Lehrstuhl für Messsystem- und Sensortechnik

Diversitäre Zugangs- und Sicherheitsmechanismen angewendet in automatisierten Gebäuden

Günter Westermeir

Vollständiger Abdruck der von der Fakultät für Elektrotechnik und Informationstechnik der Technischen Universität München zur Erlangung des akademischen Grades eines

Doktor-Ingenieurs

genehmigten Dissertation.

Vorsitzender:		Univ.-Prof. Dr.-Ing. habil. G. Rigoll
Prüfer der Dissertation:	1.	Univ.-Prof. Dr.-Ing., Dr.-Ing. habil. F. Schneider, i.R.
	2.	Univ.-Prof. Dr.-Ing. K. Diepold

Die Dissertation wurde am 22.01.2004 bei der Technischen Universität München eingereicht und durch die Fakultät für Elektrotechnik und Informationstechnik am 08.07.2004 angenommen.

Diversitäre Zugangs- und Sicherheitsmechanismen angewendet in automatisierten Gebäuden

Dipl.-Ing. Günter Westermeir

Kurzfassung

Feldbusse finden mittlerweile nicht nur in industriellen Automatisierungsanlagen oder im Automotive-Bereich Anwendung, sondern auch in der Elektroinstallation von Zweck- und Wohngebäuden. Die dabei entstehenden Anwendungen zur Überwachung und Sicherung von Objekten können durch die systemübergreifende Vernetzung diverser Gewerke effektiver realisiert werden. Diese Arbeit gibt einen Überblick über moderne Techniken im Bereich der Gebäudeautomatisierung, mit Blick auf die Anwendung zur Zugangskontrolle. Sowohl unterschiedliche Verfahren zur Authentisierung als auch zur Sicherung entsprechender Bereiche gegen Manipulation werden dabei untersucht. Nach der Analyse der Anforderungen an die Zugangskontrolle zu automatisierten Gebäuden im Zweck- und Wohnungsbau, zeigt diese Arbeit einen konkreten Vorschlag zur Realisierung solcher Systeme. Im Kern der Arbeit wird die Kombination diverser Mechanismen zur Authentisierung beschrieben und eine Methode zur gesicherten Datenübertragung auf dem EIB/KNX Installationsbus definiert.

Abstract

The field bus technology meanwhile is not only used by automation plants or within the automotive range, but also in the electricity installation of functional and residential buildings. Monitoring and safety applications for objects of interest can be more effectively realized by using the system-spreading network technologies of the different areas. This work gives an overview of modern techniques with respect to building automation, emphasizing on access control. Different procedures for authentication and for safety devices of buildings against manipulation are examined thereby. After analyzing the requirements of access control to functional and residential automated buildings, this work gives a detailed suggestion on the realization of such systems. In the core of the work the combination of various authentication mechanisms is described, as well as a method for the secured data communication on the EIB/KNX installation bus is defined.

Inhaltsverzeichnis

1 Einführung 1

1.1 Motivation 1
1.2 Zielsetzung 2
1.3 Gliederung der Arbeit 3

2 Stand von Wissenschaft und Technik 5

2.1 Gebäudeautomatisierung 5
2.1.1 Gebäudesystemtechnik 6
2.1.2 Offene Bussysteme 7
2.1.3 Spezielle Bussysteme 9
2.1.4 Kombination von Bussystemen 10
2.2 Zugangsmechanismen 11
2.2.1 Wissensbasierte Verfahren 11
2.2.2 Besitzbasierte Verfahren 12
2.2.3 Biometrische Verfahren 14
2.2.4 Statistisches Maß 16
2.2.5 Zugangskontrollsysteme 18
2.3 Sicherheitsmechanismen 18
2.3.1 Moderne Alarmtechnik 18
2.3.2 Verfahren zur Datenverschlüsselung 22
2.3.3 Datenverschlüsselung am Gebäudebussystem 26
2.3.4 Mechanische Sicherheit 28

3 Analyse der Systemanforderungen 33

3.1 Zweigeteilter Ansatz 33
3.2 Dienstmerkmale der Zugangskontrolle 34
3.2.1 Zugangsmechanismen 34
3.2.2 Sicherheit 35
3.2.3 Komfort 35
3.2.4 Konfiguration 35
3.3 Spezielle Dienstmerkmale des Gebäudebusses 35
3.3.1 Aktoren 36
3.3.2 Sensoren 36
3.4 Erweiterte Anwendungen 37
3.4.1 Visualisierung 37
3.4.2 Prozessabbild 37
3.4.3 Fernzugriff und Fernmelden 38

3.4.4 Featurecontroller 38
3.5 Zusammenfassung des Systemkonzepts 38

4 Multimodale Zugangskontrolle 41

4.1 Konzept der Sensorfusion 41
4.2 Bewertung von Authentisierungsmechanismen 41
4.2.1 Bestimmung der Fehlerraten 42
4.2.2 Entscheidungsfindung 43
4.2.3 Notation 44
4.2.4 Besitz- und wissensbasierte Systeme 45
4.2.5 Verifikation und Identifikation 46
4.2.6 Strategischer Entscheidungsraum 47
4.3 Kombination zweier Authentisierungsmechanismen 48
4.3.1 Konjunktion dualer Systeme 49
4.3.2 Disjunktion dualer Systeme 49
4.3.3 Fazit 50
4.4 Sensorfusion n-Systeme 51
4.4.1 Konjunktion 52
4.4.2 Disjunktion 53
4.4.3 Variationen 54
4.5 Klassifizierung der Arbeitspunkte 56
4.5.1 Entscheidungsraum 56
4.5.2 Sicherheit und Komfort 56
4.5.3 Aussagequalität 58
4.5.4 Automatische Strategieauswahl 58
4.6 Weitere Betrachtungen 59
4.6.1 N-Benutzer Systeme 59
4.6.2 Hybride Systeme 60
4.6.3 Auswerteverfahren und Inkompatibilitäten 60
4.6.4 Einsatzmöglichkeiten 60

5 Gesicherte Datenübertragung 63

5.1 Sichere Sensornetzwerke 63
5.2 Voraussetzungen 64
5.3 Das AES Verschlüsselungsverfahren 64
5.3.1 Eigenschaften 65
5.3.2 Die Zustandsmatrix 66
5.3.3 Mathematische Voraussetzungen 66
5.3.4 Der Algorithmus 68
5.3.5 Stärken des Verfahrens 73
5.4 Das SEIB-Kommunikationsprotokoll 74
5.4.1 Notation 74
5.4.2 Kommunikationsprinzip 75

5.5 Implementierung 77
5.5.1 Schlüsselgenerierung 77
5.5.2 Datenverschlüsslung 78
5.5.3 Signaturbildung 79
5.5.4 Synchronisation 81
5.5.5 Re-Synchronisation 81
5.5.6 Routing und Adressierung 82
5.5.7 Physical-Mode 83
5.5.8 Schlüsselverwaltung und Inbetriebnahme 83
5.5.9 Sensor-/Aktorproblematik 85
5.6 Ressourcenanalyse 85
5.7 Anwendung 86

6 Umsetzung des Gesamtsystems 87

6.1 Überblick 87
6.2 Der Security Server 88
6.2.1 TINI-Hardware 89
6.2.2 Buszugriff 90
6.2.3 Das TINI-Betriebssystem 91
6.2.4 Die Server Software 92
6.3 Die Zugangsmechanismen 99
6.3.1 Schnittstellendefinition am CAN-Bus 99
6.3.2 Biometrische Sensoren 101
6.3.3 Elektronische Schlüssel 105
6.4 Die Secure BCU 111
6.4.1 Hardware 112
6.4.2 Software 114
6.4.3 Sensor/Aktor-Applikation 115
6.5 Ausblick 116

7 Zusammenfassung 119

7.1 Sensorfusion im Zugangskontrollsystem 119
7.2 Verschlüsselte Datenübertragung im EIB/KNX 120
7.3 Integration in ein Gesamtsystem 121
7.4 Marktchancen 122

Anhang A Der Europäische Installationsbus 123

A.1 Entstehung und Verwendung 123
A.2 Technische Grundlagen des Bussystems 123
A.2.1 Der Physical-Layer von EIB-TP Netzwerken 124
A.2.2 Der EIB-Link-Layer 126
A.2.3 Der EIB-Network-Layer 126

A.2.4 Der EIB-Transport-Layer 128
A.2.5 Der EIB-Application-Layer 129
A.3 EIB-Telegramme und der Interworking Standard 129
A.4 Die Buskoppeleinheit 130

Anhang B Schaltpläne 133

B.1 Security Server TINI-basiert 133
B.2 ID Modul Fingerabdruckerkennung Interface 135
B.3 RSC 300 Sprechererkennung Interface 137
B.4 Atmel Smart Card Interface 138
B.5 125 kHz Transponder Interface 139
B.6 Personal Area Network Interface 140
B.7 MSP430 Secure BCU 142
B.8 EIB/KNX Meldelinien Applikation 144
B.9 EIB/KNX Blockschloss Applikation 145
B.10 Security Server IPC-basiert 147

Abkürzungsverzeichnis 149

Abbildungsverzeichnis 153

Tabellenverzeichnis 157

Literaturverzeichnis 159

1 Einführung

1.1 Motivation

Bei der Recherche zu dieser Arbeit brachte ein Zitat des Internet Magazins „Das Umwelthaus“ [Umwelt 2003] die Eigenschaften von Fenstern und Türen auf einen Punkt. Die Aussage lautete folgendermaßen:

„Durch die Tür gehen wir und durch die Fenster sehen wir. Das muss als Grundvoraussetzung reichen.“

Dieser Aussage muss man zustimmen, schließlich wurden Türen und Fenster genau dafür geschaffen. Neben diesen Grundvoraussetzungen kann man im heutigen Wohnungs- und Zweckbau sicherlich noch deutlich mehr erwarten. Angefangen bei energietechnischen Merkmalen wie Isolierung und Dichtigkeit, über das Design und den Einsatz neuartiger Materialien, bis hin zum Bedienkomfort und zur erreichbaren Sicherheit. Die letzten beiden Punkte sind Gegenstand dieser Arbeit geworden, wobei sich die Frage stellt, ob der eine den andern Punkt ausschließt und umgekehrt.

Betrachtet man die Statistik des Jahres 2002 des Bundeskriminalamtes [PKS 2002] bezüglich Diebstähle mit erschwerten Bedingungen, also Einbrüchen in an sich verschlossene Wohnungen, so erkennt man, dass bundesweit 130055 Einbrüche verübt wurden, wovon 45361 tagsüber begangen wurden. Lediglich 34,6 % aller Einbrüche blieben dabei erfolglose Versuche, bei denen die Täter entweder unterbrochen oder durch einbruchshemmende Maßnahmen abgehalten wurden. Diese Zahlen wecken bei Bewohnern automatisch ein steigendes Verlangen nach mehr Sicherheit. Gerade im heutigen Hightech-Zeitalter sollte dies eigentlich kein Problem mehr darstellen.

Die „Kölner Studie 2001“ des Polizeipräsidium Köln [Köln 2002], welche alle 3 Jahre fortgeschrieben wird, schlüsselt für den Raum Köln die Täterarbeitsweisen (modi operandi) auf. In der in Abbildung 1.1 auf der Folgeseite dargestellten Grafik, welche die 1159 erfassten Einbrüche an fensterlosen Türen unterscheidet, ist zu erkennen, dass neben dem Aufhebeln die zweithäufigste Methode das Öffnen ohne erkennbare Spuren ist. Entweder waren die Türen hier nicht ausreichend mechanisch sicher, oder sie waren überhaupt nicht verschlossen.

In solchen Fällen hätte eine „intelligente“ Tür, welche stets verschlossen ist, sich aber demjenigen, der zum Zutritt berechtigt ist, öffnet, einen Einbruch vermeiden können. Im Idealfall sollte das Öffnen einer derartigen Tür bequem ohne Schlüssel, nur mit Stimme oder Fingerabdruck möglich sein. Sie sollte zur Grundausstattung eines jeden Hauses bereits dazugehören und absolut sicher gegen Manipulationen sein. Bestimmte Besucher, wie Kaminkehrer oder Handwerker, dürften nur zu definierten Zeiten

eintreten und alles müsste sich einfach konfigurieren lassen. Um solche Szenarien realisieren zu können ist eine aufwändige, für Privatanwender kaum finanzierbare und höchstens als Sonderanfertigung machbare Schließanlage notwendig.

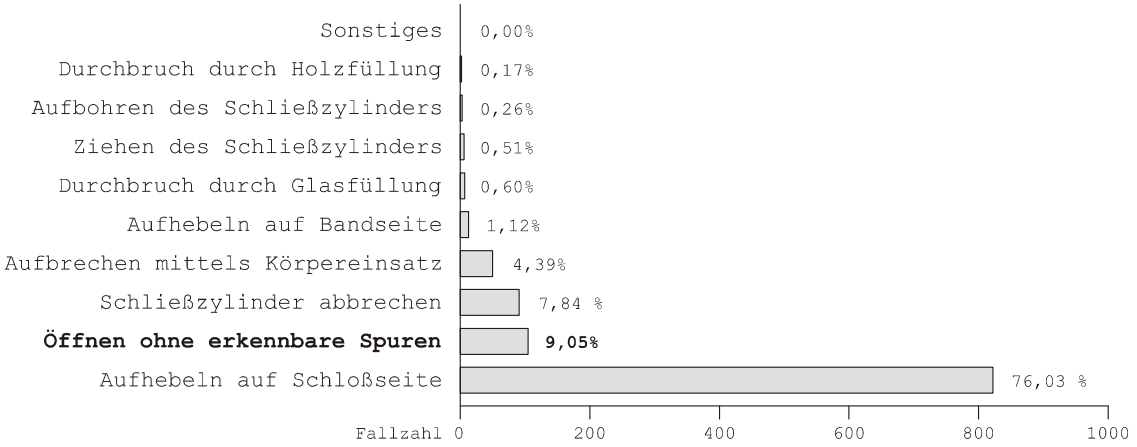

Abbildung 1.1: Täterarbeitsweisen an fensterlosen Türen, Quelle: Kölner Studie 2001

Die meisten Schließanlagensysteme, die heute auf dem Markt verfügbar sind, sind von ihrem Funktionsumfang und Bedienkomfort für den Einsatz in gewerblichen Gebäuden und Nutzbauten konzipiert worden. Die heute am Markt erhältlichen Systeme für Privatanwender stellen von ihrem Funktionsumfang und Erweiterungsmöglichkeiten proprietäre Insellösungen dar, da diese weder auf mittlerweile auch im Wohnungsbau verwendete Feldbussysteme zugreifen, noch ein akzeptables Maß an Sicherheit bieten. Daher sind grundlegende Untersuchungen an Sensorsystemen erforderlich, die einen komfortablen, aber trotzdem sicheren Zugang zu automatisierten Gebäuden ermöglichen.

1.2 Zielsetzung

Innerhalb des Forschungsprojektes tele-Haus, welches vom 01.10.1999 bis 31.03.2003 vom Bundesministerium für Bildung und Forschung (BMBF) gefördert wurde, entstand eine Arbeitsgruppe, die sich mit der Thematik der Personen- und Anwesenheitserkennung beschäftigte. Das darin entstandene Konzept der „Intelligente Tür“ ist der Ausgangspunkt für die Realisierung einer sicheren und komfortablen Zugangskontrolle ([Westermeir 2003b], [Westermeir 2003c]).

Ziel dieser Arbeit ist es, die Lücke zwischen spezialisierten Hochsicherheitssystemen und sogenannten Baumarktapplikationen zu schließen. Es wird nachgewiesen, dass das hier im folgenden vorgestellte System sowohl einen vergleichsweise hohen Komfort für den Nutzer bieten als auch höheren Ansprüchen an die Sicherheit der Zugangskontrolle genügen kann. Die Integration neuartiger Sensoren und die Entwicklung entsprechender Algorithmen bilden den Kern dieser Arbeit, wobei stets auf die Möglichkeit zur

effizienten Realisierung mit Komponenten, die einem Dauereinsatz im Wohnungsbau standhalten können, geachtet wird.

1.3 Gliederung der Arbeit

Die Arbeit konzentriert sich im ersten Teil weniger auf die mechanischen Elemente einer solchen „Intelligenten Tür“ als auf die notwendigen elektronischen Komponenten und deren integrierter Software, die zum Betrieb notwendig ist. Dies sind im speziellen die diversen Sensorsysteme, welche auf einheitlicher Basis zusammengeführt werden müssen, sowie die Auswertung der entstehenden Authentifizierungsdaten. Die in dieser Arbeit getroffene, eingeschränkte Auswahl an Sensorsystemen muss stellvertretend für eine große Zahl unterschiedlicher Authentifizierungsmechanismen betrachtet werden. Die Beschreibung der Authentifizierungsvorgänge und der anschließenden Gewichtung der unterschiedlichen Messwerte, soll eine definierte Aussage über die erreichte Sicherheit ermöglichen. Eine Bewertung der Vorgänge kann dem Benutzer später erlauben, in Form von einstellbaren Stufen zwischen einem Komfort- und Sicherheitszugang zu unterscheiden.

Der zweite Schwerpunkt dieser Arbeit liegt auf der für Sicherheitssysteme notwendigen sicheren Übermittlung gewonnener Ergebnisse über ein im Gebäude installiertes Feldbussystem in einer Art und Weise, die eine Manipulation der Daten ausschließt. Dabei werden sowohl Sensoren als auch Aktoren in die Betrachtung miteinbezogen. Im Rahmen dieser Arbeit wurde stellvertretend für die verschiedenen Bussysteme im Zweck- und Wohnungsbau der in Deutschland am häufigsten installierte Europäische Installationsbus (EIB) verwendet, der sich zeitgleich zur Erstellung dieser Arbeit innerhalb eines Convergence Prozesses mit dem European Home System EHS und dem BatiBUS zum gemeinsamen Standard KONNEX vereinte.

2 Stand von Wissenschaft und Technik

Um den aktuellen Stand der wissenschaftlichen und technischen Fortschritte auf dem Gebiet der Zugangs- und Sicherheitstechnik an automatisierten Gebäuden aufzeigen zu können, ist es notwendig, Zugangskontrollsysteme, Schließ- und Alarmanlagen mit Blick auf die Integrationsmöglichkeiten in vernetzten Gewerken zu untersuchen. Abbildung 2.1 zeigt die wichtigsten Funktionsblöcke eines automatisierten Gebäudes, welche im Rahmen dieser Arbeit einheitlich miteinander integriert werden.

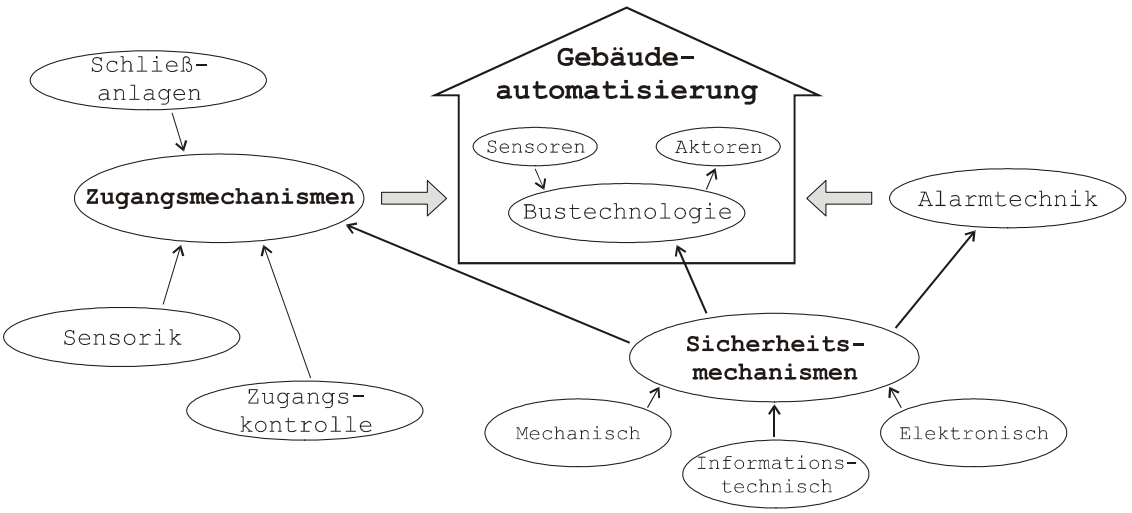

Abbildung 2.1: Zugangs- und Sicherheitsmechanismen am automatisierten Gebäude

Der folgende Abschnitt gibt einen Überblick über relevante Systeme, die bereits großflächig im Einsatz sind, sich noch in Entwicklung befinden oder auch spezialisierte Lösungen darstellen. Es werden sowohl vernetzte Zugangsmechanismen in Betracht gezogen als auch zugehörige Sicherheitstechniken für Gewerke im herkömmlichen Sinn und für automatisierte Gebäude.

2.1 Gebäudeautomatisierung

Im Szenario eines automatisierten Gebäudes spielen die eingesetzten Technologien die wichtigste Rolle. Wenn vor wenigen Jahrzehnten eine bewegungsaktivierte Außenbeleuchtung noch eine technische Errungenschaft darstellte, ist es heute bereits Stand der Technik, nahezu alle elektrischen und elektronischen Komponenten an und in Gebäuden miteinander zu vernetzen ([Kriesel 1998], [Seip 2000]). Die Vernetzung der einzelnen Gewerke soll zur Steigerung des Komforts, der Sicherheit und zur Einsparung von natürlichen Ressourcen beitragen. Multimediale und kommunikationstechnische Anwendungen, die innerhalb der letzten Jahre immer mehr an Bedeutung in der Gebäudeautomatisierung gewinnen, stellen andere Anforderungen an die Zugriffsver-

fahren, Bandbreite und Topologie [Werthsch 2003], so dass diese nicht innerhalb dieser Arbeit diskutiert werden.

2.1.1 Gebäudesystemtechnik

Unter Gebäudesystemtechnik versteht man die Automatisierung der Funktionsabläufe betriebstechnischer Anlagen in Gebäuden. Dazu gehören im klassischen Sinn die Beleuchtungsteuerung, Heizungs-, Klima- und Belüftungssysteme sowie mittlerweile auch die Zugangskontrolle im Zweckbau. Grundlage dafür sind Bussysteme, die die verschiedenen Gewerke miteinander vernetzen, damit die heutigen Anforderungen an die Gebäudeinstallation hinsichtlich

- Sicherheit und Komfort,
- flexibler Raumnutzung,
- zentraler und dezentraler Steuerungen,
- intelligenter Verknüpfungen,
- Kommunikations- und Fernwirkmöglichkeiten,
- sowie Energie- und Betriebskostenminimierung

erfüllt werden. Besonders in großen Bürogebäuden wie zum Beispiel Banken, wo auf ein Höchstmaß an Flexibilität, Sicherheit und Komfort Wert gelegt wird, kommen diverse Installationsbusse zum Einsatz. Durch die Verwendung offener Bussysteme, wie beispielsweise dem Europäische Installationsbus oder dem Local Operating Network, ist der Einsatz von Komponenten unterschiedlicher Hersteller und Anbieter möglich, da die Komponenten interoperabel sein müssen. Offene Bussysteme machen Insellösungen überflüssig. Sie ermöglichen es, verschiedene Gewerke miteinander zu verbinden, was Material- und Logistikkosten einspart. So lassen sich Beleuchtung, Sonnenschutz, Heizung, Lüftung, Tür- und Fensterüberwachung, Melder und Anzeigen, zeitabhängige Steuerung, Energie- und Gebäudemanagement kombinieren. Zahlreiche Studien und Forschungsprojekte zeigen, dass durch die Gewerke umfassende Vernetzung je nach Anwendungsfall bis zu 60% der Energiekosten für Beleuchtung und bis zu 30% der Heizkosten durch konsequente Nutzung der Automatisierungstechnik nachhaltig eingespart werden können. Dies zeigt unter anderem der dem Deutschen Bundestag durch die Enquete-Kommission im Jahre 2002 vorgelegte Schlussbereicht zur nachhaltigen Energieversorgung [Enquete 2002], zu dem Forschungsergebnisse zahlreicher Institute beigetrugen. Ähnliche Ergebnisse konnten bereits im Jahre 2000 durch das Schweizer Bundesamt für den Stromverbrauch in vernetzten Haushalten nachgewiesen werden [Schweiz 2000]. Seit die Gebäudesystemtechnik zu einem

Begriff wurde, wurden parallel mehrere offene Bussystem entwickelt, die in den nachfolgenden Abschnitten kurz aufgeführt sind.

2.1.2 Offene Bussysteme

Sogenannte offene Bussysteme der Gebäudesystemtechnik sind genau definierte Feldbusse, für die beliebige Hersteller Produkte entwickeln. In der Regel gibt es zu jedem System eine Organisation, die das System definiert und Produkte von Firmen entsprechend zertifiziert [deSpecial 1999].

2.1.2.1 Europäischer Installationsbus

Der Europäische Installationsbus (EIB) ist ein dezentrales Bussystem mit genau definierten Schnittstellen und einem normierten Übertagungsprotokoll nach dem ISO/OSI Modell (International Standard Organisation Open System Interconnection). Der Buszugriff der einzelnen Teilnehmer wird nach dem CSMA/CA-Verfahren (Carrier Sense Multiple Access/Collision Avoidance) geregelt, wobei mehr als 60000 Teilnehmer adressiert werden können, die mittels Koppler und Router in logische Segmente aufgeteilt sind. Die Übertragungsgeschwindigkeit liegt bei 9600 bit/s auf dem Twisted Pair Medium. Es sind ebenfalls Powerline und drahtlose Medien definiert. Die European Installation Bus Association (EIBA) in Brüssel organisiert die Arbeiten der beteiligten, zum größten Teil deutschen Firmen und zertifiziert deren Produkte, die somit zueinander kompatibel sind. Eine genaue Beschreibung der EIB Technik wird im Anhang A gegeben.

2.1.2.2 BatiBUS

Der BatiBUS ist ein standardisiertes BUS-System, welches seinen Ursprung vor allem in Frankreich hat. Die Firmen, die Komponenten für den BatiBUS produzieren, sind im BatiBUS Club International (BCI) organisiert. Die Produkte müssen durch die Laboratoire Central des Industries Electriques (LCIE) zertifiziert werden. Als Medium ist Twisted Pair definiert, wobei eine Datenrate von 4800 bit/s bei beliebiger Topologie erreicht wird. Der Buszugriff basiert auf dem CSMA Verfahren, wobei die Adressen der Teilnehmer über DIP-Switches oder Codiertaster fest eingestellt sind.

2.1.2.3 European Home Systems

Nachdem sich europäische Konzerne zu einer Projektgruppe für BUS-Systeme zusammengeschlossen hatten, wurde zur Durchsetzung von Standards aus diesem Projekt die European Home System Association (EHSA) gegründet. Technisch entspricht der EHS dem CEBus, welcher 1992 in USA durch die Electronic Industries Association entwickelt wurde. Derzeit werden die zwei Medien Twisted Pair mit 48 kbit/s und Powerline mit 2400 bit/s unterstützt. Es können beliebige Topologien

realisiert werden, wobei das Zugriffsverfahren nach CSMA verwendet wird. Es lassen sich mehr als 10^{12} Teilnehmer adressieren. Das EHS Standards Control Committee (SCC) ist für die Weiterentwicklung und die Integrität des Systems verantwortlich. Alle Produkte unterliegen einem Zertifizierungsprozess.

2.1.2.4 Konnex

Während der Zeit, in der diese Arbeit entstand, wurde ein sogenannter Convergence Prozess gestartet, der das Ziel hat, mehrere dieser Bussysteme zu vereinheitlichen. Im Jahre 1999 wurde die Konnex Association gegründet, eine Vereinigung, die zum Großteil das Personal der EIBA übernommen hat. Das Konnex System definiert den Zusammenschluss von BatiBUS, EHS und EIB, welcher kurz als KNX bezeichnet wird [Konnex 2002]. Derzeit besteht die Konnex Spezifikation aus der Definition diverser Gateways, die eine Zusammenarbeit der unterschiedlichen Bussysteme ermöglichen. In Zukunft wird es Endgeräte geben, die ein Superset der drei Bussysteme beinhalten und ohne Gateways untereinander kommunizieren. Bereits heute werden vorläufige Konnex Logos vergeben, die eine entsprechende Zertifizierung voraussetzen.

Auf Grund der Tatsache, dass das Konnex System einen europaweiten, offenen Standard darstellt und somit in nächster Zukunft weiter zum Einsatz kommen wird, als auch der Möglichkeit, neue Ansätze in den Convergence Prozess mit einbringen zu können, stützt sich die Arbeit im Folgenden auf den als EIB/KNX bezeichneten Industriestandard.

2.1.2.5 Local Operating Network

Die Local Operating Network Technologie (LON) stammt ursprünglich aus den USA und basiert auf Mikrochips der Firma Echelon [Echelon 2001]. Es ist ein gewerkeübergreifendes Gebäudemanagement-System mit dem Ziel der Energieeinsparung und der Erhöhung des Komforts. Die komplette Technologie, die LON zugrunde liegt, wird als LonWorks bezeichnet. Je nach Medium sind Datenraten zwischen einigen kbit/s und 1,5 Mbit/s erreichbar, wobei wie bei EIB Systemen auch hier beliebige Topologien realisiert werden können. Die Sprache des LON heißt LonTalk-Protokoll und ist einheitlich für alle Knoten bereits in den als Neuron-Chip bezeichneten Transceivern implementiert. Die Adressierung unterscheidet Domains, Subnets und Nodes, so dass über 30000 Teilnehmer pro Domain miteinander kommunizieren können. Zahlreiche Hersteller produzieren Sensoren und Aktoren zur Anbindung an LON. Ein Standardisierungsgremium (LONMARK) überwacht die Kompatibilität der Anwendungen, indem es Standards setzt und Aktualisierungen beschließt. In Europa wird LON hauptsächlich im Zweckbau eingesetzt. Genauere Details sind in [Dietrich 1999] beschrieben.

2.1.2.6 X-10

Anfang der 70er Jahre wurde dieses System in den USA entwickelt. Das System nutzt die vorhandene Elektroinstallation, wodurch es entsprechend kostengünstig ist. Nach der X-10 Spezifikation sind nur wenige Kommandos zugelassen, so dass diese für komplexe Anwendungen nicht ausreichen und durch die Anwenderfirmen beliebig erweitert werden. Dadurch ist keine Kompatibilität unter den verschiedenen Herstellern gewährleistet. Die Kommunikation läuft nach einem Sender-Empfänger Prinzip mit Hilfe einer sogenannten Steuerkonsole.

2.1.3 Spezielle Bussysteme

Neben den offenen Bussystemen der Gebäudesystemtechnik existieren eine Reihe proprietärer Busse, welche meist nur von einem Hersteller unterstützt werden. Einige dieser Systeme sollen hier kurz erwähnt werden:

Actor T-Bus — Der Actor T-Bus entspricht von seinen Eckdaten etwa dem EIB, ist aber nicht kompatibel. Einfache Bedienelemente wie Tastfelder und Standardschalter des EIB System können als Applikationen verwendet werden.

DALI — Digital Addressable Lighting Interface ist ein Lichtsteuersystem basierend auf einem zentralen Controller. Es erlaubt das komfortable Steuern von Lichtszenen hauptsächlich für Büroräume und öffentliche Einrichtungen.

FTS — Das Ferntastsystem (FTS) ist ein sehr einfaches und preiswertes System, welches vorrangig für Beleuchtungs- und Jalousiemanagement eingesetzt wird.

LCN — Local Control Network ist ein ähnliches Multi-Master System wie EIB oder LON, welches über eine zusätzliche Ader zur Versorgungsleitung kommuniziert.

PHC — Peha House Control basiert auf einem SPS-System und ist für den privaten Wohnungsbau konzipiert. Es wird im Elektro-, Heizungs-, Lüftungs- und Sicherheitsbereich eingesetzt.

SMART — SMART-House-System ist ein zentrales System das vor allem für den Neubau gedacht ist. Die breitbandige Übertragung wird auch zur Übertragung von Audio- und Videosignalen genutzt.

tebis-TS — Das System entspricht dem EIB, benutzt aber ein eigenes Datenprotokoll. Die Konfiguration wird über ein sogenanntes Verknüpfungsgerät vorgenommen. Es dient hauptsächlich zur Realisierung von Beleuchtungs- und Beschattungsanlagen sowie Heizung- und Alarmierungssystemen.

Z-BUS Der Z-Bus ist ein einfaches System, das über einen zusätzliche Ader zu den Versorgungsleitungen nach dem Sender-Empfänger-Prinzip arbeitet.

2.1.4 Kombination von Bussystemen

Einen wichtigen Aspekt der Gebäudeautomatisierung stellt, auf Grunde der Vielfalt der eingesetzten Systeme, die Kombination der unterschiedlichen Bussysteme innerhalb eines automatisierten Gebäudes dar. Neben wissenschaftlichen Ansätzen zur Integration unterschiedlicher Systeme in die Heimautomatisierung [Werthsch 2003] und der Definition von Mechanismen, die unterschiedliche Systeme ineinander übergehen lassen (Konnex Convergence Prozess), werden meist Gateways entwickelt. Solche Gateways erlauben in der Regel das Ankoppeln niederratiger Steuerbusse an ein übergeordnetes Backbone System. Ziel ist hierbei die Visualisierung oder das Management der angeschlossenen Gebäudebussysteme [Weinzierl 2001]. Für solche Zwecke gibt es zum Beispiel das CONTINUUM System der Firma AndoverControls, eine Weiterentwicklung des INFINITY Systems, welches auf Computernetzwerken basiert und für komplexe Systeme mit großen Datenmengen geeignet ist. Über entsprechende Gateways können unter anderem Videoüberwachungs-, EIB, LON und SPS Systeme integriert werden.

Für nahezu alle Gebäudeautomatisierungssysteme sind von den jeweiligen Herstellern diverse Gateways für Fernwirktechniken erhältlich. Diese Gateways erlauben Verbindungen über ISDN oder analoge Telefonleitungen zu Businstallationen. Ziel dabei ist die Überwachung bestimmter Gerätezustände, das Steuern bestimmter Systeme oder die Fernwartung und Konfiguration. Die technischen Ausführungen liegen dabei zwischen Softwarelösungen für Personal Computer über integrierte Embedded Lösungen bis zu Gatewaypaaren, die alle Bussignale tunneln, um eine Installation räumlich zu verlagern. Einige der Techniken sind bereits in [Kranz 1997] beschrieben.

Auf Grunde der immer stärkeren Verbreitung von Computernetzwerken, basierend auf dem TCP/IP Protokoll (Transfer Control Protocol / Internet Protocol), bewegt sich der Trend für Gateways der Gebäudeautomatisierung in Richtung von Service Schnittstellen, die standardisierte Dienste der Feldbus- oder Internettechnik bieten. Im folgenden sind beispielhaft zwei embedded Gateways in Form von Reiheneinbaugräten beschrieben.

Das DISCH Gateway IP der Firma Disch GmbH ist der erste verfügbare embedded EIB/OPC Server, der den EIB direkt an Ethernet anbindet. OPC (OLE for Process Control) stellt einen Industriestandard dar, der den Zugriff auf Systeme der Prozessautomatisierung unter anderem über diverse Netzwerke definiert. Die Einbindung von Sensoren und Aktoren über Computernetzwerke basiert hierbei auf Microsoft's OLE (Object Linking and Embedding) Technik. Am EIB angeschlossenen Busteilnehmer können dadurch mit beliebiger Software, die OPC Schnittstellen unterstützt, über TCP/IP Netzwerke visualisiert und gesteuert werden.

Der Internet Controller ic.1 drEIB der Firma ICONAG AG ist ein embedded EIB Gateway mit integriertem Webserver. Über das im Internet verwendete HTTP-Protokoll (Hypertext Transfer Protocol) lassen sich die am EIB angeschlossenen Teilnehmer über HTML-Seiten (Hyper Text Markup Language) visualisieren und steuern. Das Gerät übernimmt zusätzliche Funktionen wie das Protokollieren von Zuständen, das Auslösen zeitlicher Ereignisse oder Melden von Betriebszuständen. Der Internet Controller kann sowohl direkt an Ethernet-Netzwerke angeschlossen werden als auch über ein Internet-Portal per ISDN angerufen werden.

2.2 Zugangsmechanismen

Auf Grund zahlreicher Entwicklungen diverser Verfahren zur Authentisierung von Personen, sowie der stetigen Leistungssteigerung und Miniaturisierung der Computerhardware, finden solche Technologien mittlerweile auch im Bereich der Gebäudesystemtechnik immer häufiger Anwendung. Systeme, ähnlich wie sie in Hochsicherheitsanlagen und Banken seit Jahrzehnten eingesetzt und auch weiter verbessert wurden, werden, wenn auch in etwas vereinfachter Form, bereits zur Zugangskontrolle für Wohn- und Hotelanlagen angeboten. Ausschlag gebend hierfür ist der Trend zu integrierten, sehr kompakten Lösungen, die ein hohes Maß an Sicherheit bieten. Die verwendeten Verfahren lassen sich in drei Gruppen einteilen; wissensbasierte, besitzbasierte und biometrische Verfahren. Im folgenden werden die wichtigsten Sensoren für diese Verfahren kurz gezeigt.

2.2.1 Wissensbasierte Verfahren

Die einfachste Form der elektronischen Authentisierung ist der PIN-Code (Personal Idetification Number), eine Zahl, die nur derjenige kennen sollte, der sich beispielsweise Zutritt verschaffen, oder am Bankautomaten Geld abheben will. Hierzu gehört auch die TAN (Transaction Number), welche nur für einen einzigen Vorgang gültig ist. Diese wird meist zusammen mit einer PIN benutzt. In der einfachsten Form werden diese Nummern über einen Zahlentastenblock eingegeben, wohingegen bei Computersystemen mit alphanumerischer Tastatur ganze Passwörter oder auch sogenannte Einmal-Passwörter, ähnlich der TAN, abgefragt werden. Als Sensoren kann man hier die Tasten bezeichnen, über die die Eingabe gemacht wird.

In der Regel liefern diese außer dem zugeordneten Zeichen keine weiteren Informationen. Es gibt jedoch Arbeiten auf dem Gebiet der Analyse des dynamischen Tippverhaltens von Benutzern. Wissenschaftler an der New York University und dem Bell Communications Research Center haben dahingehend bereits weiterführende Arbeiten veröffentlicht [Monrose 1997]. Mittels Mustererkennungsverfahren, basierend auf Zeitmessungen der Tastenanschläge, wird der Anmeldevorgang mit gespeicherten Trainingsdatensätzen des jeweiligen Benutzers verglichen. Dieses als Keystroke-Scan

bezeichnete Verfahren wird von vielen Firmen untersucht, um beispielsweise auf das Alter von Personen zu schließen, die sich im Internet als volljährig ausgeben.

2.2.2 Besitzbasierte Verfahren

Die gängigste Art der Authentisierung von Personen gegenüber diversen Systemen basiert auf dem Besitz eines Schlüssels. Dieser kann sowohl mechanisch oder, für diese Arbeit interessant, elektronisch sein. Die Variante der geringsten Sicherheit ist hierbei die Magnetstreifenkarte, sie dient lediglich zum Transport von Informationen wie beispielsweise der Kontonummer bei der EC-Karte, weshalb diese meist mit einem wissensbasiertem Verfahren oder der Verifikation per Unterschrift kombiniert wird.

Die Magnetkartentechnik wird heute bereits großflächig durch integrierte, elektronische Lösungen ersetzt. Diese können beispielsweise in Form von Smart Cards, Transpondern oder iButtons ausgeführt sein. Abbildung 2.2 zeigt verschiedene Ausführungen dieser Systeme. Die Bauformen reichen vom Scheckkartenformat über Schlüsselanhänger, Ringen und Folien, bis hin zu Glaskapseln.

Abbildung 2.2: Smart Cards, iButtons und diverse Transponder

Der wesentliche Unterschied liegt hauptsächlich beim Übertragungsmedium. Smart Cards [Rankl 2002] und iButtons [Dallas 2000] sind mit elektrischen Kontakten ausgestattet, über die seriell Daten übertragen werden und der Controller mit Strom versorgt wird. Transponder hingegen werden induktiv mit Strom versorgt, wobei auch die Daten in beide Richtungen entsprechend übertragen werden [Finkenz 2002]. Die Datenrate liegt bei wenigen kByte/s, wobei je nach System eine Entfernung zwischen der Übertragungseinrichtung und dem Transponder von einem Zentimeter bis zu etwa einem Meter erreicht wird. Oft werden auch kleine Handsender als Transponder

bezeichnet. Diese sind mit einer Batterie ausgestattet und übertragen ihre Daten mittels modulierten, elektromagnetischen Wellen oder infrarotem Licht. Dieses Prinzip findet hauptsächlich in Schließanlagensystemen von Automobilen Verwendung. Der Authentisierungsvorgang wird dabei meist per Tastendruck ausgelöst.

Die Smart Card und Transponder-Technik gilt als sicherer als Magnetkarten, da moderne Versionen über ein beschränktes Maß an Rechenleistung und Datenspeicher verfügen. Die Daten, die den Benutzer authentifizieren, sind in einem geschützten Speicherbereich abgelegt und können nur unter der Verwendung kryptographischer Funktionen in Verbindung mit geheimen Schlüsselzahlen ausgelesen werden. Dies verhindert das Reproduzieren solcher Schlüssel durch Dritte. Besonders interessant sind Java Smart Cards [Chen 2002] oder Dallas iButtons, die eine Java Virtual Machine mit Unterstützung für unterschiedliche Verschlüsselungsverfahren zur Verfügung stellen [JCM 2000]. Die stetige Weiterentwicklung der Mikrocontrollertechnologie sowie die Bemühungen, solche Systeme zu standardisieren, erlaubt es mittlerweile, mehrere Anwendungen in einem System zu realisieren. Neben der Verwendung zur Authentifizierung sowie zur Speicherung von Benutzerdaten, sind solche Datenträger auch als elektronische Ausweise oder Geldbörsen geeignet. Der einzige Nachteil besteht darin, dass der Benutzer jederzeit das Gerät mit sich führen muss, und es somit leicht verloren oder gestohlen werden kann. Um den Missbrauch durch unberechtigte Personen zu verhindern, überprüft die Smart Card eine einzugebende PIN, die nur die berechtigte Person kennt, bevor diese ihren eigentlichen Zweck erfüllt und sich gegenüber dem Kartenserver, meist mittels einer Challenge-Response-Methode, authentifiziert. Aktuelle Forschungsarbeiten gehen bereits dazu über, Karten zu entwickeln, bei denen sich der Benutzer per Fingerabdruck authentisieren muss. Der Referenzfingerabdruck der Person ist dabei in der Smart Card gespeichert und verlässt diese auch nicht [Schels 2002]. Diese Verfahren werden als MOC-Verfahren (Match-on-Card) bezeichnet, wobei die Bauform nicht an Karten gebunden ist, hierfür gebräuchlich ist auch der Begriff „Token“. Großflächig wird ein solches System bereits im südostasiatischen Sultanat Brunei als digitaler Personalausweis eingesetzt [Sietmann 2002]. Die eingesetzte Technologie stammt von der deutschen Firma Dermalog Identification Systems GmbH, die AFIS-Systeme (Automated Fingerprint Identification Systems) herstellt. Erste Prototypen der Firma Siemens oder der Biometric Associates, Inc. [BAI 2002] beinhalten auch den Scanner für die Fingerabdrücke mit auf der Prozessorkarte.

Ein weiteres, besitzbasiertes Verfahren ist die Authentisierung mittels dynamisch vernetzter Kleingeräte, die am Körper getragen werden und nach dem Personal Area Network Prinzip (PAN) miteinander kommunizieren. Dabei handelt es sich um voll netzwerkfähige Systeme wie Mobiltelefone oder Organizer, die um den Benutzter herum, bis zu einem maximalen Abstand von 10 Metern, mit anderen Geräten kommunizieren. Als Netzwerktechnik kann beispielsweise Bluetooth oder, wie später in dieser Arbeit detailliert beschrieben, die Datenübertragung per Hautkontakt dienen.

2.2.3 Biometrische Verfahren

Mittels biometrischer Verfahren werden physiologische, statische Merkmale wie der Fingerabdruck, die Netzhaut und Augeniris, die Hand- und Gesichtsgeometrie, der Geruch oder die Lippenform zur Authentisierung von Personen herangezogen. Die Analyse dynamischer Kennwerte wie der zeitliche Verlauf der Sprache, Schrift, Bewegung oder eines Tastenanschlages sind ebenfalls biometrische Verfahren zur Authentisierung. Eine genaue Beschreibung aller Systeme würde den Rahmen dieser Arbeit sprengen, deshalb sollen hier nur die wichtigsten Systeme vorgestellt werden. Ein umfassender Überblick wird unter anderem in [AFR 2003] gegeben. Abbildung 2.3 zeigt die durch die International Biometric Group (IBG) evaluierte Aufteilung der Marktsegmente der aktuell eingesetzten biometrischen Systeme.

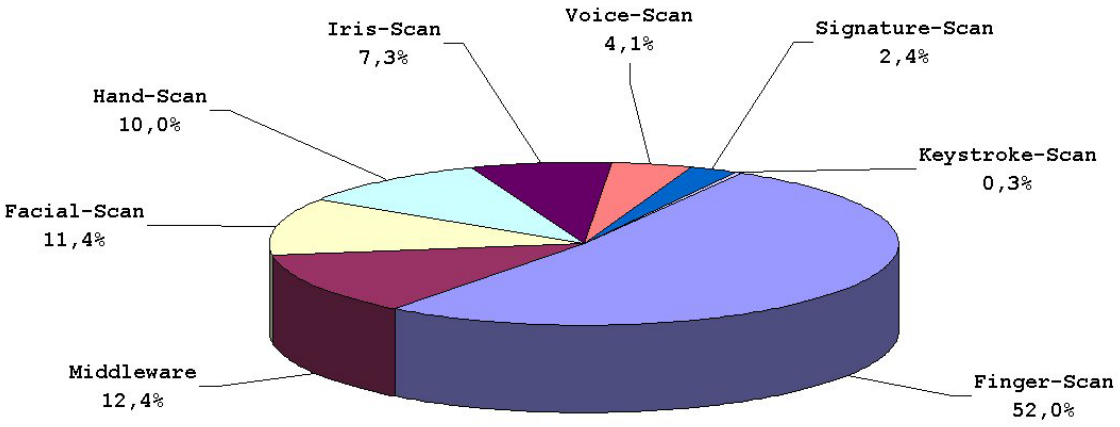

Abbildung 2.3: Marktaufteilung biometrischer Systeme 2003, Quelle: International Biometric Group

Der Fingerabdruck stellt das bekannteste und wahrscheinlich älteste biometrische Merkmal zur Identifikation von Personen dar [Busch 2002]. Das Analyseprinzip basiert stets auf dem Abbild des Fingerabdruckes. Zahlreiche Sensoren sind dafür bereits auf dem Markt erhältlich. Angefangen bei optischen Sensoren, wie sie in Videokameras Verwendung finden, oder Scannerzeilen, ähnlich wie bei Flachbettscannern, über kapazitive Sensoren bis hin zu Ultraschallsensoren der Firma OPTEL, die alle ein Graustufenabbild der Fingeroberfläche darstellen. Abbildung 2.4 zeigt den Siemens FingerTIP Sensor, der bereits in zahlreichen Zugangskontrollsystemen eingesetzt wird.

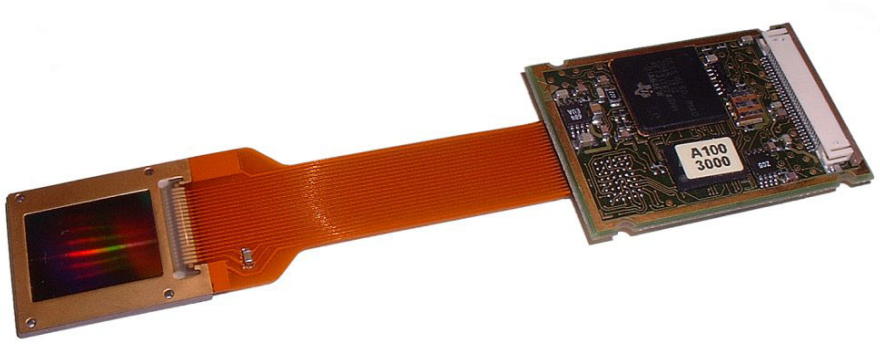

Abbildung 2.4: Siemens FingerTIP Sensor mit TopSec ID Modul

Dieser auf CMOS Technik basierende Sensor ist in der Lage, kapazitiv ein mit 8 Bit quantisiertes Graustufenbild von 224 x 288 Pixel der Sensorfläche von 11 x 14 mm² aufzunehmen und über eine einfache parallele Schnittstelle zur Verfügung zu stellen. Die Bilddaten des Fingerabdruckes werden dann mit Methoden der Bildverarbeitung auf die Anordnung der Hautleisten (Hügel und Täler) hin untersucht. Von besonderem Interesse sind die Minutien, Merkmale wie Gabeln, Verzweigungen und Inseln, die für den Vergleich mit gespeicherten Referenzmustern herangezogen werden. In Abbildung 2.4 ist auch das Siemens TopSec ID Modul zu sehen, welches genau diese Merkmalextraktion vornimmt. Ein solches Modul erlaubt den Vergleich eines Fingerabdruckes mit bis zu 1000 gespeicherten Referenzmustern innerhalb einer Sekunde.

Neben der Auswertung von Fingerabdrücken sind die mit am häufigsten eingesetzten biometrischen Verfahren die Analyse der Hand- und Gesichtsgeometrie. Im wesentlichen dienen hier Kameras zur Aufnahme der Bilder, wobei bei der Vermessung der Handgeometrie nur der Schattenwurf berücksichtigt wird. Die Form und Länge der Finger so wie des Handrückens sind hier die zu messenden Parameter. Deutlich komplexer ist der Aufwand zur Vermessung der Gesichtsgeometrie, da die Messergebnisse unabhängig von der Beleuchtungsstärke, dem Bildhintergrund, der Stellung des Kopfes sowie Veränderungen im Haarwuchs sein sollen. Hierzu wird das Gesicht durch elastische Graphen repräsentiert (Elastic Graph Matching), an deren Kreuzungspunkten sich charakteristische Merkmale wie Augen, Nase, Kinn oder ähnliches befinden. Mit Hilfe neuronaler Netze werden diese Daten mit Referenzbildern verglichen. In den USA werden derzeit zur Terrorismusbekämpfung entsprechende Systeme an Flughäfen eingesetzt, mit dem Ziel, jeden Passagier auf dessen Identität zu prüfen. Neben dem Elastic Graph Matching gibt es zahlreiche weitere Methoden zur Gesichtserkennung.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) und das Bundeskriminalamt (BKA) beauftragte das Fraunhofer Institut für Graphische Datenverarbeitung (FhG-IGD), eine Studie über "Vergleichende Untersuchung Biometrischer Identifikationssysteme" (BioIS) durchzuführen. Die Studie liefert genaue Aussagen über die unterschiedlichen Analyseverfahren, angewendet auf biometrische Identifikationssysteme.

Ähnlich dem Fingerabdruck kann auch der Augenhintergrund (Netzhaut) oder die Augeniris zur Authentifizierung herangezogen werden. Die Iriscode-Erzeugung geht auf Bildverarbeitungstechniken des britischen Forschers John Daugman zurück. Zur Erfassung wird ein hochauflösendes Bild der Iris aufgenommen, welche über 200 verschiedene Merkmale trägt und sich prinzipiell besser zur Authentifizierung eignet als der Fingerabdruck [Busch 2002].

Bei der Sprachanalyse werden gesprochene beliebige oder vorher festgelegte Texte analysiert, wobei letzteres Verfahren eine wesentlich niedrigere Fehlerrate liefert. Um die Sprechererkennung aus aufgezeichneten Lauten trennscharf durchzuführen, verwenden die Forscher und Entwickler Methoden der Signalverarbeitung. Das zeitabhängige Signal der gesprochenen Worte wird mit seinen frequenzspezifischen Energieanteilen über die Zeit in Spektrogrammen aufgezeichnet und nach einer dynamischen Zeitnormierung mit den entsprechenden Frequenzen des Referenzsignals verglichen [Vary 1998]. Zu solchen Zwecken sind mittlerweile spezialisierte Chipsätze erhältlich, die diese Analyseverfahren beinhalten, wie zum Beispiel der Sensory RSC-300 Mikrocontroller [Sensory 2000], der später in dieser Arbeit genauer beschrieben wird.

Bei der Auswertung biometrischer Merkmale geht es in der Regel darum, die Identität einer Person festzustellen, wobei zwischen zwei Vorgängen unterschieden wird. Die Identifikation und die Verifikation. Bei der Identifikation werden die aufgenommenen Merkmale mit den Merkmalen aller gespeicherten Personen verglichen, um aus der Menge aller Benutzter denjenigen herauszufinden, der sich authentisieren will. Bei der Verifikation steht von vorne herein fest wer sich authentisieren will, beispielsweise durch die Verwendung einer Smart Card, so dass die Merkmale nur mit einer Referenz verglichen werden müssen.

Bei biometrischen Systemen stellt sich immer wieder die Frage, ob die Sensoren überlistet werden können. Um dies zu verhindern, werden die Systeme mit einer Lebenddetektion kombiniert. Bei Fingerabdrücken beispielsweise kann mittels infrarotem Licht der Blutsauerstoffgehalt gemessen werden oder bei der Gesichtserkennung das Blinzeln mit dem Augenlid. Schwierig ist dies bei der Sprachanalyse, weshalb Systeme entwickelt wurden, die dem Benutzer jedes Mal eine Frage stellen, die richtig beantwortet werden muss.

2.2.4 Statistisches Maß

Wegen der natürlichen Variation der biometrischen Merkmale arbeitet jeder der mehrstufigen Auswertealgorithmen der diversen Authentisierungssysteme mit gewissen Toleranzschwellen. Hier wird bestimmt, welche Abweichung der aufgenommenen Merkmale zu den Referenzmerkmalen für eine erfolgreiche Authentisierung ausreicht. Mit zunehmenden Anforderungen an die Übereinstimmung der Merkmalsvektoren nimmt die Rate der fehlerhaft abgewiesenen Personen zu (FRR – False Rejection Rate).

Setzt man hingegen die Toleranzschwelle herab, steigt die Anzahl der fälschlich als autorisiert erkannten Personen (FAR – False Acceptance Rate).

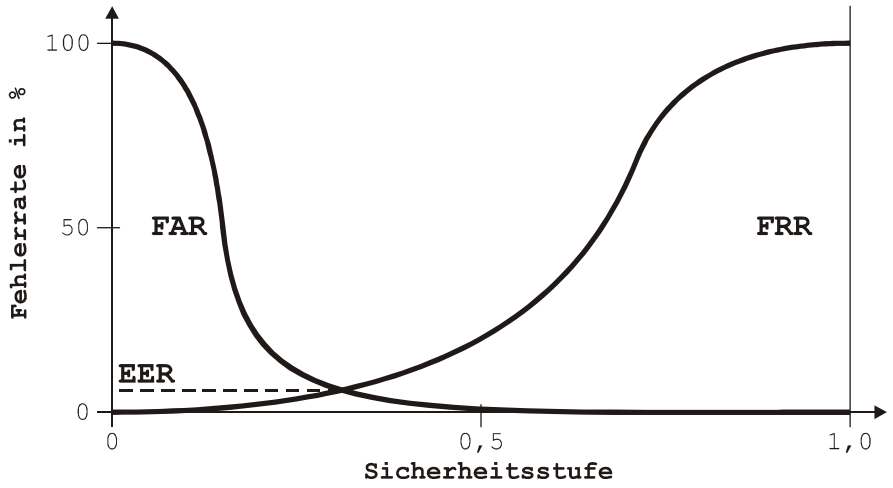

Abbildung 2.5: Typische Badewannenkurve

Abbildung 2.5 zeigt die typische Darstellung der FAR und FRR in einem Diagramm, welches als Badewannenkurve bezeichnet wird. Die Toleranzschwelle, beziehungsweise die gewählte Sicherheitsstufe ist hierbei auf eins normiert. Die Gleichfehlerrate (EER – Equal Error Rate) ist ein Maß für die Güte des Erkennungssystems und wäre im Idealfall gleich Null. Ziel der Hersteller solcher Systeme ist es, die Toleranzschwelle genau in diesen Punkt zu legen. Tatsächlich liegt sie bei aktuellen Systemen deutlich höher als bei 0 %. Tabelle 2.1 zeigt die Ergebnisse von Feldversuchen des Fraunhofer-IGD im Jahre 1999 und der T-Systems Nova Studie im Jahre 2000. Die Abweichungen der durchschnittlichen FRR zeigt, dass diese Zahlen nur einen Trend angeben, wie sicher die verschiedenen biometrischen Verfahren zueinander sind. Die Aussagekraft der Zahlen hängt sehr stark von den Messbedingungen ab, die bei beiden Studien verwendet wurden.

Tabelle 2.1: Fehlerraten unterschiedlicher biometrischer Systeme

FRR	Fraunhofer-IGD (1999)	T-Systems Nova (2000)
Iriserkennung	0,45 %	1,6 %
Gesichtserkennung	2,35 %	1,5 %
Fingerabdruck	5,73 %	21 %
Sprecherverifikation	-	32 %
Unterschrift	14,58 %	54 %

2.2.5 Zugangskontrollsysteme

Auf Basis der oben genannten Authentisierungsmechanismen existieren bereits zahlreiche Zugangskontrollsysteme. Viele dieser Systeme arbeiten autark oder dienen zur Authentisierung von Personen gegenüber Rechnern, die wiederum mit Schließanlagensystemen gekoppelt sind oder zur Aufzeichnung personenbezogener Daten verwendet werden.

Einige der Systeme erlauben den direkten Anschluss an Gebäudebussysteme, wie das Winkhaus highSecurity System mit elektronischen Schließzylindern und in den Schlüsseln integrierten Transpondern. Die Steuerelektronik, die zum Schließzylinder gehört, speichert und verwaltet die Anlagendaten, prüft und erteilt die Schließfreigaben der Zylinder bei berechtigten Schlüsseln, sperrt unberechtigte Schlüssel und organisiert Schaltfunktionen über den EIB.

Ein System von SimonsVoss erlaubt die Vernetzung von digitalen Schließzylindern und Blockschlössern per LON. Mittels einer Netzwerksoftware und eines LON-Gateway kann das Schließ- und Organisationssystem als ein per Personal Computer gesteuertes Zugangskontrollsystem verwendet werden. Die Schließzylinder selbst werden über aktive, mit Batterie gespeiste Transponder bedient. Auch die Ankopplung der Zylinder und Blockschlösser an den LON geschieht über eine verschlüsselte 868 MHz Funkverbindung.

2.3 Sicherheitsmechanismen

Der folgende Abschnitt beschreibt die wichtigsten Sicherheitsmechanismen, welche an Gebäuden angewendet werden können. Diese umfassen elektronische Systeme der Alarmtechnik und informationstechnische Mechanismen auf Feldbusebene für automatisierte Gebäude. Die mechanische Sicherheit in Gebäuden, die nach dem Stand der Technik erreicht werden kann, wird hier ebenfalls umrissen.

2.3.1 Moderne Alarmtechnik

Die moderne Alarmtechnik umfasst heutzutage nicht nur leistungsfähige Sensorik zum Erkennen von Gefahren, Einbruchs- und Manipulationsversuchen sowie der Weiterleitung von Signalisierungen, sondern auch der Vernetzung aller Systeme und die Integration in die Gebäudesystemtechnik. Bei der Planung, Installation und Instandhaltung von Gefahren- und Einbruchmeldeanlagen wird nach anerkannten Regel der Technik vorgegangen. Diese Regeln sind unter anderem in Normen und Richtlinien niedergelegt. Die VDE-Klassifikation (Verband der Elektrotechnik, Elektronik und Informationstechnik) beschreibt nach VDE 0830 die Anforderungen an Alarmanlagen hinsichtlich Übertragungseinrichtungen, Energieversorgung, elektromagnetischer Verträglichkeit, Anwendungsregeln und Methoden für Umweltprüfungen. Die VDE 0830 Klassifikation [VDE 0830] entspricht den DIN-Normen (Deutsches Institut für

Normung e.V.) DIN EN 50130, 50131, 50132, 50134 und 50136. Innerhalb der Norm DIN VDE 0833 Teil 1 bis 3 sind Festlegungen der Gefahrenmeldeanlagen für Brand, Einbruch und Überfall definiert [VDE 0833]. Gefahren- und Einbruchmeldeanlagen nach heutigem Stand der Technik müssen die oben genannten Normen einhalten.

