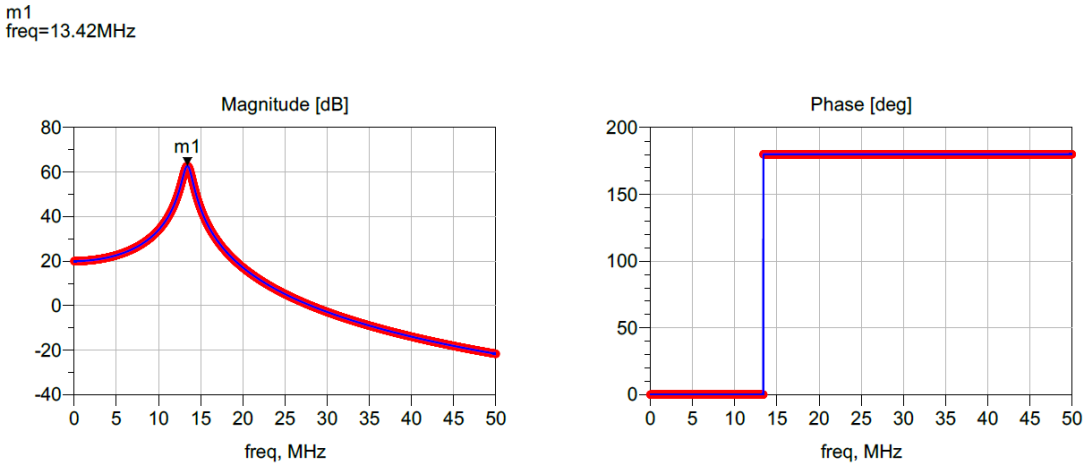


Abbildung 4.9: Simulation des Design 4

Die Dummies **Design A** bis **Design B1** entsprechen den Designs 1 bis 4 mit durchgehender Dielektrikumsschicht. Dies bedeutet, dass es keine elektrische Verbindung zwischen den Chippads und der Spule gibt. Diese kann somit unabhängig des darunter liegenden ICs vermessen werden.

4.4.2 my-d Proximity

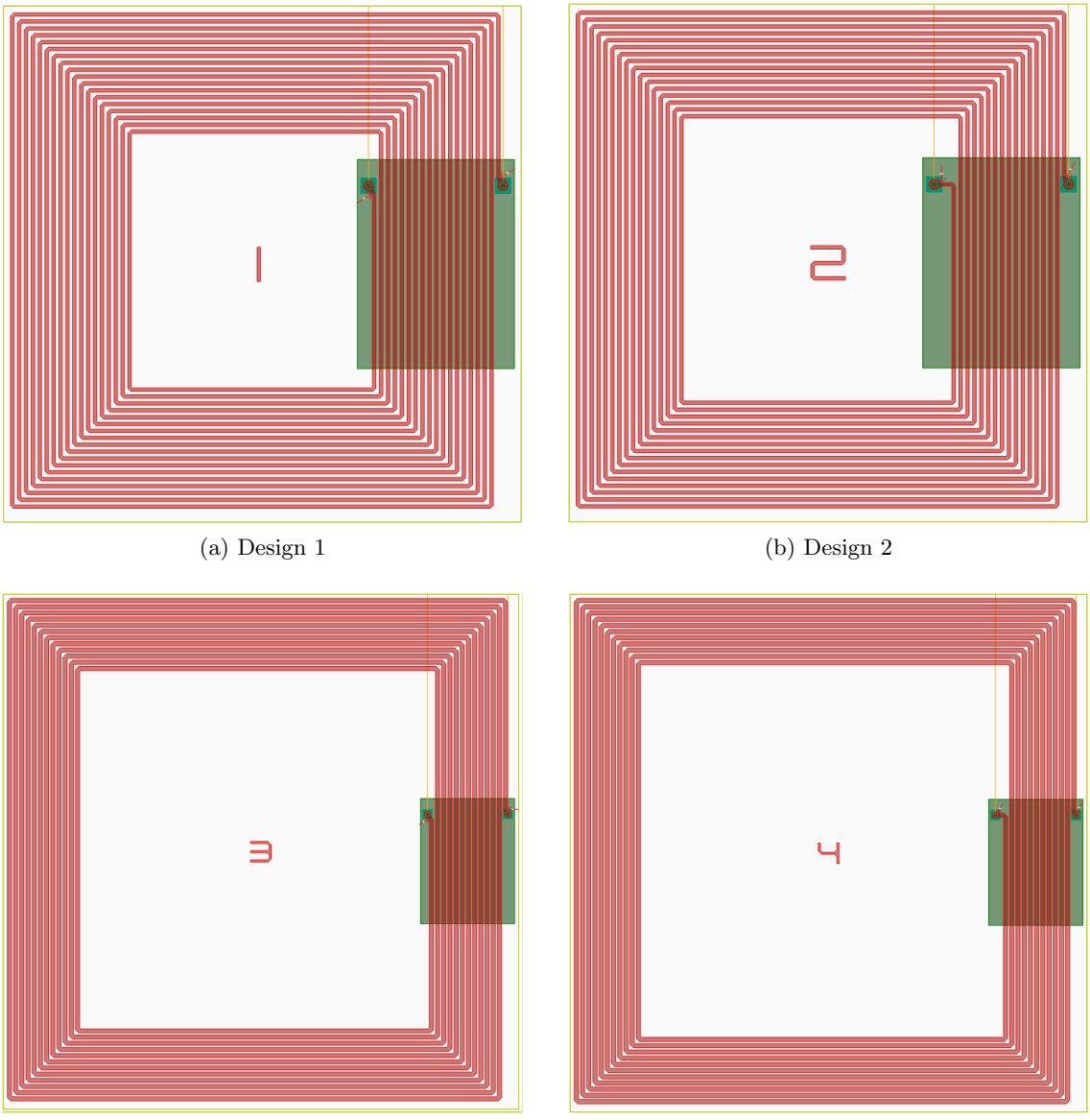
Die Designs 5 und 6 beinhalten den my-d Proximity IC. Dieser verfügt, wie bereits in Tabelle 3.2 erwähnt, über eine Eigenkapazität von 17 pF. Dadurch ist es bei diesen Designs nötig einen zusätzlichen Kondensator von 100 pF zu verbauen.

Design 5 (Abbildung 4.13a) beinhaltet den IC (oben im Bild) und den Kondensator (unten im Bild). Um eine gute elektrische Verbindung zu gewährleisten wird der Kondensator über mehrere Vias mit der Spule verbunden. Abbildung 4.11 zeigt die Simulation dieses Designs.

Design 6 (Abbildung 4.13b) ist das 5x5 mm große Äquivalent zu Design 5, enthält aber die mit 40 μm doppelt so breite Spule. Dies ist aufgrund der Packagegröße von 5x5 mm möglich. Die Simulation ist in Abbildung 4.12 zu sehen. Es ist ersichtlich, dass die gewünschte Resonanzfrequenz der beiden Designs sehr gut angenähert wird.

4.4.3 my-d Move

Die Designs 13 und 14 beinhalten den my-d Move IC. Dieser verfügt, wie bereits in Tabelle 3.2 dargestellt, über eine Eigenkapazität von 17 pF. Deshalb ist es auch bei diesen Designs nötig einen zusätzlichen Kondensator von 100 pF zu verbauen. Der IC ist außerdem sehr klein, dadurch ist es nicht mehr möglich die Spule zwischen den Pads zu führen und gleichzeitig die benötigte Anzahl an Windungen unterzubringen. Aus diesem Grund wird der IC innerhalb der Spule platziert und die äußere Verbindung mit der Spule über ein eingelegtes metallisiertes Siliziumplättchen hergestellt. Dieses Siliziumplättchen wird als Untertunnelung bezeichnet. Dadurch wir eine zweite Spulenlage vermieden.



(a) Design 1

(b) Design 2

(c) Design 3

(d) Design 4

Abbildung 4.10: Layout der Packages mit my-d Vicinity IC

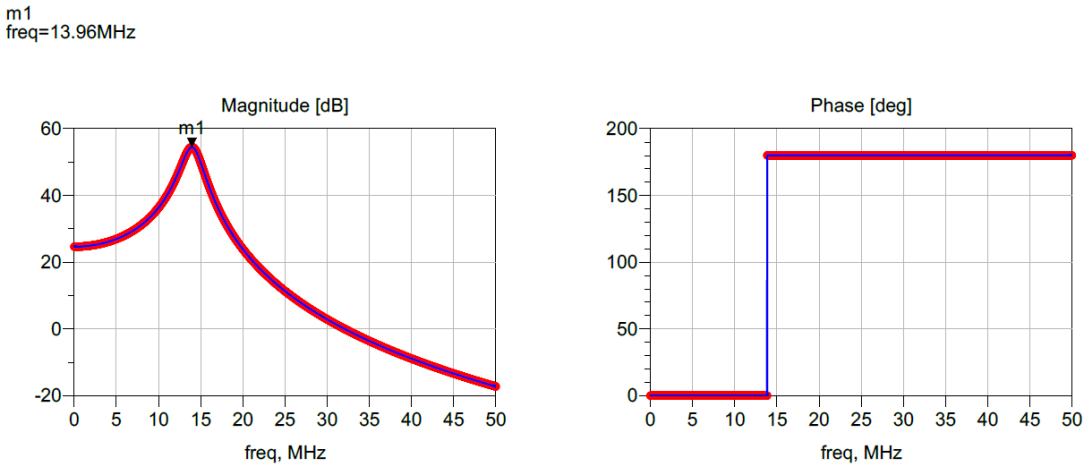


Abbildung 4.11: Simulation des Design 5

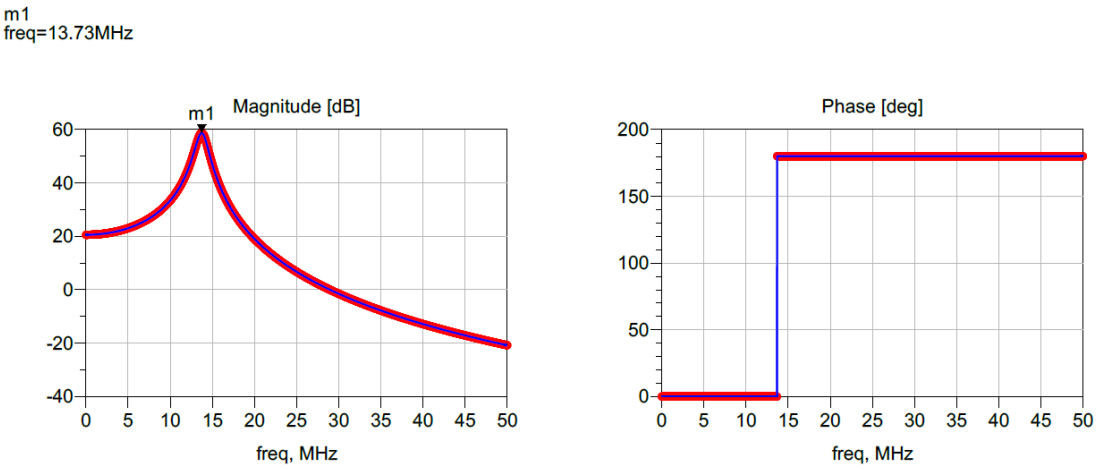
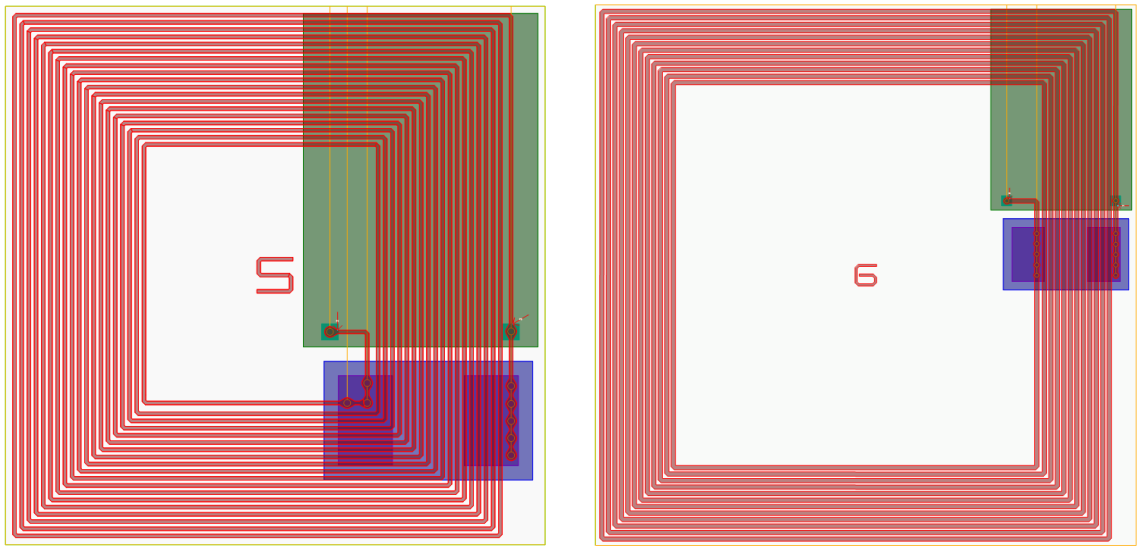


Abbildung 4.12: Simulation des Design 6



(a) Design 5 (b) Design 6

Abbildung 4.13: Layout der Packages mit my-d Proximity IC

Design 13 (Abbildung 4.16a) beinhaltet den IC (mittig im Bild), den Kondensator (rechts unten im Bild) und die Untertunnelung (rechts oben im Bild). Um eine gute elektrische Verbindung zu gewährleisten wird der Kondensator wieder über mehrere Vias mit der Spule verbunden. Abbildung 4.14 zeigt die Simulation dieses Designs.

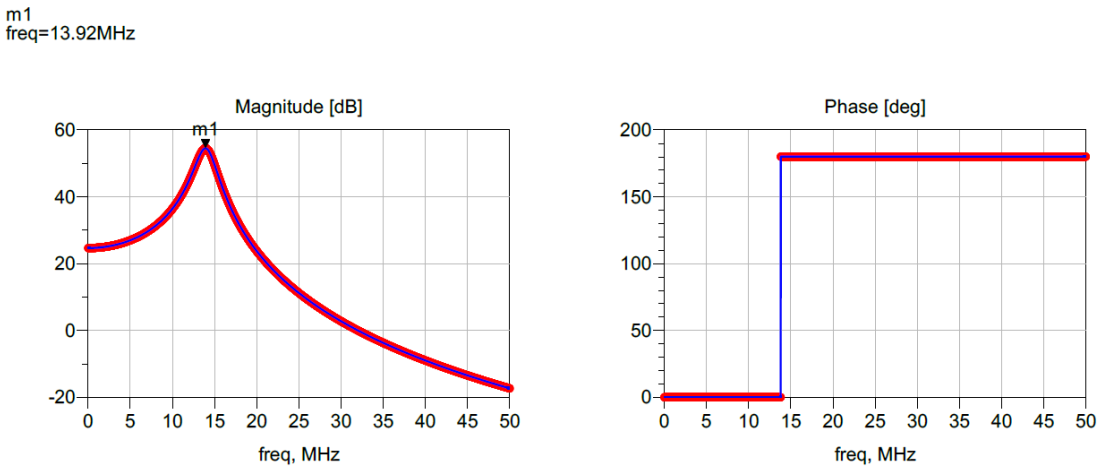


Abbildung 4.14: Simulation des Design 13

Design 14 (Abbildung 4.16b) ist das 5x5 mm große Äquivalent zu Design 13, enthält aber die mit 40 μm doppelt so breite Spule. Dies ist aufgrund der Packagegröße von 5x5 mm möglich. Die Simulation ist in Abbildung 4.15 zu sehen. Es ist ersichtlich, dass die gewünschte Resonanzfrequenz der beiden Designs wieder sehr gut angenähert wird.

