Sicherheitsanalyse von Gebäudeautomationsnetzen auf Feldbusebene am Beispiel von KNX

Masterarbeit

Universität Rostock
Fakultät für Informatik und Elektrotechnik
Institut für Informatik
Lehrstuhl für Informations- und Kommunikationssysteme

vorgelegt von:	Johannes Goltz
Matrikelnummer:	213205061
geboren am:	03.07.1993 in Chemnitz
Erstgutachter:	Prof. Dr. rer. nat. Clemens H. Cap
Zweitgutachter:	Prof. Dr. rer. nat. habil. Andreas Heuer
Betreuer:	Dr.-Ing. Thomas Mundt
Abgabedatum:	26. April 2018

Danksagung

An dieser Stelle möchte ich mich besonders bei Dr. Thomas Mundt bedanken, der meine Masterarbeit betreut hat und mir während der Bearbeitungszeit immer beratend zur Seite stand.

Weiterhin möchte ich auch Simeon Wiedenmann und Martin Peters meinen persönlichen Dank aussprechen. Neben der Hilfe bei der Korrektur sind zusammen in gemeinsamen Gesprächen viele Ideen gereift, ohne die die Arbeit so nicht möglich gewesen wäre.

Johannes Goltz,
Rostock, den 26. April 2018

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

EIB	Europäischer Installationsbus
EEPROM	Electrically Erasable Programmable Read-Only-Memory 10
DAF	Destination address flag 12
CSMA/CA	Carrier Sense Multiple Access / Collision Avoidance 14
UART	Universal Asynchronous Receive Transmit 15
LSB	Least Significant Bit 15
MSB	Most Significant Bit 15
APCI	Application layer protocol control information 16
LTE	Logical Tag Extended Mode 17
DPT	Datapoint type 17
UDP	User Datagram Protocol 24
TCP	Transmission Control Protocol 24
DDoS	Distributed Denial of Service 30
QoS	Quality of Service 30
ETS	Engineering Tool Software 31
DoS	Denial of Service 35
PDU	Protocol Data Unit 39
ASAP	Application Layer Service Access Point 39
BSI	Bundesamt für Sicherheit in der Informationstechnik 43
IDS	Intrusion Detection System 60
CVSS	Common Vulnerability Scoring System 77

Kapitel 1

Einleitung

Hausautomatisierung im privaten Umfeld hat auch die Gebäudeautomation in industriellen Anwendungen und die damit verbundenen Probleme weiter in den Vordergrund rücken lassen. Die Verknüpfung von intelligent gesteuerten Heizungen oder Klimaanlagen in Verbindung mit Thermostaten, die Lichtsteuerung per Bewegungsmelder und die Schaffung einer zentralen Monitoring-Lösung bringt viele Vorteile mit sich. Neben diesen Vorteilen sind aber auch einige zum Teil gravierende Nachteile im Sinne von Sicherheitslücken in den bestehenden Installationen und Protokollen zu finden.

Für Neubauten, aber auch bestehende Gebäude, ist es wichtig zu wissen welche Kabel für welchen Zweck, wo verlegt wurden. Sind Datenleitungen im Zweifel sogar offen sichtbar? Es ist auf jeden Fall zu prüfen, ob Leitungen angeschlossen sind und welche Geräte eventuell erreichbar sind. Bei einer Bestandsaufnahme ist es wichtig, die Einschätzung zur Gefährdung quantifizierbar zu machen. Diese Arbeit soll Möglichkeiten Aufzeigen, wie Risiken in Bussystemen bestimmt werden können und welche Verteidigungsmaßnahmen getroffen werden können, um sich gegen Angreifer zu schützen. Dabei soll nicht die Anlage gegen ein neues System getauscht werden, sondern es soll gezeigt werden, wie eine Verbesserung des Sicherheitsniveaus vorgenommen werden kann und wie neue Anlagen in Bezug auf Sicherheit geplant werden sollten.

1.1 Fragestellungen der Arbeit

KNX stellt den Nachfolger des europäischen Installationsbusses (EIB) dar. 1999 schloss sich der EIB mit anderen europäischen Vereinigungen zu KNX zusammen [Ass13]. Trotz zwischenzeitlicher Aktualisierung ist der Standard aufgrund der Abwärtskompatibilität immer noch stark mit Altlasten belastet. Die Kompatibilität mit älteren Geräten ist ein besonders wichtiger Punkt, da die Bauteile in Gebäuden nicht regelmäßig aktualisiert werden und daher auch über viele Jahrzehnte zusammen funktionieren müssen.

Früher waren Gebäudeautomationssysteme häufig abgeschottete Systeme, die nur diesem Zweck dienten und nicht mit anderen Netzen verknüpft waren. Heute hat sich dies allerdings gewandelt. Durch das Internet lassen sich zum Beispiel die Systeme von verschiedenen Standorten bequem zentral verwalten und für die Fehlersuche ist es für Elektroinstallationsfirmen einfacher per VPN einen Zugang zum gewünschten Gebäude zu haben, als tatsächlich physisch vor Ort die Fehlersuche ausführen zu müssen. Durch diese Vernetzung hat sich allerdings auch die Gefährdungseinschätzung deutlich geändert, während die Standardisierung nicht an diese Situation angepasst wurde. Neben fehlender Authentisierung gibt es auch keine nennenswerte Verschlüsselung und selbst die Filterung von Nachrichten auf dem Bus, die eigentlich von Kopplern verschiedener Segmente vorgesehen ist, wird häufig aus Gründen der Bequemlichkeit und Vereinfachung beim Debugging nicht genutzt. Dies wiederum führt zu paradiesischen Zuständen für potenzielle Angreifer, die eine wahre Flut an Angriffsmöglichkeiten ausnutzen können.

Auch aufgrund dieser Umstände wächst das Interesse an der Thematik und so schätzen 69 Prozent einer Umfrage die Gefahr für Industriesteuerungssysteme als hoch oder kritisch ein [GW17]. Hausautomationssysteme sind hierbei nur ein kleiner Teil der Industriesteuerungssysteme.

Weiterhin ist anzumerken, dass die Protokolle in Bezug auf Sicherheitsfunktionen sehr schlecht entworfen wurden. Trotzdem besteht die Möglichkeit Installationen derart zu betreiben, dass ein gewisses Maß an Sicherheit gewährleistet werden kann. Zumindest Versuche des Eindringens oder der Manipulation können festgestellt werden.

Diese Arbeit untersucht, folgende Problematiken anhand des Feldbusses KNX als Beispielvertreter für ein Gebäudeautomationssystem.

1. Wie kann die Gefährdung in einem Netz oder Netzsegment gemessen werden und lässt sich diese sinnvoll quantifizieren?
   Dies ist besonders wichtig, um weitestgehend automatisiert Schwachpunkte in einem System aufdecken zu können und gezielte Gegenmaßnahmen zu ergreifen. Dabei soll vor allem ein Wert für das Risiko dieser Bereiche bestimmt werden, der dann die Grundlage für die Erkennung von Schwachpunkten liefert.

2. Wie kann die Infrastruktur sinnvoll gegen Angriffe gesichert werden und welche Maßnahmen sollten für die Verteidigung ergriffen werden?
   Die Beantwortung der Frage ist eng mit der ersten Frage verbunden, da Problemstellen selbstverständlich zuerst identifiziert werden müssen, um anschließend Methoden zu entwickeln gegen diese Probleme vorgehen zu können. An dieser Stelle soll auch gezielt betrachtet werden, wie eine Zoneneinteilung aus dem Blickwinkel der Sicherheit optimal vorgenommen werden kann. Neben der Betrachtung aus Protokoll- und Telegrammsicht muss dabei auch die physische Planung und Umsetzung des Netzes genauer betrachtet werden.

3. Lässt sich eine Erkennung von sicherheitskritischen und damit besonders gefährdeten Punkten vollständig automatisieren?
   Wünschenswert wäre die komplette Automatisierung des Prozesses Probleme in Gebäudeautomationsnetzen auffinden zu können. Neben der schnelleren Bearbeitung wird so auch sichergestellt, dass ein rein objektives Verfahren genutzt wird, und keine subjektiven Meinungen in den Prozess einfließen. Diese Frage hängt dabei ebenfalls eng mit Frage eins zusammen. Zum einen ist es wichtig das Risiko überhaupt quantifizierbar und messbar bestimmbar zu machen, um den Prozess überhaupt automatisieren zu können, zum anderen ist die Automatisierung für eine mögliche Bestimmung des Risikos sehr angenehm.

1.2 Überblick über die Arbeit

Die Arbeit lässt sich in drei grobe Teile gliedern. Kapitel 1 und 2 motivieren das Thema und geben einen Überblick über die nötigen grundlegenden Informationen zum Verständnis. In Kapitel 3, 4 und 5 wird beschrieben, wie Angriffe auf Gebäudeautomationsnetze aussehen und kategorisiert werden können. Es werden auch einige Beispiele konkret vorgestellt. Im Kapitel Risikoeinstufung von KNX-Netzen (4) wird gezeigt, wie ein Risiko für Netzsegmente oder auch ganzen Netzen abgeschätzt werden kann, während Kapitel 5 Maßnahmen vorstellt, die der Verteidigung von Angriffen dienen können und somit auch das Risiko solcher Angriffe minimieren. Im letzten Teil wird ein Demonstrator konzeptioniert und projektiert, sowie die Arbeit in Kapitel 7 zusammengefasst. Dabei wird auch ein Ausblick auf offene Fragestellungen gegeben.

Kapitel 2

Grundlagen

Dieses Kapitel gibt einen ersten Überblick zu den Grundlagen von KNX als einen Vertreter der Feldbusse, zur Planung von Zonen in IP-Netzen und auch zur Funktionsweise von Netflows. Während KNX die Grundlage für alle weiteren Betrachtungen bietet, werden die Zoneneinteilung und Netflows in Kapitel 5 noch einmal aufgegriffen.

Um die Thematik genauer verstehen zu können, beschreibt Definition 1 was unter einem Bussystem zu verstehen ist.

Definition 1. *Ein Bus beschreibt ein „Kommunikationsmedium und -methode zwischen zwei oder mehreren Einrichtungen mit Schnittstellen für serielle Datenübertragung.“ In der Regel wird auch eine linienförmige Topologie als Bus bezeichnet. [DIN16]*

Das Beispiel KNX wurde als Vertreter der Bussysteme gewählt, da es im Gebäude (Konrad-Zuse-Haus, Albert-Einstein-Str. 22, 18059 Rostock) als Gebäudeautomationsbus eingesetzt wird. Die Ergebnisse sind allerdings zu großen Teilen auf andere Bussysteme übertragbar. Definition 2 erläutert den Begriff der Gebäudeautomation genauer.

Definition 2. *Gebäudeautomation ist die „Bezeichnung der Einrichtungen, Software und Dienstleistungen für automatische Steuerung und Regelung, Überwachung und Optimierung sowie für Bedienung und Management zum energieeffizienten, wirtschaftlichen und sicheren Betrieb der technischen Gebäudeausrüstung.“ [DIN16]*

2.1 KNX als Vertreter eines Feldbusses

Der EIB stellt den Vorgänger von KNX dar. In diesem Kapitel sollen die Grundlagen von KNX als industrielles Kommunikationssystem vorgestellt werden. KNX dient dabei zur informationstechnischen Vernetzung von Haus- und Gebäudeautomationstechnik. Über das Bussystem können Sensoren, Aktoren, Steuer- und Regelgeräte sowie Bedien- und Beobachtungsgeräte zusammen kommunizieren und die entsprechenden Funktionen umsetzen. Hierfür wird ein gemeinsames Medium zur Kommunikation genutzt [Ass13]. Aktionen werden dabei in der Regel durch Sensoren ausgelöst, die ein Datentelegramm über den Bus an bestimmte Aktoren aussenden, welche den Eingang bestätigen und die entsprechenden Aktionen umsetzen. Beim KNX handelt es sich um einen offenen Standard, sodass auch Geräte verschiedener Hersteller miteinander kommunizieren können und somit der Kunde bei der Wahl der einzelnen Komponenten deutlich mehr Möglichkeiten hat [Ass13].

Bei konventionellen Installationen wird für jedes Gewerk, zum Beispiel Licht oder Heizung, eine Firma beauftragt, die die Planung und die Umsetzung übernimmt. Dies bedeutet allerdings einen erhöhten Aufwand bezüglich der Installation und auch der Fehlersuche oder Wartung. Eine Verknüpfung von unterschiedlichen Komponenten ist dabei nur sehr schwierig umzusetzen [MHH09]. Durch den Einsatz eines Gebäudeautomationsbusses müssen die entsprechenden Gewerke gemeinsam geplant werden. Die Verknüpfung der einzelnen Komponenten führt zu mehr Funktionalität, Flexibilität und auch einem erhöhten Komfort, da derartige Systeme vergleichsweise deutlich leichter an neue Anforderungen anpassbar sind. Der Nachteil des Einsatzes eines KNX-Systems gegenüber einer konventionellen Installation liegt vor allem im Preis. Dies ist auch der Grund, dass sich derartige Systeme in der Regel nur lohnen, wenn flexible und schnelle Anpassungen der Installationen nötig sind, oder sehr spezielle Funktionen umgesetzt werden sollen [MHH09].

2.1.1 Übertragungsmedien

Bei KNX handelt es sich um ein Bussystem. Hierbei ist der Physical-Layer (OSI-Layer 1) allerdings nicht zwangsweise vorgegeben und je nach Einsatzzweck können unterschiedliche Medien zur Übertragung der Daten genutzt werden. Neben dem „klassischen“ Twisted Pair (KNX TP) gibt es auch weitere standardisierte Medien

wie Power Line (KNX PL), Radio Frequency (KNX RF) und Ethernet (KNXnet/IP) [Ass13]. Die zu sendenden Daten werden von dem KNX-Gerät in ein entsprechendes physikalisches Signal umgewandelt, welches dann über den Bus verteilt wird.

Im Folgenden wird lediglich die Umsetzung von KNX auf Twisted-Pair-Kabel betrachtet. Die genaue Betrachtung weiterer Übertragungsmedien ist für die Arbeit aus zeitlichen Gründen und dem Mangel an solchen Geräten nicht möglich. Zudem ist zu sagen, dass sich die Ergebnisse dieser Arbeit als allgemeingültig für KNX angesehen werden können, da lediglich die Datenrate und die Buszugriffsverfahren bei anderen Übertragungsmedien unterschiedlich sind. Zu KNX-IP ist anzumerken, dass dies nur im Bereich von Bereichs- oder Hauptlinien eingesetzt werden kann.

Bei der Lösung mittels Twisted Pair beträgt die Übertragungszeit für ein Bit 104 μs. Damit kann man die Datenrate wie in 2.1 zu sehen berechnen [MHH09].

$$R = \frac{1}{T} = \frac{1\ Bit}{104\ \mu s} \approx 9615\ \frac{Bit}{s} \approx 9,6\ \frac{kBit}{s} \tag{2.1}$$

Das Übertragungsmedium wird dabei von unterschiedlichen Akteuren genutzt. Die Wichtigsten lassen sich in folgende Kategorien einteilen [Ass13]:

- Systemgeräte - (z. B.: Spannungsversorgungsgerät, Busleitung, Koppler, IP-Gateway, ...)
- Sensoren - (z. B.: Tastsensor, Temperatursensor, Bewegungsmelder, ...)
- Aktoren - (z. B.: Schaltaktor, Heizung, ...)

Diese Teilnehmer agieren im Betrieb miteinander und ermöglichen durch einen gegenseitigen Nachrichtenaustausch die Steuerung der verschiedenen Komponenten.

2.1.2 Logische Strukturierung von KNX

Grundsätzlich lassen sich bei einer KNX-TP-Installation zwei Netze unterschieden. Zum einen gibt es das Energieversorgungsnetz mit Wechselspannung von 230 Volt und zum anderen gibt es das Kommunikationsnetz. Auf diesem liegt eine Spannung

von 32 bis 20 Volt an [DIN04c]. Die beiden Netze sind dabei physikalisch vollständig voneinander getrennt [MHH09].

Zwei KNX-Geräte sind immer über eine Busleitung verbunden. An diese werden folgende Anforderungen gestellt. Die Länge der Leitungen kann nicht beliebig gewählt werden, da dies die Kommunikation zum Erliegen bringen würde. Durch die starke Erhöhung der Signallaufzeiten würde die Datenrate zu sehr absinken und eine Kommunikation wäre nur noch bedingt möglich. Außerdem würde die Spannung bei zu großer Entfernung zur Spannungsversorgung stark abfallen. Dies wiederum würde zur Fehlfunktion von Komponenten führen. Genaueres dazu in den folgenden Abschnitten zu Linien und Teilnehmern.

KNX-Anlagen sind auf der logischen Ebene immer hierarchisch aufgebaut, wie in Abbildung 2.1 zu sehen. Es werden dabei für die physikalischen Adressen Bereiche, Linien und Teilnehmer unterschieden. Die Untergliederung ist in einer Baumstruktur geordnet [SHS17]. Im Folgenden sollen die Bereiche der Struktur jeweils kurz vorgestellt werden (nach [MHH09]).

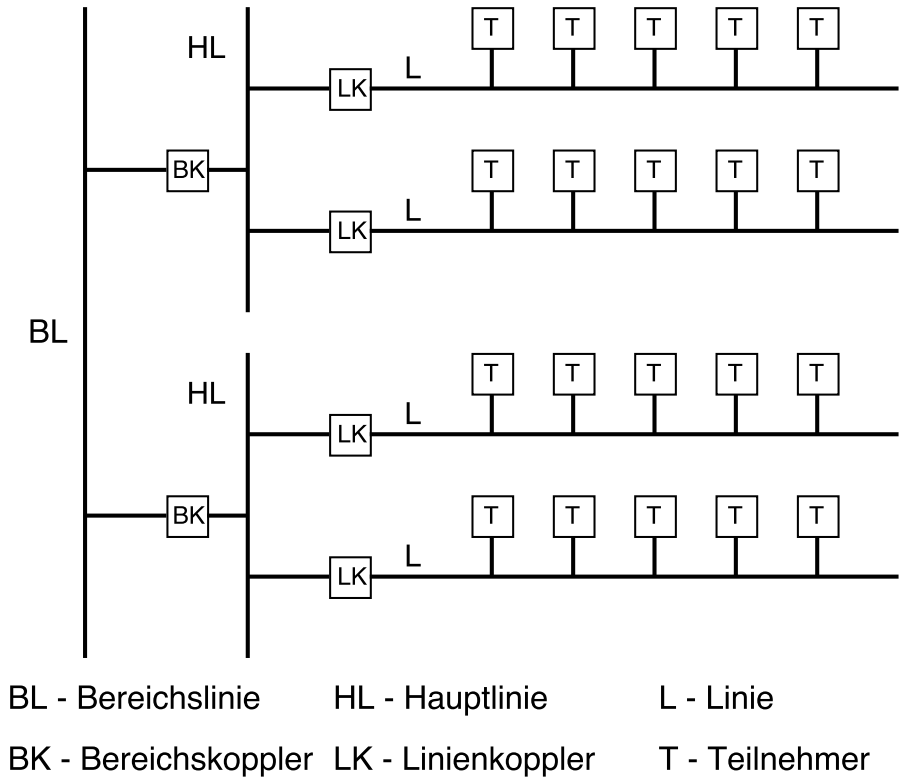

Abbildung 2.1: Darstellung der logischen Gliederung von KNX-Systemen in Bereiche, Hauptlinien und Linien mit entsprechenden Teilnehmern (nach [MHH09])

Bereiche

Bereiche werden durch einzelne Hauptlinien gebildet und können über Bereichskoppler mit der Bereichslinie verbunden werden. Diese bildet die hierarchisch am höchsten angeordnete Busverbindung (auch Backbone-Line) [Ass13].