2.3.1.1 Gefahrenmeldeanlagen

Eine Gefahrenmeldeanlage überwacht automatisch Gegenstände auf Diebstahl oder Flächen und Räume auf unbefugtes Eindringen. Eine solche Anlage hat zudem die Aufgabe über Sensoren, Störungen und Gefahren auszuwerten, zu signalisieren und weiterzuleiten. Die Sensoren sind entweder ständig aktiv oder werden über eine Scharfschalteeinrichtung ein- und ausgeschaltet. Zugängliche Türen und Deckel der Anlage müssen im scharfgeschalteten Zustand der Anlage auf Öffnen (Sabotage) überwacht werden. Je nach VdS-Richtlinien (Verband der Schadenversicherer) ist das auch während des unscharfen Zustands der Anlage nötig. VdS zertifizierte Meldeanlagen, Sensoren und Aktoren werden in Sicherheitsklassen eingestuft, anhand denen Versicherungsunternehmen deren Beiträge bemessen. Abbildung 2.6 zeigt den technischen Aufbau von Gefahrenmeldeanlagen. Dazu gehören Brandmeldezentralen (BMZ), Einbruchmeldezentralen (EMZ) sowie in den meisten Fällen manuell auslösbare Überfallmeldezentralen (ÜMZ).

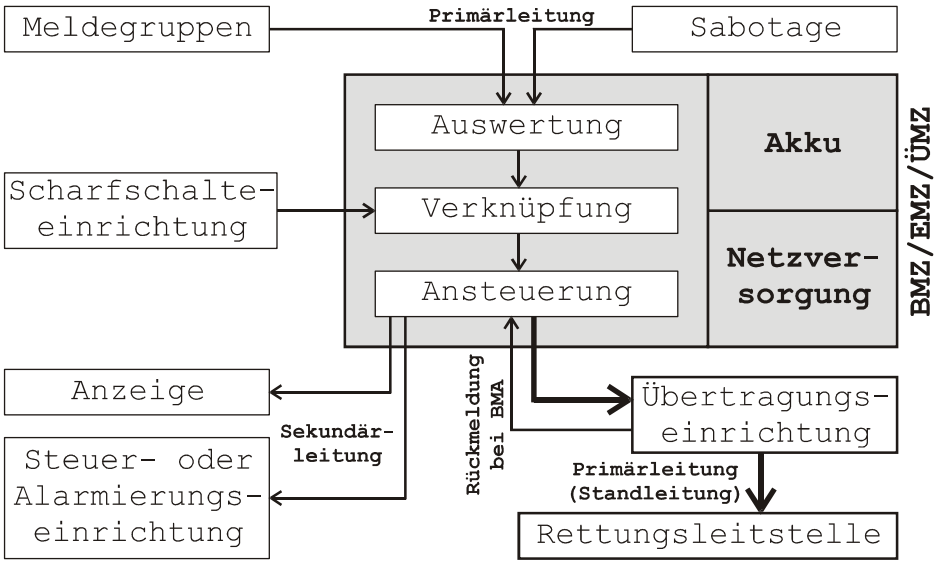

Abbildung 2.6: Aufbau von Gefahrenmeldeanlagen nach DIN VDE 0833

Die einzelnen Meldesysteme unterscheiden sich hauptsächlich durch die daran angeschlossenen Sensoren, welche sich in fünf Gruppen einteilen lassen:

- **Außenhautüberwachung** Magnetkontakte, Reedkontakte, Lichtschranken
  Glasbruchsensoren (piezoelektrisch, akustisch)
- **Außenraumüberwachung** Bewegungsmelder (pyroelektrisch, infrarot)
  Videosensorik (optisch)
- **Verschlussüberwachung** Riegelschaltkontakte
  Fensterverschlusskontakte
- **Innenraumüberwachung** Notrufdrücker, Geldscheinkontakt
  Bewegungsmelder (pyroelektrisch, infrarot)
  Videosensorik (optisch)
- **Technische Melder** Rauchmelder (optisch, chemisch)
  Gasmelder (optisch, chemisch)
  Wassermelder

Um sowohl Alarme als auch Sabotagen detektieren zu können, wird ein geschlossener Stromkreis mit einer maximalen Anzahl von Sensoren über eine primäre Meldeleitung gebildet. Das Kurzschließen oder Öffnen des Stromkreises, innerhalb eines durch einen Schmitt-Trigger definierten Widerstandsbereiches, löst unmittelbar eine Signalisierung an der Auswerteschaltung der Gefahrenmeldeanlage aus.

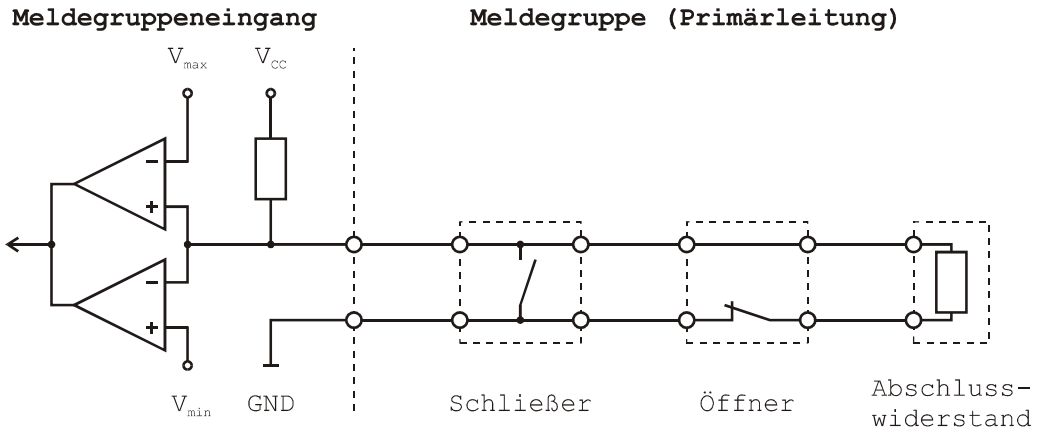

Abbildung 2.7: Prinzip einer Meldeleitung nach ABB STOTZ-KONTAKT GmbH

Abbildung 2.7 zeigt das Schaltungsprinzip einer solchen primären Meldeleitung, wie sie in modernen Anlagen eingesetzt werden. Es können sowohl passive als auch aktive Melder angeschlossen werden, solange der Stromverbrauch einen durch die Schaltung vorgegebenen Wert nicht überschreitet. Davon hängt auch die maximale Anzahl pro Gruppe anschließbarer Melder ab.

2.3.1.2 Meldeanlagen der Gebäudesystemtechnik

Um den für diese Arbeit relevanten Stand der Technik zu zeigen, werden im folgenden die wichtigsten Meldeanlagen betrachtet, die den Europäischen Installationsbus in der Form integrieren, dass darüber Meldesensoren angeschlossen sind. Einbruch- und Gefahrenmeldeanlagen, die den EIB/KNX lediglich zum Steuern von Beleuchtungen und anderen Aktoren verwenden, werden hier nicht betrachtet.

Bereits in den ersten installierten EIB-Anlagen wurden „alarmnahe“ Anwendungen realisiert, die dem Bewohner zusätzliche Sicherheit boten. Dies sind vor allem die Anwesenheitssimulation mittels Beleuchtungssteuerung aber auch der Einsatz von Bewegungs- und Präsenzmeldern am Bussystem.

Die Firma ABB STOTZ-KONTAKT GmbH vertreibt unter der Bezeichnung L208 eine, je nach Erweiterungsgrad, bis zur VdS-Klasse C zugelassene Alarmzentrale mit EIB/KNX-Anbindung. Primär dient die Anlage für den EIB/KNX zur Ansteuerung der Beleuchtung und zusätzlicher Melder im Gefahrenfall, sowie zur Anwesenheitssimulation. Die Scharfschaltung der Anlage kann ebenfalls über den EIB/KNX veranlasst werden. Die Anlage selbst verfügt über 9 Meldegruppeneingänge, wovon 8 über den EIB erweitert werden können. Die Kommunikation zwischen der Meldezentrale und den weiteren Meldegruppen basiert auf der grundsätzlich für die EIB-Technik definierten Übertragung von sogenannten Kommunikationsobjekten. Diese Objekte stellen im Netzwerk Zustände mit einer Größe von einem Bit bis zu 14 Byte dar, die innerhalb der Anwendungsebene 7 des ISO/OSI Modells in allen Teilnehmern synchronisiert werden. In diesem Fall ist das System, auf Grund der nicht garantierbaren Integrität und Authentizität von EIB/KNX Telegrammen, nicht mehr nach den VdS-Richtlinien klassifizierbar. EIB/KNX Geräte wie Bewegungs- und Präsenzmelder, oder einfache Taster können zur Alarmierung verwendet werden.

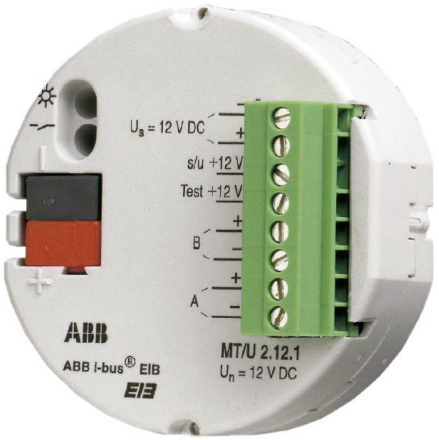

Abbildung 2.8: Zone Terminal MT/U 2.12.1, Quelle: ABB STOTZ-KONTAKT GmbH

Spezielle ABB i-bus Koppler vom Typ M/TU 2.12.1 (siehe Abbildung 2.8) ermöglichen den direkten Anschluss von jeweils zwei Meldegruppen an den EIB/KNX. Eine

Signalisierung erfolgt hierbei über Standard Kommunikationsobjekte, so dass diese auch unabhängig von einer L208 Meldezentrale verwendet werden können. Das Entfernen von Meldelinien-Kopplern wird durch zyklische Überwachung der Objekte umgesetzt. Eine rudimentäre Gefahrenmeldeanlage kann somit in einer EIB/KNX Installation realisiert werden, jedoch ohne Anspruch auf eine Klassifizierung.

Ein ähnliches System der Firma Merten mit der Produktlinienbezeichnung ARGUS *CONTROL* stützt sich vollständig auf den EIB/KNX als Kommunikationsmedium zwischen Sensoren und Aktoren. Die Übertragung basiert auf Standard-Telegrammen, welche Kommunikationsobjekte transportieren. Über Buskoppler mit binären Eingängen werden Glasbruchmelder und Reedkontakte, in Form von Schließern, an den EIB/KNX angebunden. Eine Anzeigeinheit dient zur Visualisierung der maximal 12 Meldelinien. Das zyklische Abfragen der Meldekoppler erlaubt das Erkennen von Leitungsunterbrechungen am Bussystem. Eine spezielle Spannungsversorgung für das Bussystem kann zur Überbrückung von Stromausfällen mit einem Akkumulator erweitert werden. Teil des Systems sind auch EIB/KNX Bewegungsmelder sowie Schlüsselschalter zur Scharfschaltung des Systems. Sirenen, Blitzgeräte und automatische Sprachausgaben werden über EIB/KNX Schaltaktoren gesteuert. Sabotagelinien an den Bedien- und Anzeigeelementen lösen bei Manipulation Alarm aus. Das Gesamtsystem unterliegt keiner Zertifizierung.

2.3.2 Verfahren zur Datenverschlüsselung

Einen sehr wichtigen Aspekt bei der digitalen Übertragung von Daten stellt die Sicherheit des Übertragungskanals dar. In großen Netzwerken wie beispielsweise dem Internet, wo sämtliche Daten über unzählige Router und Server verschickt werden, ist es mit vertretbarem Aufwand kaum möglich, das Abhören oder Verändern der Daten mit Sicherheit zu vermeiden. Dies gilt auch für die vergleichsweise kleinen Netzwerke automatisierter Gebäude. Übertragungsmedien wie Powerline oder Funk machen es Angreifern besonders einfach, an die übertragenen Daten zu gelangen. Dies ist bisher auch der Grund dafür, dass Zugangskontrollsysteme und Alarmanlagen keinen Gebrauch von Gebäudebussystemen für die Übertragung sensibler Daten machen. Die wenigen Systeme, die diesen Aspekt außer Betracht lassen, können nicht zertifiziert werden und bestehen daher kaum am Markt.

Seit der maschinellen Datenübertragung bemühen sich Wissenschaftler darum, die übertragenen Nachrichten so zu verändern, dass sie nur vom entsprechenden Empfänger gelesen werden können. Dieses Forschungsgebiet wird als Kryptographie bezeichnet und beschäftigt sich mit folgenden Basisdiensten (siehe [Schneier 1996], [Spitz 2002]):

- **Authentizität** Die Herkunft einer Nachricht muss nachvollziehbar sein, so dass ein fremder Datensatz erkannt wird.

- **Integrität** Der Empfänger soll erkennen, ob eine Nachricht bei der Übertragung verändert wurde.
- **Verbindlichkeit** Der Urheber einer Nachricht muss eindeutig sein, so dass dieser nicht leugnen kann, die Daten gesendet zu haben.
- **Vertraulichkeit** Eine abgehörte Nachricht darf für den Angreifer nicht lesbar sein, das Abhören wird somit verhindert.

Die Grundlage zur Realisierung der Basisdienste stellen Verschlüsselungsverfahren dar. Diese lassen sich abstrakt mittels folgender Algorithmen beschreiben [Wohlm 2001]:

- **Generate** Algorithmus zur Erzeugung geeigneter Schlüssel
- **Encrypt** Algorithmus zur Berechnung eines Chiffretextes *c* aus einem Klartext *m* mit Hilfe des Schlüssels K_1
- **Decrypt** Algorithmus zur Entschlüsselung des Klartextes *m* aus dem Chiffretext *c* mit Hilfe des Schlüssels K_2

Abbildung 2.9 zeigt den prinzipiellen Ablauf einer verschlüsselten Datenübertragung.

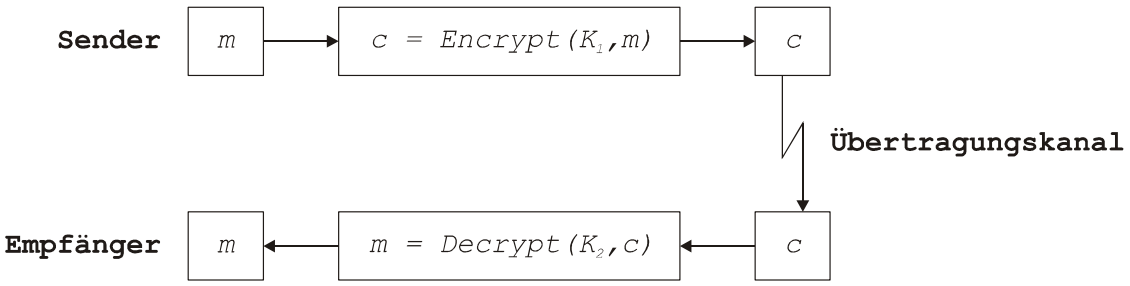

Abbildung 2.9: Darstellung des Verschlüsselungsprinzips

Die Algorithmen besitzen die Eigenschaft, dass zu jedem Schlüssel K_1 ein eindeutiger Schlüssel K_2 existiert, derart, dass der Ver- und Entschlüsselungsalgorithmus invers zueinander sind. Bei asymmetrischen Verfahren sind die Schlüssel K_1 und K_2 unterschiedlich. Bei symmetrischen Verfahren, wie sie im Rahmen dieser Arbeit verwendet werden, wird ein geheimer Schlüssel $K = K_1 = K_2$ verwendet.

2.3.2.1 Symmetrische Verschlüsselung

Symmetrischen Verfahren zeichnen sich im Idealfall durch geringen Speicherverbrauch und eine schnelle Abarbeitung aus. Man spricht auch von Blockchiffrierungen, da in der Regel immer ganze Datenblöcke mit einem Blockschlüssel auf einmal ver- bzw.

entschlüsselt werden. Die Datenblock- und Schlüsselgrößen liegen, je nach Verfahren, im Bereich zwischen 40 und 512 Bit. Die Stärke der Verfahren basiert auf der Diffusion eines verschlüsselten Datenblocks, das heißt, dass sich der Chiffre vollständig ändert, wenn auch nur ein Zeichen im Klartext verändert wird. Dies könnte mit einer gut gewählten Ersetzungstabelle realisiert werde, welche zugleich den geheimen Schlüssel darstellt. Dies scheitert aber an der immensen Größe der Tabelle, so dass diese durch eine Rechenvorschrift realisiert werden muss, welchen den Schlüssel als Parameter hat. Wissenschaftler haben in den letzten Jahren eine große Reihe solcher Algorithmen entwickelt, welche häufig auf Feistel-Netzwerken basieren, siehe Abbildung 2.11. In einem solchen Netzwerk wird der zu verschlüsselnde Datenblock in zwei Hälften geteilt, wobei ein Teil mit dem Schlüssel verarbeitet wird und zur Konfusion mit der anderen Hälfte XOR verknüpft wird. Nach dem Tausch der beiden Teile wird das Netzwerk erneut in mehreren Runden durchlaufen. Im Idealfall lässt sich aus dem Chiffre kein Rückschluss auf den geheimen Schlüssel machen, selbst wenn der Klartext bekannt ist. Hier würde nur ein Brute-Force Angriff, das Durchprobieren aller möglichen Schlüssel, zum Ziel führen, so dass die Sicherheit des Verfahrens direkt proportional zur Schlüssellänge ist. Gute Algorithmen sind offengelegt, so dass Kryptoanalytiker diese auf Schwachstellen untersuchen können. Vier der bekanntesten Algorithmen seien hier kurz genannt:

- **DES** — Der Data Encryption Standard wurde von der Firma IBM und der NSA (National Security Agency) entwickelt und 1976 zum Standard anerkannt [Schneier 1996]. DES wurde in verschiedenen Varianten weiterentwickelt und findet bis heute Anwendung bei einer Blocklänge von 64 Bit und einer Schlüssellänge von 56 Bit.
- **IDEA** — Der International Data Encryption Algorithm wurde 1990 an der Eidgenössischen Technischen Hochschule in Zürich entwickelt mit dem Ziel, Schwachstellen von DES zu vermeiden [Selke 2000]. Bei einer Blocklänge von 64 Bit und einer Schlüssellänge von 128 Bit findet das Verfahren viele Anwendungen, unter anderem bei der Verschlüsselung von E-Mails.
- **Blowfish** — Das Verfahren wurde im Jahre 1993 von dem bekannten Kryptospezialisten Bruce Schneier entwickelt und ist nicht patentrechtlich geschützt, so dass es frei verwendet werden kann. Hierbei handelt es sich um ein Verfahren mit einer Blocklänge von 64 Bit und einer variablen Schlüssellänge von bis zu 448 Bit [Schneier 1996]. Der Algorithmus ist unter 2.3.3 beschrieben.

- **AES** Der Advanced Encryption Standard, der von den beiden Forschern Joan Daemen und Vincent Rijmen entwickelt wurde [Daemen 2002], ging im Jahre 2000 aus einem mehrjährigen Auswahlverfahren als Sieger hervor. Bei einer Blocklänge von 128 Bit und Schlüssellängen von 128, 192 und 256 Bit tritt er die Nachfolge des DES an. Der Algorithmus ist im Kapitel zur gesicherten Datenübertragung beschrieben.

2.3.2.2 Asymmetrische Verschlüsselung

Asymmetrische Verfahren werden oft als Public-Key-Verfahren bezeichnet, da ein Schlüssel frei zugänglich gemacht wird, wobei der andere Schlüssel geheim gehalten wird. Die Grundlagen für asymmetrische Verfahren wurden bereits 1976 von Whitfield Diffie und Martin Hellmann [DiffieHell 1976] vorgestellt. Sie beruhen darauf, dass die Umkehrfunktion zum Exponenten modulo einer Primzahl nur sehr schwer zu berechnen ist. Die bekanntesten Vertreter sind sicherlich das RSA-Verfahren (Rivest Shamir Adleman) und der ElGamal Algorithmus, bei denen üblicherweise Schlüssellängen von 768 bis 2048 Bit eingesetzt werden. Das 1985 von Taher ElGamal erfundene, gleichnamige Verschlüsselungsverfahren [ElGamal 1985] beruht auf der Schwierigkeit, diskrete Logarithmen über einem endlichen Körper zu berechnen, entsprechend der Diffie-Hellmann-Theorie. Der Algorithmus ist selbst nicht patentrechtlich geschützt, wurde aber bis 1997 durch ein Diffie-Hellman Patent abgedeckt und ist somit heute frei verwendbar [Schneier 1996]. Das Verhältnis von geheimen Schlüssel x zum öffentlichen Schlüssel y sowie den zugehörigen Parametern g und p lautet wie folgt:

$$y = g^x \bmod p \tag{2.1}$$

Dabei wird für p eine möglichst große Primzahl gewählt. x und g müssen natürliche Zahlen zwischen 1 und p-1 sein. Bei kleinen Zahlen lassen sich die Logarithmen durch Probieren ermitteln; für große Moduln von etwa 150 Stellen ist das im Allgemeinen mit einem technisch vertretbaren Aufwand zum heutigen Zeitpunkt nicht mehr möglich.

Zur Verschlüsselung einer Nachricht m wählt der Absender eine beliebige Zahl k, welche zwischen 1 und p-1 liegen muss, und somit zu p relativ prim ist. Er berechnet die zu übertragenden Daten a und b nach folgenden Vorschriften:

$$a = g^k \bmod p \tag{2.2}$$

$$b = y^k m \bmod p \tag{2.3}$$

Der Empfänger kann die Nachricht *m* mittels des geheimen Schlüssels *x* aus *a* und *b* wie folgt zurückgewinnen:

$$m = \frac{b}{a^x} \bmod p \tag{2.4}$$

Zu beachten ist, dass stets alle Rechenoperationen modulo *p* berechnet werden, wobei gilt:

$$a^x \equiv g^{xk} (\bmod p) \tag{2.5}$$

$$\frac{b}{a^x} \equiv \frac{y^k m}{a^x} \equiv \frac{g^{xk} m}{g^{xk}} \equiv m (\bmod p) \tag{2.6}$$

Durch diese Konstruktion ist sichergestellt, dass die Gleichung eindeutig lösbar ist. Der mathematische Hintergrund ist in [Schneier 1996] detailliert beschrieben.

RSA wurde in den Jahren 1977 und 1978 von den drei Kryptographen Ron Rivest, Adi Shamir und Leonard Adleman [RSA 1978] entwickelt. Es beruht auf zahlentheoretischen Eigenschaften, die das Rechnen in Restklassen aufweisen. Es war das erste Public-Key-Verfahren, das sich im praktischen Einsatz bewährt hat.

Auf Grund der mathematischen Anforderungen an ein Rechnersystem sind die asymmetrischen Algorithmen deutlich langsamer als die Blockverfahren, weshalb diese häufig miteinander kombiniert werden. Solche Hybridverfahren dienen dazu, auf sicherem Weg den geheimen Schlüssel für die eigentliche, symmetrische Datenübertragung auszuhandeln, oder kombiniert mit Hash-Funktionen Daten zu signieren.

Der ElGamal Algorithmus eignet sich, genau so wie RSA, für solche digitale Signaturen. Hierbei wird mittels einer Hash-Funktion, wie sie beispielsweise unter den Begriffen MD4, MD5, SHA oder RIPE-MD (MD steht für Message Digest, SHA für Secure-Hash-Algorithm) bekannt sind, eine Art Prüfsumme erzeugt [Ertel 2001]. Dieser Hash-Wert oder sogar die ganzen zu signierenden Daten werden mit dem geheimen Schlüssel chiffriert, so dass der Empfänger die Authentizität der Daten mit dem öffentlichen Schlüssel überprüfen kann. Für diesen speziellen Zweck wurde 1991 der Digital Signature Algorithm (DSA), der heute noch zum Signieren von E-Mails per PGP (Pretty Good Privacy) verwendet wird, durch die NSA entwickelt [DSS 1994].

2.3.3 Datenverschlüsselung im Gebäudebussystem

Das Fraunhofer Institut für Mikroelektronische Schaltungen und Systeme (Fraunhofer-IMS) hat in Zusammenarbeit mit der IPAS GmbH in Duisburg eine Technik zur sicheren Datenübertragung über den EIB entwickelt [GHKB 2003]. Basierend auf der

Übertragung von Standard-Kommunikationsobjekten nutzt das entwickelte Verfahren als Container für die verschlüsselten Daten den 14 Byte EIB Standarddatentyp EIS-15 (EIB Interworking Standard), der zur Übertragung eines 14 Byte Textstrings definiert ist [IPAS 2002]. Abbildung 2.10 zeigt die Zusammensetzung der 14 Byte Telegrammdaten. Von den 14 zur Verfügung stehenden Bytes werden lediglich 8 Bytes verwendet, die restlichen 6 Bytes sind Füllbytes und transportieren, im Gegensatz zu der in dieser Arbeit vorgestellten Methode, keinerlei Information.

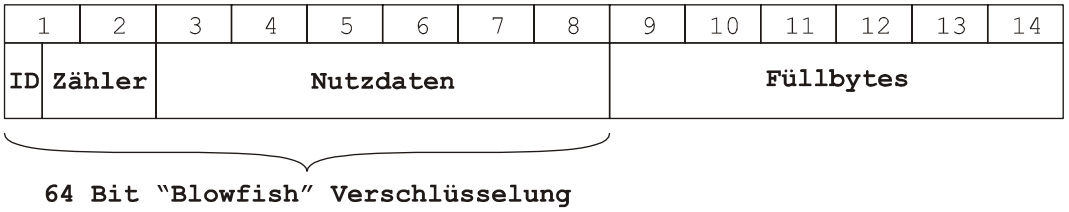

Abbildung 2.10: Aufbau des Datencontainers nach Fraunhofer-IMS und IPAS

Die 8 Byte Daten, die die eigentliche Information beinhalten, werden nach dem Blowfish-Verfahren verschlüsselt. Blowfish besteht wie viele andere Blockverfahren aus einem sogenannten Feistel-Netzwerk und ist für Anwendungen auf 32-Bit-Mikroprozessoren optimiert, bei denen die Schlüssel nicht sehr häufig gewechselt werden. Der Algorithmus benötigt weniger als 5 kByte Programmspeicher und besteht aus zwei Teilen, der Schlüsselexpansion und der Datenverschlüsselung. Bei der Schlüsselexpansion wird der geheime Schlüssel in verschiedene Teilschlüssel zu insgesamt 4168 Bit umgewandelt. Die Verschlüsselung selbst besteht aus einer einfachen Funktion, die 16 mal durchlaufen wird. Jede Runde besteht aus einer schlüsselabhängigen Permutation sowie einer schlüssel- und datenabhängigen Substitution. Alle Operationen sind Additionen und XOR-Verknüpfungen von 32-Bit-Worten. Pro Runde sind 4 Tabellenindizierungen notwendig. Abbildung 2.11 zeigt die vereinfachte Darstellung des Blowfish-Verfahrens.

Die Entschlüsselung verläuft genau wie die Verschlüsselung, nur werden die Teilschlüssel P1, P2 ... P18 in umgekehrter Reihenfolge benutzt. Innerhalb der 8 Byte Telegrammdaten, die verschlüsselt übertragen werden, entscheidet eine 4 Bit Service-ID im Empfänger, wie die 6 Byte Nutzdaten weiter verarbeitet werden. Dies kann zum Beispiel ein Poll-Request für einen neuen Schlüssel, die Bestätigung für den korrekten Empfang eines solchen Schlüssels oder die Übermittlung sensibler Daten sein. Ein 12 Bit Zähler innerhalb der verschlüsselten Sequenz verhindert das Wiedereinspielen von Telegrammen, die bereits gesendet wurden. Der Zähler wird mit jedem Telegramm um eins erhöht, so dass nur Busteilnehmer mit Kenntnis über den geheimen Schlüssel, neue, gültige Telegramme erzeugen können.

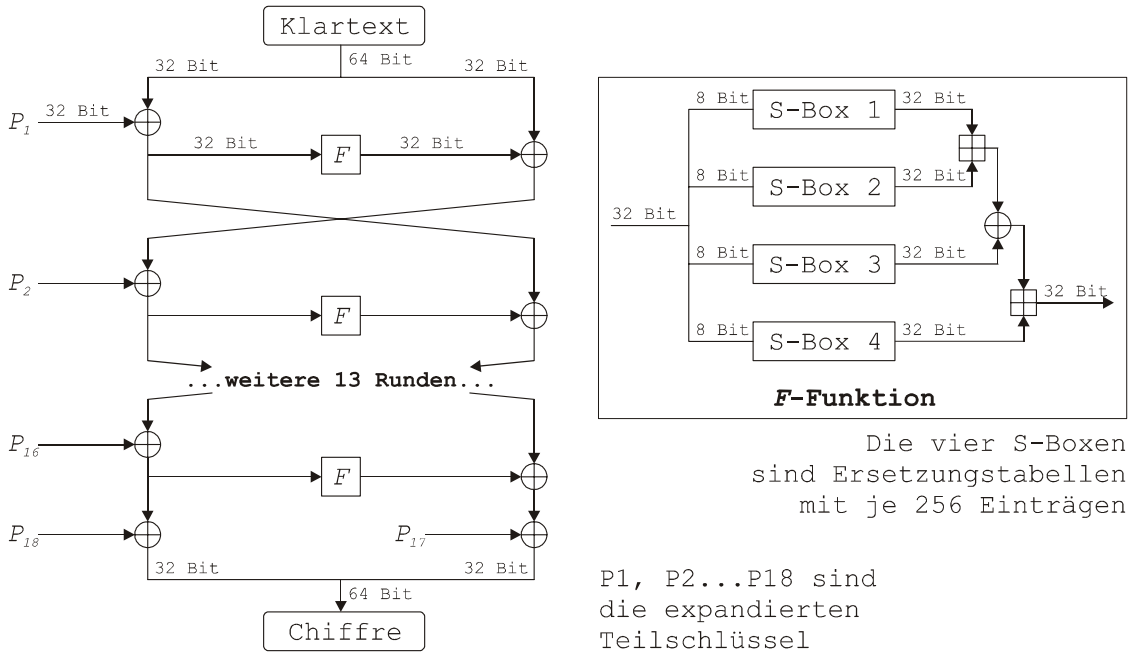

Abbildung 2.11: Darstellung des Feistel-Netzwerks des Blowfish-Verfahrens

Um den geheimen Schlüssel innerhalb des EIB-Netzwerkes für alle gesicherten Busteilnehmer bei Bedarf austauschen zu können, verwaltet jeder Teilnehmer neben dem Kommunikationsobjekt, welches zur verschlüsselten Kommunikation verwendet wird, zusätzlich ein zweites Kommunikationsobjekt. Diesem Objekt ist ein eigener, bei der Installation festgelegter, geheimer Schlüssel zugeordnet. Über dieses Objekt kann ein sogenannter Key-Master, ein entsprechender Busteilnehmer oder ein angeschlossener PC, neue Schlüssel vergeben oder auf Anfrage den momentan verwendeten Schlüssel übermitteln.

In einer ersten Anwendung wurde ein per EIB vernetztes Zeiterfassungssystem realisiert [Russak 2002]. Ein Transponderlesesystem überträgt hierbei die Userdaten einer Transponderkarte per EIB an ein EIB/Ethernet Gateway (IPAS EIB/IP ComBridge), welches die Daten an einen PC mit einer Zugangskontrollsoftware leitet. Weitere Sensoren und Aktoren sind in Vorbereitung.

Ein weiterer Ansatz, Daten verschlüsselt über den Europäischen Installationsbus zu übertragen, sollte von der Firma eDevelopment in Russland kommen. Die Firma musste aber die Forschungen auf diesem Gebiet aufgeben, so dass keine weiteren Informationen zur Verfügung stehen.

2.3.4 Mechanische Sicherheit

Neben den elektronischen Systemen zur Sicherstellung der Authentizität desjenigen, der sich Zutritt verschaffen will, sowie den Systemen zur Erkennung von Eindringungs- und Manipulationsversuchen, stellen die mechanischen Elemente eines abzusichernden

Bereichs einen wesentlichen Teil eines Gesamtsystems dar. Da die vorliegenden Arbeit ausschließlich einen elektro- und informationstechnischen Entwurf von Zugangs- und Sicherheitsmechanismen beschreibt, sei hier kurz der Stand der Technik im privaten Wohnungsbau anhand von einbruchshemmenden Wohnungseingangstüren und Fenstern dargestellt.

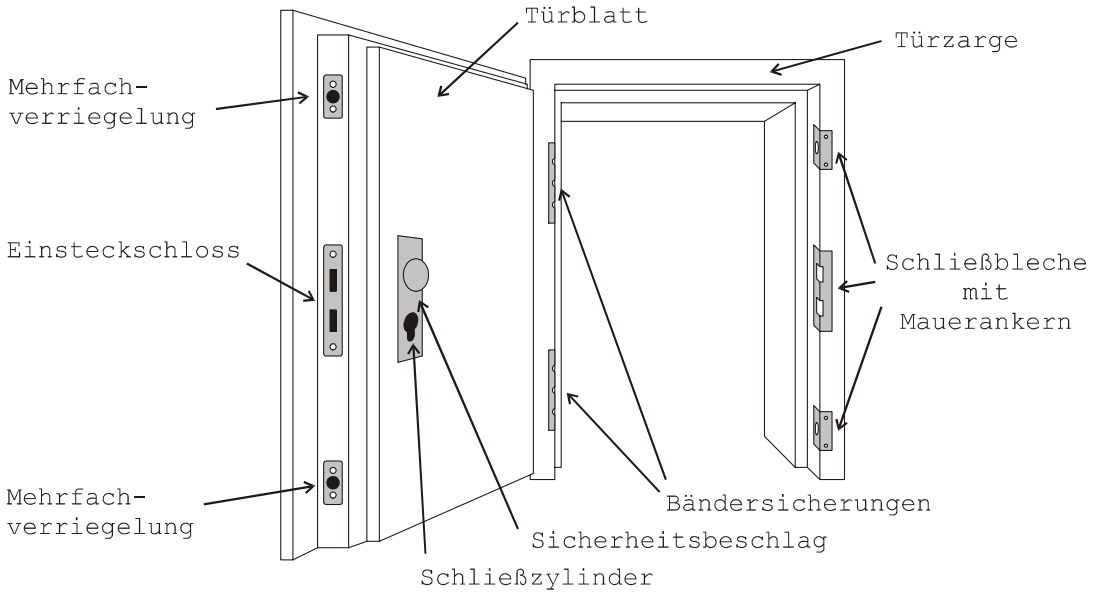

Abbildung 2.12: Aufbau einer Tür

Eine entsprechend fachgerechte Montage vorausgesetzt, werden einbruchshemmende Türen nach der Norm DIN V ENV 1627 in sechs Widerstandsklassen unterteilt. Tabelle 2.2 zeigt die Klassifizierung, welche auf Grund von Untersuchungen der Vorgehensweise verschiedener Tätergruppen erstellt wurde.

Für private Wohngebäude reichen in der Regel einbruchshemmende Türen der Klassen 1 bis 3, wohingegen bei Gewerbeobjekten und öffentlichen Gebäuden die Klassen 4 bis 6 Verwendung finden. Eine Werksbescheinigung des Herstellers sowie ein Kennzeichnungsschild im Türfalz sind der Nachweis dafür, dass die Tür dem Werksmuster entspricht, welches in einem zugelassen Prüfinstitut auf die angestrebte Widerstandsklasse hin untersucht wurde.

Der Verriegelungsmechanismus, der die Tür im geschlossen Zustand hält, wird heute in der Regel durch ein sogenanntes Sicherheitseinsteckschloss realisiert. Die Anforderungen an die Festigkeit des Schlosses, speziell des Schließriegels und des Schlosskastens werden gemäß der Norm DIN 18251 klassifiziert. Bei elektrischen Motorblockschlössern, wie es auch im Rahmen dieser Arbeit bei der Realisierung eingesetzt wird, gehören selbstverriegelnde Panikschlösser zum aktuellen Stand der Technik. Eine Steuerfalle bringt hierbei das Schloss automatisch in den verriegelten Zustand, sobald die Tür geschlossen wird. Das Öffnen geschieht entweder über den integrierten Motor oder alternativ über den Schließzylinder. Mittels weiterer Zusatzschlösser im Türblatt,

welche meist mit Schwenk- und Hakenschwenkriegeln ausgestattet sind, kann eine Mehrfachverriegelung realisiert werden.

Tabelle 2.2: Widerstandsklassen nach DIN V ENV 1627

Klasse	Tätertyp und Vorgehensweise
1	Bauteile der Widerstandsklasse 1 weisen Grundschutz gegen Aufbruchversuche mit körperlicher Gewalt wie Gegentreten, Gegenspringen, Schulterwurf, Hochschieben oder Herausreißen auf.
2	Der Gelegenheitstäter versucht zusätzlich mit einfachen Werkzeugen, wie Schraubendreher oder Zange und Keil, das verschlossene und verriegelte Bauteil aufzubrechen.
3	Der Täter versucht zusätzlich mit schwerem Hebelwerkzeug das verschlossene und verriegelte Bauteil aufzubrechen.
4	Der erfahrene Täter setzt zusätzlich Schlagwerkzeuge sowie Bohrwerkzeuge ein.
5	Der erfahrene Täter setzt zusätzlich Elektrowerkzeuge, wie zum Beispiel Bohrmaschine, Stich- oder Säbelsäge und Winkelschleifer mit einem maximalen Scheibendurchmesser von 125 mm ein.
6	Der erfahrene Täter setzt zusätzlich leistungsfähige Elektrowerkzeuge, wie zum Beispiel Winkelschleifer mit einem maximalen Scheiben-durchmesser von 230 mm ein.

Der Schließzylinder und der Schutzbeschlag, welcher ein Abziehen oder Abbrechen nach DIN 18257 verhindern soll, bilden einen weitern Schwachpunkt, der besonders geschützt wird. Abgesehen von elektronischen Schließzylindern und kompletten Schlössern, wie sie oben beschrieben werden, kann von mechanischen Schließzylindern gemäß DIN 18252/18254 eine erhöhte Nachschließsicherheit und ein verstärkter Bohrschutz mittels Kernpanzerung erwartet werden. Das Kopieren von mechanischen Schlüsseln für derzeitig moderne Zylinder wird durch unterschiedlichste Schlüsselkanalprofile, Kalottenprofile und Schließprofile in drei Dimensionen erschwert. Eine zusätzliche Kipphebelabtastung wie sie zum Beispiel bei der Firma Winkhaus in Schließzylindern integriert wird, verhindert zusätzlich das Drehen der Mechanik mittels nicht passender Schlüssel oder anderem Werkzeug. Abbildung 2.13 zeigt die schematische Darstellung eines mechanischen Profilschließzylinders nach dem heutigen Stand der Technik.

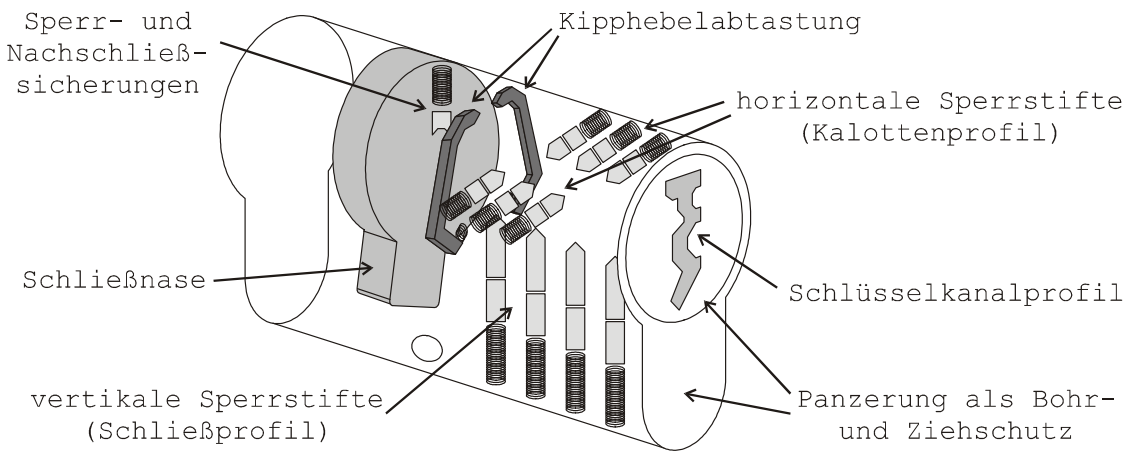

Abbildung 2.13: Vereinfachte Darstellung eines modernen Schließzylinders

Nach dem selben System wie bei Türen werden auch Fenster und Fenstertüren nach der Norm DIN V ENV 1627 in Widerstandsklassen unterteilt [SiWo 2002]. Einbruchhemmende Beschlagsteile mit umlaufender Verriegelung, sogenannte Pilzkopfzapfen und spezielle Schließteile im Rahmen, sowie ein abschließbarer Griff gemäß DIN 18104 werten ein Fenster zum Sicherheitsfenster der Widerstandsklasse 1 nach Norm auf. Technologisch hochstehendes Verbundsicherheitsglas (VSG) – Glasscheiben, die durch eine extrem reißfeste Zwischenschicht nach DIN EN 356 fest miteinander verbunden sind – gekoppelt mit einbruchhemmenden Beschlagsteilen und abschließbarem Griff zeichnen das Sicherheitsfenster der Widerstandsklasse 2 nach Norm aus. Zusätzliche Fenstergitter oder einbruchshemmende Rollläden und Rollgitter mit automatischer Verriegelung sind ebenfalls für alle Widerstandsklassen verfügbar.

3 Analyse der Systemanforderungen

Um ein Struktur ausarbeiten zu können, die es erlaubt, unterschiedliche Mechanismen der Zugangskontrolltechnik im Bereich der Gebäudeautomatisierung einzusetzen, ist es notwendig, die daran gestellten Anforderungen zu analysieren. Das bereits vorgestellte Spektrum diverser Mechanismen zur Authentisierung von Personen gegenüber automatischen Systemen erfordert die Reduktion auf eine sinnvolle Auswahl. Ebenso müssen alle Stellen gefunden werden, an denen adäquate Sicherheitsmechanismen einzusetzen sind. Abgestimmt auf die Zielgruppe der Anwender soll im Rahmen dieser Arbeit ein Optimum an Sicherheit und Komfort erreicht werden.

3.1 Zweigeteilter Ansatz

Betrachtet man einerseits die Anwendungsmöglichkeiten von Zugangsmechanismen im allgemeinen und andererseits die durch ein automatisiertes Gebäude gegebenen Technologien, ergeben sich zwei Ansatzpunkte für weitere Überlegungen. Abbildung 3.1 zeigt, wo sich die Basistechnologien mit den Ansatzpunkten überschneiden.

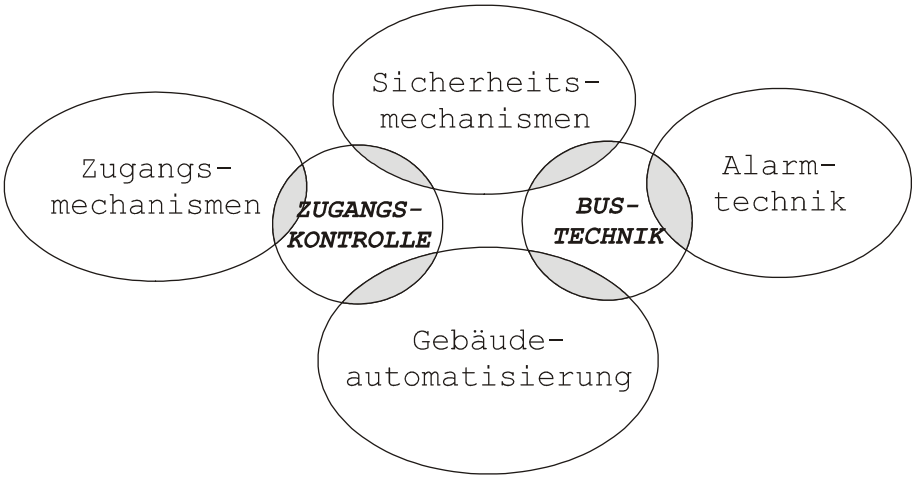

Abbildung 3.1: Zweigeteilter Ansatz zur Erstellung eines Konzeptes

Es ist zu erkennen, dass sowohl im Bereich der Zugangskontrolle als auch bei der eingesetzten Bustechnik innerhalb des automatisierten Gebäudes Forschungsbedarf hinsichtlich angewandter Sicherheitsmechanismen besteht. Da als Zielgruppe insbesondere auch Privatanwender betrachtet werden müssen, steht neben dem Komfort der zusätzliche Gewinn durch erweiterte Anwendungen mit im Vordergrund. Es ist möglich, die Systeme durch Dienstmerkmale zu beschreiben, welche im Folgenden, aufgeteilt nach Zugangskontrolle, Bustechnik und erweiterte Anwendungen gezeigt werden.

3.2 Dienstmerkmale der Zugangskontrolle

Ziel eines Zugangskontrollsystems ist es, bestimmten Personen den Zugang zu gesicherten Bereichen zu gewähren, nachdem diese mit höchstmöglicher Zuverlässigkeit identifiziert wurden. In erster Linie dienen hierzu unterschiedliche Zugangsmechanismen, welche je nach Typ, mehr oder weniger sicher gegen Manipulationen sind. Zum anderen spielt auch der Komfort, gerade im privaten Bereich eine große Rolle, so dass hier ein entsprechendes Interface zur Konfiguration und Verwaltung gefunden werden muss.

3.2.1 Zugangsmechanismen

Die in Kapitel 2 getroffene Unterscheidung zwischen wissensbasierten, besitzbasierten und biometrischen Authentisierungsmechanismen deckt das Spektrum aller derzeit bekannten Systeme ab. Die für den Benutzer wohl unbequemste Variante basiert auf wissensbasierten Mechanismen, also beispielsweise auf Zahlencodeschlössern, da der Code vergessen werden kann. Besitzbasierte Systeme wie Transponder oder Smart Cards bieten eine sehr hohe Sicherheit, können aber auch verloren, oder von fremden Personen benutzt werden. Biometrische Mechanismen hingegen sollen den Missbrauch durch andere Personen verhindern, stellen aber einen hohen technischen Aufwand dar.

Tabelle 3.1: Bewertung von Authentisierungsmechanismen

Mechanismus	**Komfort**	**Sicherheit**	**Aufwand**
wissensbasiert	sehr gering	hoch	sehr einfach
besitzbasiert	gering	sehr hoch	neutral
biometrisch	sehr hoch	hoch	sehr hoch

Tabelle 3.1 zeigt eine einfache Bewertung der drei Formen von Mechanismen zur Authentisierung, aufgeteilt nach Komfort, Sicherheit und technischen Aufwand. Die Bewertung zeigt die während dieser Arbeit gewonnenen Erfahrungen mit den einzelnen Systemen. Da gerade der technische Aufwand je nach System sehr unterschiedlich ist und der damit verbundene Kostenfaktor eine große Rolle spielt, sollte eine Auswahl der Authentisierungsmechanismen möglichst bedarfsgerecht erfolgen. Dies kann durch eine einheitliche Schnittstelle erreicht werden. Die horizontale Integration wird dabei durch definierte Hard- und Softwareschnittstellen realisiert. Grundvoraussetzung dafür ist ein dezentrales System, bei dem jeder Mechanismus zur Authentisierung eine eigene Verarbeitungseinheit integriert hat. Die Entscheidung, ob der identifizierten Person Zutritt gewährt wird, sowie die Steuerung entsprechender Aktoren übernimmt ein spezieller Teilnehmer im Systemverbund.

3.2.2 Sicherheit

Nicht jeder Mechanismus bietet dieselbe Sicherheit gegen Manipulationen oder gegen eine falsche Identifikation, so dass durch die Kombination mehrerer Systeme eine Steigerung der Sicherheit erwartet werden kann. Um dies nachweisen zu können muss für alle Mechanismen ein einheitliches Maß für die Qualität der Authentisierungsergebnisse gefunden werden, welches sich als Angabe für die Sicherheit eignet. In der Regel werden durch Hersteller solcher Mechanismen zwei Angaben gemacht. Dies sind die Falschakzeptanzrate und die Falschabweisungsrate eines bestimmten Betriebsmodus. Das Maß der Falschakzeptanz lässt sich als Sicherheitsangabe verwenden. Je niedriger diese ist, desto sicherer ist offensichtlich die Zugangskontrolle.

3.2.3 Komfort

Neben den unter 3.2.1 gezeigten Komfortmerkmalen der unterschiedlichen Typen von Authentisierungsmechanismen stellt auch die Falschabweisungsrate ein Maß für die Bewertung im praktischen Einsatz dar. Eine Tür, die jede Person abweist, ist zwar sehr sicher, ist als Zugangsmöglichkeit aber nicht sehr geeignet. Bei der Kombination diverser Mechanismen ist zu erwarten, dass die Anzahl fälschlich abgewiesener Personen gegenüber einem Einzelsystem steigt, und es mit zunehmender Anzahl von Systemen immer unpraktikabler wird sich zu authentisieren. Diese Zusammenhänge werden im anschließenden Kapitel hinsichtlich der Möglichkeiten zur Verknüpfung der Authentisierungsergebnisse untersucht. Hierzu gehören auch Methoden, die bei einem möglichen Ausfall von Sensoren für das Einhalten der gewählten Sicherheitsbedingung sorgen.

3.2.4 Konfiguration

Der Benutzer eines Systems mit diversen Zugangsmechanismen sollte nach seinen Bedürfnissen den Grad der Sicherheit und des Komforts bestimmen können. Dies kann sowohl die Hardware als auch die Software betreffen. Wie im Abschnitt 3.2.1 sind dafür einheitliche Hardware- und Softwareschnittstellen notwendig. Der Busteilnehmer, der für die Verknüpfung der Authentisierungsergebnisse zuständig ist, sollte zusätzlich ein Interface zur Konfiguration aufweisen. Ausgehend von einem Serversystem kann dies eine standardisierte Netzwerkanbindung sein, die entsprechende Dialoge an Visualisierungsclients übermittelt, ähnlich einem Webbrowser. Wie dies sinnvoll realisiert werden kann, wird im Kapitel zur Realisierung des Gesamtsystems untersucht.

3.3 Spezielle Dienstmerkmale des Gebäudebusses

Der größte Nachteil von Bussystemen, wie sie in der Gebäudesystemtechnik Verwendung finden, ist das Fehlen einer vor Missbrauch gesicherten Datenübertragung. Dies liegt daran, dass solche Systeme für Steuerungsaufgaben im Zweckbau entwickelt

wurden, zu Zeiten, als die Leistungsfähigkeit von Mikrocontrollern noch verhältnismäßig gering war. Das Ansteuern, beispielsweise eines Türöffners, stellt prinzipiell kein Problem dar. Da es aber sehr einfach ist, Telegramme am Gebäudebus zu protokollieren und zu senden, empfiehlt es sich nicht, sicherheitstechnische Anlagen darüber zu steuern. Durch die Entwicklung der Powerline- und Funkübertragung wird ein möglicher Missbrauch noch einfacher.

3.3.1 Aktoren

Um Aktoren sicherheitstechnischer Systeme über einen niederratigen Gebäudebus steuern zu können, müssen folgende Eigenschaften der Datenübertragung vorhanden sein:

- **Authentisch** Die Herkunft eines Telegramms muss nachvollziehbar sein. Busteilnehmer ohne Kenntnis eines geheimen Schlüssels dürfen keine gültigen Telegramme erzeugen können.
- **Integer** Es darf nicht möglich sein, dass Telegramme während der Übertragung durch weitere Busteilnehmer verändert und beim Empfänger als gültig erkannt werden.
- **Vertraulich** Abgehörte und protokollierte Telegramme dürfen für Angreifer nicht lesbar sein.
- **Dezentral** Ein Telegramm muss bei Bedarf auch mehrere Empfänger gleichzeitig steuern können.
- **Unidirektional** Um die benötigte Bandbreite zur Übertagung eines Objektes nicht zu erhöhen, muss ein einzelnes Telegramm für die Übermittlung ausreichen.

Selbstverständlich darf die Standardkommunikation auf dem Gebäudebussystem durch die Übermittlung gesicherter Telegramme nicht beeinträchtigt werden. Die gesicherte Übertragung muss über alle eventuellen Router und Koppler hinweg ermöglicht werden.

3.3.2 Sensoren

Für die von sicherheitsrelevanten Sensoren erzeugten Daten gilt für die Übertragung dasselbe wie für die Steuertelegramme an Aktoren im vorigen Abschnitt. Die einzige zusätzliche Bedingung ist, dass eine Unterbrechung des Übertragungsweges erkannt werden muss. Eine solche Unterbrechung der Übertragung kann sowohl durch das Ausbleiben eines Telegramms oder das Überlasten des Bussystems durch eine maximale Anzahl von Telegrammen pro Zeiteinheit erreicht werden. In beiden Fällen muss der Empfänger das Fehlen der Sensordaten erkennen.

3.4 Erweiterte Anwendungen

Neben den primären Diensten der Zugangskontrolle und den speziellen Merkmalen des Gebäudebussystems ergeben sich durch die Konzentration aller Sensordaten im Server, sowie der Integration höherratiger Datennetze erweiterte Anwendungen. Darunter sind sekundäre Dienste zu verstehen, die den Anwendern über die Zugangskontrolle und die Integration gesicherter Sensoren und Aktoren hinaus Anwendungsmöglichkeiten bieten. Möglich ist dies durch Ausnutzen der bereits vorhandenen Hardware zur Visualisierung und Steuerung aller Teilnehmer am Gebäudesystembus, zum Fernzugriff sowie zum Fernmelden und zur Steuerung einfacher, zeitlicher Abläufe.

3.4.1 Visualisierung

Da der Server eine Anbindung zum Gebäudebussystem hat, stehen diesem alle Informationen über Zustände der einzelnen Sensoren und Aktoren zur Verfügung. Über die Anbindung von Clients zur Visualisierung der Konfigurationsdialoge können dort auch alle gesammelten Informationen angezeigt werden. Über einen entsprechenden Rückkanal lassen sich auch Aktoren neue Zustände zuweisen. Damit die Clients nicht ständig mit dem Server verbunden sein müssen, kann dieser ein Prozessabbild der vernetzten Applikationen im Gebäude speichern, welches über die gesamte Betriebsdauer aktualisiert wird.

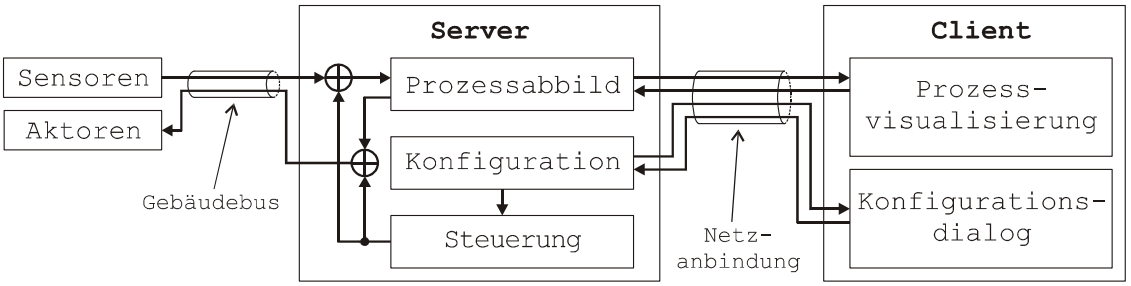

Abbildung 3.2: Kommunikationsstruktur zwischen Gebäudebus und Netzanbindung

Die in diesem Fall bestehende Kommunikationsstruktur im Gebäudesystembus, dem Server und der höherratigen Anbindung von Clients zeigt Abbildung 3.2.

3.4.2 Prozessabbild

Die im Server abgebildeten Zustände aller Sensoren des Gebäudesystembusses lassen sich nicht nur zur Visualisierung nutzen, sondern auch für die Zugangskontrolle. Das Prozessabbild kann serverintern dazu dienen, auf Grund von Zustandsänderungen innerhalb des Gebäudesystems, auf die Anwesenheit von Personen zu schließen und entsprechend die Sicherheitsbedingungen der Zugangskontrolle zu verändern. Im Fall, dass entsprechende Sensoren eine Gefahr erkennen (z.B. Feueralarm, Einbruch oder

eine hilfsbedürftige Person), kann die Zugangstür automatisch entriegelt werden, um dem Rettungspersonal Zutritt zu verschaffen.

3.4.3 Fernzugriff und Fernmelden

Mit der Verwendung eines standardisieren Protokolls bei der Netzwerkanbindung wird es automatisch möglich, auf den Server aus der Ferne zuzugreifen. Es bietet sich zum Beispiel das TCP/IP Protokoll an, welches den Datentransfer über das Internet erlaubt. Zu beachten ist dann aber die Möglichkeit, für andere Personen auf den Server zuzugreifen. Eine entsprechende Absicherung der Verbindung oder der Einsatz einer adäquaten Zugriffskontrolle sind dann notwendig. Ein Fernzugriff ist besonders dann interessant, wenn ein oder mehrere Gebäude von einem anderen Standort aus überwacht und gesteuert werden sollen. Dies betrifft nicht nur die Zugangskontrolle sondern auch die gesamte vernetzt Haustechnik. Das Absetzen von E-Mail Benachrichtigungen, Netmessages oder SMS-Nachrichten über Internetdienste oder direkt angebundene Fernmeldeeinrichtungen bei Störungen oder Alarmen lassen sich ebenfalls realisieren. Bei nicht vorhandener Anbindung an das Internet kann durch eine Verbindung zu einem Fernmeldenetz (Analog- oder ISDN-Modem) die Möglichkeit zur Einwahl in das hausinterne Netzwerk geboten werden. Basierend auf dem TCP/IP Protokoll kann hierfür eine PPP-Verbindung (Point to Point Protocol) aufgebaut werden.

3.4.4 Featurecontroller

Unter Verwendung der Rechenleistung des Serversystems können einfache, zeit- oder ereignisgesteuerte Aktionen im Gebäudebussystem ausgelöst werden. Denkbare Funktionen eines solchen Featurecontrollers sind die Anwesenheitssimulation durch Steuerung der Beleuchtung und Beschattung oder auch die Regelung der Heizungsanlage. Auch hierfür sind entsprechende Konfigurationslösungen notwendig.

3.5 Zusammenfassung des Systemkonzepts

Auf Grund der Analyse der notwendigen Eigenschaften, die ein System zur Anbindung diverser Authentisierungsmechanismen in automatisierten Gebäuden aufweisen muss, zeigt sich, dass im Mittelpunkt ein dienstanbietendes Gateway stehen wird. Folgende Merkmale sind dabei zu realisieren:

- Einheitliche Anbindung diverser Authentisierungsmechanismen
- Datenfusion kombinierter Sensoren
- Auswahlmöglichkeiten zwischen hoher Sicherheit und hohem Komfort
- Dialoggesteuerte Konfiguration

- Gesicherte Anbindung von Sensoren und Aktoren über den Gebäudebus
- Visualisierung und Steuerung aller Zustände von Sensoren und Aktoren
- Konfiguration automatischer Steuerungsabläufe
- Fernzugriff und Übertragung von Meldungen über entsprechende Netzwerke

Dieses Gateway, im Folgenden als Security Server bezeichnet, kommuniziert über unterschiedliche Bussysteme einerseits mit den Authentisierungsmechanismen, andererseits mit dem automatisierten Gebäude. Ein drittes, höherratiges Medium ermöglicht die Konfiguration, Überwachung und Steuerung, sowohl innerhalb des Gebäudes als auch aus der Ferne. Abbildung 3.3 zeigt die schematische Darstellung dieses Konzeptes.

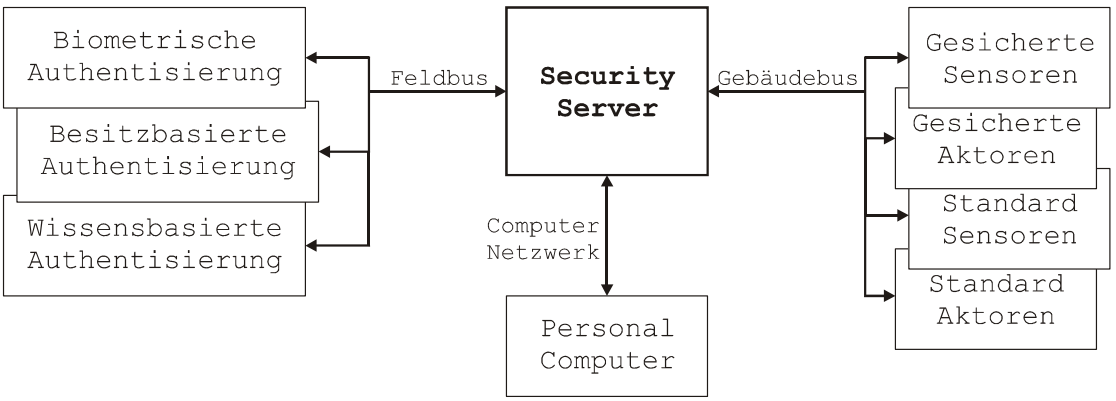

Abbildung 3.3: Darstellung des Gesamtkonzeptes

Ausgehend von dieser Anforderungsanalyse beschreiben die folgenden zwei Kapitel das Konzept für die Zugangskontrolle zu automatisierten Gebäuden mittels eines embedded Servers und eine Variante zur Realisierung der gesicherten Datenübertragung, angepasst an das EIB/KNX Bussystem.