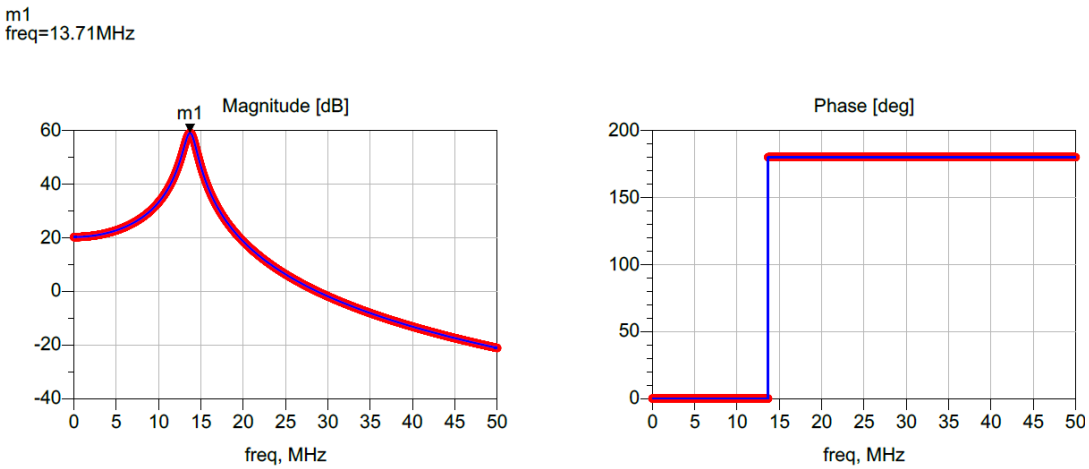
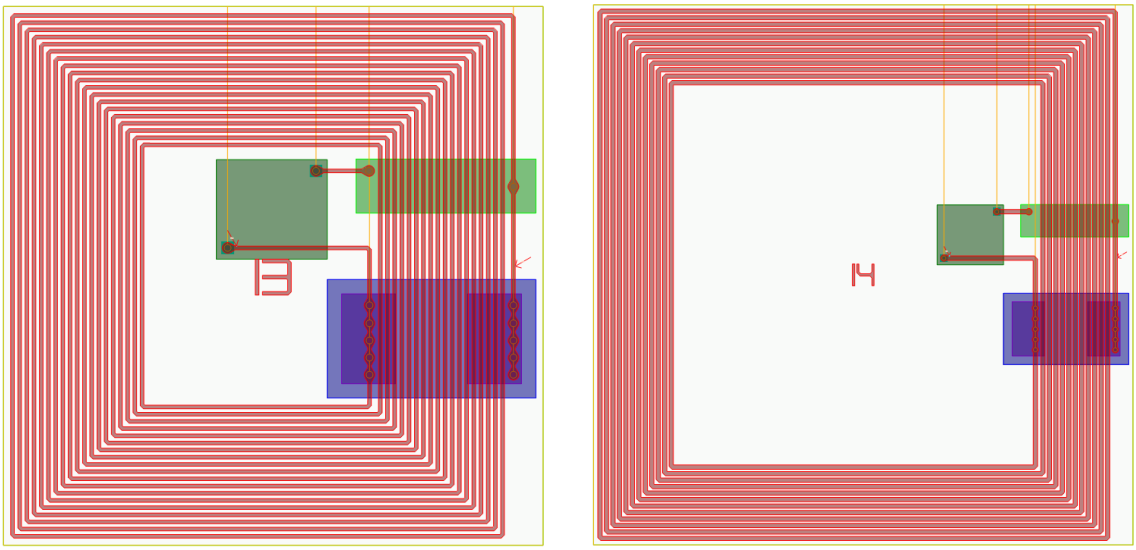


Abbildung 4.15: Simulation des Design 14



(a) Design 13 (b) Design 14

Abbildung 4.16: Layout der Packages mit my-d Move IC

4.4.4 CIPURSE Move

Die Designs 7 bis 12 beinhalten den CIPURSE Move IC. Dieser verfügt, wie bereits in Tabelle 3.2 erwähnt, ebenfalls über eine Eigenkapazität von 17 pF. Deshalb ist es auch bei diesen Designs nötig einen zusätzlichen Kondensator von 100 pF zu verbauen. Aufgrund der Größe des ICs ist es auch hier manchmal nötig, den IC in die Mitte zu verschieben und die Kontaktierung mit der äußeren Seite der Spule über ein metallisiertes Siliziumplättchen zu realisieren.

Design 7 (Abbildung 4.26a) beinhaltet den IC (oben im Bild) und den Kondensator (unten im Bild). Zusätzlich enthält diese Variante eine Ferriteinlage, welche die Windungszahl reduziert und die Spule damit zwischen die Anschlusspads des ICs passt. Abbildung 4.17 zeigt die Simulation dieses Designs.

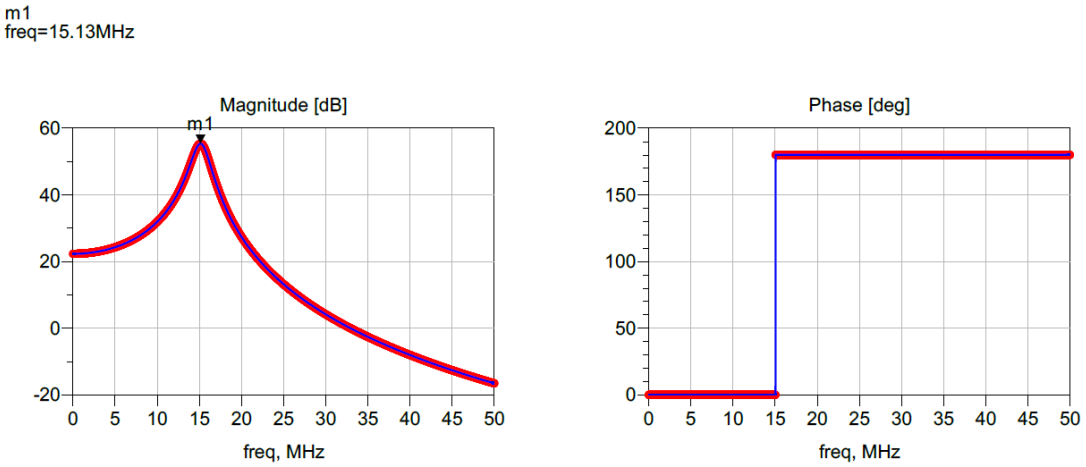


Abbildung 4.17: Simulation des Design 7

Design 7m (Abbildung 4.26b) ist äquivalent zu Design 7. Allerdings wurden hier, wie unter Aufzählung 3.3 Punkt 6 erklärt, zwei Windungen weniger ausgeführt. Die Simulation ist in Abbildung 4.18 zu sehen.

Design 8 (Abbildung 4.26c) beinhaltet den IC (mittig im Bild), den Kondensator (rechts unten im Bild), die Untertunnelung (rechts oben im Bild) sowie die 40 μm breite Spule. Die Simulation ist in Abbildung 4.19 zu sehen.

Design 9 (Abbildung 4.26d) beinhaltet den IC (mittig im Bild) und den Kondensator (rechts unten im Bild). Im Gegensatz zu Design 8 ist hier die Spule 20 μm breit und passt somit zwischen die Anschlusspads des IC, daher kann auf die Untertunnelung verzichtet werden. Die Simulation ist in Abbildung 4.20 zu sehen.

Design 9m und **Design 9p** (Abbildungen 4.26e und 4.26f) sind äquivalent zu Design 9. Allerdings wurden, wie unter Aufzählung 3.3 Punkt 6 erklärt, bei Design 9m zwei Windungen weniger und bei Design 9p zwei Windungen mehr ausgeführt. Die Simulationen sind in Abbildung 4.22 und Abbildung 4.21 zu sehen.

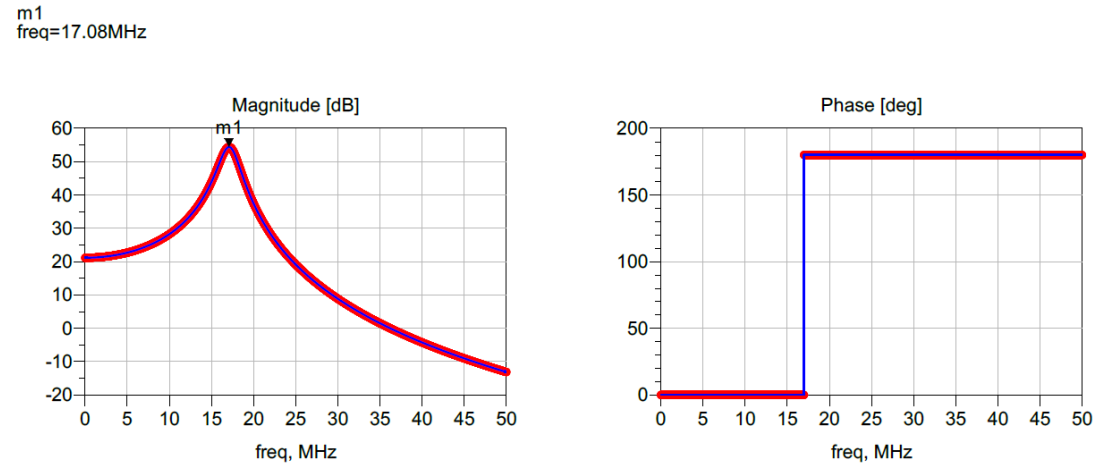


Abbildung 4.18: Simulation des Design 7m

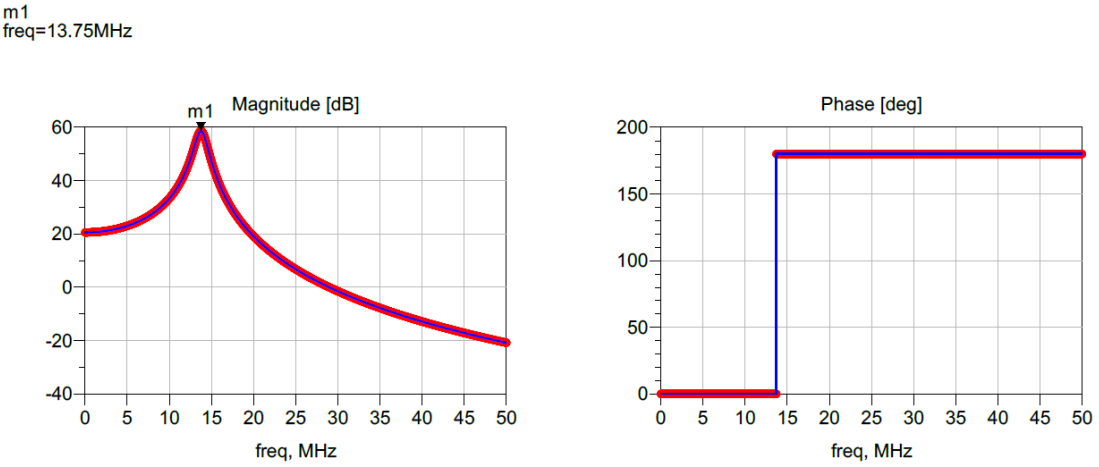


Abbildung 4.19: Simulation des Design 8

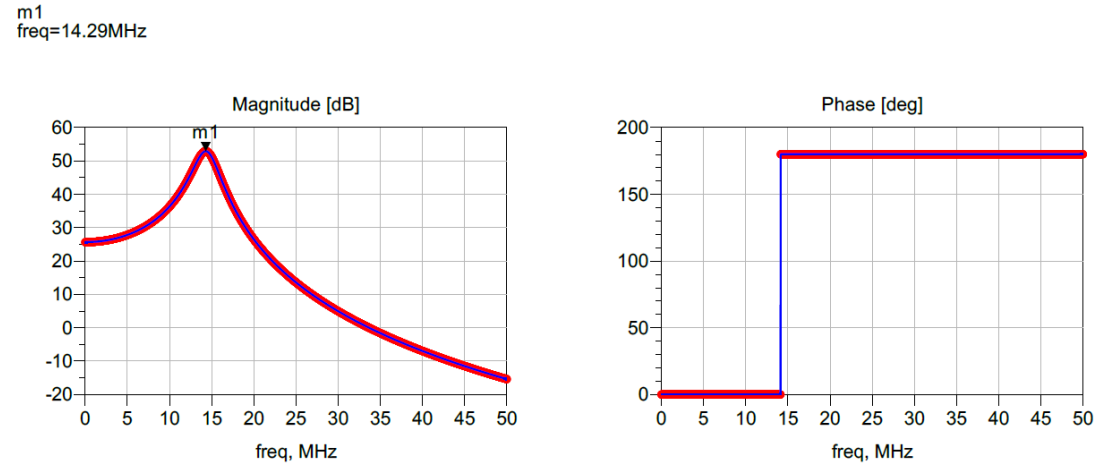


Abbildung 4.20: Simulation des Design 9

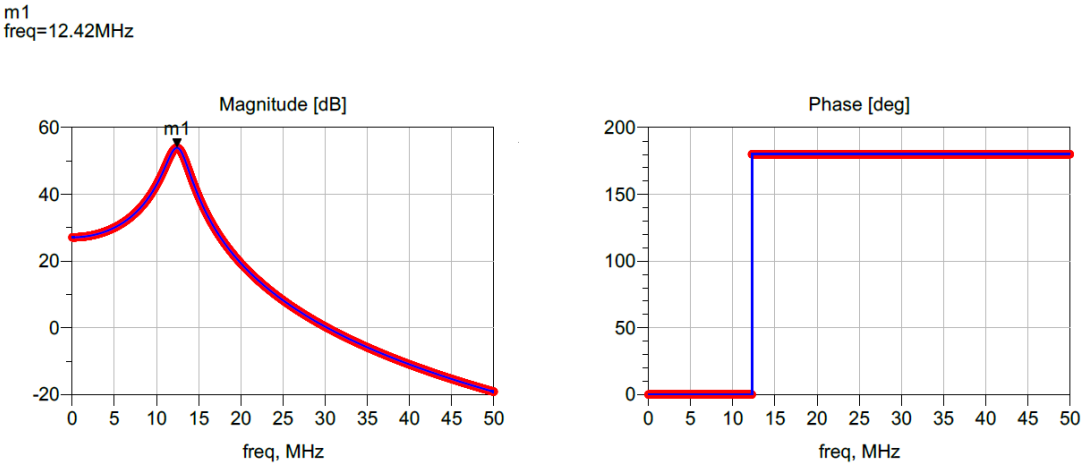


Abbildung 4.21: Simulation des Design 9p

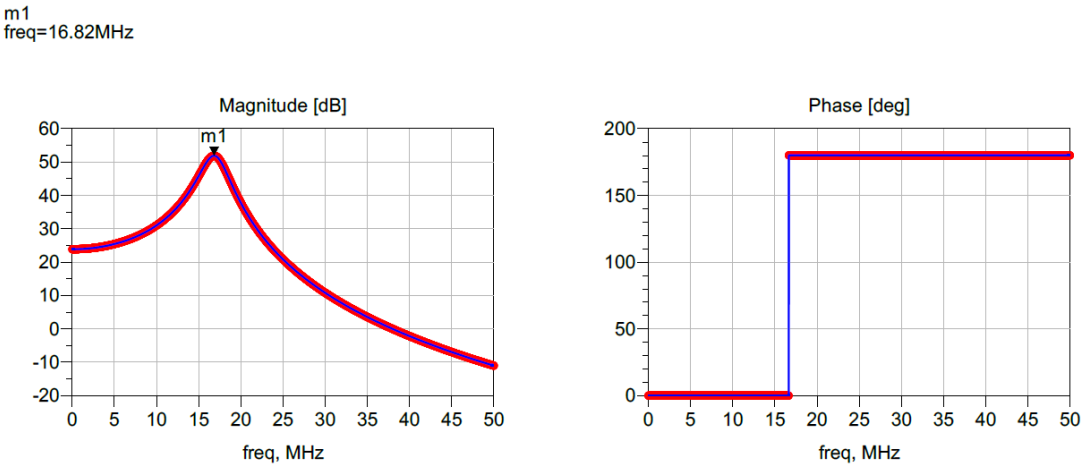


Abbildung 4.22: Simulation des Design 9m

Design 10 (Abbildung 4.26g) beinhaltet den IC (mittig im Bild), den Kondensator (rechts unten im Bild) und die Untertunnelung (rechts oben im Bild). Im Gegensatz zu Design 7 gibt es hier keine Ferriteinlage, wodurch die Windungsanzahl erhöht werden muss und nicht mehr zwischen die Anschlusspads des ICs passt. Darum ist hier wieder eine Untertunnelung nötig. Die Simulation ist in Abbildung 4.23 zu sehen.

