Bundesamt
für Sicherheit in der
Informationstechnik

Dokument ist noch aktuell. (Stand 2020)

Messung der Abstrahleigenschaften von RFID-Systemen (MARS)

Projektdokument 1: Teilbericht zu den Möglichkeiten des passiven Mitlesens einer RFID-Kommunikation

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 (0)22899 9582 - 5331
E-Mail: rfid@bsi.bund.de
Internet: http://www.bsi.bund.de

Inhaltsverzeichnis

1. Zielsetzung

RFID-Systeme werden mittlerweile in vielen Bereichen eingesetzt, um gespeicherte Daten automatisch und schnell zu identifizieren. Sie werden in Zukunft auch in zunehmendem Maß für sicherheitsrelevante Zwecke genutzt werden. Die Studie „Messung der Abstrahleigenschaften von RFID-Systemen“ (MARS) wurde in Auftrag gegeben, um die Angriffsmöglichkeiten und die Robustheit von RFID Systemen zu untersuchen. Sie gliedert sich in die Hauptpunkte:

- passives Mitlesen der Kommunikation bei ISO 14443 und ISO 15693
- aktives Auslesen der Tags über große Entfernungen
- aktives Stören der Kommunikation für alle zu untersuchenden Systeme
- Simulation eines „Blocker-Tags“ für das System nach ISO 14443

Das vorliegende Projektdokument 1 stellt die Messergebnisse zum Punkt „passives Mitlesen der Kommunikation bei ISO 14443- und ISO 15693-Systemen“ dar.

2. Begriffsbestimmung

Bei der Diskussion möglicher Gefährdungen für RFID-Systeme ist häufig zu beobachten, dass Begrifflichkeiten nicht eindeutig verwendet werden. Aus diesem Grund soll innerhalb des vorliegenden Dokuments eine einheitliche Terminologie verwendet werden, die im Folgenden beschrieben wird.

2.1 Passives Mitlesen einer Kommunikation

Beim passiven Mitlesen wird die bestehende Kommunikation zwischen einem Transponder und einem Reader durch eine passive dritte Partei, den Angreifer, abgehört. Die passive Partei greift nicht aktiv in die Kommunikation zwischen Lesegerät und Transponder ein, sondern beschränkt sich ausschließlich auf das Mithören der stattfindenden Kommunikation.

2.2 Aktives Auslesen eines Transponders

Während des aktiven Auslesens versucht ein Angreifer, einen Transponder direkt anzusprechen. Zu diesem Zweck verwendet der Angreifer ein (modifiziertes) Lesegerät, das ihm durch eine geeignete Wahl der Sendeleistung sowie der verwendeten Antenne eine Erhöhung der Lesereichweite gestattet.

2.3 Aktives Stören einer Kommunikation

Unter dem aktiven Stören einer RFID-Kommunikation versteht man die Beeinflussung des Kommunikationsvorganges durch einen Störsender. Im (un-)günstigsten Fall führt die Verwendung eines Störsenders zur Unterbrechung der Kommunikation zwischen Lesegerät und Transponder.

2.4 Passives Stören einer Kommunikation

Unter dem passiven Stören einer RFID-Kommunikation versteht man die Beeinflussung des Kommunikationsvorganges durch abschirmende Maßnahmen, die das elektromagnetische Feld des RFID-Systems beeinflussen. Im (un-)günsigsten Fall führt das passive Stören zur Unterbrechung der Kommunikation zwischen Lesegerät und Transponder.

Ein Sonderfall des passiven Störens stellt die Verwendung des sogenannten Blocker-Tags dar. Hierbei wird ein passiver Transponder, das Blocker-Tag, in das Lesefeld eingebracht. Das Blocker-Tag

beeinflusst das Kommunikationsprotokoll derart, dass ein Selektieren von Transpondern im Lesefeld nahezu beliebig lange zeitlich verzögert wird.

3. Kurzbeschreibung der betrachteten Technologie

Die Radio Frequency Identification-Technologie kann als automatisches Identifikations- und Datenerfassungssystem mit kontaktloser Datenübermittlung auf Basis der Radiofrequenztechnologie definiert werden. Anwendung findet diese Technologie z.Zt. hauptsächlich in den Bereichen

- Industrieautomation,
- Zutrittssysteme,
- Tieridentifikation,
- Warenmanagement und
- bei elektronischen Wegfahrsperren.

Für den praktischen Einsatz verwendet man sogenannte RFID-Systeme. Ein RFID-System besteht dabei immer aus einem Transponder, der die zu speichernden und bei Bedarf zu übermittelnden Informationen enthält, einem Schreibgerät zur Programmierung und dem Schreiben von Identifikationsdaten auf den Transponder sowie einem Lesegerät, das die im Transponder enthaltenen Informationen ausliest. RFID-Systeme gibt es in unterschiedlichsten Ausführungen. Allgemein bekannt sind die einfachsten Systeme zur Warensicherung in Kaufhäusern. Hierbei kommen 1-bit-Transponder zum Einsatz, die unter Ausnutzung physikalischer Effekte ausschließlich eine Ja/Nein-Information speichern und nicht explizit beschreibbar bzw. programmierbar sind. Darüber hinausgehend existiert eine Vielzahl weiterer Systeme, die in die Bereiche

- Speicherkapazität,
- „Intelligenz“ bzw. Rechenleistung,
- Reichweite und
- Versorgungsart

klassifiziert werden können.

Im Rahmen dieses Dokuments werden Systeme beliebiger Speicherkapazität und Rechenleistung betrachtet, die in die Reichweitenklassifizierung „Proximity“ und „Vicinity“ eingeordnet werden können und rein passiv, d.h. ohne eigene Stromversorgung arbeiten. Die grundsätzliche Funktionsweise der untersuchten Systeme wird in den folgenden Abschnitten kurz beschrieben.

3.1 Proximity Coupling (ISO 14443 – Systeme)

Aufbau und Funktion von Proximity-Coupling-Systemen werden in der Norm ISO 14443 beschrieben. Vorgesehen sind Proxymity-Coupling-Systeme für einen Betriebsabstand von bis zu 0,15 m. Der Aufbau des Transponders wird mit Verweis auf die Norm ISO 7810 geregelt, die Abmessungen von 85,72 mm x 54,03 mm vorsieht. Weitergehende mechanische Anforderungen (Biege- und Torsionsbelastung) sowie Anforderungen an die Resistenz gegen UV-, Röntgen- und elektromagnetische Strahlung sind in ISO 14443-1 beschrieben.

Die Kopplung erfolgt induktiv, wie in Abschnitt 3.3 beschrieben. Das Lesegerät verwendet ein elektromagnetisches Wechselfeld der Frequenz 13,56 MHz, die Karte enthält eine Antennenspule mit ca. 3 bis 6 Windungen. Durch die Norm festgelegte Feldstärken für das zu erzeugende Magnetfeld liegen in einem Bereich von 1,5 A/m und 7,5 A/m. Es gibt Proxymity-Transponder des Typs A und des Typs B, da die ISO kein einheitliches Kommunikationsinterface spezifizieren konnte. Für den Einsatz ergeben sich dadurch zunächst keine gravierenden Unterscheidungen.

Beide Kartentypen sind in der Lage, in beide Übertragungsrichtungen eine Übertragungsrate von mindestens 106 kbit/s zu erreichen. Die Unterscheidungen liegen in der verwendeten Modulationsart und der Bitkodierung des zu übertragenden Datenstroms.

3.2 Vicinity Coupling (ISO 15693 – Systeme)

Aufbau und Funktion von Vicinity-Coupling-Systemen werden in der Norm ISO 15693 beschrieben.

Vorgesehen sind Vicinity-Coupling-Systeme für einen Betriebsabstand von bis zu 1,00 m. Der Aufbau des Transponders wird mit Verweis auf die Norm ISO 7810 geregelt, die Abmessungen von 85,72 mm x 54,03 mm vorsieht. Weitergehende mechanische Anforderungen (Biege- und Torsionsbelastung) sowie Anforderungen an die Resistenz gegen UV-, Röntgen- und elektromagnetische Strahlung sind in ISO 15693-1 beschrieben.

Die Kopplung erfolgt induktiv, wie in Abschnitt 3.3 beschrieben. Das Lesegerät verwendet ein elektromagnetisches Wechselfeld der Frequenz 13,56 MHz, die Karte enthält eine Antennenspule mit ca. 3 bis 6 Windungen. Durch die Norm festgelegte Feldstärken für das zu erzeugende Magnetfeld liegen in einem Bereich von 0,115 A/m und 7,5 A/m.

Für die Kodierung des zu übertragenden Datenstroms stehen zwei Methoden zur Verfügung, woraus sich Übertragungsraten von 6,62 kbit/s (long distance mode) und 26,48 kbit/s (fast mode) ergeben. Die höhere Übertragungsrate kann immer dann gewählt werden, wenn die Reichweite des Systems nicht ausgeschöpft werden soll (bspw. bei abgeschirmten Lesegeräten).

3.3 Energieversorgung

Sowohl Systeme nach ISO 14443 als auch Systeme nach ISO 15693 verwenden zur Energieversorgung des Transponders und zur Datenübertragung die induktive Kopplung. Ein induktiv gekoppelter Transponder besteht dabei aus einem elektronischen Datenträger und einer großflächigen Spule, die als Antenne dient.

Induktiv gekoppelte Transponder werden fast ausschließlich passiv, ohne Verwendung einer Stützbatterie betrieben. Dies bedeutet, dass die gesamte zum Betrieb der Steuerlogik, State-Machine oder Mikroprozessor, notwendige Energie durch das Lesegerät zur Verfügung gestellt werden muss.

Zur Energieversorgung des Transponders wird von der Antennenspule des Lesegerätes ein hochfrequentes, elektromagnetisches Feld erzeugt, welches den Querschnitt der Spulenfläche und den Raum um die Spule durchdringt. Ein Teil des ausgesendeten Feldes durchdringt die Antennenspule des Transponders, welcher sich in einiger Entfernung zur Spule des Lesegerätes befindet. Durch Induktion wird an der Antennenspule des Transponders eine Spannung erzeugt. Diese Spannung wird gleichgerichtet und dient der Energieversorgung des Transponders. Zur Vorbereitung der Datenübertragung wird der Antennenspule des Lesegerätes ein Kondensator parallelgeschaltet, dessen Kapazität so gewählt wird, dass zusammen mit der Spuleninduktivität der Antennenspule ein Parallelschwingkreis gebildet wird, dessen Resonanzfrequenz der Sendefrequenz des Lesegerätes entspricht. Die Antennenspule des Transponders bildet zusammen mit einem Kondensator ebenfalls einen Schwingkreis, welcher auf die Sendefrequenz des Lesegerätes abgestimmt ist. Die Anordnung der beiden Spulen kann auch als Transformator interpretiert werden, wobei zwischen den beiden Windungen jedoch nur eine sehr schwache Kopplung besteht.

Für die eigentliche Informationsübertragung wird bei der induktiven Kopplung meist das Verfahren der Lastmodulation bzw. das Verfahren der Lastmodulation mit Hilfsträger verwendet. Hier wird nur kurz das Verfahren der Lastmodulation beschrieben, da lediglich ein prinzipielles Verständnis für die Art und Weise der Datenübertragungstechnik notwendig ist, um die Funktionsweise von induktiv gekoppelten RFIDs nachvollziehen zu können.