4 Multimodale Zugangskontrolle

4.1 Konzept der Sensorfusion

Die multimodale Zugangskontrolle beschreibt ein PAC-System (Physical Access Control), bei dem mehr als nur ein Mechanismus zur Authentisierung herangezogen wird. Die prinzipielle Idee besteht darin, beliebige biometrische, besitz- und wissensbasierte Mechanismen zu kombinieren, um damit die Sicherheit gegenüber einem monolithischen System zu erhöhen. Hierbei spielen auch die Kosten und der erreichbare Komfort eine entscheidende Rolle. Abbildung 4.1 zeigt den internen Informationsfluss eines solchen Systems.

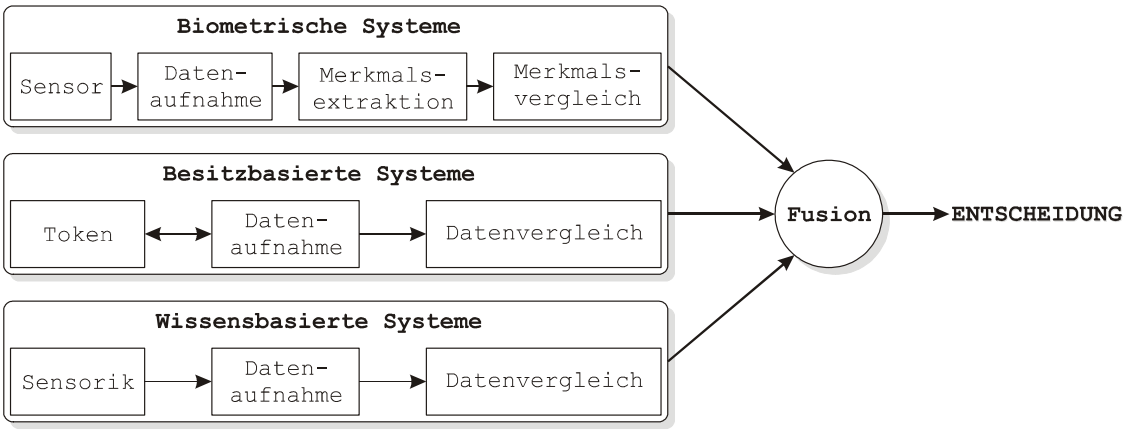

Abbildung 4.1: Sensorflow eines multimodalen Systems

Innerhalb dieses Kapitels soll gezeigt werden, wie sich die unterschiedlichen Mechanismen einheitlich beschreiben lassen und welche Möglichkeiten sich für die Fusion der Authentisierungsergebnisse ergeben. Ziel ist es, für automatische Systeme eine Regel zu definieren, bei gegebenem Sicherheitsniveau die geeignetste Sensorkombination zu wählt. Es soll dabei der beste Kompromiss zwischen Komfort und Sicherheit erreicht werden.

4.2 Bewertung von Authentisierungsmechanismen

Im Kapitel zum Stand von Wissenschaft und Technik konnte bereits die grundlegendste Bewertungsform für biometrische Systeme gezeigt werden. Diese gemeinsame Darstellung der Falschakzeptanz- und Falschabweisungsrate in einem Diagramm, in Form einer Badewannenkurve, gibt Auskunft über die Fehlerraten in Abhängigkeit eines Entscheidungskriteriums.

4.2.1 Bestimmung der Fehlerraten

Um die Leistungsfähigkeit eines Systems zur automatischen Authentisierung zu ermitteln, muss eine möglichst große Anzahl von Verifikationen durchgeführt werden. Man spricht hierbei von Verifikationen, da die aufgenommenen Muster immer mit einer Referenz verglichen werden. Bei einer Authentisierung, bzw. Identifikation wird meist ein Muster mit vielen Referenzen verglichen. Dieser Sachverhalt wird folgend genauer besprochen. Auf Grund natürlicher Schwankungen biometrischer Merkmale und messtechnischer Unvollkommenheiten ist das Ergebnis einer Verifikation nie mit absoluter Sicherheit, sondern nur mit einer statistischen Wahrscheinlichkeit vorhersagbar. Um also eine solche Aussage treffen zu können, wird die Wahrscheinlichkeitsdichtefunktion für die Falschakzeptanz und die Falschabweisung ermittelt. Hierbei wird nicht die boolesche Aussage des Systems betrachtet, sondern das Ähnlichkeitsmaß der verglichenen Muster, welches zur Entscheidungsfindung dient.

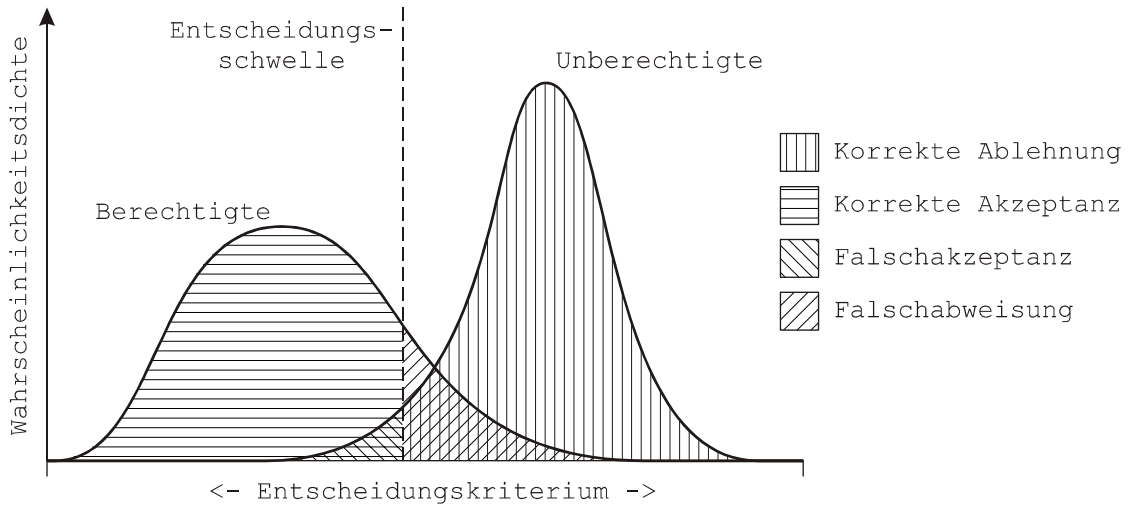

Abbildung 4.2 zeigt beispielhaft eine idealisierte Darstellung der Wahrscheinlichkeitsdichten für Verifikationsversuche durch berechtigte und unberechtigte Personen an einem zu bewertenden System. Die jeweilige Fläche unterhalb der Funktion entspricht der 100% Wahrscheinlichkeit, dass eine Verifikation stattgefunden hat. Die Abszisse stellt hierbei das Ähnlichkeitsmaß der verglichenen Muster dar. Dies könnte beispielsweise die Hamming-Distanz zweier Bitmuster sein. Im Idealfall würden sich beide Kurven nicht schneiden, so dass das System sicher zwischen berechtigten und unberechtigten Personen unterscheiden kann. Dies wird auch als Separierbarkeit oder Entscheidbarkeit eines Authentisierungsmechanismus bezeichnet. Eine Möglichkeit, die Zuverlässigkeit einer Entscheidung darzustellen, besteht in der Angabe eines Maßes dafür, wie weit sich die Zustandsbereiche überlappen beziehungsweise wie weit sie voneinander getrennt sind. Diesem Ansatz, aus dem Bereich der Signalverarbeitung, folgt das Entscheidbarkeitsmaß *d'* (D-Prime), welches sich durch die Mittelwerte μ

und Standardabweichungen σ der a priori modal vorausgesetzten Dichtefunktionen berechnet [Daugman 2000]:

$$d' = \frac{|\mu_1 - \mu_2|}{\sqrt{\frac{1}{2}\left(\sigma_1^2 + \sigma_2^2\right)}} \tag{4.1}$$

Je größer *d'*, desto besser kann der biometrische Mechanismus zwischen einzelnen Individuen unterschieden. Unter reellen Bedingungen sind Überschneidungen beider Funktionen vorhanden, so dass es von wesentlicher Bedeutung ist, die Entscheidungsschwelle richtig zu platzieren. Die in Abbildung 4.2 schräg schraffierten Schnittflächen sind dabei äquivalent zur Falschakzeptanzrate und zur Falschabweisungsrate für den gewählten Arbeitspunkt.

4.2.2 Entscheidungsfindung

Variiert man die Entscheidungsschwelle und trägt die Fehlerraten als Funktion des Entscheidungskriteriums in ein Diagramm ein, so ergeben sich die typischen Fehlerkurven (Badewannenkurve). Man kann das Kriterium eliminieren, indem man die korrespondierenden Paare der FAR und FRR als Koordinaten in ein Diagramm überträgt. Dies führt zur Receiver Operating Characteristic (ROC) beziehungsweise zum Neyman-Pearson Diagramm. In den meisten Fällen wird statt der FRR die Korrektakzeptanzrate angegeben, welche die Kurve lediglich umkehrt. Abbildung 4.3 zeigt die für diese Arbeit wesentlichen Darstellungsformen.

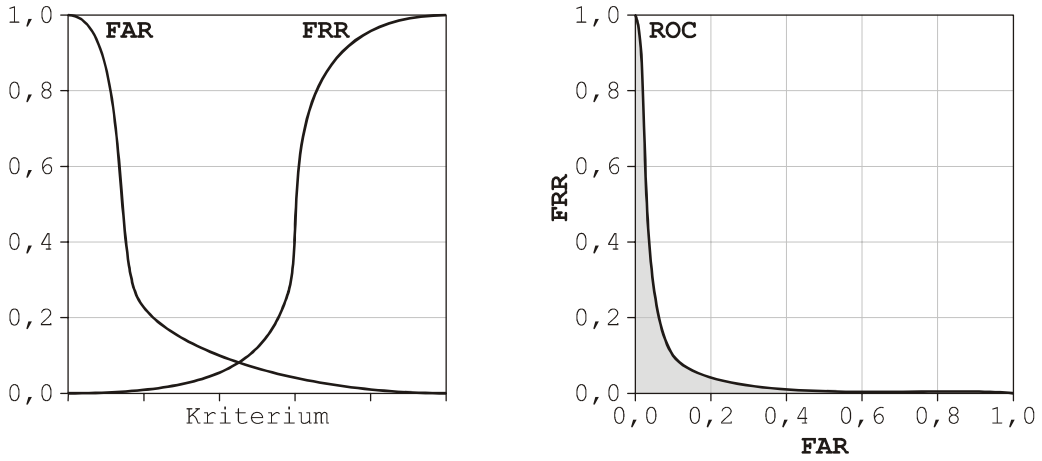

Abbildung 4.3: Darstellungsformen der Fehlerkurven

Die Separierbarkeit, und damit die Stärke eines Authentisierungsmechanismus, zeigt sich in der ROC durch die Fläche unterhalb der Kurve. Je kleiner die Fläche ist, beziehungsweise je näher sich die Kurve an die Koordinatenachsen annähert, desto

präzisere Aussagen lassen sich über die boolesche Entscheidung eines Systems machen. Die meisten Hersteller von biometrischen Systemen, gerade im unteren Preissegment, beschreiben deren Mechanismen nur durch die Angabe eines FAR-FRR Paares. Diese Werte gelten in der Regel unter Laborbedingungen mit kooperativen Benutzern, stellen aber das einzige, direkt verwertbare Maß dar, auf welches diese Arbeit im folgenden aufbaut. Der Punkt, der dadurch in der ROC-Darstellung beschrieben ist, stellt somit den Arbeitspunkt dar.

Eine durch das National Physical Laboratory verfasste Studie [CESG 2001] beschäftigt sich mit dem Test verschiedener biometrischer Systeme unter reellen Bedingungen. Dort wurde versucht, sieben biometrische Systeme genau zu untersuchen, um die jeweiligen Verfahren gegeneinander vergleichen zu können. Abbildung 4.4 zeigt einen Teil der Ergebnisse, welche in Form einer ROC dargestellt sind. Die verwendete, doppelt logarithmische Darstellung zeigt, wie sich biometrische Systeme in den jeweiligen Arbeitspunkten zum Teil um mehrerer Zehnerpotenzen unterscheiden.

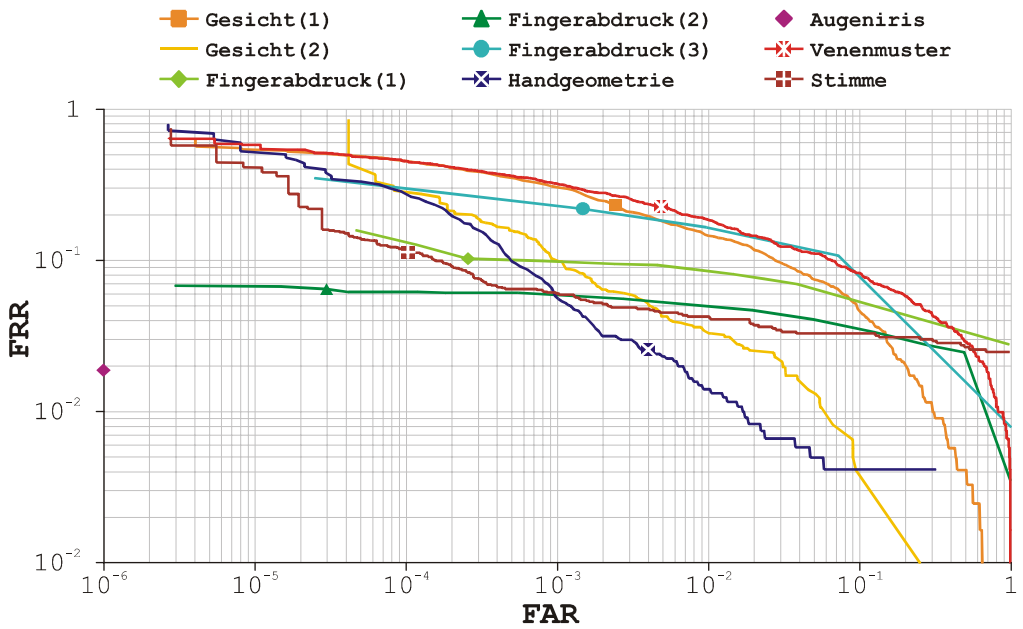

Abbildung 4.4: Unabhängig gemessene ROC-Kurven, Quelle: CESG 2001

Zu diesen Tests wurden 200 Frauen und Männer unterschiedlicher Altersgruppen hinzugezogen und jeder Verifikationsvorgang wurde in den Statistiken berücksichtigt. Die oben gezeigten Ergebnisse liegen dabei um etliche Zehnerpotenzen über den üblichen Herstellerangaben, so dass diese Angaben als Richtwerte zu verstehen sind.

4.2.3 Notation

Folgende Notation dient zur Beschreibung elementarer Ereignisse und statistischer Größen:

- A und B stellen die Mengen elementarer Ereignisse zweier Mechanismen zur Authentisierung dar
- $A(N)$ ist ein System mit N zu vergleichenden Referenzmustern
- $A_1,...,A_{n-1},A_n$ beschreiben n Elementarmengen, voneinander unabhängiger Mechanismen
- $P_{CAR}(A)$ ist die Wahrscheinlichkeit einer Korrektakzeptanz des Systems A
- $P_{CRR}(A)$ ist die Wahrscheinlichkeit einer Korrektabweisung des Systems A
- $P_{FAR}(A)$ ist die Wahrscheinlichkeit der Falschakzeptanz des Systems A
- $P_{FRR}(A)$ ist die Wahrscheinlichkeit der Falschabweisung des Systems A
- $P_{FAR(i)}(A)$ ist die Wahrscheinlichkeit der Falschakzeptanz des Systems A bezogen auf eine Person i
- $P_{FRR(i)}(A)$ ist die Wahrscheinlichkeit der Falschabweisung des Systems A bezogen auf eine Person i
- $\{P_1,...,P_n\}_{\max}$ ist die höchste aller Wahrscheinlichkeiten P_1 bis P_n

4.2.4 Besitz- und wissensbasierte Systeme

Im multimodalen System zur Zugangskontrolle muss es auch möglich sein, besitz- und wissensbasierte Mechanismen zu integrieren. Hierfür ist eine Bewertung ähnlich der biometrischen Einrichtungen notwendig. Mit statistischen Methoden lassen sich auch hier eine FAR und eine FRR bestimmen. Dazu ist es, wie bei biometrischen Systemen, notwendig eine große Anzahl von Authentisierungsversuchen durchzuführen. Die statistische Signifikanz wird erreicht, wenn die Performanzwerte in Abhängigkeit von der Versuchszahl mit einer definierten Wahrscheinlichkeit innerhalb eines bestimmten Fehlerintervalls liegen. Als Faustregel ("Doddington's Regel") gilt, dass so viele Versuche zu machen sind, bis mindestens 30 Fehlerfälle auftreten [Porter 1997]. Bei guten Systemen mit sehr niedrigen Fehlerraten sind hier durchaus etliche Millionen Versuche notwendig.

Da besitz- und wissensbasierte Systeme optimal separierbare Ergebnisse liefern, also reine Ja/Nein-Entscheidungen, lassen sich die Fehlerraten sehr leicht aus den Authentisierungsergebnissen ermitteln. Je größer die Anzahl unabhängiger Personen ist, die sich möglichst oft an einem System authentisieren, desto repräsentativer ist das Endergebnis. Für die an einem Mechanismus A vorgenommenen Untersuchungen mit N Personen ergeben sich die Fehlerraten folgendermaßen:

$$P_{FAR}(A) = \frac{1}{N}\sum_{i=1}^{N} P_{FAR(i)}(A) = \frac{1}{N}\sum_{i=1}^{N} \frac{\text{Anzahl falscher Akzeptanzen der unberechtigten Person } i}{\text{Gesamtanzahl der Angriffe der unberechtigten Person } i} \tag{4.2}$$

$$P_{FRR}(A) = \frac{1}{N}\sum_{i=1}^{N} P_{FRR(i)}(A) = \frac{1}{N}\sum_{i=1}^{N} \frac{\text{Anzahl Abweisungen der berechtigten Person } i}{\text{Gesamtanzahl der Versuche der berechtigten Person } i} \tag{4.3}$$

Entsprechend bilden diese Mechanismen genau einen Arbeitspunkt in der Receiver Operating Characteristic ab.

Wissensbasierte Systeme, wie PIN-Code Schlösser, werden auf Grund der relativ geringen Informationsmenge (z.B. 4 numerische Zeichen) und der Tatsache, dass reelle Personen häufig fehlerhafte Eingaben machen, den jeweiligen Arbeitspunkt sehr weit vom Koordinatenursprung entfernt abbilden. Besitzbasierte Systeme hingegen, sofern der zugehörige Token (eindeutiges Merkmal) nicht in Besitz einer unberechtigten Person gelangt oder das Merkmal gefälscht werden kann, haben den Arbeitspunkt auf der Ordinate. Die Falschabweisungsrate ist lediglich durch Übertragungs- oder Benutzerfehler gegeben, die den Austausch von Informationen zwischen Token und Leseeinheit behindern.

4.2.5 Verifikation und Identifikation

Wie bereits erwähnt, besteht ein Unterschied zwischen Verifikation und Identifikation. Der Unterschied liegt in der Anzahl der Referenzmuster, die mit dem aktuell zu prüfenden Muster verglichen werden müssen. Sobald es mehr als eine Referenz gibt kann es zu Falschidentifikationen kommen. Dies bedeutet, dass zwar einer berechtigten Person Zutritt gewährt wird, diese aber als eine andere erkannt wurde. Die Raten für eine Falschakzeptanz und Falschabweisung sind abhängig von der Anzahl der gespeicherten Referenzen und somit auch von der FIR (False Identification Rate). Die entsprechenden Fehlerraten für Systeme mit *N* Referenzen können mittels folgender in [Bromba 2003] aufgestellten Formeln berechnet werden. Diese gelten für den idealisierten Fall, dass bei einer Mehrfacherkennung der Zutritt verweigert wird und für alle Personen, entsprechend der Statistik, gleichwertige Merkmale gewonnen wurden:

$$P_{FIR}\big(A(N)\big) = (N-1)P_{FRR}(A)P_{FAR}(A)\big(1-P_{FAR}(A)\big)^{N-2} \tag{4.4}$$

$$P_{FAR}\big(A(N)\big) = N \cdot P_{FAR}(A)\big(1-P_{FAR}(A)\big)^{N-1} \tag{4.5}$$

$$P_{FRR}(A(N)) = 1 - (1 - P_{FRR}(A) - P_{FAR}(A) + N \cdot P_{FRR}(A)P_{FAR}(A))(1 - P_{FAR}(A))^{N-2} \quad (4.6)$$

Im Fall, dass die Falschzuweisung keine Rolle spielt, beispielsweise bei der einfachen Zutrittskontrolle, können die Fehlerraten vereinfacht dargestellt werden [Bromba 2003]:

$$P_{FAR}(A(N)) = 1 - (1 - P_{FAR}(A))^{N} \quad (4.7)$$

$$P_{FRR}(A(N)) = P_{FRR}(A)(1 - P_{FAR}(A))^{N-1} \quad (4.8)$$

Das Prinzip zur automatisierten, multimodalen Zutrittskontrolle wird hier im folgenden als Näherung mit den Wahrscheinlichkeiten der FAR und FRR für die Verifikation vorgestellt. Dies ist mit ausreichender Genauigkeit möglich, da die statistischen Angaben für die meisten Authentisierungsmechanismen einige Dekaden unterhalb der 100% Wahrscheinlichkeit liegen und in den häufigsten Anwendungsfällen $N<10$ Benutzerreferenzen in das System eingespeist werden. Systeme für N Benutzer werden in Abschnitt 4.6.1 genauer betrachtet.

4.2.6 Strategischer Entscheidungsraum

Wie bereits im Kapitel zur Analyse des Systems beschrieben, kann das Entscheidungskriterium als Maß von Sicherheit und gegebenenfalls Komfort betrachtet werden. So gesehen bewegen sich die Arbeitspunkte in der ROC monoton fallend von maximaler Falschrückweisung ($P_{FRR}(A)=1$) zu maximaler Falschakzeptanz ($P_{FAR}(A)=1$). Bei der Findung einer Entscheidungsstrategie nach Neyman-Pearson werden die relevanten Bereiche als liberaler und konservativer Entscheidungsraum bezeichnet [Daugman 2000]. Abbildung 4.5 zeigt diese Entscheidungsräume.

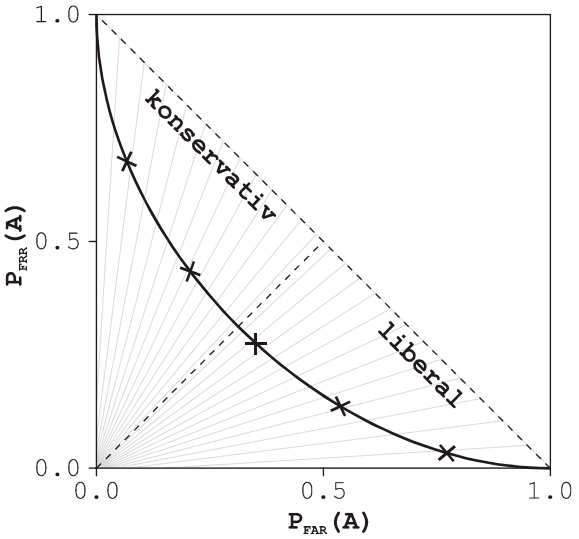

Abbildung 4.5: Strategische Entscheidungsräume der ROC

Die Gleichfehlerrate trennt hierbei die beiden Bereiche, wobei der Übergang fließend ist. Oberhalb der dargestellten, diagonalen Grenze überschreitet die Summe beider Wahrscheinlichkeiten 100%. Dort existieren in der Regel keine Arbeitspunkte, da dieses System nur falsche Entscheidungen treffen würde und dessen Wahrscheinlichkeitsdichtefunktionen nicht separierbar wären.

4.3 Kombination zweier Authentisierungsmechanismen

Ausgehend davon, dass es zwei elementare Ereignisse e_0 (Zutritt verweigert) und e_1 (Zutritt gewährt) gibt, können die Wahrscheinlichkeiten für kombinierte Systeme mittels der Korrektakzeptanz- und Korrektablehnungsraten hergeleitet werden. Die Wahrscheinlichkeiten für die CAR (Correct Acceptance Rate) und die CRR (Correct Rejection Rate) eines einzelnen Systems *A* ergeben sich aus den korrespondierenden Fehlerraten. Eine richtige Akzeptanz, beziehungsweise Ablehnung durchgeführt zu haben, ergibt sich unter den Bedingungen für die Wahrscheinlichkeiten einer falschen Person Zutritt zu gewähren, sowie die richtige Person abzuweisen mit $0 \le P_{FAR}(A) \le 1$ und $0 \le P_{FRR}(A) \le 1$ folgendermaßen:

$$P_{CAR}(A) = P_{FRR}(\overline{A}) = 1 - P_{FRR}(A) \tag{4.9}$$

$$P_{CRR}(A) = P_{FAR}(\overline{A}) = 1 - P_{FAR}(A) \tag{4.10}$$

4.3.1 Konjunktion dualer Systeme

Werden die Authentisierungsdaten zweier Mechanismen miteinander fusioniert, so besteht die Menge aller Ereignissen $E=\{e_{00}, e_{01}, e_{10}, e_{11}\}$ aus vier möglichen Elementarereignisse. Bei einer einfachen UND-Verknüpfung errechnet sich die FAR aus dem Ereignis e_{11}, wenn beide Systeme den Zutritt gewähren. Ist dies bei zwei unabhängigen Systeme *A* und *B* der Fall, errechnet sich die FAR folgendermaßen:

$$P_{FAR}(A \cap B) = P_{FAR}(A)P_{FAR}(B) \tag{4.11}$$

Daraus folgt, dass die Wahrscheinlichkeit, einer unberechtigten Person Zutritt zu gewähren, insgesamt kleiner oder gleich ist als bei einem Einzelsystem, so dass man von einer Steigerung der Sicherheit sprechen kann.

Für dasselbe duale System ergibt sich die FRR aus den Ereignissen e_{00}, e_{01} und e_{10}. Vorausgesetzt ist hier die Authentisierung einer berechtigten Person:

$$P_{FRR}(A \cap B) = P_{FRR}(A)P_{FRR}(B) + P_{FRR}(B)P_{CAR}(A) + P_{CAR}(B)P_{FRR}(A) \tag{4.12}$$

Nach Auflösen von $P_{CAR}(A)$ und $P_{CAR}(B)$ mit anschließender Vereinfachung ergibt sich:

$$P_{FRR}(A \cap B) = P_{FRR}(A) + P_{FRR}(B) - P_{FRR}(A)P_{FRR}(B) \tag{4.13}$$

Daraus folgt, auf Grund der Tatsache, dass das Produkt beider FRR immer kleiner oder gleich dem der geringeren FRR ist, dass die Gesamt-FRR höher als die der Einzelsysteme ist. Es werden also mehr Personen fälschlicherweise abgewiesen werden als bei einem einzelnen Mechanismus, was eine Komforteinbuße bedeutet.

4.3.2 Disjunktion dualer Systeme

Bei der ODER-Verknüpfung zweier Mechanismen kehren sich die Verhältnisse gegenüber der Konjunktion um. Zu einer Falschakzeptanz führen in diesem Fall die Ereignisse e_{01}, e_{10} und e_{11}, sofern sich eine unberechtigte Person authentisiert:

$$P_{FAR}(A \cup B) = P_{CRR}(A)P_{FAR}(B) + P_{FAR}(A)P_{CRR}(B) + P_{FAR}(A)P_{FAR}(B) \tag{4.14}$$

Nach Auflösen von $P_{CRR}(A)$ und $P_{CRR}(B)$ mit anschließender Vereinfachung ergibt sich:

$$P_{FAR}(A \cup B) = P_{FAR}(A) + P_{FAR}(B) - P_{FAR}(A)P_{FAR}(B) \tag{4.15}$$

Es ist zu erkennen, dass bei einer ODER-Verknüpfung der Ergebnisse die Falschakzeptanz des Gesamtsystems gegenüber der einzelnen Mechanismen steigen wird, umgekehrt zum UND-verknüpften System.

Die zugehörige Falschabweisung ergibt sich aus dem elementaren Element e_{00}, für den Fall, dass sich eine berechtigte Person authentisiert:

$$P_{FRR}(A \cup B) = P_{FRR}(A)P_{FRR}(B) \tag{4.16}$$

Hier verringert sich die Falschabweisungsrate durch die Kombination der Authentisierungsergebnisse.

4.3.3 Fazit

Am Beispiel für die Fusion zweier reeller, unterschiedlich starker Systeme, wie sie im Kapitel zur Umsetzung des Gesamtsystems beschrieben sind, sind in Tabelle 4.1 die entsprechenden Fehlerraten bestimmt. System *A* ist eine Fingerabdruckerkennung, System *B* eine Spracherkennung.

Tabelle 4.1: Konjunktion und Disjunktion zweier reeller Systeme

	A	B	$A \cap B$	$A \cup B$
P_{FAR}	$1{,}00 \cdot 10^{-6}$	$6{,}00 \cdot 10^{-2}$	$6{,}00 \cdot 10^{-8}$	$6{,}00 \cdot 10^{-2}$
P_{FRR}	$5{,}00 \cdot 10^{-3}$	$6{,}00 \cdot 10^{-2}$	$6{,}47 \cdot 10^{-2}$	$3{,}00 \cdot 10^{-4}$
Fehlersumme	$5{,}00 \cdot 10^{-3}$	$1{,}20 \cdot 10^{-1}$	$6{,}47 \cdot 10^{-2}$	$6{,}03 \cdot 10^{-2}$

Anhand der Zahlenwerte ist zu erkennen, dass sich bei der UND-Verknüpfung die FAR deutlich verbessert und die FRR etwas schlechter wird, sich aber nahe an der FRR des schwächeren Systems hält. Bei der ODER-Verknüpfung verhält es sich entsprechend umgekehrt. Betrachtet man jedoch die Anzahl der Fehlentscheidungen pro Authentisierung (Falschakzeptanz plus Falschabweisung) ist zu erkennen, dass die Anzahl falscher Authentisierungen bei beiden Kombinationen insgesamt mehr werden als dies bei dem stärkeren Verfahren der Fall ist. Die Kombination zweier Systeme ist nur dann sinnvoll, wenn man den Arbeitspunkt mehr in Richtung des konservativen Entscheidungsraum (Konjunktion) oder in Richtung des liberalen Entscheidungsraum (Disjunktion) verlagern will, ohne Rücksicht auf die Anzahl der gesamten Fehlentscheidungen zu nehmen.

4.4 Sensorfusion n-Systeme

Bei der Verknüpfung mehrer Authentisierungsmechanismen ergeben sich weitere Kombinationsmöglichkeiten als dies bei Einzel- oder Dualsystemen der Fall ist. Es können zwischen einem und bis zu *n* Systeme zur Authentisierung herangezogen werden. Die Anzahl möglicher Kombinationen *k* bei *n* Systemen ergibt sich folgendermaßen, wobei Null-Elemente und Wiederholungen ausgeschlossen sind (Binomischer Satz [Bronstein 1991]):

$$k(n) = \sum_{i=1}^{n} \binom{n}{i} = \sum_{i=0}^{n} \binom{n}{i} - \binom{n}{0} = 2^n - 1 \tag{4.17}$$

Jede dieser Kombinationen erzeugt eine eigene Menge elementarer Ereignisse, die sich aus den binären Varianten der eingesetzten Zugangsmechanismen ergibt. Innerhalb dieser Mengen mit mehr als zwei Elementen existieren diverse Verknüpfungsstrategien. Diese können die Konjunktion (Schnittmenge), Disjunktion (Verschmelzung) oder Kombinationen daraus sein, so dass jede Strategie einen Arbeitspunkt innerhalb der ROC abbildet.

Tabelle 4.2: Kombinationen und Strategien dreier Systeme

Kombinationen	Elementarmenge	Strategien
A	$\{e_0, e_1\}$	*A*
B	$\{e_0, e_1\}$	*B*
C	$\{e_0, e_1\}$	*C*
A, B	$\{e_{00}, e_{01}, e_{10}, e_{11}\}$	$A \cap B$, $A \cup B$
B, C	$\{e_{00}, e_{01}, e_{10}, e_{11}\}$	$B \cap C$, $B \cup C$
A, C	$\{e_{00}, e_{01}, e_{10}, e_{11}\}$	$A \cap C$, $A \cup C$
A, B, C	$\{e_{000}, e_{001}, e_{010}, e_{011}, e_{100}, e_{101}, e_{110}, e_{111}\}$	$A \cap B \cap C$, $A \cup B \cup C$, $A \cap (B \cup C)$, $A \cup (B \cap C)$, $B \cap (A \cup C)$, $B \cup (A \cap C)$, $C \cap (A \cup B)$, $C \cup (A \cap B)$

Tabelle 4.2 zeigt beispielhaft alle Kombinationen samt Elementarmengen und möglicher Entscheidungsstrategien, die sich mit drei Mechanismen *A, B* und *C* ergeben. Auf Grund der zahlreichen Kombinationen und damit verbundenen Strategien kann hier im folgenden nur eine Berechnungsvorschrift angegeben werden.

Die wichtigste Kombination ist die Fusion aller Mechanismen, bei der *n* Authentisierungsergebnisse zur Entscheidungsstrategie beitragen. Die Elementarmenge besteht

dabei aus 2^n Ereignissen, die je nach gewählter Strategie in die Berechnung des Arbeitspunktes miteinbezogen werden. Alle Kombinationen mit Ordnungen kleiner *n* lassen sich rekursiv mit derselben Vorschrift berechnen.

4.4.1 Konjunktion

In einem System *n*-ter Ordnung, bei dem alle Authentisierungsergebnisse UND-verknüpft werden, berechnet sich sie Wahrscheinlichkeit einer Falschakzeptanz aus dem Produkt aller Falschakzeptanzraten, der an der Authentisierung beteiligten Mechanismen A_1 bis A_n. Hier liegen nur die Ergebnisse der Falschakzeptanzen e_1 aller gleichzeitig gewährten Zutritte zugrunde (e_{111} bei obigem Beispiel eines Dreifachsystems):

$$P_{FAR}\left(A_1 \cap \ldots \cap A_n\right) = \prod_{i=1}^{n} P_{FAR}\left(A_i\right) \tag{4.18}$$

Bei der Berechnung der Falschabweisungsrate hingegen müssen alle 2^n-1 Ereigniselemente berücksichtigt werden. Es kann immer nur eines dieser Ereignisse eintreten, so dass die Berechnungsvorschrift als disjunktive Normalform dargestellt werden muss. Das Ergebnis einer Falschabweisung e_0 eines Mechanismus wird durch die Menge *A* dargestellt, die Negation e_1 durch die Menge $\overline{A}$ beziehungsweise die entsprechende Korrektakzeptanz. Am Beispiel für drei Systeme *A*, *B* und *C* ergibt sich die Wahrscheinlichkeit einer Falschabweisung folgendermaßen:

$$\begin{aligned} P_{FRR}(A \cap B \cap C) = {} & P_{FRR}(A)P_{FRR}(B)P_{FRR}(C) + P_{FRR}(A)P_{FRR}(B)P_{FRR}(\overline{C}) \\ & + P_{FRR}(A)P_{FRR}(\overline{B})P_{FRR}(C) + P_{FRR}(A)P_{FRR}(\overline{B})P_{FRR}(\overline{C}) \\ & + P_{FRR}(\overline{A})P_{FRR}(B)P_{FRR}(C) + P_{FRR}(\overline{A})P_{FRR}(B)P_{FRR}(\overline{C}) \\ & + P_{FRR}(\overline{A})P_{FRR}(\overline{B})P_{FRR}(C) \end{aligned} \tag{4.19}$$

Nach Auflösen der Negationen und anschließender Vereinfachung lässt sich die FRR des Dreifachsystems aus den gegebenen Fehlerraten der Einzelsysteme entsprechend ermitteln:

$$\begin{aligned} P_{FRR}(A \cap B \cap C) = {} & P_{FRR}(A) + P_{FRR}(B) + P_{FRR}(C) - P_{FRR}(A)P_{FRR}(B) \\ & - P_{FRR}(A)P_{FRR}(C) - P_{FRR}(B)P_{FRR}(C) \\ & + P_{FRR}(A)P_{FRR}(B)P_{FRR}(C) \end{aligned} \tag{4.20}$$

Die Falschabweisungsrate eines konjunktiv verknüpften, multimodalen Systems lässt sich auch rekursiv, mit Hilfe der Berechnungsvorschrift für Dualsysteme ermitteln. Das

Assoziativgesetz erlaubt die Paarbildung der Elementarmengen, so dass Ergebnisse dualer Systeme wieder in dualen Systemen zusammengefasst werden können:

$$P_{FRR}(A_1 \cap ... \cap A_n) = P_{FRR}(((A_1 \cap A_2) \cap A_3) ... \cap A_n) \tag{4.21}$$

Automatisierte Systeme können auf diese Weise einfach Fehlerraten einer beliebigen Anzahl von Mechanismen ohne das Aufstellen einer Normalform ermitteln. Wie bei dualen Systemen verschlechtert sich die gesamte Falschabweisungsrate gegenüber dem schwächsten System. Bei sehr ungleich starken Systemen verändert sich die FRR nur geringfügig, so dass als Näherung die des schwächsten Systems herangezogen werden kann. Betrachtet man die Falschabweisungsrate eines dualen Systems, so ist zu erkennen, dass die FRR immer kleiner oder gleich der Summe beider Fehlerraten ist:

$$P_{FRR}(A \cap B) = P_{FRR}(A) + P_{FRR}(B) - P_{FRR}(A)P_{FRR}(B) \leq P_{FRR}(A) + P_{FRR}(B) \tag{4.22}$$

Da sich ein konjunktives *n*-System auch durch die rekursive UND-Verknüpfung dualer Kombinationen beschreiben lässt, führen obige Betrachtungen zu folgendem Ergebnis:

$$\{P_{FRR}(A_1),...,P_{FRR}(A_n)\}_{\max} \leq P_{FRR}(A_1 \cap ... \cap A_n) \leq \sum_{i=1}^{n} P_{FRR}(A_i) \tag{4.23}$$

4.4.2 Disjunktion

Zur Berechnung der Falschakzeptanzrate *n* kombinierter Systeme, unter Verwendung einer einfachen ODER-Strategie, werden die Ereignisse e_1 der Falschakzeptanz und e_0 der Korrektabweisung beziehungsweise Negation betrachtet. Es ergeben sich somit 2^n-1 Ereigniskombinationen die zur Zutrittsgewährung führen. Die Berechnung ist dabei äquivalent zur Vorgehensweise bei der Bestimmung der Falschabweisungsrate in konjungierten Systemen. Dies ist folgend am Beispiel dreier Systeme *A*, *B* und *C* in bereits vereinfachter Form dargestellt:

$$\begin{aligned} P_{FAR}(A \cup B \cup C) = {} & P_{FAR}(A) + P_{FAR}(B) + P_{FAR}(C) - P_{FAR}(A)P_{FAR}(B) \\ & - P_{FAR}(A)P_{FAR}(C) - P_{FAR}(B)P_{FAR}(C) \\ & + P_{FAR}(A)P_{FAR}(B)P_{FAR}(C) \end{aligned} \tag{4.24}$$

In automatisierten Systemen kann die Falschakzeptanzrate auch durch Paarbildung der Elementarmengen rekursiv ermittelt werden, ohne die disjuntive Normalform über alle relevanten Ereignisse aufstellen zu müssen:

$$P_{FAR}(A_1 \cup ... \cup A_n) = P_{FRR}(((A_1 \cup A_2) \cup A_3) ... \cup A_n) \tag{4.25}$$

Wie bei dualen Systemen verschlechtert sich auch hier die gesamte Falschakzeptanzrate gegenüber dem schwächsten System. Bei sehr ungleich starken Systemen verändert sich die FAR nur geringfügig, so dass als Näherung die des schwächsten Systems herangezogen werden kann. Betrachtet man die Falschakzeptanzrate eines dualen Systems, so ist zu erkennen, dass die FAR immer kleiner oder gleich der Summe beider Fehlerraten ist:

$$P_{FAR}(A \cup B) = P_{FAR}(A) + P_{FAR}(B) - P_{FAR}(A)P_{FAR}(B) \leq P_{FAR}(A) + P_{FAR}(B) \tag{4.26}$$

Da sich ein disjunktives *n*-System auch durch die rekursive ODER-Verknüpfung dualer Kombinationen beschreiben lässt, führen obige Betrachtungen zu folgendem Ergebnis:

$$\{P_{FAR}(A_1),...,P_{FAR}(A_n)\}_{\max} \leq P_{FAR}(A_1 \cup ... \cup A_n) \leq \sum_{i=1}^{n} P_{FAR}(A_i) \tag{4.27}$$

Die Falschabweisungsrate eines Systems *n*-ter Ordnung, bei einer einfachen ODER-Strategie, ergibt sich aus dem Produkt aller Falschabweisungsraten der beteiligten Mechanismen A_1 bis A_n. Es liegen nur die Ergebnisse der Falschabweisungen e_0 aller gleichzeitig abgewiesenen Zutrittsversuche zugrunde (e_{000} bei obigem Beispiel eines Dreifachsystems):

$$P_{FRR}(A_1 \cup ... \cup A_n) = \prod_{i=1}^{n} P_{FRR}(A_i) \tag{4.28}$$

4.4.3 Variationen

Bei der Berechnung der Fehlerraten von Systemen mit Strategien, die über die einfache Konjunktion und Disjunktion hinausgehen, kann hier keine generelle Berechnungsvorschrift gegeben werden. In jedem Fall werden sich die Strategien aus einfachen Verknüpfungen zusammensetzen lassen. Es ist dabei zu beachten, dass die Axiome der Wahrscheinlichkeitsrechnung, speziell das Distributivgesetzt, für voneinander unabhängige Ereignisse gelten und hier nicht greifen. Folgendes Beispiel soll dies verdeutlichen:

$$P_{FAR}(A \cap (B \cup C)) \neq P_{FAR}((A \cap B) \cup (A \cap C)) \tag{4.29}$$

Nach Einsetzten der Wahrscheinlichkeiten und Auflösen folgt:

$$\begin{aligned} &P_{FAR}(A)P_{FAR}(B) + P_{FAR}(A)P_{FAR}(C) - P_{FAR}(A)P_{FAR}(B)P_{FAR}(C) \\ &\neq P_{FAR}(A)P_{FAR}(B) + P_{FAR}(A)P_{FAR}(C) - P_{FAR}(A)P_{FAR}(B)P_{FAR}(A)P_{FAR}(C) \end{aligned} \tag{4.30}$$

Das mehrfache Verknüpfen einer Ereignismenge führt zu einem falschen Ergebnis, da das Ereignis der Authentisierung an jedem Mechanismus genau einmal eintritt.

Durch diverse Kombinationen lassen sich die Arbeitspunkte innerhalb der ROC verschieben. Konjunktionen verlagern den Arbeitspunkt dabei mehr in Richtung des konservativen Entscheidungsbereichs, Disjunktionen mehr in Richtung des liberalen Bereichs. Abbildung 4.6 zeigt die Receiver Operating Characteristic dreier kombinierter Systeme, wie sie im Kapitel zur Umsetzung des Gesamtsystems beschrieben sind.

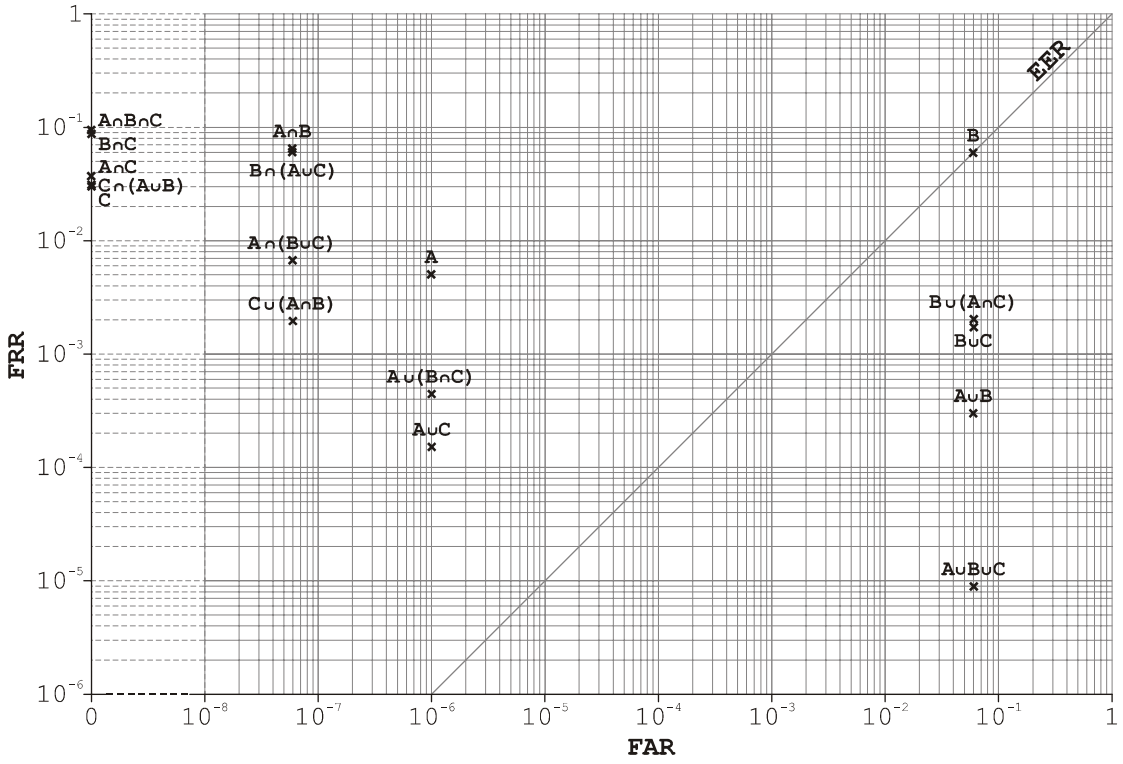

Abbildung 4.6: Beispiel einer ROC aller Varianten eines Dreifachsystems

Es handelt sich hierbei um eine Fingerabdruckerkennung ($P_{FAR}(A) = 1 \cdot 10^{-6}$, $P_{FRR}(A) = 5 \cdot 10^{-3}$), eine Spracherkennung ($P_{FAR}(B) = 6 \cdot 10^{-2}$, $P_{FRR}(B) = 6 \cdot 10^{-2}$) und ein Smart Card Interface ($P_{FAR}(C) = 0$, $P_{FRR}(C) = 3 \cdot 10^{-2}$). Die Falschabweisungsrate von 3% des entwickelten Smart Card Mechanismus ergibt sich aus einer Testreihe von 100 Authentisierungsvorgängen und ist auf elektromechanische Kontaktierungsprobleme der Leseeinheit zurückzuführen. Es gilt zu beachten, dass bei jeder Kombination der Ordnung *n* sich die Person auch an *n* Mechanismen authentisieren muss. Zum Beispiel bei der ODER-Verknüpfung dreier Systeme; dort werden die Authentisierungsergebnisse disjunkt, der Proband jedoch muss alle drei Mechanismen benutzen.

4.5 Klassifizierung der Arbeitspunkte

Wie bereits beschrieben, lassen sich die jeweiligen Verknüpfungsstrategien nach konservativen und liberalen Entscheidungen klassifizieren. Für den Anwender eines solchen Zugangssystems ist es jedoch wichtiger, ein Maß für die Sicherheit festzulegen, ohne den Komfort unnötig zu verschlechtern. Im Optimalfall sollte der Administrator eines solchen Systems lediglich einen Wert für die Sicherheit festlegen müssen. Das System wählt dann selbstständig eine geeignete Strategie aus.

4.5.1 Entscheidungsraum

Nach den Überlegungen aus 4.4.1, 4.4.2 und 4.4.3 können die Grenzen, innerhalb dieser sich die Arbeitspunkte alle Strategien befinden, bestimmt werden. Die Eckpunkte, die den Entscheidungsraum aufspannen, bilden dabei die FAR und FRR der Konjunktion beziehungsweise der Disjunktion aller Mechanismen.

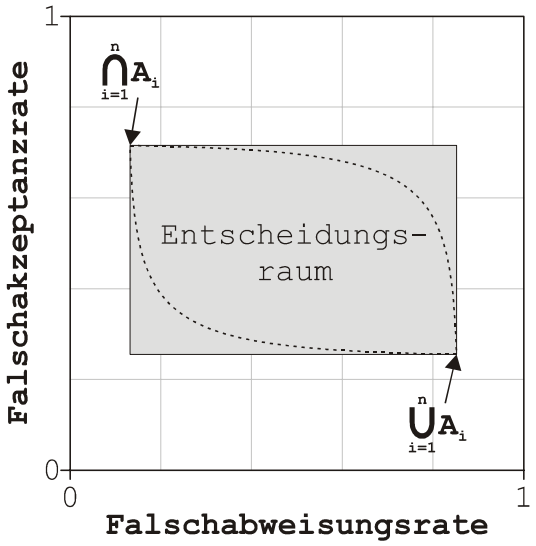

Abbildung 4.7: Strategischer Entscheidungsraum kombinierter Systeme

Abbildung 4.7 stellt beispielhaft den rechteckigen Entscheidungsraum dar. Innerhalb der Grenzen dieser Fläche finden sich alle Entscheidungsräume sämtlicher Kombinationen kleinerer Ordnung. Die in dieser Arbeit betrachtete rechteckige Form stellt eine Näherung dar. Die Arbeitpunkte sämtlicher Strategien liegen in einem kleineren Bereich, der in der Abbildung gestrichelt angedeutet ist und hier nicht näher untersucht wird.

4.5.2 Sicherheit und Komfort

Die Sicherheit eines multimodalen Zugangskontrollsystems lässt sich als Zahlenwert durch die Falschakzeptanzrate darstellen. Die obere und unter Grenze der Fehlerrate,

welche sich, wie im vorherigen Abschnitt beschrieben, aus der Konjunktion und Disjunktion bestimmen lassen, bilden die minimal und maximal erreichbare Sicherheit des Systems. Das Benutzerinterface wird die Einstellung später innerhalb dieses Bereichs zulassen.

Ein Maß für den Komfort eines multimodalen Zugangskontrollsystems zu finden ist schwieriger, da hier auch das subjektive Empfinden eine Rolle spielt. Die Ordnung der Strategie, also die Anzahl der zur Authentisierung herangezogenen Mechanismen ist ein Wert, der direkt dazu herangezogen werden kann. Je kleiner die Ordnung, desto komfortabler ist der Zugang. Ebenso stellt die Falschabweisungsrate ein Maß für den Komfort dar, da das Abweisen berechtigter Personen eine Komforteinbuße bedeutet. Idealerweise müsste jeder Authentisierungsmechanismus eine Komfortbewertung mit sich bringen, anhand dessen ein automatisches System die Strategie mit dem höchsten Komfortfaktor im Bereich der eingestellten Sicherheit ermitteln kann.

Tabelle 4.3: Einschätzung biometrischer Verfahren, Quelle: [Bromba 2003]

Biometrisches Merkmal	Komfort	Genauigkeit	Verfügbarkeit	Kosten
Fingerabdruck				
Unterschrift (dynamisch)				
Gesichtsgeometrie				
Iris				
Retina				
Handgeometrie				
Fingergeometrie				
Venenstruktur Handrücken				
Ohrform				
Stimme				
DNA bzw. DNS				
Geruch	?			?
Tastenanschlag				
Vergleich: Passwort				

Tabelle 4.3 zeigt nach heutiger Realisierungen bedingte Einschätzungen für biometrische Systeme, die sich mit neuen Lösungen deutlich verschieben können. Auf diese Weise ließe sich der erreichbare Komfort einer Kombination durch das Produkt der Einschätzungen aller verwendeten Mechanismen ermitteln. Voraussetzung der Komfortbewertungen ist die Skalierung auf das Standardintervall (0, 1). Dabei steht 0 für geringsten Komfort und 1 für maximalen Komfort. Da diese nur subjektiv zu bestimmen sind, werden im Rahmen der vorliegenden Arbeit nur die Fehlerraten und die Ordnung des Systems betrachtet.

4.5.3 Aussagequalität

Ähnlich der Separierbarkeit eines Einzelsystems kann auch für multimodale Systeme ein Qualitätsmaß angegeben werden. Es bieten sich hierfür drei Methoden an; die Fehlersumme, das Fehlerprodukt und der Abstand des Arbeitspunktes zum Koordinatenursprung. Am besten eignet sich die Fehlersumme beziehungsweise die Gesamtfehlerwahrscheinlichkeit der jeweiligen Strategie, da dieses Maß unmittelbar in eine Aussage formuliert werden kann und sich linear zur jeweiligen Falschakzeptanzrate und Falschabweisungsrate verhält.

$$P_{Fehler}(Strategie_k) = P_{FAR}(Strategie_k) + P_{FRR}(Strategie_k) \tag{4.31}$$

Die Summe beider Wahrscheinlichkeiten bleibt innerhalb des Standardintervalls, da es sich andernfalls um nichtseparierbare Wahrscheinlichkeitsdichtefunktionen einiger oder aller innerhalb der jeweiligen Strategie verknüpften Mechanismen handeln würde.

4.5.4 Automatische Strategieauswahl

In einem multimodalen Zugangskontrollsystem werden zunächst, entsprechend der definierten Berechnungsvorschriften, für alle Entscheidungsstrategien die Fehlerraten berechnet. Die Ergebnisse lassen sich nach der zu erreichenden Sicherheit klassifizieren, indem die jeweiligen Falschakzeptanzraten untersucht werden. Tabelle 4.4 zeigt die nach der FAR sortierten Entscheidungsstrategien des Beispielssystems aus 4.4.3, dessen Realisierung später in dieser Arbeit beschriebenen ist. Die Angaben der Tabelle sind auf zwei Nachkommastellen gerundet. Es ist gut zu erkennen, dass sich Gruppen mit sehr ähnlichen Falschakzeptanzraten bilden. Dies liegt an den um einige Zehnerpotenzen unterschiedlichen Fehlerraten der einzelnen Systeme. Die schwächeren Falschakzeptanzraten disjunkter Strategien dominieren gegenüber den stärkeren, so wie dies bei den Falschabweisungen konjungierter Strategien der Fall ist.

Um nun für eine gewählte Sicherheitsstufe (Falschakzeptanzrate) die komfortabelste beziehungsweise geeignetste Strategie zu wählen, werden die Arbeitspunkte mit der innerhalb einer definierten Toleranz nächstniedrigen Falschakzeptanzrate bestimmt. Aus der Menge dieser Strategien wird das mit der niedrigsten Fehlersumme als Arbeitspunkt ausgewählt. Alternativ kann auch die Strategie mit der niedrigsten Ordnung gewählt werden, um den Komfort zu maximieren. Die Toleranz, mit der die Menge geeigneter Strategien bestimmt wird, sollte so groß gewählt werden, dass immer mindestens ein Arbeitspunkt innerhalb dieser liegt. Es kann beispielsweise ausreichend sein, über den gesamten Bereich der Arbeitspunkte nur drei Abschnitte zu definieren („konservativ“, „mittel“ und „liberal“), über die der Administrator das Systemverhalten bestimmen kann.

Tabelle 4.4: Strategietabelle des Beispielsystems 3. Ordnung

FAR	Entscheidungsstrategie	Ordnung	Fehlersumme
0,00	C	1	$3{,}00 \cdot 10^{-2}$
	$C \cap (A \cup B)$	3	$3{,}03 \cdot 10^{-2}$
	$A \cap C$	2	$3{,}49 \cdot 10^{-2}$
	$B \cap C$	2	$8{,}82 \cdot 10^{-2}$
	$A \cap B \cap C$	3	$9{,}28 \cdot 10^{-2}$
$6{,}00 \cdot 10^{-8}$	$C \cup (A \cap B)$	3	$1{,}94 \cdot 10^{-3}$
	$A \cap (B \cup C)$	3	$6{,}79 \cdot 10^{-3}$
	$B \cap (A \cup C)$	3	$6{,}01 \cdot 10^{-2}$
	$A \cap B$	2	$6{,}47 \cdot 10^{-2}$
$1{,}00 \cdot 10^{-6}$	$A \cup C$	2	$1{,}51 \cdot 10^{-4}$
	$A \cup (B \cap C)$	3	$4{,}42 \cdot 10^{-4}$
	A	1	$5{,}00 \cdot 10^{-3}$
$6{,}00 \cdot 10^{-2}$	$A \cup B \cup C$	3	$6{,}00 \cdot 10^{-2}$
	$A \cup B$	2	$6{,}03 \cdot 10^{-2}$
	$B \cup C$	2	$6{,}18 \cdot 10^{-2}$
	$B \cup (A \cap C)$	3	$6{,}21 \cdot 10^{-2}$
	B	1	$1{,}20 \cdot 10^{-1}$

Die multimodale Zugangskontrolle hat gegenüber monolithischen System, neben der Möglichkeit die Sicherheit zu erhöhen, zwei weitere große Vorteile. Zum einen erweisen sich solche Systeme toleranter gegenüber biometrischen Merkmalsveränderungen wie beispielsweise der Alterung von Personen, zum anderen handelt es sich um ein redundantes System. Bei Störungen oder einem Ausfall einer oder mehrer Mechanismen verringert sich die maximale Ordnung des Systems. Insofern dies automatisch erkannt wird, kann das System selbstständig die nächstsichere Verknüpfungsstrategie wählen, die den fehlerhaften Mechanismus ausschließt. Wenn auf Grund hoher Sicherheitsanforderungen oder eines geringen Toleranzbereiches kein sicherer Arbeitspunkt verfügbar ist, muss der Zugang verweigert werden.

4.6 Weitere Betrachtungen

4.6.1 N-Benutzer Systeme

Wie bereits unter 4.2.5 beschrieben, besteht zwischen der Verifikation und der Identifikation ein Unterschied in der Anzahl der zu vergleichenden Referenzen eines Authentisierungsmechanismus. Je mehr Referenzen zu vergleichen sind, desto höher wird die Wahrscheinlichkeit einer Falschakzeptanz beziehungsweise Falschabweisung,

solange die Identität der Person eine Rolle spielt. Bei der einfachen Zugangskontrolle, bei der die Identität der Person keine Bedeutung hat, verringert sich jedoch die Falschabweisungsrate eines Einzelsystems [Bromba 2003]. In der Regel ist die Identität bei den hier vorgestellten Verfahren zur multimodalen Zugangskontrolle ausschlaggebend. Es ist zu vermeiden, dass sich mehrere Person an den verschiedenen Mechanismen gleichzeitig authentisieren.

Um ein multimodales System für N Benutzer zu bestimmen, müssen erst die Fehlerraten der Einzelsysteme für N Referenzen erweitert werden, bevor die oben beschriebenen Operationen angewendet werden können. Das Erweitern der berechneten Strategien für die Verifikation um die Anzahl der eingespeicherten Referenzen führt zu einem falschen Ergebnis, da die Fehlerwahrscheinlichkeiten dann nicht mehr als voneinander unabhängig betrachtet werden können.

4.6.2 Hybride Systeme

Eine weitere Strategie, die nicht im Rahmen dieser Arbeit beschrieben ist, ist der Einsatz der kombinierten Zugangskontrolle als eine Art hybrides Systeme. Ein solches System nutzt einen, oder mehrere Mechanismen zur Auswahl der Person und einen oder mehrere andere zur anschließenden Verifikation. Hier wird bei der eigentlichen Authentisierung jeweils nur ein Referenzmuster mit den Sensordaten verglichen, so dass die Fehlerraten niedriger gehalten werden können. Das im Kapitel zur Umsetzung des Gesamtsystems beschriebene Sprachmodul basiert auf einer solchen Technologie, indem sequentiell erst der Benutzer bestimmt wird und anschließend ein zweites Sprachmuster zur Verifizierung herangezogen wird. Bei der Fusion der Authentisierungsergebnisse für die in dieser Arbeit beschriebenen multimodalen Systeme müssen solche Mechanismen jeweils als Einzelsystem betrachtet werden.