Linien

Linien können über Linienkoppler an Hauptlinien angeschlossen werden. Es ist auch möglich mehrere Linien zu nutzen, um die Ausfallsicherheit zu erhöhen oder auch verschiedene Busabschnitte von Telegrammen zu entlasten. Im Standard sind zwei unterschiedliche Varianten für den Aufbau der Linien bei KNX TP vorgesehen. Zum einen gibt es TP1-64. Hier kann eine Linie aus bis zu vier Liniensegmenten mit jeweils maximal 64 Teilnehmern bestehen. Die drei Liniensegmente, welche das erste der vier Liniensegmente erweitern, müssen dabei parallel geschaltet werden, da einzelne Telegramme maximal über sechs Koppler weitergeleitet werden. Ein Linienkoppler zählt als Teilnehmer, da er eine physikalische Adresse besitzt. Zum anderen gibt es die Variante TP1-256. Diese besteht aus nur einem Liniensegment, wobei daran bis zu 256 Teilnehmer angeschlossen werden können. Mehr Geräte sind generell nicht möglich, da zur Adressierung der Teilnehmer lediglich 8 Bit vorgesehen sind.

Teilnehmer im KNX-Bus benötigen nicht zwangsweise eine eigene Stromversorgung, sondern können über die auf dem Bus anliegende Spannung versorgt werden. Dafür werden Spannungsversorgungen benötigt. Auf den Leitungen einer Linie, beziehungsweise eines Liniensegments liegt eine Spannung von 30 Volt an. Spannungsversorgungen gibt es in zwei Ausführungen mit 640 mA und 320 mA [SHS17]. Sollten zwei Spannungsversorgungen auf der gleichen Linie oder im gleichen Bereich eingesetzt werden, müssen diese mindestens 200 Meter voneinander entfernt installiert sein. Durch die Trennung in unterschiedliche Linien und Liniensegmente ist es möglich, dass auch beim Ausfall einzelner Stromversorgungen der Rest des Busses weiterhin funktioniert und nur ein Teil der Komponenten von der Kommunikation abgeschnitten ist [MHH09].

Teilnehmer

Teilnehmer werden einzelnen Linien und damit auch Bereichen zugeordnet. Es gibt keine Geräte ohne Zuordnung. Die Entfernung zwischen den beiden am weitesten Entfernten Teilnehmern eines Liniensegments darf 700 Meter nicht überschreiten. Die Länge der Leitung zwischen einem Teilnehmer und einer Spannungsversorgung darf 350 Meter nicht überschreiten, da ansonsten der Spannungsabfall über die Distanz zu groß wäre [MHH09].

2.1.3 Adressierung

Es werden zwei Arten von Adressen unterschieden. Neben physikalischen Adressen für Unicasts gibt es auch Gruppenadressen für Multicasts.

Physikalische Adressen

Die physikalische Adresse ist für jedes Gerät eindeutig und dient der Übertragung der entsprechenden Applikation von der Programmiersoftware aus. Damit kann das Gerät konfiguriert werden. Beim Aufbau und der Inbetriebnahme wird diese im Electrically Erasable Programmable Read-Only-Memory (EEPROM) gespeichert. Physikalische Adressen werden in der Punktnotation geschrieben und sind folgendermaßen gegliedert:

```
1 Bereich.Linie.Teilnehmer
```

Die Adresse 1.1.12 beschreibt somit den zwölften Teilnehmer auf der ersten Linie im ersten Bereich [Ass13]. Für die physikalischen Adressen sind in den Telegrammen 2 Byte vorgesehen. Die Aufteilung erfolgt dabei wie in Tabelle 2.1 dargestellt.

höherwertiges Byte								niederwertiges Byte							
B7	B6	B5	B4	B3	B2	B1	B0	B7	B6	B5	B4	B3	B2	B1	B0
B3	B2	B1	B0	L3	L2	L1	L0	T7	T6	T5	T4	T3	T2	T1	T0
Bereich				Linie				Teilnehmer							
Subnetz-Adresse															

Tabelle 2.1: Aufbau der physikalischen Adressen bei KNX-Telegrammen in Bits (nach [DIN04b]).

Damit kann es maximal $2^4 = 16$ Bereiche, $2^4 = 16$ Linien und $2^8 = 256$ Teilnehmer geben. Insgesamt können somit höchstens $2^{16} = 65536$ Adressen vergeben werden.

Dabei ist zu beachten, dass Linienkoppler in der Regel die Adresse Bereich.Linie.0 und Bereichskoppler die Adresse Bereich.0.0 erhalten. Dies erhöht die Übersichtlichkeit der Anlagen. Linienverstärker wiederum müssen eine Adresse erhalten, die größer 0 ist [MHH09].

Logische Adressen

Neben den physikalischen gibt es noch Gruppenadressen. Diese werden zur besseren Unterscheidbarkeit mit Schrägstrichen geschrieben (z. B.: 1/1, oder 1/2/1). Gruppenadressen werden zur Kommunikation der Geräte untereinander genutzt, da sie entsprechende Kommunikationsobjekte der einzelnen Komponenten enthalten. Es gibt die Gruppenadressen mit Zwei- und Drei-Ebenen-Struktur. Im Telegramm sind für diese Adressen zwei Byte vorgesehen, von denen allerdings nur 15 Bit genutzt werden. Der Aufbau ist in Tabelle 2.2 gezeigt.

höherwertiges Byte								niederwertiges Byte							
B7	B6	B5	B4	B3	B2	B1	B0	B7	B6	B5	B4	B3	B2	B1	B0
H4	H3	H2	H1	H0	U10	U9	U8	U7	U6	U5	U4	U3	U2	U1	U0
Hauptgruppe					Untergruppe										

Tabelle 2.2: Aufbau der 2-Ebenen-Gruppenadressen bei KNX-Telegrammen in Bits (nach [SHS17]).

Beim Einsatz von Zwei-Ebenen-Gruppenadressen kann es demnach $2^5 = 32$ Hauptgruppen und $2^{11} = 2048$ Untergruppen geben. Die Adressen werden dann wie folgt geschrieben:

```
1 Hauptgruppe/Untergruppe
```

Für die Drei-Ebenen-Gruppenadressen ist die Aufteilung der Bits in Tabelle 2.3 gezeigt. Die Notation erfolgt genauso wie die für die Zwei-Ebenen-Gruppenadressen, nur dass noch eine weitere Ebene mit einem Schrägstrich eingeführt wird.

höherwertiges Byte								niederwertiges Byte							
B7	B6	B5	B4	B3	B2	B1	B0	B7	B6	B5	B4	B3	B2	B1	B0
H4	H3	H2	H1	H0	M2	M1	M0	U7	U6	U5	U4	U3	U2	U1	U0
Hauptgruppe					Mittelgruppe			Untergruppe							

Tabelle 2.3: Aufbau der 3-Ebenen-Gruppenadressen bei KNX-Telegrammen in Bits (nach [SHS17]).

Bei der Nutzung von Drei-Ebenen-Gruppenadressen sind damit $2^5 = 32$ Hauptgruppen, $2^3 = 8$ Mittelgruppen und $2^8 = 256$ Untergruppen möglich. Die Hauptgruppen 14 und 15 werden in der Regel nicht verwendet, da diese in den Filtertabellen von Kopplern in der Regel keinen Platz finden und Pakete dieser Zuordnung in der Defaulteinstellung verworfen werden [MHH09]. Sollten sie trotzdem benötigt werden, müssen Koppler entsprechend konfiguriert werden, dass diese Nachrichten weitergeleitet werden [SHS17].
Einige Zuordnungen von Hauptgruppen zu Funktionen sind inzwischen häufig anzutreffen [MHH09]:

- 0: Zentralfunktionen/Alarme
- 1: Licht/Steckdosen
- 2: Rollläden/Jalousien
- 3: Heizung

Um unterscheiden zu können, ob es sich um eine physikalische oder eine Gruppenadresse innerhalb eines Telegramms handelt, wird das „Destination address flag (DAF)“ gesetzt. Ist dieses auf „0“ gesetzt, handelt es sich um eine physikalische Adresse, beim Wert „1“ um eine Gruppenadresse [MHH09].

2.1.4 Kommunikationsablauf

Die Kommunikation auf dem KNX-Bus wird mittels Kommunikationsobjekten abgewickelt. Diese spielen für den Nachrichtenaustausch zwischen verschiedenen Teilnehmern im laufenden Betrieb eine zentrale Rolle. Es ist der Applikationssoftware möglich, mithilfe der Kommunikationssoftware und Kommunikationsobjekten, mit anderen Teilnehmern über Telegramme zu kommunizieren. Kommunikationsobjekte können dabei folgende Daten enthalten [MHH09]:

- Bitfolge (1 Bit, 4 Bit, 8 Bit, ...)
- Variable (Integer, Float, ...)
- Zeit- oder Datumsangabe
- Text (z.B.: 10 ASCII-Zeichen)

Jedes Kommunikationsobjekt verfügt über eine Reihe von Attributen, die dieses näher beschreiben. Zu den Attributen gehören [MHH09]:

- Nummer
- Name
- Funktion
- Gruppenzugehörigkeit
- Länge
- Flags (K-Kommunikation, L-Lesen, S-Schreiben, Ü-Übertragen, A-Aktualisieren, I-Lesen beim Initialisieren)

Die Flags sind standardmäßig vorbelegt und werden nur im Ausnahmefall geändert. Sie sind dazu da, den Schreib- und Lesezugriff auf Kommunikationsobjekte zu regeln. Um Funktionen zu realisieren, werden die Objekte in der Projektierungssoftware zu diesen hinzugefügt. Dabei müssen alle Kommunikationsobjekte vom gleichen Typ sein. In jeder Funktionsgruppe müssen mindestens ein sendendes und ein empfangendes Kommunikationsobjekt vorkommen. Dabei dürfen sendende Kommunikationsobjekte maximal einer Gruppe zugeordnet werden, während empfangende Objekte auch in unterschiedlichen Gruppen vorkommen dürfen [MHH09]. Die Gruppenadresse wird im laufenden Betrieb für den Austausch der Daten zur erfolgreichen Umsetzung der Funktion genutzt.

In Tabelle 2.4 ist gezeigt, wie der zeitliche Ablauf für ein Standarddatentelegramm mit zwei Byte Nutzlast und dem dazugehörigen Bestätigungstelegramm aussieht. In der Summe dauert ein vollständiger Nachrichtenaustausch damit etwa $20,176\ ms$.

Aktivität	**Dauer in Bitzeiten**	**Dauer in μs**
Zeit, die Bus mindestens frei sein muss	53	5512
Datentelegramm wird gesendet	$8 \cdot (11 + 2) + 11 = 115$	11960
Pause	15	1560
Bestätigungstelegramm wird gesendet	11	1144
Summe:	194	20176

Tabelle 2.4: Dauer des vollständigen Nachrichtenaustausches bei einem Standarddatentelegramm der Zugriffsklasse zwei mit zwei Nutzdatenbytes (nach [MHH09]).

KNX-Geräte, welche Pakete versenden wollen, prüfen immer zuerst, ob der Bus frei ist. Je nach Prioritätsklasse werden hierfür 50 oder 53 Bitzeiten gelauscht. Sollten mehrere Teilnehmer zeitgleich ein Paket versenden wollen, kommt es zu einem

Konflikt. Diesen wird immer einer der Teilnehmer gewinnen. Dies kommt durch die dominante „0“ und die rezessive „1“. Sollten zwei Teilnehmer zeitgleich senden, wird der Teilnehmer gewinnen, der die höhere Prioritätsklasse besitzt. Es sind zwei unterschiedliche Klassen vorgesehen. Zugriffsklasse eins enthält System-, Alarm- und Wiederholungstelegramme. Diese Telegramme können nach dem Warten von 50 Bitzeiten versendet werden. In Zugriffsklasse zwei fallen Vorzugs- und Normaltelegramme. Diese können versendet werden, sobald der Bus für 53 Bitzeiten frei war. Sollten zwei Teilnehmer zeitgleich mit der gleichen Zugriffsklasse Telegramme absenden, so kommt Carrier Sense Multiple Access / Collision Avoidance (CSMA/CA) zum Einsatz. Hierbei kommen folgende Bits für die Entscheidung über den „Gewinner“ des Buszugriffes zum Tragen: Prioritätsbit (P1 und P0), Wiederholungsbit (R) (siehe Tabelle 2.6) und die Bits der Quelladresse [MHH09]. Die verschiedenen Kombinationen für die Prioritäten sind in Tabelle 2.5 gezeigt. Da das Bit P0 zuerst gesendet wird, hat es eine höhere Gewichtung als das Bit P1.

B3 P1	**B2 P0**	**Priorität**	**Nutzung**
0	0	Systempriorität	Telegramme hoher Priorität, Systemkonfiguration, Managementprozeduren
1	0	Dringliche Priorität	Nur für dringende Telegramme
0	1	Normale Priorität	Default für kurze Telegramme
1	1	Niedrige Priorität	Für lange Telegramme, Burst-Traffic, oder ähnliches

Tabelle 2.5: Möglichkeiten der Belegung der Prioritätsbits P0 und P1 und die entsprechenden Nutzungsszenarien (nach [DIN04b]).

Sobald ein Telegramm bei einem Empfänger nicht erfolgreich empfangen wurde, wird es durch das negative Bestätigungstelegramm erneut gesendet, wobei das Wiederholungsflag gesetzt wird und es automatisch in der Zugrissklasse eins (also nach 50 Bitzeiten warten) gesendet wird. Mehr dazu unter Abschnitt 2.1.5.

Sollte ein Empfänger außerhalb der Linie oder dem aktuellen Bereich liegen, so muss das Telegramm entsprechend vom Linien- oder Bereichskoppler weitergeleitet werden. Linienverstärker besitzen dabei keinerlei Filterfunktion sondern leiten das Telegramm unverändert in den anderen Bereich der Linie weiter. Koppler hingegen können Telegramme in andere Bereiche wahlweise immer weiterleiten, filtern oder generell blockieren. Sollte ein Fehler bei der Übertragung auftreten, wird der Versand bis zu dreimal wiederholt [MHH09]. Standarddatentelegramme können dabei

über bis zu sechs Koppler oder Verstärker weitergeleitet werden. Um diese Weiterleitungen zu zählen, gibt es im fünften Byte des Telegramms einen Routingzähler mit 3 Bit (siehe Tabelle 2.7).

2.1.5 Telegramme

Auslöser für Kommunikation unter den Geräten sind in der Regel einzelne Ereignisse von Sensoren. Dies kann ein Tastendruck, aber auch ein periodisch ausgelöstes Ereignis sein. Der Sensor versendet das Datentelegramm nach dem Auslösen an die entsprechende Gruppenadresse. Der Empfang des Telegramms wird anschließend von allen Teilnehmern in der Gruppe bestätigt. Grundsätzlich werden bei KNX drei unterschiedliche Arten von Telegrammen unterschieden [MHH09]. Diese werden im weiteren Verlauf vorgestellt. Um zu Unterscheiden um welche Art von Telegramm es sich handelt werden die ersten zwei Bits im ersten Byte des Telegramms entsprechend gesetzt. Zu sehen ist dies in Tabelle 2.6.

0. Byte								
B7	B6	B5	B4	B3	B2	B1	B0	
1	0	R	1	P1	P0	0	0	Standarddatentelegramm
0	0	R	1	P1	P0	0	0	erweitertes Datentelegramm
1	1	1	1	0	0	0	0	Abfragetelegramm
x	x	0	0	x	x	0	0	Bestätigungstelegramm

Tabelle 2.6: Aufbau des ersten Bytes eines Telegramms (Steuerfeld) bei KNX in Bits zur Angabe der Telegrammart (nach [DIN04c]).

Das Bit B5 gibt dabei an, ob es sich um ein Wiederholungstelegramm handelt und B3 mit B2 geben die unterschiedlichen Prioritätsklassen an.
KNX-Telegramme werden auf dem Bus als Universal Asynchronous Receive Transmit (UART)-Zeichen versendet. Das bedeutet, dass jedes Byte einzeln über den Bus versendet wird. Ein UART-Zeichen beginnt immer mit einem Startbit, welches den Wert „0“ besitzt. Anschließend folgen die 8 Datenbits (von Least Significant Bit (LSB) nach Most Significant Bit (MSB)) mit einem Paritätsbit für eine gerade Parität und einem Endbit mit dem Wert „1“. Nach jedem einzelnen UART-Zeichen wird eine Pause von 2 Bitzeiten eingelegt [MHH09].

Datentelegramm

Es gibt zwei unterschiedliche Datentelegramme in der Norm. Das Standarddatentelegramm besitzt bis zu 16 Bytes an Nutzdaten, während das erweiterte Datentelegramm bis zu 255 Bytes an Nutzdaten aufnehmen kann. Im Normalbetrieb sind allerdings häufig Telegramme mit zwei Bytes Nutzlast zu erwarten [MHH09]. In Tabelle 2.7 ist die Struktur eines Standarddatentelegramms gezeigt.

0. Byte	1./2. Byte	3./4. Byte	5. Byte			6. - 21. Byte	22. Byte
1 Byte	2 Byte	2 Byte	1 Byte			2 - 16 Byte	1 Byte
			1 Bit	3 Bit	4 Bit		
Steuer-feld	Quell-adresse	Ziel-adresse	Adresstyp (DAF)	Routing-zähler	Nutzdaten-länge	Nutzdaten	Prüffeld

Tabelle 2.7: Aufbau des Standarddatentelegramms bei KNX in Bits (nach [MHH09]).

Das DAF gibt an, ob es sich um eine physikalische oder Gruppenadresse handelt, und ist das erste Bit des fünften Bytes eines Telegramms.

Für den Routingzähler sind drei Bit im Telegramm vorgesehen. Damit sind Werte zwischen null und sieben möglich. Diese haben folgende Bedeutung (nach [SHS17]):

- Routingzähler 7: Nutzung zur Konfiguration/Wartung, das Telegramm wird beliebig häufig weitergeleitet und der Zählerstand wird dabei nicht verändert.
- Routingzähler 1 bis 6: Das Telegramm wird weitergeleitet und der Zählstand wird um eins reduziert.
- Routingzähler 0: Das Telegramm wird verworfen und nicht mehr weitergeleitet.

Aufgrund dieser Art der Weiterleitung ist es nicht möglich, dass mehr als sechs Linien- oder Bereichskoppler zwischen zwei Busteilnehmern bestehen, da diese sich sonst nicht erreichen würden. Im fünften Byte des Datentelegramms wird weiterhin die Länge der Nutzdaten mit vier Bit angegeben.

Neben der Weiterleitung der Pakete vom Absender zum entsprechenden Empfänger ist es natürlich auch sehr wichtig, die Pakete auf Anwendungsebene zuordnen zu können. Dafür hilft die sogenannte Application layer protocol control information (APCI). Darin ist codiert, ob Informationen angefordert werden, geschrieben/aktualisiert werden sollen, oder ob eine Information zurück geliefert werden muss.

6. Byte								7. Byte								
B7	B6	B5	B4	B3	B2	B1	B0	B7	B6	B5	B4	B3	B2	B1	B0	
0	0	0	0	0	0	B3	B2	B1	B0	D5	D4	D3	D2	D1	D0	
						0	0	0	0	0	0	0	0	0	0	A_GroupValue_Read
						0	0	0	1							A_GroupValue_Response
						0	0	1	0							A_GroupValue_Write
						1	0	1	1	0	0	0	1	0	1	A_UserManufacturerInfo_Read
						1	0	1	1	0	0	0	1	1	0	A_UserManufacturerInfo_Response
						1	1	0	0	0	0	0	0	0	0	A_DeviceDescriptor_Read
						1	1	0	1	0	0	0	0	0	0	A_DeviceDescriptor_Response
						1	1	1	0	0	0	0	0	0	0	A_Restart

Tabelle 2.8: Einige Beispiele für die Belegung der Bits in der APCI von Datentelegrammen (nach [DIN04a]).