Wird ein resonanter Transponder in das magnetische Wechselfeld der Antenne des Lesegerätes gebracht, entzieht dieser dem magnetischen Feld Energie. Die dadurch hervorgerufene Rückwirkung des Transponders auf die Antenne des Lesegerätes kann als transformierte Impedanz in der Antennenspule des Lesegerätes dargestellt werden. Das Ein- und Ausschalten eines Lastwiderstandes an der Antenne des Transponders bewirkt eine Veränderung der transformierten Impedanz und damit Spannungsänderungen an der Antenne des Lesegerätes. Dies entspricht in der Wirkung einer Amplitudenmodulation durch den entfernten Transponder. Steuert man das An- und Ausschalten des

Lastwiderstandes durch Daten, können diese Daten vom Transponder zum Lesegerät übertragen werden. Eine solche Form der Datenübertragung bezeichnet man als Lastmodulation.

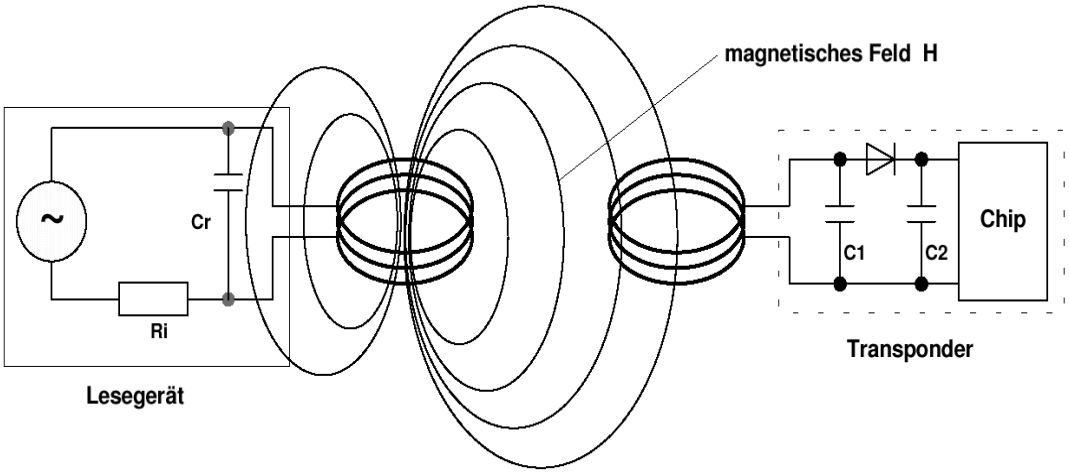

Abbildung 1: Die induktive Kopplung eines RFID-Systems nach [FINK2002]

Die Rückgewinnung der Daten im Lesegerät geschieht durch eine Gleichrichtung der an der Antenne des Lesegerätes abgegriffenen Spannung. Der Vorgang kann als Demodulation eines amplitudenmodulierten Signals verstanden werden.

4. Theoretische Überlegungen zur Bestimmung der maximalen Reichweite für passives Mitlesen

Theoretische Betrachtungen in [NXP2007] führten zu den im Folgenden dargestellten Ergebnissen. Benannt werden hier lediglich Endergebnisse und keine ausführlichen Herleitungen.

4.1 Feldstärke und Signalleistung

Die maximale zu erreichende Reichweite für das passive Mitlesen einer RFID-Kommunikation hängt hauptsächlich von der Signalstärke, mit der Lesegerät und Transponder miteinander kommunizieren sowie vom jeweiligen Umgebungsrauschen ab.

Setzt man voraus, dass die zu bestimmende magnetische Feldstärke $\vec{H}(x)$ aus der Betrachtung einer Ringspule resultiert, lässt sich der Betrag der Feldstärke entlang der Achse einer Kreisspule nach dem Biot-Savart-Gesetz im Nahfeld darstellen als:

$$H(x) = \frac{I\,r^2}{2\left(r^2 + x^2\right)^{3/2}}$$

Dabei entspricht *r* dem Radius der verwendeten Kreisspule, *I* dem durch die Spule fließenden Strom und *x* dem Abstand vom Mittelpunkt der Kreisspule entlang der Rotationsachse.

Setz man voraus, dass der Betrag der Signalleistung

$$\vec{S} = \vec{H} \times \vec{E}$$

sich aufgrund der für das Fernfeld geltenden 90^0-Beziehung zwischen $\vec{H}$ und $\vec{E}$ in einer Freiraum-Umgebung als Produkt der Beträge der Einzelkomponenten zu

$$S_{signal} = H \cdot E$$

ergibt, kann man mit Hilfe der Beziehung $E = H/Z_0$ (Freiraumwellenwiderstand Z_0=377Ω) berechnen:

$$S_{signal} = H \cdot E$$
$$= H \cdot \frac{H}{Z_0}$$
$$= \frac{1}{Z_0} \cdot H^2$$

4.2 Rauschleistung

Die zu berücksichtigende Rauschleistung ergibt sich als Summe des Umgebungsrauschens und des Eigenrauschens des Messempfängers. Für die idealisierte Betrachtung wird das Eigenrauschen des Empfängers als nicht vorhanden angenommen, so dass analog zur vorhergehenden Betrachtung gilt:

$$S_{noise} = E_{noise} \cdot H_{noise}$$

Typische Werte für das Umgebungsrauschen sind grundsätzlich in [ERC1999] kategorisiert und aufgeführt. Es ergibt sich die Tabelle:

ERC-Kategorie	Elektrische Feldstärke (Rauschen) E_{noise} [dBµV/m]	Magnetische Feldstärke (Rauschen) H_{noise} [dBµA/m]	Rauschleistung S_{noise} [dBm]
Business	24.6	-26.9	-91.2
Residental	20.3	-31.2	-95.5
Quiet Rural	0.4	-51.4	-110.6

Tabelle 1: Kategorisierung der Rauschleistung nach [NXP2007] und [ERC1999] für eine Datenrate von 106 kBit/s

4.3 Reichweite für das passive Mitlesen im Nahfeld

Die Reichweite für das passive Mitlesen im Nahfeld kann durch das Signal-Rauschverhältnis abgeschätzt werden, wobei die verwendeten Rauschpegel [ERC1999] entnommen wurden. Die Signalfeldstärke kann im Nahfeld, wie schon in Kapitel 4.1 dargestellt, über das Biot-Savart-Gesetz ermittelt werden und ergibt sich als

$$H_{signal}(x) = \frac{I_{2s} \cdot N_2 \cdot r_2^2}{2(r_2^2 + x^2)^{3/2}}$$

mit N_2 als Anzahl der Antennenwindungen und r_2 als Antennenradius.

Abschließend ergibt sich das Signal/Rausch-Verhältnis für die Klassen “Business”, “Residental” und “Quiet Rural” nach [ERC1999] als:

$$S/N = \left(\frac{H_{signal}(x)}{H_{noise}} \right)^2$$

$$= \left(\frac{1}{H_{noise}} \cdot \frac{I_{2s} \cdot N_2 \cdot r_2^{\,2}}{2 \cdot (r_2^{\,2} + x^2)^{3/2}} \right)^2$$

Das untenstehende Diagramm zeigt die Verläufe des Signal/Rausch-Verhältnisses unter Berücksichtigung unterschiedlicher Parameter für das Umgebungsrauschen.

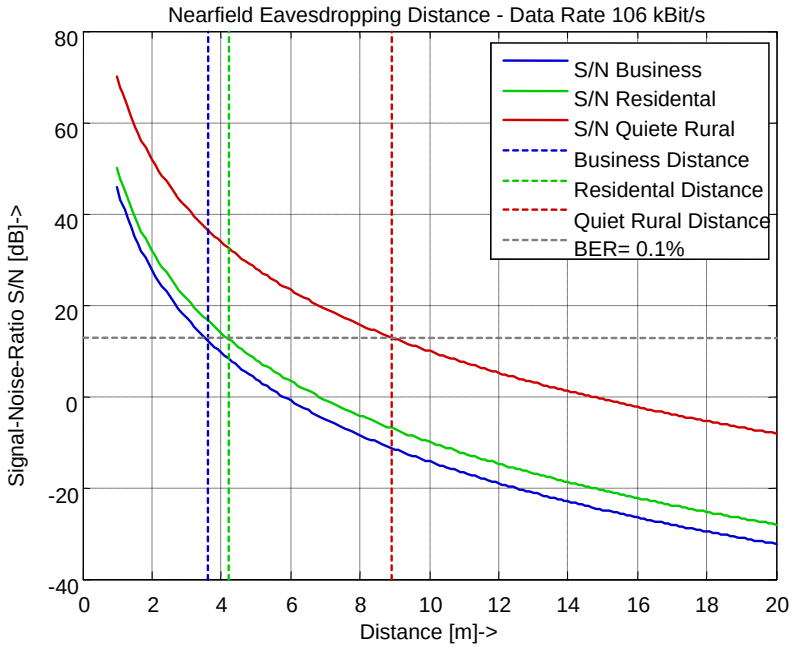

Diagramm 1: Signal/Rausch-Verhältnis für unterschiedliches Umgebungsrauschen aus [NXP2007]

Ebenfalls Einfluss auf die maximal mögliche Mithörentfernung hat die verwendete Übertragungsrate sowie die maximal tolerierbare Bitfehlerrate. Nähere Betrachtungen hierzu finden sich in [NXP2007].

4.4 Fazit der theoretischen Betrachtung

Die durchgeführten Betrachtungen zeigen für übliche Einsatz-Umgebungen von RFID-Systemen (Rausch-Klassen „Business“ und „Residental“) einen theoretischen Maximalabstand von ca. 4 m für das passive Mitlesen der Kommunikation zwischen Transponder und Lesegerät. Erwähnt werden soll, dass die Mitleseentfernung reduzierende Annahmen, wie das Eigenrauschen des Messempfängers, hier explizit nicht getroffen wurden um die Möglichkeiten des theoretisch Machbaren auszuloten.

5. Versuchsdurchführung

Innerhalb der durchzuführenden Untersuchungen sollten für typische ISO 14443- und ISO 15693-Systeme (siehe Anhang 1) die maximalen Abstände für das passive Mitlesen der Kommunikation zwischen Reader und Transponder mit geeigneten Messmethoden ermittelt werden.

Exemplarisch war für das ISO 14443-System eine Interpretation der mitgelesenen Inhalte vorzunehmen. Dabei waren die interpretierten Inhalte in geeigneter Weise auf einem PC-System darzustellen.

Der Aufbau der Kommunikation zwischen Reader und Karte beginnt bei beiden betrachteten Systemen mit dem Informationsaustausch der Kartennummer. Im Anschluss daran kann beim betrachteten ISO 14443-System ein individueller Schlüssel vereinbart und auf verschlüsselten Betrieb umgeschaltet werden.

Bei den Messungen wurde immer die zu Beginn der Kommunikation im Klartext übermittelte bekannte Kartennummer genutzt, um festzustellen, ob das Mitlesen erfolgreich war. Die sich anschließende Kommunikation zwischen Reader und Transponder wurde nicht untersucht.

Das System nach ISO 14443 und auch das System nach ISO 15693 arbeiten auf der selben Frequenz von 13,56 MHz, verwenden dabei aber unterschiedliche Übertragungsverfahren. Für die Versuchsdurchführung wurde ein modulares Empfänger-System gebaut, das aus einem für beide Systeme verwendbaren Empfangsteil und zwei unterschiedlichen systemspezifischen Auswertern besteht. Diese können je nach Bedarf an das Empfangsteil angesteckt werden.

Um die Mithörreichweite zu erhöhen, wurde weiterhin ein Spezialvorverstärker entwickelt. Da sich jedoch zeigte, dass der Einsatz eines reinen Vorverstärkers keine Vorteile mit sich brachte, wurde er für die endgültigen Messungen nicht verwendet.