4.6.3 Auswerteverfahren und Inkompatibilitäten

So wie in dieser Arbeit die Kombinationen der booleschen Entscheidungen untersucht wurden, könnten auch die Entscheidungskriterien, die innerhalb der einzelnen Mechanismen zur Abweisung oder Akzeptanz geführt haben, fusioniert werden ([Brunelli 1995], [Fischholz 2000]). Dies Auswertung auf Integrationsebene wird von den meisten Mechanismen jedoch nicht unterstützt und ist somit mittels einfachen und kostengünstigen Lösungen schwer zu realisieren. Ebenfalls unberücksichtigt bleibt die Wahrscheinlichkeit, dass sich auf Grund ungeeigneter Merkmale durch einen Mechanismus keine Referenzmuster einer Person erzeugen lassen. Die FER (Failed Enrolment Rate) wird von Herstellern selten angegeben.

4.6.4 Einsatzmöglichkeiten

Multimodale Identifikationsverfahren können überall dort eingesetzt werden, wo eine Authentizitätsbestimmung notwendig ist. Vorteil dieser Technik ist unter anderem die

erhöhte Toleranz gegenüber natürlichen Änderungen biometrischer Merkmale. Entsprechende Kombinationsstrategien verringern hierfür die Falschabweisungsrate. Die sich ergebende Redundanz erlaubt innerhalb technischer Grenzen Ausfälle und Störungen zu kompensieren. In Umgebungen, wo ein Höchstmaß an Sicherheit gefordert ist, werden schon lange diverse Mechanismen zu einem System kombiniert. Im privaten Bereich, wo der Kostenfaktor eine entscheidende Rolle spielt, haben sich elektronische Systeme noch nicht großflächig durchsetzen können. Die Verknüpfung kosteneffizienter Systeme, die als monolithische Lösung die Ansprüche einer Zugangskontrolle kaum erfüllen, bietet hier den Ansatz diese Lücke zu schließen. Die einfache Konfigurierung mittels eines Kriteriums, das die geeignete Fusionsstrategie bestimmt, erlaubt auch nicht technisch versierten Personen ein solches System zu betreiben.

5 Gesicherte Datenübertragung

5.1 Sichere Sensornetzwerke

Bussysteme, wie sie heute im Zweck- und Wohnungsbau vermehrt Verwendung finden, zeichnen sich durch einfache Installation, robustes Datenübertragungsverhalten und eine Vielzahl von angepassten Sensor- und Aktorapplikationen für Beleuchtung, Klimatisierung und Medienanwendungen aus. Ein großer Nachteil der Bussysteme ist das Fehlen einer vor Missbrauch gesicherten Datenübertragung. Dies liegt daran, dass solche Systeme ursprünglich für einfache Steuerungsaufgaben entwickelt wurden, zu Zeiten, als die Leistungsfähigkeit von Mikrocontrollern noch verhältnismäßig gering war. So kam es, dass Systeme wie der EIB/KNX nie für sicherheitstechnische Anwendungen in Betracht gezogen wurde. Die Entwicklung der Powerline- und Funkübertragung für den EIB/KNX macht diesen noch anfälliger gegen Manipulationen.

Etliche Forscher und Entwickler haben diese Problematik in den letzten Jahren erkannt und arbeiten an Sicherheitsprotokollen für Sensornetzwerke. Ziel dieser Arbeiten ist es, eine gegen Missbrauch gesicherte Datenübertragung in selbstorganisierenden, meist drahtlosen Netzwerken zu realisieren [Perrig 2002]. Als Einschränkung gegenüber drahtgebundenen Feldbussen wird dabei die verhältnismäßig geringe Energieversorgung der Sensorknoten und die niedrigen Übertragungsraten gesehen. Anwendungsgebiete sind hier unter anderem Gefahrenmeldesysteme, Monitorsysteme für Vitalparameter sowie Logistiksysteme und militärische Anwendungen. Vorreiter dieser Technologie ist eine Sammlung von Protokollen mit der Bezeichnung SPINS (Security Protocols for Sensor Networks) [SPINS 2002]. SPINS beschreibt zwei Protokolle für die Anwendungsebene des OSI-Modells: SNEP und µTESLA. SNEP (Secure Network Encryption Protocol) gewährleistet Vertraulichkeit, Authentizität und Aktualität zwischen den Kommunikationspartnern, µTESLA realisiert einen authentischen Broadcast. Beide Systeme basieren auf dem symmetrischen Verschlüsselungsverfahren RC5 [Schneier 1996], welches neben der Schlüssel- und Blocklänge auch die Anzahl der zu durchlaufenden Runden als Parameter hat. Realisiert wurde das System auf sogenannten SmartDust-Sensorknoten, welche über, im Vergleich zu einem herkömmlichen PC, sehr eingeschränkte Ressourcen verfügen. In eine ähnliche Richtung gehen die Arbeiten der ZigBee-Alliance [ZigBee 2003]. Der als ZigBee bezeichnete Kurzstreckenfunk basiert auf dem IEEE-Standard 802.15.4. Er definiert verschiedene Übertragungsraten und bietet unter anderem die Möglichkeit zur symmetrischen Verschlüsselung per AES.

Das im folgenden vorgeschlagene Kommunikationsprinzip SEIB (Secure European Installation Bus) zur gesicherten Datenübertragung auf dem EIB/KNX wurde im Rahmen dieser Arbeit entwickelt. SEIB basiert teilweise auf SNEP, erweitert dieses aber um ein moderneres Verschlüsselungsverfahren und ist auf die für den EIB/KNX definierte, objektbezogene Kommunikationsstruktur angepasst.

5.2 Voraussetzungen

Eine der wichtigsten Voraussetzungen, Daten gesichert über den EIB/KNX übertragen zu können, ist es, das bestehende Kommunikationssystem nicht zu beeinträchtigen. Wie im Anhang beschrieben, erlaubt EIB/KNX prinzipiell zwei Verbindungsarten; die für den Betrieb wichtige, verbindungslose Kommunikation über Kommunikationsobjekte und die verbindungsorientierte Kommunikation für Konfigurationszwecke. Die Verarbeitung der Telegramme richtet sich dabei nach dem ISO/OSI-Referenzmodell (International Standard Organisation's Open System Interconnection Modell) (ISO 7498), so dass die Kommunikation über Linien- und Bereichskoppler hinweg möglich ist.

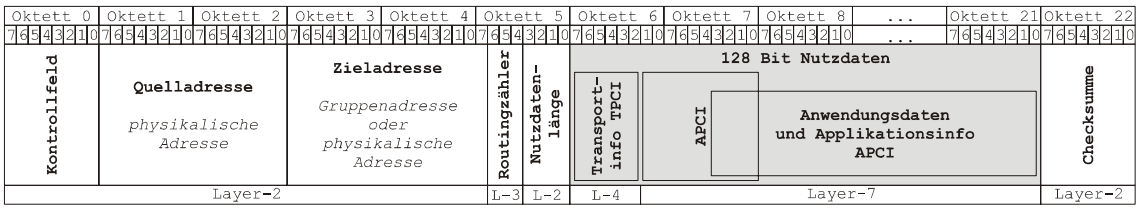

Abbildung 5.1: EIB/KNX Telegrammaufbau

Betrachtet man den in Abbildung 5.1 dargestellten Aufbau eines Standardtelegramms, so ist zu erkennen, dass obige Voraussetzung erfüllt werden kann, indem alle niederen Layer, bis einschließlich Layer-3, in herkömmlicher Weise zum Transport von Daten verwendet werden. Es gilt, die gesicherte Datenübertragung innerhalb des Transport- und Application-Layers (Layer-4 und Layer-7) zu realisieren. In diesem als NSDU (Network Service Data Unit) bezeichnetem Nutzdatenbereich können bis zu 16 Byte Daten übertragen werden. Die für Steuerungsaufgaben verwendete verbindungslose Kommunikation mit einem oder mehreren Partnern definiert zur Übertragung von Daten jeweils nur ein Telegramm, so dass in diesem sowohl die vor Missbrauch geschützte Information als auch ein Beweis für die Authentizität des Absenders enthalten sein muss. Das Aushandeln eines sicheren Übertagungskanals oder das Verwenden asymmetrischer Verschlüsselungsverfahren, welche eine beidseitige Kommunikation mit mehreren Telegrammen voraussetzen, kommen daher nicht in Frage. Diese Überlegungen führen dazu, ein symmetrisches Verfahren zu verwenden, welches nach heutigem Stand der Wissenschaft auch bei kleinen Schlüssel- und Blockgrößen höchsten Ansprüchen an die Sicherheit genügt.

5.3 Das AES Verschlüsselungsverfahren

Der Advanced Encryption Standard (AES) spezifiziert ein durch das Federal Information Processing Standard (FIPS) anerkanntes Verschlüsselungsverfahren [FIPS 197], welches entwickelt wurde, digitale Daten zu schützen und den bekannten Data Encryption Standard (DES) in Zukunft abzulösen. Der DES Algorithmus wird bereits

seit 1975 in unzähligen kryptographischen Anwendungen eingesetzt. Aufgrund diverser entwickelter Verfahren der differenziellen und linearen Kryptoanalyse, sowie der sich nach dem Moore'schen Gesetz alle 1½ Jahre verdoppelnden Rechenleistung, ist es mit handelsüblicher Hardware möglich, den Algorithmus innerhalb weniger Stunden zu knacken.

Der Rijndael Algorithmus [Daemen 2002] von Joan Daemen und Vincent Rijmen sowie 14 weitere Verschlüsselungsverfahren gingen 1998 aus einem dreijährigen Auswahlverfahren, welches durch das National Institute of Standards and Technology (NIST) initiiert wurde, hervor. Eine Gemeinde von anerkannten Kryptographen wählte daraus die besten 5 Kandidaten, aus denen das NIST im Jahre 2000 den Rijndael Algorithmus als den Advanced Encryption Algorithmus vorschlug. Ende 2001 wurde der Algorithmus veröffentlicht und tritt seither die Nachfolge des DES an.

5.3.1 Eigenschaften

Um am Auswahlverfahren teilnehmen zu können, mussten die eingereichten Algorithmen folgende minimale Eigenschaften erfüllen:

- Symmetrisches Verschlüsselungsverfahren mit geheimen Schlüssel (derselbe Schlüssel wird sowohl zum Ver- wie auch zum Entschlüsseln der Daten verwendet)
- Die Daten müssen blockweise in Größen von 128 Bit zu verschlüsseln sein
- Schlüssellängen von 128, 192 und 256 Bit müssen verwendbar sein
- Der zum AES gewählte Algorithmus darf in keiner Form geschützt werden, so dass er Lizenz- und Gebührenfrei von jedem eingesetzt werden kann

Einige weitere wichtige Kriterien mussten erfüllt werden um das etablierte DES-Verfahren, welches auch als 3DES (Tripple-DES) weiterentwickelt wurde, ablösen zu können:

- Resistenz gegen bekannte Angriffsverfahren
- Effektive und ressourcensparende Realisierbarkeit in Soft- und Hardware
- Realisierbar auf 8 Bit Plattformen (z.B. SmartCards und Low-Cost-Mikrocontroller)
- Keine schwachen Schlüssel, d.h. jede beliebige Schlüsselzahl ist gleich gut geeignet und muss nicht speziell generiert werden

- Laufzeitkonstant (Ver- und Entschlüsselungszeit ist unabhängig von der gewählten Schlüsselzahl und den Inhalten der Datenblöcke)

5.3.2 Die Zustandsmatrix

Da es sich beim AES um einen Blockalgorithmus handelt, werden die zu ver- bzw. entschlüsselnden Daten jeweils in Blöcke zu 128 Bit bzw. 16 Byte unterteilt und spaltenweise, wie in Abbildung 5.2 dargestellt, in einer Zustandsmatrix abgelegt.

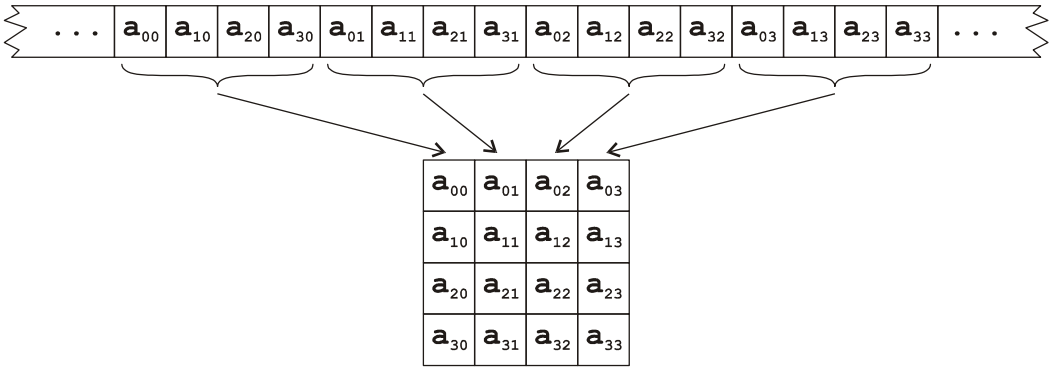

Abbildung 5.2: Aufbau der Zustandsmatrix

Der AES Algorithmus erlaubt mehrere Kombinationen aus Block- und Schlüssellänge. Gegenstand dieser Arbeit war stets eine Block- und Schlüssellänge zu je 128 Bit (AES-128), so dass im Folgenden nur der Algorithmus für diese Datengrößen beschrieben wird. Die Zustandsmatrix ist demnach in vier Spalten zu je vier Zeilen aufgebaut.

5.3.3 Mathematische Voraussetzungen

Alle Datenbytes, die innerhalb des AES Algorithmus verarbeitet werden, stellen Elemente eines endlichen Feldes dar, eines Galois-Feldes GF(2^8) [Lidl 1986]. Es können folglich nur die Zahlen 0 bis 255 enthalten sein. Ergebnisse aus Additionen oder Multiplikationen zweier Elemente GF(2^8) ergeben ebenfalls nur ein Element GF(2^8). Um dies sicherstellen zu können wird jedes Byte als ein Polynom mit Koeffizienten {0, 1} betrachtet, welche durch die Bits repräsentiert werden:

$$b_7 x^7 + b_6 x^6 + b_5 x^5 + b_4 x^4 + b_3 x^3 + b_2 x^2 + b_1 x + b_0 = \sum_{i=0}^{7} b_i x^i \qquad (5.1)$$

Bei einer Addition zweier solcher Polynome werden die Koeffizienten gleicher Potenz addiert, wobei bei der GF(2^8)-Arithmetik ein Übertrag zum nächst höheren Koeffizienten einfach unterdrückt wird (modulo 2). Es ist zu erkennen, dass es sich hierbei um

eine bitweise XOR-Verknüpfung (dargestellt durch $\oplus$) handelt. Folglich entspricht eine Addition auch genau einer Subtraktion. Hard- und softwaretechnisch ist die XOR-Operation sehr einfach und sehr schnell zu realisieren.

Eine Multiplikation (dargestellt durch $\bullet$) in der polynomischen Betrachtungsweise GF(2^8) hingegen entspricht im wesentlichen der Multiplikation von Polynomen, wobei das Endergebnis modulo einer binären Primzahl vom Grad 8 dividiert wird. Für den AES Algorithmus ist dies die Zahl 283_d. Das entsprechende Polynom ist definiert als:

$$m(x) = x^8 + x^4 + x^3 + x + 1 \tag{5.2}$$

Da diese Zahl vom Grad 8 ist, ist garantiert, dass das Moduloergebnis, also der Rest der Division, maximal vom Grad 7 ist und damit die Bedingung für GF(2^8) Elemente erfüllt ist. Die Multiplikation an sich ist einfach durch eine bitweise Verschiebung eines Faktors zu realisieren. Wenn der Koeffizient an entsprechender Stelle im zweiten Faktor das Element {1} enthält, wird das Ergebnis mittels einer XOR-Operation aufaddiert. Die abschließende Moduloberechnung besteht aus Subtraktionen des definierten Polynoms $m(x)$ durch XOR-Operationen, ausgehend vom höchstwertigen Bit der Multiplikation. Der verbleibende Rest ist dann das gesuchte Endergebnis.

```
Byte multiply (Byte a, Byte b)
{
      Byte position;
      Byte x = 0;

      for (position=0; position<8; position++)
      {
            if (b & 0x01)
            {
                  x = x ^ a;
            }
            b = b >> 1;
            if (a & 0x80)
            {
                  a = a << 1;
                  a = a ^ 0x1b;
            }
            else a = a << 1;
      }
      return x;
}
```

Abbildung 5.3: C-Code zur Berechnung der Multiplikationen

Bitschiebeoperationen sind in Hard- und Software ebenso einfach zu realisieren wie XOR-Operationen. Für die Multiplikation ist innerhalb dieser Arbeit der in Abbildung 5.3 gezeigte Quellcode entstanden, welcher auf einen möglichst geringen Speicher-

verbrauch optimiert ist. Um eine möglichst schnelle Abarbeitung zu garantieren, werden in den meisten AES Implementierungen zwei Tabellen generiert, aus denen mittels einer einfachen Operation das Ergebnis gelesen werden kann. Diese Tabellen benötigen zusammen aber mindestens 512 Byte Speicher, die in sehr kleinen Systemen nicht immer verfügbar sind.

5.3.4 Der Algorithmus

Ausgangspunkt für alle weiteren Operationen des Verschlüsselungsvorganges ist die Zustandsmatrix, an der in mehreren Durchgängen, hier auch als Runden bezeichnet, vier byteorientierte Transformationen ausgeführt werden. Diese sind nachfolgend genauer erklärt.

5.3.4.1 Byteweises Ersetzen (SubBytes)

Bei der SubBytes-Transformation handelt es sich um ein nichtlineares, byteweises Ersetzen jedes einzelnen Elements der Zustandsmatrix durch ein anderes GF(2^8) Element. Die Zuordnung ist durch die sogenannte S-Box gegeben. Abbildung 5.4 zeigt, wie jedes Element der Zustandsmatrix mittels der S-Box transformiert wird. Die S-Box, welche für den AES Algorithmus stets dieselbe ist, wird innerhalb des Programmcodes meist als festes Array von 256 Elementen gespeichert.

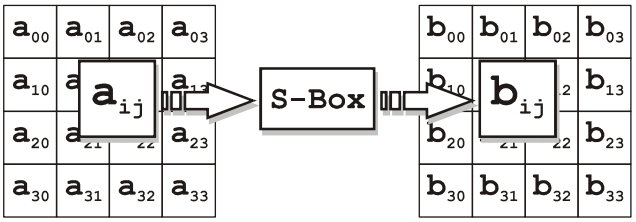

Abbildung 5.4: Ersetzen der Elemente der Zustandsmatrix

Die Designkriterien für die S-Box wurden unter anderem mit Hilfe der Betrachtung differentieller und linearer Kryptoanalysen aufgestellt und sind in [Daemen 2002] genauer beschrieben. Die einzelnen Elemente der S-Box ergeben sich aus zwei Transformationen. Mittels der ersten Transformation wird das multiplikativ inverse Element aus GF(2^8) gebildet, wobei das Nullelement stets auf sich selbst abgebildet wird. Die Transformation kann in Byte-Schreibweise folgendermaßen dargestellt werden:

$$b^{-1}(x) = a(x) \bmod m(x) \tag{5.3}$$

Die zweite Berechnungsvorschrift besteht aus einer affinen Transformation, welche folgend in Matrizenschreibweise angegeben ist:

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} b_0^{-1} \\ b_1^{-1} \\ b_2^{-1} \\ b_3^{-1} \\ b_4^{-1} \\ b_5^{-1} \\ b_6^{-1} \\ b_7^{-1} \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \tag{5.4}$$

Der umgekehrte Vorgang (InvSubBytes) besteht aus der inversen affinen Transformation gefolgt von einer multiplikativen Invertierung des Elements. Für diese inverse S-Box wird aus Performancegründen das entsprechend inverse Bytearray zur S-Box fest im Quellcode gespeichert.

5.3.4.2 Verschieben der Zeilen (ShiftRows)

Bei der ShiftRow-Transformation werden die Zeilen der Zustandsmatrix nach einem festen Schema zyklisch verschoben. Abbildung 5.5 verdeutlicht diesen Vorgang.

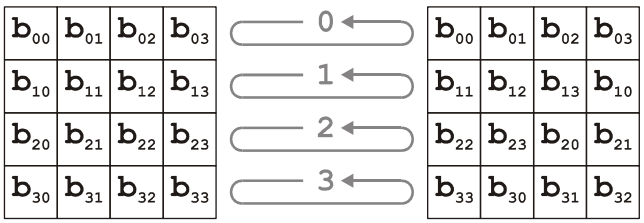

Abbildung 5.5: Verschieben der Zeilen in der Zustandsmatrix

Bei Blocklängen von 128 Bit, respektive einer Zustandsmatrix mit 16 Elementen, bleibt die erste Zeile unverändert, alle anderen werden jeweils um 1, 2 und 3 Positionen zyklisch nach links verschoben. Bei der umgekehrten Funktion (InvShiftRows), die zur Entschlüsselung verwendet wird, wird nach rechts verschoben.

5.3.4.3 Mischen der Spalten (MixColumns)

Bei der MixColumns-Transformation werden die vier Spalten der Zustandsmatrix unabhängig voneinander bearbeitet. Die Vektoren (Spalten) werden mit einem festem Polynom $p(x)$ modulo x^4+1 multipliziert.

$$p(x) = \{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\} \tag{5.5}$$

Der Vorgang kann für die Zustandsmatrix als Matrizenmultiplikation angegeben werden:

$$\begin{bmatrix} b'_{00} & b'_{01} & b'_{02} & b'_{03} \\ b'_{10} & b'_{11} & b'_{12} & b'_{13} \\ b'_{20} & b'_{21} & b'_{22} & b'_{23} \\ b'_{30} & b'_{31} & b'_{32} & b'_{33} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \bullet \begin{bmatrix} b_{00} & b_{01} & b_{02} & b_{03} \\ b_{10} & b_{11} & b_{12} & b_{13} \\ b_{20} & b_{21} & b_{22} & b_{23} \\ b_{30} & b_{31} & b_{32} & b_{33} \end{bmatrix} \tag{5.6}$$

Am Beispiel des ersten Elements der Zustandsmatrix ist die Operation auf Basis der XOR-Verknüpfung zu sehen:

$$b'_{00} = \begin{bmatrix} 02 & 03 & 01 & 01 \end{bmatrix} \bullet \begin{bmatrix} b_{00} \\ b_{10} \\ b_{20} \\ b_{30} \end{bmatrix} = 2 \bullet b_{00} \oplus 3 \bullet b_{10} \oplus 1 \bullet b_{01} \oplus 1 \bullet b_{30} \tag{5.7}$$

Das Polynom wurde so gewählt, dass die Matrizenmultiplikation mit der inversen Matrix bei der Datenentschlüsselung (InvMixColumns) die Zustandsmatrix wiederherstellt. Diese muss selbstverständlich GF(2^8) konform gebildet werden und lautet:

$$P^{-1} = \begin{bmatrix} 14 & 11 & 13 & 09 \\ 09 & 14 & 11 & 13 \\ 13 & 09 & 14 & 11 \\ 11 & 13 & 09 & 14 \end{bmatrix} \tag{5.8}$$

5.3.4.4 Addieren des Rundenschlüssels (AddRoundKey)

Die vierte und letzte Transformation der Zustandsmatrix ist die sogenannte AddRoundKey-Operation. Hierbei werden die 16 Elemente der Zustandsmatrix bitweise XOR verknüpft mit einem Rundenschlüssel, der individuell für jede Runde im Algorithmus aus dem eigentlichen geheimen Schlüssel erzeugt wird. Hierbei wird der Schlüssel (hier 128 Bit) auf dieselbe Weise wie die Datenblöcke (Abbildung 5.2) in Spalten aufgeteilt, von denen jeweils vier Spalten eine Schlüsselmatrix ergeben. Die erste zu verwendende Schlüsselmatrix *K*[0] ist identisch mit dem geheimen Schlüssel, alle weitern ergeben sich durch die Schlüsselerweiterung. Abbildung 5.6 zeigt die in dieser Arbeit verwendete Implementierung zur Erweiterung der Rundenschlüssel. Diese Funktion kann verwendet werden, ohne alle Schlüssel vorher berechnen zu müssen.

Um Speicher zu sparen kann der Algorithmus, bei Übergabe der Rundenzahl, direkt die Zustandsmatrix bearbeiten. Hierbei werden neue Vektoren (Spalten der Schlüsselmatrix) durch eine Transformation mit der S-Box (siehe 5.3.4.1), einer zyklischen Rotation der Vektorelemente sowie der Addition einer Rundenkonstante im Element 0 des vorherigen Vektors erzeugt.

```
addroundkey(Byte *block, Byte *key, Byte round)
{
      const Byte rcon[11] = {1,2,4,8,16,32,64,128,27,54,108};
      Byte roundkey[16], r, t;

      for (t=0; t<16; t++) roundkey[t] = key[t];

      for (t=0; t<round; t++)
      {
            vector[0] = sbox[roundkey[13]]^rcon[t];
            vector[1] = sbox[roundkey[14]];
            vector[2] = sbox[roundkey[15]];
            vector[3] = sbox[roundkey[12]];

            for (r=0; r<4; r++)
            {
                  vector[0] = roundkey[0+4*r]^vector[0];
                  vector[1] = roundkey[1+4*r]^vector[1];
                  vector[2] = roundkey[2+4*r]^vector[2];
                  vector[3] = roundkey[3+4*r]^vector[3];
                  roundkey[0+4*r] = vector[0];
                  roundkey[1+4*r] = vector[1];
                  roundkey[2+4*r] = vector[2];
                  roundkey[3+4*r] = vector[3];
            }
      }
      for (t=0; t<16; t++) block[t] block[t]^roundkey[t];
}
```

Abbildung 5.6: C-Code zur Erweiterung der Rundenschlüssel

Die Rundenkonstante ergibt sich aus 2^{i-1}, wobei die Zahlen aber innerhalb der Menge $GF(2^8)$ bleiben. Die anderen drei Vektoren einer Schlüsselmatrix werden aus XOR-Verknüpfungen des jeweils vorherigen Vektors und dem Vektors an selbiger Stelle der vorigen Schlüsselmatrix gebildet. In den original Beschreibungen des Rijndael Algorithmus werden diese Vektoren als 4 Byte Worte betrachtet, die gespeichert in einem linearen, eindimensionalen Array mit 4 Elementen einen Rundenschlüssel darstellen.

5.3.4.5 Die Ver- und Entschlüsselung

Wie bereits oben erwähnt durchlaufen die zu verschlüsselnden Daten, in Form der Zustandsmatrix, die vier Operationen (SubBytes, ShiftRows, MixColumns und AddRoundKey) in mehreren Runden (Abbildung 5.7).

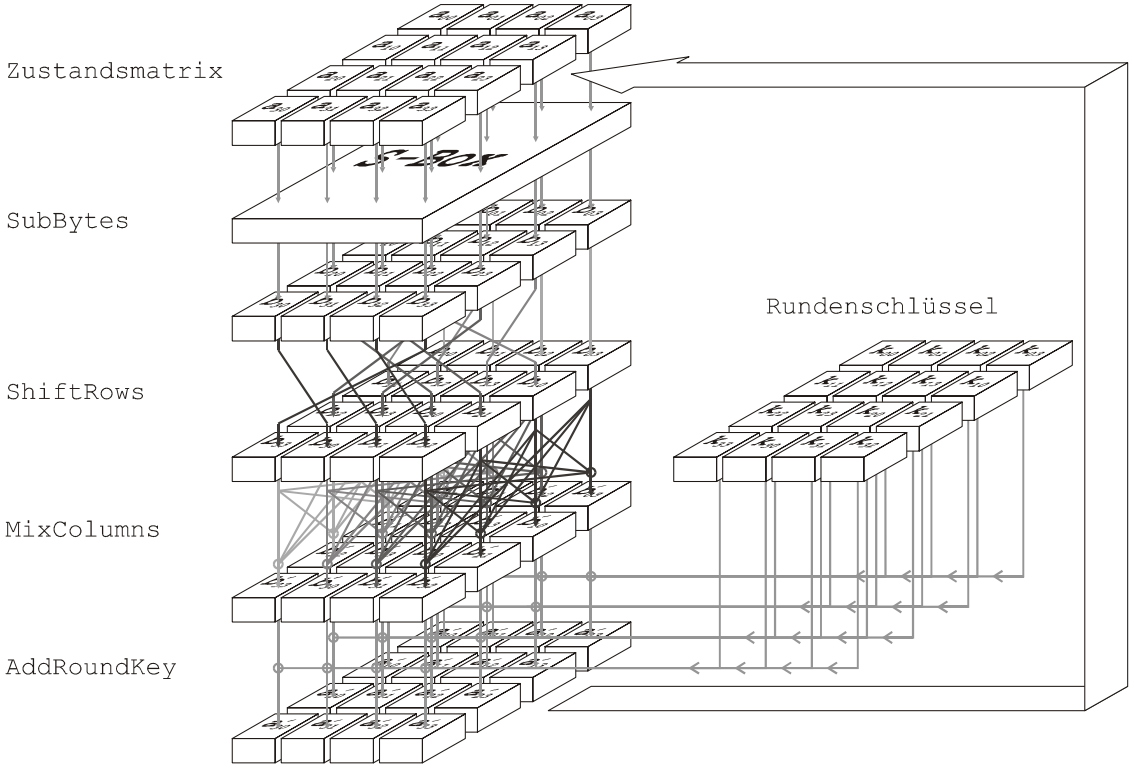

Abbildung 5.7: Grafische Darstellung einer AES-128 Verschlüsselungsrunde

Die Anzahl dieser Durchläufe ist beim AES-Algorithmus abhängig von der Schlüssellänge. Die in dieser Arbeit verwendete Schlüssellänge von 128 Bit erfordert 10 Durchläufe. Eingeleitet wird das Verschlüsselungsverfahren mit einer AddRoundKey-Operation, danach folgen 10 Runden in denen jeweils alle vier Operationen in obiger Reihenfolge durchlaufen werden. Nur in der letzten Runde wird keine MixColumns-Transformation ausgeführt. Abbildung 5.8 zeigt einen Pseudo-Quellcode zur Verschlüsselung der Zustandsmatrix.

Das verschlüsselte Endergebnis steht abschließend wieder in Form einer Matrix zur Verfügung. In der Programmiersprache C wird in der Regel ein Zeiger, oder in Java eine Instanz eines Objektes der Zustandsmatrix, an die vier Transformationsfunktionen übergeben. Der Entschlüsselungsvorgang entspricht von der Vorgehensweise der Verschlüsselung, nur dass der Ablauf und die Reihenfolge exakt umgekehrt durchlaufen werden. Bis auf die AddRoundKey-Operation, bei der die Rundenzahl von 10 abwärts gezählt wird, werden jeweils die invertierten Funktionen (InvSubBytes, InvShiftRows und InvMixColumns) verwendet.

```
// 128 Bit AES Verschlüsselung
begin

      AddRoundKey(Zustandsmatrix, K[0])

      for round = 1 to 9
            SubBytes(Zustandsmatrix)
            ShiftRows(Zustandsmatrix)
            MixColumns(Zustandsmatrix)
            AddRoundKey(Zustandsmatrix, K[round])
      end for

      SubBytes(Zustandsmatrix)
      ShiftRows(Zustandsmatrix)
      AddRoundKey(Zustandsmatrix, K[10])

end
```

Abbildung 5.8: Pseudo-Quellcode zur Datenverschlüsselung

5.3.5 Stärken des Verfahrens

Seit der Veröffentlichung des AES-Verfahrens bemühen sich zahlreiche Kryptoanalytiker darum, Methoden zu finden, den Algorithmus zu „knacken“. Dies bedeutet, eine Methode zu entwickeln, die es erlaubt, mit vertretbaren Mittel innerhalb einer vertretbaren Zeit den richtigen geheimen Schlüssel zu finden. Geht man von einem perfekten Algorithmus aus, ist die Stärke des Verfahrens direkt proportional zur Länge des verwendeten Schlüssels. Das bedeutet, wenn er nicht anders lösbar ist, muss der Angreifer alle möglichen Schlüssel durchprobieren, um verschlüsselte Daten zu dechiffrieren (Brute-Force Attacke). Bei einer Schlüssellänge von 128 Bit sind dies $2^{128} \approx 3{,}4 \cdot 10^{38}$ mögliche Schlüssel. Geht man davon aus, dass etwa 700 Instruktionen (300 für das Erweitern des Schlüssels und 400 für die Entschlüsselung selbst) notwendig sind um einen Schlüssel zu testen, müsste der Höchstleistungsrechner, der im Jahre 2005 am Leibnitz Rechenzentrum in München in Betrieb gehen soll, mit einer Spitzenleistung von 40 TFlop/s, knapp $1{,}9 \cdot 10^{20}$ Jahre rechnen, um alle Kombinationen zu testen.

Die zum derzeitigen Stand aktuellste Methode, mit Aussicht auf Erfolg, ist die sogenannte XSL-Methode der beiden Mathematiker Nicolas Courtois und Josef Pieprzyk [Courtois 2002]. Sie konzentrieren sich auf die S-Box, die für die Unvorhersehbarkeit der verschlüsselten Daten zuständig ist, und beschreiben ganze Klassen von Chiffrierungen mittels sehr großer Systeme quadratischer Gleichungen. Bei AES-128 sind dies 8000 Gleichungen mit 1600 Variablen. Derartige Systeme lassen sich im Allgemeinen nicht mit vertretbarem Rechenaufwand lösen, doch in diesem Fall sind starke Vereinfachungen mittels der XSL-Methode möglich. Sie nutzt aus, dass die

Gleichungssysteme überbestimmt und schwach besetzt sind mit einer besonders regulären Struktur. Es ist denkbar, auf diese Weise den Rechenaufwand auf etwa 2^{100} Rechenoperationen zu reduzieren, was in einigen Jahren möglicherweise in vertretbarer Zeit ausgeführt werden kann.

Insgesamt ist die Sicherheit des Algorithmus bei Kryptoanalytikern noch umstritten, obwohl keine der bekannten linearen und differentiellen Kryptoanalysen sowie weitere bekannte Attacken mehr als 7 Runden brechen kann (10 Runden werden bei AES-128 angewendet). Der AES Chiffrierungsalgorithmus eignet sich auf Grund seiner Einfachheit, Sicherheit und freien Verfügbarkeit besonders für die im folgenden vorgestellte Methode zur gesicherten Datenübertragung.

5.4 Das SEIB-Kommunikationsprotokoll

Das SEIB-Kommunikationsprotokoll, welches im Rahmen dieser Arbeit entstand, realisiert die Vertraulichkeit, Authentizität, Integrität und Aktualität der übertragenen Nachrichten. Dies wird mit Hilfe von symmetrischen Verschlüsselungs- und Prüfoperationen erreicht. Da in Sensorknoten in der Regel nur eine geringe Menge Speicherplatz und eine relativ geringe Rechenleistung zur Verfügung stehen, ist die Minimierung des Programmcodes und die Optimierung des Rechenaufwandes eine wichtige Aufgabe. Daher wird bei SEIB nur ein kryptographischer Algorithmus zur Schlüsselgenerierung und Verschlüsselung, sowie als Pseudozufallszahlengenerator, ähnlich dem SNEP-Protokoll, verwendet. Dies ist in diesem Fall der AES-128 Standard, mit einer Schlüssel- und Blocklänge von 128 Bit. Zur Bildung einer Checksumme, welche zusammen mit der Verschlüsselung für die Integrität und Authentizität sorgt, dient ein CRC (Cyclic Redundancy Code) unter Verwendung eines geeigneten Generatorpolynoms.

5.4.1 Notation

Folgende Notation dient zur Beschreibung des Protokolls und der verwendeten kryptographischen Operationen:

- A und B stellen zwei Kommunikationspartner dar
- $A \rightarrow B : M$ Übertragung der Nachricht M von A nach B
- M ist die zu übermittelnde Nachricht
- $M_1 \mid M_2$ stellt die Konkatenation zweier Nachrichten dar
- K beschreibt einen symmetrischen Schlüssel K
- $\{M\}_{(K,C)}$ ist die verschlüsselte Nachricht M unter Verwendung des Schlüssels K und eines Parameters C

- $CRC(M)$ beschreibt das Bilden einer Checksumme über die Nachricht M

5.4.2 Kommunikationsprinzip

SEIB basiert, ähnlich wie es bei anderen Protokollen gehandhabt wird, auf einem Zähler, der in die Verschlüsselung der Sensordaten mit einbezogen wird. Dieses variable Element sorgt dafür, dass Telegramme, die dieselbe Information transportieren, bei jeder Übertragung für einen potentiellen Angreifer unterschiedlich aussehen. Die Größe dieser Zählvariable bestimmt dabei die maximale Anzahl unterschiedlicher Telegramme. Voraussetzung für eine gegen Replay-Attacken[1] gesicherte Übertragung, ist die einmalige Verwendung eines jeden Zählwertes. Dies entspricht dem One-Time-Pad Prinzip [Schneier 1996]. Der Zählraum der Variable sollte dabei so groß gewählt werden, dass während der Lebenszeit eines Netzwerkknotens niemals derselbe Wert zweimal benutzt wird. Wichtig für die Kommunikation zweier oder mehrerer Knoten ist die Verwaltung synchroner Zähler. Der Wert muss dabei nach einer festen Regel für jedes Telegramm geändert werden. In dem hier vorgestellten Verfahren reicht das einfache Inkrementieren des Wertes, nachdem ein Telegramm erfolgreich bei allen Teilnehmern empfangen wurde. Das eingesetzte Verschlüsselungsverfahren garantiert dabei die statistische Gleichverteilung über die Blockgröße, so dass Rückschlüsse auf einen Zählerstand durch Angreifer nicht möglich sind.

Durch die Datenverschlüsselung wird die Vertraulichkeit realisiert. Das bedeutet, dass ein Angreifer, ohne Kenntnis des geheimen Schlüssels, keinen Rückschluss auf die gesendeten Informationen ziehen kann. Da in EIB/KNX-Netzwerken überwiegend Steuerungsinformationen übermittelt werden, ist es ebenso wichtig, die Authentizität und Integrität zu gewährleisten. Eine einfache Aktualität der Daten wird unter anderem durch das Einbeziehen des Zählerwertes in die Verschlüsselung realisiert. Auch das Bilden von Plaintext-Krypttext[2] Paaren wird durch den Zähler verhindert. Unter Kenntnis der übermittelten Daten, welche oft nur ein einziges Steuerbit darstellen, können leicht Plaintext-Krypttext Paare generiert werden. Eine große Anzahl solcher Informationen könnte zur Berechnung des geheimen Schlüssels verwendet werden.

Einem Angreifer ist es zu diesem Zeitpunkt aber noch möglich, gefälschte Telegramme in das Netzwerk einzuspeisen, welche durch Netzwerkknoten fehlinterpretiert werden. Dies würde zwar nicht zu einem gewünschten Ergebnis führen, aber mit Sicherheit einen Schaden anrichten. Die Daten müssen zusätzlich eindeutig mit einer Signatur

---

[1] Replay-Attacken stellen Angriffe dar, bei denen gesendete Telegramme aufgezeichnet und zu einem späteren Zeitpunkt in das Netzwerk wieder eingespeist werden.

[2] Ein Plaintext-Krypttext Paar besteht aus einer unverschlüsselten und zugehörig verschlüsselten Nachricht. Je nach Stärke des Verschlüsselungsalgorithmus kann es möglich sein, aus einer bestimmten Anzahl solcher Paare den geheimen Schlüssel zu berechnen.

gekennzeichnet werden. Im SNEP-Protokoll wird hierzu eine mit dem Zähler verknüpfte MAC-Signatur (Message Authentication Code) über die gesamten verschlüsselten Daten gebildet. Diese Signatur authentisiert eindeutig den Absender und garantiert die Integrität der Daten.

Da in EIB/KNX Telegrammen nur 16 Byte Nutzdaten übermittelt werden können, abgesehen von Long-Data-Frames, welche nicht durch die Standardkommunikation definiert sind, wird der gesamte Bereich durch die AES-128 Verschlüsselung ausgenutzt. Es gilt, einen Mechanismus zu finden, die Authentizität und Integrität innerhalb der verschlüsselten Daten zu realisieren. Hierzu ist es notwendig, einen Teil des Nutzdatenbereichs für die Bildung einer Art von Signatur zu reservieren, welche im Wesentlichen aus einer Checksumme besteht. Die Größe, die hierfür verwendet wird, steht in direktem Bezug zur Anzahl möglicher Kollisionen, die sich durch die Abbildung der Daten auf die im Verhältnis kleinere Signatur ergeben. Diese Signatur dient dem Empfänger dazu, nach Entschlüsselung der Nachricht ihre Integrität und somit auch die Authentizität des Senders zu prüfen.

Eine sinnvolle Kombination aller Mechanismen erfordert für diese Arbeit im Wesentlichen zwei nur den rechtmäßigen Kommunikationspartnern bekannte Elemente. Dies ist ein symmetrischer Schlüssel K_{encr}, der unter Einbeziehung eines Zählers (CTR Counter-Modus) zur Ver- und Entschlüsselung der Telegramme dient, sowie ein pseudozufälliger Initialwert C_{init}, der bei der Inbetriebnahme des Netzwerkes als Startwert des Zählers verwendet wird. Ein potentieller Angreifer hat somit keine Möglichkeit nach einem Neustart des Netzwerkes auf die Zählvariable zu schließen. Um in diesem Fall das Wiedereinspielen bereits aufgezeichneter Telegramme nach einem Neustart zu Verhindern, ist es notwendig, jeweils einen neuen Initialwert zu vergeben. Im Abschnitt zur Implementierung des Systems wird eine entsprechende Vorgehensweise beschrieben.

Es ist möglich, die oben genannten zwei Elemente durch einen einzigen, für alle Teilnehmer bekannten Wert zu realisieren. Dies entspricht aber nicht der Vorgehensweise für kryptographische Systeme, da bei Bekanntwerden eines dieser Schlüsselwerte durch mögliche erfolgreiche Angriffe alle Mechanismen außer Kraft gesetzt werden. Deshalb werden hier, nach dem Prinzip aus SNEP, die zwei relevanten Werte K_{encr} und C_{init} aus einem Hauptschlüssel K_{master} gewonnen. Dies hat zudem den Vorteil, dass in jedem Netzwerkknoten nur ein Schlüssel verwaltet werden muss. Die entsprechende Methode wird im nächsten Abschnitt beschrieben.

Unter der Voraussetzung dass M die zu übertragenden Daten darstellen und C der aktuell berechnete Zählwert ist, lässt sich die zu übertragende Nachricht folgendermaßen beschreiben:

$$A \rightarrow B : \{M \mid CRC(M)\}_{(K_{encr}, C)} \tag{5.9}$$

Auf diese Weise lassen sich die im Kapitel 3 analysierten Eigenschaften zur gesicherten Datenübertragung in EIB/KNX-Systemen effektiv umsetzen:

- **Vertraulich** Die Verschlüsselung der gesamten Daten mittels K_{encr} verhindert das Lesen der Informationen durch Angreifer, wobei das Einbeziehen des Zählers Replay-Angriffe unmöglich macht.
- **Integer** Durch die Bildung einer Checksumme über die gesendeten Daten kann der Empfänger die Integrität der Daten prüfen.
- **Authentisch** Dadurch, dass die gebildete Checksumme innerhalb des verschlüsselten Datenbereichs übertragen wird, bildet diese somit eine Art Signatur, die den Absender authentisiert.
- **Dezentral** Ein oder mehrere Empfänger im Netzwerk können, unter Kenntnis des Schlüssels K_{master}, nach dem Prinzip der Gruppenkommunikation im EIB/KNX erreicht werden, solange sie am Multicast-Verfahren teilnehmen und ihren Zähler synchronisieren.
- **Unidirektional** Da alle Informationen innerhalb eines Telegramms während des Betriebes übertragen werden können, bleibt das Kommunikationsprinzip des EIB/KNX vollständig erhalten. Die Buslast wird, je nach Anwendungsfall, nur geringfügig erhöht, da stets Telegramme maximaler Länge übertragen werden.

5.5 Implementierung

Nachfolgend wird beschrieben wie die einzelnen Teile des SEIB-Protokoll auf Basis des AES-128 Verschlüsselungsverfahren effektiv zu realisieren sind.

5.5.1 Schlüsselgenerierung

Der Schlüssel K_{encr}, sowie der Initialzählerwert C_{init} werden aus dem Hauptschlüssel K_{master} generiert. Dies wird nach dem in SNEP angewendeten Prinzip realisiert, indem der Hauptschlüssel als Schlüsselinput einer AES-Verschlüsselung eingesetzt wird. Nacheinander werden zwei konstante Werte (1 und 2) verschlüsselt, so dass die zwei

entstandenen Kryptblöcke zu je 128 Bit als Schlüssel und Zähler verwendet werden können. Der Vorgang kann entsprechend beschrieben werden:

$$K_{encr} = \{1\}_{(K_{master})} \tag{5.10}$$

$$C_{init} = \{2\}_{(K_{master})} \tag{5.11}$$

Auf diese Weise werden zwei voneinander unabhängige Werte erzeugt. Selbst wenn einer dieser Werte durch Analysen der Datenübertragung bekannt wird, ist es auf Grund der Stärken des AES-Verfahrens [Daemen 2002], nach derzeitigem Stand der Wissenschaft, nicht möglich, Rückschlüsse auf den Hauptschlüssel zu ziehen. Jeder Netzwerkknoten muss bei der Inbetriebnahme oder nach einem Schlüsseltausch diese Operation einmal durchführen. Es ist hier auch möglich, andere Zahlenwerte zu verschlüsseln, solange alle Knoten dieselben Werte verwenden. Dies ändert aber nichts an der Qualität des erzeugten Schlüssels und des Zählers.

5.5.2 Datenverschlüsslung

Datenverschlüsselung wird bei SEIB eingesetzt, um die Vertraulichkeit der Nachrichten zu gewährleisten. Zur Verschlüsselung wird auch hier AES-128 im Stromchiffrier-Modus eingesetzt. Der Output der AES-Funktion wird dabei mit dem Klartext, hier der EIB/KNX Nutzdatenbereich, bitweise addiert [Schneier 1996]. Dies entspricht dem One-Time-Pad-Prinzip, welches hier nur kryptographisch sicher ist, da der Output von AES pseudozufällig ist. Abbildung 5.9 zeigt den detaillierten Vorgang der Ver- und Entschlüsselung.

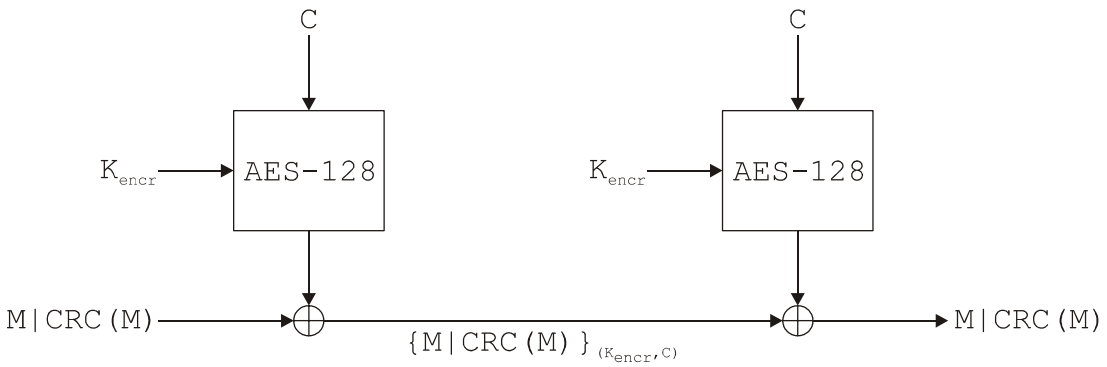

Abbildung 5.9: Stromchiffrierung im Counter-Modus

Wie man der Abbildung entnehmen kann, wird der Klartext *M* nicht an den AES-Algorithmus übergeben. Statt dessen benutzen beide Kommunikationspartner den Zähler *C*, der nach dem erfolgreichen Empfang einer Nachricht inkrementiert wird. Bei einem Überlauf des Zählers beginnt der Zählvorgang bei Null, so dass auf Grund der

Größe des Zählers von 128 Bit bis zu $2^{128} \approx 3{,}4 \cdot 10^{38}$ variable Elemente erzeugt werden können. Bei einer Übertragungsrate von 9600 Bit/s übersteigt dies bei weitem jede Lebenszeit einer EIB/KNX-Installation. Mit dieser Technik wird erreicht, dass einerseits jede Nachricht ein anderes Chiffrat zur Folge hat, selbst wenn der Inhalt gleich ist, und andererseits die Ent- und Verschlüsselungsoperationen identisch sind. Dafür müssen allerdings beide Kommunikationspartner denselben Zählerwert haben, die Zähler müssen synchron sein. Die Synchronisation der Zähler kann nur dann gefährdet werden, wenn eine oder mehrere Nachrichten zwischen Sender und Empfänger verloren gehen. Gehen nur einige wenige Nachrichten verloren, so können die beiden Kommunikationspartner die Zähler wieder re-synchronisieren, indem sie eine vorher bestimmte Anzahl nächst größere Zählerwerte testen.

Die oben gezeigte Methode der sogenannten Stromchiffrierung bietet zwei Vorteile für die Performance der Netzknoten; da sich während des Betriebes der Schlüssel K_{encr} nicht verändert, müssen die im AES verwendeten Rundenschlüssel nur einmal generiert werden und da nur der Zähler C zu verschlüsseln ist, können ein oder mehrere Werte bereits im Voraus, zum Beispiel währende der Übertragungsphase von Telegrammen berechnet werden.

5.5.3 Signaturbildung

Wie bereits erwähnt, ist es im Rahmen dieser Arbeit notwendig, eine möglichst eindeutige Signatur über die zu sendenden Daten zu bilden. Auf Grund der Rahmenbedingungen, die durch die Größe des Nutzdatenbereichs, des verwendeten Verschlüsselungssystems und des EIB/KNX-Kommunikationsprinzips gegeben sind, muss die Signatur innerhalb des Nutzdatenbereichs eingebracht werden. Daraus ergibt sich eine Einschränkung der Größe der Signatur und des Bereichs, in dem die eigentlichen Nutzdaten transportiert werden. Da in den Anwendungsfällen, für die die gesicherte Übertagung konzipiert ist, fast ausschließlich kurze Steuerungsinformationen (z.B. Türöffner-Signalisierung) oder Zustandsmeldungen von Gefahrenmeldern übertragen werden, ist diese Einschränkung akzeptabel.

Als Verfahren zur Feststellung der Integrität kommt ein CRC-Prinzip mit einer Größe von 32 Bit zum Einsatz [Tanenbaum 2002]. Das CRC-32 Prinzip basiert auf folgendem Generatorpolynom und findet unter anderem Anwendung bei der Bildung von Checksummen bei der Datenübertragung im Ethernet oder der Integritätsprüfung bei PKZIP-Dateien:

$$g(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1 \qquad (5.12)$$

Das Bilden einer solchen CRC-Checksumme kann sowohl in Hard- als auch Software sehr leicht umgesetzt werden und stellt keine hohen Ansprüche an die dafür notwendigen Ressourcen. Im Gegensatz zu Hash-Algorithmen oder der Verwendung kryp-

tographischer Funktionen im CBC-Modus (Cipher-Block-Chaining-Modus) kann mit einem CRC leicht ein 32 Bit Wert erzeugt werden, der zur Prüfung der Integrität im Rahmen der gesicherten Datenübertragung im EIB/KNX herangezogen wird.

Die anschließende Verschlüsselung der gesamten Nachricht, einschließlich der CRC-Checksumme, führt automatisch zur Authentisierung, da sich nur unter Kenntnis des geheimen Schlüssels die CRC-Checksumme aus den empfangenen Daten rekonstruieren und mit der neuberechneten CRC über die Nutzdaten vergleichen lässt. Im Folgenden wird diese als CRC-Signatur bezeichnet. Zur Bildung der CRC-Signatur werden die 12 Byte Nutzdaten (Oktett 6 bis 17) mittels eines CRC-Algorithmus und dem Generatorpolynom $g(x)$ verrechnet. Abbildung 5.10 zeigt, wie die Signatur in die Network Service Data Unit des EIB/KNX-Telegramm eingebettet ist.

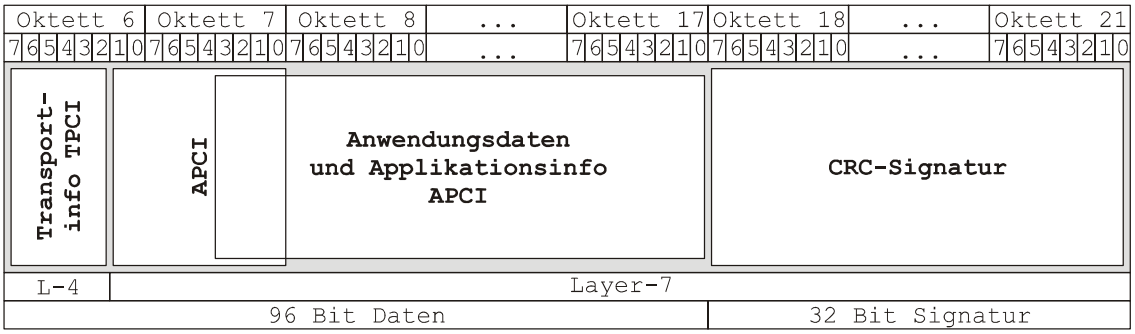

Abbildung 5.10: EIB/KNX-Nutzdatenbereich (NSDU)

Kryptographisch betrachtet bietet diese Form eines Hash-Wertes keine sehr umfassende Sicherheit. Dadurch, dass 96 Bit Daten auf 32 Bit Checksumme abgebildet werden, kommt es zu einer großen Anzahl von sogenannten Kollisionen, also gleichen Signaturen für verschiedene Daten. Manipulationen an den Daten sollen vordergründig erkannt werde, wohingegen eine Korrektur von Daten in dieser Anwendung keine Rolle spielt. Solange ein potentieller Angreifer keine Kenntnis über geheime Schlüssel oder irgendwelche Zählerstände hat, besteht eine Attacke darin, mittels Zufallsdaten eine gültige Signatur zu erzeugen, um das System mit falschen Informationen zu stören. Im einfachsten Fall, um einen mehrfachen Angriff mit denselben Daten zu vermeiden, reicht es, immer dasselbe Telegramm zu senden. Der Zähler, der mit der Verschlüsselung verknüpft ist, wird das Telegramm bei der Entschlüsselung im Empfänger in jeweils neue, sich nicht wiederholende Daten umrechnen. Für einen guten Hash-Algorithmus, mit einer Blockgröße von r Bit, ergibt sich die Wahrscheinlichkeit p für die Bildung einer gültigen Signatur bei n Versuchen folgendermaßen:

$$p(n) = n \cdot 2^{-r} \tag{5.13}$$

Im ursprünglichen Ansatz zu dieser Arbeit kam ein 16 Bit CRC zum Einsatz, dessen Größe aber eine Beeinflussung des Netzwerkes innerhalb eines kleinen Zeitraums mit

hoher Wahrscheinlichkeit ermöglicht. Sicherlich spielt auch die Wahl eines geeigneten Generatorpolynoms für die Bildung einer CRC-Checksumme eine Rolle bei der Anzahl möglicher Kollisionen. Das hier eingesetzte Polynom, welches für die meisten 32 Bit Summen angewendet wird, ist entsprechend entwickelt, bei typischen kleinen Manipulationen (1 Bit und 2 Bit Änderungen) und häufigen Übertragungsfehlern, sogenannten Bursts, Mehrfachbitfehler in der Größenordnung des Generatorpolynoms, keine Kollisionen zu erzeugen. Bezogen auf das Anwendungsgebiet des EIB/KNX und dessen niedrige Übertragungsraten, stellt das beschriebene Verfahren gegenüber allen anderen bekannten Sicherheitsmechanismen dieses Gebäudebussystems derzeit die sicherste Variante für die Übertragung sensibler Daten dar.

Die bereits in [Westermeir 2001b], [Westermeir 2001c] und [Westermeir 2001d] vorgestellte Methode zur gesicherten Übertragung von Daten auf dem EIB/KNX basierte auf einem synchronen Zähler, der innerhalb des Nutzdatenbereichs statt der Signatur eingebettet wurde. Die Überprüfung des synchronen Zählerstandes bietet ein ähnliches Maß für die Integrität und, zusammen mit der Verschlüsselung, für die Authentizität der Daten. Replay-Angriffe würden durch diese Technik aber deutlich einfacher möglich, da sich bereits nach 2^{32} Telegrammen die Zählerstände wiederholen.

5.5.4 Synchronisation

Zur Synchronisation der Zähler dient vor allem der Initialzählerwert C_{init}, der wie oben beschrieben aus dem Hauptschlüssel K_{master} generiert wird. Für das vorgeschlagene Kommunikationsprinzip ist es nicht ratsam, nach einer Unterbrechung der Stromzufuhr oder nach einem servicebedingtem Abschalten des Netzwerkes wieder mit dem Initialwert zu zählen zu beginnen. Dies könnte sehr leicht für Replay-Attacken missbraucht werden. Hierfür bieten Standard Buskoppler beziehungsweise die in Kapitel 6 definierte Hardware die Möglichkeit, bei Verlust der Busspannung für einen kurzen Zeitraum Kommandos auszuführen, um den Busknoten in einen definierten Zustand zu versetzen. Hier muss der aktuelle Zählerstand in einen nichtflüchtigen, gegen Auslesen geschützten Speicherbereich übertragen werden. Das Generieren und Einstellen eines Initialwertes ist somit nur nach dem Austauschen des Hauptschlüssels notwendig. Diese Prozedur ist grundsätzlich bei einer Erstinbetriebnahme erforderlich.

5.5.5 Re-Synchronisation

Die Re-Synchronisation stellt eine Maßnahme dar, bei der ein Buskoppler versucht, seinen Zählwert an die laufende Kommunikation anzupassen. Dies kann notwendig sein, wenn durch Übertragungsfehler oder aus Performancegründen ein oder mehrere Telegramme, die an eine relevante Adresse gesendet wurden, vom Empfänger nicht bearbeitet wurden. Der Empfänger erkennt dies an ungültigen Signaturen und kann durch Austesten einer vorher bestimmten Anzahl nächsthöherer Zählwerte versuchen, wieder an der Kommunikation teilzunehmen.

5.5.6 Routing und Adressierung

Die in Abbildung 5.11 dargestellten Kommunikationsebenen verdeutlichen, wo im ISO/OSI-Layer-Modell die Datenverschlüsselung stattfindet.

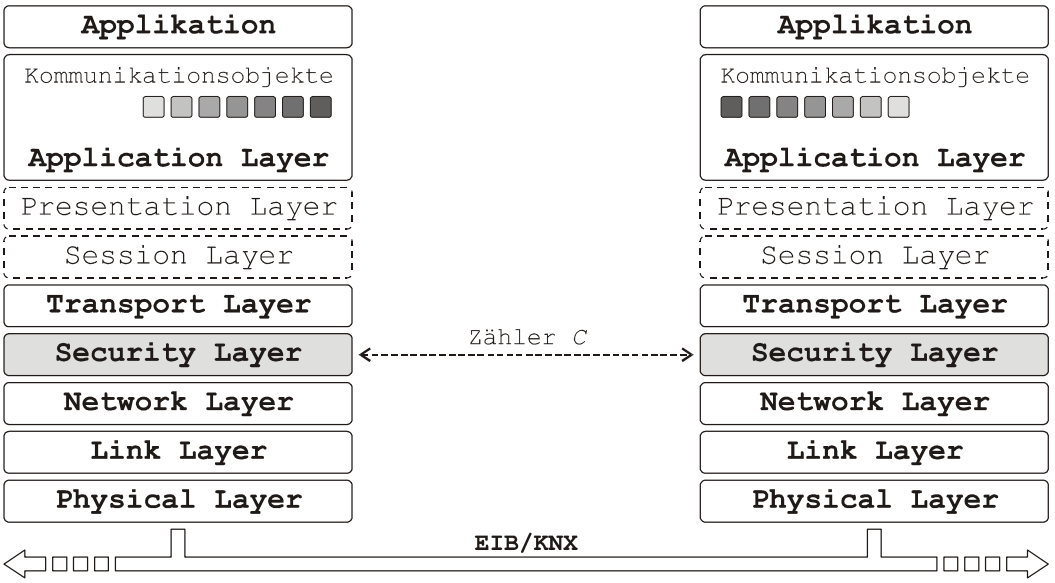

Abbildung 5.11: Protokoll-Layer der gesicherten Übertragung

Auf Grund der Tatsache, dass bis einschließlich des Network-Layers keine Veränderungen an der Kommunikationsstruktur vorgenommen wird, bleiben alle Übertragungseigenschaften des EIB/KNX erhalten. Dies ist insbesondere für die Routingeigenschaften der Telegramme sehr wichtig. Eine Kommunikation über Linien- und Bereichskoppler hinweg unterliegt keinerlei Einschränkungen und erfordert keine zusätzlichen Einstellungen innerhalb der Koppler.