Auffällig in Tabelle 2.8 ist, dass die Bits B7 bis B2 des sechsten Bytes eines Standardtelegramms nicht belegt sind. Dies liegt daran, dass sie für weitere Kommunikationsformen wie zum Beispiel Logical Tag Extended Mode (LTE)-Telegramme benötigt werden [SHS17]. Weiterhin sind bei A_GroupValue_Response und A_GroupValue_Write die Bits D5 bis D0 nicht belegt. Diese werden hier zur Codierung nicht benötigt. Sollte die Nutzdatenlast sechs Bit nicht überschreiten, wird sie in den freien Bits des siebten Bytes eingetragen. Ansonsten wird sie ab dem achten Byte übertragen und kann maximal eine Länge von 14 Byte besitzen.

In der Norm sind unterschiedliche sogenannte Datapoint type (DPT) hinterlegt. Diese enthalten folgende Informationen [DIN09]:

- Anzahl und Länge der Datenfelder
- Codierung der zu übermittelnden Informationen
- Wertebereich, der Übertragen werden kann
- Einheit der übertragenen Daten

Benannt werden die DPTs mithilfe einer Haupt- und Unternummer (jeweils 16 Bit Wertebereich). Die Trennung erfolgt durch einen Punkt. Hauptnummern beschreiben Format und Codierung des jeweiligen Typs, während die Unternummer Wertebereich und Einheit spezifiziert. In den Tabellen 2.9 und 2.10 sind zwei Beispiele vorgestellt.

Format:	1 bit: B_1							
Octet-Nummer:	1							
Feld-Namen:								b
Codierung:								B
Wertebereich:	$b = \{0, 1\}$							
Einheit:	Keine							
PDT:	PDT_BINARY_INFORMATION							

Datenpunkt-Typen		
ID	**Name**	**Codierung:** b
1.001	DPT_Switch	$0 = Off$, $1 = On$
1.002	DPT_Bool	$0 = False$, $1 = True$
1.003	DPT_Enable	$0 = Disable$, $1 = On$
...		
1.007	DPT_Step	$0 = Decrease$, $1 = Increase$

Tabelle 2.9: Codierung unterschiedlicher binärer DPTs (nach [DIN09])

Format:	4 bit: B_1U_3							
Octet-Nummer:	1							
Feld-Namen:						Schritt-Wert		
Codierung:					B	U	U	U
Wertebereich:	$c = \{0, 1\}$, Schritt-Wert= $[000_b ... 111_b]$							
Einheit:	Keine							
PDT:	PDT_GENERIC_01							

Datenpunkt-Typen		
Daten-Feld	**Beschreibung**	**Codierung**
c	Erhöhen/Verringern der Helligkeit	Siehe 1.007, $0 = Verringern$, $1 = Erhöhen$
Schritt-Wert	Höhe der Veränderung in einem Bereich von 0 bis 100%, oder Unterbrechung der Änderung	$001_b \ldots 111_b$: Schritte Anzahl der Intervalle = $2^{Schritt-Wert-1}$ 000_b: Abbruch

Tabelle 2.10: DPTs zum Dimmen mit Codierung und Erläuterung zu den Werten (nach [DIN09])

Abfragetelegramm

Das Abfragetelegramm dient dazu, je ein Byte an Information von bis zu 15 anderen Busteilnehmern abzufragen. Das Telegramm wird dabei an eine Gruppenadresse gesendet. Die einzelnen Slaves (Teilnehmer die auf die Anfrage Antworten) haben für die Informationen einen bestimmten Zeitschlitz, in dem diese gesendet werden. Abfragetelegramme werden beispielsweise genutzt um zu prüfen ob bestimmte Teilnehmer noch erreichbar sind [MHH09].

Bestätigungstelegramm

Bestätigungstelegramme werden immer auf Nachrichten von anderen Teilnehmern ausgesendet. Sollten Empfänger in einer anderen Linie liegen, wird der Empfang durch den Koppler bestätigt. Das Bestätigungstelegramm wird auch als Summentelegramm bezeichnet, da es sich durch die Bestätigung der unterschiedlichen Teilnehmer überlagert. Das ist in Tabelle 2.11 zu sehen. Sollte einer der Empfänger beschäftigt sein, wird er für die Bits B1 und B0 jeweils eine „0“ senden, die durch ihre Dominanz die rezessive „1“ überschreibt, sodass der Sender ein „BUSY“ erhält. Bestätigungstelegramme werden 5 Bitzeiten nach dem Empfang des ursprünglichen Telegramms gesendet und besitzen immer ein Byte Nutzdaten, die Bedeutung ist in Tabelle 2.11 gezeigt [SHS17].

B7 N1	B6 N0	B5	B4	B3 b1	B2 b0	B1	B0	
1	1	0	0	1	1	0	0	ACK
1	1	0	0	0	0	0	0	BUSY
0	0	0	0	1	1	0	0	NAK
0	0	0	0	0	0	0	0	NAK + BUSY

Tabelle 2.11: Aufbau des Bestätigungstelegramms bei KNX in Bits mit den unterschiedlichen Bedeutungen (nach [DIN04c]).

Sollte der Sender ein „NACK“ auf sein gesendetes Telegramm erhalten, wird er das Telegramm bis zu drei Mal erneut senden. Um die erneute Verarbeitung für Empfänger zu verhindern, die das Telegramm möglicherweise bereits erfolgreich empfangen haben, wird dabei ein Wiederholungsflag gesetzt, sodass diese Empfänger das Telegramm ignorieren können. Zudem wird das Paket beim Versenden durch das Flag höher priorisiert.

2.2 Zonenkonzept

Dieser Abschnitt beschreibt Möglichkeiten zur Bildung von Zonen innerhalb des Netzes und wie damit eine Erhöhung des Sicherheitslevels erreicht werden kann. Grundsätzlich liefern unterschiedliche Zonen die Möglichkeit, einzelne Segmente des Netzwerkes besser von anderen zu isolieren. Potenziellen Angreifern soll es so erschwert werden nach einem erfolgreichen Einbruch schnell das gesamte Netzwerk zu übernehmen. Weiterhin können Zonen jedoch auch ohne Hinblick auf den Sicherheitsgedanken dazu genutzt werden das Netzwerk logisch zu gliedern und daher übersichtlicher zu gestalten, sowie die Auslastung zu minimieren. Durch eine verkleinerte Broadcast-Domäne verringert sich damit auch die Netzlast.

Das folgende Beispiel soll dies verdeutlichen. Ein Unternehmen hat seine gesamte Infrastruktur in einem gemeinsamen Netzwerk und eine Firewall am Perimeter[1]. Schafft ein Angreifer es diese Firewall, zum Beispiel durch eine Sicherheitslücke, zu überwinden, hat er sofort Zugriff auf alle Teilnehmer im Netzwerk und deren dort angebotene Dienste. Sollten einige Geräte in anderen Subnetzen stehen, die von weiteren Firewalls getrennt sind, wäre zusätzlicher Aufwand zur Überwindung dieser Firewalls nötig. Dies würde den Angreifer aufgrund der reduzierten Zugangsmöglichkeiten deutlich aufhalten beziehungsweise eventuell sogar komplett stoppen.

2.2.1 Aufbau eines Zonenkonzeptes im IP-basierten Umfeld

Definition 3 beschreibt eine Sicherheitszone genauer. Grundsätzlich geht es bei der Bildung von Zonen darum Systeme zu einem Netzsegment zusammenzufassen, welche bezüglich der Sensitivität der darauf gespeicherten oder verarbeiteten Informationen und des Risikos angegriffen zu werden ähnlich sind [Nor05].

Definition 3. *Eine Sicherheitszone ist eine logische Gruppierung von Ressourcen wie Systemen, Netzwerken oder Prozessen welche sich in Bezug auf das akzeptable Risiko ähneln [Nor05].*

Nach der Definition würde es sich daher beispielsweise anbieten einen Webserver, einen Public-DNS-Server und einen Mail-Relay-Server in einer Zone zu gliedern.

[1] Außengrenze zu weiteren externen Netzwerken (z. B. Internet)

Der DNS-Server für interne Einträge und der Mail-Server, welcher die Mails an die entsprechenden Nutzer zustellt, sollten jedoch in einem internen Server-Bereich liegen und durch weitere Firewalls geschützt sein. Diese Systeme müssen nicht aus dem Internet erreichbar sein und sollten aufgrund der sensibleren Informationen besser geschützt werden, da die Schadwirkung Angriffs hier höher ist [Nor05]. Zusätzlich sollte auch für jeden Dienst eine eigene Serverinstanz genutzt werden. Sollte es einem Angreifer gelingen einen Dienst erfolgreich zu übernehmen, kann er eventuell Systemrechte gewinnen und damit alle auf dem System verwendeten Dienste übernehmen. Dies lässt sich durch die Nutzung unterschiedlicher Server für unterschiedliche Dienste erschweren. Zusätzlich sollte beim Aufteilen eines Dienstes auf mehrere Server und Zonen im Idealfall auch unterschiedliche Software genutzt werden, um die Angreifbarkeit weiter zu minimieren. Durch die Trennung der Services auf unterschiedliche Server steigt zudem die Ausfallsicherheit der einzelnen Dienste. Sollte ein Server ausfallen, sind nicht gleich mehrere Dienste betroffen. Allerdings steigt mit der Anzahl der verwendeten Server- und Softwareprodukte auch der Monitoring- und Wartungsaufwand sowie die finanzielle Belastung für das Unternehmen.

Durch eine stärkere Gliederung des Netzwerks in kleinere Teile verkleinert sich zugleich die Broadcast-Domäne, was zu einer Entlastung des Netzes führt. Die Segmentierung wirkt sich also durchaus nicht nur in Bezug auf Sicherheitsaspekte positiv auf die Infrastruktur aus.

Bezüglich Client-Systemen wird im besten Fall auch eine Trennung in unterschiedliche Netzsegmente vorgenommen. Verkabelte Clients sind in der Regel stationär und lassen sich deutlich besser überwachen, was zum Beispiel das aktuelle Patch-Level angeht. Kabellos eingebundene Endgeräte hingegen sind in dieser Hinsicht deutlich schwieriger zu überwachen und sollten daher auch in einer extra Zone eingegliedert werden [Nor05].

Grundsätzlich kann an allen Zonenübergängen der Netzverkehr überwacht und eingeschränkt werden. Dies wird in der Regel durch Firewalls und Router realisiert. Diese Geräte bestimmen, welcher Teilnehmer wie mit anderen kommunizieren darf. Eine feinere Netzstruktur führt daher auch zu einer besseren Steuerungs- und Kontrollmöglichkeit der Datenströme.

2.2.2 Zonenkonzept nach dem IT-Grundschutz des BSI

Das Bundesamt für Sicherheit in der Informationstechnik stellt mit dem IT-Grundschutz-Katalog eine Sammlung an zu prüfenden Sicherheitsrisiken und entsprechenden Maßnahmen dagegen vor [Bun16]. Eine dieser Maßnahmen (M4.449) beschreibt die Einführung eines Zonenkonzeptes.

Unterschiedliche Komponenten im Netzwerk sollten danach in Zonen eingeteilt werden, welche wiederum durch eigenständige Sicherungsmaßnahmen geschützt sind. Auf diese Art und Weise lässt sich für jede Komponente ein optimales Level an Sicherheit erreichen. Sollte es einem Angreifer gelingen ins System einzudringen, so ist es deutlich schwerer auf alle Netzkomponenten Zugriff zu erlangen, wenn diese in Zonen eingeteilt sind. Bei der Erstellung muss natürlich beachtet werden, ob und wenn ja welche Kommunikation zwischen den Zonen nötig ist, um die Sicherungsmaßnahmen an den Übergängen so scharf wie irgend möglich einstellen zu können. Typischerweise werden die Sicherheitszonen nach folgenden Punkten unterschieden [Bun16]:

- Eigentümer der Prozesse und Daten
- Schutzbedarf der Informationsobjekte
- Benutzergruppen und Komponenten mit Zugriffsrecht auf Informationsobjekte
- Bedrohungen
- Sicherheitsmaßnahmen

2.2.3 Zonenkonzept für KNX

In KNX gibt es durch die Vergabe der Adressen und der Anzahl an Teilnehmern pro Linien schon aus organisatorischer Sicht die Notwendigkeit das Netzwerk in Zonen einzuteilen. Zur Adressierung und logischen Strukturierung ist im vorherigen Absatz (siehe 2.1.2) eine Möglichkeit beschrieben.

Bei dieser Art von Zonenbildung werden allerdings hauptsächlich die Nutzung von möglichst wenig Kabel und die wirtschaftlichen Aspekte zur Grundlage der Bildung der Zonen herangezogen, nicht jedoch eventuelle Sicherheitsbedenken. Zusätzlich ist

die Bildung von Zonen interessant, um die Auslastung der Segmente zu reduzieren, da bei weniger Teilnehmern der Broadcastverkehr reduziert wird. Der reduzierte Telegrammverkehr sorgt weiterhin dafür, dass das unerlaubte Mitschneiden auf dem Bus weniger Informationsgewinn erlaubt.

Durch geschickte Einteilung der Bereiche, Linien und Geräte-Adressen kann unter Umständen Kabel gespart werden, was natürlich auch den Arbeitsaufwand zum Verlegen reduziert und damit die Anschaffungskosten minimiert. Allerdings ist zu prüfen, inwieweit eine einfache Erweiterung der Anlage vorgesehen sein sollte und umsetzbar ist.

2.3 Netflow

In diesem Abschnitt wird die Netflow-Technik generell vorgestellt. Sie soll zur Überwachung des Netz- oder Busverkehrs genutzt werden. Die aggregierten Daten können dabei auf Anomalien untersucht werden und bieten damit eine Möglichkeit Angriffe oder Fehler festzustellen. Dabei wird an dieser Stelle von Netflows in IP-Netzwerken ausgegangen und nicht von Bus-Netzwerken. In Kapitel 5 wird allerdings die Verbindung zu KNX und damit zu den Bus-Netzen geschlossen.

Ein Flow in Bezug auf Netzwerke ist laut [QZCZ04] folgendermaßen definiert:

Definition 4. *Ein Flow wird definiert als eine Menge von IP-Paketen, die einen Observationspunkt in einem Netzwerk während eines definierten Zeitintervalls traversieren. Alle Pakete, die zu einem bestimmten Flow gehören, haben eine Menge gemeinsamer Eigenschaften. Jede Eigenschaft ist dabei das Ergebnis der Anwendung einer Funktion auf die folgenden Werte:*

1. *Ein oder mehrere Paket-Header-Felder (z.B.: IP-Adresse), Transport-Header-Felder (z.B.: Ziel-Port-Nummer), oder Anwendungs-Header-Felder (z.B.: RTP Header-Felder)*
2. *Eine oder mehrere Charakteristiken des Pakets selbst (z.B.: Nummer, MPLS-Label, ...)*
3. *Eines oder mehrere Felder, welche von der Paketverwaltung abgeleitet werden können (z.B.: Next Hop IP-Adresse, Ausgabe-Interface, ...)*

Ein Paket wird einem Flow zugeordnet, wenn es alle Eigenschaften des entsprechenden Flows erfüllt.

Es ist daher möglich Flows zu erfassen, die nicht über eine Transmission Control Protocol (TCP)-Verbindung arbeiten, sondern zum Beispiel nur User Datagram Protocol (UDP) nutzen [SSS+10].

2.3.1 Flow Monitoring

Grundsätzlich sind Flow Monitoring Systeme von der Architektur immer ähnlich aufgebaut. Es werden dabei mehrere Stufen unterschieden [HCT+14]:

1. Mitschnitt von Paketen
2. Erstellung von Flows und Export
3. Datensammlung
4. Datenanalyse

Die einzelnen Schritte werden im Folgenden jeweils separat betrachtet.

2.3.2 Mitschnitt von Paketen

Für den Mitschnitt müssen vorab bestimmte Beobachtungspunkte festgelegt werden, an denen der Datenverkehr überwacht werden soll. Diese sollten in der Regel an strategisch günstigen Punkten angebracht sein. Welche Punkte genau gewählt werden, hängt von den zu sammelnden Informationen ab. Häufig sind hierbei Netzgrenzen oder auch Zonengrenzen sinnvoll. Dazu gehört selbstverständlich auch der Übergangspunkt zwischen Netzwerkperimeter und internem Netz. In Abbildung 2.2 sind die entsprechenden Sensoren, die ausgebracht werden sollten, um alle Broadcast-Domänen zu überwachen, rot markiert.

Ein solcher Beobachtungspunkt wird auch als Observationspunkt bezeichnet. Dies können daher Router, Ports, oder auch einzelne Interfaces sein. Ein Observationspunkt kann dabei auch wieder mehrere Obervationspunkte enthalten [QZCZ04]. Grundsätzlich können die genutzten Geräte zur Überwachung des Netzverkehrs in folgenden Kategorien eingeteilt werden [HCT+14]:

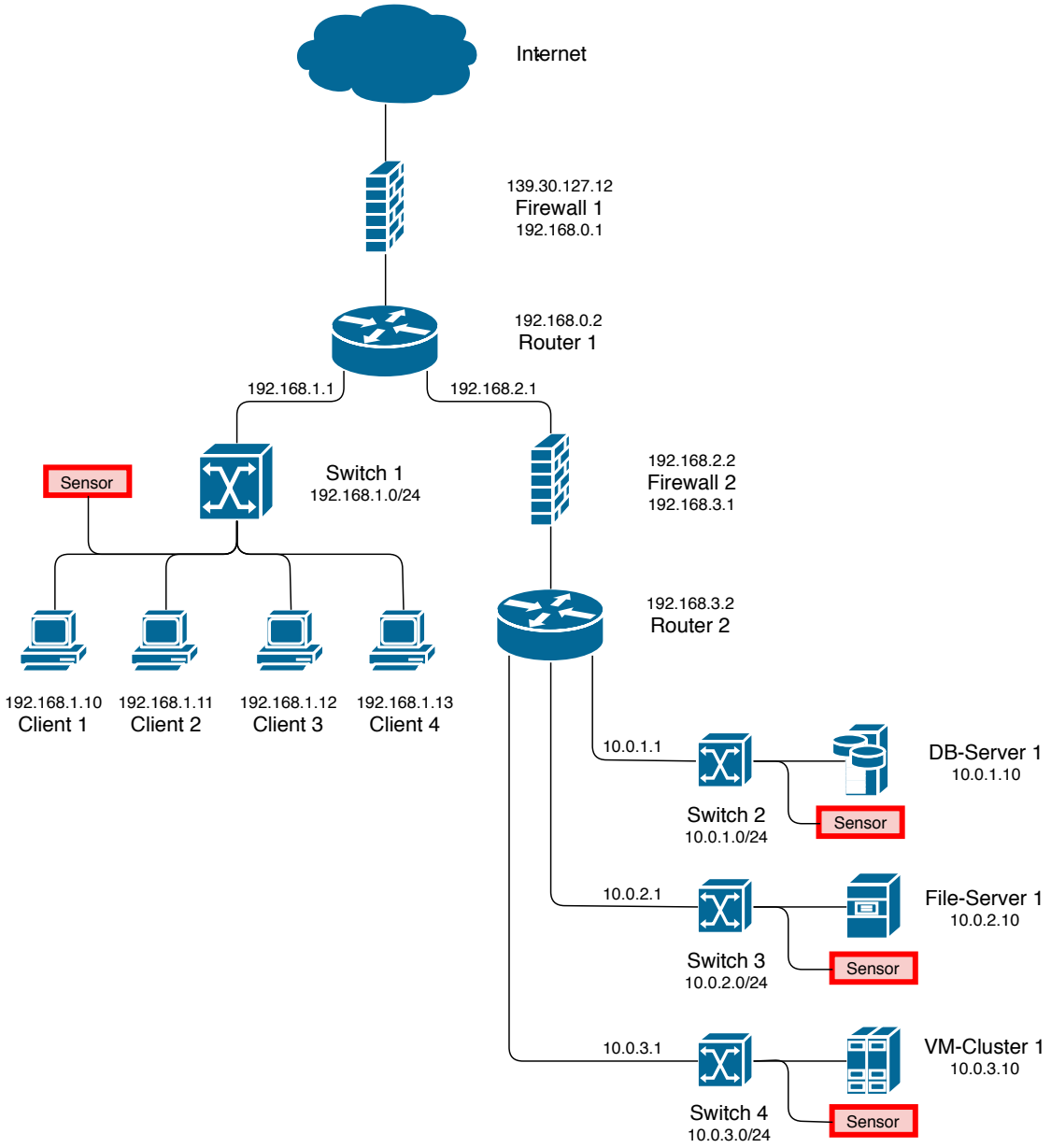

Abbildung 2.2: Beispielhafter Netzplan mit Segmentierung in unterschiedliche Netze und mehreren Firewalls

- In-Line-Modus: Das Gerät zum Mitschnitt ist direkt mit der physikalischen Leitung verbunden und kann ausgetauscht oder abgeschaltet werden, ohne dass die Datenverbindung unterbrochen wird.
- Mirror-Modus: Das Gerät, durch welches der Datenverkehr geleitet wird, gibt diesen auf einem anderen Interface oder Port gespiegelt aus. Hierdurch kann es allerdings zu Verzögerungen oder auch zusätzlichem Jitter kommen, was eventuelle Analysen verfälschen kann.