Eine ausführliche Beschreibung der entwickelten und verwendeten Hardware mit Schaltbildern, Schaltungsbeschreibungen etc. findet sich in Anhang 2.

5.1 Das ISO 14443-System

5.1.1 Messaufbau für das ISO 14443-System

Um auf die für die Messungen erforderliche Bandbreite zu kommen, mussten die verwendeten Antennen fehlangepasst betrieben werden. Je nach Grad der Fehlanpassung kann es dabei zu Mantelwellen auf dem Antennenkabel kommen. Um diese zu vermeiden, wurden insgesamt 11 Ferritringe über das Antennenkabel verteilt. Zusätzlich wurden an vier Stellen des Kabels etwas größere Ringkerne verwendet, durch die das Kabel mehrfach gesteckt wurde.

Für die Messungen wurde der Empfänger mit angestecktem Auswerter und die 15V-Stromversorgung auf einem Laborwagen platziert, auf dem auch der erforderliche PC aufgebaut war.

Damit die Empfangsantenne nicht das Störspektrum des Rechners empfängt, wurde die zu vermessende Funkstrecke in ca. 4 m Abstand vom Laborwagen quer dazu aufgebaut. Der Reader wurde auf einem Stativ befestigt und so eingerichtet, dass er genau zur Mithörantenne strahlt und sich dabei genau auf der Mittelsenkrechten der Mithörantenne befindet (siehe Abbildung 2 und Abbildung 3).

Die mitzuschreibende Karte wurde direkt auf dem Reader befestigt. In dieser Anordnung empfängt die Mithörantenne die maximale Energie der Karte und es ergibt sich somit die maximal mögliche Mithörentfernung. Sobald eine der Antennen oder die Karte in einem anderen Winkel montiert wird, sinkt die Mithörentfernung stark ab.

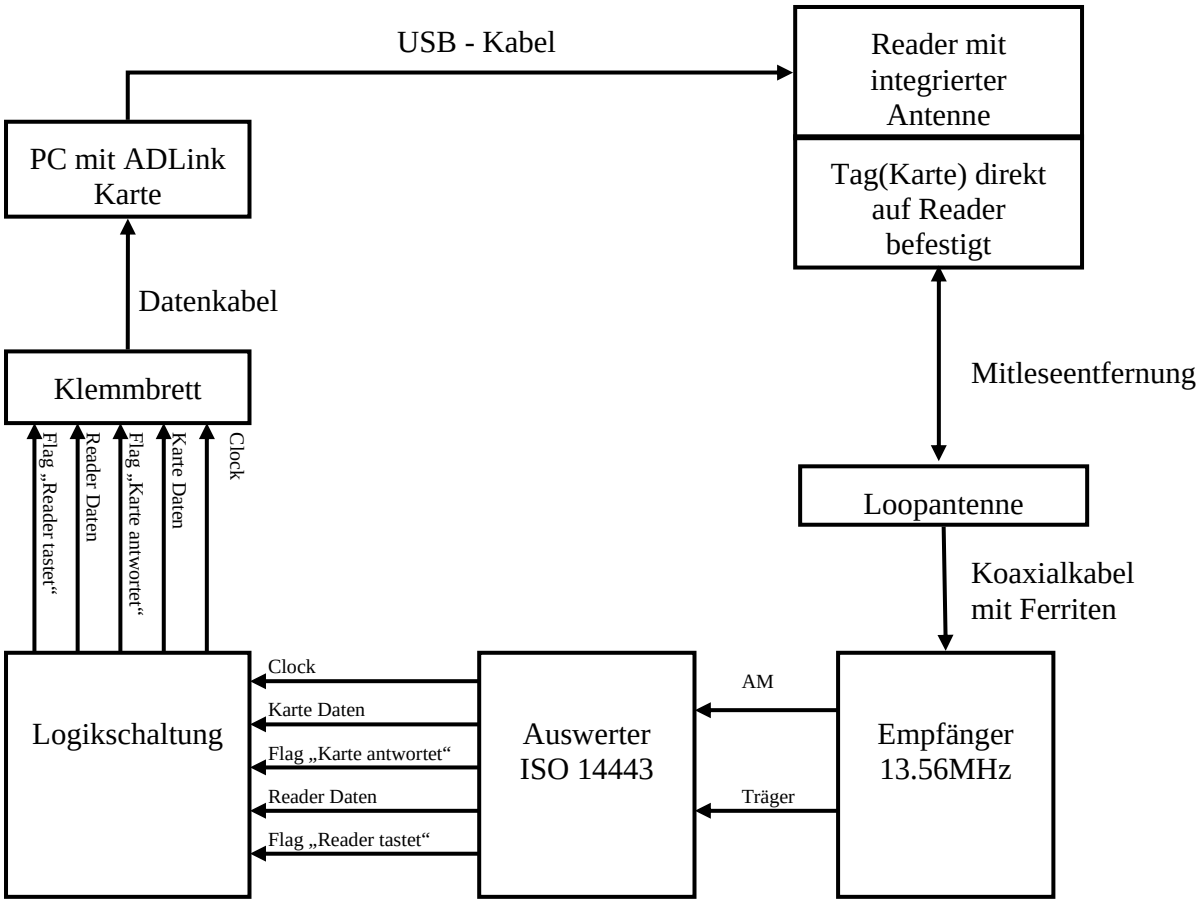

Abbildung 2: Schema-Darstellung des Messaufbaus für das ISO 14443-System

Abbildung 3: Fotos des Messaufbaus für das ISO 14443-System incl. Antennenkabel

5.1.2 Versuchsdurchführung und Messergebnisse

In dem oben beschriebenen Messaufbau wurde die zu Beginn der Kommunikation im Klartext übermittelte Kartennummer mitgelesen. Anschließend wurde die Anzahl der korrekten Lesevorgänge ermittelt. Die nachfolgende Kommunikation wurde bei der Fehleranalyse nicht berücksichtigt.

Beim ISO 14443-System erbrachte die 25cm-Antenne das beste Mithör-Ergebnis. Eine weitere Verbesserung ergab sich, sobald die Resonanz (= Mittenfrequenz) der Antenne auf eine um die halbe Seitenbandfrequenz höhere oder tiefere Frequenz abgeglichen wurde, wobei der Wert des Dämpfungswiderstands konstant blieb. Für die Messungen wurde die Antenne auf die höhere Lage von ca.13,984 MHz abgeglichen.

Die ermittelten Ergebnisse sind in Tabelle 2 und Abbildung 4 dargestellt.

Abstand	richtig erkannt
150cm	100,00%
160cm	100,00%
170cm	100,00%
180cm	100,00%
190cm	100,00%
200cm	100,00%
210cm	100,00%
220cm	100,00%
230cm	100,00%
240cm	80,00%
250cm	40,00%
263cm	10,00%

Tabelle 2: Messergebnisse ISO 14443-Mithören

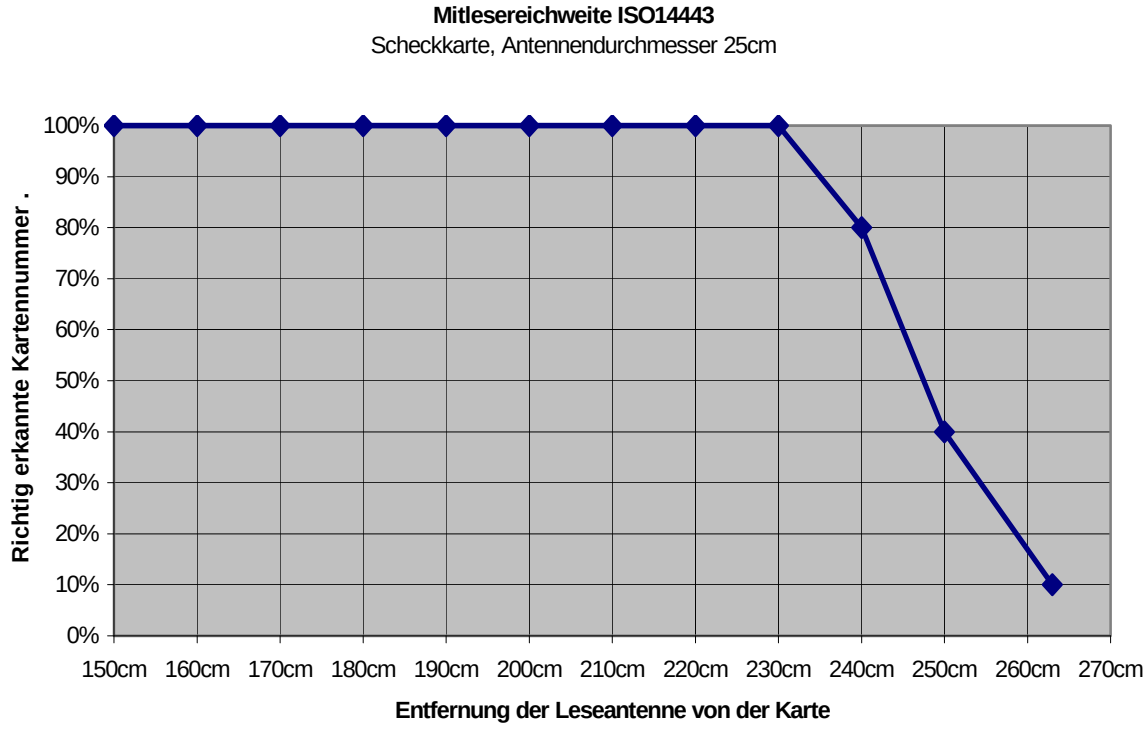

Abbildung 4: Mitlesereichweite ISO 14443

Bis zu einer Entfernung von 2,30 m war es möglich, die Kartennummer richtig mitzulesen. Bei größerer Entfernung stieg die Zahl der falsch erkannten Werte rasch an und bei einer Entfernung von ca. 2,45 m war nur noch die Hälfte der mitgelesenen Kartennummern richtig. Diese Entfernung kann als Mitlesegrenze interpretiert werden. Es wurden jeweils 100 Kartennummern zur Auswertung herangezogen.

5.2 Das ISO 15693-System

5.2.1 Messaufbau für das ISO15693-System

Der Messaufbau für das ISO 15693-System ist ähnlich gestaltet wie der des ISO 14443-Systems. Bei diesem System hatten Voruntersuchungen gezeigt, dass Antennen mittlerer Größe (ca. 40 cm Durchmesser) die besten Mithörergebnisse brachten. Deshalb wurde für die Messungen eine Ringantenne mit einem Durchmesser von 40 cm ausgewählt und auf die Mittenfrequenz von ca. 13,772 MHz abgeglichen.

Auch hier wurden die oben beschriebenen Maßnahmen gegen Mantelwellen getroffen.