Nach wie vor können auch die beiden Adressierungsarten, physikalische Adressierung und Gruppenadressierung, unterschieden werden, so dass theoretisch auch weiterhin alle vier Verbindungsvarianten realisierbar sind. Dies sind die verbindungslose Kommunikation mit einem, mehreren oder allen Teilnehmern und die verbindungsorientierte Kommunikation mit einem Teilnehmer. Die notwendige Voraussetzung hierfür ist der Erhalt des Transport-Layers, was innerhalb der oben vorgestellten Mechanismen zur gesicherten Datenübertragung ermöglicht wurde. Komplikationen treten bei den Varianten der Kommunikation einzelner Teilnehmer über die physikalische Adresse auf, da es durchaus mehrere Partner sein können, die bei Bedarf mit einem Teilnehmer entsprechende Verbindungen pflegen. Dies betrifft vor allem die Konfiguration von Buskopplern über das Netzwerk. Die Verwaltung von Schlüsseln und die Synchronisation der involvierten Zähler stellen in der Praxis zu hohe Ansprüche an die Kommunikationspartner. Deshalb muss der Security-Layer grundsätzlich alle physikalisch adressierten Telegramme (Destination Address Flag = 0) transparent passieren lassen, insofern sich der Buskoppler in einem speziellen Physical-Mode befindet.

Eine Ausnahme bilden Broadcast-Telegramme, sie dienen zur Konfiguration der physikalischen Adresse, dem Auffinden von Buskopplern oder der Vergabe von Domainadressen. Dies ist grundsätzlich nur im Programmier-Modus möglich, der bei Standard-Buskopplern durch Betätigung der Programmiertaste oder bei bekannter Adresse per Netzwerkbefehl erreicht wird. Diese Serviceaufrufe sind an der Zieladresse mit dem Wert Null zu erkennen und sollten nicht durch den Security-Layer bearbeitet werden.

5.5.7 Physical-Mode

Der Physical-Mode stellt einen Betriebszustand des gesicherten Buskopplers dar, der es erlaubt, Transportverbindungen mit anderen Teilnehmern aufzubauen. Dabei ist der physikalische Eingriff durch einen Benutzer notwendig, zum Beispiel durch Drücken der Programmiertaste des Buskopplers für mehrere Sekunden. Würde es diesen Mechanismus nicht geben, könnte ein Angreifer, der Zugang zum EIB/KNX hat, jederzeit leicht die Applikation für seine Zwecke abändern. Dieser Modus betrifft auch zwei verbindungslose Betriebsarten. Diese erlauben das Lesen und Schreiben sogenannter EIB-Objekte, strukturiert abgebildete Variablen zur Speicherung spezifischer Daten und das Zurücksetzen von Schlüsseln der Secure-BCU. Der Zugriff auf EIB-Objekte wird durch Buskoppler ab der Version 2 (BCU2) unterstützt. Ein nicht näher beschriebener Timeout-Mechanismus muss den Physical-Mode automatisch deaktivieren, sobald keine Transportverbindungen mehr zum Buskoppler bestehen.

5.5.8 Schlüsselverwaltung und Inbetriebnahme

Grundsätzlich ist für jede Gruppenadresse, die durch eine Secure-BCU verwendet wird, ein eigener Hauptschlüssel, die generierten Schlüssel und der Zähler zu verwalten. Nach einer Erstinbetriebnahme einer Secure-BCU, welche ausschließlich im Physical-Mode stattfinden kann, ist eine Kommunikation mittels des Schlüssels und Zählers, welche zusammen mit der eigentlichen Applikation übertragen wurden, möglich. Grundsätzlich besteht in diesem Moment die Gefahr, dass ein Angreifer an der Kommunikation teilnimmt. Die Erstinbetriebnahme sollte deshalb in sicherer Umgebung vorgenommen werden.

Während des Betriebes kann es notwendig sein, neue Hauptschlüssel für spezifische Gruppenadressen zu vergeben. Da dies auch ohne physikalischen Eingriff möglich sein muss, ist hierfür eine sichere Vorgehensweise zu definieren. Ausgehend vom Multicast-Verfahren, welches bei der Gruppenkommunikation angewandt wird, sind innerhalb dieser Arbeit vier weitere Applikations-Kommandos hinzugekommen. Abbildung 5.12 gibt einen Überblick über alle, mittels des vorgestellten Prinzips verschlüsselten Kommandos.

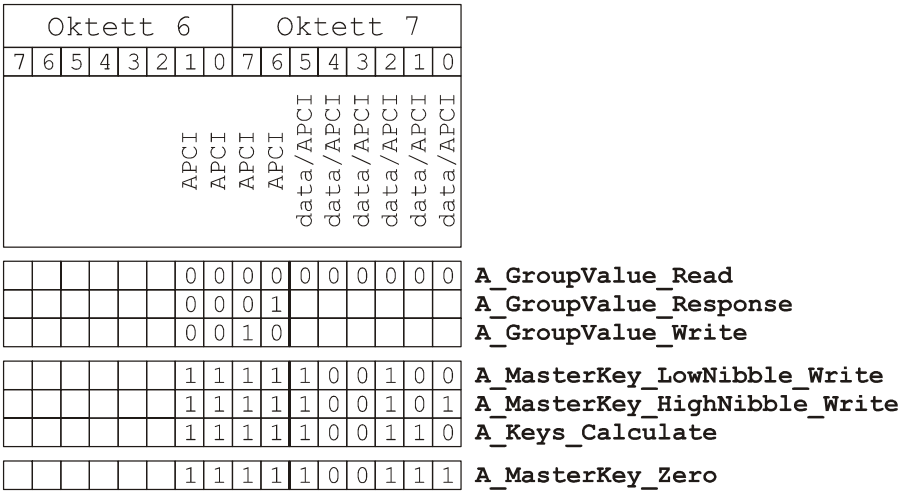

Abbildung 5.12: Verschlüsselte Multicast-Applikations-Kommandos

Für die Übertragung der Befehle und Parameter gilt immer folgende Prämisse; der Zählerstand für die Verschlüsselung wird erst inkrementiert wenn der Empfang eines entsprechenden Telegramms durch ein sofortiges Acknowledge-Zeichen entsprechend der EIB/KNX Standardkommunikation quittiert und durch keinen weiteren Teilnehmer per negativem Acknowledge entwertet wurde.

- **A_MasterKey_LowNibble_Write** Übertragung der unteren 8 Byte des neuen Hauptschlüssels K_{master}.
- **A_MasterKey_HighNibble_Write** Übertragung der oberen 8 Byte des neuen Hauptschlüssels K_{master}.
- **A_Keys_Calculate** Neuberechnung von K_{encr} und C_{init} aus dem Hauptschlüssel. Der Zähler C wird neu initiiert. Alle folgenden Telegramme werden unmittelbar anhand der neuen Werte verarbeitet.
- **A_MasterKey_Zero** Der Hauptschlüssel K_{master} wird auf Null gesetzt.

Das Kommando A_MasterKey_Zero könnte auch im Physical-Mode unverschlüsselt ausgeführt werden. Dies erlaubt die Wiederinbetriebnahme von Buskopplern ohne die Übertragung der vollständigen Applikation, zum Beispiel bei Änderungen in der Verteilung von Gruppenadressen.

5.5.9 Sensor-/Aktorproblematik

Das gesamte Prinzip der gesicherten Datenübertragung im EIB/KNX dient zur Steuerung sicherheitsrelevanter Systeme, wie zum Beispiel Türöffnermechanismen. Wenn es allerdings notwendig ist, die Übertragung von Daten innerhalb einer bestimmten Zeit zu garantieren, müssen Statustelegramme in periodischen Abständen gesendet werden. Der involvierte Empfänger muss dabei die Kommunikation überwachen und bei ihrem Ausbleiben notwendige Aktionen auslösen. Diese Vorgehensweise ist bei der Anbindung von Gefahrenmeldern auszuführen. Der zeitliche Abstand zwischen zwei aufeinanderfolgenden Telegrammen muss entsprechend der Anwendung an die zu erwartende Buslast angepasst werden.

5.6 Ressourcenanalyse

Standard-Buskoppler, wie sie heute in der EIB/KNX-Gebäudesystemtechnik eingesetzt werden, bieten ein gutes Interface zur Realisierung vielfältiger Hard- und Softwareapplikationen. Über entsprechende Schnittstellen ist auch die Manipulation an Telegrammen innerhalb der unterschiedlichen Layer möglich. Leider ist man dabei auf einen relativ leistungsschwachen Prozessor beschränkt, der zudem nur sehr geringe Speicher-Ressourcen für eigene Anwendungen verfügbar macht. Einige Hersteller sind bereits dazu übergegangen, Buskoppler mit neuerer Hardware für ihre Zwecke zu entwerfen, so wie auch im Rahmen dieser Arbeit eine neue Hardwareplattform entwickelt wurde. Entsprechende Details sind im Kapitel zur Umsetzung des Systems beschrieben.

Die Realisierung des vorgestellten Übertragungsprotokolls erfordert eine Reihe von zusätzlichen Ressourcen innerhalb des EIB/KNX-Kommunikationsstack, welche in Tabelle 5.1 als Richtwerte aufgeführt sind. Es handelt sich dabei um Durchschnittswerte für eine codeoptimierte Umsetzung auf einem 8 Bit-Mikrocontroller.

Tabelle 5.1: Ressourcenaufstellung für den Speicherbedarf

		ROM/FLASH	**RAM**
Ver-/Entschlüsselung	AES	ca. 2,5 KByte	56 Byte
Je Gruppenadresse	K_{master}	16 Byte	-
	K_{encr}	-	16 Byte
	C	16 Byte	16 Byte
Signatur	CRC32	ca. 150 Byte	ca. 20 Byte
Protokoll-Stack	Security-Layer	ca. 1 KByte	ca. 50 Byte
Σ	**1 Gruppenadresse**	**ca. 4 KByte**	**ca. 158 Byte**

Neben den reinen Speicherressourcen ist auch eine ausreichend schnelle Abarbeitung der notwendigen Operationen erforderlich. Ausgehend von einer Busauslastung bei 100% ergibt sich der zeitliche Abstand zwischen zwei aufeinander folgenden

Telegrammen im Twisted-Pair Medium mit maximaler Datenlänge zu 26,4 ms, zuzüglich der Übertragungsdauer eines Quittierungs-Zeichens und einer Arbitierungspause von 2 ms. Innerhalb dieser Zeit muss die Rechenleistung mindestens für die Abarbeitung des Standard-Kommunikationsstacks, der eigentlichen Anwendung des Buskopplers, und je einem vollständigen Ent- und Verschlüsselungsvorgang reichen. Dieser Vorgang tritt zum Beispiel auf, wenn explizit der Zustand eines Kommunikationsobjektes per Polling-Mechanismus abgefragt wird. Eine entsprechend schnelle Reaktion auf einen solchen Request ist zwar nicht zwingend erforderlich, erhält aber die maximale Performanz des EIB/KNX-Netzwerkes.

Die Umsetzung des Verfahrens auf einem mit 12 MHz getakteten 8051 Derivat, bei 12 Takten pro Zyklus, erlaubt die Abarbeitung der durch den Security-Layer geforderten Operationen für das Codieren oder Dekodieren eines Telegramms innerhalb von 5 ms. Der Programmcode war dabei nur auf Codegröße, nicht aber auf Laufzeit optimiert.

Nachteil gegenüber der Standardübertragung im EIB/KNX ist die Verlängerung der Telegramme, da grundsätzlich 128 Bit im Transportdatensegment übertragen werden müssen. Ein einfaches, binäres Schaltobjekt wird bei der gesicherten Übertragung nicht mehr innerhalb von 9 Byte, sonder mit einem 23 Byte langen Telegramm übertragen. Dies führt, je nach verwendetem Medium und bei Einsatz der gesicherten Datenübertragung zu einer Erhöhung der Buslast, die bei der Planung eines EIB/KNX Netzwerkes berücksichtigt werden muss.

5.7 Anwendung

Hauptanwendungsgebiet in der Automatisierung von Gebäuden für das oben vorgestellte Verfahren ist die Alarmierungstechnik von Gefahrenmeldern. Mittels der gesicherten Datenübertragung können sowohl im Wohn- als auch im Zweckbau parallel zur bereits vorhandenen Gebäudesystemtechnik schnell diverse Meldelinien realisiert werden. Die Gefahrenmeldeanlage ist dabei auch Teil der EIB/KNX-Installation und kann somit alle Vorteile der vernetzten Installationstechnik nutzen. Sicherheitskritische Aktoren, wie Türöffner oder Fensterantriebe, lassen sich genauso in das Netzwerk einbinden wie Authentisierungsstationen oder Zeiterfassungssysteme.

Sämtliche EIS-Datentypen (EIB Interworking Standard für Gruppenkommunikation) können im Rahmen der gesicherten Datenübertragung übertragen werden. Einzige Ausnahme bildet der EIS-Typ 15 – Character String – für den sich die maximale Länge (MAXDATA = 14 Byte) auf 10 Byte reduziert.

6 Umsetzung des Gesamtsystems

6.1 Überblick

Im Rahmen der Arbeiten im Projekt tele-Haus entstand ein Demonstratoraufbau, der alle wesentlichen Elemente diverser Zugangs- und Sicherheitsmechanismen enthält, welche an einem mit EIB/KNX ausgestatteten Gebäude angewendet werden können. Neben einer Standard EIB Grundausstattung (Netzteil mit Drossel, Serielle Schnittstelle, Schaltaktor und Tasterapplikation) enthält der mobile Aufbau eine miniaturisierte Tür mit einem integrierten Motorblockschloss. Abbildung 6.1 zeigt eine schematische Darstellung aller im Demosystem integrierten Elemente.

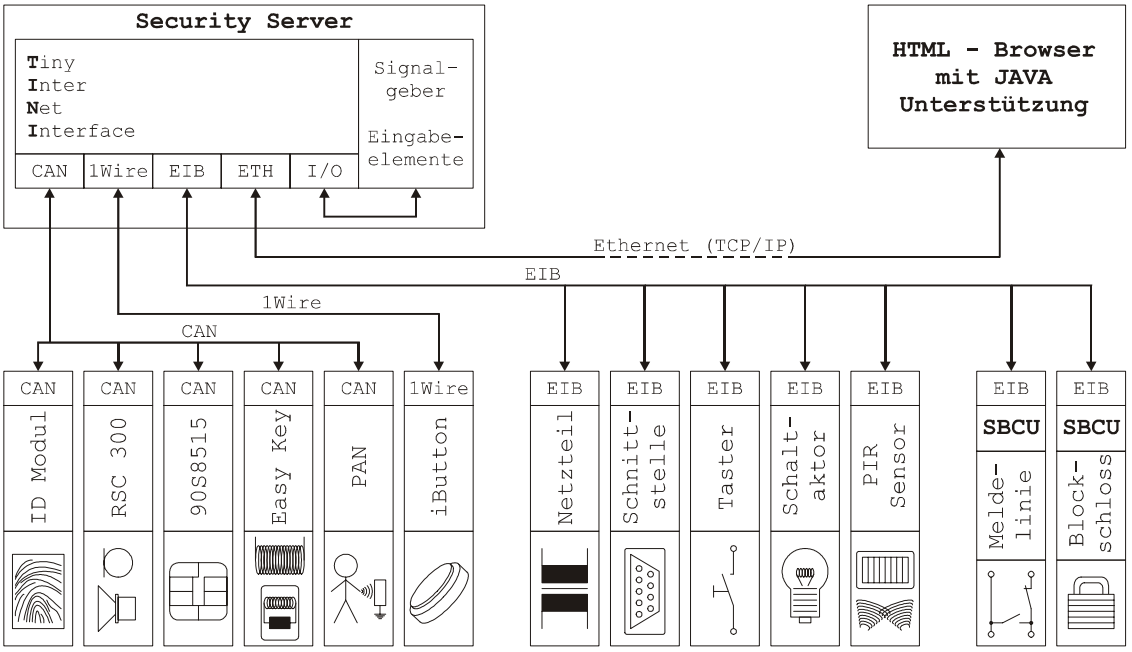

Abbildung 6.1: Darstellung aller Komponenten des Demosystems

Der zur Konfigurierung, Überwachung und Steuerung dargestellte HTML-Browser ist dabei nicht Teil der Anlage, sondern ein beliebiger, im Netzwerk vorhandener Personal Computer oder ein Web-Pad. Bei den Standard-Komponenten handelt es sich um einen 2-fach Aktor sowie um eine Doppeltasterwippe der Firma Siemens, über welche zwei voneinander getrennte Leuchtmittel gesteuerte werden können. Ein 180° Passiv-Infrarot (PIR) Melder der Firma Busch-Jaeger, welcher innerhalb des Projektes tele-Haus entwickelt wurde, steuert bewegungsaktiviert ebenfalls eines der Leuchtmittel. Abbildung 6.2 zeigt die Rückansicht der Demonstratoreinheit. Unten links sind die Basiskomponenten der EIB/KNX Installation zu erkennen, darüber die beiden Secure Buskoppler samt Glasbruchsensor und Blockschlossaktor. Auf der rechten Seite

befinden sich die per CAN-Bus vernetzten Authentisierungseinheiten sowie der embedded TINI Security Server.

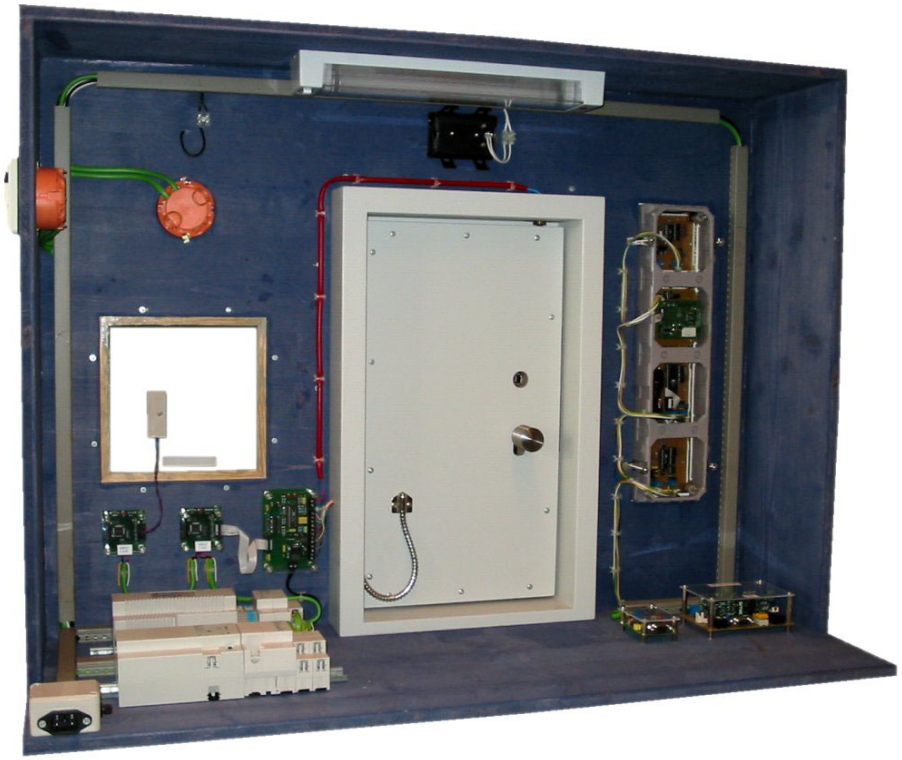

Abbildung 6.2: Rückansicht der Demonstratoreinheit

In den folgenden Abschnitten werden die einzelnen Elemente und deren Umsetzung in Hard- und Software beschrieben, wobei nicht näher auf die Standard EIB/KNX Installation eingegangen wird. Detaillierte Informationen zur Funktionsweise, Topologie und Programmierung dieser Komponenten können im Anhang nachgelesen werden.

6.2 Der Security Server

Die zentrale Einheit des gesamten Authentifizierungssystems stellt der Security Server dar. Hauptaufgabe des Servers ist es, eine Reihe diverser Schnittstellen zur Verfügung zu stellen und diese durch die Bereitstellung von dafür geeigneten Diensten zu bedienen. Eine äußerst effektive und kostengünstige Variante hierfür ist der Einsatz eines sogenannten TINI-Boards der Firma Dallas Semiconductor. Der embedded Rechner hat die Größe eines PS/2 SIMM Speicherriegels und basiert auf dem leistungsfähigen 8051 kompatiblen Mikrocontroller DS80C390. Als Speicher für den Prozessor wird ein statisches RAM eingesetzt, das je nach Ausführung 512 KByte oder 1 MByte Kapazität aufweist. Da dieser Speicher nicht nur als Arbeits-, sondern auch als Programm- und Datenspeicher verwendet wird, ist dieser zusätzlich über eine

Lithiumbatterie gepuffert, so dass Daten und Anwendungen auch nach einer Unterbrechung der Stromzufuhr erhalten bleiben. Das notwendige Betriebssystem samt Java Virtual Machine (JVM) und UNIX-ähnlicher Benutzeroberfläche ist in einem 512 KByte großen Flashspeicher untergebracht. Da diese embedded Einheit vollständig in Java programmiert wird, ist es möglich, die Software mit frei erhältlichen, stets auf dem neuesten Stand befindlichen Java-Compilern schnell, zuverlässig und vor allem plattformunabhängig zu programmieren [Flanagan 2002].

6.2.1 TINI-Hardware

Der Einplatinencomputer verfügt über eine Ethernetschnittstelle inklusive Transceiver (10BaseT) und zwei serielle RS232 Schnittstellen, sowie eine CAN (Controller Area Network) [Lawrenz 2000], 2Wire (I^2C) und 1Wire Schnittstelle. Neben den Busschnittstellen bietet die Einheit alle Adress- und Datenleitungen am 72-poligen Sockel an, so dass weitere Komponenten angebunden werden können. Die eingangs erwähnte 1Wire Schnittstelle ist eine Entwicklung der Firma Dallas Semiconductor. Diese für sogenannte 1Wire.NET Komponenten ausgelegte Schnittstelle benötigt neben der Masseleitung lediglich eine Versorgungsleitung, die gleichzeitig zur Datenübertragung im Master-Slave Verfahren verwendet wird. Neben Speicherbauteilen, Zählern und Sensoren lassen sich sämtliche iButton Geräte, wie beispielsweise der Cryptobutton-Schmuckring oder Schlüsselanhänger ansteuern. Solche Komponenten eignen sich sehr gut zur Zugangskontrolle oder in Form von Zählern und Temperatursensoren zur zusätzlichen Aufnahme von Verbrauchswerten innerhalb eines Gebäudes. Nähere Informationen zur Verbrauchsdatenerfassung mittels 1Wire Elementen und TINI Rechnern sind unter [Bintern 2003] beschrieben.

Abbildung 6.3 zeigt den während der Arbeit entstandenen Aufbau des Security Servers. In der Mitte ist das senkrecht montierte TINI-Board zu erkennen, wie es in der Demonstratoreinheit verbaut ist. Die 8,0 x 12,0 cm^2 große Platine bietet Schraubklemmen zum Anschluss der 12 Volt Versorgungsspannung, von CAN-Bus Teilnehmern, 1Wire Einheiten, einer RJ45 Ethernetschnittstelle und einem seriellen RS232 Interface für Wartungszwecke. Der für den Betrieb des CAN-Busses notwendige Transceiver [Etschberg 2002] mit zuschaltbarem Abschlusswiderstand ist auf der Basisplatine installiert. Eine weitere Schraubklemme erlaubt den Anschluss an das EIB/KNX Gebäudebussystem. Die hierfür notwendige Interfaceschaltung, welche ebenfalls Teil der Basisplatine ist, wird im folgenden Abschnitt beschrieben. Sämtliche Schaltpläne zum Security Server befinden sich im Anhang dieses Dokumentes.

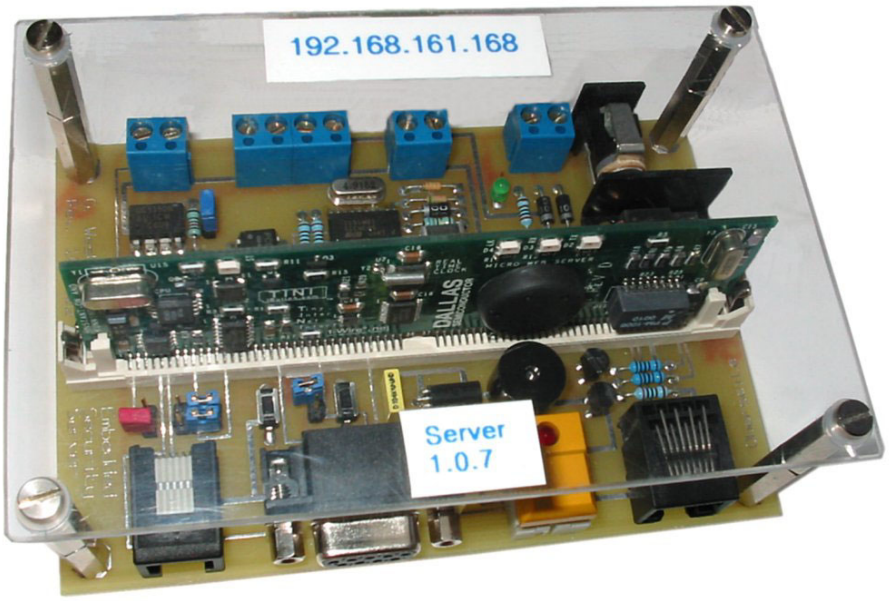

Abbildung 6.3: Aufbau des TINI Security Servers

Zusätzliche Komponenten auf der Basisplatine sind diverse Jumper, ein Taster sowie ein akustischer Signalgeber, welche über I/O-Leitungen des TINI-Boards per Software abgefragt und gesteuert werden können. Die verwendeten Leitungen sind nicht Teil des Adress- und Datenbusses, sondern ab Revision D der 1 MByte Version des TINI-Boards hinzugekommene Standard I/O-Anschlüsse.

6.2.2 Buszugriff

Ein wesentlicher Teil der Hardware des Servers stellen die unterschiedlichen Schnittstellen zu den diversen Bussystemen dar, weshalb einige hier speziell erwähnt werden.

Während die serielle Serviceschnittstelle nach RS232 Standard, sowie die 10 Mbit Ethernetschnittstelle nach IEEE 802.3 und das 1Wire.NET Interface auf dem TINI-Board bereits vollständig integriert sind, ist der Anschluss eines CAN-Transceivers extern notwendig. Hierfür empfehlen sich Bausteine vom Typ Philips PCA82C250 oder Texas Instruments UC5350N. Zur Anbindung des Servers an den EIB/KNX Gebäudesystembus wird die serielle Schnittstelle, welche auch für Servicezwecke verwendet wird, auf Basis der TTL-Anschlüsse verwendet. Ein Jumper erlaubt das Wechseln zwischen dem EIB/KNX-Betrieb und der Servicekonsole. Die zweite auf dem Board befindliche serielle Schnittstelle dient intern zur Kommunikation mit 1Wire Komponenten. Um mit dem Gebäudebussystem kommunizieren zu können, bieten sich standardisierte Buskoppeleinheiten (siehe Anhang A) an. Da diese aber eine zeitkritische Kombination aus Hard- und Softwarehandshake zur Datenübertragung auf ihrem Interface verwenden [Westermeir 2001a], sind diese unter der nichtrealzeitfähigen Java-

Umgebung nicht verwendbar. Auch das in neueren Versionen der Buskoppler verwendete FT1.2 Protokoll stellt hohe Anforderungen an den Kommunikationspartner.

Da der in den Buskopplern integrierte Kommunikationsstack nur eine begrenzte Anzahl von Objekten innerhalb eines EIB/KNX-Netzwerkes bedienen kann, wäre es notwendig, über den Link-Layer zu kommunizieren. Für diesen Zweck vertreibt die Firma Siemens den sogenannten TPUART-IC (Twisted Pair Universal Asynchronous Receiver Transmitter), ein ASIC (Application Specific Integrated Circuit), der in einem 20-poligen SOIC-Gehäuse alle notwendigen Analogelemente und digitalen Schnittstellen vereint. Der Baustein bietet ein serielles Interface mit einer Baudrate von 19200 Bit/s im „Normal Mode“ und übernimmt alle wesentlichen Funktionen zur Sicherung der Datenübertragung [TPUART 2001]. Um sogenannte Brummschleifen über die Stromversorgung des Servers zu vermeiden, welche die Kommunikation auf dem Gebäudebus beeinflussen, müssen die Verbindungen zwischen TINI-Board und TPUART mittels Optokoppler galvanisch getrennt werden. Im Anhang B ist der entsprechende Schaltplan dargestellt.

Für alle restlichen Schnittstellen sind lediglich die entsprechenden Steck- und Schraubkontakte auf der Basisplatine herausgeführt.

6.2.3 Das TINI-Betriebssystem

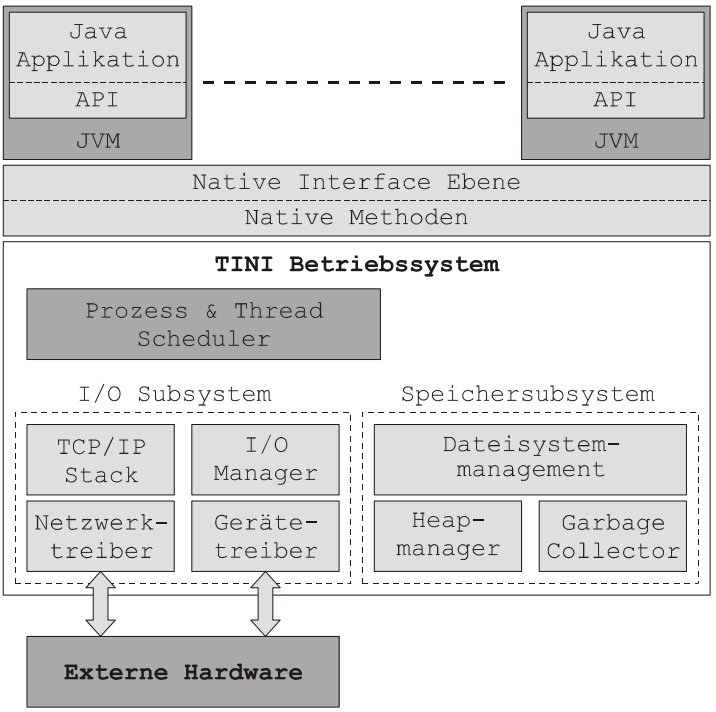

Abbildung 6.4: Interne Struktur des TINI Betriebssystems

Abbildung 6.4 zeigt die interne Struktur des TINI-Betriebssystems. Auf Grund des integrierten Betriebssystems kann das TINI-Board über die als SLUSH bezeichnete

UNIX-ähnliche Oberfläche mittels Zugriff über eine Kommandokonsole per Ethernet oder serieller Schnittstelle bedient werden. Ein kompletter TCP/IP Stack ermöglicht unter anderem die Implementierung diverser Netzwerkdienste wie Web-Server, Filetransfer per FTP (File Transfer Protocol) oder den Zugang per TELNET.

Es können mehrere Applikationen, gekapselt durch deren Java Virtual Machines, zur selben Zeit quasi parallel ausgeführt werden. Die einzelnen Anwendungen können wiederum beliebige Threads im Sinne der objektorientierten Programmierung in Java starten. Auf dieser Basis setzt die im Folgenden beschriebene Security Server Software auf. Weitergehende Informationen zum TINI-Board und zur Programmierung sind in [Loomis 2001] verfügbar.

6.2.4 Die Server Software

Die für den Server erstellte Java-Software setzt sich aus einer Reihe von Klassen zusammen, die mit dem Java 2 Software Development Kit 1.4.1 erstellt wurden. Grundlage für das TINI Betriebssystem war die Version 1.10.

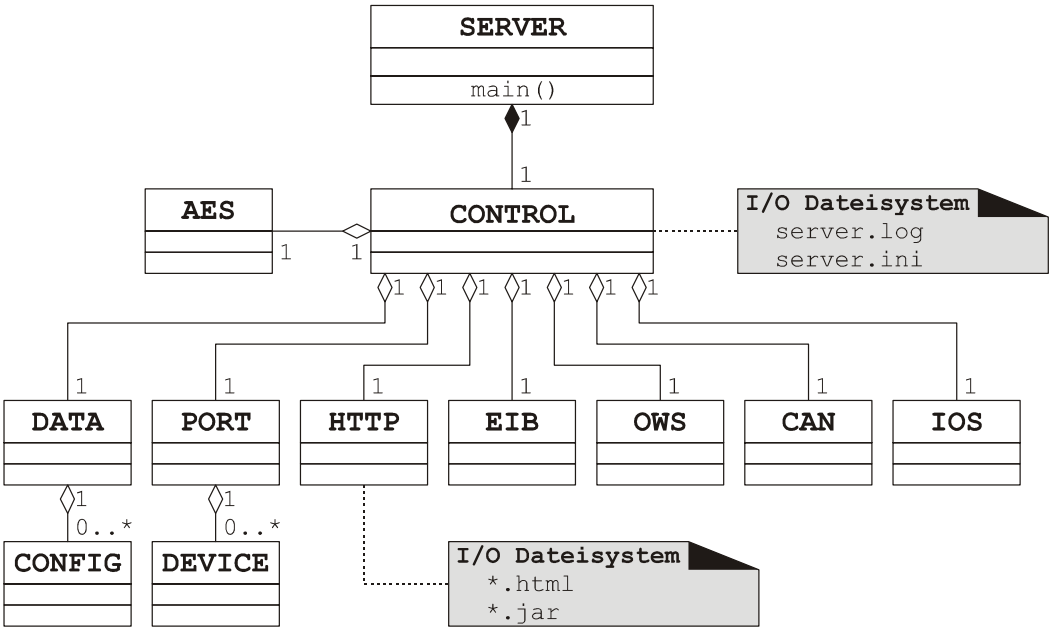

Abbildung 6.5: Klassenstruktur der Serversoftware

Die in Abbildung 6.5 als UML-Diagram (Unified Modeling Language) [Oestereich 1998] dargestellte Klassenstruktur zeigt, wie sich die im Server verwendete Software zusammensetzt. Das zentrale Element der Anwendung stellt die Klasse CONTROL dar, welche als Instanz aus dem Hauptprogramm gestartet wird. Um ein möglichst flexibles Softwaremodell zu erhalten, sind sämtliche Schnittstellen zur Außenwelt über entsprechende Klassen gekapselt, so dass diese unabhängig von der Serversoftware getestet werden konnten. Die Objekte der Treiberklassen kommunizieren hierbei über

Methodenaufrufe mit den übergeordneten Klassen. Die folgenden Abschnitte beschreiben kurz die Funktionsweise der wichtigsten Objekte und die durch die Instanz der Klasse CONTROL gegebenen Funktionen.

6.2.4.1 Schnittstellen zur Hardware

Die vier Klassen EIB, OWS, CAN und IOS kapseln die entsprechenden Hardware-Schnittstellen des EIB/KNX, des 1Wire und CAN-Busses sowie der Taster, Jumper und Signalgeber an den I/O-Leitungen über einfache Methodenaufrufe. Entsprechende Basisklassen, welche über ein Native-Interface mit der Hardware kommunizieren, stellt das TINI Software Development Kit zur Verfügung. Jede dieser vier Klassen erzeugt einen eigenen Thread, in dem die Zustände der Schnittstellen überwacht werden. Initiiert wird der Vorgang durch die Methode startService() und beendet durch den Aufruf von stopService(), welche von jeder Klasse unterstützt werden. Trifft an einer der Schnittstellen ein Telegramm ein, oder ändert sich der Zustand an einer I/O-Leitung, veranlasst der assoziierte Thread die Aufbereitung der Daten. Dies ist insbesondere bei der EIB Klasse notwendig, da die vorgeschriebene Zwangspause von 2 bis 2,5 ms zwischen zwei aufeinanderfolgenden Telegrammen nur schwer mittels der Javacomm API zu detektieren ist. Hierfür entstand ein effektiver kleiner Algorithmus, der aus dem empfangenen Datenstrom die einzelnen Telegramme extrahiert, in dem sich der Empfänger an empfangenen Servicebytes synchronisiert und anhand des gesendeten Längenbytes das Ende der Telegramme überprüft. Die Empfängerthreads rufen dann entsprechend Methoden in der Klasse CONTROL auf und übergeben die Daten, so dass diese dort weiterverarbeitet werden können. Zur Ausgabe von Daten über die Schnittstellen, sowie zum Bearbeiten von Telegrammen, stellen die vier Klassen weitere Methoden zur Verfügung.

6.2.4.2 Der Web-Server

Die Klasse HTTP verwendet die durch Dallas Semiconductor vorgegebene Klasse HTTPServer und realisiert einen einfachen Web-Server, der auf Port 80 eingehende GET-Requests verarbeitet. Dies ist die einzige Klasse, die außer den Methoden startService() und stopService() keine weiteren Kommunikationsbeziehungen und Funktionen besitzt. Der erzeugte Web-Server Thread arbeitet unabhängig und stellt entsprechenden Clients, wie Webbrowsern, Teile des TINI-Filesystems zur Verfügung. Dies sind hier die HTML-Dateien mit den Webseiten zur Steuerung und Konfiguration, so wie die dazugehörigen Java-Applets. Abbildung 6.6 zeigt eine solche durch einen Browser dargestellte HTML-Datei zur Visualisierung von Gerätezuständen am EIB/KNX Gebäudesystembus.

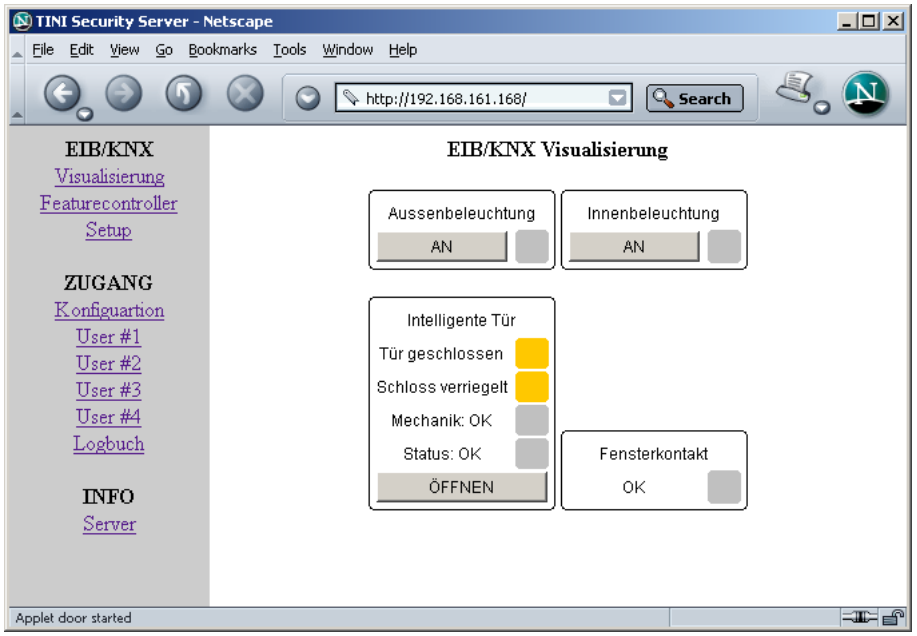

Abbildung 6.6: Screenshot der EIB/KNX Visualisierung

Das Aussehen und die Verhaltensweise der Dialoge basiert auf der HTML-Programmierung und stellt hier nur eine sehr einfache Variante dar ([Münz 2001], [Niederst 2002]). Die linke Navigationsleiste stellt Links auf die zum Betrieb notwendigen Dialogseiten bereit, welche innerhalb des rechten Frames dargestellt werden. Alle aktiven Elemente, die das Verändern von Parametern oder das Visualisieren und Steuern von Busteilnehmern erlauben, basieren auf Java-Applets [Steyer 2001], deren Erscheinungsbild und Funktion durch Parameter innerhalb der HTML-Dateien angepasst werden. Der nachfolgende Abschnitt beschreibt die entstandenen Applets.

6.2.4.3 Visualisierung und Konfiguration

Um eine bidirektionale Kommunikationsbeziehung, wie sie beispielsweise für die Visualisierung benötigt wird, über einen normalen Webbrowser zwischen User und Server zu realisieren, existieren prinzipiell zwei Möglichkeiten.

Zum einen das Einbinden aktueller Informationen zur Laufzeit durch serverseitiges Generieren der HTML-Seiten während des Abrufens durch den Client. Diese Technik wird als CGI-Technik bezeichnet. CGI (Common Gateway Interface) ist eine Schnittstelle des Web-Servers. Sie erlaubt es, die Anfragen eines Web-Browsers an Programme auf dem Web-Server weiterzureichen und von diesem ausführen zu lassen. Solche Programme können beispielsweise Formulareingaben aus HTML-Dateien verarbeiten, auf dem Server-Rechner Daten speichern und dort gespeicherte Daten auslesen. Auf diese Weise werden Web-Seiten zu Oberflächen für "Anwendungen", beispielsweise für elektronische Warenbestellung oder zum Abfragen von Datenbanken [Münz 2001]. Diese Technik erlaubt nur während des Abrufens der Web-Seite neue

Inhalte einzubinden und eignet sich somit nur bedingt für die Visualisierung von Zuständen innerhalb der Gebäudesystemtechnik.

Zum anderen gibt es die Möglichkeit, Java-Applets in HTML-Seiten einzubinden. Diese Applets sind eigenständige Java-Anwendungen, die innerhalb einer Virtual Machine des Web-Browsers ausgeführt werden können. Hier obliegt es dem Programmierer, eine bidirektionale Kommunikationsbeziehung zum Server aufzubauen, insofern serverseitig eine Gegenstelle als Kommunikationspartner zur Verfügung steht.

Diese Technik findet in der Security Server Software Verwendung, sowohl zur Steuerung und Visualisierung der EIB/KNX Komponenten am Gebäudesystembus, als auch zur Konfigurierung der Betriebsparameter. Die hierfür notwendigen Klassen PORT und DATA bilden die notwendigen Gegenstellen auf der Serverseite. Die Funktionsweise beider Objekte ist sehr ähnlich. Sie warten jeweils auf einen Verbindungsaufbau auf einem definierten TCP/IP-Port, um für jedes verbundene Applet eine Instanz der Klasse DEVICE beziehungsweise der Klasse CONFIG zu erstellen. Diese sind jeweils solange existent, bis die damit verbundenen Applets terminiert werden. Dies geschieht automatisch beim Wechsel zu einer anderen Web-Seite im Browser, bei Unterbrechung der Verbindung oder beim Beenden des Clients.

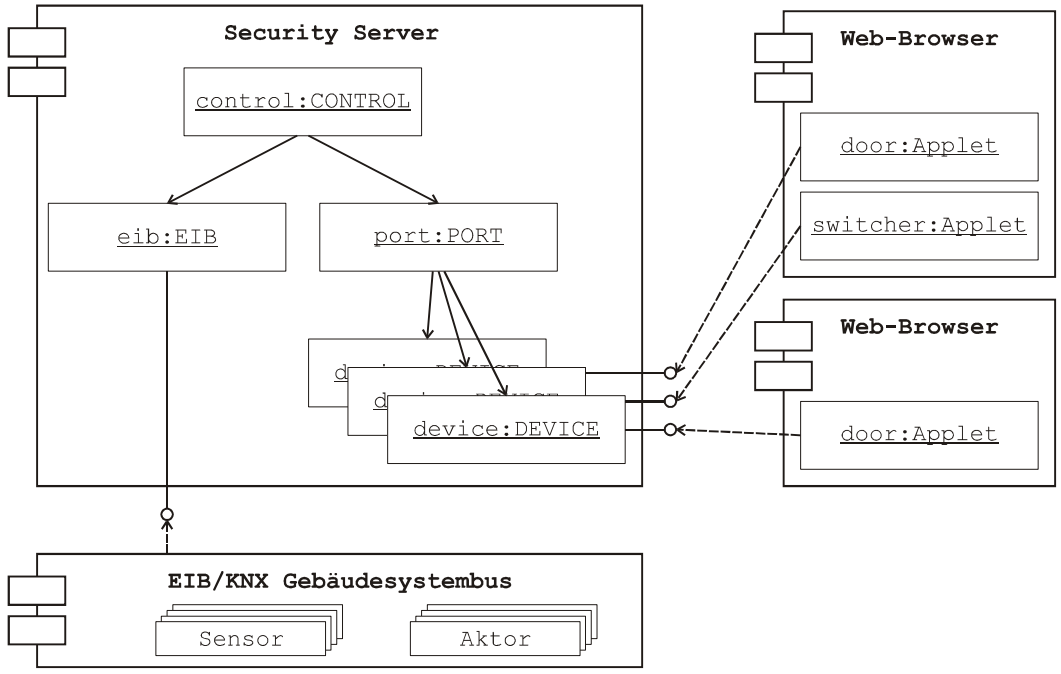

Abbildung 6.7: Kommunikationsbeziehung zwischen Browser, Server und EIB/KNX

Abbildung 6.7 zeigt am Beispiel der Gerätevisualisierung die Kommunikationsbeziehungen zwischen den Applets in verbundenen Web-Browsern, dem Security Server und dem EIB/KNX Gebäudesystembus. Alle vom EIB/KNX empfangenen Telegramme werden durch die Klasse EIB an die Klasse CONTROL geleitet und dort ausgewertet. Hier werden auch, wie in Kapitel 5 beschrieben, verschlüsselte Telegramme

entschlüsselt. Alle Telegramme stehen nun der Klasse PORT zur Verfügung, welche diese an jede Instanz der Klasse DEVICE weiterleitet, so dass alle verbundenen Visualisierungsapplets alle Telegramme erhalten. Dies entspricht dem dezentralen Prinzip des Broadcast-Verfahrens, welches beim EIB/KNX angewendet wird. Je nach Parametrierung des Applets, welches über die HTML-Seite festgelegt wird, kann dieses ein oder mehrere, wie beim Applet zur Visualisierung der vier Türobjekte, Objektzustände gleichzeitig visualisieren. Auf demselben Weg können auch die Applets Telegramme erzeugen, welche schließlich über den Server auf den EIB/KNX gesendet werden. Wurde das Telegramm erfolgreich übertragen und das assoziierte Objekt innerhalb des Netzwerkes aktualisiert, wird das entsprechende Telegramm im Server reflektiert und an alle Applets versendet, so dass diese sich synchronisieren können.

Auf einem sehr ähnlichen Prinzip basiert der Konfigurationsvorgang, für den entsprechende Applets innerhalb der HTML-Seiten aufgerufen werden. Abbildung 6.8 zeigt den Screenshot einer entsprechenden Oberfläche zur Konfigurierung einiger Parameter der Zugangskontrolle.

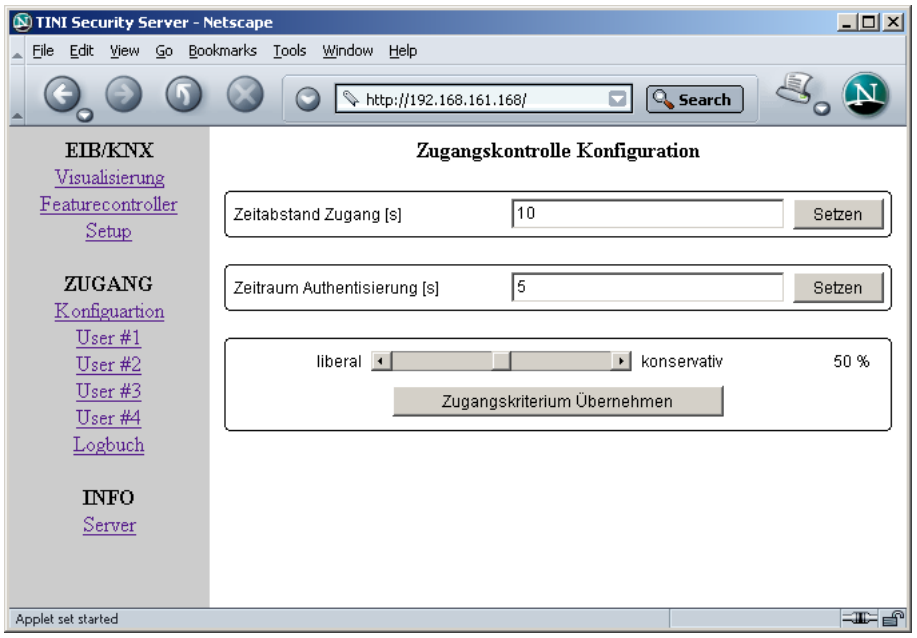

Abbildung 6.8: Screenshot einer Konfigurationsoberfläche

Die drei gestarteten Applets ermöglichen es dem Benutzer, Attribute innerhalb des Servers direkt zu parametrieren. Abbildung 6.9 zeigt den Quellcode, der ein Applet zum Verändern der Systemvariable „t_authent“ startet. Es werden als Parameter lediglich die Beschriftungen sowie der Variablenname übergeben. Für jedes dieser Applets erzeugt die Instanz der Klasse DATA ein Objekt vom Typ CONFIG, welches mit dem Applet auf einem definierten TCP/IP-Port kommuniziert.

```
<APPLET ARCHIVE="set.jar" CODE="set.class" WIDTH=500 HEIGHT=35>
 <PARAM NAME="type"      VALUE="t_authent">
 <PARAM NAME="label"     VALUE="Zeitraum Authentisierung [s]">
 <PARAM NAME="button"    VALUE="Setzen">
</APPLET>
```

Abbildung 6.9: Parameterübergabe an Applets zur Konfigurierung

Die assoziierte Systemvariable wird nach dem Verbindungsaufbau als Zeichenkette an das Browserapplet übergeben und angezeigt. Ändert der Benutzer den Parameter und betätigt den Button, so wird der neue Wert an die Klasse DATA weitergereicht, dort überprüft und das entsprechende Attribut der Klasse CONTROL verändert. Die neue Einstellung wird sofort wirksam und im Konfigurationsfile des Servers serialisiert gespeichert. Das in Abbildung 6.8 mittig dargestellte Applet entspricht dem obigen Beispiel. Das Applet zum Festlegen des Zugangskriteriums oder der Benutzerdaten sowie die Applets zum Konfigurieren des Featurecontrollers basieren auf dem gleichen Prinzip, verändern aber zum Teil mehrere Systemvariablen gleichzeitig.

6.2.4.4 Die zentrale Klasse CONTROL

Den zentralen Teil der Serversoftware bildet die Klasse CONTROL, welche den gesamten Nachrichtenfluss innerhalb des Servers steuert. Diese Klasse stellt selbst die beiden Methoden startService() und stopService() zur Verfügung, so dass eine Hauptroutine definiert alle Services starten und beenden kann. Die Instanz der Klasse CONTROL ist im Gesamtsystem für folgende Aufgaben zuständig:

- Weiterleiten der EIB/KNX-Telegramme vom Bussystem zu den Applets und umgekehrt, wobei gesicherte Telegramme entsprechend Kapitel 5 ver- und entschlüsselt werden.
- Verwaltung des Schlüssels zur Bearbeitung gesicherter EIB/KNX-Telegramme und Initiierung von Synchronisations- und Schlüsselerneuerungsvorgängen.
- Auswertung von EIB/KNX-Telegrammen zum Auslösen von Alarmen, insbesondere wenn Sensordaten über einen definierten Zeitraum ausbleiben.
- Auswerten von CAN-Telegrammen und 1Wire-Informationen, die innerhalb eines festgelegten Zeitraumes zusammenhängend eintreffen, nach den Definitionen aus Kapitel 4.
- Verwaltung der Userdaten und Verknüpfung mit den eingestellten Kriterien und Authentisierungsergebnissen nach Kapitel 4.
- Senden verschlüsselter EIB/KNX-Telegramme an die Applikation zum Ansteuern des Motorblockschlosses bei erfolgreicher Authentisierung.

- Schreiben einer Log-Datei im Dateisystem mit Informationen zu allen Authentisierungsversuchen.
- Schreiben und Lesen der serialisierten Konfigurationsparameter im Dateisystem.
- Auslösen zeitlicher Ereignisse am EIB/KNX-System nach den eingestellten Parametern des Featurecontrollers.
- Auswerten von Gerätezuständen im EIB/KNX-System, um im Gefahrenfall die Türe zu öffnen oder um Rückschlüsse auf die Anwesenheit von Personen zu ziehen.
- Versenden von Meldungen über das Netzwerk (E-Mail, Netmessage usw.) bei Eintreten definierter Ereignisse.

Um die in dieser Arbeit beschriebenen Methoden zur gesicherten Datenübertagung und multimodalen Zugangskontrolle evaluieren und nachweisen zu können, war es nicht notwendig, alle Funktionen in der Demonstratoreinheit zu integrieren. Dies betrifft insbesondere das Versenden von Meldungen über das Netzwerk und die Funktionalität eines Featurecontrollers sowie eine komfortable Möglichkeit, die biometrischen Systeme (Fingerabdruck und Spracherkennung) über den Server zu konfigurieren. Das Aufzeichnen von Sprachmustern und der Enrolment-Vorgang zum Einspeichern von Fingerabdrücke muss an den entsprechenden Modulen manuell vorgenommen werden.

Die Konfigurationsdaten werden in serialisierter Form im TINI-Filesystem gespeichert. Das Java Software Development Kit stellt entsprechende Methoden zur Verfügung, welche es erlauben, unterschiedliche Datentypen in einen Datenstrom zu wandeln, um diese dann in einer Datei zu speichern oder über Netzwerkverbindungen zu senden. Die entsprechenden Parameter können während der Laufzeit, oder beim Start der Applikation wieder zurückgewonnen werden.

Zum Ver- und Entschlüsseln der gesicherten EIB/KNX-Telegramme stellt die Klasse AES alle notwendigen Methoden für das 128 Bit Verfahren bereit. Verschiedene Versuche haben gezeigt, dass die Bearbeitungsgeschwindigkeit durch das TINI-Board vom verwendeten Algorithmus stark abhängig ist. Obwohl die embedded Plattform auf einem schnellen 8Bit-Mikrocontroller basiert, verhält sich die Ver- bzw. Entschlüsselungsdauer, im direkten Vergleich zur Implementierung in C, um den Faktor 50 langsamer. Der Grund dafür liegt bei den Prozessprioritäten innerhalb des TINI-Betriebssystems und der Umsetzung der Java Vitual Machine auf dem verwendeten Controller. Um eine ausreichend schnelle Verarbeitung der gesicherten Telegramme zu ermöglichen, war es nötig, die Schlüsselexpansion bereits bei der Instanziierung der Klasse vorzunehmen. Auf diese Weise ist es aber nicht möglich, eine maximale Buslast auf dem EIB/KNX zu bedienen. Für den Fall, dass sich im System mehrere gesicherte Sensoren befinden, die in sehr kurzen Zeitintervallen ihre verschlüsselten Sensordaten übertragen, empfiehlt es sich, ein Native-Interface einzusetzen. Ein solches Interface

erlaubt das Ausführen von angepasstem Maschinencode, wie er von Assemblern oder C-Compilern erstellt wird, aus der Java-Umgebung heraus.

6.3 Die Zugangsmechanismen

Um die diversen Zugangsmechanismen mit dem Security Server verbinden zu können, stehen am hier verwendeten TINI-Server unterschiedliche Schnittstellen zur Verfügung, die es erlauben, unterschiedliche Netzwerk-Topologien zu realisieren. Da das System möglichst flexibel und unabhängig von den verwendeten Authentisierungsmechanismen sein soll, ist es notwendig ein Bussystem zu verwenden, welches die Kommunikation über mehrere Meter in beide Richtungen erlaubt. Jeder Teilnehmer sollte von sich aus eine Verbindung initiieren können, um den Server über den Versuch einer Authentisierung zu informieren. Von den zur Verfügung stehenden Schnittstellen eignen sich hier lediglich der EIB oder der CAN-Bus. Da der CAN-Bus bei niedrigen Übertragungsraten kaum Ansprüche an den physikalischen Aufbau stellt und eine große Anzahl von entsprechenden Controllern auf dem Markt erhältlich sind, fand dieser primär im Demosystem Verwendung. Eine sekundäre Anbindung unterschiedlicher Authentisierungsmechanismen über den EIB/KNX ist ebenfalls möglich. Hier ist es aber dringend zu empfehlen, wie in Kapitel 5 beschieben, verschlüsselte Telegramme zu verwenden. Eine derartige Anbindung der Zugangssensorik wurde im Rahmen dieser Arbeit nicht realisiert. Bei der hier verwendeten Vernetzung per CAN-Bus sind keine weiteren Sicherheitsmechanismen zum Einsatz gekommen, da für diese Versuchs- und Demozwecke davon ausgegangen werden kann, dass die Mechanismen innerhalb der Türsäule gegen Manipulation mechanisch gesichert sind. Um hier von vorne herein einen möglichen Schwachpunkt zu vermeiden, müssen auch auf dem CAN-Bus die Telegramme verschlüsselt werden. Da innerhalb einer CAN-Nachricht maximal nur 8 Datenbytes versendet werden können, empfiehlt sich ein Verschlüsselungsverfahren mit entsprechender Blockgröße. Geeignet erscheint hierbei zum Beispiel das Blowfish-Verfahren von Bruce Schneier [Schneier 1996]. Entsprechende symmetrische Schlüssel müssen dann innerhalb der einzelnen Mechanismen verwaltet werden. Hierfür können die beim EIB/KNX System gewonnenen Erkenntnisse aus Kapitel 5 direkt auf den CAN übertragen werden.

6.3.1 Schnittstellendefinition am CAN-Bus

Um von den verwenden Authentisierungsmechanismen möglichst unabhängig zu sein und bei Bedarf neue Systeme nachrüsten zu können, ist es notwendig, für die auf dem CAN-Bus zu übertragenden Telegramme eine Regel zu definieren. Das entstandene Protokoll ist eine Entwicklung, die auf dem standardisierten CAN2.0A-Protokoll aufsetzt [Etschberg 2002]. Es gibt vor, wie die Daten eines CAN Telegramms interpretiert werden müssen.

Um die Kommunikation zu vereinfachen, benutzt jedes CAN-Modul nur einen einzigen Nachrichten-Identifier, so dass jedes Modul unter einer definierten Adresse erreichbar ist. Dies bedeutet, dass jedes Modul nur Nachrichten auswerten kann, welche an seine Adresse verschickt worden sind. Tabelle 6.1 listet alle CAN-Module mit ihren jeweiligen Adressen auf.

Tabelle 6.1: Zuordnung der 11 Bit CAN-Identifier

Mechanismus	**11 Bit Identifier**
Security Server	0
Smart Card	1
Transponder	2
Spracherkennung	3
Fingerabdruck	4
Personal Area Network	5

Die Adresse 0 (Security Server) nimmt eine Sonderstellung ein. Sie wird von den Modulen als Standardadresse benutzt. Müssen zum Beispiel Module selbständig eine Nachricht versenden, so wird sie an diese Standardadresse geschickt. Die Nachrichten, die über den CAN-Bus verschickt werden können, sind auf maximal 8 Byte Datenlänge beschränkt. Alle Nachrichten haben denselben Aufbau, der in Abbildung 6.10 dargestellt ist.