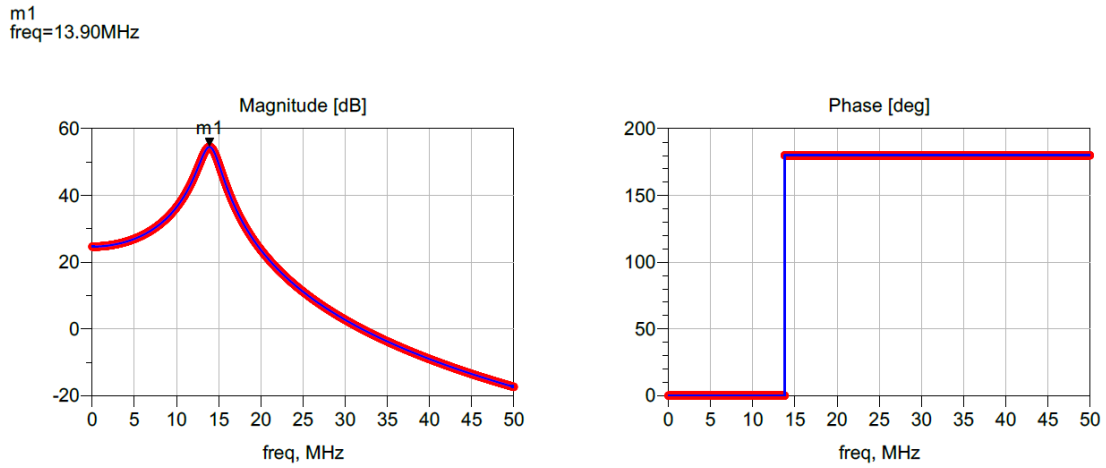


Abbildung 4.23: Simulation des Design 10

Design 11 (Abbildung 4.26h) beinhaltet den IC (mittig im Bild) und den Kondensator (unten im Bild). Im Gegensatz zu Design 8 gibt es hier eine Ferriteinlage, wodurch die Windungsanzahl verringert werden kann und zwischen die Anschlusspads des ICs passt. Darum ist hier keine Untertunnelung nötig. Die Simulation ist in Abbildung 4.24 zu sehen.

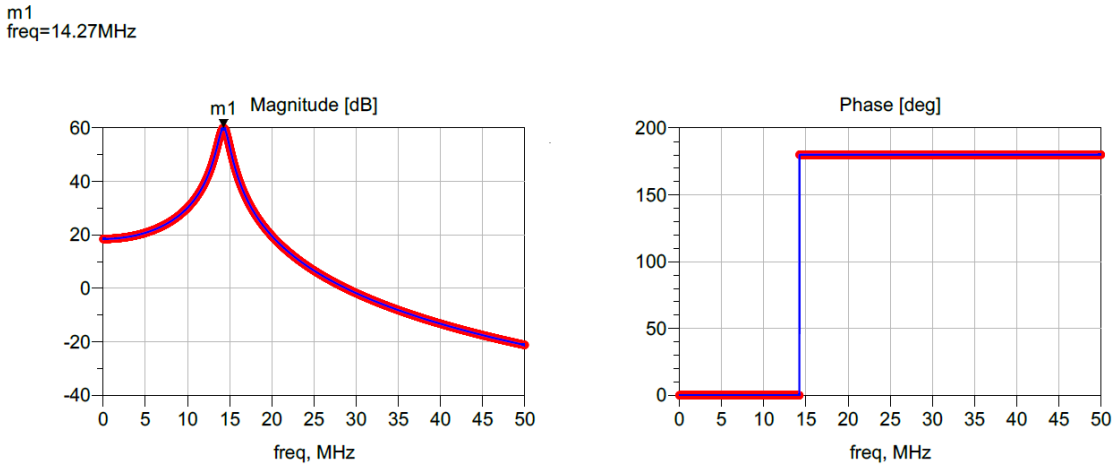


Abbildung 4.24: Simulation des Design 11

Design 12 (Abbildung 4.26i) beinhaltet nur den IC ohne Ferriteinlage und Kondensator. Um die benötigte Anzahl Windungen ausführen zu können, wird die Spule bei diesem Layout zweilagig ausgeführt. Die Simulation ist in Abbildung 4.25 zu sehen.

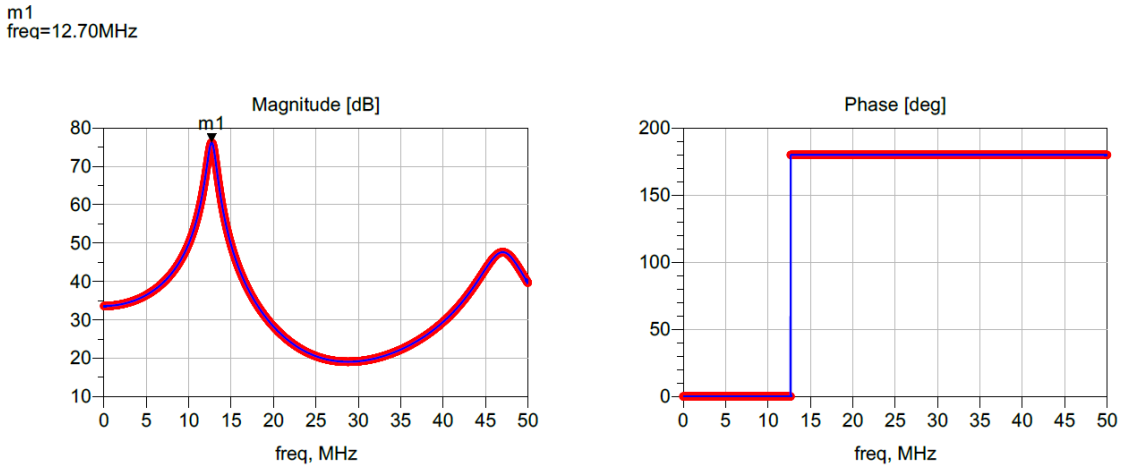


Abbildung 4.25: Simulation des Design 12

Das Dummy **Design C** entspricht dem zweilagigen Design 12 mit durchgehender Dielektrikumsschicht. Mit diesem Dummy kann die zweilagige Spule ohne Einfluss des ICs vermessen werden.

4.5 3D-Simulation und Materialuntersuchung

Um eine repräsentative Ansicht der Feldverteilung in 3D sowie dessen Verzerrung bei unterschiedlichen Grundmaterialien zu erhalten, wurde ein Design mit Ansys HFSS (Abschnitt 4.2) simuliert.

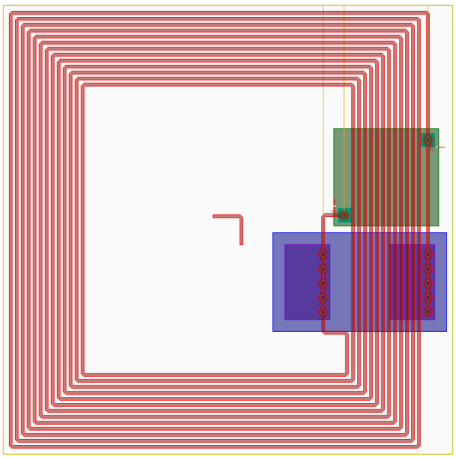
Die in Abbildung 4.27 dargestellten 3D-Simulationen zeigen eine Designvariante, welche mit und ohne Ferrit, sowie auf verschiedenen Materialien simuliert wurden. Die Skalierung ist über alle Abbildungen konstant, um eine einfache optische Vergleichbarkeit zu gewährleisten.

In Abbildung 4.27a ist ein freier Tag zu sehen, d.h. in der Luft und ohne Kontakt zu anderen Materialien. Der selbe Tag mit Ferrit ist in Abbildung 4.27b zu sehen. Diese beiden Bilder dienen als Referenz um zu zeigen, wie die Feldverteilung unter normalen Bedingungen, also ohne Einfluss von externen Umständen, aussieht.

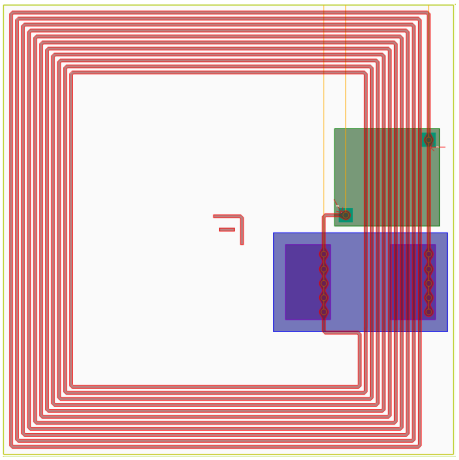
Materialien wie Glas oder Diamant mit keiner bzw. geringer elektrischer Leitfähigkeit weisen einen vernachlässigbaren Einfluss auf die Feldverteilung auf, wie in den Abbildungen 4.27c, 4.27d, 4.27e und 4.27f gezeigt wird. In diesen Materialien können sich nämlich keine Wirbelströme ausbilden, welche mit ihrem eigenen Magnetfeld ansonsten das Erregerfeld schwächen würden. Weitergehende Analysen zum Einfluss von Wirbelströmen auf das Erregerfeld können unter [QC07] nachgelesen werden.

Elektrisch leitfähigen Materialien wie Eisen, oder in Schmuck eingesetztes Silber und Gold, weisen solche Wirbelströme auf. Die dadurch hervorgerufenen Magnetfelder wirken der Ursache (dem Erregerfeld) entgegen und schwächen es dadurch, wie in den Abbildungen 4.28a, 4.28c und 4.28e sehr deutlich erkennbar ist.

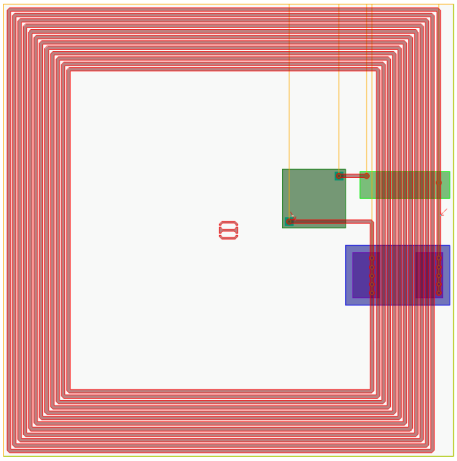
Ferrite weisen eine hohe relative Permeabilität (magnetische Leitfähigkeit) sowie eine sehr geringe elektrische Leitfähigkeit auf.



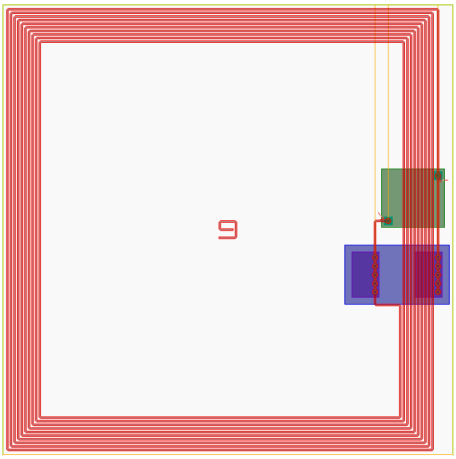
(a) Design 7



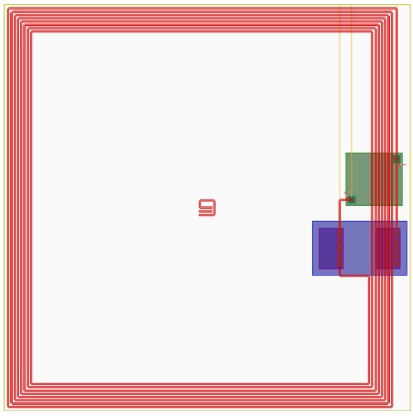
(b) Design 7m



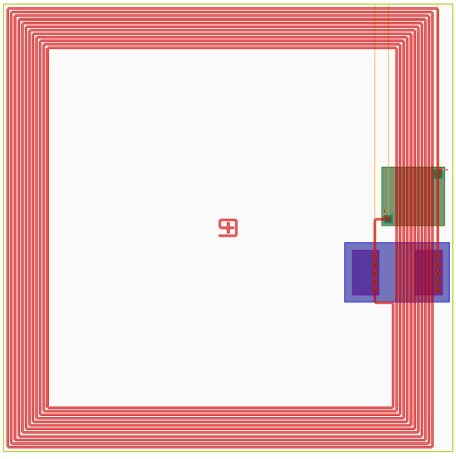
(c) Design 8



(d) Design 9

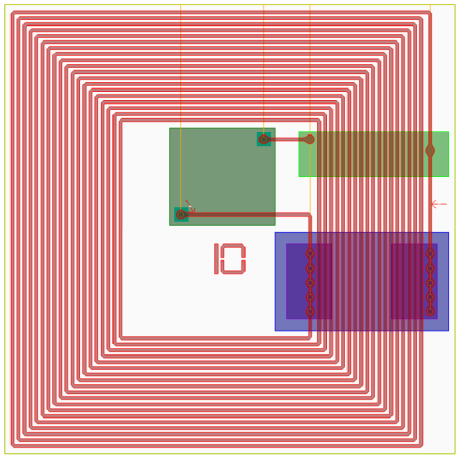


(e) Design 9m

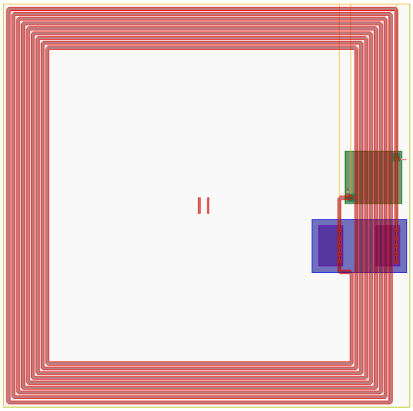


(f) Design 9p

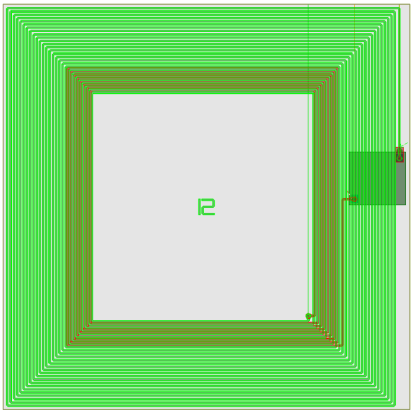
Abbildung 4.26: Layout der Packages mit CIPURSE Move IC