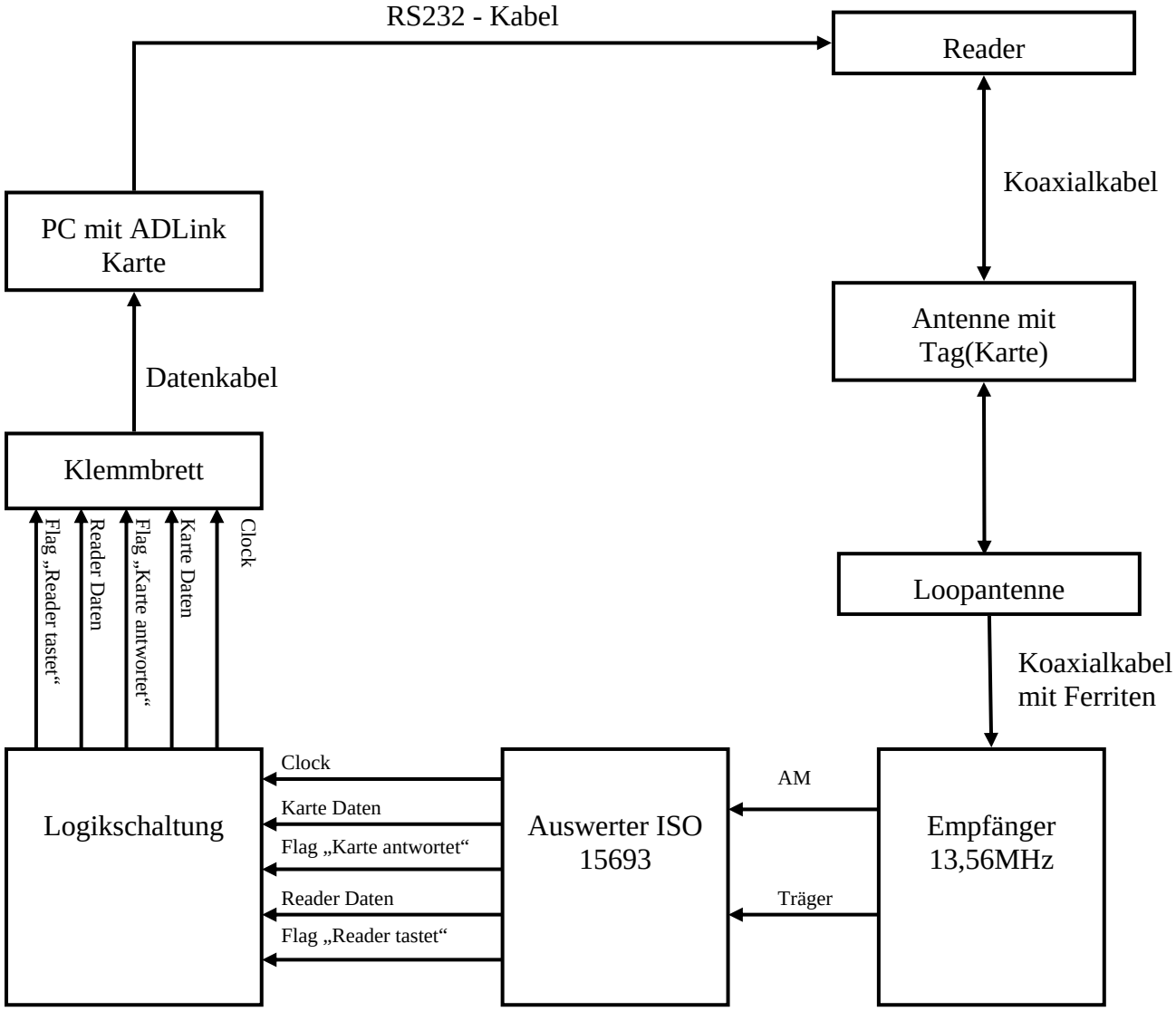

Abbildung 5: Schema-Darstellung des Messaufbaus für das ISO 15693-System

5.2.2 Versuchsdurchführung und Messergebnisse

In dem oben beschriebenen Messaufbau wurde, wie bereits für das ISO 14443-System beschrieben, die zu Beginn der Kommunikation im Klartext übermittelte Kartennummer mitgelesen. Anschließend wurde die Anzahl der korrekten Lesevorgänge ermittelt. Die nachfolgende Kommunikation wurde bei der Fehleranalyse nicht berücksichtigt.

Die ermittelten Ergebnisse sind in Tabelle 3 und Abbildung 7 dargestellt.

Abstand	richtig erkannt
190cm	100,00%
200cm	100,00%
210cm	100,00%
220cm	100,00%
230cm	100,00%
240cm	100,00%
250cm	98,00%
260cm	80,00%
270cm	20,00%
280cm	14,00%
290cm	12,00%
295cm	10,00%

Tabelle 3: Messergebnisse ISO 15693-Mithören

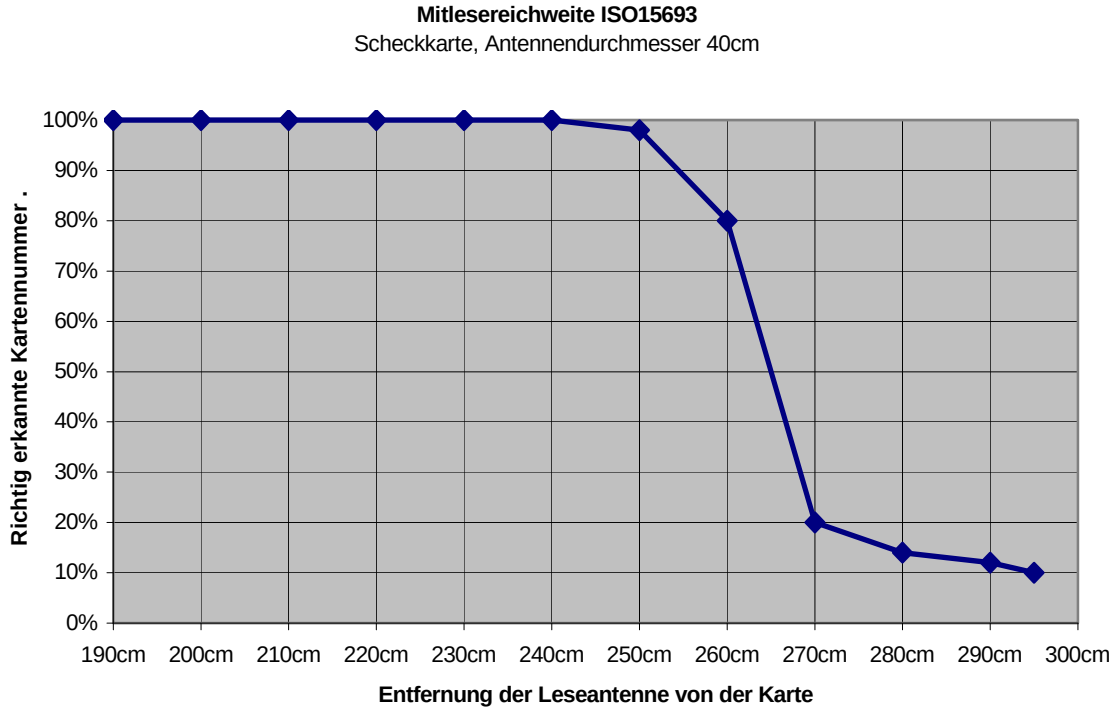

Abbildung 6: Mitlesereichweite ISO 15693

Die Kartennummer konnte bis zu einer Entfernung von 2,40 m richtig mitgelesen werden. Die maximale Mitlesereichweite liegt bei etwa 2,65 m (50 %). Es wurden jeweils 100 Kartennummern zur Auswertung herangezogen.

6. Fazit

Grundsätzlich ist es möglich, die Kommunikation eines ISO 14443- oder ISO 15693-Systems passiv mitzuhören. Dies darf nicht mit der Möglichkeit zum aktiven Auslesen eines Transponders aus der Ferne verwechselt werden.

Überraschend war, dass es trotz speziell abgestimmter Empfänger sowie angepasster Antennen nicht möglich war, die mit einfacheren Mitteln bereits gemessenen Mithörentfernungen signifikant zu erhöhen [FIKE04].

Weiterhin muss darauf hingewiesen werden, dass die Entfernungen von ca. 2,45 m für das ISO 14443-System bzw. 2,65 m für das ISO 15693-System in einer Laborumgebung gemessen wurden. Dementsprechend ist für das Übertragen der Messergebnisse auf eine echte Einsatz-Situation eines RFID-Systems zu berücksichtigen, dass in der Betriebsumgebung des RFID-Systems befindliche Erzeuger elektromagnetischer Wellen die messbaren Mithörentfernung massiv negativ beeinflussen können.

Ebenso ist zu berücksichtigen, dass bei beiden Messungen eine optimale Ausrichtung von RFID-System zu Mithör-Empfänger vorlag. Ein geringfügiges Abweichen von dieser optimalen, orthogonalen Ausrichtung hatte eine sofortige Verschlechterung des Pegelwertes der mitgehörten Kommunikation zur Folge.

Grundsätzlich kann somit festgestellt werden, dass die Gefährdung des Mithörens einer RFID-Kommunikation im betrachteten Frequenzbereich theoretisch, wie in Kapitel 4 aufgeführt, zwar eine gewisse Relevanz hat, jedoch in der Praxis eher von untergeordneter Bedeutung ist.

Die Ergebnisse für das passive Mitlesen wurden in einer seperaten Untersuchung für den ePass überprüft. Demnach sind anhand dieser Messergebnisse die Grenzen der reellen, d.h. auswertbaren Mitlesbarkeit für den ePass im Bereich von unter vier Metern als Maximalentfernung anzusetzen. Dieses jedoch auch nur mit äußerst großem Aufwand. Die Messergebnisse zeigten, dass spätestens bei einer Entfernung von vier Metern so deutliche Veränderungen des Empfangssignals vorhanden sind, dass die Daten nicht mehr fehlerfrei wiederherstellbar sind. Selbst mit sehr aufwändiger Empfangstechnik ist eine fehlerfreie Decodierung dieser Daten nicht mehr zu erwarten.

Literaturverzeichnis

[DTE] Vertriebspartner für RFID-Systeme, weiterführende Informationen unter http://www.dte.de

[ERC1999] European Radiocommunications Committee (ERC) within the European Conference of Postal and Telecommunications Administrations (CEPT), Propagation Model and Interference Range Calculation for Inductive Systems 10kHz - 30MHz, Marbella, February 1999, verfügbar unter http://www.ero.dk/doc98/Official/Pdf/REP069.PDF

[FEIG] Hersteller von RFID Systemen, weiterführende Informationen unter http://www.feig.de

[FINK2002] Finkenzeller, K., RFID-Handbuch – Grundlagen und praktische Anwendungen induktiver Funkanlagen, Transponder und kontaktloser Chipkarten, 3., aktualisierte und erweiterte Auflage, Carl Hanser Verlag, München 2002

[FIKE04] Finke, T., Kelter, H., Radio Frequency Identification – Abhörmöglichkeiten der Kommunikation zwischen Lesegerät und Transponder am Beispiel eines ISO14443-Systems, Online verfügbar unter http://www.bsi.de/fachthem/rfid/Abh_RFID.pdf.

[MeGu] Meinke, Hans H., Gundlach Friedrich-Wilhelm, Taschenbuch der Hochfrequenztechnik, 4., Auflage, Springer Verlag 1986

[MIFARE] Philips – mifare MF EV 800, weiterführende Informationen unter http://www.mifare.de

[NXP2007] AN200701: ISO/IEC 14443 Eavesdropping and Activation Distance, NXP 2007, beziehbar über NXP Semiconductors

[PEG] MF EV 800 Quick Introduction Sheet, weiterführende Informationen unter http://www.semiconductors.philips.com/acrobat_download/other/identification/PE065910.pdf

Anhang 1: Verwendete RFID-Systeme

Aufgrund ihrer Verbreitung im Markt sowie der Bedeutung für den Einsatz im Bereich von Identifikationssystemen und Logistik, wurden für das Durchführen der Messungen ein ISO 14443-System von Philip bzw. NXP Semiconductors und ein ISO 15693-System der Firma DTE ausgewählt.