In Abbildung 2.3 ist gezeigt, welche Schritte beim Sammeln der Pakete durchlaufen werden. Zuerst werden die Paket-Header gelesen und die beobachteten Pakete mit Zeitstempeln versehen. Im weiteren werden die Pakete vor allem verkürzt und gefiltert. Die Nutzlast der Pakete findet bei der Flow Analyse in der Regel keine Beachtung und wird nicht weiter betrachtet [HCT+14]. Dies führt zu einer starken Einsparung an zu analysierenden Daten. Zusätzlich können im Schritt der Filterung/Klassifizierung Pakete herausgefiltert werden, welche für die Analyse uninteressant sind.

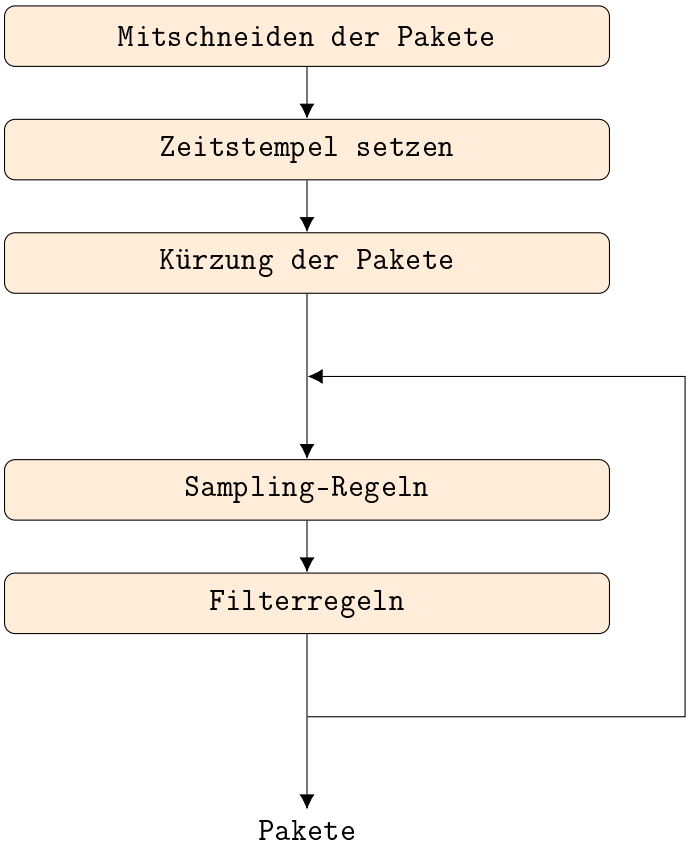

Abbildung 2.3: Funktionsweise des Mitschnitts von Paketen nach [HCT+14]

Der Sinn der Regeln für das Sampling von Paketen und der Filterregeln liegt darin, möglichst viele uninteressante Informationen vor der Verarbeitung auszusortieren und somit weniger Daten weiterverarbeiten zu müssen. Beim Sampling wird entschieden, ob alle Pakete betrachtet werden, oder ob nur ein Teil analysiert wird. Sobald nicht mehr alle Pakete betrachtet werden, gibt es grundsätzlich zwei unterschiedliche Strategien zur Möglichkeit der Wahl der Pakete. Zum einen kann die Auswahl der zu analysierenden Pakete zufällig erfolgen, oder es kann ein deterministischer Algorithmus gewählt werden - im einfachsten Fall wird jedes n-te Paket betrachtet. Der zufällige Mechanismus bietet den Vorteil, dass mit diesem auch regelmäßig auftretende Pakete erfasst werden. Bei deterministischen Algorithmen kann dies deutlich leichter fehlschlagen und regelmäßig auftretende Pakete werden eventuell nie erfasst [HCT+14].

2.3.3 Erstellung von Flows und Export

Die Pakete, die einen Observationspunkt traversieren, werden im Metering-Prozess bewertet und zu Flow-Records zusammengefasst. Flow-Records beinhalten detaillierte Informationen zu einem konkreten Flow und dessen Parametern. Dabei werden die Paket-Header und auch das weitere Vorgehen mit dem Paket betrachtet. Wenn neue Pakete mit dem entsprechenden Schlüssel für einen bereits bestehenden Flow gesammelt werden, muss der Flow aktualisiert werden. Sollte der Schlüssel noch nicht existieren, wird ein neuer Flow angelegt. Folgende Aktionen können durchgeführt werden [QZCZ04]:

- Hinzufügen neuer Flow-Records
- Aktualisierung der bestehenden Flow-Records
- Berechnung von Flow-Statistiken
- Detektion von abgelaufenen Flows
- Ableitung weiterer Flow-Eigenschaften
- Übergabe von Flow-Records zum Export-Prozess
- Löschung von Flow-Records

Die zusammengefassten Flow-Daten werden vor dem Export in entsprechenden Caches zwischengespeichert. Folgende Situationen können dazu führen, dass ein Cache Eintrag gelöscht wird [HCT+14]:

- Aktiver Timeout (Flow ist schon sehr lange aktiv - durch Timeout wird Zwischenstand exportiert)
- Idle Timeout (Es wurden keine aktiven Pakete für einen Flow über eine gewisse Zeit beobachtet.)
- Ressourcen Probleme (Es ist möglich spezielle Parameter zu beobachten und Timeouts zur Laufzeit zu verändern, um spezielle Ressourcenanforderungen zu erfüllen.)
- Natürliche Beendigung eines Flows (Empfang eines FIN oder RST Flags in einem TCP-Paket beendet den zugehörigen Flow.)

Zu den Timeouts kann gesagt werden, dass grundsätzlich längere Zeiten wünschenswert sind, da dies zu einer höheren Verdichtung der Daten führt und so das Netz mit weniger Exports belastet wird. Auf der anderen Seite dauert es aber auch länger, bis entsprechende Flows sichtbar werden. Daher muss abgewogen werden, worauf die Prioritäten liegen, oder ob eventuell mit einem entsprechenden Rahmen an Variabilität der Timeout-Zeit dieser dynamisch je nach Netzauslastung festgelegt werden kann.

Sobald die Flows zusammengefasst wurden, können diese erneut gefiltert werden. Hierbei kann neben dem Prüfen auf einzelne Attribute auch ein Prüfen mit Hilfe von Hash-Werten eingesetzt werden. Dabei wird ein Hash über gewissen Attributwerten erstellt und geprüft, ob dieser in einem entsprechend gültigen Wertebereich liegt [HCT+14]. Der Export-Prozess läuft dabei auf jedem Observationspunkt und leitet die Daten an einen Kollektor weiter. Bei diesem können die entsprechenden Records gespeichert oder auch weiter verarbeitet werden [QZCZ04].

2.3.4 Datensammlung

Die Sammlung der exportierten Flow-Daten wird vom sogenannten Flow-Collector übernommen. Die Exports können auch an mehreren Stellen im Netzwerk gesammelt werden. Im Collector-Prozess werden die Daten vor der endgültigen Analyse weiter angepasst. Dazu kann beispielsweise eine Anonymisierung der Werte gehören. Andererseits kann auch hier weiter gefiltert werden oder Daten können zusammengefasst und so weiter verdichtet werden [HCT+14].

Eine grundsätzliche Frage bildet an dieser Stelle die Speicherung der Flows. Es ist zu entscheiden, welche Art von Speichermedium verwendet werden soll. Neben persistentem Speicher für die längere Aufbewahrung der Daten zu Vergleichszwecken kann der Einsatz von volatilem, aber in der Regel deutlich schnellerem, Speicher bei besonderen Performance-Ansprüchen sinnvoll sein. Weiterhin muss die Art der Speicherung entschieden werden. Dabei lassen sich grundsätzlich folgende Arten unterscheiden [HCT+14]:

- Dateien - Schnelles Schreiben/Lesen von Einträgen in einfachen Dateien, allerdings sind die Möglichkeiten der Anfragen stark begrenzt.
- Zeilen basierte Datenbanken - „Klassische“ Datenbanken wie zum Beispiel MySQL - hier liegt das Problem darin, dass immer eine ganze Zeile zur Analyse eingelesen werden muss.
- Spalten basierte Datenbanken - Beispielsweise FastBit - Vorteil liegt im Zugriff, da nur die für die Analyse notwendigen Attribute gelesen werden.

Neben der Zugriffsgeschwindigkeit sollte vor einer entsprechenden Auswahl festgelegt werden, wie komplex die zu formulierenden Anfragen sind und auch ob es bestimmte Anforderungen an den zu Verfügung stehenden Speicherplatz gibt.

2.3.5 Datenanalyse

Die Datenanalyse ist der letzte Schritt in der Verarbeitung der Flows. Hierbei kann besonderer Wert auf folgende drei Punkte gelegt werden [HCT+14]:

1. Flow Analyse und Erstellung von Berichten
2. Erkennung von Gefährdungen
3. Analyse von Diensten

Punkt eins gibt einen besonders guten Überblick über die Netzsituation. Es ist möglich abzuschätzen, zu welchen Zeiten welche Lastszenarien auftreten, beziehungsweise welche Hosts beispielsweise besonders viel Traffic generieren. Damit kann zum Beispiel dafür gesorgt werden, die Auslastung von bestimmten Netzsegmenten gezielt zu reduzieren oder Engpässe zu beseitigen. Diese Analyse der Flows und auch die Berichterstattung und das Absetzen von Alarmen sind Fähigkeiten, die jedes Flow Monitoring Setup bieten sollte [HCT+14].

Es ist allerdings auch möglich anhand der Flows bestimmte Angriffe mehr oder weniger gut zu detektieren. Besonders gut funktioniert dies bei Distributed Denial of Service (DDoS)-Attacken, Netzwerk-Scans, der Verteilung von Würmern oder Botnet-Kommunikation [HCT+14]. Durch den zusätzlichen Einsatz von Listen, auf denen die „Vertraulichkeit“ von IP-Adressen aufgeführt wird, oder auch durch den Einsatz von IP-Blacklists ist es damit möglich einige Angriffe nicht nur zu detektieren, sondern auch entsprechende Aktivitäten zu unterbinden.

Netflows können weiterhin für die Analyse des Status von Diensten genutzt werden. Es ist beispielsweise möglich, mit einem regelmäßigen Request eine Ressource bei einem Webserver anzufragen, und dann den Flow mit der entsprechenden Antwort zu analysieren. Somit lässt sich ohne administrativen Zugriff auf den Webserver feststellen, ob dieser die entsprechenden Anfragen beantwortet und wie schnell.

2.3.6 Nutzung von Netflows

Netflows unterstützen bei der Analyse der Netzauslastung, Quality of Service (QoS), Überwachung oder auch Angriffserkennung. Bezüglich der Netzsicherheit helfen Netflows nicht nur bei der Detektion von Angriffen, sondern können auch bei der Wahl entsprechender Verteidigungsmaßnahmen hilfreich sein [QZCZ04].

2.4 Stand der Technik

Dieser Abschnitt soll kurz die bereits möglichen Sicherheitsfeatures unter KNX Version 2.1 beschreiben (nach [SHS17]). Auch bei der KNX Association wurde das Sicherheitsproblem erkannt und ab KNX Version 2.1 wurden besonders neue Sicherheitsfeatures eingeführt. Diese werden von Geräten mit Systemprofilen zwei, sieben, sowie B unterstützt. Die Systemprofiltypen können als Generationen von Geräten betrachtet werden.

Generation eins wurden weiter zu Generation zwei und sieben entwickelt. System sieben wurde anschließend wieder weiter zu System B entwickelt [KNX]. Die Generationen drei bis sechs sind nicht vorhanden. Die Schaffung von neuen Sicherheitsfeatures liegt vor allem auch darin begründet, dass neben dem klassischen Medium Twisted Pair mit RF (Radio Frequency) auch ein Medium unterstützt

wird, welches kabellos arbeitet und damit besonders gegen Manipulationen gesichert werden muss [SHS17].

Mit den neuen Sicherheitsfeatures sollen vor allem die folgenden Schutzziele erreicht werden [SHS17]:

- Vertraulichkeit
- Integrität
- temporäre Unversehrtheit

Die Features sind ab Engineering Tool Software (ETS)-Version 5.5 verfügbar. Umgesetzt werden die Maßnahmen auf dem Bus mittels dem sogenannten „KNX Data Security“. Damit ist es möglich Telegramme nicht nur zu authentisieren, sondern auch eine symmetrische Verschlüsselung zu nutzen. Die Verschlüsselung erfolgt auf der Anwendungsschicht. Während der Projekterstellung wird ein Schlüssel in der ETS festgelegt. Die Software erzeugt projektspezifische Werkzeugschlüssel, die anschließend auf Geräte übertragen werden. Dabei wird der Schlüssel zu keiner Zeit im Klartext über den Bus gesendet, sondern mittels eines gerätespezifischen „Factory Device Set up Keys“, welchen alle Geräte von Werk aus besitzen und welcher während der Planung in die ETS-Software eingegeben wird, verschlüsselt. Nach diesem Schritt wird von dem Gerät nur noch dieser Werkzeugschlüssel zur Kommunikation akzeptiert. Während der Projektierung werden zudem Laufzeitschlüssel von der ETS erzeugt, die die Kommunikation im Betrieb verschlüsseln. Diese werden durch den Werkzeugschlüssel verschlüsselt auf die Geräte übertragen [SHS17].

Die hier vorgestellten Mechanismen verbessern das Konzept von KNX in Hinsicht auf die Sicherheit deutlich. Nur durch den konsequenten Einsatz von Authentisierung und Verschlüsselung ist es möglich, die oben genannten Schutzziele überhaupt erreichen zu können. Die in dieser Arbeit vorgestellten Maßnahmen dienen dazu das höchst unsichere Konzept von KNX ohne Neuanschaffungen so zu überarbeiten, dass zumindest ein Mindestmaß an Sicherheit garantiert werden kann.

Neben den Sicherheitsmechanismen bei KNX gibt es auch bereits entsprechende Vorgehensweise bei der Erstellung von Netzwerkzonen unter Berücksichtigung der Sicherheit und auch die Umsetzung von Risikoanalysen ist bereits standardisiert. Die Konzepte dafür wurden jedoch ausschließlich für die IP-basierte Welt entwickelt

und müssen für den Einsatz bei Bussystem entsprechend adaptiert werden. Das Konzept der Zonenbildung wurde bereits in Kapitel 2.2 näher beschrieben, während die Risikoanalyse nach BSI-Standard 200-3 ([BSI17]) in Kapitel 4.1 näher betrachtet wird.

Kapitel 3

Angriffe auf Gebäudeautomationsnetze

Gebäudeautomationsnetze sind in der Regel in unterschiedliche Bereiche gegliedert. Neben der Feldebene, an der die einzelnen Sensoren und Aktoren direkt angeschlossen sind, befindet sich darüber noch eine Automations- und Managementschicht. Während die Netzwerke zur Automation der Steuerung von Gebäudetechnik zu Beginn noch galvanisch, sprich via Air Gap, von globalen Netzen wie dem Internet getrennt waren, hat sich dies in der heutigen Zeit drastisch geändert. Vor allem die Managementschicht ist in der Regel mit dem Internet verbunden, um komfortabler auf Systeme zugreifen zu können. Auch einige Komponenten in der Automationsschicht verfügen teilweise über Verbindungen zu externen Netzwerken. Häufig wird dies genutzt, um herstellerseitig den Support zu vereinfachen [MW16]. Dies führt allerdings zu der Situation, dass die Kunden der Systeme selbst nicht genau wissen, an welchen Stellen eventuelle Zugänge eingerichtet sind [MW16].

Dieses Kapitel soll einen Überblick über mögliche Angriffsvektoren liefern und diese klassifizieren. Aufgrund der hier beschriebenen Szenarien soll im späteren Verlauf geprüft werden, ob und inwieweit die entwickelten Techniken Angriffe vereiteln können.

3.1 Sicherheitsansprüche

Vor der Betrachtung der eigentlichen Angriffe soll zunächst festgehalten werden, welche relevanten Sicherheitsansprüche existieren. Daraus lässt sich anschließend ableiten, welche Angriffe besondere Bedrohungen darstellen.

Grundsätzlich sollten die Daten auf einem sicheren Weg versendet werden und der Zugriff auf Managementkomponenten darf nur autorisierten Benutzern genehmigt werden. Für den sicheren Versand der Daten ist es wichtig, dass diese vertraulich, integer und auch nicht verzögert zugestellt werden [GKNP06]. Weiterhin sollte es nach Möglichkeit einen Update-Mechanismus geben und das System sollte skalierbar aufgebaut sein, um die Erweiterbarkeit später zu vereinfachen. Durch die Schaffung der Update-Möglichkeit ist ein Betrieb über mehrere Jahrzehnte einfacher möglich, da auf diesem Weg potenzielle Fehler beseitigt werden können. Gerade weil Komponenten in diesem Bereich besonders lange Zeit eingesetzt werden, sollte für ein Sicherheitskonzept auch die Kompatibilität mit bestehenden Installationen im Auge behalten werden [GKNP06].

3.2 Klassifikation von Angriffen

Angriffe gegen Gebäudeautomationssysteme können unterschiedlich klassifiziert werden. Folgende Einteilungsmöglichkeiten sollen kurz vorgestellt werden:

1. Klassifikation nach benötigtem Vorwissen
2. Klassifikation nach Ort der Ausführung
3. Klassifikation nach Schadwirkung
4. Klassifikation nach Detektierbarkeit

Im Weiteren wird die Einteilung nach dem benötigten Vorwissen besonders genau betrachtet. Eine ausführliche und genaue Betrachtung aller Optionen würde den Rahmen der Arbeit überschreiten. Trotz dessen soll eine Idee gegeben werden, welche weiteren Klassifizierungen möglich sind.