(g) Design 10

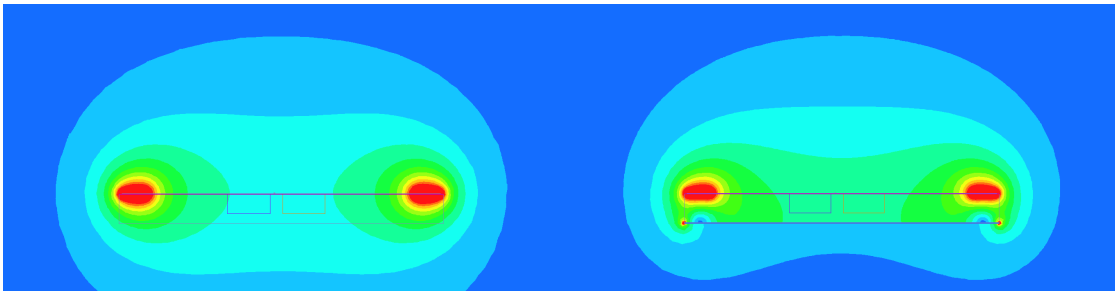


(h) Design 11

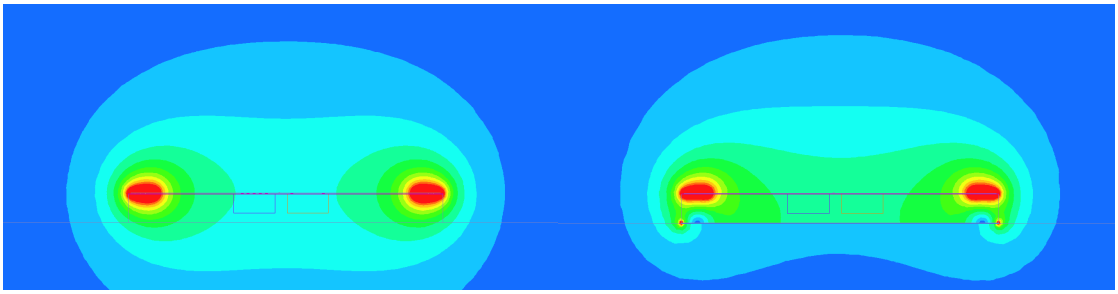


(i) Design 12

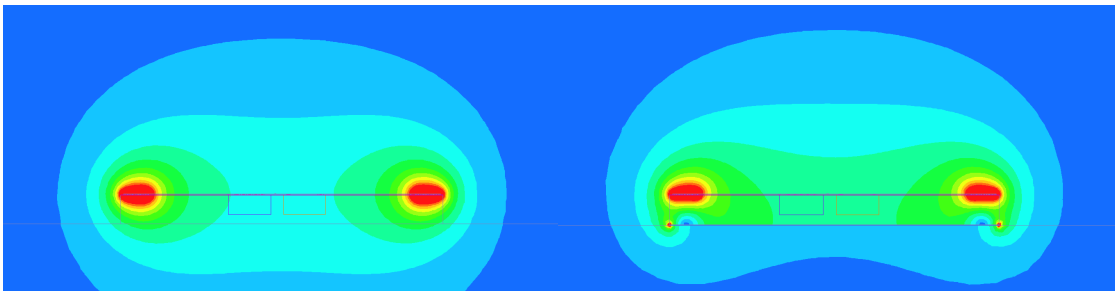
Abbildung 4.26: Layout der Packages mit CIPURSE Move IC (Fortsetzung)



(a) Luft (b) Luft + Ferrit



(c) Diamant (d) Diamant + Ferrit

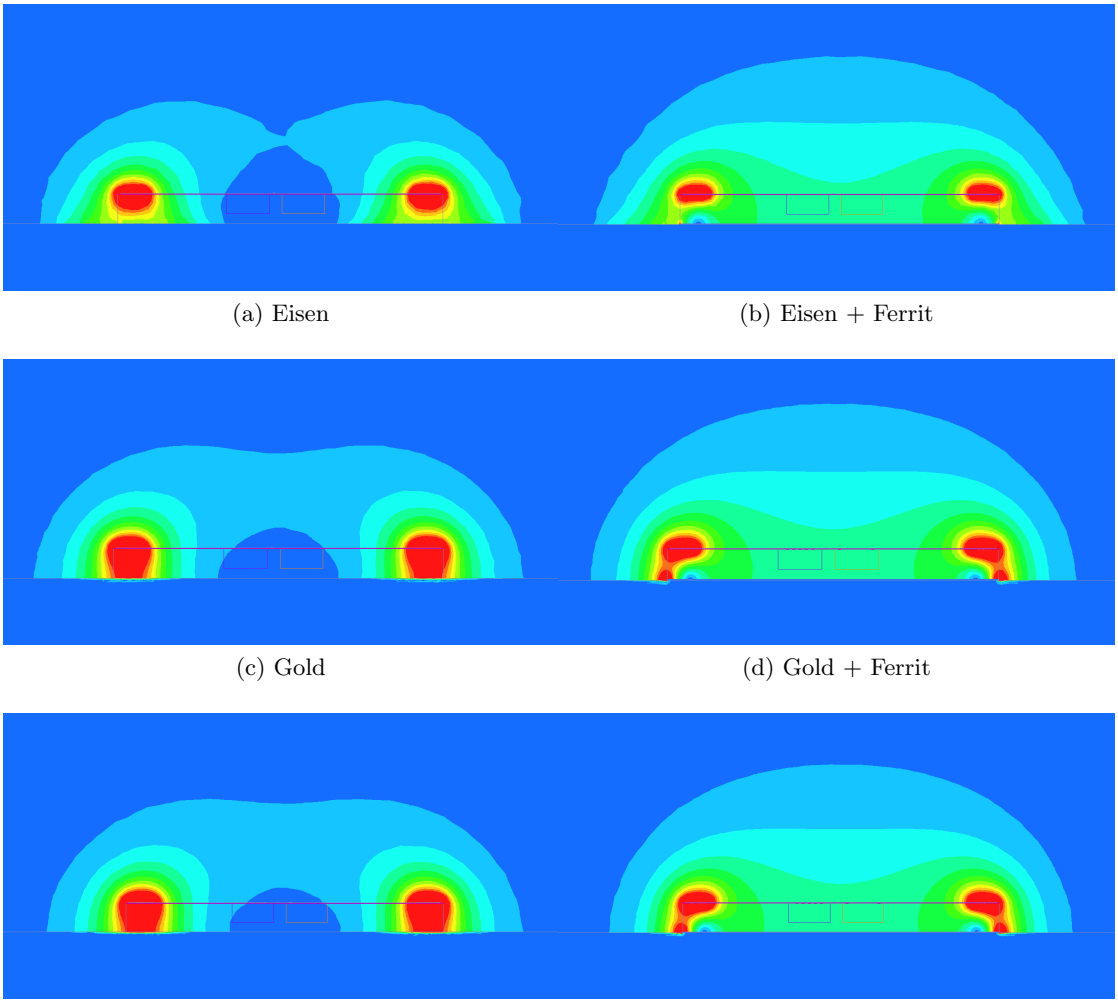


(e) Glas (f) Glas + Ferrit

Abbildung 4.27: H-Feld Verteilung eines Packages auf nicht leitfähigem Untergrund

Eine Ferritschicht zwischen Tag und leitfähiger Oberfläche schirmen deshalb das Erregerfeld vor dem Untergrund ab und verhindern dadurch wiederum die Ausbildung von Wirbelströmen, sowie einer damit einhergehenden Schwächung des Erregerfeldes, wie in den Abbildungen 4.28b, 4.28d und 4.28f sehr gut erkennbar ist. Die Verteilung des Feldes über dem durch Ferrit geschützten Bereich ähnelt dem eines freien Tags in der Luft, wie in Abbildung 4.27b zu sehen ist. Am Rand des Tags, an dem der Ferrit endet, kann trotzdem sehr gut der Einfluss des darunter liegenden Materials aufgrund der Verzerrung der Feldverteilung gezeigt werden.

Die bei diesen Simulationen verwendeten Materialparameter sind unter Tabelle 4.1 aufgeführt.



(a) Eisen (b) Eisen + Ferrit

(c) Gold (d) Gold + Ferrit

(e) Silber (f) Silber + Ferrit

Abbildung 4.28: H-Feld Verteilung eines Packages auf leitfähigem Untergrund

4.6 Demos

4.6.1 Android Applikation

Wird ein Smartphone an einen CIPURSE Tag gehalten, wird, wie in Abbildung 4.29 dargestellt, ein Authentifizierungsprozess gestartet. Dabei wird zuerst eine Verbindung mit dem Tag hergestellt. Anschließend wird mittels gegenseitiger Authentifizierung, sowie dem Applikationsschlüssel, ein gesicherter Kommunikationskanal aufgebaut um die auf dem Tag gespeicherte Applikationsinfo auszulesen. Danach wird der selbe Vorgang verwendet um einen weiteren gesicherten Kanal mit dem Authentifizierungsschlüssel aufzubauen, um damit den eigentlichen Inhalt des Tags auszulesen. Stimmt dieser mit dem erwarteten Inhalt überein, wird der Tag als verifiziert gewertet und eine entsprechende Meldung ausgegeben. Wenn der Inhalt nicht übereinstimmt wird die Verifizierung als gescheitert angesehen und ebenfalls eine Meldung auf dem Bildschirm ausgegeben.

Material	**relative Permittivität** ϵ_r **[.]**	**relative Permeabilität** μ_r **[.]**	**elektrische Leitfähigkeit** σ **[Siemens/m]**
Ferrit	12,0	1000	0,01
Silizium	11,9	1,0	0
FR4 (epoxy)	4,4	1,0	0
PET	3,2	1,0	0
Luft	1,0006	1,0000004	0
Vakuum	1,0	1,0	0
Diamant	16,5	1,0	0
Glas	5,5	1,0	0
Silber	1,0	0,99998	$61 \cdot 10^6$
Gold	1,0	0,99996	$41 \cdot 10^6$
Eisen	1,0	4000	$10,3 \cdot 10^6$

Tabelle 4.1: Materialparameter für die 3D-Simulation der H-Feld Verteilung

MainActivity

In der *MainActivity* Klasse werden zuerst alle nötigen Initialisierungen der GUI vorgenommen. Sobald der Android *NfcAdapter* einen neuen Tag in Reichweite erkennt wird ein Event ausgelöst, welches einen neuen Kommunikationskanal via *CommsChannel* zum Tag öffnet. Konnte dieser Kommunikationskanal erfolgreich geöffnet werden, wird *sampleOperation()* aus der *CommandLibraryDemo* Klasse aufgerufen.

CommsChannel

Die *CommsChannel* Klasse übernimmt die Kommunikation mit dem CIPURSE Tag über eine CIPURSE spezifische externe Bibliothek.

Diese Bibliothek stellt folgende Methoden zur Verfügung:

- *byte[] transmit(byte[])*: Sendet ein Byte Array an den Tag und verarbeite die Antwort. Sofern ein Kommando mit Datenanfrage übertragen wurde, wird das Ergebnis dieser Anfrage verarbeitet, ansonsten wird nur geprüft, ob das Kommando erfolgreich war.
- *void open()*: Schließt eine offene Verbindung und stellt eine neue Verbindung her.
- *void close()*: Schließt die Verbindung.
- *void reset()*: Wenn bereits ein Tag verbunden ist, wird diese Verbindung zuerst getrennt und anschließend eine neue hergestellt.
- *bool isOpen()*: Mit dieser Methode kann abgefragt werden, ob bereits ein offener Kanal zu einem Tag geöffnet ist. Es wird *true* zurück gegeben, wenn bereits ein Kanal offen ist, ansonsten *false*.

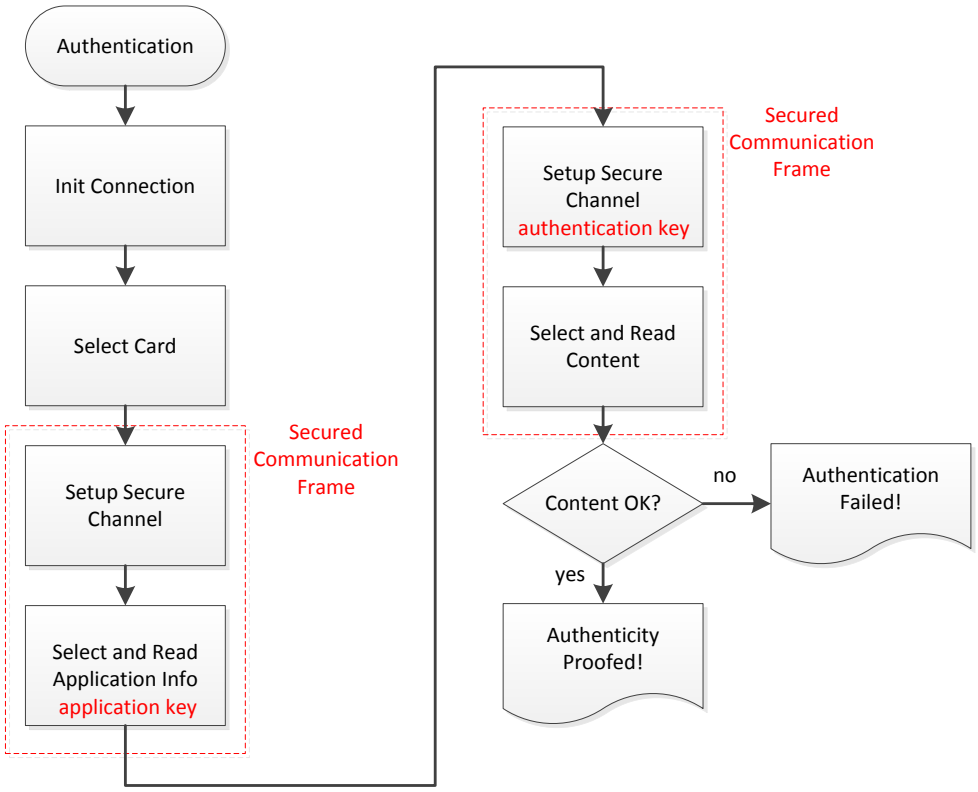


Abbildung 4.29: Flussdiagramm der Android Demo

CommandLibraryDemo

Die Hauptklasse implementiert den Authentifizierungsalgorithmus nach Abbildung 4.29. Die Methode *sampleOperation()* wird von der *MainActivity* aufgerufen sobald ein Tag in Reichweite ist.

Hier wird neben der gegenseitigen Authentifizierung auch das Auslesen der Daten durchgeführt. Sie übernimmt außerdem die Fehlerhandhabung im *errorHandler()*. Dieser vergleicht die erhaltene mit der gewünschten Antwort und gibt im Fehlerfall eine Meldung aus.