ISO 14443-System „Philips – Mifare MF EV 800“

Das System basiert auf dem Pegoda Reader MF RD700. Das Evaluation Kit [PEG] unterstützt die ISO 14443A- und MIFARE®-Classic Systeme. Es arbeitet auf 13,56 MHz mit einer Sendeleistung von ca. 320 mW. Das Reader-Kit besteht aus Reader-Modul mit integrierter Antenne. Die relativ große Antenne sitzt unterhalb der gewölbten Plastikschale.

Detaillierte Informationen, sowie Produktbeschreibungen für das hier verwendete Evaluation Kit „MF EV 800“ sind über den Hersteller oder dessen Vertriebspartner beziehbar [MIFARE].

Abbildung A1: "Philips - Mifare" Reader

Abbildung A2: Tags: Armbanduhr (oben), Karte "Doppelpunkt", Karte 4k, Karte Ultra Light (von rechts nach links)

ISO 15693-Sytem von DTE MR-100

Dieses System unterstützt die ISO 15693. Es arbeitet mit einer Sendeleistung von ca. 2,3 W. An das System können externe Antennen angeschlossen werden. Detaillierte Informationen, sowie Produktbeschreibungen für den hier verwendeten Evaluation Kit „DTE MR-100“ sind über den Hersteller [DTE] oder dessen Vertriebspartner [DTE] beziehbar.

Abbildung A3: Reader von FEIG Elektronic ID ISC.MR100

Abbildung A4: Antenne

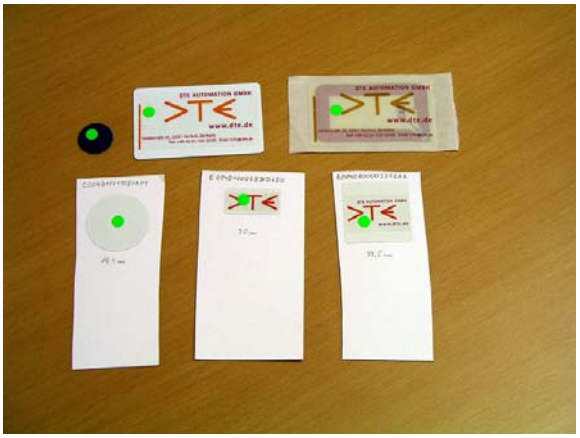

Abbildung A5: Verwendete Tags

Anhang 2: Verwendete Hardware

Für die Messungen des Mithörens war zunächst geplant, diese mit vorhandener technischer Ausrüstung vorzunehmen. Bei ersten Versuchen stellte sich heraus, dass die schwachen und amplitudengetasteten Antwortsignale der Karte mit den vorhandenen Geräten nicht zu empfangen waren. Aus diesem Grund wurde ein speziell auf die zu untersuchenden Systeme zugeschnittenes Empfangsteil entwickelt und gebaut.

Es wurde dabei das folgende Konzept zugrunde gelegt:

Nachdem sowohl das System nach ISO 14443 als auch das System nach ISO 15693 auf der selben Frequenz 13,56 MHz arbeiten und die Übertragung bei beiden Systemen mittels Amplitudentastung erfolgt, wurde ein 13,56 MHz-AM-Empfänger entwickelt, der mit beiden Systemen arbeitet und an den je nach Bedarf ein systemspezifischer Auswerter angesteckt wird.

Um die Mithörreichweite zu erhöhen wurde ein Spezialvorverstärker entwickelt und gebaut, der aufgrund seiner Eigenschaften die Kartenantwort stärker anhebt als das von Lesegerät kommende Trägersignal.

Im späteren Verlauf der Untersuchungen stellte sich jedoch heraus, dass der Einsatz eines Vorverstärkers statt eines Gewinns schlechtere Ergebnisse brachte. Der ohnehin viel zu starke Readerträger wurde trotz Abschwächung verstärkt und die Antwortspektren der Karte verschwanden im Umgebungsrauschen.

Bei den endgültigen Messungen musste aus diesem Grund auf den Einsatz eines Verstärkers verzichtet werden.

In den folgenden Abschnitten finden sich die Beschreibungen der für Messzwecke verwendeten Hardware-Komponenten. Dies sind

- die magnetischen Loop-Antennen,
- der Vorverstärker,
- das allgemeine Empfangsteil und
- die Auswerter für die ISO 14443- und ISO 15693-Kommunikation.

Verwendete magnetische Loop-Antennen

Im Rahmen der durchzuführenden Messungen wurden Schleifenantennen verschiedener Größe angefertigt. Für das Messen der maximalen Mithörreichweite wurde daraus die optimale Antenne gewählt und entsprechend den Anforderungen abgeglichen.

Abbildung A6 zeigt die gewählte Anpassschaltung.

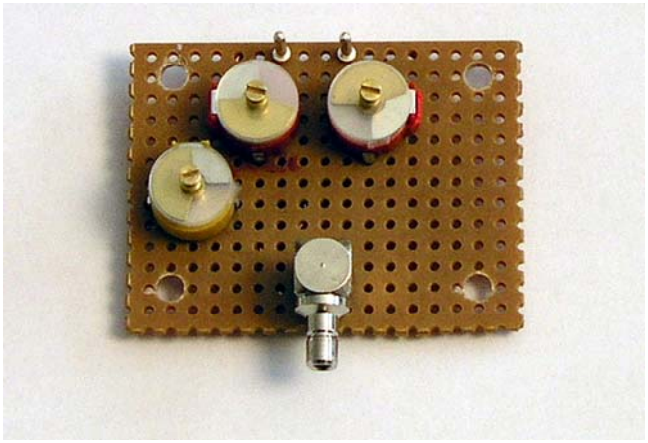

Abbildung A6: Anpassschaltung (hier noch ohne Zusatzkondensatoren)

Die in Abbildung A7 dargestellte Schleife wird mit den beiden Kondensatoren C_1 und C_2 (bestehend aus einem Trimmer und je nach Erfordernis noch einem festen Zusatzkondensator) auf 13,56 MHz in Resonanz gebracht.

Mit dem Trimmer C_k wird die Antennenimpedanz auf die Kabelimpedanz von 50 Ohm transformiert.

Aufgrund der hohen Schwingkreisgüte mussten einige der Antennen noch zusätzlich mit einem Widerstand R_d bedämpft werden. Dies war notwendig, um die Antennen breitbandiger zu machen, da die Übertragung mit hoher Bitrate – und somit hoher Bandbreite – stattfindet.

Die Antennen wurden aus 1,5 mm² Kupferschaltdraht hergestellt, mittels Kabelbindern auf Hartfaserplatten montiert und über die in Abbildung A6 dargestellte Anpassschaltungen angeschlossen, wobei jede Antenne am Netzwerkanalysator auf die für ihre Größe optimale Impedanz abgeglichen wurde.

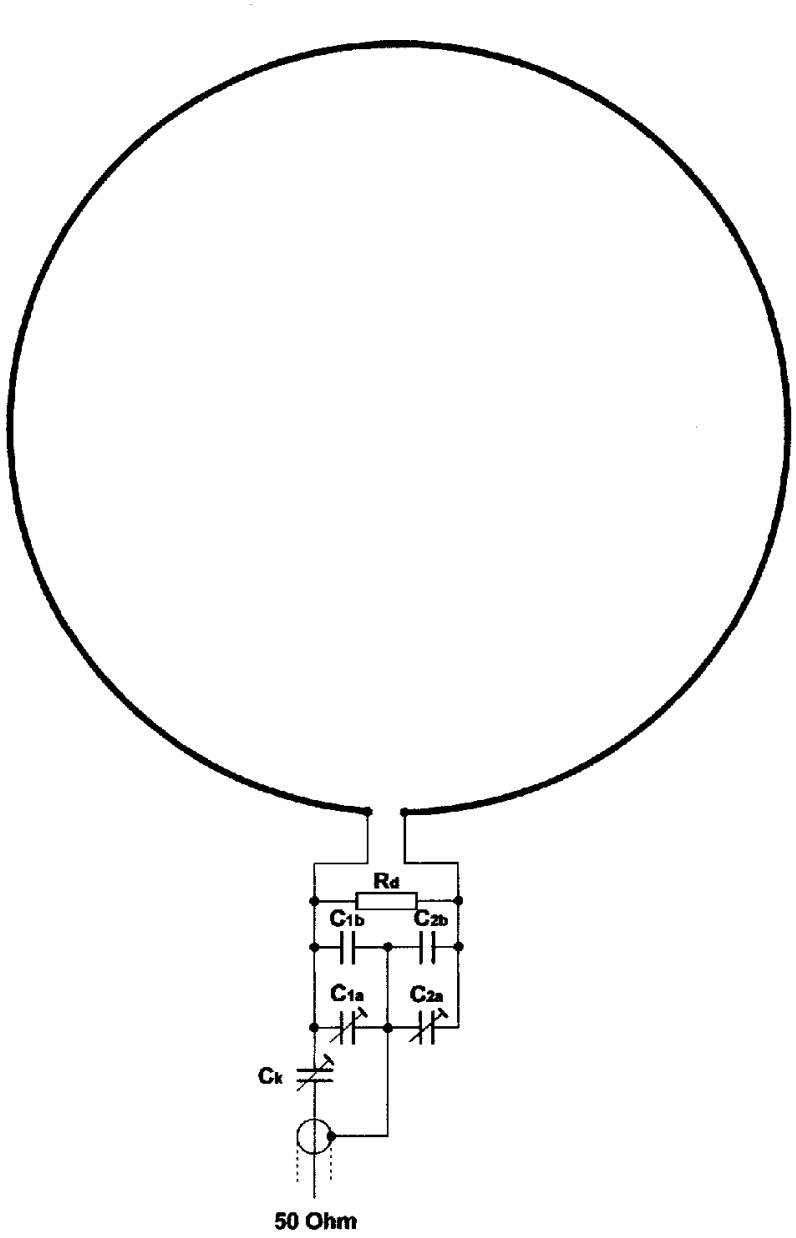

Abbildung A7: Schaltung der verwendeten Loopantennen

Vorverstärker

Die folgende Abbildung zeigt das Schaltbild des verwendeten Vorverstärkers.