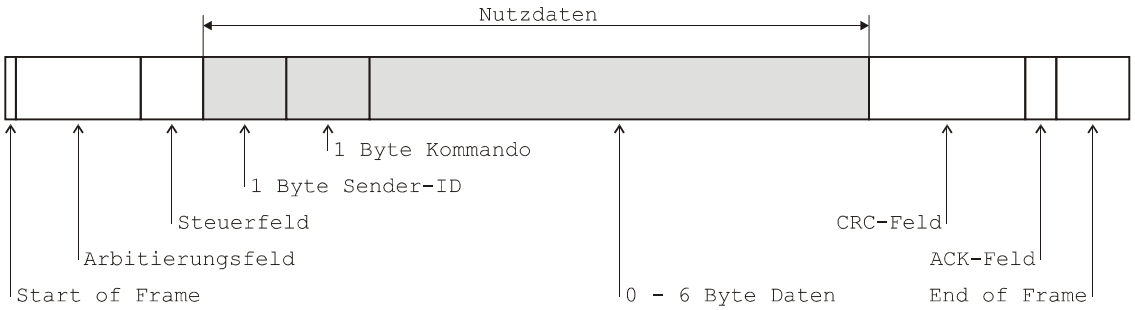

Abbildung 6.10: Aufbau eines CAN-Telegramms

Die Sender-ID ist die CAN-Adresse des Absenders, wobei diese auf 8 Bit beschränkt ist, so dass insgesamt bis zu 255 Zugangsmechanismen adressiert werden können. Wird eine Antwort benötigt, so wird sie an diese Adresse geschickt. Das Kommando-Byte identifiziert die Art der Nachricht. Eine Auflistung aller derzeit vorgesehenen Befehle ist in Abbildung 6.11 zusammengefasst. Jede Nachricht kann 0 bis 6 Byte Daten beinhalten. Ob und wie viele Byte Daten in einem Telegramm zu finden sind, wird durch das Kommandobyte festgelegt.

7	6	5	4	3	2	1	0	
Kommandobyte								
0	0	0	0	0	0	0	1	Status Request, wird von jedem Modul beantwortet
0	0	0	0	0	0	1	0	Status OK, Modul vorhanden und betriebsbereit
0	0	1	0	0	0	0	0	Smart Card Authentisierung starten
0	0	1	0	0	0	0	1	Smart Card Authentisierung OK (4 Byte ID)
0	0	1	0	0	0	1	0	Smart Card Authentisierung fehlgeschlagen (1 Byte Fehlercode)
0	0	1	1	0	0	0	1	Transponder Authentisierung OK (4 Byte ID)
0	0	1	1	0	0	1	0	Transponder Authentisierung fehlgeschlagen (1 Byte Fehlercode)
0	1	0	0	0	0	0	1	Sprache Authentisierung OK (4 Byte ID)
0	1	0	0	0	0	1	0	Sprache Authentisierung fehlgeschlagen (1 Byte Fehlercode)
0	1	0	1	0	0	0	0	Fingerabdruck Authentisierung starten
0	1	0	1	0	0	0	1	Fingerabdruck Authentisierung OK (4 Byte ID)
0	1	0	1	0	0	1	0	Fingerabdruck Authentisierung fehlgeschlagen (1 Byte Fehlercode)
0	1	1	0	0	0	0	1	PAN Authentisierung OK (4 Byte ID)
0	1	1	0	0	0	1	0	PAN Authentisierung fehlgeschlagen (1 Byte Fehlercode)

Abbildung 6.11: Aufbau des Kommandobytes

Die Status-Request-Abfragen dienen zum Auffinden vorhandener Module. Der Server kann mittels dieser Telegramme sehr schnell, zum Beispiel beim Start der Applikation, die vorhandenen Authentisierungsmechanismen ermitteln, so dass der Benutzer sein System ohne Konfigurationsaufwand erweitern kann. Der bei einer fehlgeschlagenen Authentisierung zurückgegebene Fehlercode dient zu Diagnosezwecken während der Entwicklungsphase und ist hier nicht näher beschrieben. Er gibt Auskunft darüber, ob zum Beispiel beim Smart Card Modul ein Kommunikationsfehler auftrat, oder ob ein kartenfremder Gegenstand eingesteckt wurde.

6.3.2 Biometrische Sensoren

Bei der Auswahl von biometrischen Sensoren stehen als messbare Größen der Fingerabdruck, die Stimme sowie das Abbild des Gesichtes oder der Hände im Vordergrund. Weil die Stimme so wie der Fingerabdruck relativ einfach zu erfassen sind und von jedermann stets bei sich getragen werden, konzentrierten sich die Arbeiten hauptsächlich auf entsprechende Sensoren für diese beiden biometrischen Verfahren.

6.3.2.1 Fingerabdruckerkennung

Die Wahl des entsprechende Sensors zur Aufnahme von Fingerabdrücken fiel auf den FingerTIP Sensor der Firma Siemens [TopSec 2000]. Dieser kapazitive CMOS-Sensor hat in der Sensoroberfläche eingearbeitete Kondensatorplatten, mit einer Auflösung von 513 Platten pro Zoll, bei 224 x 288 Sensoren, die in Verbindung mit der Fingeroberfläche vollständige Kondensatoren bilden. Das Prinzip der Fingerabdruckerfassung basiert dabei auf den unterschiedlichen Kapazitäten, welche sich aus dem wechselnden Abstand der Rillen und Hügel des Fingerabdrucks zur Sensorfläche ergeben. Je größer der Abstand, desto geringer die Kapazität. Somit wird ein 8 Bit Graustufenabbild des

Rillenprofils eines Fingers durch den Sensor digitalisiert. Über eine parallele Schnittstelle werden die Bilddaten zur Übertragung an einen Host bereitgestellt.

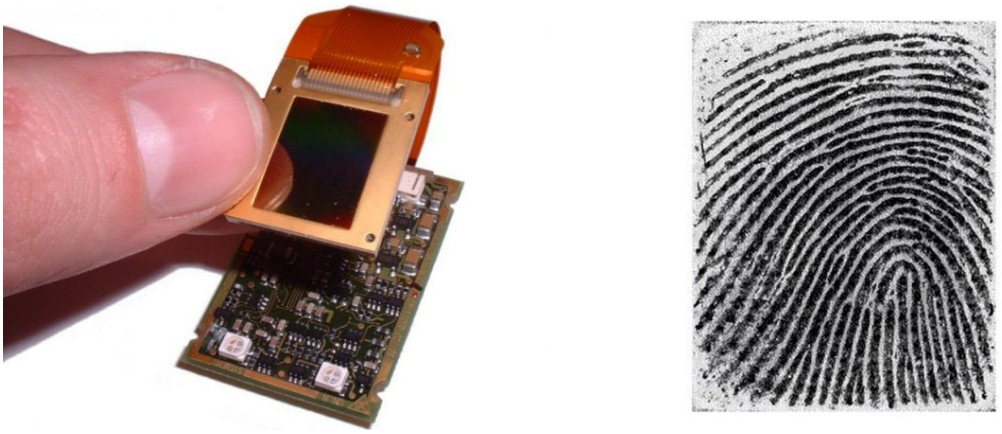

Abbildung 6.12: Siemens FingerTIP Sensor mit ID-Modul und Sensorbild

Ein solcher Host, welcher die aufgenommenen Bilddaten mittels komplexer mathematischer Algorithmen zur Bildverarbeitung aufbereiten und weiterverarbeiten muss, benötigt eine relativ hohe Rechenleistung, um in akzeptabler Zeit Fingerabdrücke zu vergleichen. Eine entsprechende embedded Plattform mit der Bezeichnung TopSec ID Modul, welche in Abbildung 6.12 zu sehen ist, wurde ebenfalls von der Firma Siemens auf den Markt gebracht. Das ID Modul empfängt die Daten des FingerTIP Sensors über die parallele Schnittstelle und kann bis zu 1400 Fingerabdrücke auf dem internen Flashspeicher archivieren. Das Modul unterscheidet mehrere Modi, in denen es betrieben werden kann. Zu erwähnen sind der Autonomous- und Host-Modus. Im Autonomous-Modus arbeitet der Sensor selbständig. Durch ein externes Signal startet das Modul selbstständig einen Authentifizierungsprozess und signalisiert eine Übereinstimmung der extrahierten Merkmale mit einer gespeicherten Referenz über einen Steuerausgang. Im Host-Modus, der für diese Arbeit relevant ist, sind zahlreiche Befehle definiert, über die das Modul konfiguriert und gesteuert werden kann. Ein für diese Arbeit entstandenes Interface steuert den Authentisierungsvorgang und kommuniziert mittels eines CAN-Interfaces mit dem Security Server.

Die biometrischen Eigenschaften des Moduls sind durch eine False Acceptance Rate von $FAR < 1 \cdot 10^{-6}$, sowie einer False Rejection Rate von $FRR < 5 \cdot 10^{-3}$, bei realen Bedingungen und kooperativen Nutzern, angegeben. Die Zeit für das Encoding des Fingerabdrucks liegt bei etwa einer Sekunde, wobei das Matching mit gespeicherten Mustern jeweils 5 ms beansprucht.

Kern des CAN-Interfaces ist der Mikrocontroller AT89C4051 von Atmel. Er führt die Konfiguration der Schnittstellen und die Steuerung des Datenverkehrs über das Interface durch. Die serielle Schnittstelle des Mikrocontrollers wird für die Verbindung mit dem ID Modul verwendet. Ein zweites, wesentlich zur Funktion beitragendes Bauteil ist der Full-CAN-Controller MCP2510 von Microchip. Er erlaubt beliebigen

Mikrocontrollern eine komfortable Kommunikation mit dem CAN 2.0 A/B Protokoll nach ISO 11898. Seine Aufgabe ist es, die CAN-Schnittstelle zu implementieren. Dazu gehört die Aufbereitung der Nachrichten im CAN-Format sowie das Senden und Empfangen der Daten auf dem CAN. Ein Transceiver, wie er auch im Security Server verwendet wird, bereitet die Signalpegel entsprechend dem CAN-Standard auf.

Abbildung 6.13 zeigt die Schaltung des CAN Interface, wie es auf allen Authentisierungsmodulen, die in den folgenden Abschnitten beschrieben werden, realisiert ist. Der vollständige Schaltplan des Moduls zur Authentisierung per Fingerabdruck ist im Anhang zu finden.

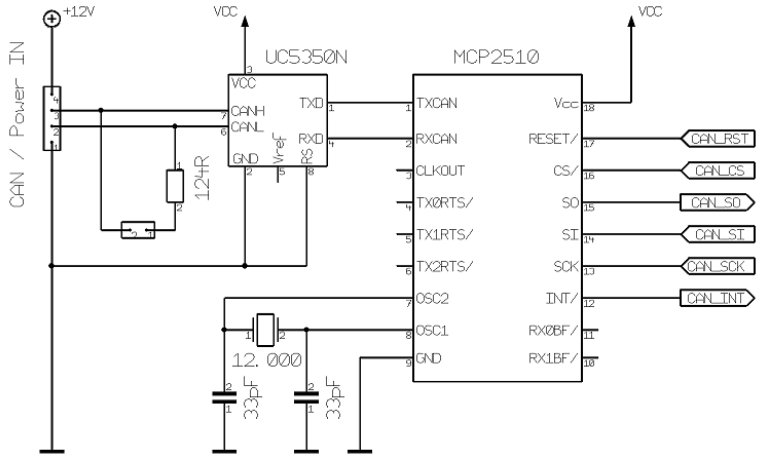

Abbildung 6.13: Schaltplan des CAN-Interface

6.3.2.2 Spracherkennung

Als weiteres biometrisches System entstand ein Modul zur Verifikation per Stimme. Da auch hier, wie bei der Einheit zur Authentisierung per Fingerabdruck, eine kostengünstige embedded Lösung angestrebt war, fiel die Wahl auf eine Hardware aus dem Konsumerbereich. Als Basis zur sprecherabhängigen Authentifizierung dient der Sprachprozessor RSC-300 der Firma Sensory [Sensory 2002]. Dieser Signalprozessor erlaubt die Programmierung von Anwendungen zur Sprachanalyse und Sprachsynthese mit einer ANSI-C Programmierumgebung. Die im Signalprozessor integrierte Hardware umfasst sowohl A/D- als auch D/A-Wandler mit steuerbaren Verstärkern, einen 4 MIPS Prozessorkern mit für die meisten Anwendungen ausreichendem RAM-Speicher und eine Sprachverarbeitungseinheit. Über mehrere I/O-Ports kann Flashspeicher für Anwendungen und Daten, sowie weitere beliebige Hardware angeschlossen werden. Die Softwareentwicklungsumgebung bietet Funktionen zur sprecherunabhängigen und sprecherabhängigen Spracherkennung, die für Anwendungen der Sprecheridentifikation und Sprecherverifikation herangezogen werden können. Das System bietet auch die Möglichkeit des „Continuous Listening“, bei der der Controller fortlaufend alle

Audiosignale analysiert, bis ein Stichwort erkannt wird. Abbildung 6.14 zeigt ein Rapid Prototyping Modul, welches im Rahmen dieses Projektes verwendet wurde.

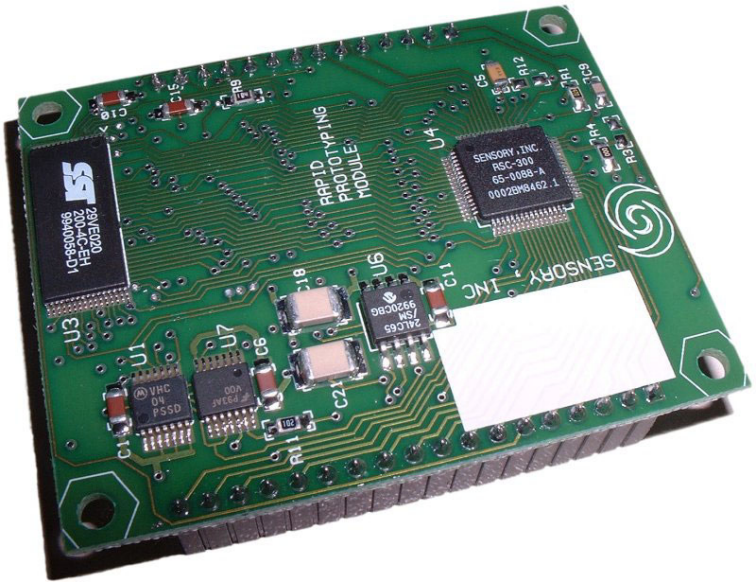

Abbildung 6.14: RSC-300 Prototyping Modul

Ziel der Arbeiten war es, ein kostengünstiges Modul zu entwickeln, dass es mehreren Personen erlaubt, sich an einer Türstation mittels ihrer Stimme zu authentifizieren. Versuche mit dem Prototyping Modul zeigen eine Erkennungswahrscheinlichkeit bei sprecherabhängigen Word-Spot Anwendungen entsprechend der durch den Hersteller gemachten Angaben.

Die biometrischen Eigenschaften des Controllers sind durch eine Equal Error Rate von $EER < 6 \cdot 10^{-2}$ bei leisen Umgebungsgeräuschen angegeben. Unter optimalen Bedingungen (hochwertiges, ausgerichtetes Mikrofon bei geringem Störgeräuschepegel) ist eine Erkennungswahrscheinlichkeit von 99% erreichbar.

Entstanden ist eine Software für den RSC-300 Controller mit einer zweistufigen Sprechererkennung, um den bei einer einstufigen Lösung benötigten Vergleich eines aufgenommenen Musters mit mehr als einem gespeicherten Muster zu vermeiden. Dabei übernimmt die erste Stufe die Auswahl des Benutzers mittels eines Passworts, das jedoch nicht geheim sein muss, da die zweite Stufe den Sprecher anhand seiner eindeutigen Merkmale in der Sprache verifiziert. Die zweite Stufe muss somit aufgenommene Muster nur noch mit einem einzigen Muster vergleichen, da sich der Benutzer bereits mit seinem Passwort identifizieren lässt. In der ersten Stufe wird die Benutzernummer ermittelt, in der zweiten Stufe findet die eigentliche Verifikation statt.

Für Versuchszwecke ist die Einheit mit Tasten ausgestattet, die es erlauben, neue Teilnehmer einzuspeichern. Die Trainingssequenz wird jeweils für die Identifikation und für die Verifikation zweimal aufgenommen. Versuche haben gezeigt, dass sich die Erkennungswahrscheinlichkeit durch drei oder vier Testmusteraufnahmen nicht

wesentlich verbessern lässt. Die gemittelten Testmuster werden im Flashspeicher dauerhaft abgelegt. Jedem Teilnehmer wird hierbei eine eindeutige ID zugewiesen, welche bei erfolgreicher Authentisierung an den Security Server übermittelt wird. Das Modul befindet sich während des Betriebes im Continuous-Listening-Modus, so dass eine Identifikation automatisch stattfindet. Wurde ein Teilnehmer erkannt, fordert das Modul per synthetisierter Sprache dazu auf, sich per Stimme zu verifizieren.

Hardwareseitig ist der RSC-300 Signalprozessor, wie bei der Fingerabdruckerkennung, über einen CAN Controller an den Security Server angebunden. Der entsprechende Schaltplan ist im Anhang dargestellt. Als Mikrofon und Lautsprecher dienen Elemente der Sprechanlage, welche heute zur Grundausstattung einer Türsäule gehören.

6.3.3 Elektronische Schlüssel

Die kostengünstigste und sicherste Methode zur Authentifizierung sind sogenannte elektronische Schlüssel. Diese können in Form von kontaktierbaren oder kontaktlosen Smart Cards, Transpondern oder, wie in Kapitel 2 dargestellt, als Ringe oder Schlüsselanhänger ausgeführt sein. Sicher sind entsprechende Systeme vor allem deshalb, weil moderne Versionen über ein beschränktes Maß an Rechenleistung und Datenspeicher verfügen. Die Daten, die den Benutzer authentifizieren, sind in einem geschützten Speicherbereich abgelegt und können nur unter der Verwendung kryptographischer Funktionen in Verbindung mit geheimen Schlüsselzahlen ausgelesen werden. Dies verhindert das Reproduzieren solcher Schlüssel durch Dritte. Im einfachsten Fall sind solche elektronische Schlüssel als nichtveränderbare Seriennummern realisiert. Das bedeutet, dass bei der Produktion bereits eine eindeutige, nur einmal vergebene Signatur eingebracht wird, die mit einfachen Methoden nicht rekonstruiert werden kann.

6.3.3.1 Smart Card

Chipkarten oder Smart Cards, wie sie häufig bezeichnet werden, haben sich in den letzten Jahren sehr weit verbreitet, da sie durch eine Reihe von interessanten Eigenschaften beschrieben werden können [Rankl 2002]:

- Geringe Abmessungen und hohe mechanische Stabilität
- Niedrige Herstellungskosten
- Implementierung getrennter Anwendungen und Speicherung kleinerer Datenmengen möglich
- Einfache Technik der Chipkartenleseeinheiten
- Lesen und Ändern der Daten ohne großen technischen Aufwand möglich

- Hohe Sicherheit gegen Manipulation und Fälschung durch Einsatz kryptographischer Verfahren

Wegen dieser Eigenschaften eignen sich Chipkarten ideal für den Transport kleiner Datenmengen, die gegen unbefugten Fremdzugriff gesichert und trotzdem schnell veränderbar sein müssen. Die bekanntesten Beispiele für ihren Einsatz sind die Telefon- und Geldkarte. Da zahlreiche Methoden entwickelt wurden, elektronische Schlüssel zum Beispiel zu klonen oder zu manipulieren, muss im Szenario zur Authentisierung an der Eingangstüre alles außerhalb der Smart Card und des Kartenlesers als unbekannt betrachtet werden. Erst wenn sich beim Versuch einer Authentisierung die Smart Card gegenüber dem Kartenleser und dieser wiederum gegenüber der Smart Card als „vertrauenswürdig“ erweisen kann, darf die Karte entsprechende Daten ihres Besitzers an die Leseeinheit übertragen. Ein solches Verfahren wird als Mutual-Authentication bezeichnet und findet bei der Realisierung dieser Arbeit Anwendung.

Für dieses Projekt fiel die Entscheidung für ein Kartensystem auf eine Prozessorkarte für allgemeine Verwendungszwecke. Auf dieser Karte, mit der Bezeichnung „Funcard“, befindet sich der Atmel-Mikrocontroller AT90S8515. Der Controller besteht aus einer 8-Bit CPU, die mit einer maximalen Taktfrequenz von 8 MHz betrieben werden kann. Zudem hat er 8 KByte Flash als Programmspeicher, 512 Byte SRAM und 512 Byte EEPROM mit auf dem Chip. Wie alle Controller dieser Baureihe ist er über ein SPI-Interface (Serial Programming Interface) programmierbar. Da diese Art Mikrocontroller weit verbreitet ist, existiert eine Reihe von Compilern und Werkzeugen zur Programmierung. Zusätzlich zum Mikrocontroller befindet sich auf der Funcard noch ein EEPROM-Speicherbaustein. Dieser Baustein ist der AT24C64, ein serielles EEPROM mit einer Größe von 8 KByte, welches zum Beispiel zur Speicherung von zusätzlichen Benutzerdaten verwendet werden kann. Neben Versorgungsspannung, Masse, Takt und Reset sind die drei Leitungen des SPI-Interfaces herausgeführt. Dies ermöglicht eine Programmierung der Karte, sowie die Kommunikation mit der Gegenstelle, wobei bei dieser Arbeit die Leseeinheit der Master ist.

Die Gegenstelle, welche sich von außen zugänglich an der Tür befindet, besteht ebenfalls aus einem Atmel AT90S8515 Controller, der über eine ähnliche Schaltung wie die biometrischen Systeme mit dem CAN-Bus verbunden ist. Der entsprechende Schaltpan ist im Anhang abgebildet. Zur Authentifizierung der Karte bzw. der Karten aller Benutzer gegenüber der Gegenstelle wurde eine Software nach dem Challenge-Response-Verfahren entwickelt [Paulke 2002]. Das Challenge-Response-Verfahren ermöglicht die Überprüfung eines gemeinsamen Geheimnisses, ohne dieses explizit zu nennen. So kann zum Beispiel die Kommunikation zwischen Karte und Leser abgehört werden, ohne dass das Geheimnis für den Lauscher erkennbar wird. Der Ablauf der Mutual-Authentication mittels des Challenge-Response-Verfahrens ist in Abbildung 6.15 dargestellt.

Eine fremde Leseeinheit hat somit keine Möglichkeit an Daten in der Karte zu gelangen. Das hierbei verwendete Verschlüsselungsverfahren ist der AES-128 Algorithmus, welcher ebenfalls bei der Datenverschlüsselung auf dem EIB/KNX Bussystem innerhalb dieser Arbeit verwendet wird. Der geheime Schlüssel, welcher sowohl der Karte als auch dem Leser bekannt ist, befindet sich jeweils in einem per Hardware gegen Auslesen gesicherten Speicherbereich.

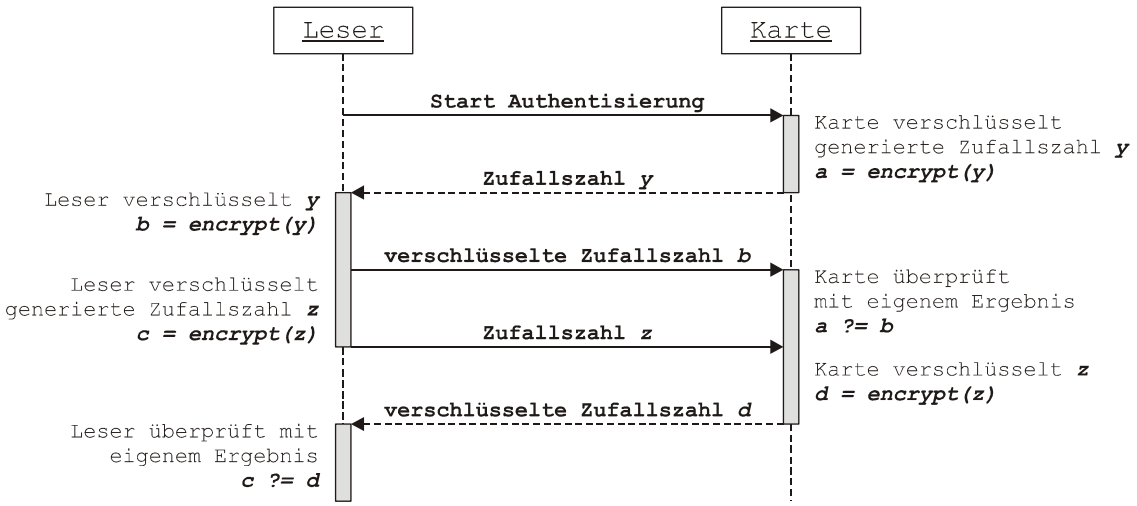

Abbildung 6.15: Ablauf des Challenge-Response-Verfahrens

Die Zufallszahl, welche für das Challenge-Response-Verfahren notwendig ist, wird durch einen Algorithmus erzeugt, der mit einem Initialwert gespeist werden muss. Dieser Wert, der auch als Random Seed bezeichnet wird, wird jeweils neu erzeugt und nach jedem Authentisierungsvorgang wieder in der Karte abgelegt, so dass keine Laufzeitangriffe auf die Pseudo-Zufallszahl ermöglicht werden. Das Chipkartenmodul stellt der „Intelligenten Tür“ eine sehr sichere Methode zur Benutzererkennung zur Verfügung. Derzeit sind auf den Karten 4 Byte Identifier gespeichert, welche dem entsprechenden Benutzer zugeordnet sind. Der Leser und die Karte verwenden denselben geheimen Schlüssel. Um die Sicherheit gegen Plaintext-Crypttext-Angriffe zu erhöhen, könnten beide Systeme unterschiedliche Schlüssel verwenden, die aber auch beiden Teilnehmern bekannt sein müssen. Bei erfolgreicher Authentisierung sendet das Chipkartenmodul ein CAN-Telegram nach den Definitionen im Abschnitt 6.3.1 an den Security Server.

6.3.3.2 Transponder

Transponder sind eine Art „passive Sendeeinheit“. Sie benötigen keine eigene Stromversorgung, sondern werden von einer Transponderleseeinheit induktiv mit Strom versorgt, sobald sie in den Wirkungsbereich des Leser kommen [Finkenz 2002]. Jeder Transponder verfügt in der Regel über eine eindeutige ID. Wird nun ein Transponder in die Nähe eines Lesers gebracht, so sendet dieser seine ID an den Leser, welcher über

seine Sendespule diese Nachricht dekodiert. Da die grundlegende Kommunikation mit dem Transponder sehr aufwendig zu realisieren ist, kommt für diesen Authentisierungsmechanismus der Easy Key Multireader der Firma IQ-Automation zum Einsatz. Die Transponderleseeinheit sendet über eine serielle Schnittstelle die Daten eines im Empfangsbereich befindlichen Transponders, je nach Konfiguration, automatisch an ein Hostsystem.

Das Hostsystem ist in diesem Fall eine Mikrocontrollerschaltung, basierend auf einem 8051 kompatiblen Atmel Controller, der sowohl für die Steuerung des CAN-Interfaces als auch des Transponderlesers zuständig ist. Er liest mit Hilfe des Lesers einen Transponder in Reichweite aus, überprüft dessen ID, und verschickt eine entsprechende Nachricht über das CAN-Interface zum TINI-Board [Paulke 2002]. Abbildung 6.16 zeigt den Aufbau des Transpondermoduls, das aus der Sende-/Empfangsspule, der Leseeinheit und dem Steuercontroller mit der CAN-Anbindung besteht. Entsprechende Schaltpläne sind im Anhang zu finden.

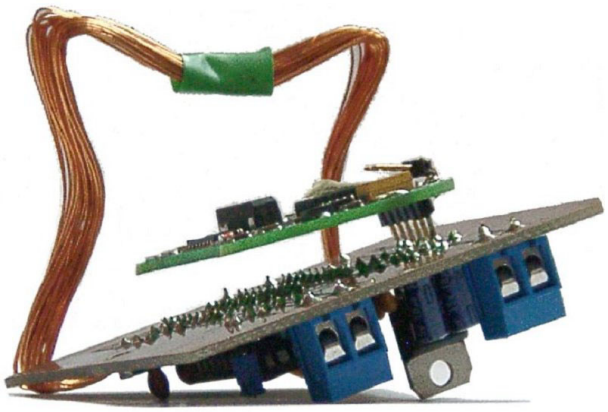

Abbildung 6.16: Multireader mit Hostsystem und Antenne

Grundsätzlich können bei dieser Lösung Transponder der Typen H4002, V4050-64 oder V4050-40 verwendet werden, welche in allen erdenklichen Bauformen (Schlüsselanhänger, Aufkleber, Armbanduhren, Glaszylinder usw.) erhältlich sind. Manche Typen besitzen neben der eindeutigen ID noch zusätzlichen Speicher, der kontaktlos über die Leseeinheit geschrieben und gelesen werden kann. Als System zur Authentisierung bietet die hier verwendete Transpondertechnik die geringste Sicherheit, stellt aber auf Grund der sehr niedrigen Kosten und einfachen Bedienung eine komfortable, zusätzliche Möglichkeit dar.

6.3.3.3 iButton

Sehr gut geeignet zur Zugangskontrolle sind sogenannte iButtons der Firma Dallas Semiconductor [Dallas 2000]. Dies sind 1Wire-Buskomponenten unterschiedlichster Funktionstypen. Sie sind in einem robustem, metallischen Gehäuse, ähnlich einer Knopfzellen Batterie vergossen. Abbildung 6.17 zeigt exemplarisch die Maße eines

einfachen Seriennummern-iButtons. Es gibt passende Halterungen in Form von Schlüsselanhängern oder auch Ausprägungen in Form von Schmuckringen (siehe Kapitel 2).

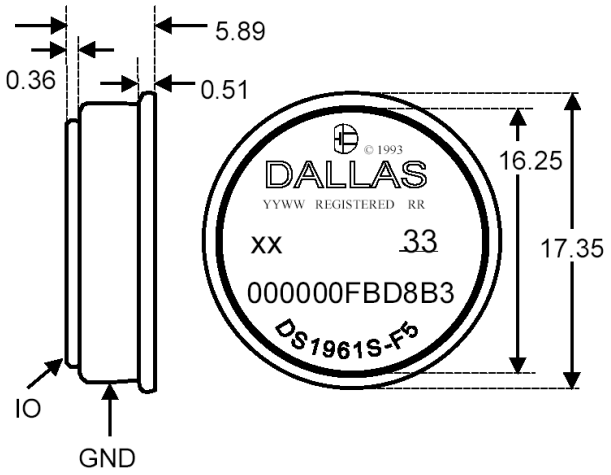

Abbildung 6.17: Darstellung eines iButtons, Quelle: Dallas Semiconductor

Neben einer eindeutigen 64 Bit Seriennummer (8 Bit 1Wire-Typ, 48 Bit ID, 8 Bit Checksumme), die jedes produzierte 1Wire-Element identifiziert, gibt es auch spezielle Crypto-iButtons, die auf einer Java Virtual Machine mit Unterstützung für SHA-1, RSA, DES und tripple DES basieren [JCM 2000]. Dort ist ein kompletter Mikrocontroller samt nichtflüchtigem Speicher integriert, der mehrere, voneinander unabhängige Java-Applets speichern und ausführen kann. Neben der Verwendung zur Authentifizierung gegenüber einem Server, sowie zur Speicherung von Benutzereinstellungen der Hauseinrichtung, sind solche Datenträger auch als elektronische Ausweise oder Geldbörsen geeignet. Der Bewohner drückt den iButton an eine Kontaktiereinheit und stellt somit für kurze Zeit eine Verbindung zum Server und gleichzeitig die notwendige Anbindung an eine Spannungsversorgung her. Dieser kann daraufhin einen verschlüsselten Authentifizierungsvorgang starten, ähnlich der Smart Card, und die gespeicherte Identifikationsinformation auslesen. Diese Technik ist Bestandteil der TINI Java Technologie. Für diese Zwecke ist entsprechende Software im Internet verfügbar. Die Serverklasse OWS im Security Server übernimmt die Kommunikation und ließt die im iButton gespeicherten Daten automatisch aus, sobald ein 1Wire-Element am Bussystem durch einen Polling-Thread erkannt wird. Gegenüber der CONTROL Klasse verhält sie sich wie die Klasse CAN.

6.3.3.4 Personal Area Network

Unter PAN (Personal Area Network) versteht man die kabellose Verbindung zwischen unterschiedlichen elektronischen Geräten, die sich in der Nähe einer Person innerhalb eines Radius von bis zu 10 m befinden. Die Übermittlung der Daten kann per Infrarot, Funk oder Hautkontakt erfolgen. Die Daten über die Haut zu versenden, war die Idee

von Thomas Zimmerman [Zimmer 1996], einem Mitarbeiter des IBM-Forschungszentrum Almaden in Kalifornien, der 1996 zum ersten Mal die neue Datenübertragungsmöglichkeit vorgestellt hat. Diese Idee wurde von IBM nicht weiter verfolgt, da es zur damaligen Zeit keine geeigneten Geräte gab. Mobile Geräte wie Notebooks, Personal Digital Assistants (PDA), Mobiltelefon, oder Armbanduhren, wie sie in den letzten Jahren entwickelt worden sind, könnten mittels dieser Technologie durch Berührung problemlos untereinander digitale Daten austauschen [Zimmer 1999]. Das in Abbildung 6.18 dargestellte Blockdiagramm verdeutlicht das Prinzip, welches der Datenübertragung per Hautkontakt zugrunde liegt.

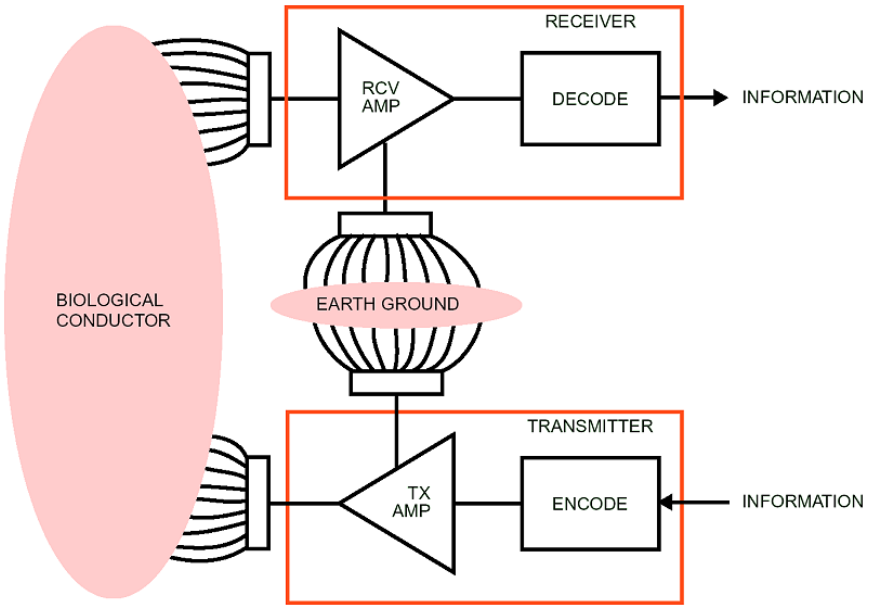

Abbildung 6.18: Prinzipdarstellung eines PAN-Systems, Quelle: IBM Systems Journal

Dieses Prinzip kann beispielsweise verwendet werden, um elektronischen Organizern den Austausch von Visitenkarten zu ermöglichen, sobald deren Träger sich zur Begrüßung die Hände reichen. Der Vorteil gegenüber herkömmlichen drahtlosen Verfahren ist die Schwierigkeit des Abhörens, da zwingend ein Hautkontakt hergestellt werden muss. Die Idee, diesen Mechanismus zur Zugangskontrolle zu verwenden wurde von der bayerischen Firma Ident Technology AG aufgegriffen [Ziegler 2002], aber noch nicht vollständig umgesetzt.

Basierend auf den obigen Kenntnissen entstand im Rahmen dieser Arbeit der Ansatz zur Benutzerauthentisierung gegenüber dem Security Server per Hautkontakt [Crista 2003]. Die Daten werden hierbei nach dem OOK (On/Off Key) Modulationsverfahren bei einer Trägerfrequenz von 250 kHz seriell mit 4800 Bit/s übertragen. Die entsprechenden Schaltungen des Türstations-Interfaces und des Mobilteils sind im Anhang abgebildet. Das Mobilteil ist batteriebetrieben und kann an einer beliebigen Stelle des Körpers getragen werden, solange die Antenne mit der Haut Verbindung hat. Die Türstation benutzt die metallische Türklinke als Sende- und Empfangsantenne, so dass bei ihrer

Berührung eine wechselseitige Datenübertragung möglich ist. Diese Schaltung verfügt auch über ein CAN-Interface, über welches die Authentisierungsdaten an den Security Server übermittelt werden. Sowohl Mobilteil wie auch die Gegenstation basieren auf einem 8051 kompatiblen Mikrocontroller. Prototypen der Schaltungen sind in Abbildung 6.19 dargestellt.

Das Prinzip der Authentisierung basiert auf dem selben Prinzip wie bei der unter 6.3.3.1 vorgestellten Lösung des Smart Card Interfaces. Die Türstation sendet dabei fortlaufend ein Startsignal, so dass ein betriebsbereites Mobilteil, welches sich im Idealfall in einem Stromsparmodus befindet, mit der eigentlichen Authentisierung nach dem Challenge-Response-Verfahren beginnen kann.

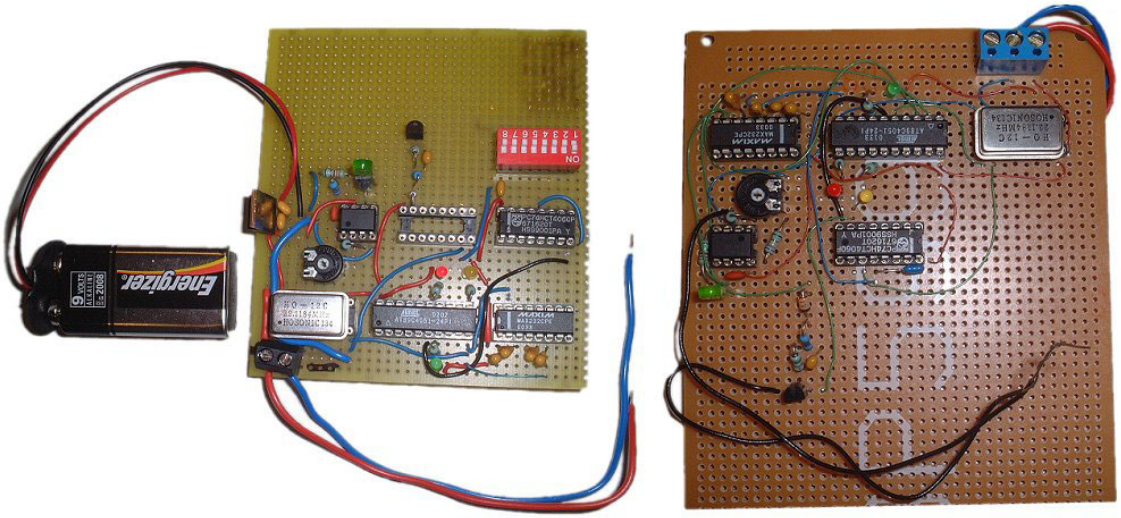

Abbildung 6.19: Experimentelle Prototypen der PAN-Schaltungen

Wie bei dem Smart Card Interface startet das Gerät des Benutzers eine Mutual-Authentication, um sich von der Identität der Türstation zu überzeugen, bevor es deren Anfragen beantwortet. Das AES-128 Verschlüsselungsverfahren kommt auch hierbei zum Einsatz. Da es bei der Datenübertragung leicht zu Unterbrechungen, zum Beispiel durch Zittern, trockne oder nasse Haut, kommen kann, werden alle Nachrichten durch Header- und Trailerzeichen gekennzeichnet. Entsprechende Timeout-Mechanismen veranlassen eine erneute Datenübertragung. Bei erfolgreicher Authentisierung sendet das PAN-Interface ein CAN-Telegram nach den Definitionen gemäß Abschnitt 6.3.1 an den Security Server.

6.4 Die Secure BCU

Um auf dem EIB/KNX verschlüsselt kommunizieren zu können, reicht die Rechnerleistung herkömmlicher Buskoppler, wie sie bisher zur Steuerung von Geräten benutzt wurden, nicht aus. Es war daher notwendig, eine leistungsstärkere Hardware zu

entwerfen, die dem in Kapitel 5 beschriebenen Anforderungen zur gesicherten Datenübertragung gerecht werden kann.

6.4.1 Hardware

Die notwendigen Voraussetzungen, die eine Hardware erfüllen muss, um als eigenständiger, gesicherter Busteilnehmer am EIB/KNX betrieben werden zu können sind hier kurz aufgelistet:

- Geringer Stromverbrauch, um mit über die Busleitungen versorgt zu werden
- Serielle Schnittstelle, sowie analoge und digitale I/O-Leitungen
- Geringe Abmessungen inklusive Programm- und Datenspeicher

Diese Eigenschaften werden nicht von allen Mikrocontrollern gleichzeitig unterstützt, so dass die Wahl auf ein Derivat der Firma Texas Instruments fiel. Die Controller der Serie MSP430 zeichnen sich durch einen äußerst geringen Stromverbrauch bei einer verhältnismäßig hohen Verarbeitungsleistung aus (16Bit RISC, 8 MHz, 250 µA) und stellen zum Programmieren und Debuggen ein JTAG-Interface zur Verfügung. Der Typ MSP430F149 der in dieser Arbeit verwendet wurde, bietet darüber hinaus 60 KByte Flashspeicher, zwei serielle Schnittstellen und Analogeingänge an.

Ziel bei der Entwicklung einer geeigneten Hardware war es, an den primären Schnittstellen der Secure BCU kompatibel zu allen Standard Buskopplern zu bleiben, damit auch weiterhin vorhandene Applikationen betrieben werden können. Dies betrifft die PEI-Schnittstelle, welche im Anhang beim Europäischen Installationsbus beschrieben ist. Der einzige Unterschied liegt dabei bei den Logikpegeln der Schnittstelle, da moderne Controller mit 3,3 Volt anstatt 5 Volt betrieben werden. Eine Einschränkung diesbezüglich betrifft aber nur einen geringen Teil vorhandener Applikationen, da bereits einige Hersteller dazu übergegangen sind, 3,3 Volt Systeme zu entwickeln. Zur Kommunikation mit dem EIB/KNX dient, wie bereits im Abschnitt 6.2.2 beschrieben, ein TPUART-IC der Firma Siemens, welcher auch eine stabilisierte Spannungsversorgung bereitstellt, die aus den Busleitungen gewonnen wird und mit 10 mA belastet werden darf. Abbildung 6.20 zeigt ein vereinfachtes Blockschaltbild aller in der Secure BCU enthaltenen Bausteine und die zugehörigen Verbindungen.

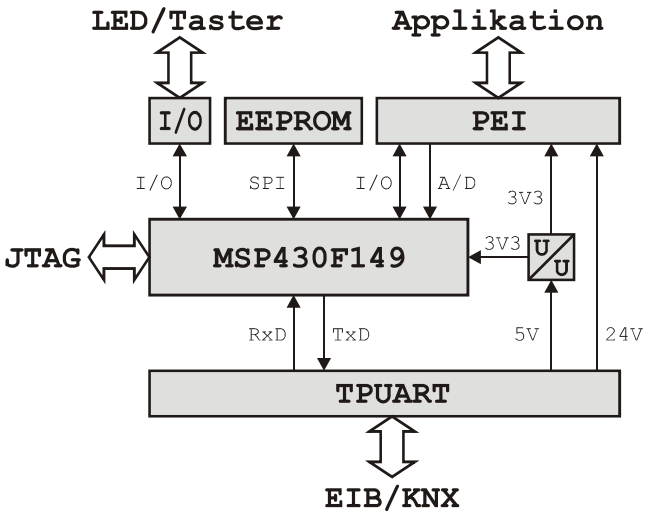

Abbildung 6.20: Blockschaltbild der Secure BCU

Ein zusätzlicher Eeprom-Speicher bietet die Möglichkeit bequem Schlüssel und Objektparameter dauerhaft zu speichern, ohne den internen Flash Speicher zu benutzen. Eine Leuchtdiode und ein Taster, welche Bestandteil eines jeden Buskopplers sind, dienen zum Wechsel und zur Anzeige von verschiedenen Betriebsmoden. Der vollständige Schaltplan der Secure BCU ist im Anhang beigefügt.

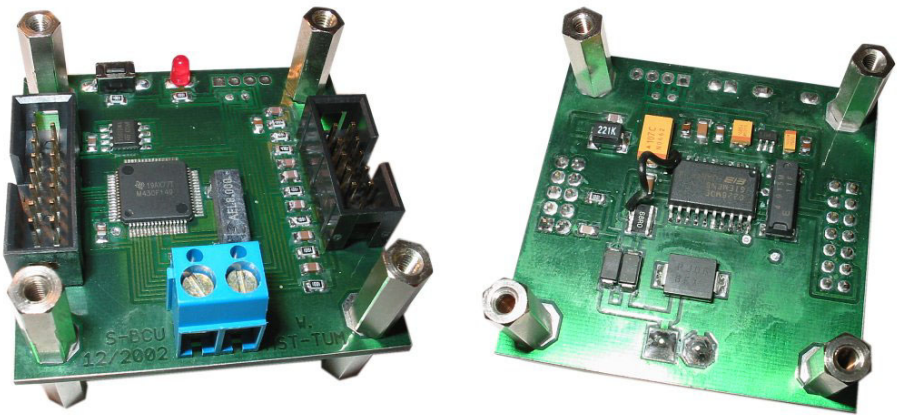

Abbildung 6.21: Ansicht der Ober- und Unterseite der Secure BCU

Abbildung 6.21 zeigt den fertigen Aufbau einer Secure BCU in SMD Technologie, so wie diese zweifach in die Demonstratoreinheit integriert ist. Die Kantenlänge der Prototypen-Platine beträgt 5 Zentimeter. Alle Komponenten finden leicht in einer herkömmlichen Unterputzdose Platz.

6.4.2 Software

Die Software der Secure BCU ist vollständig in C geschrieben und basiert im wesentlichen auf einem interruptgesteuerten Treiber für den TPUART-IC. Der Treiber kapselt die vom TPUART bereitgestellten Funktionalitäten des Physical-Layers und des Link-Layers in der Weise, dass der Empfang von Telegrammen, die über die Adressen der Kommunikationsobjekte an die BCU gerichtet sind, mit einem immediate Acknowledge bestätigt werden. Dieses zeitkritische Detail des Übertragungsprotokolls ist notwendig, um ein wiederholtes Senden des Telegramms zu verhindern. Jede BCU im Netzwerk, die auf diese Gruppenadresse reagiert, sendet diese Bestätigung zur selben Zeit, so dass beim Absender eine Antwort ankommt. Fehlerhaft übertragene Telegramme werden vom TPUART an der Checksumme erkannt und automatisch negativ bestätigt. Im Sendebetrieb übernimmt der TPUART das Wiederholen nicht quittierter Telegramme automatisch. Alle korrekt empfangenen Daten werden in einem Puffer gespeichert und dort durch die restlichen Layer der Protokollstacks bearbeitet. Abbildung 6.22 zeigt den internen Aufbau des Protokollstacks, der sich größtenteils an der IOS/OSI-Struktur standardisierter Buskoppler orientiert.

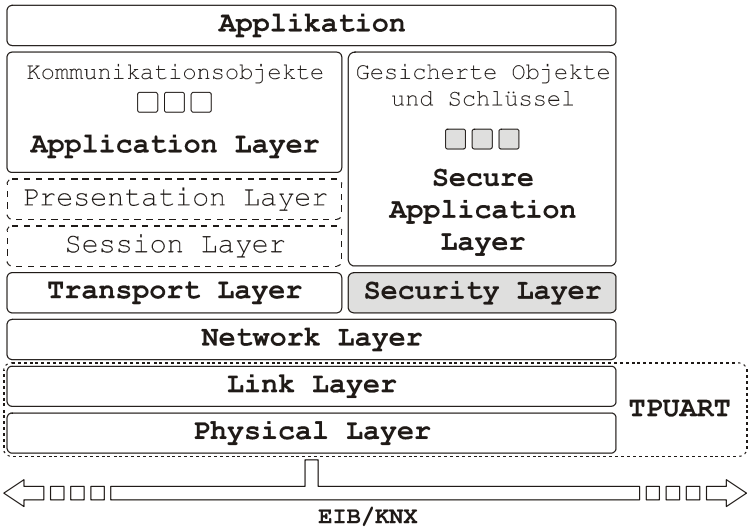

Abbildung 6.22: Interne Layer-Struktur der Secure BCU

Entsprechend Kapitel 5 werden Telegramme, die als gesichert konfigurierte Objekte übertragen, durch den als Security-Layer bezeichneten Programmteil bearbeitet. Hier werden die 16 Byte Nutzdaten mittels des AES-128 Algorithmus ent- bzw. verschlüsselt. Die Implementierung des Algorithmus benötigt dazu circa 2 Millisekunden. Da der vollständige EIB-Protokollstack relativ umfangreich ist und zur Demonstration des gesicherten Übertragungsverfahrens nicht komplett realisiert werden muss, sind im Rahmen dieser Arbeit bisher nur die notwendigsten Elemente integriert worden. Dies sind im Besonderen die Verwaltung von Adress- und Zuordnungstabellen, sowie von Kommunikationsobjekten. Die Applikationen, die die jeweilige Funktionalität eines

Buskopplers bestimmen, werden im Normalfall über den EIB/KNX in den Flashspeicher der BCU geladen. Der dafür notwendige Programmteil zum Aufbau von Transportverbindungen ist in diesen Prototypen nicht integriert, so dass die Software extern geladen werden muss. Vollständige Implementationen eines Protokollstacks für MSP430 Controller sind jedoch am Institut und bei externen Firmen in Entwicklung. Die hier entstandenen Programmteile zur Bearbeitung der gesicherten Datenübertragung lassen sich bei Bedarf schnell in ein bestehendes System integrieren.

6.4.3 Sensor/Aktor-Applikation

Mittels der oben beschriebenen Secure BCU ist es möglich, sicherheitsrelevante Sensoren und Aktoren gemäß der gesicherten Datenübertragung aus Kapitel 5 über ein EIB/KNX-Netzwerk zu verbinden. Um dies innerhalb der Demonstratoreinheit zeigen zu können, entstanden zwei zur Standard-PEI kompatible Applikationen. Die Sensor-Applikation erlaubt das Anbinden einer Meldelinie an eine BCU, die Aktor-Applikation das Ansteuern eines Motorblockschlosses der Firma effeff vom Typ 509. Schaltpläne beider Applikationen befinden sich im Anhang. Zu Demonstrationszwecken wurde statt eines Glasbruchmelders ein Erschütterungskontakt eingesetzt. Die Softwareapplikation der Sensor-BCU wurde so realisiert, dass alle 10 Sekunden der Status des Sensors übertragen wird. Im Falle eines Alarmes (Erschütterung des Fensters) wird sofort ein entsprechendes Telegramm ausgelöst. Der Security Server überwacht die entsprechende Gruppenadresse des Melders und löst je nach Zustand einen akustischen Alarm aus. Trifft länger als 12 Sekunden kein Telegramm ein, weil die Busverbindung unterbrochen wurde, wird ebenfalls der Alarm ausgelöst.

Die Applikation zur Ansteuerung des Motorblockschlosses erlaubt das Verstellen eines elektrischen Motorriegels, sowie das Abrufen der mechanischen Zustände des Blockschlosses (Türe offen/zu, Schloss verriegelt/entriegelt, mechanische Manipulation, unterbrochene Verbindung zur Mechatronik). Ein Mikrocontroller steuert hierbei den Öffnungsvorgang und verhindert Fehlzustände (Türe geöffnet und Riegel ausgefahren). Das Motorblockschloss verriegelt die Türe automatisch im geschlossenen Zustand, so dass diese immer verschlossen ist, wie es von Versicherungsunternehmen gefordert wird. Die zugehörige Softwareapplikation in der Secure BCU verwaltet ein gesichertes Kommunikationsobjekt zur Ansteuerung des Motorriegels und vier normale Objekte die die Zustände des Schlosses und der Tür an den Security Server übermitteln. Bei erfolgreicher Authentisierung an der Tür oder bei Auslösen des Türöffners über die EIB/KNX Visualisierung im Webbrowser steuert der Security Server per verschlüsselten Telgramm das Blockschloss an.

Als zusätzliches Element der Tür ist ein autarker Schließzylinder der Firma Simons&Voss zu nennen, der in der Demonstratoreinheit das Öffnen ohne Authentisierung ermöglicht. Einerseits kann die Tür immer von innen durch drehen des Knaufs geöffnet werden (Panik-Schloss-Funktion), andrerseits kann durch das aktiv gesendete

Signal eines Handsenders der äußere Türknauf mit dem Zylinder verriegelt werden, so dass sich für einige Sekunden auch von außerhalb die Tür öffnen lässt.

6.5 Ausblick

Die Demonstratoreinheit, welche in Abbildung 6.23 von der Vorderseite abgebildet ist, entstand innerhalb der Forschungsprojektes tele-Haus, welches vom 01.10.1999 bis zum 31.03.2003 vom Bildungsministerium für Bildung und Forschung gefördert wurde.

In Zusammenhang mit diesem Projekt entstand ein Doppelhaus für Demonstrations- und Versuchszwecke in Neubiberg bei München. Eine Haushälfte, mit der Bezeichnung tele-Haus stand der Wissenschaft zur Verfügung, die andere Hälfte mit dem Namen VisionWohnen dient dazu, der Öffentlichkeit die Vorzüge eines automatisierten Hauses näherzubringen. Der Demonstratoraufbau wird dort als Teil der durch öffentliche Mittel finanzierten Forschungsergebnisse ausgestellt werden.

Abbildung 6.23: Frontansicht der Demonstratoreinheit

Hinsichtlich zukünftiger Anforderungen an ein System, wie es in dieser Arbeit beschrieben ist, ist die hier vorgestellte Hardware des Security Servers möglicherweise nicht leistungsfähig genug. Speziell die notwenige Leistungsreserve zur Bewältigung höherer Buslasten mit verschlüsselten Telegrammen auf dem EIB/KNX ist bei einem System basierend auf den TINI-Board nicht vorhanden. Zur Zeit der Erstellung diese Dokuments wurde eine neue Version des TINI-Board von Dallas Semiconductor

vorgestellt [DSTINI 2003]. Das DSTINIm400 basiert auf dem neuen DS80C400 Netzwerkcontroller und ist kompatibel zur TINI Runtime Umgebung. Das System ist derzeit noch nicht verfügbar, scheint aber für zukünftige Anwendungen geeignet zu sein.

Einen weiteren Vorschlag für einen leistungsfähigeren Server stellt der in Abbildung 6.24 dargestellte Prototyp dar. Dieser Security Server basiert auf einem embedded Internet PC (IPC@CHIP) der Firma Beck. Der IPC, in Bildmitte, integriert in einem 32 Pin Dual Inline Gehäuse ein 16 Bit Echtzeitbetriebssystem mit File-System, TCP/IP-Stack sowie einem Hardware-Interface-Layer auf einem 80186 Kern.

Abbildung 6.24: IPC-Server mit Compact Flash Erweiterung

Programmiert wird das System in C/C++ und benötigt zum Betrieb am IP-Netzwerk lediglich einen Ethernet-Transceiver. Das dargestellte System ist zusätzlich mit einem Compact Flash Laufwerk ausgestattet um aufwendige Webseiten und mehrere Anwendungen aufzunehmen. Im Anhang ist ein Vorschlag eines vollständigen Schaltplans samt Anbindung an das EIB/KNX-Netzwerk, den CAN-Bus und 1Wire angegeben. Durch die hardwarenahe Programmierung in C/C++ sowie die leistungsstarke CPU sollte eine entsprechende Performance erreicht werden. Eine Java Virtual Machine für das System ist ebenfalls erhältlich. Software für den IPC-basierten Security Server ist bisher nicht entwickelt worden.

7 Zusammenfassung

Die vorliegende Arbeit beschreibt im wesentlichen zwei Themenbereiche der modernen Gebäudesystemtechnik. Dies sind die multimodale Zugangskontrolle und die gegen Missbrauch geschützte Datenübertragung im Steuerbus automatisierter Gewerke. Das Augenmerk liegt dabei auf der Flexibilität und der, nach derzeitigem Stand der Technik, kosteneffektiven Realisierung derartiger Systeme. Die Analyse aller Anforderungen an ein modernes Konzept zur Anwendung diverser Zugangs- und Sicherheitsmechanismen hat zu einer serverbasierten Integrationslösung beider Ansätze geführt.

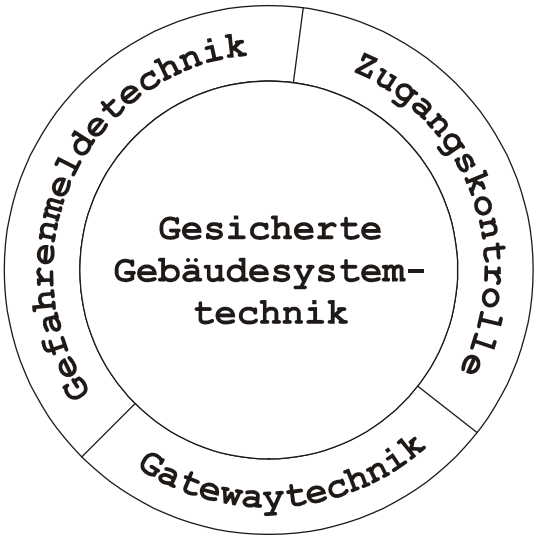

Abbildung 7.1: Technologieintegration um die Gebäudesystemtechnik

Innerhalb dieser Arbeit wird deshalb ein konkreter Vorschlag zur Umsetzung eines entsprechenden Gesamtsystems gemacht, welches sich nahtlos in bereits bestehende Installationen integrieren lässt und zusätzlich Schnittstellen zu weiteren Kommunikationsnetzen bietet. Der dadurch entstehende Mehrwert geht weit über die einfache Zugangskontrolle und gesicherte Datenübertragung hinaus. Die Kombination der Technologien schafft beispielsweise die Voraussetzungen, im Gefahrenfall Rettungswege zu öffnen und einen Notfalldienst zu alarmieren.

7.1 Sensorfusion im Zugangskontrollsystem

Im Kapitel zur multimodalen Zugangskontrolle diskutiert diese Arbeit diverse Aspekte der Fusion von Authentisierungsergebnissen von miteinander verknüpfter Mechanismen. Der Grundgedanke, der hinter dieser Arbeit steckt, ist das Erhöhen der Sicherheit durch Kombination beliebiger biometrischer, besitz- und wissensbasierter Systeme gegenüber einem monolithischen Mechanismus. Hierbei spielt unter anderem der erreichbare Komfort eine wichtige Rolle.

Untersucht wurde vor allem die Möglichkeit, entsprechende Systeme einheitlich zu beschreiben, um definierte Aussagen über die erreichbaren Verknüpfungsergebnisse machen zu können. Neben der einfachen Konjunktion und Disjunktion der booleschen Aussagen werden in der Arbeit weitere Entscheidungsstrategien vorgestellt. Schließlich werden zugehörige Berechnungsvorschriften gesammelt, die automatischen Systemen das Aufstellen der geeignetsten Fusionsstrategien erlauben, so dass anhand eines Kriteriums das Systemverhalten bestimmt werden kann.

Die Betrachtung unterschiedlicher Strategien hat ergeben, dass die Verknüpfung der Authentisierungsergebnisse nicht zwangsläufig eine Verbesserung der Zugangskontrolle zufolge hat. Es ist vielmehr möglich, das statistische Verhalten innerhalb gewisser Grenzen mehr in den konservativen oder liberalen Entscheidungsraum zu verschieben. Dies kann dazu dienen, ein Zugangssystem zu entwickeln, das sicherer oder auch weniger empfindlich gegenüber Störungen ist.

7.2 Verschlüsselte Datenübertragung im EIB/KNX

Feldbusse der Gebäudesystemtechnik, welche sich bis heute am Markt der Automatisierungstechnik profilieren konnten, kommen erst jetzt großflächig zum Einsatz. Dies liegt zum Großteil an den aktuellen Herstellungsverfahren und an zahlreichen Vermarktungsstrategien der Hersteller. Die eingesetzten Verfahren zur Übertragung der Steuerungsinformationen reichen deshalb heutigen, anspruchsvollen Anwendungen in Punkto Authentizität und Vertraulichkeit der übertragenen Daten nicht mehr. Feldbusse dieser Art finden daher kein Marktsegment im Bereich der Sicherheitstechnik.