4.6.2 PC-Demo: Zugangskontrolle

Die PC-Demo besteht aus drei Teilen:

- Einem Modell einer Tür mit mechanischem Schloss und elektronischer Aufschließsperre (siehe Unterabschnitt 4.6.2)

- Einem RFID-Lesegerät mit dazugehöriger Software sowie einer Booster-Antenne (siehe Unterabschnitt 4.6.2)
- Einem Aktor mit Steuerelektronik und einer Software zur Schlossfreigabe (siehe Unterabschnitt 4.6.2)

Die Tür

Das ca. 40cm x 25cm große Modell der Tür enthält ein Zargenschloss mit zwei zugehörigen, mechanisch identischen Schlüsseln. Einer dieser beiden Schlüssel enthält zusätzlich noch einen CIPURSE Tag an der Spitze.

Auf der Rückseite befindet sich ein Hubmagnet mit Rückstellfeder, welcher im entspannten Zustand das Schloss mechanisch sperrt. Wird dieser Hubmagnet aktiviert, zieht sich der Anker und somit die Verriegelung zurück und das Schloss lässt sich mechanisch aufsperren. Außerdem befinden sich die benötigten Elektronikkomponenten wie Relaisplatine, Spannungsversorgung etc. auf der Rückseite. Um die Kommunikation mit dem RFID-Lesegerät zu ermöglichen, wird noch eine HF-Antenne im Inneren verbaut, deren Anschluss ebenfalls auf der Rückseite herausgeführt wird.

Authentifizierung

Um den Tag auszulesen wird eine Spule in das Schloss integriert. Mithilfe eines RFID-Kartenlesegerätes und der Booster-Antenne (siehe Abbildung 4.30) sowie einer in Java geschriebenen Software wird der Tag ausgelesen bzw. die Authentifizierung des Schlüssel gegenüber dem Computer durchgeführt. Die gesamte Software wird in einer *FacilityAccessDemo* Klasse zusammengefasst. Für die Kommunikation mit der Karte werden CIPURSE spezifische Funktionen verwendet, welche als externe Bibliothek zur Verfügung stehen. Dies betrifft etwa den Aufbau des sicheren Kommunikationskanals, da hier die 3-Wege Authentifizierung durchgeführt werden muss.

Dabei wird zuerst eine Verbindung mit dem RFID-Lesegerät hergestellt. Befindet sich eine Karte auf dem Lesegerät, oder wie in diesem Fall ein Schlüssel mit integriertem Transponder im Schloss, wird diese ausgewählt. Andernfalls wird eine Zeit lang gewartet und der Vorgang von vorne begonnen (*polling*). Im Anschluss wird versucht eine gesicherte Verbindung mit der Karte aufzubauen. Dazu muss die Karte für die Anwendung konfiguriert sein, sowie über den passenden Schlüssel verfügen (*application key*).

Während dieses Prozesses wird eine sogenannte gegenseitige Authentifizierung (*mutual authentication*) durchgeführt. Das bedeutet, dass sich nicht nur die Karte gegenüber dem Lesegerät authentifizieren muss, sondern sich auch das Lesegerät gegenüber der Karte ausweisen muss. Dies geschieht mittels einer 3-Wege-Authentifizierung nach [ISO04]. Wenn dieser Prozess abgeschlossen ist steht den beiden Kommunikationspartnern zusätzlich ein temporärer Schlüssel (*session key*) zur Verfügung, um die nachfolgende Kommunikation abzusichern. Sämtliche Kommunikation die zu einer solchen gesicherten Verbindung mit einem temporären Schlüssel gehört, wird unter dem Begriff *secured communication frame* zusammengefasst.

Jetzt kann die Anwendungsinformation ausgelesen werden. Wenn diese korrekt ist wird eine neue gesicherte Verbindung aufgebaut, diesmal um die Authentifizierung durchzuführen.

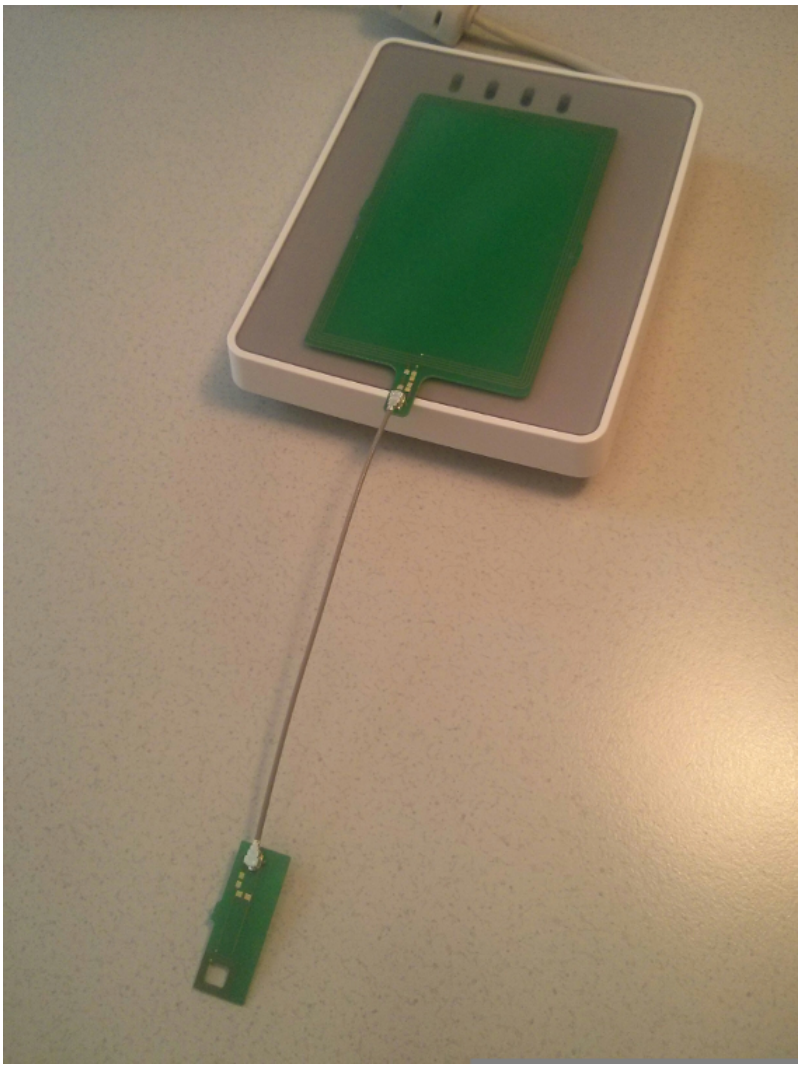


Abbildung 4.30: RFID-Lesegerät mit externer Booster-Antenne

Dazu wird der zweite Schlüssel verwendet (*authentication key*) und anschließend können die Berechtigungen ausgelesen werden. Wenn diese korrekt sind wird die Tür freigegeben. Der Zugang wird also nur gewährt, wenn die Karte für diese Anwendung konfiguriert ist und über zwei korrekte 128 Bit AES[3] Schlüssel verfügt, sowie die passenden Berechtigungen hinterlegt sind. Der Ablauf dieser Authentifizierung ist in Abbildung 4.31 ersichtlich.

Zusätzlich zur automatischen Freigabe kann das Schloss ebenfalls manuell geöffnet bzw. gesperrt werden. Nach manueller Öffnung sperrt es sich nach einer definierten Zeitspanne wieder automatisch.

[3] Advanced Encryption Standard

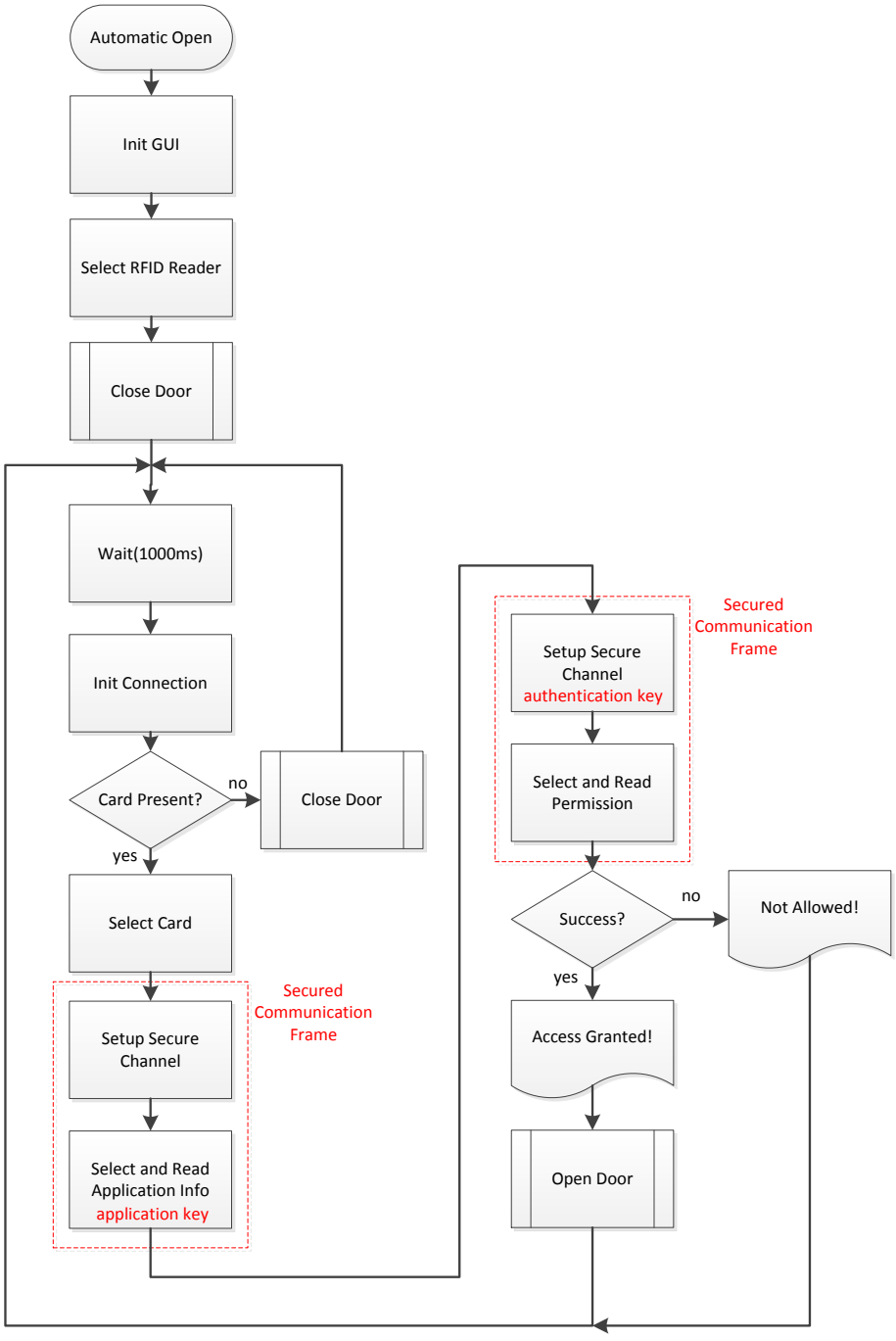


Abbildung 4.31: Flussdiagramm der PC-Demo

Freigabe

Wenn die Authentifizierung laut Abschnitt 4.6.2 erfolgreich ist, wird der Hubmagnet mittels Relais geschaltet um das Schloss freizugeben. Als Relaiskarte wird eine 4-fach USB Relaiskarte von Conrad mit einem CP2104 USB-to-UART Bridge Chip von Silicon Labs verwendet. Diese verfügt bereits über eine fertige DLL Datei, mit deren Funktionen die Relais vom PC aus geschaltet werden können. Zu diesem Zweck wird ein in C++ geschriebenes Programm verwendet, welches die Verbindung mit der Relaiskarte herstellt und das gewünschte Relais ein (*openDoor.exe*) bzw. ausschaltet (*closeDoor.exe*). Mit dem Relais wird die Versorgungsspannung auf den Hubmagneten geschaltet und der Anker zieht an, wodurch das Schloss mechanisch freigegeben wird. Der verwendete Hubmagnet ist zur Sicherheit zum dauerhaften Einschalten ausgeführt. Wenn das Relais wieder öffnet und der Hubmagnet von der Versorgungsspannung getrennt wird, wird der Anker mittels Feder wieder in seine Ausgangsposition zurück gebracht und das Schloss wieder mechanisch verriegelt. Ab diesem Zeitpunkt kann das Schloss nur noch versperrt werden.

Kapitel 5

Evaluierung der Ergebnisse

Von den in den vorigen Kapiteln vorgestellten 22 Designvarianten wurden aus Zeitgründen nur 7 gefertigt. Leider musste auf die zweilagigen Designs und auf sämtliche Varianten mit der Größe von 5x5mm verzichtet werden. Außerdem fehlten die Dummies, bei denen die Antenne isoliert von den übrigen Bauteilen ausgeführt wurde. Deshalb konnte keine alleinige Vermessung der Antenne vorgenommen werden. Gefertigt wurden die Designs mit den Nummern 1, 2, 5, 7, 7m, 10 sowie 13.
Insgesamt wurden drei Wafer im ersten Durchlauf gefertigt. Von diesen drei Wafern wurde einer vor dem finalen Fertigungsschritt entnommen, um zeitnah Messungen durchführen zu können. Die anderen beiden Wafer wurden fertig prozessiert und als einzelne Packages zur Verfügung gestellt.

5.1 Prototypen

In der ersten Charge wurde ein Wafer mit rund 230 Samples gefertigt. Auf dem Foto in Abbildung 5.1 ist dieser Wafer zu sehen. Die einzelnen Packages sind gut erkennbar. Dieser Wafer wurde vor dem letzten Fertigungsschritt entnommen und es fehlen deshalb die Ferrite auf den Packages. Dies war aufgrund von Zeitproblemen notwendig. So konnten die Prototypen schon vermessen werden bevor die Fertigung komplett abgeschlossen war. In dieser Form mussten die einzelnen Packages noch vorsichtig vom Wafer getrennt werden.

Der gezeigte Wafer enthielt Prototypen der Designs 1, 2, 5, 7, 7m, 10 und 13, jedoch ohne Ferrit. Es sind dies jeweils Varianten mit einer Größe von 3x3mm sowie unterschiedlichen ICs. Die Packages wurden entnommen und zuerst unter einem Mikroskop auf offensichtliche Produktionsfehler untersucht. Dadurch konnten fehlerhafte Samples bereits vor den Messungen aussortiert werden. Ein fehlerfreies Package mit der Designnummer 10 ist in Abbildung 5.2 zu sehen. Es sind hier die einzelnen Bauteile wie der IC in der Mitte, der Kondensator rechts unten, die Untertunnelung rechts oben und die Antenne sehr gut zu erkennen. Um beim Kondensator eine gute Verbindung mit der Spule zu erreichen, wurde diese mit mehreren Durchkontaktierungen je Anschlusspad hergestellt, wie im Foto gut erkennbar ist.