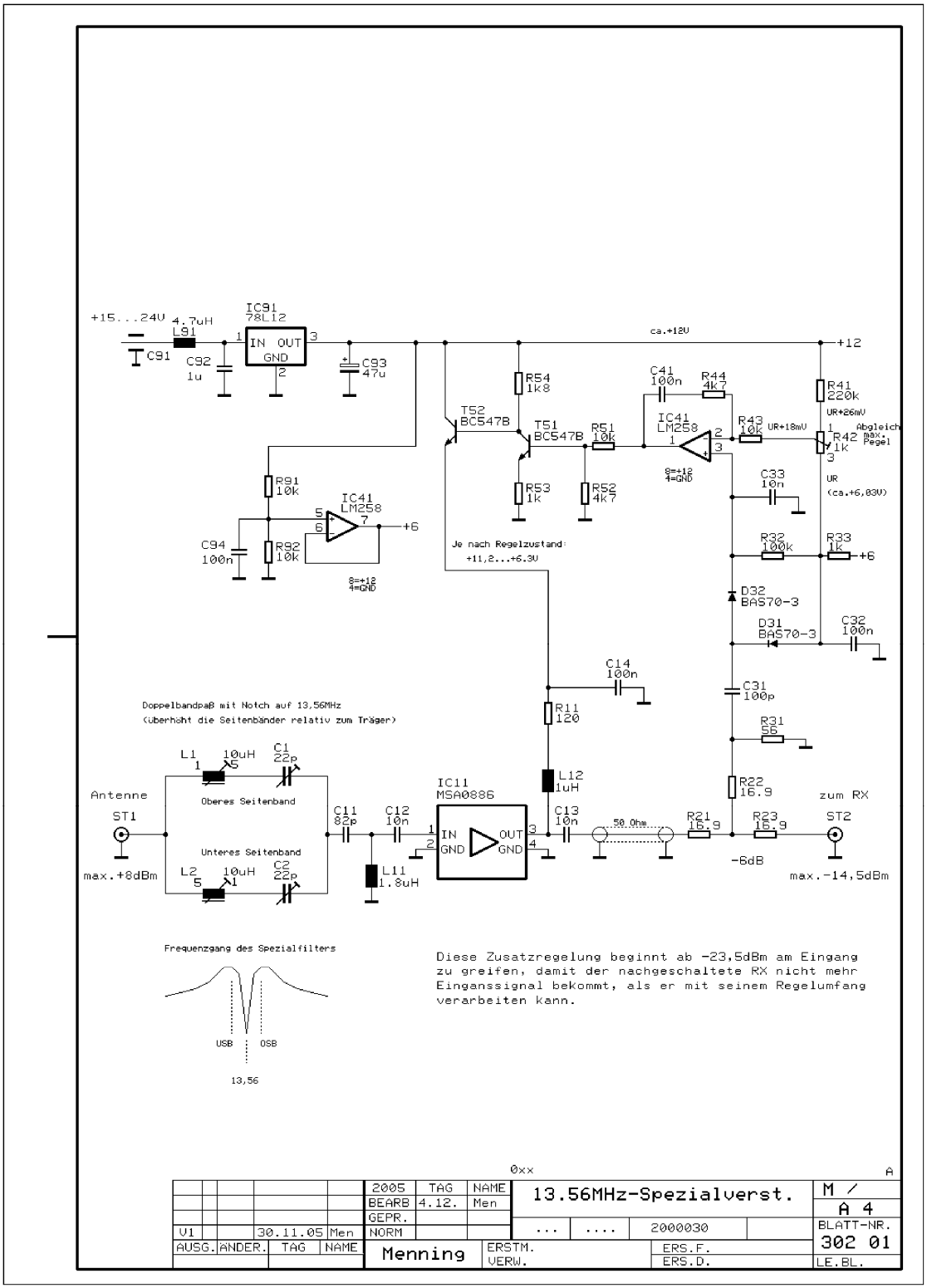

Abbildung A8: Schaltbild des Vorverstärkers

Die zu untersuchenden Systeme arbeiten im Duplex-Verfahren, was bedeutet, dass der Reader weitersendet, während die Karte antwortet. Aus diesem Grund muss die ca. 90 dB schwächere Kartenantwort in Anwesenheit des starken Readersignals detektiert werden. Wenn die Entfernung zum System etwas erhöht wird, nehmen beide Amplituden schnell ab, was dazu führt, dass das schwache Signal der Karte schnell im Rauschen verschwindet. Dementsprechend wird hier ein empfindlicher Empfänger mit hoher Dynamik benötigt, der die Kartenantwort trotz Anwesenheit des starken Reader-Signals noch lesen kann. Um diese Dynamik ausnutzen zu können, muss der Mithörempfänger möglichst weit ausgesteuert werden, damit bei diesem AM-System die Kartenantwort noch zu empfangen ist. Gleichzeitig darf der Empfänger aber nicht vom Reader-Signal übersteuert werden, da in diesem Fall die Kartenantwort ebenfalls nicht mehr zu empfangen wäre.

Aus diesem Grund wurde ein Vorverstärker entwickelt, der diesem Effekt entgegenwirkt, indem er die Spektralanteile der Kartenantwort stärker verstärkt als den ohnehin schon sehr starken Träger des Readers.

Um den bereits weit ausgesteuerten Empfänger nicht zu übersteuern, muß in einem solchen Vorverstärker eine Zusatzregelung eingebaut werden, die den an den Empfänger gelieferten Ausgangspegel begrenzt.

Funkltionsbeschreibung des Vorverstärkers

Das von der Antenne kommende Signal durchläuft ein Spezialfilter aus L1/C1 und L2/C2, welches aufgrund seiner Schaltung und eines entsprechenden Abgleichs die beiden Antwortseitenbänder möglichst unverzerrt durchlässt, während der dazwischen befindliche Reader-Träger abgeschwächt wird. Beim Abgleich muss darauf geachtet werden, dass durch das Filter auf den beiden Seitenbändern möglichst geringe Gruppenlaufzeitverzerrungen entstehen.

Das derart selektierte Signal gelangt auf einen integrierten Verstärker, der die erwünschte Verstärkung vornimmt.

Am Ausgang des Verstärkers wird das Signal in zwei Zweige aufgeteilt. Einer davon gelangt als verstärktes Ausgangssignal an ST2 während der andere Zweig zur Diode D32 führt, die daraus eine der Signalamplitude entsprechende Gleichspannung erzeugt. Diese Spannung wird in IC41 mit dem mittels R42 eingestellten Maximalwert verglichen. Sobald sie zu große Werte annimmt, wird der bis dahin am Anschlag liegende Regelkreis aktiv und regelt über T51 und T52 die Verstärkung von IC11 herunter, damit die Ausgangsamplitude nicht über den vorgegebenen Maximalwert ansteigen kann.

Allgemeiner Hinweis bzgl. der Stromversorgung aller Schaltungsteile

Da in den verschiedenen Teilen der Hardware unterschiedliche Spannungen zwischen +5V und +12V benötigt werden, wurde +15V als gemeinsame Stromversorgung für alle Teile gewählt. Diese Spannung wird innerhalb der einzelnen Geräte auf die jeweils erforderlichen Werte herunterstabilisiert. Der dabei zulässige Eingangsspannungsbereich liegt zwischen +15 und +24V, wobei aus Gründen der Verlustleistung und Erwärmung eine möglichst niedrige Spannung innerhalb dieses Bereiches zu empfehlen ist.

13,56 MHz – Empfänger für beide Systeme

Die beiden folgenden Abbildungen zeigen das Schaltbild der HF-Vorstufe und des Eingangsbandpasses sowie des eigentlichen Empfangsteils des verwendeten Empfängers.