3.2.1 Klassifikation nach Vorwissen

In Abbildung 3.1 ist eine Gliederung von Angriffen gegen Gebäudeautomationssysteme nach unterschiedlichem benötigtem Vorwissen gezeigt. Eine Darstellung als Angriffsbaum ermöglicht hierbei einen schnellen Überblick über die Einteilung. Je nach Angriff braucht die ausführende Person mehr oder weniger viel Vorwissen, um die entsprechenden Maßnahmen durchführen zu können. Die Einteilung in keine Vorkenntnisse, Basiswissen und hohes Vorwissen soll die Möglichkeit geben, die Gefahr von Angriffen besser bewerten zu können. Sollte ein Angriff ohne Vorwissen beispielsweise kritische Infrastruktur einfach lahmlegen können, so wäre diese besonders kritisch.

Sehr einfache Angriffe stellen zum Beispiel das Mitschneiden von Netzverkehr, die Wiederholung von bereits gesendetem Verkehr oder auch ein Denial-of-Service-Angriff auf einem gesamten Netzsegment dar. Für alle diese Angriffe ist allerdings physikalischer Zugang zum Bus nötig. Ein Denial of Service (DoS)-Angriff kann durch einen Kurzschluss der Datenleitung des Busses hergestellt werden und wird das komplette Segment lahmlegen. Für das Mitschneiden und Senden von Telegrammen wird auch ein Zugang zum Netz benötigt. Im einfachsten Fall wird dafür ein physikalischer Zugang genutzt. Dies könnte zum Beispiel ein Lichtschalter oder ein Bewegungssensor sein. Eine weitere Möglichkeit wäre allerdings ein KNX-IP-Gateway unter seine Kontrolle zu bringen und darüber Telegramme zu versenden. Dies wiederum erfordert deutlich höhere Kenntnisse.

Mit Hilfe von Basiskenntnissen kann der Angreifer bereits gezieltere Angriffe durchführen. Neben der Flutung des Busses mit Nachrichten ist es auch möglich, einzelne Teilnehmer gezielt lahm zu legen. Eine Möglichkeit dafür wird in Abschnitt 3.3.2 genauer vorgestellt. Mit gewissen Basiskenntnissen ist es zudem möglich, ein Bussegment zu explorieren und verbaute Geräte zu finden oder zu bestimmen. Dies kann je nach Einstellung der Linienkoppler auch über die Grenzen einzelner Segmente hinweg erfolgen. Ein hilfreiches Tool hierfür ist KNXmap (`https://github.com/takeshixx/knxmap` - siehe Abbildung 5.2 und 5.3).

Hohes Vorwissen ermöglicht komplexe Angriffe, die über die bloße Störung vom Gebäudeautomationssystem hinausreichen. Durch das Einfügen von Nachrichten können zum Beispiel bestimmte Parameter im Gebäude verändert werden. Es lassen

sich dabei alle verbundenen Geräte manipulieren. Neben Licht kann so beispielsweise auch die Heizung oder Verdunklung geregelt werden. Durch Man-in-the-Middle-Angriffe oder die Modifikation von Nachrichten können Vorgänge so manipuliert werden, dass Aktionen von Benutzern auf einmal andere Ereignisse auslösen als erwartet. Auch eine Neu- oder Umkonfiguration von Geräten zur Laufzeit ist denkbar. Einem Angreifer wäre es damit möglich bestimmte Aktionen zu blockieren und nur gezielt wenige Aktionen zuzulassen. Damit ist es auch möglich menschliches Verhalten zu manipulieren und somit Ereignisse zu erreichen, die mit dem klassischen Gebäudeautomationssystem nicht gesteuert werden können. In einem weiteren Schritt wäre es möglich durch genaue Kenntnis der Reparatur- oder Austauschprozesse Geräte austauschen zu lassen und somit auch hardwareseitig manipulierte Komponenten in das System einzuschleusen.

Abbildung 3.1: Einteilung möglicher Angriffe gegen Gebäudeautomationssysteme auf Busebene nach benötigtem Vorwissen

3.2.2 Weitere Klassifikationen

Bei der Betrachtung des Ortes ist es besonders interessant, ob ein Angreifer lokal vor Ort sein muss, um in das System eingreifen zu können, oder ob er dies auch in Ruhe von einem entfernten Arbeitsplatz kann. Zusätzlich ist zu betrachten, ob von einem Liniensegment oder Zugriffspunkt aus das gesamte Netz erreicht werden kann, oder ob ein Teil der Komponenten beispielsweise nur durch Buszugang in zugangsbeschränkten Bereichen erreicht werden kann.

Die Schadwirkung ist besonders interessant, um ein mögliches Risiko eines Angriffs einschätzen zu können. Allerdings ist die Klassifikation besonders schwer möglich. Betrachtet werden kann, ob nur einzelne Komponenten lahmgelegt werden oder gleich ganze Gruppen. Trotzdem ist es auch möglich mit einzelnen Komponenten, wie zum Beispiel Heizung oder Klimaanlage, ein gesamtes Gebäude nicht weiter nutzbar zu machen. Ein Angriff ohne direkt spürbare physische Auswirkungen kann ebenfalls eine hohe Schadwirkung haben. Das Mitschneiden von Netzverkehr und die anschließende Analyse der Daten kann beispielsweise zur Erstellung von Bewegungsprofilen genutzt werden, was ebenfalls zu einem beträchtlichen Schaden führen kann.

Weiterhin wurde die Klassifikation nach der Detektierbarkeit angesprochen (siehe 3.2). Hierbei ist zu beachten, dass es kaum möglich ist Angriffe festzustellen, die ohne Aussendung von Telegrammen auskommen. Das bloße Lauschen am Bus ist für andere Teilnehmer nicht feststellbar. Erst durch die Einbringung von Telegrammen kann es sein, dass zum Beispiel bei doppelt auftretenden Adressen oder neuen Absenderadressen ein Angriff sicher feststellbar ist.

3.3 Angriffe im Detail

Für die im weiteren Verlauf des Kapitels vorgestellten Angriffe können unterschiedliche Tools eingesetzt werden. Als eine bereits existierende Sammlung an Funktionen, die für einen Angreifer interessant sind, bietet sich KNXmap (`https://github.com/takeshixx/knxmap` - siehe Abbildungen 5.2 und 5.3) an. Die Programmiersoftware ETS vom Hersteller kann ebenfalls sehr gut für das Mitlesen und Einbringen von Telegrammen auf dem Bus genutzt werden, allerdings wird ab fünf Geräten eine bezahlte Lizenz benötigt, um ein derartiges Projekt öffnen zu können.

3.3.1 Mitschneiden von Netzwerkverkehr

Das Mitschneiden von Telegrammen auf dem Bus ist eine sehr einfache Art des Angriffs. Es ist dabei grundsätzlich kein Vorwissen nötig, lediglich ein Zugang zum Bus wird benötigt. Dieser ist zum Beispiel in Toiletten einfach zu erreichen, da hier keine Kamera-Überwachung eingesetzt werden darf, kann ein Angreifer ohne zu großen Zeitdruck und ohne die Möglichkeit gefilmt zu werden ein Gerät zum Mitschneiden von Daten anbringen. Anschließend kann über ein Gateway an diesem der gesamte Datenverkehr mitgeschnitten und auch mitgelesen werden, da üblicherweise keinerlei Verschlüsselung eingesetzt wird.

Mitgeschnittener Datenverkehr kann gesammelt und danach analysiert werden. Durch das Design des Busses, ist es dem Angreifer möglich unbemerkt Daten zu sammeln. Lesende Teilnehmer benötigen auf dem Bus keine physikalische Adresse, da sie einfach den Spannungsverlauf überwachen müssen. Solange also keine Telegramme gesendet werden, bleibt der Teilnehmer unentdeckt und kann zum Beispiel einen komplexeren Angriff planen. Hierzu können die gesammelten Daten ausgewertet werden und durch statistische Berechnungen Bewegungsprofile von Mitarbeitern oder Ähnliches erstellt werden. [MDS14]. Dazu können beispielsweise die Informationen der Schalter und Bewegungsmelder genutzt werden.

Zu beachten ist allerdings, dass je nach Konfiguration der Linien und Bereiche, sowie der Koppler zwischen diesen nur ein Teil der Telegramme mitgelesen werden kann. Je nach Einstellung ist eine starke Filterung der Pakete zu erwarten und damit nur noch ein Teil an Informationen. Dies kann unter Umständen dazu führen, dass keine komplexeren Bewegungsprofile mehr erstellt werden können.

Auch wenn der Angriff grundsätzlich einfach ausführbar ist, kann man mit den Rohdaten noch nicht sofort weiter arbeiten. Durch die numerischen Adressen gilt es zuerst herauszufinden, welche Adresse zu welcher Art von Gerät gehört. Erschwerend kommt für den Angreifer hinzu, dass die reguläre Kommunikation über Gruppenadressen abgewickelt wird, was im IP-Umfeld dem Konzept von Multicasts entspricht. Dadurch ist die Adresse von empfangenden Teilnehmern beispielsweise nie ersichtlich, da diese nur unter einer bestimmten Adresse lauschen. Der Angreifer müsste daher zum Beispiel sehr genau den zeitlichen Zusammenhang zwischen Bustelegrammen und ausgeführten Aktionen durch die Aktoren kennen oder weiter-

gehende Informationen vorliegen haben, um einfach mit den Daten weiterarbeiten zu können.

3.3.2 Denial of Service-Angriff mit Hilfe des A_Restart-Service

Der A_Restart-Service ist ein Service-Request, der vom Nutzer auf Application-Layer-Ebene gesendet werden kann, um den Neustart des Kommunikations-Controllers eines Gerätes auszulösen [DIN04a]. Die Idee bei diesem Angriff besteht darin, den Teilnehmer durch ein entsprechendes Telegramm neu starten zu lassen, und ihn somit für eine Weile an der aktiven Kommunikation zu hindern. Der Angriff kann durch häufige Hintereinanderausführung genutzt werden einen Teilnehmer beliebig lang zu blockieren. Damit wird ein DoS Angriff gegen diesen umgesetzt. Weiterhin ist es denkbar, in der Zeit des Neustarts als Angreifer in die Rolle des Teilnehmers zu schlüpfen, und so unbemerkt Angriffe durchführen zu können. Die Protocol Data Unit (PDU) könnte dabei zum Beispiel wie in Tabelle 3.1 dargestellt aussehen.

6. Byte								7. Byte							
B7	B6	B5	B4	B3	B2	B1	B0	B7	B6	B5	B4	B3	B2	B1	B0
						APCI	APCI	APCI	APCI	APCI	APCI	APCI	APCI	APCI	APCI
						1	1	1	0	0	0	0	0	0	0

Tabelle 3.1: Aufbau der PDU für ein A_Restart-Telegramm (nach [DIN04a])

Der Service-Request hat dabei folgende Parameter (nach [DIN04a]):

- **ack_request:** Parameter um eine Bestätigung auf OSI-Layer 2 als optional oder verpflichtend zu kennzeichnen.
- **priority:** Angabe der Priorität des zu übertragenden Service-Requests (Mögliche Werte: System, Urgent, Normal, Low)
- **hop_count_type:** Angabe ob hop_count auf sieben gesetzt werden soll, oder der klassische Modus genutzt werden soll.
- **Application Layer Service Access Point (ASAP):** Parameter für Service Access Point

Praktisch lässt sich diese Art von Telegrammen einfach mithilfe des bereits vorgestellten Tools knxmap versenden. Der Befehl dazu lautet wie folgt:

```
1 knxmap apci 192.168.0.190 1.1.9 Restart
```

Der erste Parameter gibt die IP-Adresse des KNX/IP-Gateways an, während die zweite Adresse für die physikalische Adresse des Netzteilnehmers steht, der neu gestartet werden soll.
Praktisch ist dieser Angriff allerdings wenig effektiv, da der Neustart von den Geräten in sehr kurzer Zeit abgeschlossen ist (etwa eine Sekunde). Damit ist auch das Zeitfenster für eventuell bösartige Handlungen sehr knapp bemessen und der Angriff kann als praktisch unwirksam angesehen werden.

Allerdings ist es möglich Anzeigen zu stören und Nutzer zum Beispiel durch das Neustarten der Software und durch veränderte Anzeigen auf dem Display kurzzeitig zu verwirren. Trotz dessen lässt sich die Schadwirkung dieses Angriffs als sehr gering einschätzen.

3.3.3 Injection von Paketen

Für das Einspielen von Telegrammen in das Bussystem sind umfangreiche Fachkenntnisse nötig, da der Angreifer wissen muss, wie er die Telegramme aufbaut, um entsprechende Aktionen auslösen zu können. Es ist allerdings auch möglich gezielt falsche Telegramme auf den Bus zu senden, um das Verhalten der Geräte bei nicht erwarteten Telegrammen zu prüfen.

Denkbar ist bei diesem Angriffsszenario vor allem auch eine Beeinflussung von Personen zu bestimmten Handlungen. Es wäre denkbar nur einzelne Lampen im Gebäude anzuschalten und so die Personen im Gebäude in bestimmte Richtungen zu „lenken“ oder auch das Licht in ausgewählten Räumen immer fünf Sekunden nachdem es eingeschaltet wurde wieder auszuschalten. Um derartige Angriffe auszuführen, braucht der Angreifer allerdings nicht nur Wissen im Bereich der Telegrammerstellung unter KNX, sondern muss auch wissen, an welchen Punkten im Gebäude welche Geräte verbaut sind und wie die Verteilung der Adressen vorgenommen wurde.

Um die Schwierigkeiten zu minimieren, können auch hierfür vorgefertigte Tools aus dem Internet genutzt werden. Erwähnenswert ist dabei vor allem xknx (`http://xknx.io`). Implementiert wurde die Software in Python mit dem async.io-Framework. Das Programm findet automatisch erreichbare KNX-IP-Gateways und wickelt die Kommunikation darüber ab. Neben einer Bus-Monitor-Funktion gibt es auch Beispiele Geräte gezielt anzusteuern, um deren Zustand zu verändern. Wie allerdings bereits in Abschnitt 3.3.1 beschrieben, ist es mit den Rohdaten ohne weitere Informationen durchaus schwierig schnell zu einem erfolgreichen Ergebnis zu kommen.

Kapitel 4

Risikoeinstufung von KNX-Netzen

In diesem Kapitel wird aufgezeigt, welche Möglichkeiten es gibt innerhalb von Hausbussystemen ein Risiko für das Netzwerk zu ermitteln. Die Analyse von verschiedenartigen Daten ermöglicht eine Abschätzung des Risikos - auch für Abschnitte des Netzes. Neben der Bewertung von statischen können zusätzlich dynamische Daten des aktuellen Netzverkehrs für diese Werte genutzt werden.

Am Ende wird ein konkreter numerischer Wert berechnet, der die Gefährdung eines konkreten Punktes im Netz beschreibt. Dieser setzt sich aus einem Vektor von einzelnen Werten zusammen, welche Risiken einschätzen. Folgende Werte sind dabei zu beachten:

- Gefährdungsklasse der angeschlossenen Geräte (siehe 4.5.1)
- Physische Zugänglichkeit der Geräte (siehe 4.5.2)
- Physische Zugänglichkeit der Leitungen (siehe 4.5.3)
- Erreichbarkeit anderer Teilnehmer (siehe 4.5.4)
- Art der Pakete (siehe 4.5.5)
- Anzahl der Pakete pro Zeiteinheit (siehe 4.5.6)

Bevor ein endgültiger Wert berechnet wird, müssen die einzelnen Punkte des Vektors noch gewichtet werden. Die statischen Werte sollten dabei eine Basis bilden, die durch die dynamischen Werte aktualisiert wird.

4.1 Risikoanalyse nach BSI 200-3

Um das Risiko eines Angriffs abschätzen zu können, gibt es viele unterschiedliche Methoden. In diesem Absatz soll knapp das Vorgehen nach dem Standard 200-3 (Risikoanalyse auf Basis von IT-Grundschutz), herausgegeben vom Bundesamt für Sicherheit in der Informationstechnik (BSI), erläutert werden.

Grundsätzlich geht es in dem Standard darum, Informationssicherheitsrisiken zu steuern. Institutionen sollen damit erfassen können, welchen Risiken sie ausgesetzt sind, um dann entsprechend gegensteuern zu können. Während bereits für viele Gefährdungen eine Analyse durch das BSI im IT-Grundschutz beschrieben wurden, kann es auch passieren, dass für spezielle Fälle eine individuelle Betrachtung des Risikos vorgenommen wird. Das Risiko wird dabei aus der Eintrittswahrscheinlichkeit und der Höhe des Schadens berechnet.

Die Risikoanalyse wird nach dem Standard nach folgenden Schritten ausgeführt ([BSI17]):

1. Schritt: Erstellung einer Gefährdungsübersicht (Liste möglicher elementarer Gefährdungen, Ermittlung zusätzlicher Gefährdungen)
2. Schritt: Risikoeinstufung (Risikoeinschätzung und -bewertung)
3. Schritt: Risikobehandlung (Risikovermeidung, -reduktion, -transfer, -akzeptanz)
4. Schritt: Konsolidierung des Sicherheitskonzepts

Als Liste elementarer Gefährdungen gibt es bereits vom BSI eine Zusammenstellung mit insgesamt 47 Elementen. Zusätzlich wurde dabei erfasst, welche Grundwerte, wie Vertraulichkeit, Integrität und Verfügbarkeit, davon hauptsächlich betroffen sind. Für jede elementare Gefährdung ist dann wiederum zu entscheiden, ob die Gefährdung für das zu betrachtende Element direkt, indirekt oder nicht relevant ist. Neben den elementaren Gefährdungen können auch weitere Gefährdungen identifiziert werden. Von Relevanz sind dabei solche, die zu einem „nennenswerten Schaden führen, und die im vorliegenden Anwendungsfall und Einsatzumfeld realistisch sind“ [BSI17].

Zur Einstufung des Risikos müssen sowohl die Eintrittshäufigkeit, als auch die potenzielle Schadenshöhe betrachtet werden. Dazu bietet es sich an, diese beiden Quantifizierungen in Kategorien einzuteilen, und dann entsprechend die Gefährdungen in diese Kategorien einzuordnen. Das Risiko kann anschließend aus einer sogenannten Risikomatrix einfach abgelesen werden. Eine derartige Matrix ist in Abbildung 4.1 gezeigt. Zu beachten ist hierbei allerdings, dass es sich nur um ein Beispiel handelt und die Matrix in jedem Fall an die eigenen Bedürfnisse im Unternehmen angepasst werden muss.