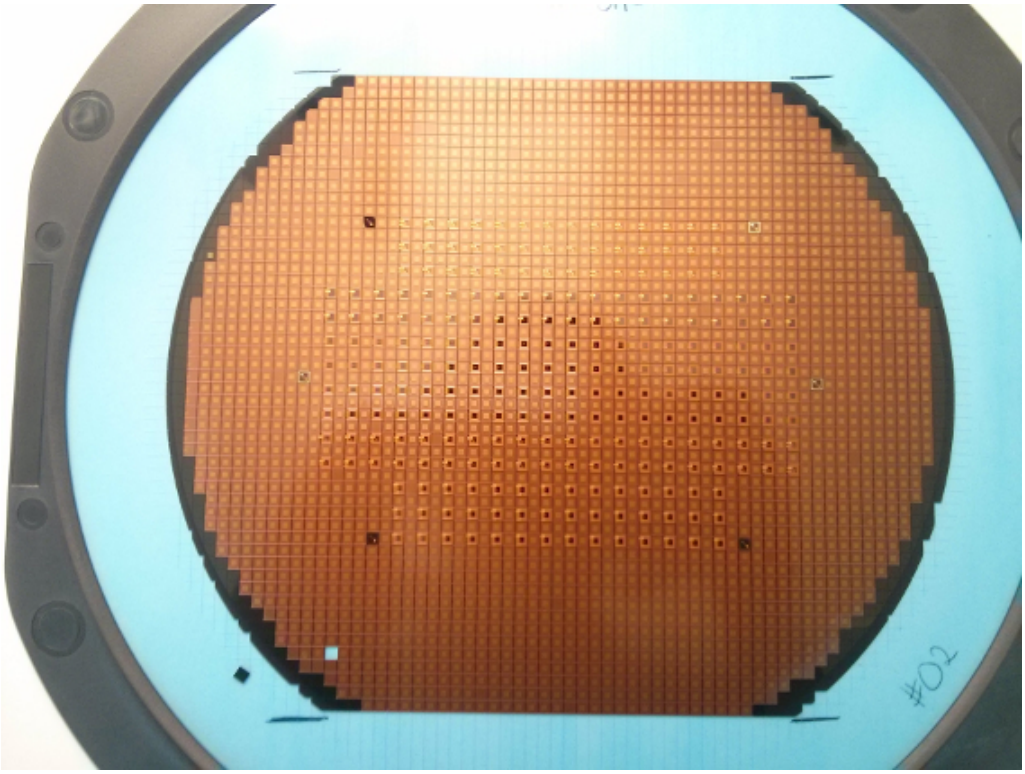


Abbildung 5.1: Foto des ersten gefertigten Wafers

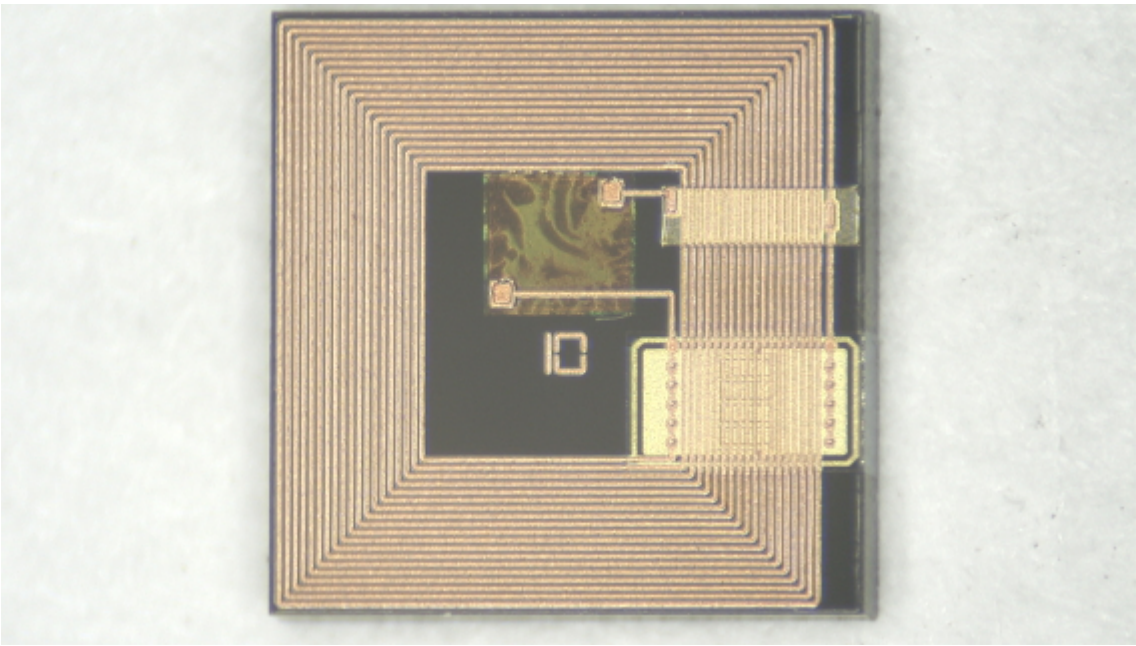


Abbildung 5.2: Foto eines 3x3 mm großen Packages unter dem Mikroskop

5.1.1 Messaufbau

Von den gefertigten Prototypen wurden funktionsfähige Exemplare entnommen und ihre Resonanzfrequenz, mit einem Testaufbau wie in Abbildung 5.3 dargestellt, gemessen. Hierfür wurde der Network Analyzer *Bode 100* von Omicron Labs [1] mit der dazugehörigen Software *Bode Analyzer Suite* verwendet.

Gemessen wurde die Impedanz der Antenne des Lesegerätes über einen vorgegebenen Frequenzbereich (*frequency sweep*). Die Leserantenne wurde dazu an den Ausgang des Messgerätes angeschlossen. Bei der Resonanzfrequenz erreicht der Realteil der Impedanz bei Reihenschwingkreisen sein Maximum. Dies ist als Scheitelpunkt der Kurve sehr gut erkennbar, wie in Abbildung 5.4a gezeigt wird.

Vor der Messung wurde der Messaufbau an der Kontaktstelle zwischen Kabel und Leserantenne kalibriert, damit Einflüsse durch die Leitungsimpedanz des Verbindungskabels nicht in das Messergebnis mit eingehen konnten. Die Impedanz der dort angeschlossenen Antenne wurde hierbei nicht berücksichtigt. Gemessen wurde der Frequenzverlauf der Samples von 5 bis 40 MHz, eine Messung ist in Abbildung 5.4 dargestellt. Diese Messung stammt von einem Sample des Designs 10, welches zwar nicht mit Ferrit entworfen wurde, zu Testzwecken trotzdem zusätzlich mit Ferrit versehen wurde. Die Resonanzfrequenz lag hier bei sehr guten 13,75 MHz.

5.1.2 Messergebnisse

Die Anzahl der vermessenen Samples je Design variierte zwischen 9 und 25, da nur funktionierende Samples vermessen wurden. Die ersten Prototypen wurden komplett ohne Ferrit geliefert. Das bedeutet, dass auch jene Designs, bei denen Ferrit vom Design vorgesehen war, diese eine Lage noch fehlte. Dies ermöglichte bei den Designs mit den Nummern 2, 7 und 7m die Messung der Resonanzfrequenz mit sowie ohne Ferrit. In Tabelle 5.1 sind die Messergebnisse dargestellt.

Diese Tabelle umfasst folgende Punkte:

- Designnummer
- Anzahl der gemessenen Samples
- die simulierte Resonanzfrequenz f_{res} in MHz
- die kleinste gemessene f_{res} aller Samples dieser Gruppe in MHz
- den gemittelten Wert über alle gemessenen f_{res} in MHz
- die höchste gemessene f_{res} aller Samples dieser Gruppe in MHz

Bei den Designs 2, 7 und 7m wurde die Resonanzfrequenz zuerst ohne Ferrit gemessen. Diese Messergebnisse sind in den jeweiligen Zeilen in Klammern dargestellt. Anschließend wurden die Ferrite auf die Packages aufgebracht und die Messungen wiederholt.

Die Messungen zeigen, dass bis auf eine Ausnahme sämtliche gemessenen Frequenzen über denen der Simulation liegen. Die gemittelten Werte der Messungen liegen zwischen 0,78 und 2,41 MHz über denen der Simulation.

[1] `https://www.omicron-lab.com/bode-100/product-description.html`

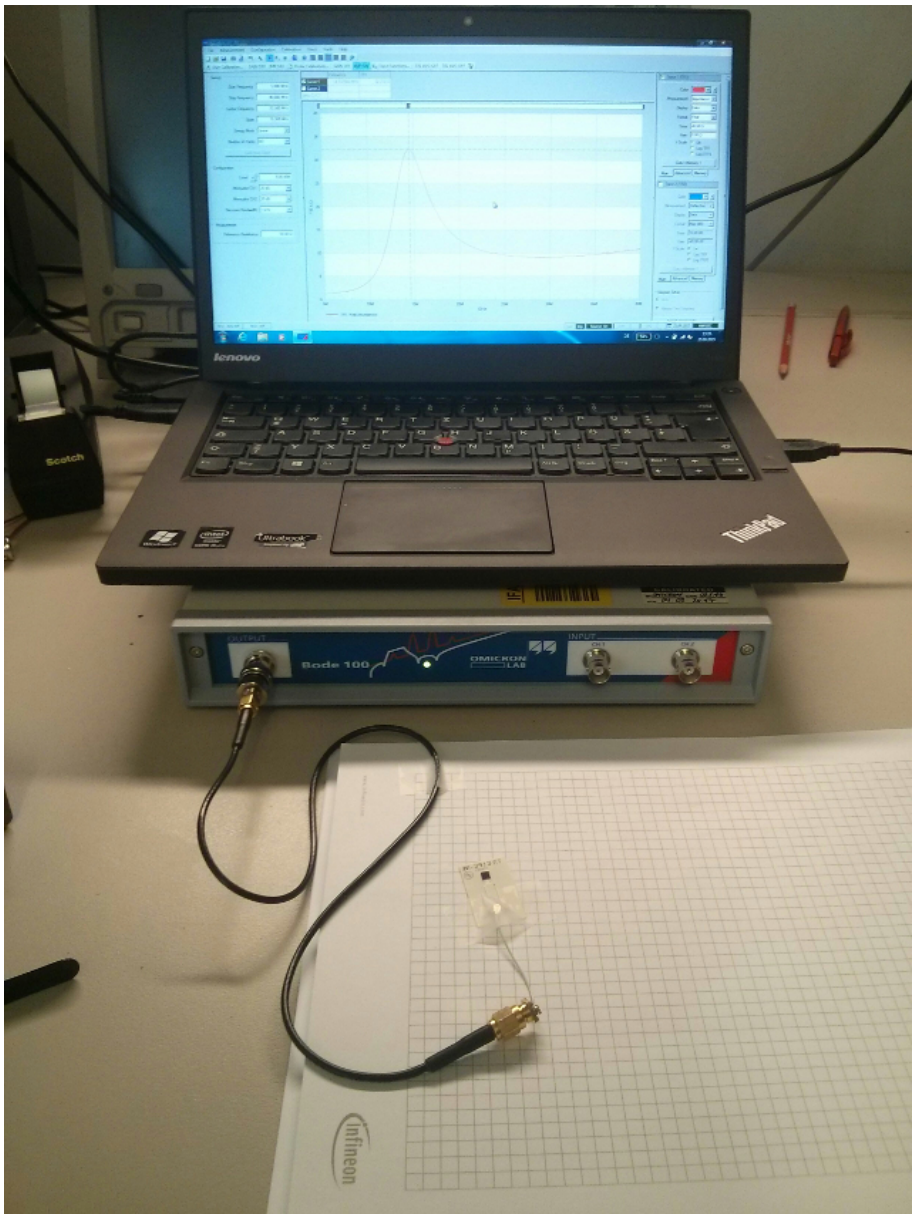
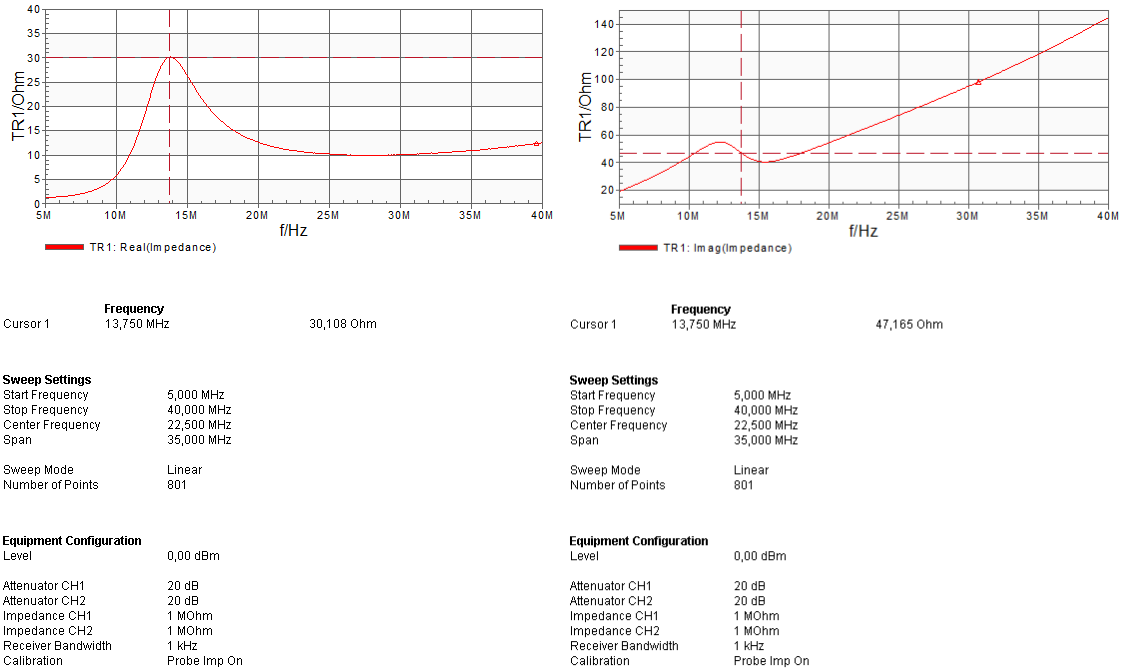


Abbildung 5.3: Aufbau zur Messung der Resonanzfrequenz

Über alle Messungen liegt eine Streuung der Werte zwischen 1,88 MHz nach unten, sowie 1,81 MHz nach oben vor. Das Design 7m hat mit einem Bereich von 2,76 MHz den größten Streubereich aller Gruppen. Die Streuung der Messergebnisse ist in Abbildung 5.5 grafisch aufgetragen. Wie anhand der Designs 2, 7 und 7m erkennbar ist, verringert sich die Resonanzfrequenz durch das Hinzufügen von Ferrit um etwa ein MHz. Da die Messungen zeigen, dass die Resonanzfrequenz bei beinahe allen Samples zu hoch ist, könnte diese mit einer zusätzlichen Ferritschicht gesenkt werden.