Das in dieser Arbeit vorgestellte Verfahren zur verschlüsselten Datenübertragung im EIB/KNX-Bussystem schließt diese Lücke. Die genaue Untersuchung des standardisierten Übertragungsverfahrens erlaubt die Einbettung gesicherter Steuerungsinformationen in das objektbasierte Synchronisationsverfahren des bestehenden Standards. Mit Hilfe des anerkannten, aktuell standardisierten, symmetrischen Verschlüsselungsverfahren AES ist es gelungen, die Integrität, Authentizität und Vertraulichkeit der Steuerungsinformationen zu realisieren. Das AES-128 Verfahren dient dabei sowohl zum Generieren symmetrischer Schlüssel, als auch zum Erzeugen von Pseudozufallszahlen und zur Stromchiffrierung. Das als SEIB bezeichnete Übertragungsprotokoll greift in Form einer zusätzlichen Protokollebene direkt in den Kommunikationsstack ein. Dies führt dazu, dass sowohl ein Mischbetrieb der Standardübertragung als auch der gesicherten Übertragung über Linien- und Bereichskoppler hinweg nach dem Multicast-Prinzip möglich ist. Die unidirektionale Übertragung ist konform zum Standardverfahren und erhöht somit die Buslast je nach Anwendungsfall nur geringfügig. Die einzige Einschränkung liegt bei der maximalen Größe der zu synchronisierenden Objektzustände, so dass bis zu 10 Byte Nutzdaten je Telegramm übertragen werden können. Darüber hinaus werden Verfahren zur Programmierung entsprechender Buskoppeleinheiten vorgestellt, die eine Manipulation durch unbefugte Personen verhindern. Auch für die

Inbetriebnahme, Re-Synchronisation und das Rücksetzten von Buskopplern werden entsprechende Maßnahmen und Dienste definiert.

Hauptanwendungsgebiet für die gesicherte Datenübertragung im EIB/KNX ist die Alarmierungstechnik von Gefahrenmeldern. Mittels des vorgestellten Verfahrens können sowohl im Wohn- wie auch im Zweckbau zur bereits vorhandenen Gebäudesystemtechnik diverse Meldelinien integriert werden. Sicherheitskritische Aktoren wie Türöffner oder Fensterantriebe lassen sich genauso in das Netzwerk einbinden wie Authentisierungsmechanismen oder Zeiterfassungssysteme.

7.3 Integration in ein Gesamtsystem

Um die Funktionsweise der diversen Zugangs- und Sicherheitsmechanismen dieser Arbeit evaluieren und nachweisen zu können, entstand ein Versuchsaufbau. Diese, im Rahmen des durch das Bundesministerium für Bildung und Forschung geförderten Verbundprojektes tele-Haus entwickelte Demonstratoreinheit, vereint eine EIB/KNX Installation mit diversen Sensoren und Aktoren, sowie eine mit Motorblockschloss ausgestattete Türe.

Mit Hilfe dieses Demonstrators konnte ein embedded Server, basierend auf einem mit Java programmierten TINI-Internetinterface, entwickelt werden. Der Server stellt sowohl TCP/IP basierte Internetdienste als auch Hard- und Softwareschnittstellen zum EIB/KNX-Gebäudebussystem und zu den per CAN vernetzten Authentisierungsmechanismen bereit. Hier sind definierte Schnittstellenprotokolle entstanden, die es erlauben, diverse Zugangsmechanismen zu integrieren, um die Authentisierungsergebnisse im Server entsprechend der beschriebenen Strategien weiterzuverarbeiten. Die Arbeit beschreibt unter anderem die Umsetzung von Diensten zur Konfigurierung und Visualisierung des Gesamtsystems per browserbasierten Internetclients.

Zur Authentisierung der Personen kommen neben einer Fingerabdruckserkennung, einem Transponder- und iButton-Interface eine eigens dafür entwickelte Lösung zur Spracherkennung und eine Smart Card Schnittstelle zum Einsatz. Darüber hinaus wird ein konkreter Vorschlag für ein Zugangssystem auf PAN-Technologie gemacht. Dieses besitzbasierte System ermöglicht die Authentisierung mittels Datenübertragung per Hautkontakt.

Ein weiteres Kernelement dieser Arbeit ist die Entwicklung einer leistungsstarken Buskoppeleinheit für den EIB/KNX. Mit diesen Netzwerkknoten konnte die verschlüsselte Datenübertragung realisiert werden. Im System des Demonstrators bilden diese eine Meldelinie zum Überwachen von Gefahrenmeldern sowie eine Aktorapplikation zur Steuerung des Motorblockschlosses.

7.4 Marktchancen

Da abzusehen ist, dass das Konnex-System als Vereinigung des EIB, EHS und BatiBUS in naher Zukunft neben LON das in Europa meistverbaute Steuerbussystem der Gebäudesystemtechnik bleiben wird, liegt es nahe, alle Anforderungen mit diesem Standard zu erfüllen. Gerade im privaten Wohnungsbau, wo das Bedürfnis nach Sicherheit und Komfort sehr ausgeprägt ist, die Kosten aber eine entscheidende Rolle spielen, könnte ein umfassendes Sicherheitskonzept, wie es in dieser Arbeit vorgestellt wird, etabliert werden.

Der Anwender selbst könnte nach dem Baukastenprinzip, entsprechend seiner Mittel und seines Sicherheitsbedürfnisses, über die Ausbaustufe seiner Anlage bestimmen. Der erreichbare Mehrwert durch die Bildung eines Gateways zwischen den unterschiedlichen Bussystemen und durch die Vereinigung der Steuerungstechnik mit der Gefahrenmeldetechnik wird dem steigenden Anspruch der Kommunikationstechnik gerecht. Die Entscheidung, ob ein Maximum an Sicherheit oder an Komfort erreicht werden soll, liegt dabei einzig und allein am Administrator des Systems.

Anhang A: Der Europäische Installationsbus

A.1 Entstehung und Verwendung

Der Europäische Installationsbus (EIB) stellt im wesentlichen ein Feldbussystem dar, das zu Begin der 90er Jahre im Zuge der sich immer weiter verbreitenden Gebäudesystemtechnik entwickelt wurde. Das Bussystem wurde hauptsächlich konzipiert zur Steuerung von Beleuchtungs-, Heizungs-, Klima- und Lüftungsanlagen in öffentlichen Gebäuden, Industrie- und Bürokomplexen. Der Vorteil gegenüber der herkömmlichen Elektroinstallation liegt in der Interoperabilität der einzelnen Gewerke. Das heißt zum Beispiel, dass die Messwerte einer EIB fähige Wetterstation sowohl von EIB kompatiblen Heizungsanlagen, Beleuchtungssteuerungen als auch Sonnenverdunklungen genutzt werden können, um diese automatisch zu steuern. Der EIB erlaubt es, wie jedes andere Bussystem auch, alle angeschlossenen Geräte von einer beliebigen Stelle aus zu überwachen und zu steuern, was diesen ursprünglich besonders für große Gebäudekomplexe interessant gemacht hatte [Jeanrond 1996]. Innerhalb der letzten Jahre allerdings konnte durch konsequente Weiterentwicklung und höhere Integration der Komponenten ein niedrigeres Preissegment anvisiert werden, was die Gebäudeautomatisierung nun auch für den privaten Bereich (Ein- und Mehrfamilienhäuser) attraktiv macht. Hinzu kommt, dass alle „echten“ EIB Geräte durch die European Installation Bus Association (EIBA) zertifiziert werden müssen, um die Kompatibilität unter den einzelnen Herstellern zu garantieren. Der Endanwender kann sich sicher sein, dass er an keinen Hersteller gebunden ist und auch, zumindest für die Lebenszeit des Objektes, die Anlage instandhalten und erweitern kann. Alle technischen Details des Systems sind im EIBA Handbook [EIBA 1999] spezifiziert. Von der EIBA wird auch die EIB Tool Software (ETS) vertrieben, mit der ein fachkundiger Elektroinstallateur eine EIB Installation planen, konfigurieren und in Betrieb nehmen kann. Im Folgenden werden die notwendigsten technischen Eigenschaften des EIB beschrieben, speziell des Twisted Pair Mediums, das im Rahmen dieser Arbeit verwendet wurde.

A.2 Technische Grundlagen des Bussystems

Zur Übertragung der Signale des EIB sind derzeit vier Medien definiert. Dies sind die Twisted Pair Verkabelung (EIB-TP) und die Powerline Übertagung (EIB-PL) auf den 230 Volt Installationsleitungen, bei denen die Buskoppler, die weiter unten beschrieben werden, über die Signalleitungen mit Energie versorgt werden. Als drahtloses Medium wurde die Übertragung per Funk (EIB-RF) in den letzten Jahren entwickelt. Zusätzliche wurde die Infrarotübertagung sowie die Datenübertagung per Glasfaser in die Spezifikationen der EIBA aufgenommen.

Die EIB.net Spezifikation schließlich ermöglicht es, den EIB mit allen Medien zu nutzen, die einen logischen Linklayer nach ISO/IEC 802-2 zur Verfügung stellen. Von

besonderem Interesse ist hier das Ethernet. Auf Basis einer erweiterten Spezifikation kann das Internet Protokoll (IP) benutzt werden, um EIB Daten transparent im LAN zur übertragen. So ist es beispielsweise möglich, mehrere, örtlich voneinander getrennte Installationen zusammen zu betreiben.

Dies ist möglich, da sich alle Teilnehmer am EIB an der im ISO/OSI-Referenzmodell (International Standard Organisation's Open System Interconnection Modell) definierten Layerstruktur orientieren. Einzige Ausnahme im EIB Modell sind die Session- und Presentationlayer, welche die Daten transparent passieren lassen, da diese für spätere Erweiterungen reserviert sind. Abbildung A.1 zeigt diese Protokollstruktur des EIB.

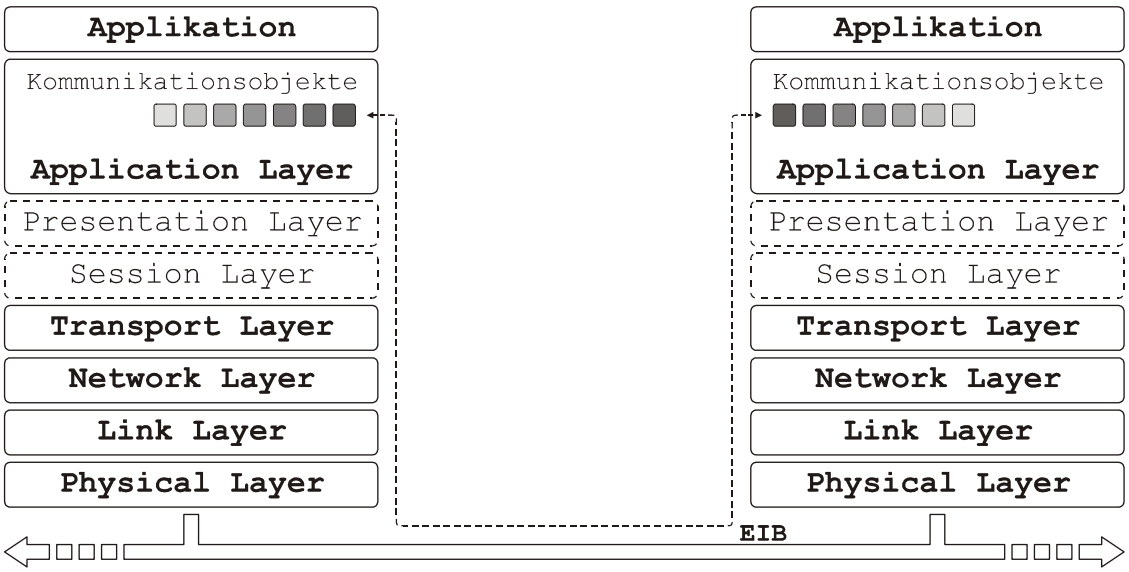

Abbildung A.1: ISO/OSI Layerstruktur des EIB

Auf Grund dieses Modells ist es am EIB möglich sowohl verbindungslos mit einem, mehreren oder allen Teilnehmern als auch verbindungsorientiert mit einem spezifischen Teilnehmer zu kommunizieren. Die meistgenutzte Variante ist die Gruppenkommunikation (verbindungslose Kommunikation mit mehreren Teilnehmern). Folgend sollen kurz die wichtigsten Layer und deren Funktion für den EIB beschrieben werden.

A.2.1 Der Physical-Layer von EIB-TP Netzwerken

Das dieser Arbeit zugrunde liegende EIB-TP System ist die am häufigsten eingesetzte Variante des EIB, da dieses Medium von den meisten Anbietern unterstützt wird und von Anfang an am weitesten entwickelt wurde. Die Datenübertragung über das Twisted Pair Medium hat folgende Charakteristik:

- Gleichzeitige Übertragung von Daten und Versorgungsspannung (30 Volt DC) über ein Adernpaar bei Einhaltung der SELV (Safety Extra Low Voltage) Sicherheitsbedingungen
- Seriell asynchroner Datentransfer, gleichspannungsfrei im Basisband bei 9600 Bit/s
- Halbduplexe, byteorientierte Kommunikation

Die für heutige Verhältnisse sehr geringe Datenrate von 9600 Bit/s hat den großen Vorteil, dass bei der Installation keine Ansprüche bezüglich Abschlusswiderstände oder der gewählten physikalischen Topologie gestellt werden.

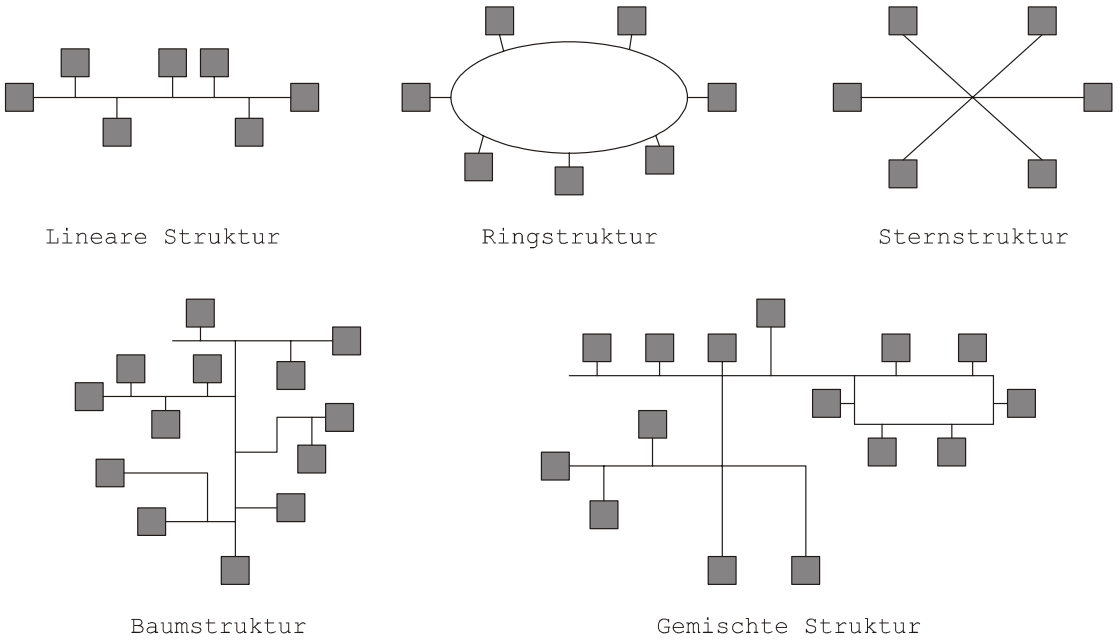

Abbildung A.2: Physikalische Topologien

Alle in Abbildung A.2 dargestellten Busstrukturen können mit dem EIB realisiert werden, solange folgende Grenzwerte eingehalten werden:

- Maximal 64 Busteilnehmer dürfen in einer Linie betrieben werden bei EIB-TP64[1]

[1] TP64 ist der ursprüngliche EIB Standard, eingeschränkt durch die Leistungsfähigkeit des verwendeten Netzteiles und der elektrischen Kopplung der Busteilnehmer. TP256 erlaubt bis zu 256 Teilnehmer pro physikalischem Segment, wobei der logische Adressraum vollständig ausgenutzt wird und insgesamt mehr als 65000 Geräte adressierbar sind.

- Die Leitungslänge innerhalb eines elektrischen Segments (Segmente werden durch Router gebildet) darf 1000 m nicht überschreiten
- Der Abstand zwischen zwei Buseilnehmern darf nicht größer als 700 m sein
- Der Abstand zwischen einer Spannungsversorgung und dem ersten Teilnehmer muss weniger als 350 m sein

A.2.2 Der EIB-Link-Layer

Die für den Buszugriff notwendigen Funktionen werden innerhalb des Link-Layer definiert. Der Zugriff selbst geschieht beim EIB nach dem CSMA (Carrier Sense Multiple Access) Verfahren, wobei Kollisionen durch eine CA (Collision Avoidance) Technik vermieden werden. Falls mehrere Teilnehmer nach einer definierten Zwangspause auf dem EIB gleichzeitig senden, entscheiden Prioritäts-Flags darüber, wer den Zugriff erhält. Für diese Arbitrierung dienen die am EIB übertragenen, dominanten 0-Bits. Bei gleicher Priorität entscheidet die im Telegramm an zweiter Stelle übertragene, eindeutige physikalische Adresse des Teilnehmers. Die Übertragung einer Checksumme über das ganze Telegramm dient zur Sicherung der Daten, welche stets von den jeweiligen Kommunikationspartnern per Acknowledge-Zeichen positiv oder negativ beantwortet werden. Da die Teilnehmer am EIB in der Regel einfache Mikrocontroller zur Datenverarbeitung verwenden, können diese auch mit einem Busy-Zeichen antworten, wenn nicht garantiert werden kann, dass alle ankommenden Daten in kurzer Zeit verarbeitet werden können. Ein Teilnehmer wiederholt den Sendevorgang bis zu dreimal mit markiertem Repeat-Flag.

A.2.3 Der EIB-Network-Layer

Im Network-Layer werden die Adressierungsarten des EIB unterschieden und die entsprechenden Dienste aufgerufen.

Physikalische Adresse															
Oktett 0								Oktett 1							
7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
Bereich				**Linie**				**Teilnehmer**							

Abbildung A.3: Aufbau der physikalischen Adresse

Die grundlegende Art ist die physikalische Adressierung, da es sich beim EIB um ein vollständiges Peer-to-Peer Netzwerk, in dem bis zu 2^{16}=65536 Geräte adressiert werden können, handelt. Der Raum für die physikalischen, im Netzwerk eindeutig zugewiesenen Adressen, wird dabei in drei logische Teile unterteilt. Dies sind die Teilnehmer,

Linien und Bereiche. Abbildung A.3 zeigt die Unterteilung der 16 Bit physikalischen Adresse.

Die strikte Unterteilung der Adressen in Bereiche, Linien und Teilnehmer resultiert aus der im Abschnitt A.2.1 beschriebenen physikalischen Aufteilung in elektrische Segmente. Linien und Bereiche werden mittels Linien- und Bereichskopplern getrennt, welche wiederum EIB-Teilnehmer darstellen.

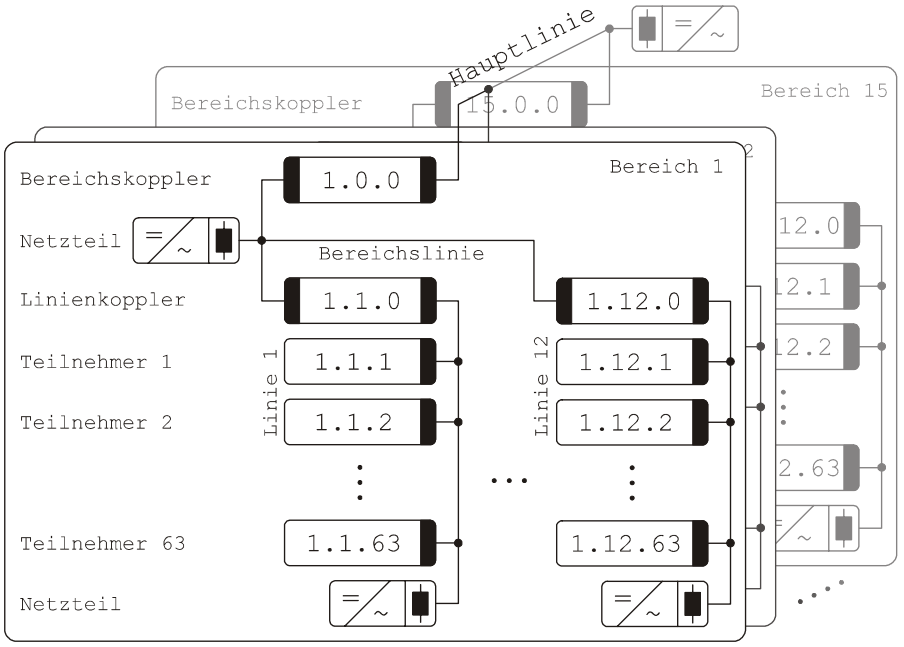

Abbildung A.4: Logische Topologie des EIB-TP64

Abbildung A.4 zeigt die vollständige physikalische und logische Topologie eines EIB-TP64 Netzwerkes. Das Einhalten dieser Zuordnung ist zwar nicht zwingend notwendig, hilft dem Installateur aber dabei, schon bei der Planung Fehler zu vermeiden. Linien könnten beispielsweise innerhalb einer Abteilung mehrere Büros versorgen und Bereiche ganze Stockwerke darstellen, welche durch die Hauptlinie verbunden sind. Ein weiterer Vorteil dieser Unterteilung ist das kontrollierte Routing innerhalb des Netzwerkes. Da die physikalische Adresse Bestandteil der auf dem EIB übertragenen Telegramme ist, können Linien- und Bereichskoppler auch die Aufgabe von Firewalls übernehmen, sofern in diesen Adressfilter für physikalische Adressen eingerichtet sind. Die eigentliche Aufgabe der Linien- und Bereichskoppler ist das Ausfiltern von Telegrammen die an Kommunikationspartner gerichtet sind, die sich nicht innerhalb eines an den Koppler angeschlossenen elektrischen Segments befinden oder deren Routingzähler abgelaufen ist.

Die am meisten beim EIB verwendete Art der Adressierung ist die Gruppenadressierung. Diese Art der Adressierung stellt für ein Gebäudebussystem die effektivste Weise zur Steuerung von Geräten dar. Basierend auf den sogenannten Kommunikationsobjekten werden in den Busteilnehmern Zustände von Geräten und Messwerte über eine

Multicast-Adressierung synchronisiert. Da alle versendeten Telegramme von allen Teilnehmern im selben elektrischen Segment, bzw. auch dort wo diese Telegramme geroutet werden, zu empfangen sind, kann die maximale Anzahl von Teilnehmern mit nur einem Telegramm erreicht werden. Die Buslast kann auf diese Weise sehr gering gehalten werden. Abbildung A.5 zeigt den Aufbau einer Gruppenadresse und deren Unterteilung in Haupt- und Untergruppe. Oft wird die Untergruppe zusätzlich noch in eine Mittelgruppe unterteilt.

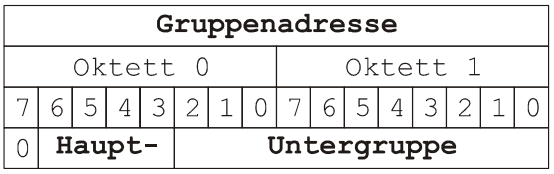

Abbildung A.5: Aufbau der Gruppenadresse

Diese logische Unterteilung hilft dem Installateur bei der Realisierung von EIB-Netzwerken. Unterschiedliche Systeme (z.B. Beleuchtung, Heizung und Sonnenschutz) können so auf Grund ihrer Funktion oder auch ihrer räumlichen Zuordnung in verschiedene Gruppen unterteilt werden. Kommunikationsobjekte, welche durch diese Gruppenadressen eindeutig im Netzwerk adressiert werden, können im einfachsten Fall einen booleschen Wert (Licht an oder Licht aus) darstellen. Die entsprechende Zuordnung wird im Application-Layer hergestellt.

Neben den oben erwähnten beiden Adressierungsarten gibt es am EIB noch die Broadcast-Adressierung zum Auffinden von Busteilnehmern, die per Lerntaste in einen speziellen Zustand gebracht wurden, um sie während der Inbetriebnahme erstmalig programmieren zu können. Die letzte Adressierungstechnik ist das Polling-Verfahren. Diese eher selten verwendete Technik ermöglicht es, von bis zu 14 Teilnehmern in einer Linie, in nur einem Telegramm Werte abzufragen. Den Teilnehmern wird hierbei jeweils ein Zeitschlitz innerhalb eines Telegramms zugewiesen, in denen diese ihre Daten übertragen.

A.2.4 Der EIB-Transport-Layer

Im Transport-Layer werden ausschließlich verbindungsorientierte Datenübertragungen zwischen zwei Busteilnehmern gesteuert. Diese Art der Kommunikation wird beim EIB für die Übertragung der Applikationsprogramme und eine Reihen von Konfigurations-aufgaben während der Inbetriebnahme von Busknoten verwendet. Mittels mehrerer Timer sowie einer Nummerierung der Datenpakete wird die Kommunikation überwacht, so dass fehlerhafte Verbindungen erkannt und gegebenenfalls abgebrochen oder neu initialisiert werden.

A.2.5 Der EIB-Application-Layer

Die oberste Ebene im Protokollstack ist der Application-Layer. Wie in Abbildung A.1 zu sehen ist, werden hier die sogenannten Kommunikationsobjekte verwaltet. Diese, durch die Gruppenadressen eindeutig adressierten Variablen, stellen die Schnittstelle zur eigentlichen Applikation dar. Die Applikation, in Form eines kleinen Programmcodes, liest beispielsweise den elektrischen Zustand eines Schalters ein und schreibt diesen in das zugeordnete Kommunikationsobjekt, oder steuert ein Lastrelais je nach Inhalt der entsprechenden Variable. Der Application-Layer veranlasst bei Änderungen das Versenden des Objektes, bzw. meldet an die Applikation wenn sich ein Zustand geändert hat. Die Zustände aller Kommunikationsobjekte mit gleicher Adresse innerhalb eines EIB-Netzwerkes werden auf diese Weise synchronisiert, so dass zu jedem Zeitpunkt, abgesehen von der Übertragungsdauer, ein eindeutiges Prozessabbild entsteht [Weinzierl 2001].

A.3 EIB-Telegramme und der Interworking Standard

Über die im vorigen Abschnitt gezeigten Layer des Protokollstacks sind die Telegramme, welche über den EIB übertragen werden, genau definiert. Abbildung A.6 zeigt den Aufbau eines vollständigen EIB-Telegramms. Die maximale Länge von 23 Byte bezieht sich auf Telegramme, die den gesamten Nutzdatenbereich benötigen. Tatsächlich können auf dem EIB auch deutlich längere Telegramme übertragen werden, sogenannte „Long Frames“, welche aber bisher nicht genauer spezifiziert wurden.

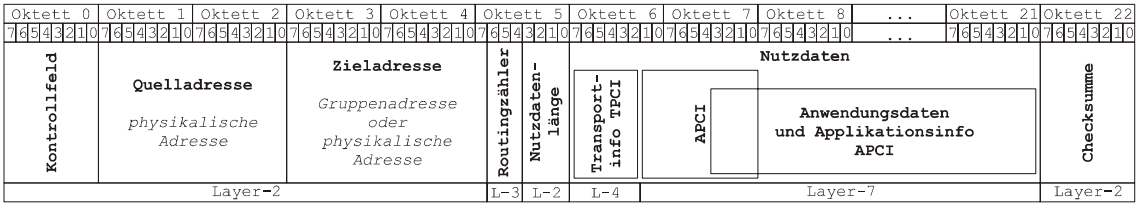

Abbildung A.6: Aufbau eines EIB-Telegramms

Die eigentlichen Nutzdaten, die in der Layer-7 Protocol Data Unit (PDU) übertragen werden, sind über den Interworking Standard definiert. Dieser beschreibt wie Messwerte und Steuerinformationen codiert sein müssen, damit garantiert ist, dass Geräte unterschiedlicher Hersteller miteinander kommunizieren können. Folgende Basisformate sind definiert:

- boolean (1 Bit)
- (un)signed short (16 Bit)
- (un)signed long (32 Bit)

- short float (16 Bit)
- IEEE float (32 Bit)
- Datum (24 Bit)
- Uhrzeit (24 Bit)
- Steuerformate wie Schalten, Dimmen und Motorkontrolle

Mittels dieser EIS-Typen (EIB Interworking Standard) können Werte nahezu aller physikalischen Größen wie Temperatur, elektrische Energie und Leistung oder Helligkeit übertragen werden. Besonders für Anlagen der Gebäude- und Heimautomatisierung entstand eine große Reihe von standardisierten Datentypen, an denen sich die jeweiligen Hersteller orientieren.

A.4 Die Buskoppeleinheit

Neben den Netzteilen, welche die elektrischen Segmente eines EIB-Netzwerkes mit Strom versorgen, sind die Buskoppeleinheiten (BCU) die wichtigsten Komponenten. Sie sind die eigentlichen Teilnehmer am EIB und müssen den oben beschriebenen Protokollstack realisieren. Grundsätzlich besteht ein Busteilnehmer aus zwei Einheiten, der Bus Access Unit (BAU) für den physikalischen Zugriff auf den Bus und dem Application Module (AM). Das AM ist im wesentlichen ein Mikrocontroller, der neben dem EIB-Kommunikationsstack die Anwendungssoftware enthält und über das Physikalische Externe Interface (PEI) mit der Anwenderschaltung verbunden ist. Abbildung A.7 zeigt den schematischen Aufbau einer BCU, wie sie von diversen Herstellern in unterschiedlichen Bauformen erhältlich ist.

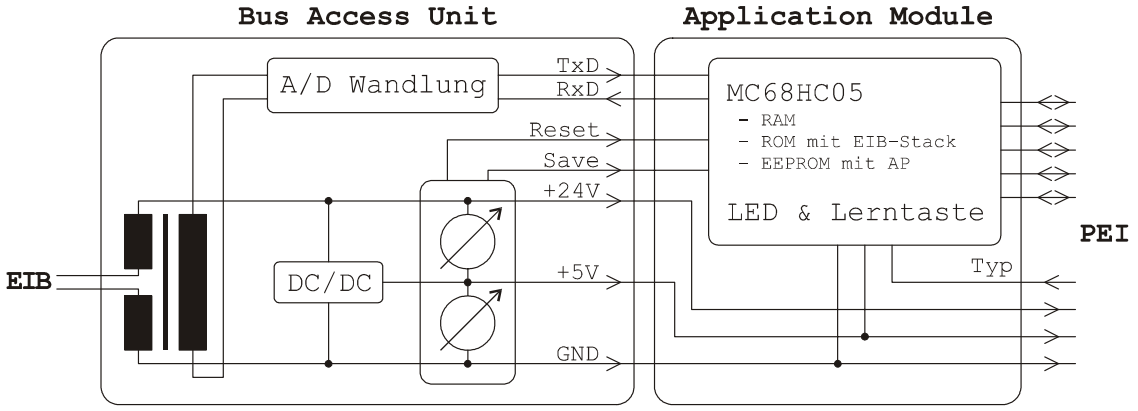

Abbildung A.7: Schematischer Aufbau einer BCU

Diese Standard Buskoppler basieren grundsätzlich auf einem Motorola MC68HC05 Controller, für den eine genaue Software API und bestimmte Speicherbereiche definiert sind, welche von der Anwendersoftware verwendet werden müssen. Alle Hersteller von

EIB-Anwendungen liefern für ihre Produkte ein fertig kompiliertes Application Program (AP), welches in einer Produktdatenbank gespeichert wird und dann der ETS zur Verfügung steht. Bei der Inbetriebnahme eines EIB-Netzwerkes wird schließlich das AP in die mit der elektrischen Anwendung verbundene BCU geladen und parametriert.

Das PEI besteht aus mehrere I/O-Leitungen, die je nach angeschlossener elektrischer Anwendung unterschiedliche Charakteristiken aufweisen. Dies können digitale Ein- bzw. Ausgänge wie auch analoge Eingänge oder serielle Schnittstellen zur Kommunikation mit anderen Controllern sein. Ein sogenannter PEI-Typ Widerstand an der Schnittstelle wählt über einen Analogeingang die zur Anwendung passende Pinbelegung des PEI aus. Die BCU selbst wird über den EIB mit Strom versorgt. Die Applikation, insofern sie mehr als die verfügbare Leistung am PEI benötigt, muss extern mit Strom versorgt werden. Der Entwickler einer EIB-Anwendung kann aber auch in seiner Anwendung die Funktionalität des AM übernehmen, muss aber dann den EIB-Protokollstack für seine Zwecke implementieren.