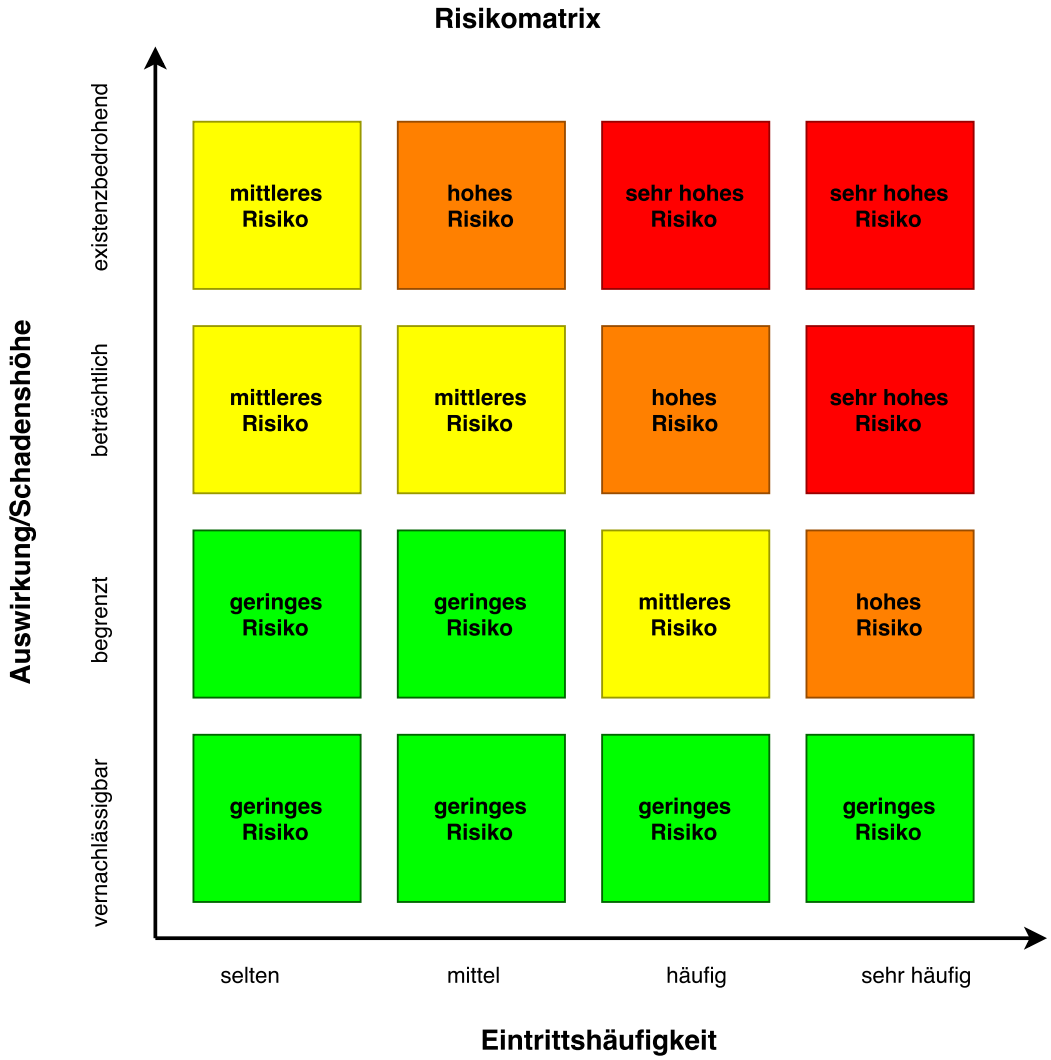

Abbildung 4.1: Matrix zur Bestimmung des Risikos bei spezifischer Eintrittswahrscheinlichkeit und entsprechendem Schaden (nach [BSI17])

4.2 Statische Daten

Statische Daten müssen nur zu Beginn einmal gesammelt werden, um damit arbeiten zu können. Sie bilden die aktuell vorliegende Installation ab und geben einen guten Überblick über den Netzaufbau und möglicherweise vorhandene neuralgische Punkte. Lediglich bei physischen Änderungen der Installation müssen diese Werte erneut betrachtet und entsprechend angepasst werden.

Zur Bestimmung werden der Gebäudeplan, der Netzplan und die Projektdatei der ETS benötigt. Als Beispiel liegt die Projektdatei für den Demonstrator auf dem Datenträger im Anhang bei. Bei gut dokumentierten Projekten ist der Netzplan nicht unbedingt nötig, da in der Projektdatei gespeichert wird, welcher Teilnehmer in welchem Bereich des Gebäudes installiert ist. Zusätzlich kann aus der Projektdatei die Kommunikation der einzelnen Komponenten über die Gruppenadressen eingesehen werden.

Zu den statischen Daten zählen die folgenden Punkte:

- Gefährdungsklasse der angeschlossenen Geräte
- Physische Zugänglichkeit der Geräte
- Physische Zugänglichkeit der Leitungen
- Erreichbarkeit anderer Teilnehmer

Aus diesen Informationen lässt sich bereits abschätzen, welche Angriffe an konkreten Orten vermutlich besonders einfach auszuführen sind und wo daher eine besondere Gefahr droht. Es kann mit den Werten daher eine erste Risikoabschätzung erfolgen. Auch das Auffinden von problematischen und damit neuralgischen Punkten ist so möglich.

4.3 Dynamische Daten

Neben dem Überblick durch die statischen Daten soll auch die Echtzeitsituation oder zumindest eine Darstellung die sich möglichst nah daran orientiert betrachtet werden. Dafür wird der auf dem Bus vorhandene Netzverkehr analysiert.

An einzelnen Observationspunkten wird dafür der Telegrammverkehr mitgelesen. Die so gesammelten Informationen können auf unterschiedliche Weise weiterverarbeitet werden. Neben der Verdichtung zu Netflows und Weiterleitung an Kollektoren zur Analyse (siehe dazu [Pet18] und [Jun18]) kann auch eine Analyse der Anwendungsdaten in den Telegrammen erfolgen. Dieses Vorgehen orientiert sich an der sogenannten „Deep Packet Inspection“. Mit beiden Techniken kann erkannt werden, welche Arten von Telegrammen versendet werden, und welcher Teilnehmer an welche Adressen sendet. Damit ist es möglich bereits einen gewissen Anteil von Angriffen zu detektieren, eventuelle Probleme frühzeitig zu erkennen und die Risikoeinschätzung entsprechend anzupassen. Weitere Informationen zur Mächtigkeit und Vor-, sowie Nachteilen der Techniken sind in Abschnitt 5.2 erläutert.

Durch eine Analyse der Anzahl und Art der Pakete kann ein Rückschluss darauf gezogen werden, wie interessant ein Bereich des Netzes für einen Angreifer ist, der lediglich Datenverkehr mitschneiden möchte. Der Risiko-Wert für einen konkreten Ort kann sich dabei auch zur Laufzeit ändern, wenn beispielsweise auf einmal mehr Daten daran vorbei fließen. Neben der reinen Anzahl und Art der Telegramme ist dabei vor allem auch der Informationsgehalt interessant. Durch die Analyse dessen können deutlich umfangreichere und aussagekräftigere Ergebnisse erzielt werden.

4.4 Sammlung von Daten

Neben den Daten, welche direkt vorliegen oder vom Bus aus mitgehört werden können, ist es auch möglich, eigenständig Informationen aus dem System abzufragen und darüber Einschätzungen zu treffen.

4.4.1 Auslesen von Werten aus der ETS-Datenbank

Während der Gebäude- und Netzplan zwar für Personen besonders gut lesbar sind, ist eine automatisierte Verarbeitung eher problematisch, da die Daten nicht immer in genormter und maschinenlesbarer Form vorliegen.

Deutlich vorteilhafter ist es daher diese Daten aus dem Backend der ETS-Software auszulesen. Diese schreibt ihre Daten in eine MS-SQL-Datenbank. Ein Auslesen ist daher grundsätzlich einfach möglich. Um das Vorgehen dabei etwas zu vereinfachen,

wurde eine Python-Anwendung (siehe Datenträger) erstellt, in der bereits einige Abfragen implementiert sind, um vor allem die Tabellenstruktur nicht selbst explorieren zu müssen.
Folgende Funktionen sind vorhanden:

- Abfrage von verbauten Geräten
- Abfrage von Geräten nach Produkt-ID
- Abfrage von Geräten nach physikalischer Adresse
- Abfrage von verfügbaren Gruppenadressen
- Abfrage von Geräten, die an einer Gruppenadresse beteiligt sind
- Abfrage von Gruppenadressen, die zu einem Gerät gehören
- Abfrage von Geräten, die über Gruppenadressen mit einem bestimmten Gerät kommunizieren

Damit ist es möglich, einen Überblick über die vorhandene Projektstruktur zu erlangen, und die Daten zugleich maschinenlesbar weiter verarbeiten zu können. Es ist beispielsweise möglich Geräte-Whitelists (siehe Kapitel 5.5) zu erzeugen oder auch Filterregeln für Linienübergänge zu erstellen, da genau gesehen werden kann, welches Gerät welche anderen Geräte erreichen muss, wenn beide Teilnehmer der gleichen Gruppenadresse sind.

4.4.2 Auslesen von Werten der Busteilnehmer

Sobald ein Zugang zum KNX-Bus besteht, ist es möglich, Informationen über die einzelnen Teilnehmer auszulesen. Dafür werden entsprechende Telegramme an die physikalischen Adressen versendet. In der Antwort erhält man allgemeine Informationen, Daten zum Applikationsprogramm und auch die Gruppenkommunikation. Mit diesen Daten kann das Gerät eindeutig identifiziert werden. Es können weiterhin Rückschlüsse gezogen werden, welche Funktionen der Teilnehmer steuert.

Die Funktion gibt die Möglichkeit die gesamte Linie zu explorieren und auch zu prüfen, welche weiteren Geräte von diesem Punkt aus erreichbar sind. Allerdings ist eine derartige Exploration sehr auffällig, da viele Telegramme an physikalische Adressen gesendet werden, was im regulären Betrieb nicht vorkommt. Weiterhin

ist anzumerken, dass zwar die Adressen und Werte abgelesen werden können, allerdings keinerlei Beschreibung dazu entnommen werden kann. Dies erschwert eine Rekonstruktion des Aufbaus sehr stark.

4.5 Entwicklung eines geeigneten Maßes

Um die Gefährdung von Netzsegmenten zu messen und somit eine mögliche Empfehlung zu eventuellen Änderungen geben zu können soll in einem ersten Schritt für jedes Gerät eine Gefährdungsklasse festgelegt werden. Neben dieser gibt es auch eine Klasse für die Zugänglichkeit der Geräte. Anschließend wird geprüft, welche Teilnehmer sich auf einer Linie befinden und was für Kommunikation auf dieser stattfindet. Mit diesen Daten lassen sich Bewertungen für Linien und Bereiche vornehmen.

4.5.1 Gefährdungsklassen für Geräte

Dieser Abschnitt stellt die geplanten Gefährdungsklassen für Geräte vor. Neben einer genaueren Beschreibung, was Geräte in dieser Klasse auszeichnet sollen auch beispielhaft KNX-Teilnehmer zugeordnet werden.

Klasse 0 - unproblematisch

Geräte in Klasse 0 sind völlig unproblematisch, da mit diesen keine KNX-Kommunikation möglich ist. Dies trifft beispielsweise auf Netzteile oder Datenschienen zu. Auszeichnend ist hierbei vor allem, dass die Geräte über keine direkte physikalische Geräteadresse verfügen, sondern nur einem Bereich und einer Linien zugeordnet sind.

Klasse 1 - geringes Gefährdungspotenzial

Klasse-1-Geräte sind häufig verbaut und haben nur einen sehr stark lokal beschränkten Wirkungsbereich. Bei einem Ausfall ist der Betrieb höchstens in einem sehr kleinen Bereich des Gebäudes gestört und bei einem Totalausfall der Komponenten ist nur mit einem geringen wirtschaftlichen Schaden zu rechnen. Ein Beispiel für derartige Geräte sind Licht- oder Jalousie-Schalter.

Klasse 2 - mittleres Gefährdungspotenzial

Eine Störung oder ein Ausfall von Geräten der Klasse 2 führt zu einer größeren Störung. Zu dieser Klasse werden beispielsweise Linienkoppler gezählt. Sollten diese lahmgelegt werden, können zwar die Geräte innerhalb der Linien noch miteinander kommunizieren, der Übergang zum restlichen System ist allerdings gestört. Zusätzlich werden hier auch Gateways jeglicher Art eingeordnet. KNX/IP-Gateways können beispielsweise erst den Zugang aus dem IP-basierten Umfeld in das hauseigene Bussystem öffnen und bieten daher eine nicht zu vernachlässigende Gefahr.

Klasse 3 - hohes Gefährdungspotenzial

Geräte mit hohem Gefährdungspotenzial sind in der Regel selten mehrfach im Gebäude verbaut und stören bei einem Ausfall den Ablauf im gesamten Wirkungsbereich / Gebäude. Sollten diese ausfallen, ist mit einem hohen finanziellen Schaden zu rechnen. Dazu zählen beispielsweise Heizungsanlagen.

4.5.2 Zugangsklassen für Geräte

Die Zugangsklassen beschreiben wie einfach ein potenzieller Angreifer Zugang zu einem Gerät und damit auch zur entsprechend verbundenen Buslinie bekommen kann. Um eine Kategorisierung und Messung des Risikos zu erlauben, wurden drei Klassen definiert, in welche sich entsprechende Geräte einordnen lassen.

Klasse 0 - zugangsbeschränkter Bereich

Geräte der Zugangsklasse 0 sind nur in zugangsbeschränkten Bereichen zu finden. Hierbei ist es wichtig, dass nur einer geringen Anzahl an Personen der Zugang möglich ist und auch eine Aufzeichnung des Zutritts geführt wird. Auf diese Art kann bei einer Manipulation der mögliche Kreis von Angreifern extrem stark eingeschränkt werden. Technikräume, welche verschlossen sind und im besten Fall noch einzeln verschlossene Schaltschränke besitzen, zählen beispielsweise in diese Klasse.

Klasse 1 - Zugang nicht offensichtlich / schwer erreichbar

In Klasse 1 sind auch Geräte zu finden, die für eine große Menge an Personen sichtbar sind, wobei der Zugang allerdings zum Beispiel durch bestimmte Montagepositionen besonders erschwert wird, oder die ohne eine Manipulation von Wänden/Schränken nicht ersichtlich sind. Als Beispiel sind hier Bewegungsmelder zu nennen. Diese werden typischerweise an der Decke angebracht und sind nicht ohne Hilfsmittel erreichbar. Weiterhin zählen hierzu Geräte oder auch Buszugänge, welche nicht ohne Weiteres sichtbar sind. Dies könnten beispielsweise Vorbereitung für die Nachrüstung von Geräten in der Wand, oder auch Schalter in Schränken sein.

Klasse 2 - Zugang einfach möglich

Klasse 2 vereint alle Geräte, bei denen der Zugang besonders einfach möglich ist. Hierzu zählen vor allem Lichtschalter oder vergleichbare Geräte. Diese sind typischerweise immer einfach sichtbar und zugänglich, da sie häufig genutzt werden. Auch die Montagehöhe dieser Geräte bietet einen einfachen Zugang, der nicht unbedingt auffällt.

4.5.3 Zugangsklassen für verlegte Leitungen

Neben der Betrachtung der Geräte an sich muss auch betrachtet werden, in welchem Bereich die Leitungen verlaufen, an denen die Busteilnehmer angeschlossen sind, da es einem Angreifer möglich ist, sich auch jederzeit mit einem Gerät an den Bus direkt anzuschließen, und so Telegramme abzufangen oder einzuschleusen.

Klasse 0 - besonders gesicherte Leitungen

Leitungen die besonders gegen einen Zugriff von außen gesichert sind fallen in Klasse 0. Dies sind Leitungen, die nur in zugangsbeschränkten Bereich verlaufen und/oder physische gegen einen Zugriff geschützt sind. Sie stellen damit kein unmittelbares Risiko dar. Bei einem Angriff kann vergleichsweise einfach nachempfunden werden, wer sich Zugriff verschafft hat und damit den potenziellen Angriff ausgeführt hat.

Klasse 1 - hausinterne Leitungen

Klasse 1 stellt Leitungen dar, welche innerhalb des Gebäudes verlaufen. Leitungen dieser Klasse sind grundsätzlich nicht offen zugänglich und verlaufen nur innerhalb des Gebäudes, werden also immer durch eine Außenwand vom Äußeren des Gebäudes getrennt.

Klasse 2 - Leitungen an/in Außenwand

Leitungen in dieser Klasse verlaufen an der äußeren Seite von Außenwänden oder in diesen. Es ist dabei denkbar, dass sich ein Angreifer durch das Wissen vom Leitungsverlauf auch von außen Zugang verschaffen kann und somit Zugriff auf das Bussystem gewinnt, obwohl er sich nicht im Gebäude befindet.

Klasse 3 - offen zugängliche Leitungen im Außenbereich

Die Gruppe von Leitungen, welche von außen am Gebäude zugänglich sind und dabei nicht hinter Verkleidungen oder Ähnlichem verlaufen, sondern beispielsweise in Außenschaltern oder Klingelanlagen enden, werden in Klasse 3 gesammelt. Ein Angreifer kann hier sehr einfach Zugriff auf den Bus gewinnen, weshalb diese Leitungen besonders kritisch betrachtet werden sollten.

4.5.4 Klassifizierung der Erreichbarkeit anderer Teilnehmer

Die Erreichbarkeit von weiteren Netzteilnehmern spielt auch eine wichtige Rolle. Es wird gezeigt, wie weit ein Angreifer von dem zu untersuchenden Punkt aus in das Netzwerk eindringen kann.

Klasse 0 - Keine weiteren Teilnehmer erreichbar

Sind keine weiteren Teilnehmer auf anderen Linien oder Bereichen erreichbar, so besteht lediglich das minimale Risiko, dass ein Angreifer die Teilnehmer erreichen kann, die ebenfalls im gleichen Bereich und an der gleichen Linie angeschlossen sind. Dies lässt sich nicht verhindern.

Klasse 1 - Einige andere Teilnehmer erreichbar

Für Klasse 1 gilt, dass einige andere Teilnehmer erreicht werden können. Dabei ist nicht erheblich, um welche Geräte es sich dabei handelt. Die einzige Bedingung ist, dass die anderen Teilnehmer in unterschiedlichen Bereichen/Linien als der Ausgangspunkt liegen.

Klasse 2 - Alle Teilnehmer erreichbar

Sobald alle Teilnehmer im gesamten Bussystem erreichbar sind, stellt dies das maximale Risiko bezüglich der Erreichbarkeit von anderen Geräten dar.

4.5.5 Klassifizierung der Menge von Paketen

Die Menge von Paketen ist ein schwer zu quantifizierendes Element bei der Betrachtung des Risikos von einzelnen Netzsegmenten. Folgende Werte bieten daher nur einen Richtwert und müssen im Zweifel weiter an die vorhandene Situation angepasst werden. Grundsätzlich kann allerdings gesagt werden, je weniger der Bus ausgelastet ist, desto weniger Informationen kann ein potenzieller Angreifer an diesem Bussegment sammeln.

Klasse 0 - Busauslastung unter 5 Prozent

Bei unter fünf Prozent Busauslastung werden vergleichsweise wenig Telegramme gesendet. Geht man von einem Standarddatentelegramm mit 2 Byte Nutzlast aus, können bei einer Busauslastung von weniger als fünf Prozent bis zu zwei Telegramme pro Sekunde gesendet werden.

Klasse 1 - Busauslastung unter 20 Prozent

Die Busauslastung beträgt bis zu 20 Prozent. Damit sind unter der Annahme in Klasse 0 bis zu 9 Telegramme pro Sekunde möglich.

Klasse 2 - Busauslastung unter 60 Prozent

Eine Busauslastung von bis zu 60 Prozent bedeutet unter obiger Annahme bis zu 29 Telegramme pro Sekunde. Ein Angreifer kann so bereits eine Vielzahl an Daten in kurzer Zeit sammeln.

Klasse 3 - Busauslastung bis 100 Prozent

In dieser Klasse ist das Bussegment bis zu 100 Prozent ausgelastet. Dies entspricht etwa 49 Telegrammen pro Sekunde unter der Annahme von Standarddatentelegrammen mit 2 Byte Nutzlast. Durch die Menge an übertragenen Informationen besteht daher ein erhöhtes Risiko, dass ein Angreifer wichtige Daten erbeutet.

4.5.6 Klassifizierung der Art von Paketen

Die Arten von Paketen sind entscheidend für die Angriffserkennung. Im regulären Betrieb treten lediglich Gruppentelegramme auf, während physikalisch adressierte Telegramme nur zur Programmierung genutzt werden.

Klasse 0 - Nur Grupppentelegramme

Auf dem Bus treten ausschließlich Gruppentelegramme auf. Diese sind für den normalen Betrieb vorgesehen. Eine Einschätzung der Gefahr dieser Pakete ist nur mit zusätzlichen Informationen zum Nachrichteninhalt möglich. Dies soll hier aber nicht betrachtet werden.