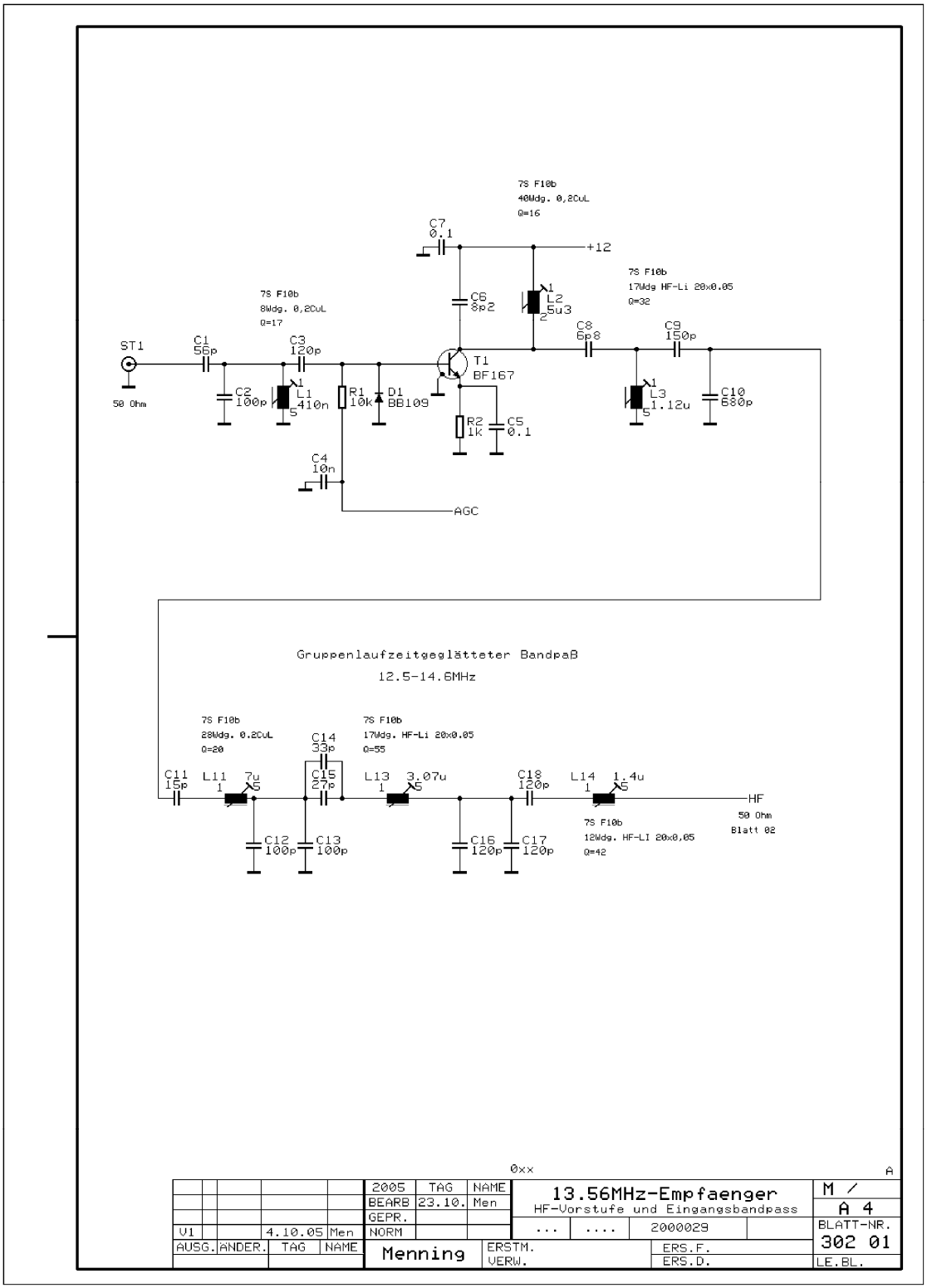

Abbildung A9: Schaltbild der HF-Vorstufe und des Eingangsbandpasses

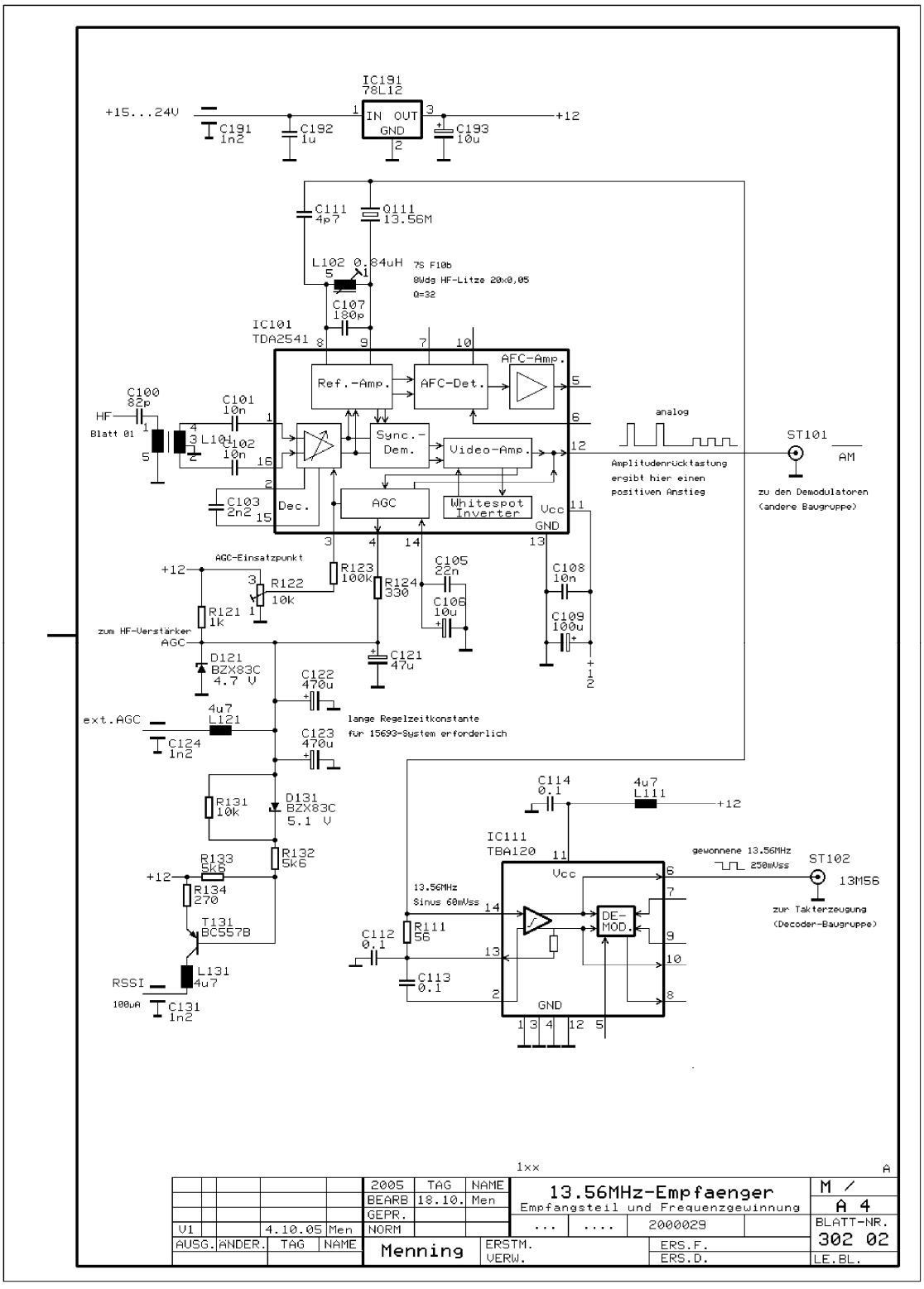

Abbildung A10: Schaltbild des Empfangsteils und der Frequenzgewinnung

Der Empfänger soll das von der Antenne kommende Signal verstärken und die darauf enthaltene Amplitudenmodulation bzw. Tastung über eine Koaxbuchse zur weiteren Verarbeitung ausgeben. Des weiteren soll er die Sendefrequenz des Readers von der Tastung befreien und als konstanten Systemtakt 13,56 MHz zur Verfügung stellen. Aus Gründen der Handhabbarkeit während des Messvorgangs wurde eine relative Feldstärkeanzeige des Eingangspegels realisiert.

Beschreibung

Das von der Antenne (bzw. vom Vorverstärker) kommende Eingangssignal durchläuft die geregelte HF-Vorstufe mit T1, die das Signal verstärkt, deren Hauptaufgabe aber darin besteht, als Regelstellglied zu fungieren. Da sich die Eingangsimpedanz des Transistors mit dem Regelzustand verändert, wurde hier eine zusätzliche Kapazitätsdiode D1 eingebaut, die so betrieben wird, dass sie einen Großteil dieser Impedanzänderungen zu kompensieren in der Lage ist.

Danach gelangt das Signal zu einem Bandpass, der alle nicht zum untersuchenden Spektrum gehörenden Frequenzen abdämpft, ohne das gewünschte Signal zu verzerren.

Das gewonnene Signal wird anschließend über den Symmetrieübertrager L101 in IC101 eingespeist. Dieser IC-Typ ist als TV-ZF-Verstärker konzipiert und somit für die Verarbeitung amplitudenmodulierter und amplitudengetaster Signale prädestiniert.

Im IC wird das Signal verstärkt, der Träger daraus wiedergewonnen und das verstärkte Signal anschließend mit dem wiedergewonnenen Träger gemischt, um die Modulation mit hoher Dynamik wiederzugewinnen (Synchron-Demodulator). Das an der Koaxbuchse anliegende Ausgangssignal beinhaltet die Trägertastung als Gleichspannungssprünge und die Seitenbänder in Basisbandlage. Seine Polarität ist invers, d.h., dass eine Trägerrücktastung einen positiven Spannungssprung am Ausgang erzeugt.

Der IC enthält ferner eine Regelspannungserzeugung, die für getastete und amplitudenmodulierte Signale optimiert ist. Diese Spannung wird für die Regelung von T1 und die Feldstärkeanzeige herangezogen.

Zur einfacheren Handhabung wird das Feldstärkemesssignal von T131 in ein gesteuertes Konstantstromsignal umgewandelt, damit ein 100µA-Instrument direkt angeschlossen werden kann.

Der in IC101 wiedergewonnene Träger wird durch ein schmales Quarzfilter (Q111) von der Trägertastung befreit und das so gewonnene 13,56 MHz-Signal anschließend in einem Begrenzerverstärker (IC111) auf einen konstanten Ausgangspegel gebracht.

Auch dieses Signal liegt an einer Koaxbuchse an, um in den systemspezifischen Auswerteschaltungen weiter verwendet zu werden.

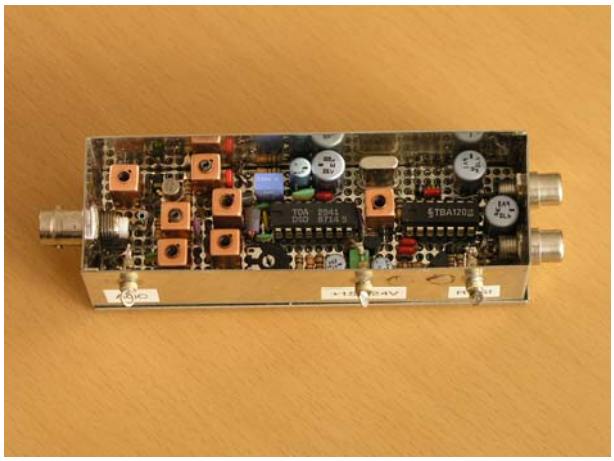

Abbildung A11: Empfänger (geöffnet)

In Abbildung A11 ist der geöffnete Empfänger zu sehen. Auf der linken Seite ist der Antenneneingang (BNC-Buchse) zu sehen, rechts sind die Chinch-Buchsen zu den Auswertemodulen erkennbar.

Die vordere Chinch-Buchse (mit „AM“ bezeichnet) führt die Basisbandinformation und die hintere Buchse („Träger“) den wiedergewonnenen 13,56 MHz-Träger des Readers.

Auswerter für ISO 14443

Die beiden folgenden Abbildungen zeigen das Schaltbild des Decoders für ISO 14443-Signale.

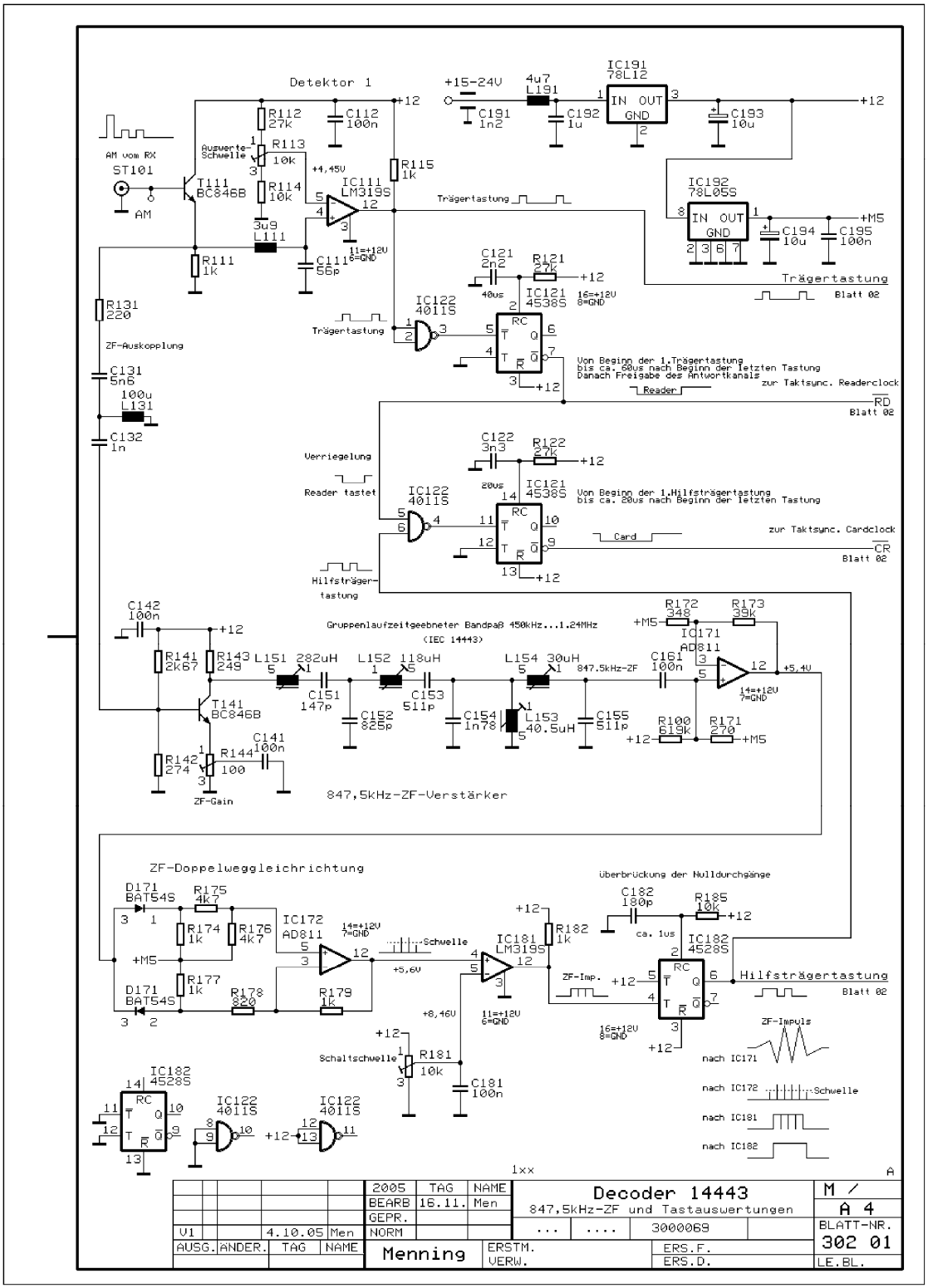

Abbildung A12: Schaltbild Decoder ISO 14443 (847,5kHz-ZF und Tastauswertung)