Anhang B: Schaltpläne

B.1 Security Server TINI-basiert

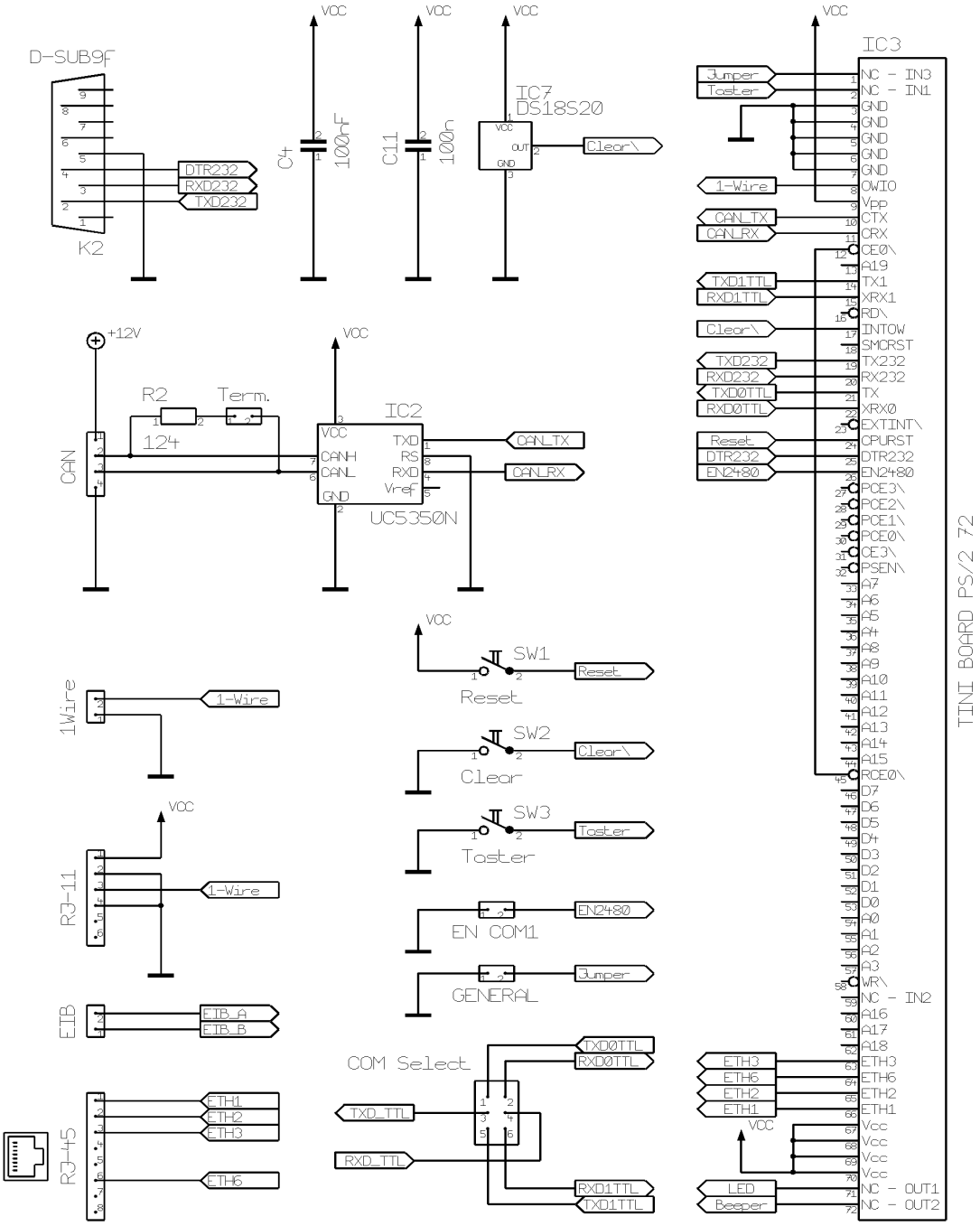

Abbildung B.1: Schaltplan Security Server TINI-basiert Teil 1

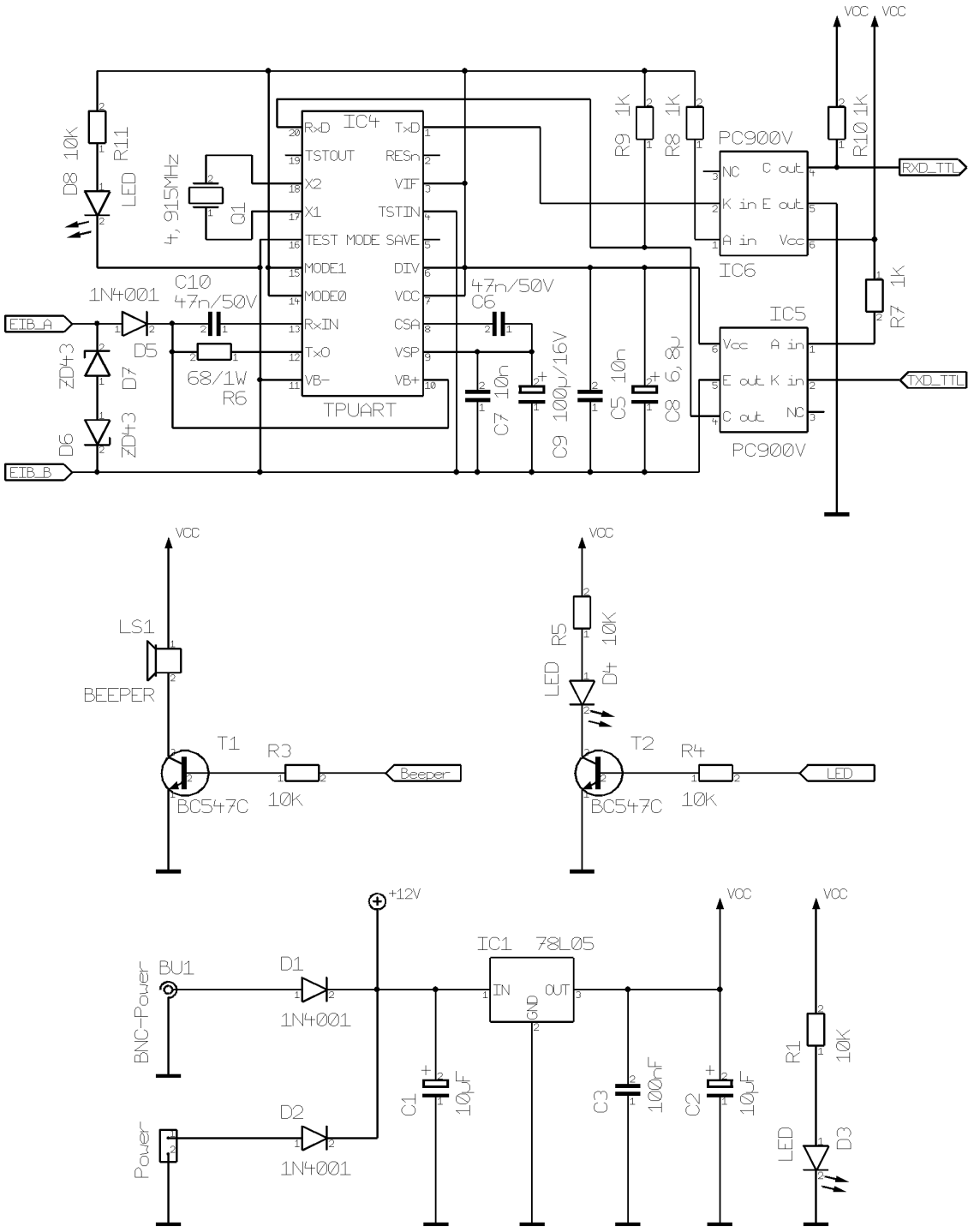

Abbildung B.2: Schaltplan Security Server TINI-basiert Teil 2

B.2 ID Modul Fingerabdruckerkennung Interface

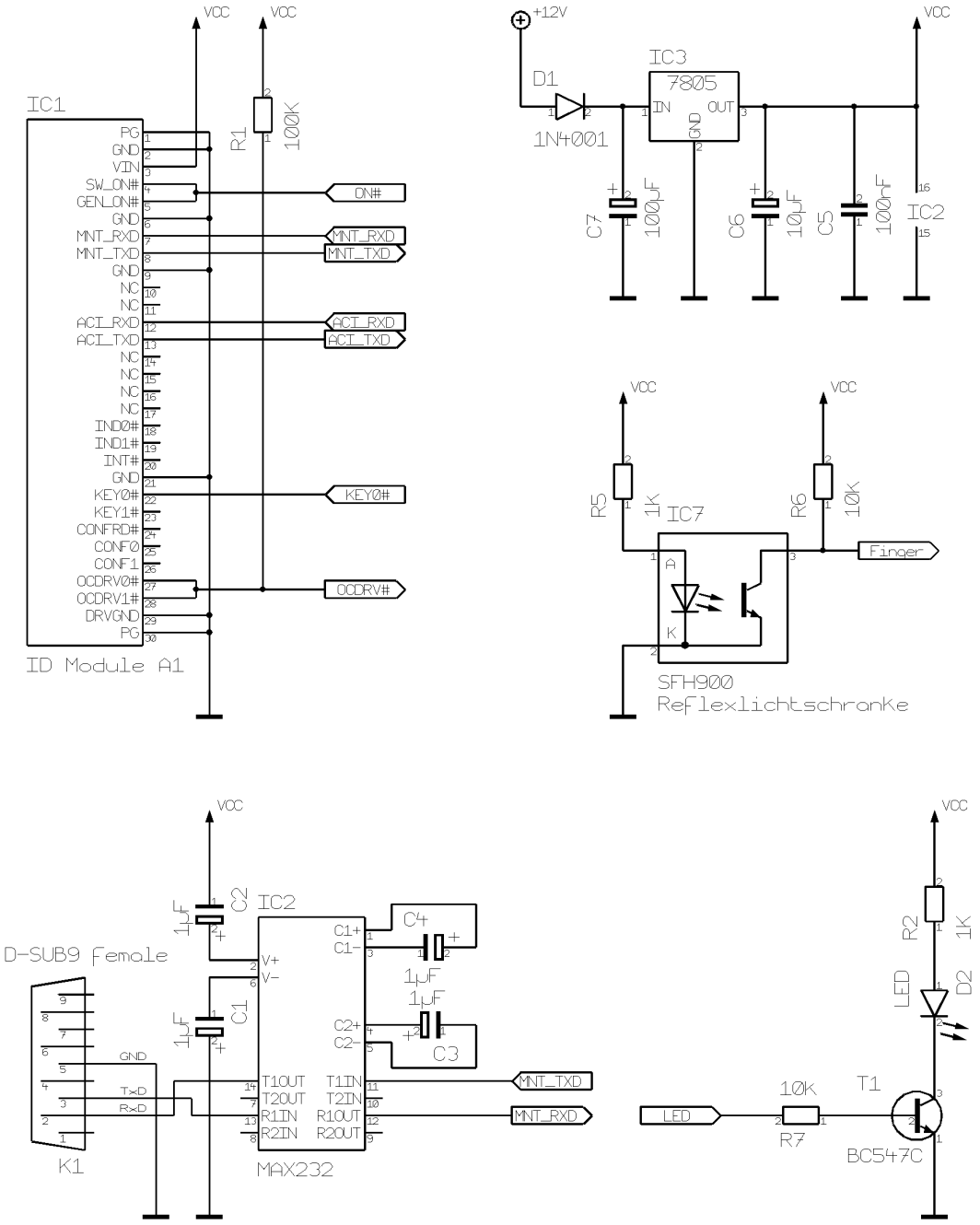

Abbildung B.3: Schaltplan ID Modul Fingerabdruckerkennung Interface Teil 1

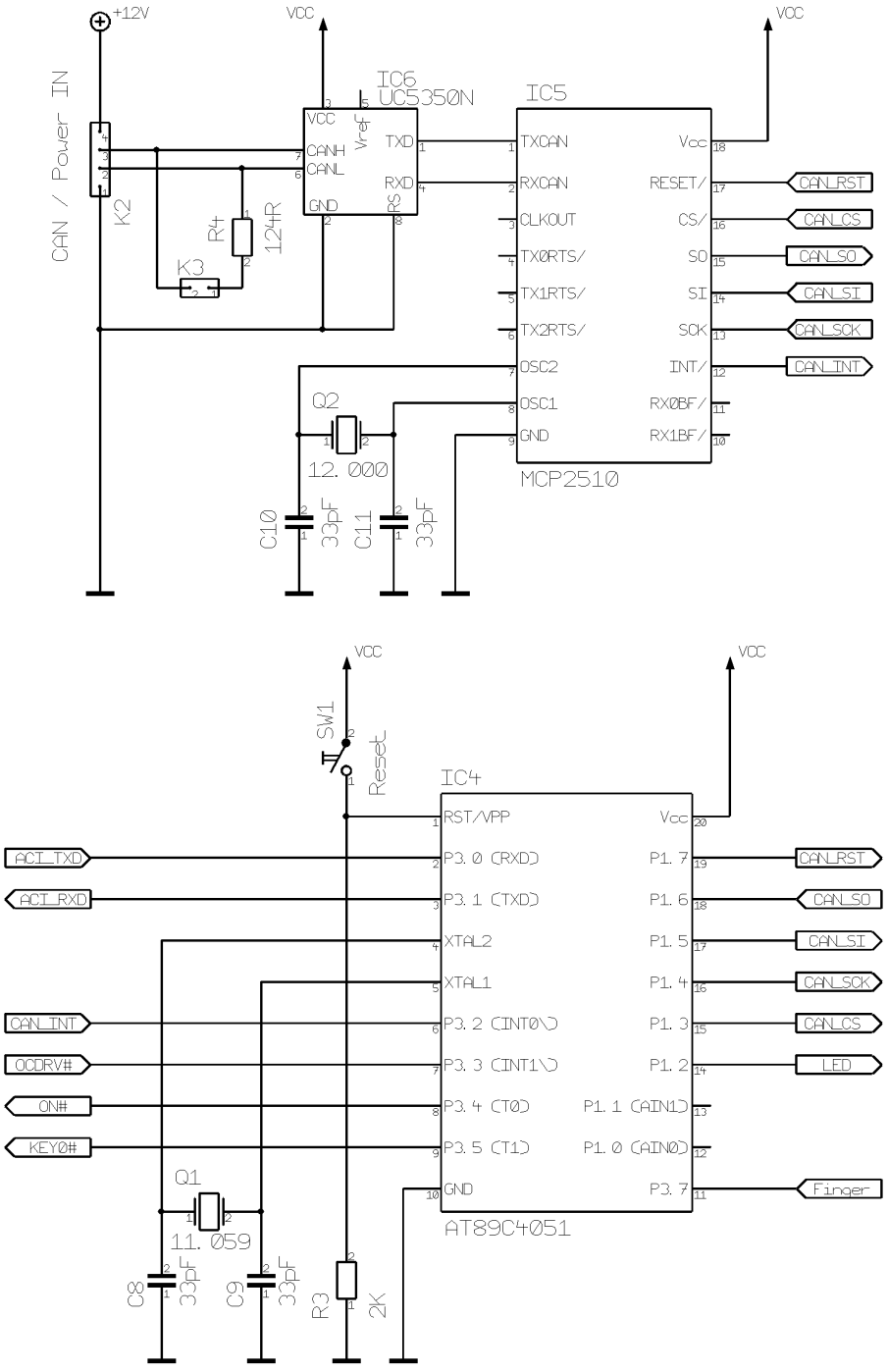

Abbildung B.4: Schaltplan ID Modul Fingerabdruckerkennung Interface Teil 2

B.3 RSC 300 Sprechererkennung Interface

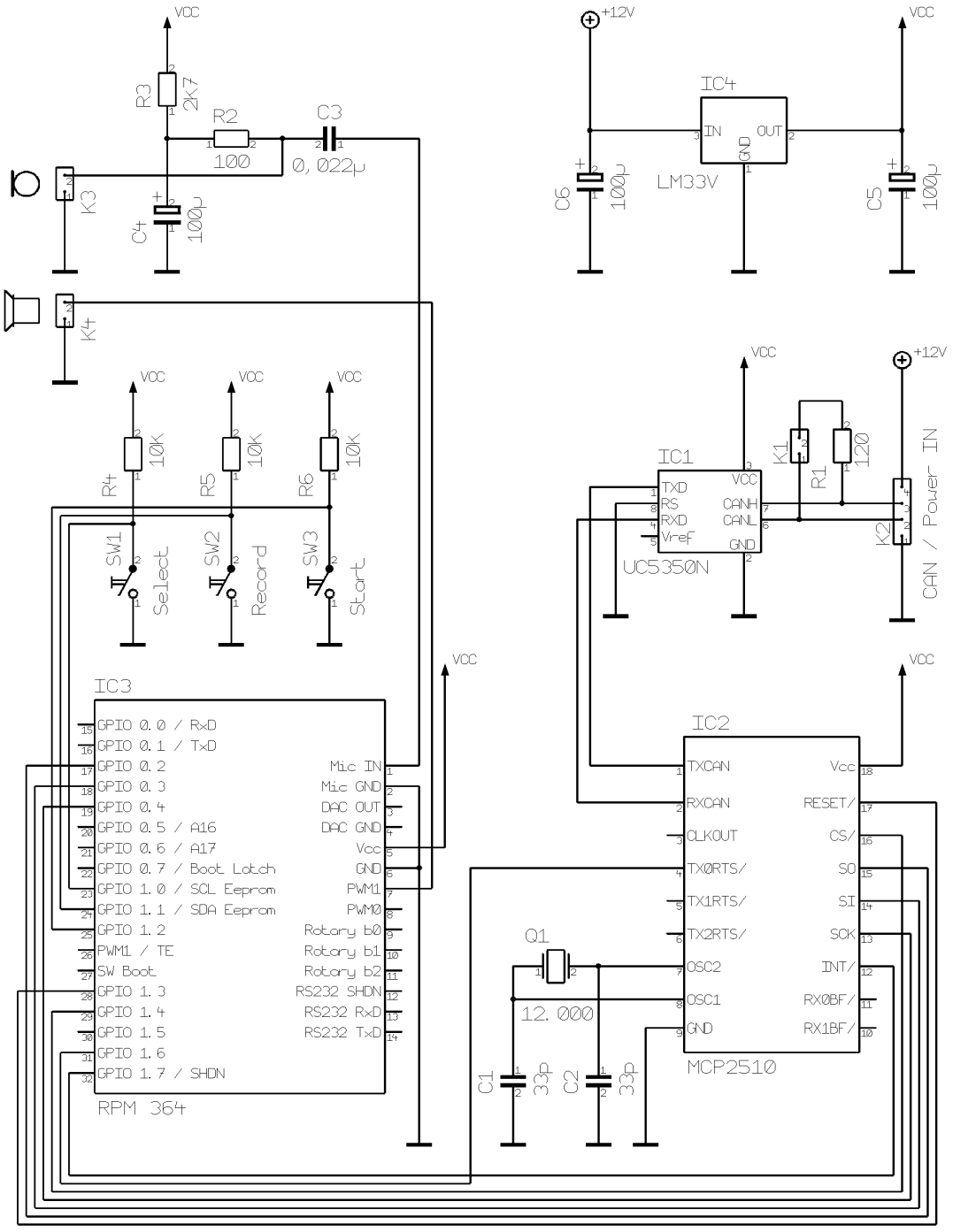

Abbildung B.5: Schaltplan RSC 300 Sprechererkennung Interface

B.4 Atmel Smart Card Interface

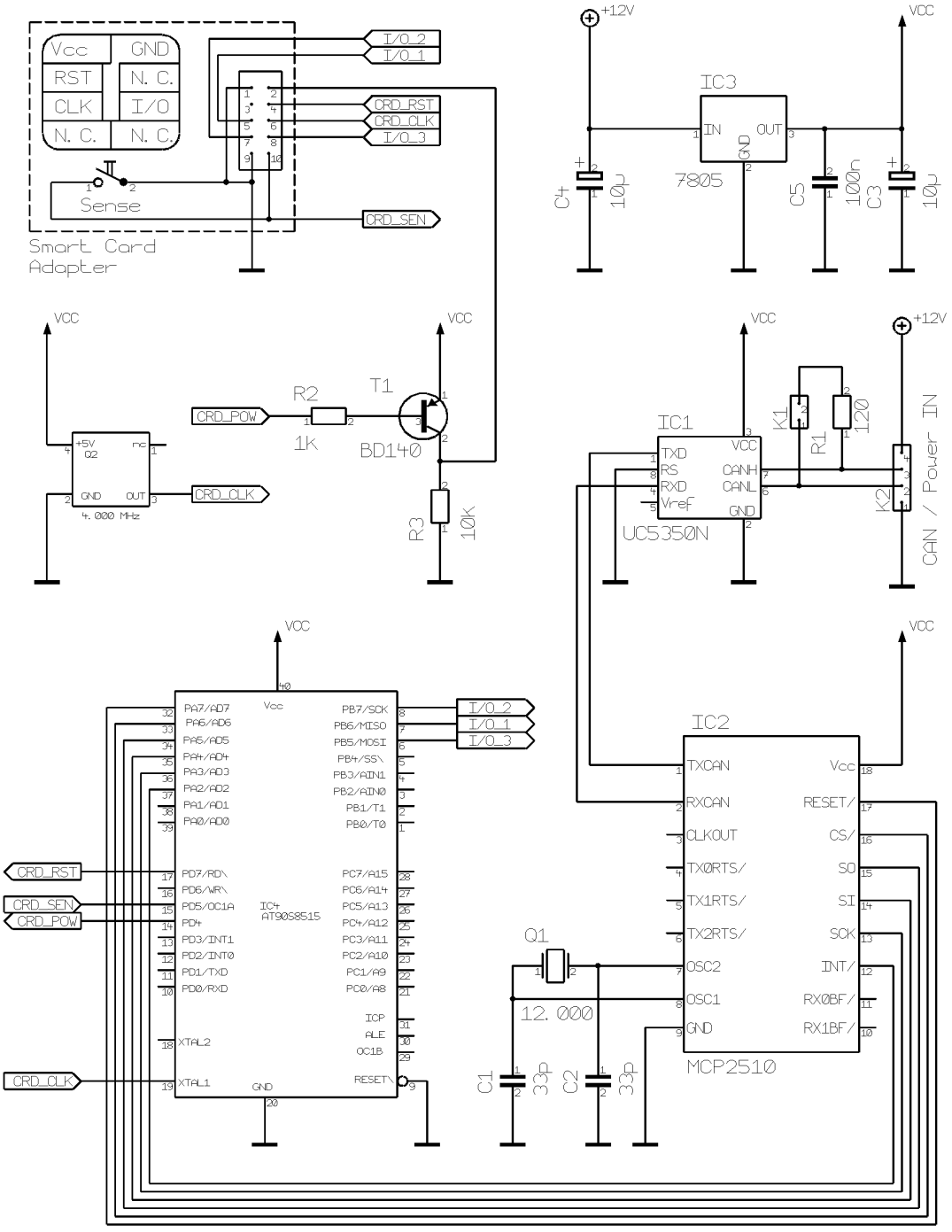

Abbildung B.6: Schaltplan Atmel Smart Card Interface

B.5 125 kHz Transponder Interface

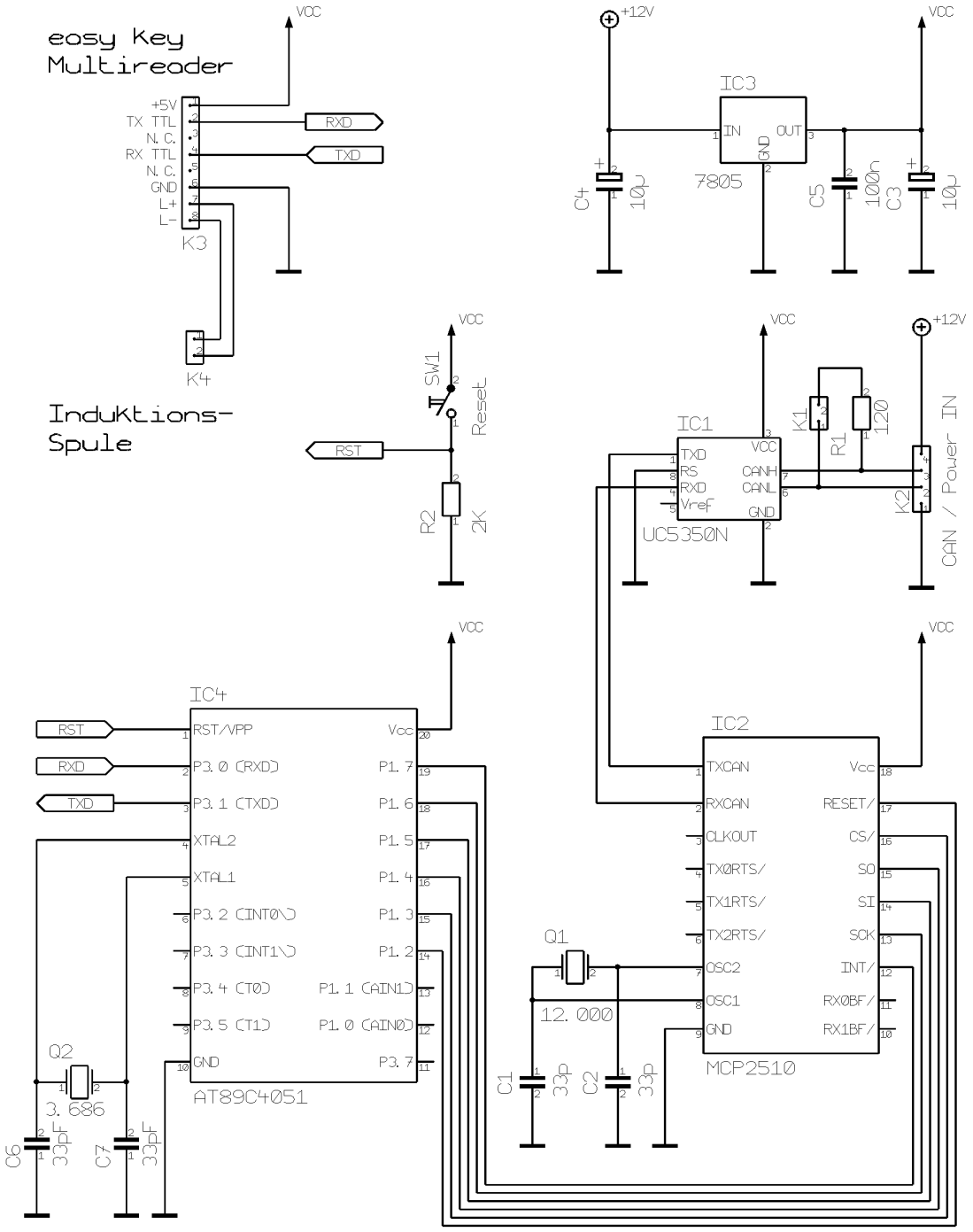

Abbildung B.7: Schaltplan 125 kHz Transponder Interface

B.6 Personal Area Network Interface

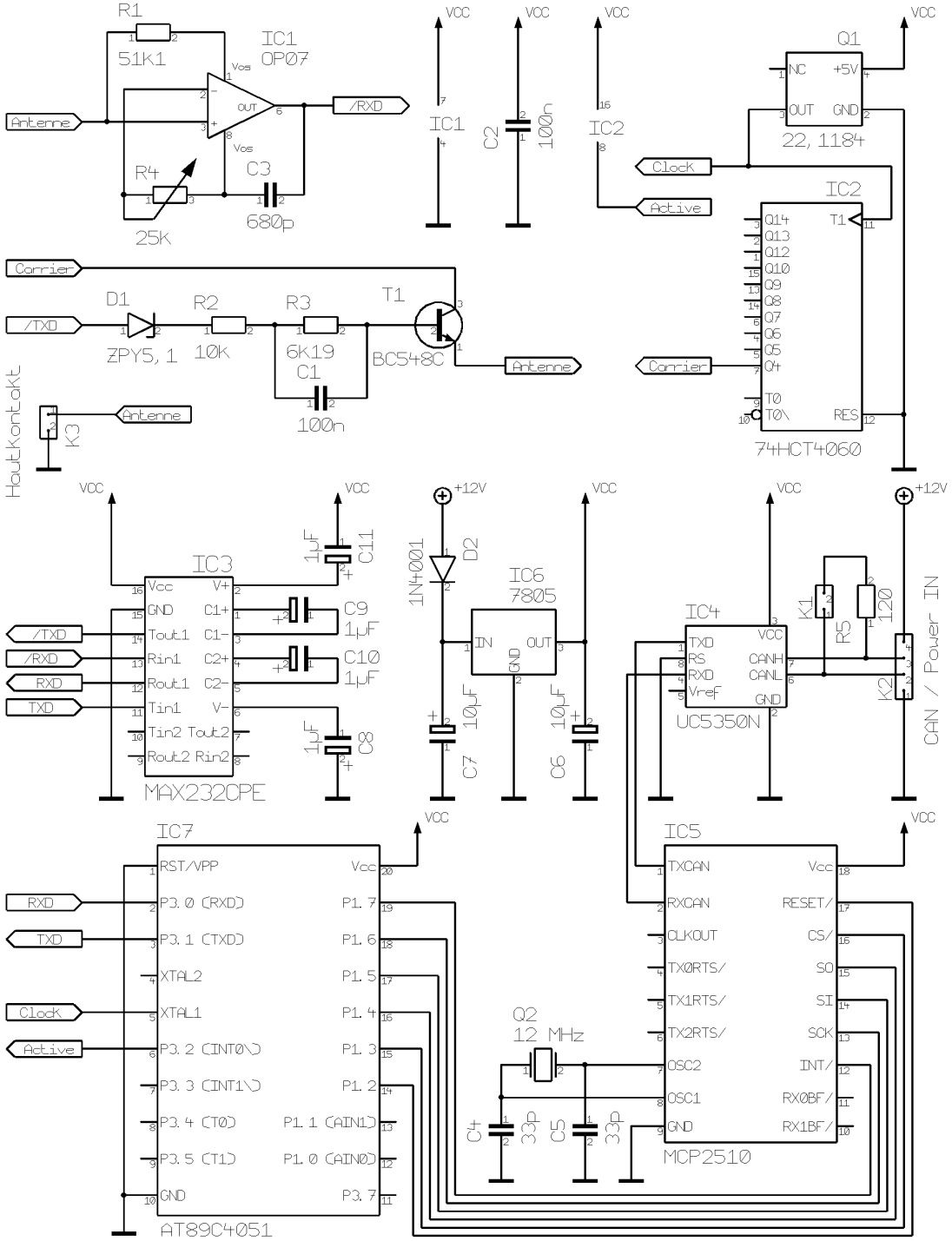

Abbildung B.8: Schaltplan Personal Area Network Interface

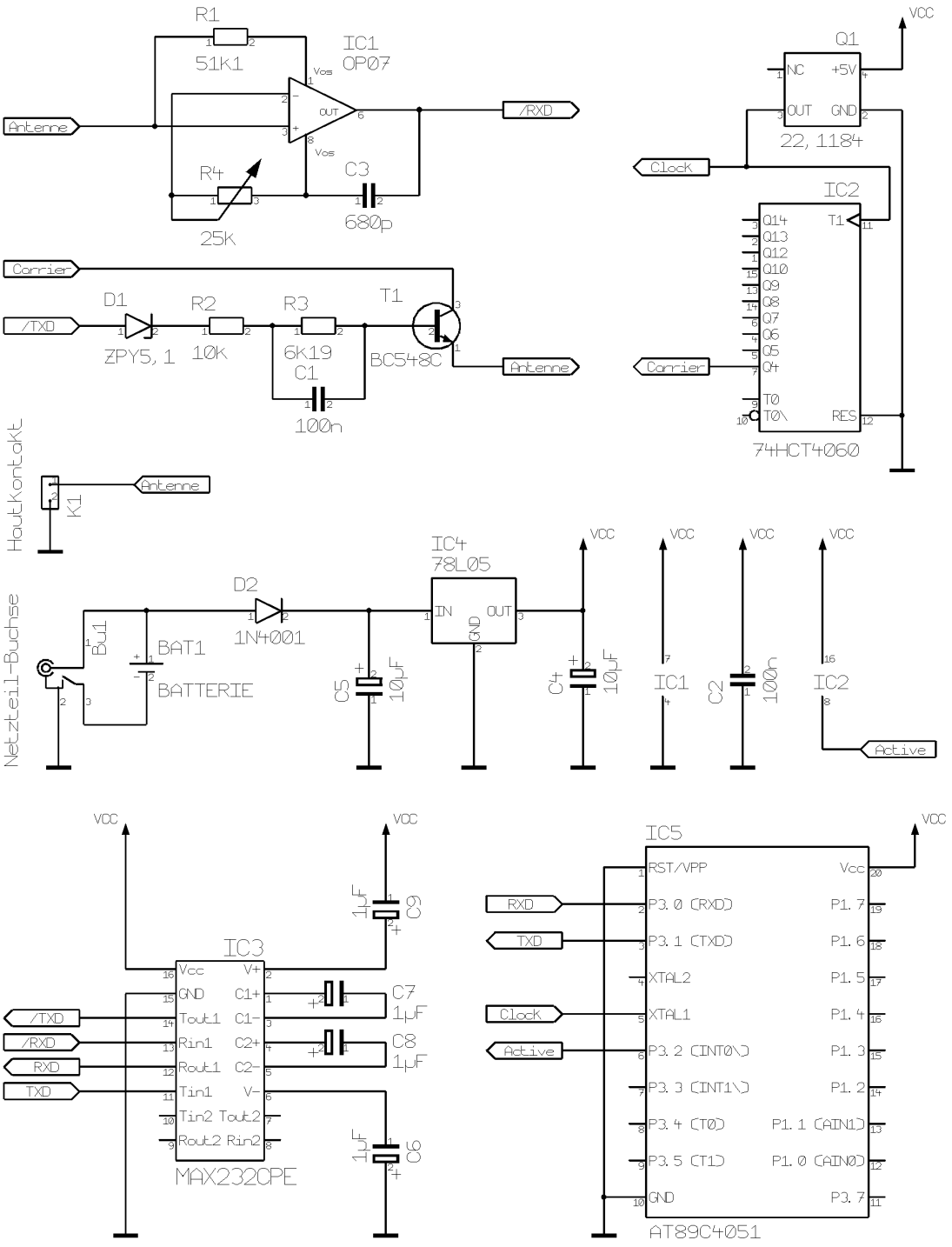

Abbildung B.9: Schaltplan Personal Area Network Mobilteil

B.7 MSP430 Secure BCU

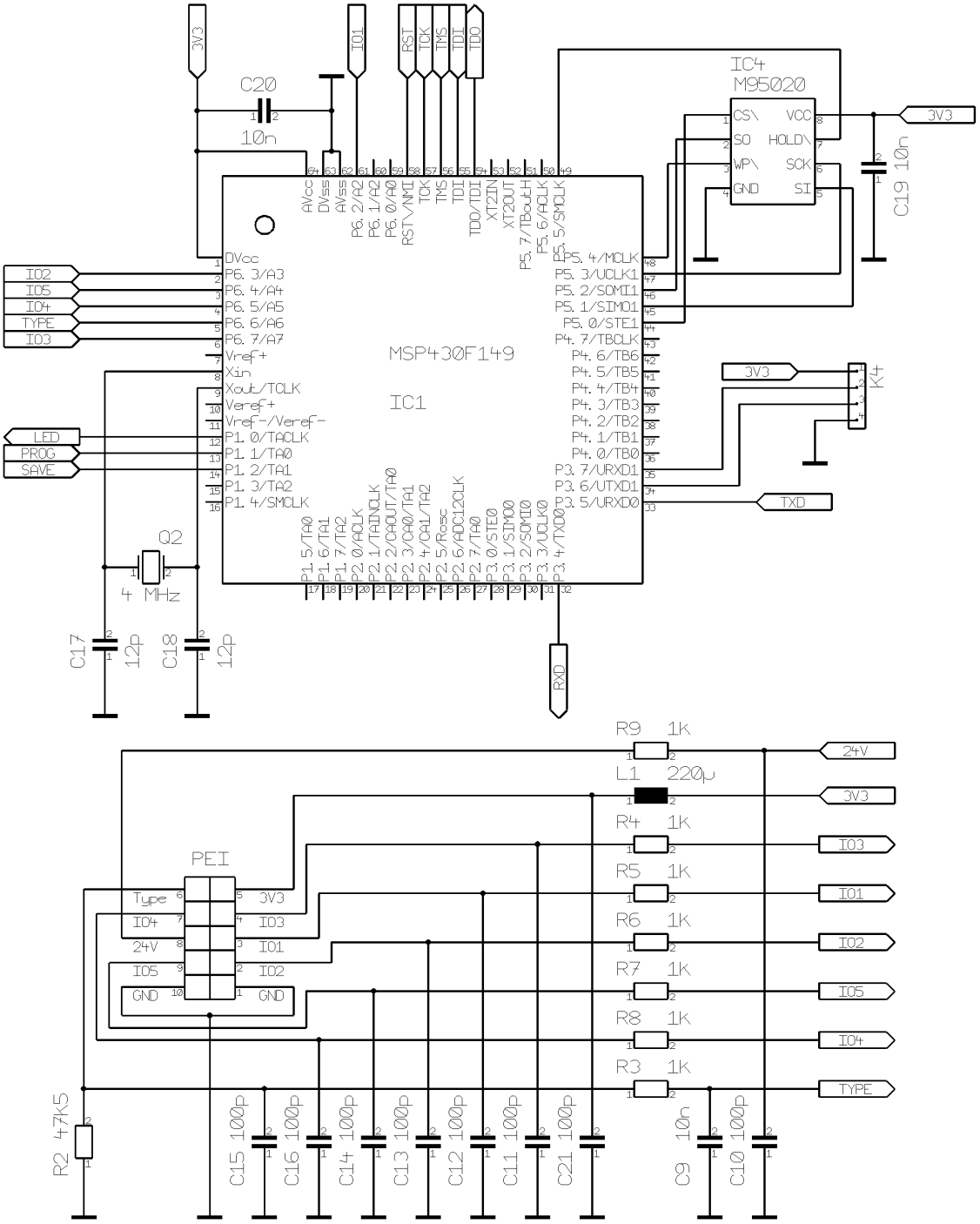

Abbildung B.10: Schaltplan MSP430 Secure BCU Teil 1

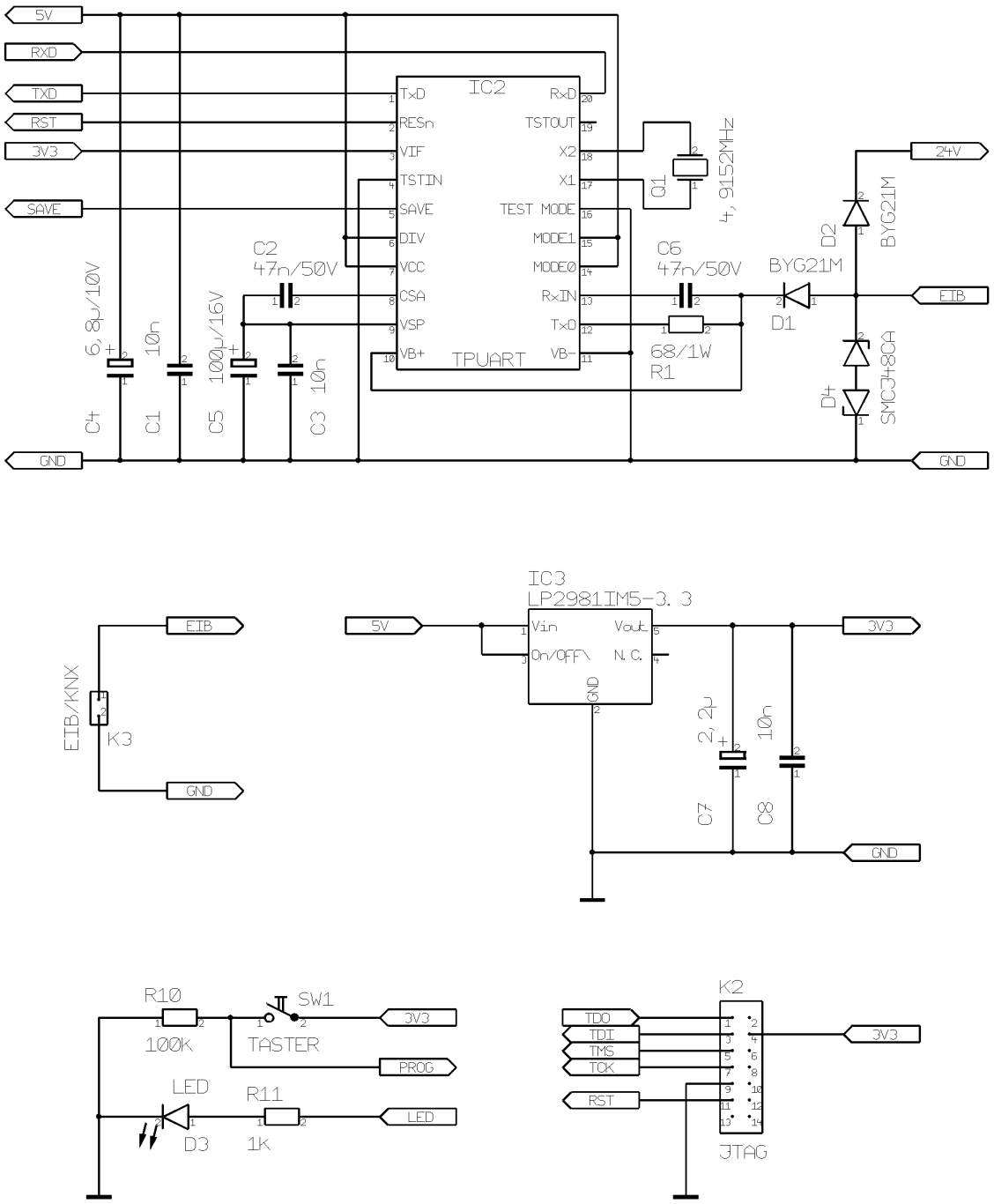

Abbildung B.11: Schaltplan MSP430 Secure BCU Teil 2

B.8 EIB/KNX Meldelinien Applikation

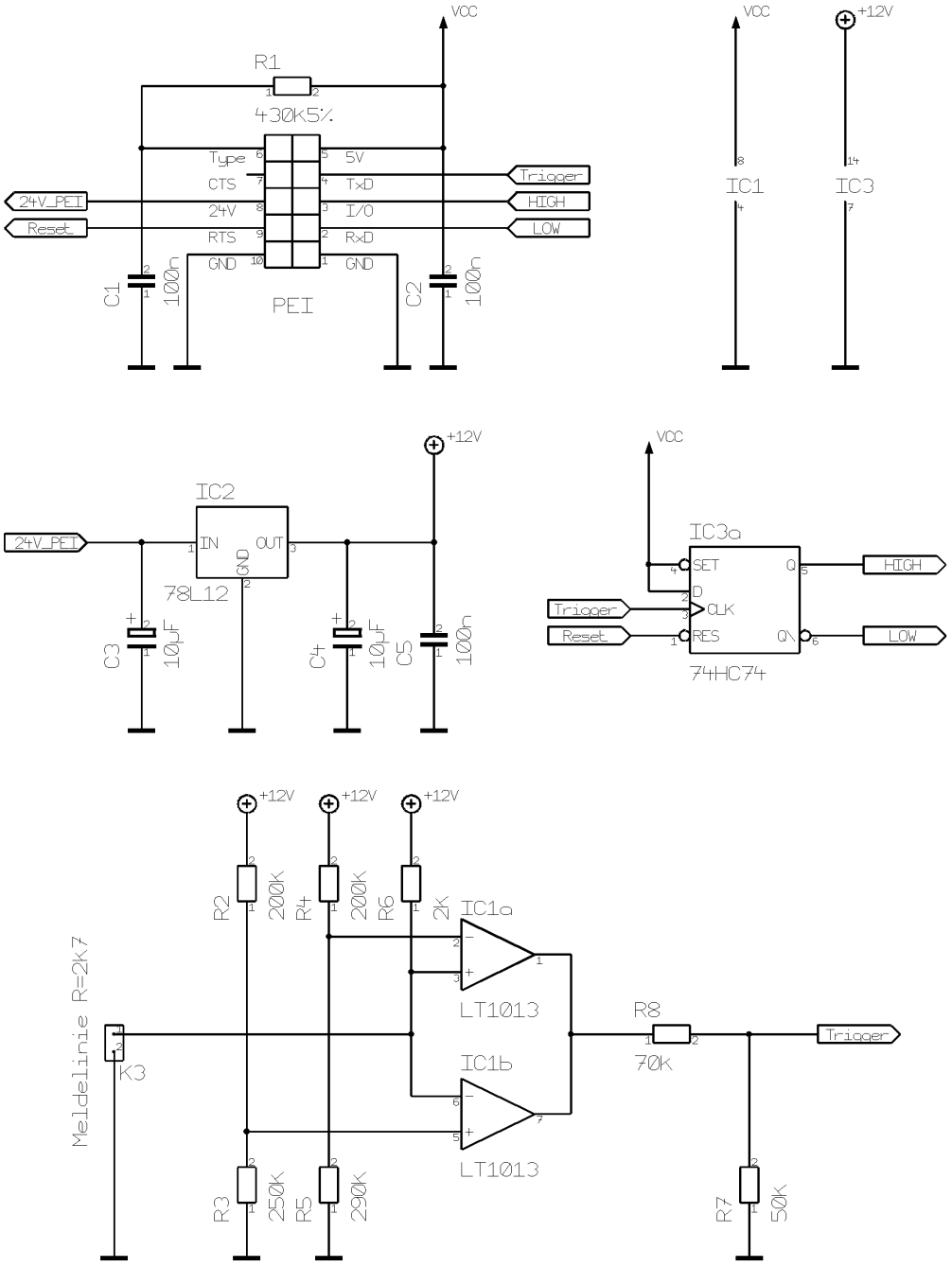

Abbildung B.12: Schaltplan EIB/KNX Meldelinien Applikation

B.9 EIB/KNX Blockschloss Applikation

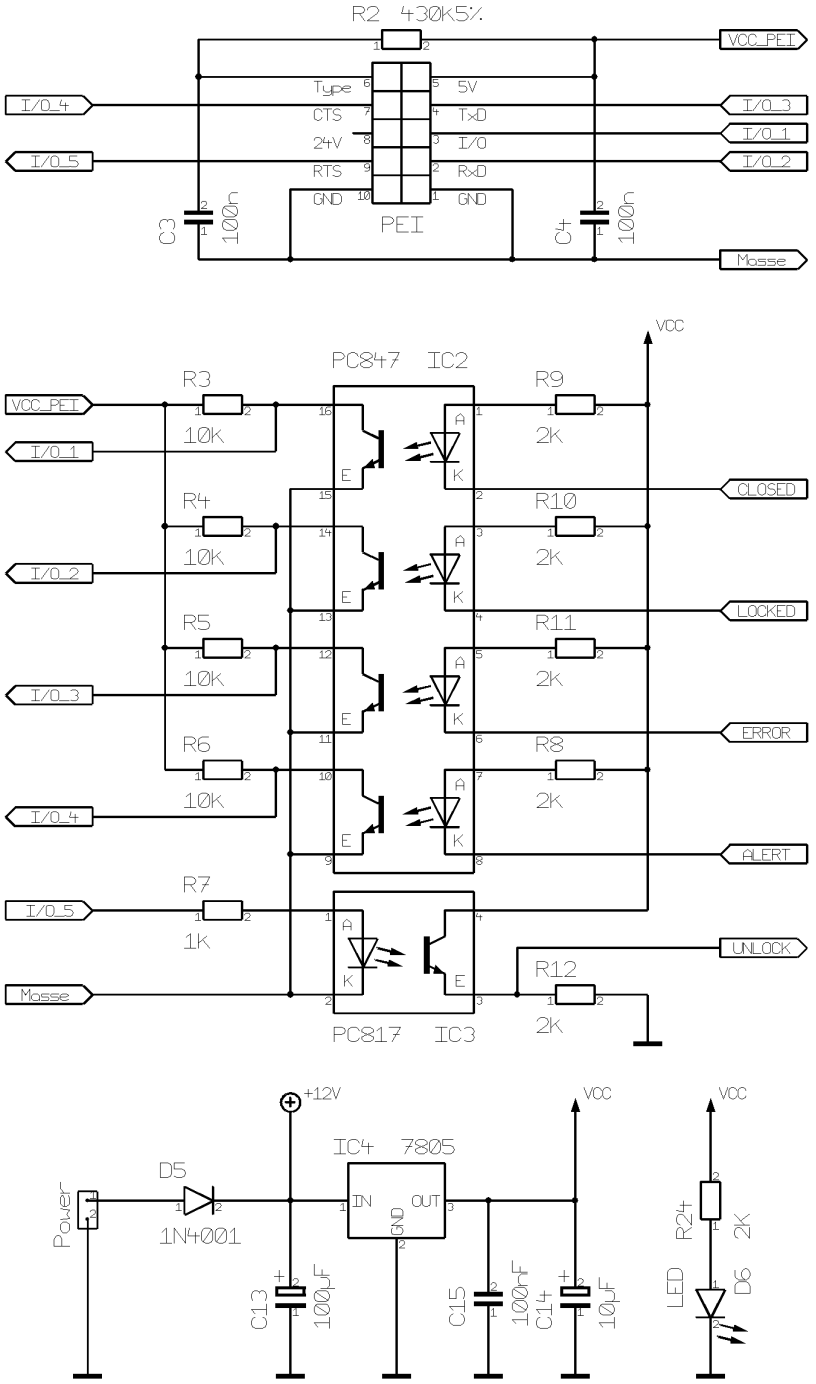

Abbildung B.13: Schaltplan EIB/KNX Blockschloss Applikation Teil 1

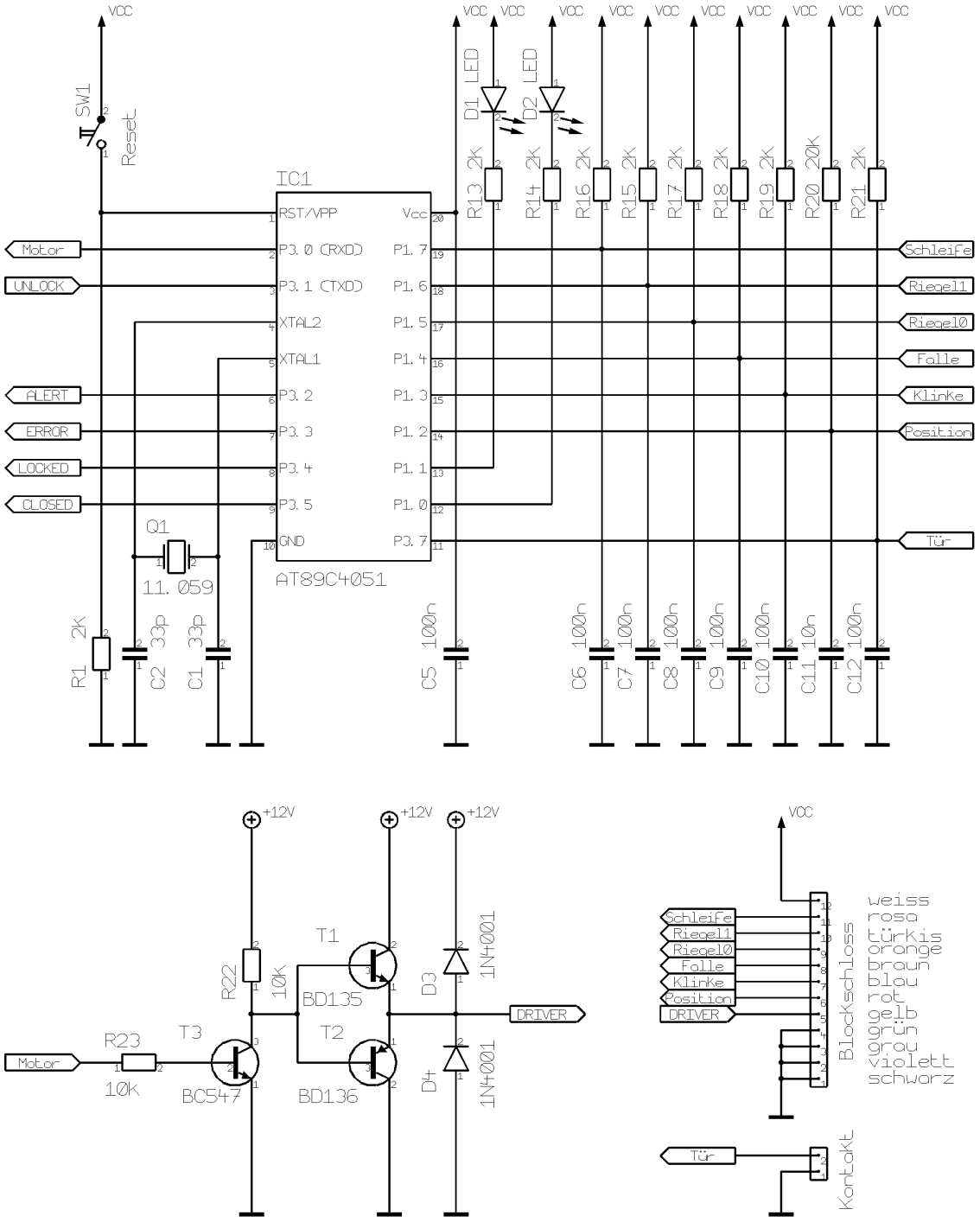

Abbildung B.14: Schaltplan EIB/KNX Blockschloss Applikation Teil 2

B.10 Security Server IPC-basiert

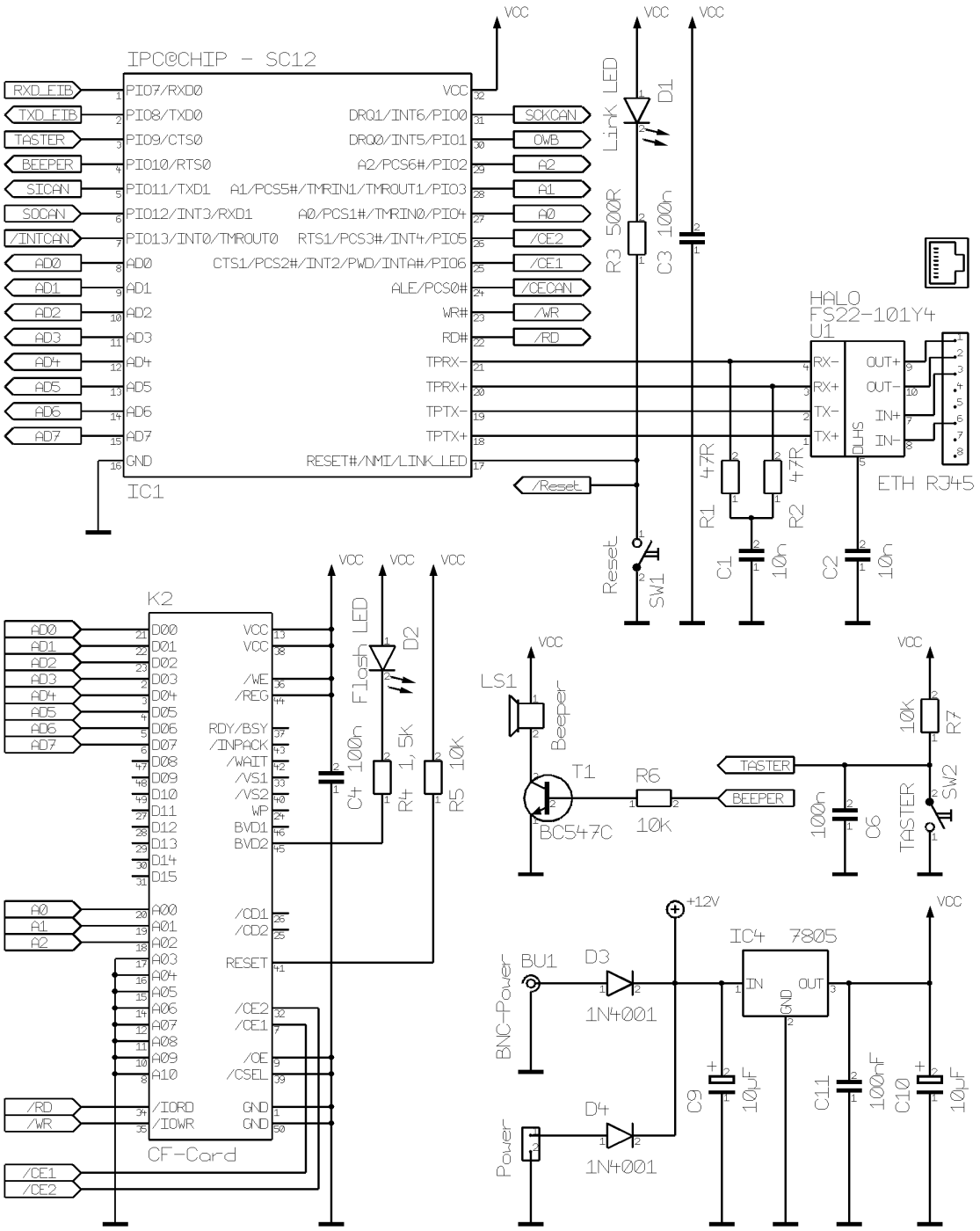

Abbildung B.15: Schaltplan Security Server IPC-basiert Teil 1

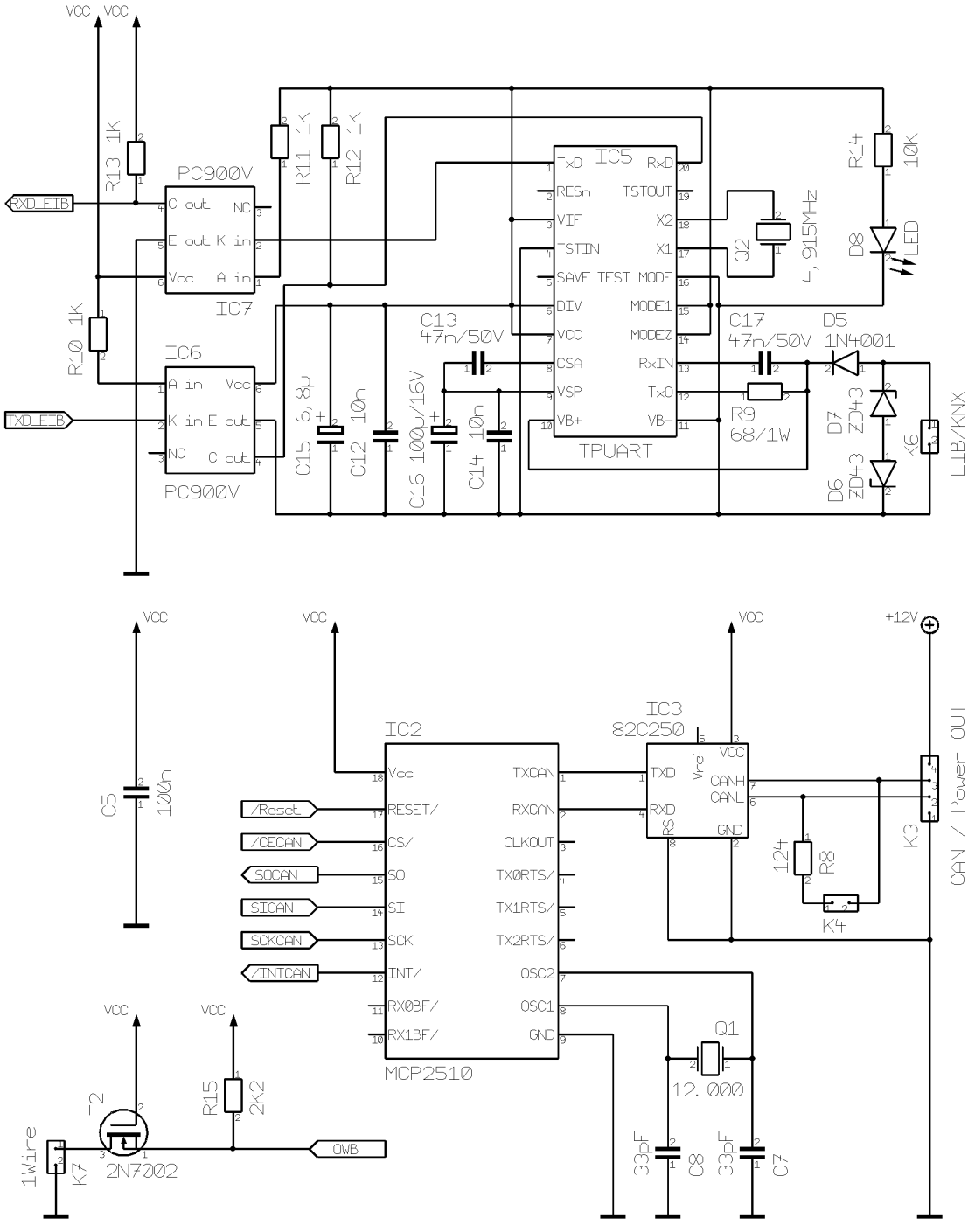

Abbildung B.16: Schaltplan Security Server IPC-basiert Teil 2

Abkürzungsverzeichnis

3DES	Tripple Data Encryption Standard
AES	Advances Encryption Standard
AM	Application Module
AP	Application Program
ASIC	Application Specific Integrated Circuit
BAU	Bus Access Unit
BCI	BatiBUS Club International
BCU	Bus Coupling Unit
BioIS	Vergleichende Untersuchung Biometrischer Identifikationssysteme
BKA	Bundeskriminalamt
BMA	Brandmeldeanlage
BMBF	Bundesministerium für Bildung und Forschung
BMZ	Brandmeldezentrale
BSI	Bundesamtes für Sicherheit in der Informationstechnik
CA	Collision Avoidance
CAN	Controller Area Network
CAR	Correct Acceptance Rate
CBC	Cipher Block Chaining
CCITT	Comité Consultatif International Téléphonique et Télégraphique
CEBus	Consumer Electronics Bus
CGI	Common Gateway Interface
CRC	Cyclic Redundancy Code
CRR	Correct Rejection Rate
CSMA	Carrier Sense Multiple Access
DALI	Digital Addressable Lighting Interface
DES	Data Encryption Standard
DIN	Deutsches Institut für Normung e.V.
DSA	Digital Signature Algorithm
EER	Equal Error Rate
EHS	European Home System
EHSA	European Home System Association
EIB	European Installation Bus
EIBA	European Installation Bus Association
EIB-PL	EIB Powerline
EIB-RF	EIB Radio Frequency
EIB-TP	EIB Twisted Pair
EIS	EIB Interworking Standard
EMZ	Einbruchmeldezentrale

EN	Europa Norm
ETS	EIB Tool Software
FAR	False Acceptance Rate
FER	Failed Enrolment Rate
FhG-IGD	Fraunhofer-Institut für Grafische Datenverarbeitung
FIPS	Federal Information Processing Standard
FIR	False Identification Rate
FRR	False Rejection Rate
FTP	File Tranfer Protocol
FTS	Ferntastsystem
HTML	Hyper Text Markup Language
HTTP	Hypertext Transfer Protocol
IBG	International Biometric Group
IDEA	International Data Encryption Algorithm
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPC	Industrie PC
ISDN	Integrated Services Digital Network
ISO	International Standard Organisation
JVM	Java Virtual Machine
KNX	Konnex
LCIE	Laboratoire Central des Industries Electriques
LCN	Local Control Network
LON	Local Operating Network
MAC	Message Authentication Code
MD	Message Digest
MOC	Match-on-Card
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OLE	Object Linking and Embedding
OOK	On/Off Key
OPC	OLE for Process Control
OSI	Open System Interconnection
PAC	Physical Access Control
PAN	Personal Area Network
PDA	Personal Digital Assistant
PDU	Protocol Data Unit
PEI	Physical External Interface
PGP	Pretty Good Privacy
PHC	Peha House Control
PIN	Personal Identification Number
PIR	Passiv-Infrarot

PPP	Point to Point Protocol
ROC	Receiver Operating Characteristic
RSA	Rivest Shamir Adleman Verschlüsselungsverfahren
SCC	Standard Control Committee
SEIB	Secure European Installation Bus
SELV	Safety Extra Low Voltage
SHA	Secure Hash Algorithm
SNEP	Secure Network Encryption Protocol
SPINS	Security Protocols for Sensor Networks
TAN	Transaction Number
TCP	Transfer Control Protocol
TINI	Tiny Internet Interface
TPUART	Twisted Pair Universal Asynchronous Receiver Transmitter
UML	Unified Modeling Language
ÜMZ	Überfallmeldezentrale
VDE	Verband der Elektrotechnik, Elektronik und Informationstechnik
VdS	Verband der Schadenversicherer
VSG	Verbundsicherheitsglas

Abbildungsverzeichnis

1.1	Täterarbeitsweisen an fensterlosen Türen	2
2.1	Zugangs- und Sicherheitsmechanismen am automatisierten Gebäude	5
2.2	Smart Cards, iButtons und diverse Transponder	12
2.3	Marktaufteilung biometrischer Systeme 2003	14
2.4	Siemens FingerTIP Sensor mit TopSec ID Modul	15
2.5	Typische Badewannenkurve	17
2.6	Aufbau von Gefahrenmeldeanlagen nach DIN VDE 0833	19
2.7	Prinzip einer Meldeleitung nach ABB STOTZ-KONTAKT GmbH	20
2.8	Zone Terminal MT/U 2.12.1	21
2.9	Darstellung des Verschlüsselungsprinzips	23
2.10	Aufbau des Datencontainers nach Fraunhofer-IMS und IPAS	27
2.11	Darstellung des Feistel-Netzwerks des Blowfish-Verfahrens	28
2.12	Aufbau einer Tür	29
2.13	Vereinfachte Darstellung eines modernen Schließzylinders	31
3.1	Zweigeteilter Ansatz zur Erstellung eines Konzeptes	33
3.2	Kommunikationsstruktur zwischen Gebäudebus und Netzanbindung	37
3.3	Darstellung des Gesamtkonzeptes	39
4.1	Sensorflow eines multimodalen Systems	41
4.2	Wahrscheinlichkeitsdichtedarstellung biometrischer Systeme	42
4.3	Darstellungsformen der Fehlerkurven	43
4.4	Unabhängig gemessene ROC-Kurven	44
4.5	Strategische Entscheidungsräume der ROC	48
4.6	Beispiel einer ROC aller Varianten eines Dreifachsystems	55
4.7	Strategischer Entscheidungsraum kombinierter Systeme	56
5.1	EIB/KNX Telegrammaufbau	64
5.2	Aufbau der Zustandsmatrix	66
5.3	C-Code zur Berechnung der Multiplikationen	67
5.4	Ersetzen der Elemente der Zustandsmatrix	68
5.5	Verschieben der Zeilen in der Zustandsmatrix	69
5.6	C-Code zur Erweiterung der Rundenschlüssel	71
5.7	Grafische Darstellung einer AES-128 Verschlüsselungsrunde	72
5.8	Pseudo-Quellcode zur Datenverschlüsselung	73
5.9	Stromchiffrierung im Counter-Modus	78
5.10	EIB/KNX-Nutzdatenbereich (NSDU)	80
5.11	Protokoll-Layer der gesicherten Übertragung	82
5.12	Verschlüsselte Multicast-Applikations-Kommandos	84

6.1	Darstellung aller Komponenten des Demosystems	87
6.2	Rückansicht der Demonstratoreinheit	88
6.3	Aufbau des TINI Security Servers	90
6.4	Interne Struktur des TINI Betriebssystems	91
6.5	Klassenstruktur der Serversoftware	92
6.6	Screenshot der EIB/KNX Visualisierung	94
6.7	Kommunikationsbeziehung zwischen Browser, Server und EIB/KNX	95
6.8	Screenshot einer Konfigurationsoberfläche	96
6.9	Parameterübergabe an Applets zur Konfigurierung	97
6.10	Aufbau eines CAN-Telegramms	100
6.11	Aufbau des Kommandobytes	101
6.12	Siemens FingerTIP Sensor mit ID-Modul und Sensorbild	102
6.13	Schaltplan des CAN-Interface	103
6.14	RSC-300 Prototyping Modul	104
6.15	Ablauf des Challenge-Response-Verfahrens	107
6.16	Multireader mit Hostsystem und Antenne	108
6.17	Darstellung eines iButtons	109
6.18	Prinzipdarstellung eines PAN-Systems	110
6.19	Experimentelle Prototypen der PAN-Schaltungen	111
6.20	Blockschaltbild der Secure BCU	113
6.21	Ansicht der Ober- und Unterseite der Secure BCU	113
6.22	Interne Layer-Struktur der Secure BCU	114
6.23	Frontansicht der Demonstratoreinheit	116
6.24	IPC-Server mit Compact Flash Erweiterung	117
7.1	Technologieintegration um die Gebäudesystemtechnik	119
A.1	ISO/OSI Layerstruktur des EIB	124
A.2	Physikalische Topologien	125
A.3	Aufbau der physikalischen Adresse	126
A.4	Logische Topologie des EIB-TP64	127
A.5	Aufbau der Gruppenadresse	128
A.6	Aufbau eines EIB-Telegramms	129
A.7	Schematischer Aufbau einer BCU	130
B.1	Schaltplan Security Server TINI-basiert Teil 1	133
B.2	Schaltplan Security Server TINI-basiert Teil 2	134
B.3	Schaltplan ID Modul Fingerabdruckerkennung Interface Teil 1	135
B.4	Schaltplan ID Modul Fingerabdruckerkennung Interface Teil 2	136
B.5	Schaltplan RSC 300 Sprechererkennung Interface	137
B.6	Schaltplan Atmel Smart Card Interface	138
B.7	Schaltplan 125 kHz Transponder Interface	139
B.8	Schaltplan Personal Area Network Interface	140
B.9	Schaltplan Personal Area Network Mobilteil	141

B.10 Schaltplan MSP430 Secure BCU Teil 1 142
B.11 Schaltplan MSP430 Secure BCU Teil 2 143
B.12 Schaltplan EIB/KNX Meldelinien Applikation 144
B.13 Schaltplan EIB/KNX Blockschloss Applikation Teil 1 145
B.14 Schaltplan EIB/KNX Blockschloss Applikation Teil 2 146
B.15 Schaltplan Security Server IPC-basiert Teil 1 147
B.16 Schaltplan Security Server IPC-basiert Teil 2 148

Tabellenverzeichnis

2.1	Fehlerraten unterschiedlicher biometrischer Systeme	17
2.2	Widerstandsklassen nach DIN V ENV 1627	30
3.1	Bewertung von Authentisierungsmechanismen	34
4.1	Konjunktion und Disjunktion zweier reeller Systeme	50
4.2	Kombinationen und Strategien dreier Systeme	51
4.3	Einschätzung biometrischer Verfahren	57
4.4	Strategietabelle des Beispielsystems 3. Ordnung	59
5.1	Ressourcenaufstellung für den Speicherbedarf	85
6.1	Zuordnung der 11 Bit CAN-Identifier	100

Literaturverzeichnis

[AFR 2003] Amberg, M.; Fischer, S.; Rößler, J.: „Biometrische Verfahren, Studie zum State of the Art“, Friedrich-Alexander-Universität Erlangen-Nürnberg, Lehrstuhl für Betriebswirtschaftslehre, 2003

[BAI 2002] Biometric Associates: „Biometric Technology for Secure Access“, Baltimore, Maryland, 2002, http://www.biometricassociates.com/

[Bintern 2003] Binternagel, L.: „Energiemonitoring in der Gebäudetechnik“, Dissertation, Technische Universität München, 2003

[Bromba 2003] Bromba, M. U. A.: „Bioidentifikation, Fragen und Antworten“, http://www.bromba.com/faq/biofaqd.htm

[Bronstein 1991] Bronstein, I. N.; Semendjajew ,K. A.: „Taschenbuch der Mathematik“, Teubner Verlagsgesellschaft, 25. Auflage, 1991, ISBN 3-8154-2000-8

[Brügge 2000] Brügge, B.; Dutoit, A. H.: „Object-Oriented Software Engineering“, Prentice Hall, 2000, ISBN 0-13-489725-0

[Brunelli 1995] Brunelli, R.; Falavigna, D.: „Person Identification Using Multiple Cues“, IEEE Transaction on Pattern Analysis and Machine Intelligence, Band 17 Nummer 10, Seite 955, 1995

[Buchholz 2002] Buchholz, J.: „Der Schlüssel zu MATLAB“, MATLAB Select, Ausgabe 1/02, Seite 22 – 27

[Busch 2002] Busch, C.; Daum, H.: „Frei von Zweifel“, c’t 2002, Heft 5, Seite 156-161, Heise Verlag, 2002

[Chen 2000] Chen, Z.: „Java Card Technology for Smart Cards“, Addison-Wesley, 2000, ISBN 0-20170-329-7

[Courtois 2002] Courtois, N.; Pieprzyk, J.: „Cryptanalysis of Block Ciphers with Overdefined Systems of Equations“, http://eprint.iacr.org/2002/044.pdf

[Crista 2003] Crista, D.-A.: „Personal Area Network (PAN) – Zugangskontrolle per Hautkontakt“, Diplomarbeit, Lehrstuhl für Messsystem- und Sensortechnik, Technische Universität München, 2003

[Daemen 1999] Daemen, J.; Rijmen, V.: „AES submission document on Rijndael“, NIST, Version 2, http://csrc.nist.gov/CryptoToolkit/aes/rijndael/Rijndael.pdf, 1999

[Daemen 2002] Daemen, J.; Rijmen, V.: „The design of Rijndael (AES – the Advanced Encryption Standard) “, Springer Verlag, 2002, ISBN 3-540-42580-2

[Dallas 2000] Dallas Semiconductor: „A Cryptography Glossary“, Dallas Semiconductor, 2000, http://www.ibutton.com/ibuttons/

[Daugman 2000] Daugman, J.: „Biometric decision landscapes. “, Technical Report No. TR482, University of Cambridge Computer Laboratory, http://www.cl.cam.ac.uk/users/jgd1000/biomdecis.pdf

[deSpecial 1999] de-Special: „Bussysteme für die Gebäudeinstallation“, Hüthig & Pflaum Verlag, 1999, ISBN 3-81010-124-9

[Dietrich 1999] Dietrich, D.; Loy, D.; Schweinzer, H.-J.: „LON-Technologie. Verteilte Systeme und Anwendungen“, Hüthig 1999, ISBN 3-77852-770-3

[Dietrich 2000] Dietrich, Kastner, Sautner: „EIB Gebäudebussystem“, Hüthig Verlag Heidelberg, 2000, ISBN 3-7785-2795-9

[DiffiHell 1976] Diffie, W.; Hellmann, M. E.: „New Directions in Cryptography“, IEEE Transactions on Information Theory, 1976

[DSS 1994] Digital Signature Standards: „NIST FIPS PUB 186“, National Institute of Standards and Technology, 1994

[DSTINI 2003] Dallas Semiconductor: „DS80C400 (DSTINIm400) Networked Microcontroller Evaluation Kit“, Dallas Semiconductor, Maxim, 2003, http://pdfserv.maxim-ic.com/en/ds/DSTINIM400.pdf

[Echelon 2001] Echelelon Corp.: „Echelon’s LonWorks Products“, Fall 2001 Spring 2002 Edition, Version A, 2001

[EIBA 1999] EIBA: „EIBA Handbook Series“, Release 3.0, Brussels, 1999

[ElGamal 1985] ElGamal, T.: „A Public-Key Cryptosystem and a Signature Scheme based on Discrete Logarithms“, Advances in Cryptology, Proceedings of CRYPTO 84, Springer Verlag 1985

[Enquete 2002] Deutscher Bundestag, Enquete-Kommission: „Ausgewählte Möglichkeiten der Steuerungs- und Regelungstechnik als Bausteine einer nachhaltigen Energiewirtschaft“, Schlussbericht zur Nachhaltigen Energieversorgung, Kapitel 4.3.7., 2002, http://www.bundestag.de/gremien/ener/schlussbericht/index.htm

[Ertel 2001] Ertel, W.: „Angewandte Kryptographie“, Fachbuchverlag Leipzig im Carl Hanser Verlag, 2001, ISBN 3-446-21549-2

[Etschberg 2002] Hofmann, R.; Etschberger, K.; et al.: „Controller Area Network. Grundlagen, Protokolle, Bausteine, Anwendungen“, Fachbuchverlag Leipzig, 2002, ISBN 3-446-21776-2

[Finkenz 2002] Finkenzeller, K.: „RFID-Handbuch“, Hanser Fachbuchverlag, 2002, ISBN 3-44622-071-2

[FIPS 197] Federal Information Processing Standards Publication 197, 2001, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[Fischholz 2000] Fischholz, R.; Dieckmann, U.: „BioID: A Multimodal Biometric Identification System“, Computer, Band 33 Nummer 2, Seite 64, 2000

[Flanagan 2002] Flanagan, D.: „Java in a Nutshell“, Deutsche Ausgabe, O'Reilly, 2002, ISBN 3-897-21332-X

[GHKB 2003] Grinewitschus, V.; Hildebrand, R.; et al.: „Gebäude-, Personen- und Datensicherheit in intelligenten Gebäudesystemen“, Fraunhofer-IMS und inHaus-Zentrum Duisburg, 2003

[IFZ 2002] Kehrer, C.; Sieberath, U.: „My home is my castle“, IFZ, Informationszentrum Fenster Türen Fassaden e. V., Rosenheim, 2002, http://www.ifz-rosenheim.de/

[IPAS 2002] Russak, O.: „Secure EIB/KNX data transmission for security critical applications“, Conference Proceedings, Konnex Scientific Conference 2002, TU-München, 2002

[JCM 2000] Java Card Management: „Java Card Management Specification 1.0b“, 2000, http://www.javacardforum.org/

[Jeanrond 1996] Jeanrond, P. F.; Horst, H. H.; Rohrbacher, H. M.: „EIB Gebäudesystemtechnik“, Pflaum Verlag München, 1996, ISBN 3-7905-0712-1

[Köln 2002] Polizeipräsidium Köln: „Kölner Studie 2001“, (Kriminal-) Polizeiliche Beratungsstelle K61, Köln, 2002, http://www.polizei-koeln.de/

[Konnex 2002] Crijns, H.: „The added Value of the KNX Standard“, Konnex Association Brussels, Proceedings, Konnex Scientific Conference 2002, München, 2002

[Kranz 1997] Kranz, H. R.; et al.: „Building Control“, Expert Verlag, 1997, ISBN 3-81691-115-3

[Kriesel 1998] Kriesel, W.; Heimbold, D.; Telschow, D.: „Bustechnologien für die Automation“, Hüthig Verlag, 1998, ISBN 3-7785-2616-2

[Lawrenz 2000] Lawrenz, W.: „CAN Controller Area Network. Grundlagen und Praxis“, Hüthig Verlag, 2000, ISBN 3-778-52780-0

[Lidl 1986] Lidl, R.; Niederreiter, H.: „Intoduction to finite fields and their applications“, Cambridge University Press, 1986

[Loomis 2001] Loomis, D.: „The TINI Specification and Developer’s Guide“, Addison Wesley Publishing Company, Boston, 2001

[Monrose 1997] Monrose, F.; Rubin, A.: „Authentication via Keystroke Dynamics“, Scientific Literature Digital Library, NEC Research Institute, 1997, http://citeseer.nj.nec.com/cs

[Münz 2001] Münz, S.: „SELFHTML“, Version 8.0, http://selfhtml.teamone.de/

[Niederst 2002] Niederst, J.: „HTML kurz & gut“, O'Reilly, 2002, ISBN 3-897-21243-9

[Oestereich 1998] Oestereich, B.: „Objektorientierte Softwareentwicklung“, R. Olden-burg Verlag, 1998, ISBN 3-486-24787-5

[Paulke 2002] Paulke, I.: „Entwicklung eines CAN-Bus-Interface zur verschlüsselten Benutzerauthentisierung mittels Smartcards und Transpondern“, Diplomarbeit, Lehrstuhl für Messsystem- und Sensortechnik, Technische Universität München, 2002

[Perrig 2002] Perrig, A.: „Secure Broadcast Communication in Wired and Wireless Networks“, Kluwer Academic Publishers, 2002, ISBN 0-792-37650-1

[PKS 2002] Bundeskriminalamt: „Polizeiliche Kriminalstatistik Berichtsjahr 2002“, Punkt 3.7, Diebstahl unter erschwerenden Umständen, 2003, http://www.bka.de/

[Porter 1997] Porter, J. E.: „On the "30 error" criterion“, National Biometric Test Center, Collected Works, 1997-2000, San Jose State University

[Rankl 2002] Rankl, W.; Effing, W.: „Handbuch der Chipkarten“, Hanser Fachbuchverlag, 2002, ISBN 3-44622-036-4

[RSA 1978] Rivest, R. L.; Shamir, A.; Adleman, L. M.: „A Method for Obtaining Digital Signatures and Public-Key Cryptosystems“, Communication of the ACM, 1978

[Russak 2002] Russak, O.: „Sichere EIB Datenübertragung für sicherheitskritische Anwendungen“, IPAS GmbH, Duisburg, 2002

[Schels 2002] Schels, A.: „Biometric Technology – Matching on Smart Cards“, Siemens AG, ICM RDC IS BIO, 2002, http://www.fingertip.de/

[Schneier 1996] Schneier, B.: „Angewandte Kryptograpie“, Addison-Wesley, Bonn, 1996, ISBN 3-89319-854-7

[Schweiz 2000] Aebischer, B.; Huser, A.: „Vernetzung im Haushalt, Auswirkungen auf den Stromverbrauch“, Schweizer Bundesamt für Energie, Schlussbericht, 2000

[Seip 1997] Seip, G. G.; Hagedorn, K.; Wacker, S.: „Handbuch Gebäudesystemtechnik“, Zentralverband Elektrotechnik- und Elektroindustrie e.V., Frankfurt, 1997

[Seip 2000] Seip, G. G.: „Elektrische Installationstechnik“, Wiley-VCH Verlag, 2000, ISBN 3-895781-60-6

[Selke 2000] Selke, G. W.: „Kryptographie, Verfahren, Ziele, Einsatzmöglichkeiten“, O’Reilly, 2000, ISBN 3-89721-155-6

[Sensory 2000] Sensory Inc.: „RSC-300/364 Data Book“, Sensory Inc., USA, 2000, http://www.voiceactivation.com/

[Sensory 2002] Sensory Inc.: „RSC-300/364 Speech Recognition Microcontroller“, Sensory Inc., USA, 2002, http://www.sensoryinc.com/

[Sietmann 2002] Sietmann, R.: „Im Fadenkreuz“, c’t 2002, Heft 5, Seite 146-155, Heise Verlag, 2002

[SiWo 2002] Polizeipräsidium Düsseldorf: „Sicheres Wohnen“, Kriminalkommissariat Vorbeugung, Kriminalpolizeiliche Beratungsstelle Düsseldorf, Düsseldorf, 2002

[SPINS 2002] Perrig, A., et al.: „SPINS: Security Protocols for Sensor Networks“, Wireless Networks 8, Kluwer Academic Publishers, 2002

[Spitz 2002] Spitz, S.: „Entwurf einer Beschreibungssprache zur Verifikation digitaler Signaturen“, Dissertation, Technische Universität München, 2002

[Steyer 1999] Steyer, R.: „Java 2“, Markt & Technik bei Heyne, Band 67, 1999, ISBN 3-453-16822-4

[Steyer 2001] Steyer, R.: „Java 2 – Kompendium“, Markt & Technik, 2001, ISBN 3-827-26039-6

[Tanenbaum 2002] Tanenbaum, A. S.: „Computer Networks“, Prentice Hall, 2002, ISBN 0-130-66102-3

[TopSec 2000] Siemens AG: „TopSec ID Module A1.0/A2.0 zur Fingerprinterkennung“, http://www.fingertip.de/“, 2000

[TPUART 2001] Siemens AG: „Technical Data EIB-TP-UART-IC“, Datasheet Revision D, Siemens AG, 2001, http://www.knx-developer.de/online/data/tpuart_d.pdf

[Umwelt 2003] Das Umwelthaus/BfC: „Fenster und Türen“, Hennef, 2003, http://www.dasumwelthaus.de/

[Vary 1998] Vary, P.; Heute, U.; Hess, W.: „Digitale Sprachsignalverarbeitung“, Teubner Verlag, 1998, ISBN 3-519-06165-1

[VDE 0830] Verband der Elektrotechnik, Elektronik und Informationstechnik: Norm VDE 0830, Teil 1 - 5 und Teil 7, Alarmanlagen, VDE-Verlag, 1997 - 2002

[VDE 0833] Verband der Elektrotechnik, Elektronik und Informationstechnik: Norm DIN VDE 0833, Teil 1 - 3, Gefahrenmeldeanlagen für Brand, Einbruch und Überfall, VDE-Verlag, 1999 – 2003

[Weinzierl 2001] Weinzierl, T.: „Integriertes Managementkonzept für die Gebäudetechnik“, Pflaum Verlag München, 2001, ISBN 3-7905-0851-9

[Werthsch 2003] Werthschulte, K.: „Integration von heterogenen Bussystemen in die Heimautomatisierung unter Verwendung von Middleware“, Dissertation, Technische Universität München, 2003

[Westermeir 1999] Westermeir G., Weinzierl T., Schneider F.: „Interfacing the EIB Bus with Windows Computers“, Proceedings EIB Scientific Conference 1999, Seite 133-145, TU-München, München, 1999

[Westermeir 2000] Westermeir G., Weinzierl T., Schneider F.: „Techniken zur Verbindung des EIB Hausbusses mit dem Personal Computer“, VDI Berichte 1530, Sensoren und Meßsysteme 2000, Seite 33-42, Ludwigsburg, 2000, ISBN 3-18-091530-7

[Westermeir 2001a] Westermeir, G.; Schneider, F.; et al.: „System Technologies for Private Homes“, Sensor Applications Volume 2 – „Sensors in Intelligent Buildings“, Seite 511-558, Weinheim: WILEY-VCH, 2001, ISBN 3-527-29557-7

[Westermeir 2001b] Westermeir, G.; Schneider, F.: „Assets and Drawbacks of Fieldbus Systems in Home Automation for Use with Security Devices“, Sensor 2001, Proceedings Vol. I, Seite 295-300, Nürnberg, 2001

[Westermeir 2001c] Westermeir, G.; Schneider, F.: „Anwendung eines Standard Feldbussystems zur Authentifizierung und Signalverarbeitung in sicherheitsrelevanten Umgebungen“, AHMT XV. Messtechnisches Symposium, Kiel, 2001, ISBN 3-8265-9122-4

[Westermeir 2001d] Westermeir, G.; Werthschulte, K.; Schneider, F.: „Secured Data Transmission for Control and Supervision of an EIB Installation using mixed Network Topologies“, Proceedings EIB Event 2001, TU-München, München, 2001

[Westermeir 2002] Westermeir, G.; Schneider, F.: „An approach to a comfortable and secure EIB/KNX home access“, Konnex Scientific Conference 2002, TU-München, München, 2002

[Westermeir 2003a] Westermeir, G.; Schneider, F.: „A comfortable and secure EIB/KNX home access“, AMA Service GmbH, SENSOR 2003 Proceedings, Seite 437 – 442, Nürnberg, 2003

[Westermeir 2003b] Westermeir, G.: “Die Intelligente Tür“, Abschlussbericht tele-Haus mit intelligenten Mikrosystemen, VDI/VDE-IT, Band 84/2003, Seite 177 – 194, Teltow, 2003, ISBN 3-89750-117-1

[Westermeir 2003c] Westermeir, G.: „Forschung und Praxis im tele-Haus“, Bundes Bau Blatt 6/2003, Bundesministerium für Verkehr, Bau- und Wohnungswesen, Seite 37 – 39, ISSN 007-5884

[Wohlm 2001] Wohlmacher, P.: „Digitale Signaturen und Sicherheitsinfrastrukturen“, it-Verlag, 2001, ISBN 3-936052-01-8

[Ziegler 2002] Ziegler, P.-M.: „Shake-Hands, Datenaustausch per Hautkontakt“, c’t 2002, Heft 22, Seite 50, Heise Verlag, 2002

[ZigBee 2003] Kinney, P.: „ZigBee Technology: Wireless Control that Simply Works“, White Paper, IEEE 802.15.4 Task Group, 2003, http://www.zigbee.org/

[Zimmer 1996] Zimmerman, T. G.: „Personal Area Networks: Near-field intrabody communication“, IBM Systems Journal, Volume 35, Numbers 3&4, 1996, http://www.research.ibm.com/journal/sj/353/sectione/zimmerman.pdf

[Zimmer 1999] Zimmerman, T. G.: „Wireless networked digital devices: A new paradigm for computing and communication“, IBM Systems Journal, Volume 38, Number 4, 1999, http://www.research.ibm.com/journal/sj/384/zimmerman.pdf