Klasse 1 - Gruppen- und Konfigurationstelegramme

Sobald auch Konfigurationstelegramme auftreten, sollte das Bussegment genauer beobachtet werden. Diese Art von Telegrammen wird in der Regel lediglich für die Konfiguration von Geräten genutzt und tritt im regulären Betrieb nicht auf. Es sollte daher sehr genau überprüft werden, warum entsprechende Telegramme detektiert wurden.

4.5.7 Gefährdungseinschätzung für Bereiche und Linien

Um die Gefährdung von Linien und Bereichen einzuschätzen, reicht es nicht die einzelnen verbauten Geräte anzusehen, sondern es muss auch beachtet werden, welche weiteren Gruppenadressen von diesen Linien / Bereichen erreicht werden können und ob damit eine Manipulation von weiteren Busteilnehmern möglich ist. Es ist daher erforderlich die Geräte auf der Linie / im Bereich an sich anzusehen und alle davon erreichbaren Geräte.

Vorstellbar wäre beispielsweise, dass ein Angreifer die physikalische Adresse eines Temperatursensors herausfindet und durch das senden von Telegrammen mit dessen Adresse und stark abweichenden Temperaturwerten versucht die Temperatur in einem Gebäudebereich zu verändern, um diesen nicht mehr nutzbar zu machen. Dabei ist auch zu prüfen, wie die Linien-/Bereichskoppler eingestellt sind und ob die Filter aktiv sind, sodass nur die Kommunikation sichtbar ist, die auch unbedingt in diesem Bereich sichtbar sein muss.

Wurde eine Linie oder ein Bereich identifiziert, der besonders schützenswert ist, dann müssen weitere Maßnahmen getroffen werden, um das gesteigerte Schutzbedürfnis zu erfüllen. Möglichkeiten hierzu werden in Kapitel 5 vorgestellt.

4.6 Einstufung des Risiko-Maßes

Dieser Abschnitt soll zeigen, wie sich das Risiko aus den oben vorgestellten Klassen berechnen lässt. Dabei wird zuerst das statische Risiko (siehe Formel 4.1) berechnet, welches anschließend mit den dynamischen Daten zu einem Live-Wert angepasst werden kann.

$$Risiko_{statisch} = \left| \begin{pmatrix} K_{Geräteklasse} \\ K_{Zugangsklasse\ (Geräte)} \\ K_{Zugangsklasse\ (Leitung)} \\ K_{Erreichbarkeitsklasse} \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{3} \\ \frac{1}{2} \\ \frac{1}{3} \\ \frac{1}{2} \end{pmatrix} \right| \cdot \frac{1}{2} \tag{4.1}$$

Um zu erreichen, dass jedes Element des Vektors zu gleichen Teilen in das Ergebnis eingeht, müssen die Werte skaliert werden. Dies gleicht die Werte durch unterschiedlich viele Klassen aus. Bei den statischen Werten sind die „Geräteklasse“ und die

„Zugangsklasse der Leitungen“ jeweils mit vier Klassen (0 bis 3) zu bewerten. Die „Zugangsklasse für die Geräte“ und die „Erreichbarkeitsklasse“ sind mit drei Klassen (0 bis 2) zu bewerten. Um diese Ungleichheit auszugleichen, müssen die Werte mit $\frac{1}{3}$ beziehungsweise $\frac{1}{2}$ multipliziert werden. Der Betrag des Vektors wird am Ende noch mit Faktor $\frac{1}{2}$ multipliziert, um einen Wertebereich zwischen 0 und 1 zu erreichen.

$$Risiko_{dynamisch} = \left| \begin{pmatrix} K_{Menge\ Pakete} \\ K_{Art\ Pakete} \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{3} \\ 1 \end{pmatrix} \right| \cdot \frac{1}{\sqrt{2}} \tag{4.2}$$

Ähnlich verhält es sich beim dynamischen Risiko (siehe Formel 4.2). Hier wird der Wert für die „Menge der Pakete“ (Klassen von 0 bis 3) mit $\frac{1}{3}$ skaliert und der Wert für die „Art von Paketen“ (Klasse 0 oder 1) mit dem Skalar eins multipliziert. Um den Wertebereich auch hier auf das Intervall zwischen 0 und 1 zu skalieren, wird der Betrag des Vektors mit dem Faktor $\frac{1}{\sqrt{2}}$ multipliziert.

$$Risiko = \left| \begin{pmatrix} Risiko_{statisch} \\ Risiko_{dynamisch} \end{pmatrix} \right| \cdot \frac{1}{\sqrt{2}} \tag{4.3}$$

Um den Gesamtwert für das Risiko (siehe Formel 4.3) bestimmen zu können wird anschließend der Betrag des Vektors aus den beiden Risiken (statisch und dynamisch) berechnet. Dieser muss wieder mit dem Faktor $\frac{1}{\sqrt{2}}$ skaliert werden, um einen Wertebereich zwischen 0 und 1 zu erreichen. Vorteilhaft wäre allerdings die Speicherung der einzelnen Werte des Risikos (statisch und dynamisch). Der Vorteil liegt darin, dass zu weiteren Berechnungen beide Werte getrennt betrachtet werden können.

4.7 Risiko im Beispielszenario

Nachfolgend soll die Berechnung des Risikos kurz an einem Beispiel nachvollzogen werden. Dafür wurden zwei Räume des Konrad-Zuse-Haus der Informatik der Universität Rostock (Albert-Einstein-Str. 22, 18059 Rostock) gewählt. Es ist zu beachten, dass nur das statische Risiko berechnet werden kann. Für den dynamischen Wert werden Live-Daten benötigt, die aus datenschutzrechtlichen Gründen nicht zur Verfügung gestellt werden konnten.

4.7.1 Raum 005 (Konrad-Zuse-Haus)

Als erstes Beispiel dient die Herrentoilette im Erdgeschoss (Raumnummer 005) hinter dem Info-Bereich. Für die Gefährdungsklasse müssen zuerst die an diese Linie **angeschlossenen Geräte** betrachtet werden. Dabei handelt es sich um ein Netzteil, einen Linienkoppler, Präsenzmelder, Taster, Displays, Lüftungssteuerungen, analoge Ausgänge und binären Schaltaktoren. Dabei sind die Geräte auf 16 Räume, den Flur und einen Schaltkasten verteilt. Durch das Vorhandensein des Linienkopplers und auch der Lüftungssteuerung fällt diese Linie in **Gefährdungsklasse 2**. Die **Zugänglichkeit der Geräte** ist mit **Klasse 2** zu bewerten, da viele Lichtschalter auf der betroffenen Linie sitzen und diese besonders leicht erreichbar sind. Zudem sind einige Räume (so auch die Toilette) öffentlich zugänglich und von Kameraüberwachung ausgeschlossen. Die Leitungen für diesen Bereich verlaufen höchst wahrscheinlich nur hausintern und sind nicht in Außenwänden verlegt. Für eine genaue Prüfung müsste der Netzplan zurate gezogen werden. Da dieser hier nicht vorliegt, wird **Gefährdungsklasse 1 für die Leitungen** angenommen. Bezüglich der Erreichbarkeit anderer Teilnehmer ist zu sagen, dass in der vorliegenden Projektdatei zum Gebäude mit der letzten Änderung vom September 2014 die Linienkoppler im Erdgeschoss und im ersten Obergeschoss komplett offen waren, während im zweiten und dritten Obergeschoss zumindest die Filter aktiv waren. Zusätzlich fällt auf, dass der Bereich von Linie 3.3.0 bezüglich der Gruppentelegramme komplett gesperrt ist. Daher würde dieser Bereich mit **Klasse 1 bezüglich der Erreichbarkeit weiterer Teilnehmer** gewertet werden.

Das statische Risiko kann nun wie in Formel 4.4 berechnet werden und ergibt einen Wert von $\approx 67,19\%$.

$$
\begin{aligned}
Risiko_{statisch} &= \left| \begin{pmatrix} K_{Geräteklasse} \\ K_{Zugangsklasse\ (Geräte)} \\ K_{Zugangsklasse\ (Leitung)} \\ K_{Erreichbarkeitsklasse} \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{3} \\ \frac{1}{2} \\ \frac{1}{3} \\ \frac{1}{2} \end{pmatrix} \right| \cdot \frac{1}{2} \\
Risiko_{statisch} &= \left| \begin{pmatrix} 2 \\ 2 \\ 1 \\ 1 \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{3} \\ \frac{1}{2} \\ \frac{1}{3} \\ \frac{1}{2} \end{pmatrix} \right| \cdot \frac{1}{2} \approx 0,6719
\end{aligned}
\tag{4.4}
$$

4.7.2 Raum 341 (Konrad-Zuse-Haus)

Als weiteres Beispiel soll der Raum für die Gebäudetechnik im dritten Obergeschoss betrachtet werden. Hier stehen die Klimaaggregate für das Gebäude und auch die Heizung. Bezüglich der angeschlossenen **Geräte** ist **Klasse 3** zu wählen, da in diesem Raum Infrastruktur steht, die nur einmal verbaut wurde, wie zum Beispiel die Wetterstation. Im Bereich der **Zugänglichkeit** ist zu sagen, dass der Raum gegen Zutritt besonders gesichert ist, und damit Klasse 0 entspricht. Allerdings sind auf der Linie noch weitere Geräte angeschlossen, die in anderen Räumen und sogar auf Fluren liegen, wodurch dieser Wert auf **Klasse 1** zu relativieren ist. Für die verlegten **Leitungen** ist ebenfalls **Klasse 1** zu wählen, da diese hausintern verlaufen und ansonsten höchstens auf dem Dach, was nicht einfach zugänglich ist. Bezüglich der Erreichbarkeit anderer Teilnehmer wurde der Linienkoppler so eingestellt, dass Gruppentelegramme gesperrt sind und so nur ein Minimum an Kommunikation möglich ist. Damit ist für die **Erreichbarkeit anderer Teilnehmer Klasse 0** zu wählen.

$$
\begin{aligned}
Risiko_{statisch} &= \left| \begin{pmatrix} K_{Geräteklasse} \\ K_{Zugangsklasse\ (Geräte)} \\ K_{Zugangsklasse\ (Leitung)} \\ K_{Erreichbarkeitsklasse} \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{3} \\ \frac{1}{2} \\ \frac{1}{3} \\ \frac{1}{2} \end{pmatrix} \right| \cdot \frac{1}{2} \\
Risiko_{statisch} &= \left| \begin{pmatrix} 3 \\ 1 \\ 1 \\ 0 \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{3} \\ \frac{1}{2} \\ \frac{1}{3} \\ \frac{1}{2} \end{pmatrix} \right| \cdot \frac{1}{2} \approx 0.5833
\end{aligned}
\tag{4.5}
$$

Nach Formel 4.5 beträgt das statische Risiko somit $\approx 58,33\%$ des maximalen Risikos.

4.7.3 Vergleich der Risiken

Die Berechnung der beiden Werte hat gezeigt, dass das Risiko für Raum 005 höher als das für Raum 341 ist. Der Unterschied liegt bei etwa 8,9 Prozent. Dies ist nicht besonders viel dafür, dass ein sehr einfach zugänglicher Raum, und ein Raum mit starken Limitierungen für den Zugang verglichen wurden. Dies liegt vor allem auch daran, dass besonders sensible Geräte an die Leitung der Linie 3.3.0 angeschlossen sind und die Linie auch in weniger zugangsgesicherten Bereichen verläuft. Beispielsweise ist hier der Flur in der dritten Etage zu nennen.

Kapitel 5

Verteidigungsmaßnahmen

Dieses Kapitel soll einen Überblick über mögliche Maßnahmen geben, die getroffen werden können, um aktuelle Bedrohungen so effizient wie möglich zu bekämpfen und entsprechende Risiken zu minimieren. Dabei gibt es sowohl Möglichkeiten ohne zusätzliche Geräte oder Barrieren installieren zu müssen, als auch Maßnahmen, die dies erfordern.

5.1 Einsatz von KNX Secure

Wie bereits eingangs beschrieben (siehe Abschnitt 2.4) bietet KNX ab Version 2.1 eine verschlüsselte Kommunikation an. Allerdings gibt es bisher kaum Produkte, die unterstützt werden und auch bei Nachfrage von Geräteanbietern konnte keine genaue Aussage getroffen werden, in welchem Zeitraum mit entsprechenden Geräten zu rechnen ist. Aufgrund dieser Tatsachen findet KNX Secure in dieser Arbeit keine weitere Aufmerksamkeit, da aktuell scheinbar noch keine Geräte großflächig im Umlauf sind und zur Nachrüstung des Standards bestehende Geräte mindestens ausgebaut und eine neue Firmware geflasht bekommen, wenn nicht sogar komplett getauscht werden müssten. Dies bedeutet einen enormen Arbeitsaufwand. Es wird daher hier betrachtet, wie bestehende Anlagen trotz fehlender Authentisierung und Verschlüsselung mit einem gewissen Maß an Sicherheit betrieben werden können.

5.2 Überwachung des Datenverkehrs im KNX-Bussystem

Um Unregelmäßigkeiten im Telegrammverkehr feststellen zu können, gibt es unterschiedliche Möglichkeiten. Neben der vollständigen Überwachung aller Telegramme können auch aggregierte Informationen in Form von Netflows zur Auswertung genutzt werden. Beide Möglichkeiten werden im folgenden Abschnitt vorgestellt.

5.2.1 Deep Packet Inspection

Neben dem Einsatz einfacher Filterregeln bei Linienkopplern, die sich an Adressinformationen orientieren, gibt es auch die Möglichkeit alle Telegramme auf OSI-Layer 7 (Application Layer) zu betrachten. Damit werden die Anwendungsinformationen decodiert und auf mögliche Schadwirkung hin untersucht.

Das Verfahren ist vor allem aus IP-basierten Netzen bekannt (siehe auch [Nor05]). Während unbekannte und mit hoher Wahrscheinlichkeit gefährliche Protokolle einfach in der Firewall blockiert werden können, werden allerdings trotzdem einige wichtige Protokolle nach außen offen benötigt, beziehungsweise sind im internen Netz von großer Wichtigkeit. Dieses Problem haben auch Angreifer erkannt und schleusen ihre Angriffe und die dafür benötigte Kommunikation über bekannte Protokolle nach außen. Dies macht es einfachen Stateful-Firewalls unmöglich potenzielle Schädlinge oder schädliche Kommunikation zu erkennen.

Deep Packet Inspection untersucht daher die Pakete genau auf Anwendungsschicht und sucht nach schädlichen Signaturen. Es ist im IP-Umfeld auch möglich, beispielsweise SSL-verschlüsselten Verkehr zu untersuchen. Dazu muss allerdings auf dem System, welches die Untersuchung durchführt der gesamte Datenverkehr entschlüsselt, untersucht und anschließend wieder verschlüsselt werden. Dies kostet neben der benötigten Performance vor allem auch eine erhöhte Latenz.

5.2.2 Anomalieerkennung in Netflows

Neben der Überwachung des gesamten Netzverkehrs kann auch eine aggregierte Version von Netflows zum Auffinden von Anomalien genutzt werden (siehe hierzu [Jun18] und [Pet18]). Für die Umsetzung dafür werden sogenannte Agenten in den unterschiedlichen Netzsegmenten oder auch Linien ausgebracht, um den Netzverkehr mitzuschneiden und zu Flows mit entsprechenden Informationen zu aggregieren. Wie dies möglich ist, wird in Kapitel 2.3 beschrieben. In [Jun18] wird eine Möglichkeit erläutert, wie das Konzept der Netflows auch für das KNX-System angepasst werden kann. Die gesammelten Flow-Daten werden anschließend zu einem Kollektor exportiert und dort analysiert. In [Pet18] wurde hierfür eine entsprechende Architektur entwickelt, wobei die Kollektoren die Daten an Analysemodule weiterleiten, die diese auf Anomalien untersuchen. Dabei ist es möglich unterschiedliche Algorithmen einzusetzen, um Probleme zu erkennen. Die Ergebnisse werden anschließend in eine Influx-Datenbank geschrieben. Ein Grafana-Backend visualisiert am Ende die Ergebnisse und schafft so die Möglichkeit schnell einen entsprechenden Überblick über die Situation im Bussystem zu gewinnen.

Ein Intrusion Detection System (IDS) auf Basis von Netflow-Daten in Bussystemen bietet dabei vor allem folgende Vorteile:

- In-band-Lösung zur Umsetzung ohne Einrichtung eines zusätzlichen Netzwerks
- Verdichtung der Daten zur Minimierung der Übertragungsmenge
- Nutzung von künstlicher Intelligenz zur Detektion von Anomalien im Netzverkehr

Neben den Vorteilen sind aber auch folgende Nachteile vorhanden:

- Informationsverlust durch Verdichtung von Daten
- Erhöhung der Buslast durch Übertragung der Flow-Daten
- Zeitverzögerung während Sammlung der Daten
- Datenschutzproblematik mit personenbezogenen Daten

Bei den Nachteilen gilt zu ergänzen, dass im Konzept nach [Pet18] keinerlei Verschlüsselung der aggregierten Daten vorgenommen wurde. Es ist also möglich, dass durch den Einsatz eines derartigen Systems die durch sinnvolle Zonen eingeführte

Trennung und Segmentierung des Netzes untergraben wird und es einem Angreifer auf der Backbone-Linie möglich, ist trotzdem den kompletten Netzverkehr zumindest in Form der Flows mitzulesen. Darauf wurde auch in der Arbeit von [Pet18] hingewiesen. Es empfiehlt sich daher dringend, in diesem Bereich eine Verschlüsselung einzusetzen!

Aus gegebenen Gründen ist entsprechend abzuwägen, ob ein Einsatz von derartigen Systemen hilfreich ist und vorgenommen werden sollte oder nicht. Zusätzlich gilt zu beachten, dass für den Einsatz der Algorithmen mit künstlicher Intelligenz ein entsprechend großer Trainingsdatenbestand vorhanden sein muss, indem mit Sicherheit keine Anomalien auftreten. Ist dies nicht der Fall, kann es zu sehr vielen Fehlmeldungen kommen. Zum einen kann ein falsch positives Ergebnis auftreten, was der Meldung eines Angriffs entspricht, der nicht tatsächlich stattgefunden hat, zum anderen können aber auch falsch negative Ergebnisse auftreten. Diese wären schlimmer, da diese nicht detektierte Angriffe darstellen.

5.3 Einsatz von Sicherheitszonen

Sicherheitszonen wie in Abschnitt 2.2 bereits beschrieben bieten eine gute Möglichkeit Netzbereiche von anderen zu trennen und somit für erhöhte Sicherheit zu sorgen. Wie im IP-basierten Umfeld sind die Überwachung des Netzverkehrs und der Einsatz von Firewalls an Zonenübergängen sinnvoll. Ähnlich verhält es sich auf der Feldbusebene. Linien- oder Bereichskoppler trennen unterschiedliche Bereiche und können auch die übertragenen Telegramme zielgerichtet filtern. Durch diese Selektion wird die Sicherheit bereits teilweise verbessert. Es ist vorteilhaft Geräte unterschiedlicher Sensibilität bezüglich Angriffen auch in unterschiedliche Zonen einzuteilen, da besonders gefährdete Zonen dann besser gesichert und überwacht werden können, als Zonen mit einfachen, nicht derart schützenswerten Teilnehmern.

5.4 Abschirmung sensibler Bereiche

Um sensible Bereiche zu schützen müssen die Busleitungen in diesen besonders gegen Zugriffe gesichert werden. Hierbei ist es wichtig, dass die gesamte Leitung in diesem Segment entsprechend gesichert ist.