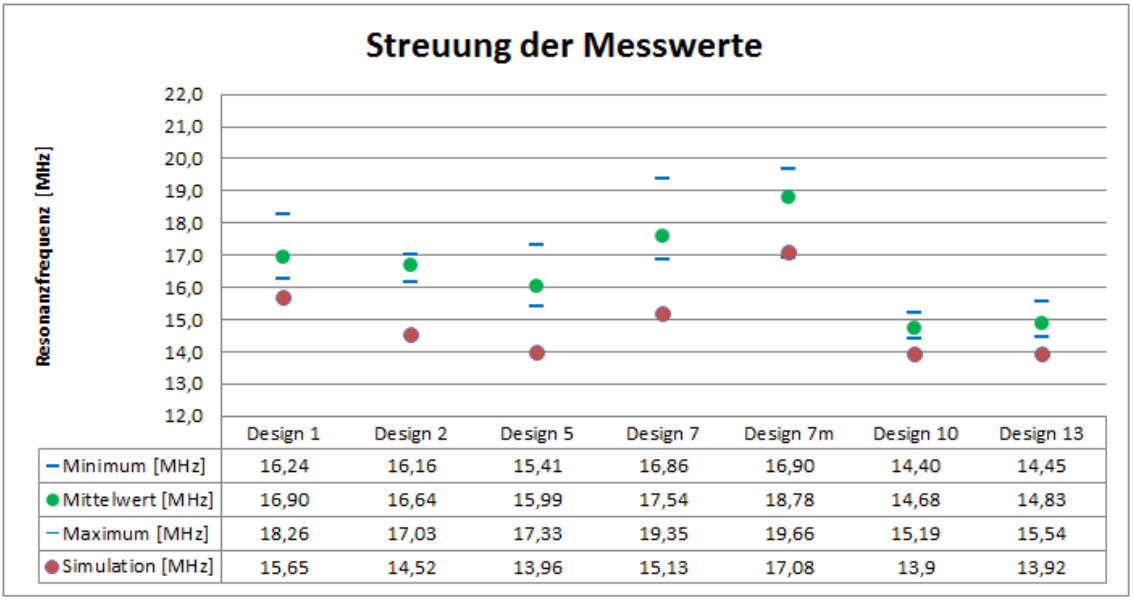
(a) Realteil (b) Imaginärteil

Abbildung 5.4: Darstellung der Messung eines Packages

Design-nummer	**Anzahl der Samples**	f_{res} **[MHz] simuliert**	f_{res} **[MHz] gemessen minimum**	f_{res} **[MHz] gemessen gemittelt**	f_{res} **[MHz] gemessen maximum**
1	25	15,65	16,24	16,90	18,26
2	19	14,52	16,16 (17,02)	16,64 (17,75)	17,03 (18,39)
5	25	13,96	15,41	15,99	17,33
7	9	15,13	16,86 (17,73)	17,54 (18,35)	19,35 (20,00)
7m	11	17,08	16,90 (17,95)	18,78 (19,88)	19,66 (20,84)
10	22	13,90	14,40	14,68	15,19
13	24	13,92	14,45	14,83	15,54

Tabelle 5.1: Vergleich der gemessenen mit den simulierten Resonanzfrequenzen

Eine Erklärung für die Abweichung der Simulation von den Messungen stellen die Bauteiltoleranzen dar. Die Simulationen beruhen auf der Annahme, dass sämtliche Bauteile wie Kondensator, IC, Spule, etc. ideal sind und daher keine Abweichungen hinsichtlich ihrer Werte aufweisen. Dies trifft bei real gefertigten Bauteilen nicht zu. Diese sind immer mit Toleranzen und Abweichungen von ihren Idealwerten behaftet. Als Beispiel soll hierbei der verbaute Kondensator dienen. Dieser hat eine Nominalkapazität von 100 pF. Laut Datenblatt liegt der Toleranzbereich bei $\pm 10\%$. In der Simulation wurde der Kondensator daher mit einer Kapazität von 100 pF verwendet, in der Realität könnte er allerdings eine Kapazität zwischen 90 und 110 pF aufweisen.



	Design 1	Design 2	Design 5	Design 7	Design 7m	Design 10	Design 13
Minimum [MHz]	16,24	16,16	15,41	16,86	16,90	14,40	14,45
Mittelwert [MHz]	16,90	16,64	15,99	17,54	18,78	14,68	14,83
Maximum [MHz]	18,26	17,03	17,33	19,35	19,66	15,19	15,54
Simulation [MHz]	15,65	14,52	13,96	15,13	17,08	13,9	13,92

Abbildung 5.5: Grafische Darstellung der Streuung der Messwerte

In Anbetracht der Tatsache, dass bereits kleine Änderungen der Kapazität in einem Schwingkreis die Resonanzfrequenz verschieben, waren diese Ergebnisse zu erwarten.

5.2 Probleme und nicht erreichte Ziele

5.2.1 Gefertigte Designs

Wie unter Abschnitt 3.3, Unterpunkte 2 und 7, dargestellt, sollten ebenso zweilagige und größere Tags mit 5x5mm hergestellt werden. Diese Varianten wurden zwar erstellt und simuliert, konnten aber leider aufgrund von Ressourcen- und zeitbedingten Engpässen in der Fertigung nicht hergestellt werden. Deshalb fehlen die Ergebnisse dieser Designs in dieser Arbeit. Eine spätere Fertigung und Evaluierung ist auf Basis dieser Arbeit jederzeit möglich.

5.2.2 Padverunreinigung

Während der Fertigung der Tags wurde außerdem ein Problem mit den Anschlusspads einiger ICs festgestellt. Diese Pads wurden als NiAuPd (Nickel-Gold-Palladium) ausgeführt anstatt aus Al (Aluminium). Dies führte während des eWLB-Fertigungsprozesses zu einer Verunreinigung der Pads. Um trotzdem das Risiko eines Ausfalls der Tags aufgrund fehlerhafter Padkontakte zu minimieren, mussten diese Verunreinigungen aufwändig mittels Laser entfernt werden, was einen erheblichen zeitlichen Aufwand bedeutete und den Zeitplan stark beeinträchtigte.

5.2.3 Bauteilhandhabung

Am Beginn des eWLB-Fertigungsprozesses müssen die ICs auf einen Handlingwafer gesetzt werden (siehe Abschnitt 2.4). Dies geschieht mittels Pick-and-Place Robotern. Einige ICs waren jedoch mit 75 μm Dicke wesentlich dünner als die vorgesehenen 120 μm, was anfangs zum Bruch einiger ICs führte und erst durch Anpassungen im Handlingprozess beseitigt werden konnte.

Bevor mit der Fertigung begonnen werden konnte, mussten einige Varianten überarbeitet werden. Aufgrund des Handlingprozesses war das notwendig, da bei Varianten mit selbem IC, aber unterschiedlichem Design, die ICs sowie Kondensatoren auf den selben relativen Koordinaten innerhalb des Tags zu liegen kommen müssen.

Bei der Untersuchung des ersten gefertigten Wafers wurden diverse Fehler gefunden, welche auf die schwierige Handhabung der Bauteile zurückzuführen sind. So sind etwa Bauteile wie der Kondensator verrutscht, was dazu führte, dass dieser beim Vereinzeln der Packages durchgesägt und damit zerstört wurde. Einige Packages weisen darüber hinaus fehlende Bauteile auf, was wiederum der schwierigen Handhabung während der Fertigung geschuldet ist.

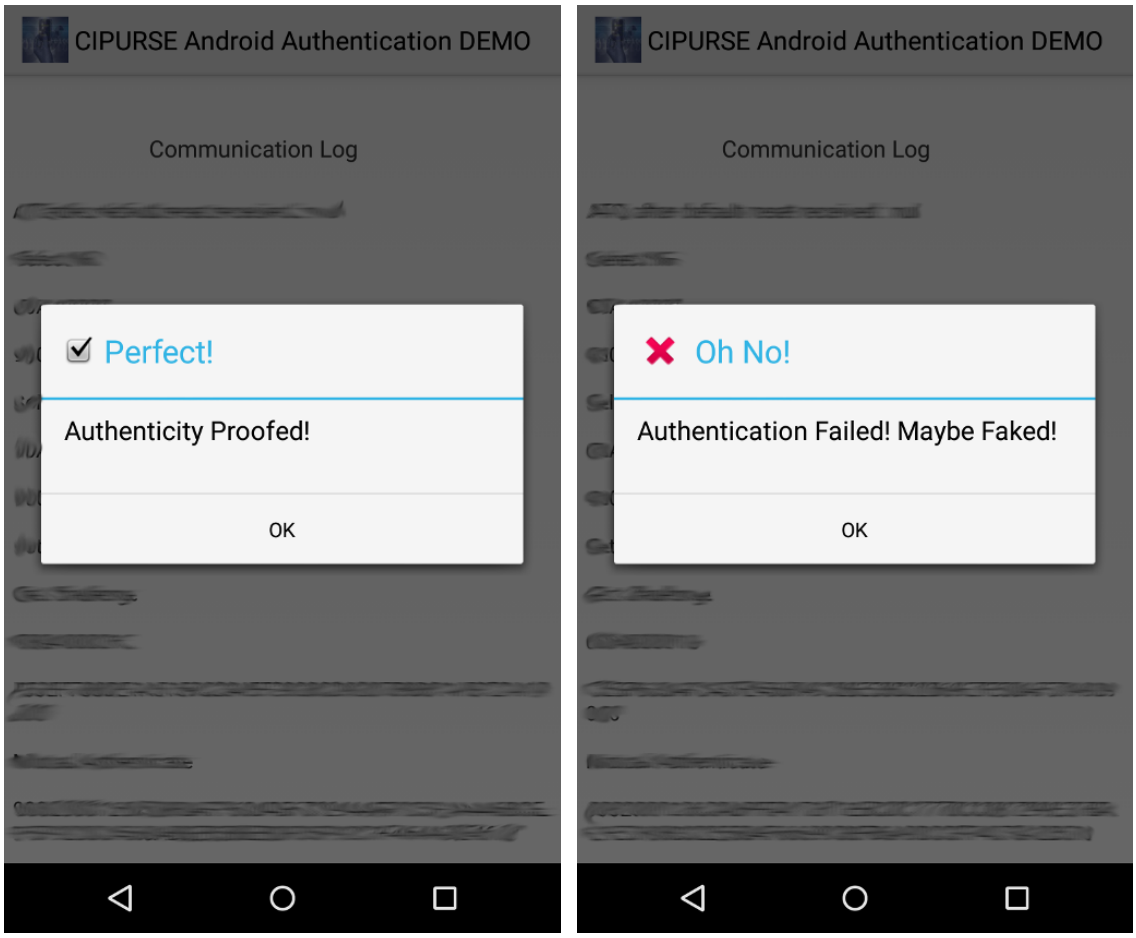
5.3 Demos

5.3.1 Android Applikation

In Abbildung 5.6 sind Screenshots der fertigen Android Demo zu sehen. Diese wurden auf einem Nexus 4 erstellt. In Abbildung 5.6a ist eine gültige Validierung zu sehen, in Abbildung 5.6b ist die Validierung fehlgeschlagen. Damit eine Kommunikation zustande kommen kann, muss der Tag exakt auf der Antenne des Smartphones abgelegt werden. Aufgrund der verschiedenen RFID-Leseeinheiten in Smartphones ist es von Gerät zu Gerät verschieden, ob der Tag erkannt wird oder nicht. Ist die Leseeinheit stark genug, um die hintere Abdeckung des Smartphones leicht zu durchdringen, ist eine Kommunikation möglich, ansonsten muss die hintere Abdeckung abgenommen werden. Verbesserung wäre mittels einer größeren Antenne auf dem Transponder zu erreichen. Designs solcher Tags wurden zwar erstellt, jedoch nicht gefertigt. Mit einer einfachen Booster-Antenne kann die Reichweite des im Smartphone integrierten Lesers jedoch soweit vergrößert werden, um eine Kommunikation zu gewährleisten. Somit sind die Transponder in der Größe 3x3mm nur bedingt für den Einsatz mit Smartphones geeignet.

5.3.2 PC-Demo: Zugangskontrolle

In Abbildung 5.7 ist die fertige PC-Demo zu sehen. Hier ist sehr gut die verwendete Elektronik auf der Rückseite (5.7b) zu erkennen. Der Transponder mit dem CIPURSE IC wurde hierzu auf der Spitze des Schlüssel aufgeklebt, wie in Abbildung 5.8 gezeigt wird. Dieser passt aufgrund seiner Größe exakt in die Öffnungen des Schlosses und konnte somit gut mit der in der Tür verbauten Antenne in Verbindung gebracht werden. Sobald dieser Schlüssel in das Schloss gesteckt wird, kommt er automatisch in die Reichweite der Antenne. Somit kann der Transponder an der Spitze mit dem angeschlossenen PC kommunizieren und die Authentifizierung wird durchgeführt. Ist diese erfolgreich, entriegelt sich die Tür und kann mechanisch aufgesperrt werden.



(a) Validierung OK (b) Validierung NICHT OK

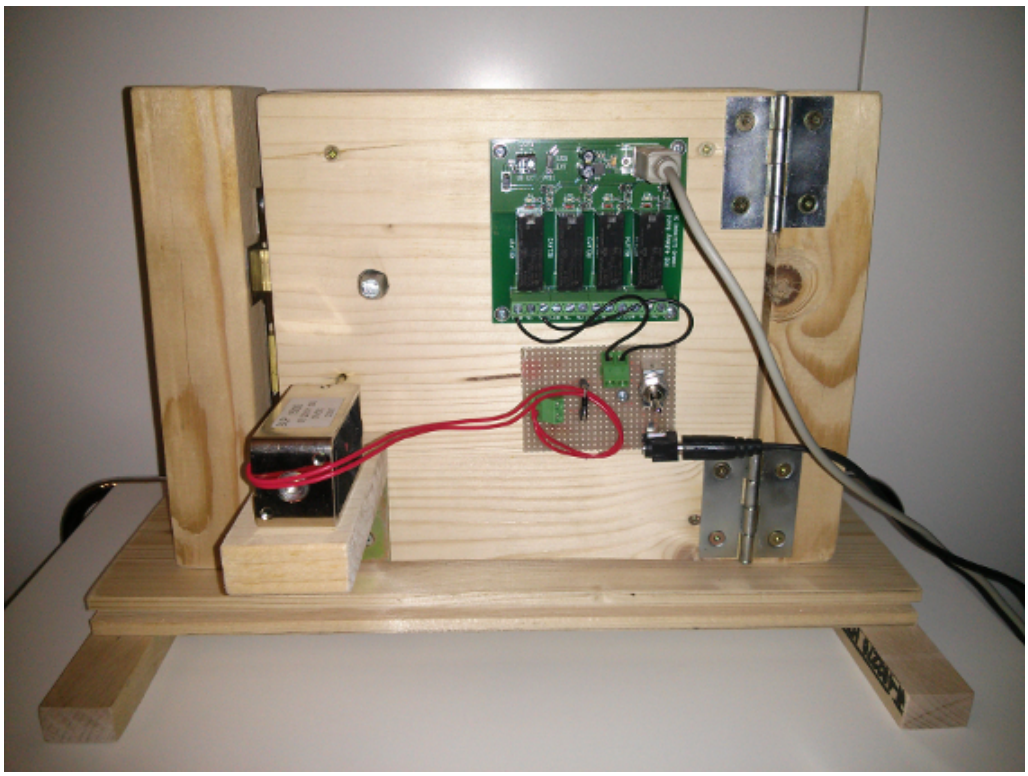
Abbildung 5.6: Android Demo

Wird der Schlüssel wieder entnommen, wird der Transponder aus dem Lesebereich der Antenne entfernt und das Schloss wird wieder automatisch verriegelt.

Ein Screenshot der GUI[2] ist unter Abbildung 5.9 zu sehen. In Abbildung 5.9a ist ein fehlgeschlagener Zutrittsversuch abgebildet. Im Log ist ersichtlich, dass die Antwort nicht mit den geforderten Daten übereinstimmen. Der Zugang wird somit, wie im Bild gezeigt, verweigert. Wird stattdessen eine gültige Zugangskennung verwendet, wie in Abbildung 5.9b, so wird der Authentifizierungsprozess, wie im Log zu sehen ist, erfolgreich durchgeführt und die Tür freigegeben.