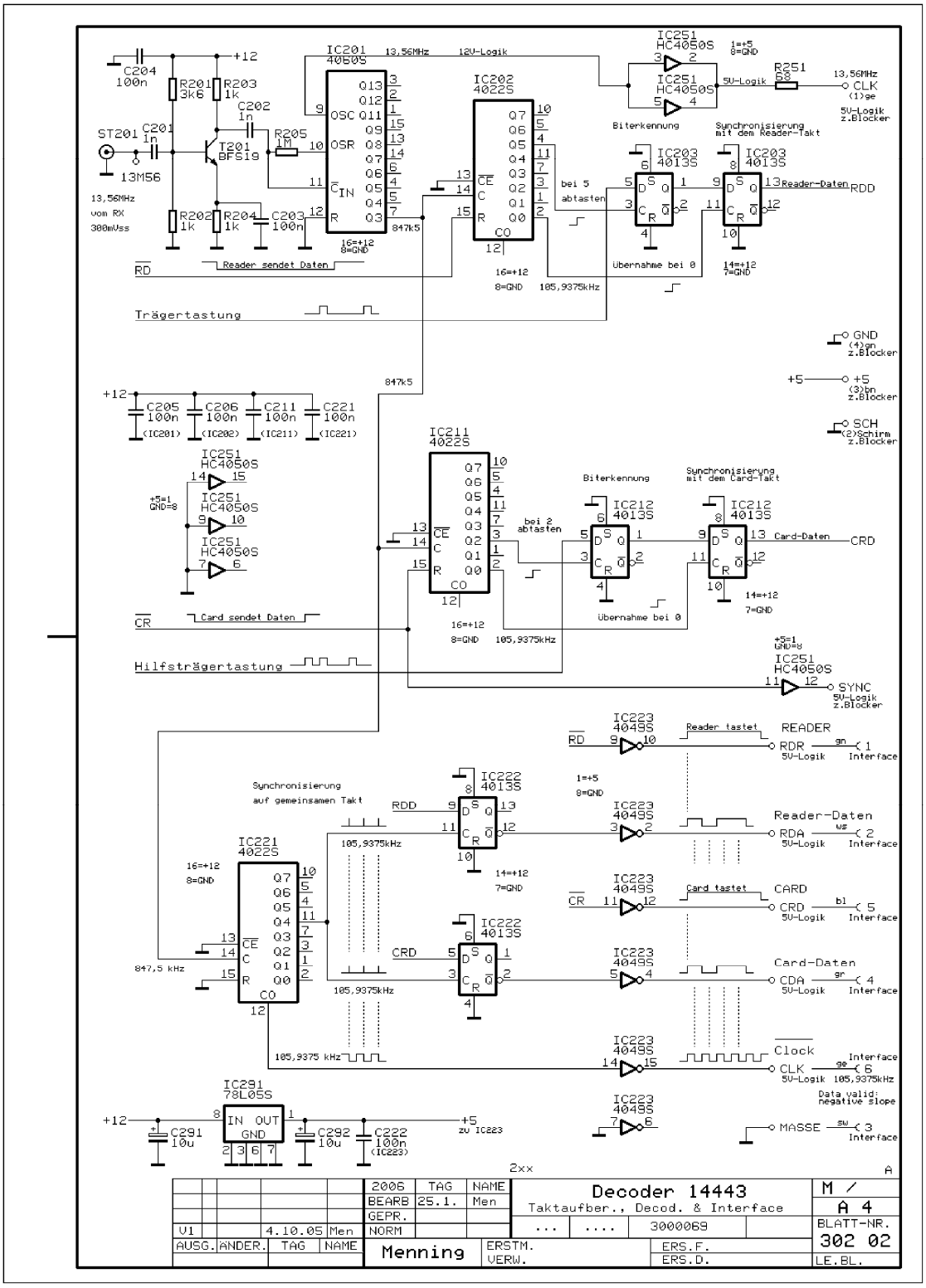

Abbildung A13: Schaltbild Decoder ISO 14443 (Taktaufbereitung, des Decoders und des Interface)

Der Auswerter soll die Daten vom Reader und von der Kartenantwort aus den vom Empfänger zur Verfügung gestellten Signalen demodulieren, aus dem Reader-Träger einen dazu passenden Takt herleiten und Steuersignale erzeugen, die angeben, wann der Reader tastet und wann die Karte antwortet. Die Ergebnisse soll er in geeigneter Form in 5V-Logik an das Interface ausgeben.

Beschreibung

Das vom Empfänger kommende AM-Signal wird zunächst über den Impedanzwandler T111 belastungsfrei abgenommen und dann in die Zweige „Reader“ und „Karte“ aufgespalten.

Das erfolgt mittels Tiefpass L111/C111 für den Reader-Zweig und Hochpass C131/L131/C132 für den Kartenzweig.

Die Amplitude des Readers wird im Komparator IC111 mit der durch R113 festgelegten Schaltschwelle verglichen und durch diesen in Tastimpulse zurückgewandelt. Diese werden auf Blatt 2 (Abbildung) mit dem aufbereiteten Takt in IC207 abgetastet und dann auf den Taktanfang synchronisiert.

Abschließend werden in IC222 die Reader- und Kartendaten auf denselben Ausgangstakt synchronisiert, um in IC223 auf den am Interfaceausgang benötigten 5V-Logikpegel gebracht zu werden.

Aus der Readertastung wird im nachtriggerbaren Monoflop IC121 ein Signal generiert, das zu Beginn der Trägertastung startet und so lange bestehen bleibt, bis der Reader spätestens innerhalb von 60 µs erneut tastet. Dieses Signal dient als Flag „Reader tastet“ und wird ebenfalls über IC223 auf 5V-Logik gebracht, da es ebenfalls am Rechner-Interface benötigt wird.

Das im Basisband als getastete Zwischenfrequenz vorhandene Antwortsignal der Karte wird in T141 verstärkt, dessen Verstärkung mit R144 einstellbar ist. Danach durchläuft es einen gruppenlaufzeitgeebneten Bandpass, der auf das hier ankommende Antwortspektrum ausgelegt ist.

Da die Tastung bei diesem System sehr schnell ist (847,5 kHz) kann ein solches Signal mit keinem normalen AM-Detektor (Diode & Kondensator) mehr verarbeitet werden. Deshalb musste hier nach anderen Wegen gesucht werden, um eine schnelle Auswertung der Tastung zu erzielen.

Aus diesem Grund wird die ZF zunächst in einem schnellen OP-Verstärker verstärkt und dann mit D171 und IC172 ohne Verwendung eines Ladekondensators doppelweggleichgerichtet. Am Ausgang von IC172 stehen somit die Halbwellen der ZF mit stets positiver Amplitude an. Diese werden anschließend im Komparator IC181 mit der in R181 eingestellten Schaltschwelle verglichen.

Danach müssen noch die darin enthaltenen Unterbrechungen aufgrund der Nulldurchgänge entfernt werden, um dieses Signal verwenden zu können. Das erfolgt im anschließenden Monoflop IC182, hinter dem die Kartentastung in weiterverarbeitbarer Form vorliegt.

Die so gewonnene Kartentastung wird in gleicher Weise, wie das bei der Readertastung der Fall ist, in IC212 mit dem aufbereiteten Takt abgetastet, auf den Taktanfang synchronisiert und zum Schluss in IC222 auf den gemeinsamen Ausgangstakt synchronisiert, bevor sie in IC223 auf den am Interface erforderlichen 5V-Logikpegel gebracht und ausgegeben wird.

Auch hier ist wieder ein Signal nötig, das ausdrückt „Karte sendet“. Dieses Signal wird in ähnlicher Weise, wie bei der Trägertastung des Readers, durch ein nachtriggerbares Monoflop (IC121) gewonnen, das ab der ersten Tastung der Karte so lange auf HI bleibt, bis die Karte mindestens ca. 20 µs lang nicht mehr geantwortet hat. Um Fehlauswertungen aufgrund von in den ZF-Kanal fallenden Oberwellen der Readertastung zu vermeiden wird die Ansteuerung dieses Monoflops so lange verhindert, wie das Signal „Reader tastet“ noch vorhanden ist.

Auch das Signal “Karte tastet“ wird über IC223 auf 5V-Logik gebracht und ans Interface ausgegeben.

Der vom Empfänger über ST201 ankommende regenerierte 13,56 MHz-Takt des Readers wird über T201 verstärkt und in IC201 auf 847,5 kHz heruntergeteilt.

Daraus wird in IC202 der Bittakt von 105,9375 kHz erzeugt, wobei dieser IC auf das Signal „Reader tastet“ synchronisiert wird und an seinem Ausgang für die weitere Verarbeitung zwei phasenverschobene Impulse erzeugt.

Dasselbe wird auch in IC211 gemacht, der aber auf das Signal „Karte antwortet“ synchronisiert wird.

So stehen für beide Daten jeweils passende Abtasttakte zur Verfügung.

Da das Interface aber nur mit einem einzigen Takt arbeiten kann, müssen die so gewonnenen Daten zum Schluss noch auf einen gemeinsamen Ausgangstakt synchronisiert werden.

Dieser Takt wird von IC201 bereitgestellt, in IC221 auf den Bittakt 105,9375 kHz heruntergeteilt und über IC223 als 5V-Logik zum Interface geführt. Gleichzeitig liefert IC221 noch einen dazu phasenverschobenen Taktimpuls für die rechtzeitige Abtastung der Reader- und Kartendaten, damit am Interface bei der fallenden Taktflanke gültige Daten zur Verfügung stehen.

Das in einem weiteren Projektdokument beschriebene Blockergerät benötigt für seine Funktion den wiedergewonnenen 13,56 MHz-Takt des Readers und das Signal „Karte antwortet“.

Der Readertakt wird hinter dem Eingangsverstärker von IC201 abgegriffen, in zwei parallelgeschalteten Gattern von IC251 auf 5V-Pegel gebracht und zum Blocker ausgegeben. Die Parallelschaltung der Gatter wird benötigt, um den Innenwiderstand der Quelle niedrig zu halten, damit die 13,56 MHz über die Koax-Steckverbindung geführt werden kann.

Das Signal „Karte antwortet“ wird ebenfalls in IC251 auf 5V-Logik gebracht und zum Blocker ausgegeben.

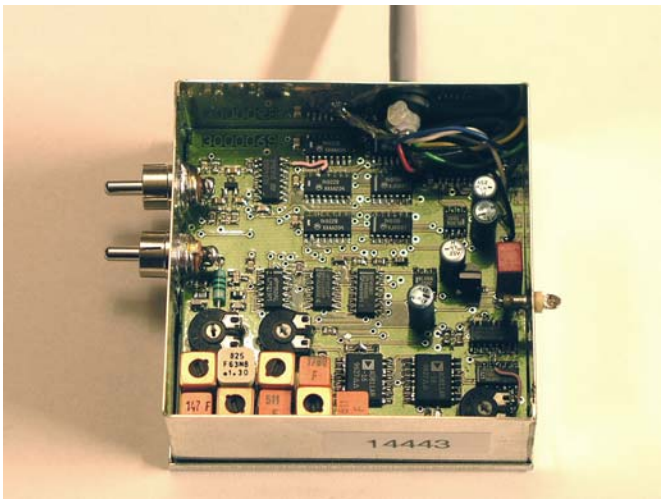

Abbildung A14: Auswerter ISO 14443 (geöffnet)

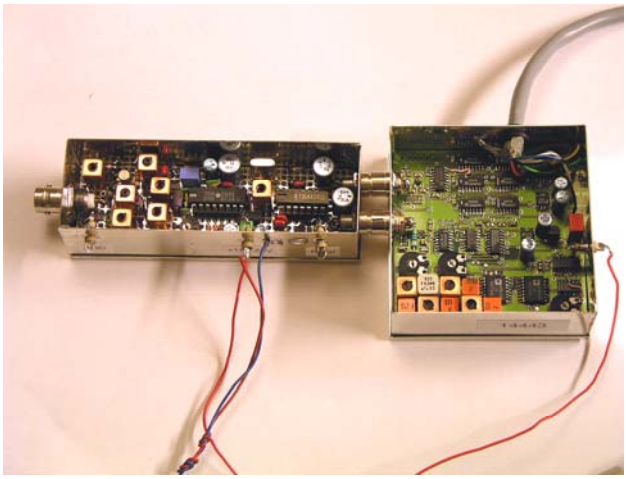

Abbildung A15: Empfänger mit angestecktem Auswerter für ISO 14443 (geöffnet)