[2]Graphical User Interface

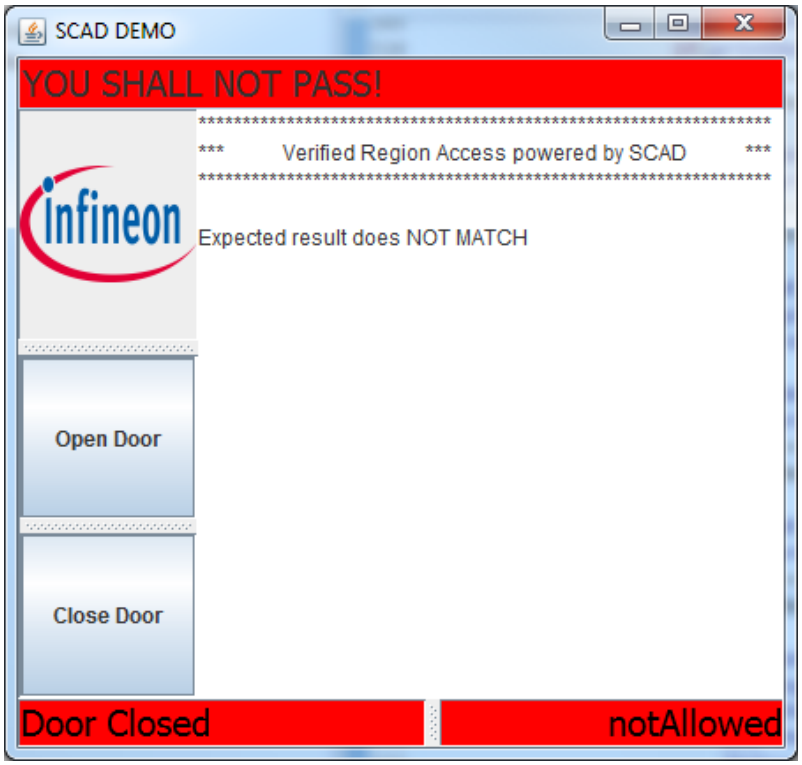
(a) Vorderseite



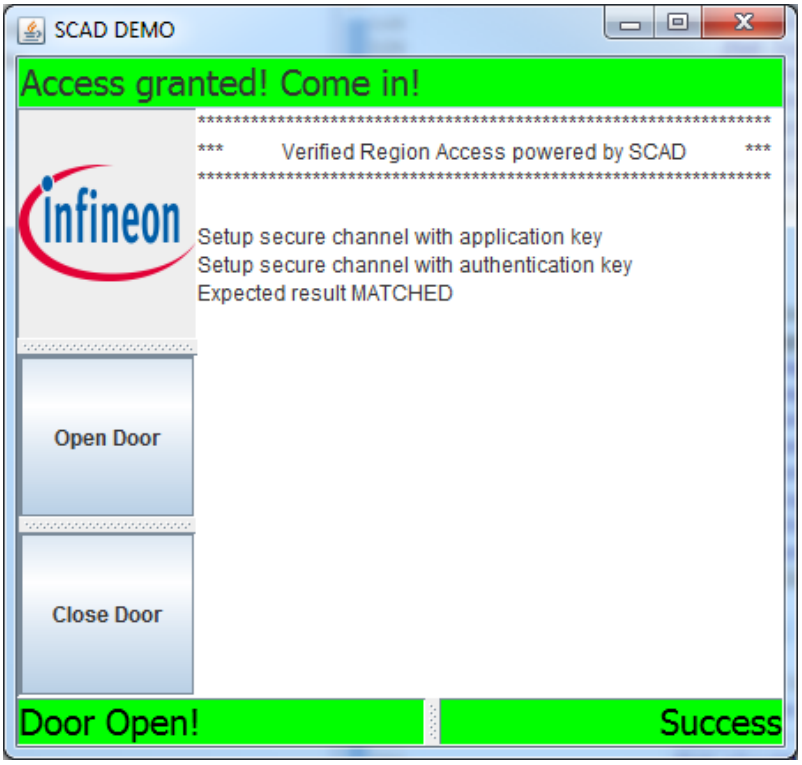
(b) Rückseite

Abbildung 5.7: PC-Demo Tür

Abbildung 5.8: Schlüssel mit und ohne CIPURSE Tag an der Spitze



(a) GUI: Zugang verweigert



(b) GUI: Zugang genehmigt

Abbildung 5.9: GUI der Java Software zur Authentifizierung und Schlossöffnung

Kapitel 6

Zusammenfassung und Ausblick

6.1 Zusammenfassung

Kontaktlose RFID-Transponder finden immer weitere Verbreitung im alltäglichen Leben. Die Anwendungen reichen hier vom kontaktlosen Bezahlen, über Schlüsselkarten zur Zutrittskontrolle bis hin zur Warensicherung. Immer mehr Smartphones werden heutzutage mit RFID-Lesegeräten ausgestattet, die es erlauben, mit solchen Transpondern zu kommunizieren.

RFID-Tags gibt es bereits in vielen verschiedenen Bauarten. Einige davon sind so klein, dass man sie in alltäglichen Gebrauchsgegenständen integrieren kann. Allerdings verfügen nur wenige dieser miniaturisierten Tags über Sicherheitsfunktionen. Während einige zwar Sicherheitsmerkmale, wie etwa einen Passwortschutz, aufweisen, fehlen weitreichendere Absicherungen, wie sie zum Beispiel Verschlüsselungen darstellen, ganz. Somit kann zwar der Inhalt eines solchen Tags vor unbefugtem Auslesen geschützt werden, die Integrität der Daten während der Übertragung ist damit jedoch komplett ungeschützt. Es existieren zwar Lösungen um den Ursprung und die Echtheit eines Tags sicherzustellen, diese Sicherheit kann allerdings nicht auf ein damit verbundenes Produkt übertragen werden.

Diese Arbeit stellte eine Möglichkeit vor, kleine RFID-Transponder herzustellen, die klein genug sind, um sie in Gebrauchsgegenständen zu integrieren, aber groß genug sind, um sie mit einem Smartphone auszulesen. Es wurden diverse Varianten mit unterschiedlichen Zielen designt und simuliert. Einige dieser Designs wurden anschließend gefertigt und vermessen.

Eine spezielle Variante enthält außerdem einen speziellen Chip mit erweiterten Sicherheitsfunktionen. Mit diesem Chip ist es möglich, eine gegenseitige Authentifizierung der beiden Kommunikationspartner durchzuführen. So ist es möglich sicherzustellen, dass nur ein Lesegerät mit den nötigen Berechtigungen mit einem solchen Transponder kommunizieren kann. Weiters kann mittels einer kryptografischen Funktion die Datenintegrität während der Übertragung gesichert werden. Da diese speziellen Transponder auch auf metallischen Oberflächen funktionieren, könnten sie in hochpreisige Produkte wie Schmuck integriert werden. Bei Bedarf kann mit Hilfe der integrierten Sicherheitsfunktionen die Authentizität des Produktes jederzeit überprüft werden.

6.2 Ausblick

Für die Zukunft wäre es möglich, die Tags noch weiter zu verbessern und an spezielle Anwendungsgebiete anzupassen.

- **Größe der Antenne:** In dieser Arbeit wurden nicht nur Packages mit einer Kantenlänge von 3x3 mm entworfen. Die 5x5 mm großen Varianten wurden zwar entwickelt, aber leider nicht gefertigt. Es konnte gezeigt werden, dass selbst mit den kleineren Varianten eine Kommunikation mit mobilen Geräten möglich ist. Allerdings ist diese Kommunikation nur mit Einschränkungen möglich. So muss etwa das integrierte Lesegerät sehr stark sein. Selbst dann muss die Lage der Antenne im Gerät genau bekannt sein und der Transponder genau an der richtigen Stelle auf das Gerät gelegt werden. Mit größeren Transpondern, wie etwa den 5x5 mm großen Varianten, sollte dieses Verhalten verbessert werden können, sodass der Einfluss des Lesegerätes sowie der Antenne minimiert werden kann.

- **Anpassung an die Resonanzfrequenz:** Wie die Messungen gezeigt haben, liegt die Resonanzfrequenz der gefertigten Prototypen über dem gewünschten Wert. Mit einigen einfachen Änderungen im Design der Tags wäre es möglich, die Einflüsse der Fertigung anhand der aktuellen Prototypen zu erfassen und zu kompensieren. Das Ansprechverhalten der Transponder könnte so verbessert werden.

- **Mehrlagige Spule:** Wie einige Designvarianten vorsahen, könnte eine Spule mit einer großen Anzahl an Windungen auch zweilagig ausgeführt werden. Somit sollte es möglich sein, auch mit den kleinen 3x3 mm großen Tags, ein besseres Ansprechverhalten zu erreichen.

- **Alternatives Fertigungsverfahren:** Es könnte auf der Basis der hier vorgestellten Designs ein weiterer Versuch mit einem alternativen Fertigungsprozess stattfinden, welcher womöglich eine Verbesserung gegenüber dem eWLB-Fertigungsprozess bringt. Als alternatives Fertigungsverfahren wäre hier LTCC (low temperature cofired ceramic) zu nennen. Dieses Verfahren erlaubt ebenfalls die Integration von dezidierten Bauteilen und ist für Hochfrequenzanwendungen ideal.

Literaturverzeichnis

[ADS] Advanced Design System. http://www.keysight.com/en/pc-1297113/advanced-design-system-ads?cc=US&lc=eng. Accessed: 2015-04-15.

[BMO+08] M. Brunnbauer, T. Meyer, G. Ofner, K. Mueller, and R. Hagen. Embedded Wafer Level Ball Grid Array (eWLB). In *Electronic Manufacturing Technology Symposium (IEMT), 2008 33rd IEEE/CPMT International*, pages 1–6, Nov 2008.

[Cip] CIPURSE Move. http://www.infineon.com/cms/en/product/smart-card-ic/contactless-memories/SLM+10TLC002L/productType.html?productType=5546d4624a56eed8014a6407eb413bf0. Accessed: 2015-04-15.

[Fin03] Klaus Finkenzeller. *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification*. John Wiley & Sons, Inc., New York, NY, USA, 3rd edition, 2003.

[GNSW11] M. Gebhart, R. Neubauer, M. Stark, and D. Warnez. Design of 13.56 MHz Smartcard Stickers with Ferrite for Payment and Authentication. In *Near Field Communication (NFC), 2011 3rd International Workshop on*, pages 59–64, Feb 2011.

[HFS] Ansys HFSS. http://www.ansys.com/Products/Simulation+Technology/Electronics/Signal+Integrity/ANSYS+HFSS. Accessed: 2015-07-01.

[ICC] Estimating the global economic and social impacts of counterfeiting and piracy. http://www.iccwbo.org/Advocacy-Codes-and-Rules/BASCAP/BASCAP-Research/Economic-impact/Global-Impacts-Study/. Accessed: 2015-08-31.

[IFA] Infineon Technologies Austria AG. http://www.infineon.at. Accessed: 2015-07-06.

[ISO04] ISO. Information technology – Security techniques – Entity authentication. ISO ISO/IEC 9798:1999, International Organization for Standardization, Geneva, Switzerland, 2004.

[ISO13a] ISO. Identification cards – Contactless integrated circuit cards – Proximity cards – Part 1: Physical characteristics. ISO ISO/IEC 14443-1:2008, International Organization for Standardization, Geneva, Switzerland, 2013.

[ISO13b] ISO. Identification cards – Contactless integrated circuit cards – Proximity cards – Part 4: Transmission protocol. ISO ISO/IEC 14443-4:2008, International Organization for Standardization, Geneva, Switzerland, 2013.

[ISO13c] ISO. Identification cards – Physical characteristics. ISO ISO/IEC 7810:2003, International Organization for Standardization, Geneva, Switzerland, 2013.

[ITI] Institut für technische Informatik. `https://www.iti.tugraz.at/cms/`. Accessed: 2015-07-06.

[JK15] K. Jaakkola and P. Koivu. Low-Cost and Low-Profile Near Field UHF RFID Transponder for Tagging Batteries and Other Metal Objects. *Antennas and Propagation, IEEE Transactions on*, 63(2):692–702, Feb 2015.

[LRT08] W. Li, D.C. Rodger, and Y.C. Tai. Implantable RF-coiled chip packaging. In *Micro Electro Mechanical Systems, 2008. MEMS 2008. IEEE 21st International Conference on*, pages 108–111, Jan 2008.

[Maxa] Maxell Coil-on-Chip ME-Y1001/ME-Y2000. `http://biz.maxell.com/en/product_security/?pci=7&pn=sp0006`. Accessed: 2015-07-06.

[Maxb] Maxell Metal Compatible Small RFID Tag. `http://biz.maxell.com/en/product_security/?pci=7&pn=sp0016`. Accessed: 2015-07-06.

[Mov] my-d Move. `http://www.infineon.com/cms/en/product/smart-card-ic/contactless-memories/SLE+66R01PN/productType.html?productType=db3a30433fa9412f013fc34dd6971e69`. Accessed: 2015-04-15.

[Mura] Murata Inlay Tags. `http://www.murata.com/en-eu/products/rfid/magicstrap/hf-inlay`. Accessed: 2015-07-06.

[Murb] Murata small HF/UHF Tags. `http://www.murata.com/en-eu/products/rfid/magicstrap/hf-single`. Accessed: 2015-07-06.

[OSP] OSPT Alliance. `http://www.osptalliance.org/the_standard`. Accessed: 2015-04-15.

[Pac15] Walther Pachler. *Miniaturized RFID Tags Exploring Passive Boosting Technologies*. PhD thesis, Graz University of Technology, 2015.

[PBHH13] W. Pachler, W. Bosch, G. Holweg, and G. Hofer. A novel booster antenna design coupled to a one square millimeter coil-on-chip RFID tag enabling new medical applications. In *Microwave Conference (EuMC), 2013 European*, pages 1003–1006, Oct 2013.

[PGB+14a] W. Pachler, J. Grosinger, W. Bosch, P. Greiner, G. Hofer, and G. Holweg. An on-chip capacitive coupled RFID tag. In *Antennas and Propagation (EuCAP), 2014 8th European Conference on*, pages 3461–3465, April 2014.

[PGB+14b] W. Pachler, J. Grosinger, W. Bosch, G. Holweg, K. Popovic, A. Blumel, and E.J.W. List-Kratochvil. A silver inkjet printed ferrite NFC antenna. In *Antennas and Propagation Conference (LAPC), 2014 Loughborough*, pages 95–99, Nov 2014.

[PGB+14c] W. Pachler, J. Grosinger, W. Bosch, G. Holweg, and C. Steffan. A miniaturized dual band RFID tag. In *RFID Technology and Applications Conference (RFID-TA), 2014 IEEE*, pages 228–232, Sept 2014.

[Pro] my-d Proximity. `http://www.infineon.com/cms/en/product/smart-card-ic/contactless-memories/SLE+66R32P/productType.html?productType=db3a30433fa9412f013fc34599a41e53`. Accessed: 2015-04-15.

[QC07] Xianming Qing and Zhi Ning Chen. Proximity Effects of Metallic Environments on High Frequency RFID Reader Antenna: Study and Applications. *Antennas and Propagation, IEEE Transactions on*, 55(11):3105–3111, Nov 2007.

[TUG] Technische Universität Graz. `http://www.tugraz.at`. Accessed: 2015-07-06.

[Vic] my-d Vicinity. `http://www.infineon.com/cms/en/product/smart-card-ic/smart-card-module/contactless-memories/SRF+55V02P+HC/productType.html?productType=db3a30433fcce646013fd279c4d024ff`.