Als Beispiel soll ein zugangsbeschränkter Raum dienen, wobei das Betreten von einzelnen Personen geloggt wird und somit jederzeit nachvollziehbar ist, wer sich wann im Raum aufgehalten hat. In diesem Raum sind die Heizungs- und Klimageräte für das gesamte Gebäude verbaut. Diese werden auf Feldbusebene mittels KNX angesteuert. Die Anschlüsse wurden in zusätzlich verschlossenen Schränken gesichert und die Leitung des Bussystems verläuft in einem Stahlrohr abgeschirmt. Der Linienkoppler, der diesen sensiblen Bereich des Busses vom Rest abkoppelt, befindet sich ebenfalls in einem zusätzlich verschlossenen Schrank. Damit ist sichergestellt, dass selbst Personen, denen der Zutritt zum Raum möglich ist, nicht ohne weitere Schlüssel ein Zugriff auf die Busleitung möglich ist. Im Linienkoppler sind die Filter aktiv, sodass auch nur Telegramme von geplanten Teilnehmern empfangen werden. Es ist wichtig den Linienkoppler in diesem besonders gesicherten Raum zu verbauen, dass ein unbefugter Zugriff an der Leitung nicht möglich ist. Dafür wurde die Leitung zusätzlich in einem Stahlrohr abgeschirmt, sodass ein abhören am Kabel, beziehungsweise einfache Manipulationen an diesem ausgeschlossen werden können.

5.5 Einführung eines Whitelisting-Konzepts

Neben den bereits vorgestellten Techniken zur Abwehr von Angriffen ist auch die Möglichkeit der Erstellung und Nutzung von Whitelisting bezüglich der Verteidigung gegen Angriffe möglich. Damit soll es dem potenziellen Angreifer erschwert werden aktiv das System zu beeinflussen. Whitelisting beschreibt das Konzept einer Auflistung von erlaubten Adressen oder auch Teilnehmern. Durch diese Liste kann mittels Lauschen auf dem Bus geprüft werden, ob unerlaubte Teilnehmeradressen auf das System zugreifen, beziehungsweise Telegramme aussenden.

5.5.1 Geräte-Whitelisting

Die Idee in dieser Technik besteht darin, Geräte auf eine Whitelist zu setzen. Das bedeutet, dass alle Geräte am Anfang als bösartig angesehen werden und zuerst auf die Whitelist übernommen werden müssen. Dazu werden die einzelnen physikalischen Adressen der Geräte auf der entsprechenden Liste vermerkt. Sobald ein Gerät über den Bus kommuniziert, welches nicht auf der entsprechenden Liste festgehalten ist, wird ein Alarm ausgelöst. Der Administrator muss dann entsprechend entscheiden, ob es sich um einen erlaubten Teilnehmer handelt, der bisher noch nicht in Erscheinung getreten ist, beziehungsweise noch nicht freigeschaltet wurde, oder ob

es sich um einen möglichen Angreifer handelt. Dann kann ebenfalls entsprechend reagiert werden.

Auf diese Art ist es allerdings nicht möglich zu erkennen, wenn ein Angreifer eine bereits bestehende und tatsächlich vergebene physikalische Adresse nutzt. Um weitere Sicherheit zu bieten, ist es möglich neben der Adresse auch zu vermerken, um welches Gerät es sich handelt und welche Kommunikation für diesen Teilnehmer typisch ist. So kann zum Beispiel davon ausgegangen werden, dass Aktoren in der Regel nicht von sich aus eine Kommunikation beginnen. Sollte zum Beginn also eine Klasse für die physikalische Adresse festgelegt werden, kann bei untypischen Telegrammen des Teilnehmers wiederum ein Alarm ausgelöst werden, welcher dann entsprechend behandelt werden muss.

5.5.2 Erstellung der Whitelist

Dieser Abschnitt fasst unterschiedliche Möglichkeiten zusammen eine derartige Whitelist zu erstellen, und mit unterschiedlichen Informationen zu den einzelnen Komponenten anzureichern.

Nutzung der ETS

Die ETS bietet eine gute Informationsbasis zur Erstellung einer Whitelist. Dieser Software liegt eine Datenbank zugrunde, welche über eine entsprechende Abfrage den Export einer Liste mit Geräten erlaubt. In Abbildung 5.1 ist eine derartige Anfrage zu sehen. Das Ergebnis ist in Tabelle 5.1 dargestellt.

```
1 SELECT     Area.Address AS AreaAddress, Area.Name AS AreaName,
    Line.Address AS LineAddress, Line.Name AS LineName, Device.
    Address AS DeviceAddress, Product.Text AS ProductText, Device.
    Description AS DeviceDescription
2 FROM       Area INNER JOIN
3 Line ON Area.ID = Line.AreaID INNER JOIN
4 Device ON Line.ID = Device.LineID INNER JOIN
5 Product ON Device.ProductID = Product.ID
6 WHERE      Area.ProjectID = 'P-02CD'
7 ORDER BY   Area.Address,Line.Address,Device.Address ASC
8
```

Abbildung 5.1: SQL-Abfrage für die Datenbank, welche von ETS genutzt wird, um eine Geräte-Liste zu erhalten.

Neben den Geräten, die aus der Anfrage extrahiert werden, ist es auch möglich, die angesprochenen Gruppenadressen pro Geräte aus der Datenbank zu extrahieren. Damit kann beispielsweise die zu erwartende Kommunikation besser eingeschätzt werden.

Weiterhin ist zu erwähnen, dass die Filter der Linienkoppler grundsätzlich genau diese Funktion erfüllen. In der ETS kann zur Projektierung nur gewählt werden, ob für bestimmte Adressen der Filter aktiv ist, Telegramme weitergeleitet werden, oder gar komplett gesperrt sind. Eine manuelle differenzierte Steuerung der Filter ist nicht möglich. Durch die vorhandenen Informationen zu den Geräten werden die Filter automatisch von der ETS angepasst. Die Entscheidung kann für folgende Kategorien vorgenommen werden (Beispiel eines Weinzierl KNX LineCoupler 650):

- Gruppentelegramme (Hauptgruppen 0 bis 13)
- Gruppentelegramme (Hauptgruppen 14 bis 31)
- Physikalisch adressierte Telegramme
- Broadcast Telegramme
- Wiederholungssenden von Gruppentelegrammen
- Wiederholungssenden von physikalisch adressierten Telegrammen
- Wiederholungssenden von Broadcasttelegrammen
- Bestätigung (ACK) von Gruppentelegrammen
- Bestätigung (ACK) von physikalisch adressierten Telegrammen

Die Unterscheidung kann dabei in die Richtung Hauptlinie nach Sublinie und umgekehrt getroffen werden.

Neben dem Zugriff auf die Datenbank gibt es auch die Möglichkeit die Diagnosefunktionen zu nutzen. Unter dem Menüpunkt „Diagnose → Physikalische Adressen...“ kann zum einen geprüft werden, ob eine Adresse bereits belegt ist, und es ist auch möglich einzelne Linien auf Teilnehmer abzusuchen. Durch eine zweite Diagnosefunktion („Diagnose → Geräteinfo“) gibt es die Möglichkeit die Informationen von einem Teilnehmer auszulesen. Dabei kann auch geprüft werden, welche Gruppenadressen durch diesen angesprochen werden.

AA	AreaName	LA	LineName	DA	ProductText	DeviceDescription
1	1.Obergeschoss	0	Hauptlinie	NULL	Power supply unit N 125/11 (230V/320mA)	51D1, Spannungsversorgung 320mA, Bereichslinie 3.OG
1	1.Obergeschoss	0	Hauptlinie	0	IP-Router N 146/02	52D2, IP-Router, Bereich 1.OG. IP:10.60.1.36 Mac: 00-0E-8C-00-28-EF
1	1.Obergeschoss	1	UV-AV 1.1 REG	NULL	Power supply unit N 125/11 (230V/320mA)	51D5, Spannungsversorgung 320mA,
1	1.Obergeschoss	1	UV-AV 1.1 REG	0	Line / backbone coupler N 140/03	51D4, EIB Linienkoppler,
1	1.Obergeschoss	1	UV-AV 1.1 REG	1	Binary input device N 262E01	53D1, B-eing. 8-fach 24V Abfragesp, A=Übersp.UV-AV1.1, B=Übersp.UV-SV1.1,
1	1.Obergeschoss	1	UV-AV 1.1 REG	2	Interface N 148/11 USB	53D2, USB-Schnittstelle auf Linie 3.4.0
1	1.Obergeschoss	1	UV-AV 1.1 REG	3	Roller shutter switch N 523/3	27D1, Rolladenaktor 4-fach, A=119 M1,BCD=120 M123

Tabelle 5.1: Resultset für die SQL-Abfrage aus Abbildung 5.1 (AA - AreaAddress, LA - LineAddress, DA - DeviceAddress)

Nutzung von KNXmap

Neben der ETS kann auch die freie Software KNXmap eingesetzt werden, um eine Liste der Busteilnehmer zu erstellen. Dafür sind folgende Befehle nötig:

```
1 knxmap scan 192.168.0.0/24
2 knxmap scan 192.168.0.190 1.1.0-1.1.255
3 knxmap scan 192.168.0.190 1.1.1 --bus-info
```

Mit dem Befehl in der ersten Zeile ist es möglich IP-Schnittstellen zu finden, um so auf den KNX-Bus zuzugreifen. Dafür kann auch ein ganzes Netz in der CIDR-Notation zum Scannen angegeben werden. Hier wurde das lokale Netz

192.168.0.0/24 angegeben. Als Rückgabe wird das KNX-IP-Gateway mit der IP-Adresse 192.168.0.190 und ein paar zusätzlichen Informationen gemeldet. Zeile zwei gibt den Befehl KNX-seitig über das Gateway die Linie 1.1.0 auf Teilnehmer abzusuchen. Der wichtigste Teil der Ausgabe ist dabei als Beispiel in Abbildung 5.2 gezeigt. Im unteren Bereich sind die einzelnen Busteilnehmer aufgelistet. Darüber werden weitere Informationen zum IP-Gateway angezeigt.

```
192.168.0.190
   Port: 3671
   MAC Address: 00:24:6D:00:29:A6
   KNX Bus Address: 1.1.25
   Additional Bus Addresses:
      15.15.250
      15.15.251
      15.15.252
      15.15.253
      15.15.254
   KNX Device Serial: 00C507020B15
   KNX Medium: KNX TP
   Manufacturer: EIBMARKT GmbH
   Device Friendly Name: KNX IP Interface 730
   Device Status:
      Programming Mode: disabled
      Link Layer: disabled
      Transport Layer: disabled
      Application Layer: disabled
      Serial Interface: disabled
      User Application: disabled
      BC DM: 0
   Project Install Identifier: 0
   Supported Services:
      KNXnet/IP Core
      KNXnet/IP Device Management
      KNXnet/IP Tunnelling
   Bus Devices:
      1.1.1
      1.1.2
      1.1.3
      1.1.5
      1.1.6
      1.1.7
      1.1.8
      1.1.9
      1.1.25
      1.1.31

Scan took 18.445719957351685 seconds
```

Abbildung 5.2: Ergebnis des Scans einer KNX-Linie mit dem Tool knxmap.

Mit Hilfe von Zeile 3 lassen sich weitere Informationen zu einzelnen Busteilnehmern auslesen. Durch den Parameter −−bus−info werden die zusätzlichen Informationen angefordert. Die Ausgabe dafür ist in Abbildung 5.3 zu sehen. Durch diese Informationen ist es auch möglich zu sehen, mit welchen Gruppenadressen der Teilnehmer kommuniziert.

```
PS C:\Users\Johannes Goltz\Documents\Universität\Masterarbeit_Lokal\knxmap> knxmap scan 192.168.0.190 1.1.1 --bus-info

Scanning 1 target(s)
Established 1 connections to target 192.168.0.190
BUS: target: 1.1.1
Bus scan took 31.1342716217041 seconds

192.168.0.190
   Port: 3671
   MAC Address: 00:24:6D:00:29:A6
   KNX Bus Address: 1.1.25
   Additional Bus Addresses:
      15.15.250
      15.15.251
      15.15.252
      15.15.253
      15.15.254
   KNX Device Serial: 00C507020B15
   KNX Medium: KNX TP
   Manufacturer: EIBMARKT GmbH
   Device Friendly Name: KNX IP Interface 730
   Device Status:
      Programming Mode: disabled
      Link Layer: disabled
      Transport Layer: disabled
      Application Layer: disabled
      Serial Interface: disabled
      User Application: disabled
      BC DM: 0
   Project Install Identifier: 0
   Supported Services:
      KNXnet/IP Core
      KNXnet/IP Device Management
      KNXnet/IP Tunnelling
   Bus Devices:
      1.1.1:
         Type: System 1 (BCU1)
         Medium: TP1
         Device State:
            Programming Mode: disabled
            Link Layer: ENABLED
            Transport Layer: ENABLED
            Application Layer: disabled
            Serial Interface: ENABLED
            User Application: ENABLED
            BC DM: 0
         Manufacturer: Busch-Jaeger Elektro
         Version: 2
         Properties:
            Device Type: b'6327'
            ManData: b'cb1b1c'
            CheckLim: b'fe'
            User Program: b'05'
            EEPROM_DUMP: b'ffcb1b1c07632722fe040a0000ffe063e01d72b7b7b703110118031804l4fe00fe01fe02fe03fe04fe050206010
7fe08fe09fe0afe0bfe0cfe0dfe0efe0ffe10fe11fe12fe13010002010302040305040605070608070908a090b0a0c0b0d0c0e0d0f0e100f11101
211131214131514161514d0ce9300ce9300ce9300cec300cec300ce9b08cecf08cec708ce9300ced300cec300ced300ced300ced300ced30
0ced300ced300ced300ced300c30000000000b0814df3bf0000660f35d787000000000000000000000000000000000000000000000904d3010b04d40
20d04d61f00547b2d821a021d34a0594421004a0000bd0dde0ada0ad60ae21f05'
            Group Addresses:
               3/0/3
               3/0/4

Scan took 31.1342716217041 seconds
```

Abbildung 5.3: Ergebnis des Scans eines KNX-Teilnehmers mit zusätzlichen Informationen (mit Hilfe von knxmap).

Kapitel 6

Demonstrator

Dieses Kapitel beschreibt die Erstellung eines Beispielszenarios, um eventuelle Angriffe simulieren zu können und auch die möglichen Verteidigungsmaßnahmen zu testen beziehungsweise am Beispiel beschreiben zu können.

6.1 Strukturierung und Zonenbildung

Zunächst soll eine Zonenbildung betrachtet werden. Diese sollte sich zumindest im Groben an aktuellen Gebäudeautomationssystemen orientieren, um ein Ergebnis zu liefern, welches möglichst nah an dem realen Umfeld liegt. Im Kapitel 2.2 wurden bereits einige Möglichkeiten vorgestellt, wie Zonen sinnvoll gebildet werden können. Dies sollte auch als Empfehlung für die Erstellung von neuen Netzen genutzt werden. Die Bildung der Zonen nach Sicherheitsaspekten wird voraussichtlich zu abweichenden Ergebnissen führen, als eine Konzeption nach Menge der zu verwendenden Leitungen und Leitungslängen.

Im Beispielszenario sollen folgende Komponenten verbaut werden:

- Linienkoppler
- Taster
- Aktor
- Netzteil

- Präsenzmelder

Damit ist es möglich ein kleines Experiment nachzubauen, in dem eine Lampe (Aktor) via Bewegungsmelder und/oder Taster ein- beziehungsweise ausgeschaltet wird. Zusätzlich sollen die Elemente auf unterschiedlichen Linien liegen. Dies spiegelt auf der einen Seite die Umsetzung in großen Projekten wieder, wie dem des Konrad-Zuse-Hauses der Informatik an der Universität Rostock, und zum anderen lässt sich so prüfen, welche Daten Linienkoppler mit gesetzten Filtereinstellungen weiterleiten. Die Aufteilung wurde wie in Abbildung 6.1 gezeigt vorgenommen.

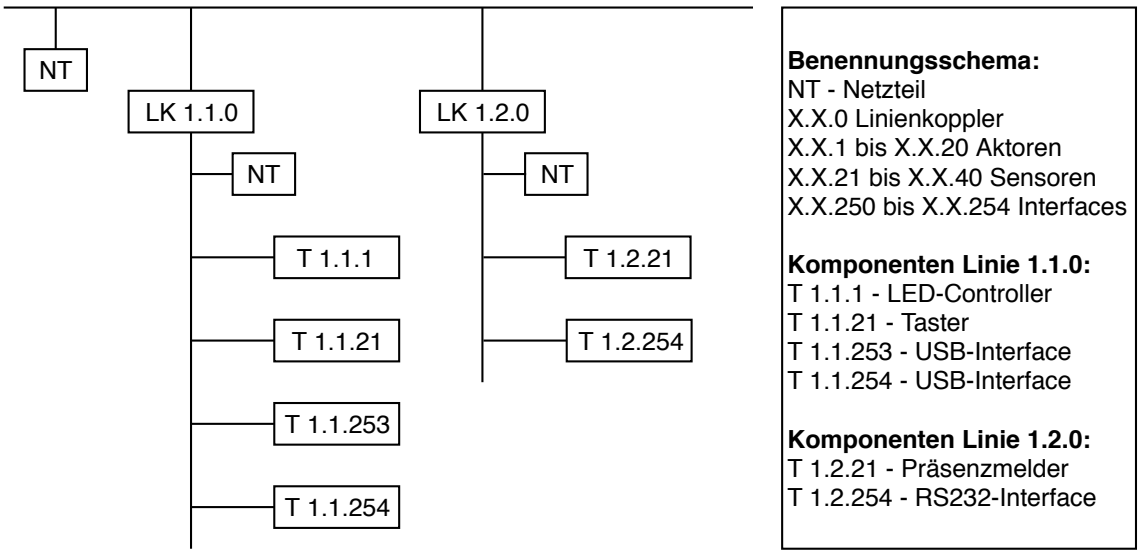

Abbildung 6.1: Planungszeichnung zum Aufbau des Experiments

In Abbildung 6.2 ist der Experimentalaufbau als Fotografie zu sehen. Die Bauteile sind entsprechend unter der Abbildung beschrieben. Der zugehörige Vierfach-Taster ist neben dem Schaltschrank verbaut, während der Bewegungsmelder unterhalb befestigt ist. Der LED-Stripe ist ebenfalls außerhalb des Schaltschranks installiert und wird durch den Taster oder den Bewegungsmelder geschaltet. Die oberen beiden Taster dienen zum Ein- beziehungsweise Ausschalten, während mit dem zweiten Tasterpaar von oben zusätzlich ein Dimmen möglich ist.

Abbildung 6.2: Schaltkasten für den Demonstrator (ohne Schaltaktor und Bewegungsmelder)
Bauteile von oben nach unten und links nach rechts: 12-Volt-Netzteil für LED-Stripe, serielle Schnittstelle, KNX-Netzteil, Linienkoppler, KNX-Netzteil, Linienkoppler, Raspberry mit USB zu KNX-Schnittstelle, 12-Volt-Netzteil für Raspberry, KNX-Netzteil mit USB-Schnittstelle, Schaltaktor für LED-Stripe

6.2 Projektierung mit Hilfe der ETS

Ausgangspunkt für die Konfiguration von Gebäudeautomationsnetzen mit dem KNX-Bussystem ist die ETS. Hier werden die Komponenten den entsprechenden Adressen zugeordnet und mit den anderen Geräten verknüpft.

Abbildung 6.3 zeigt die klassische Ansicht der ETS4 mit einem geöffneten Projekt. Auf der linken Seite wird die hierarchische Strukturierung des Gebäudes angezeigt. In diesem Bereich lassen sich die Komponenten auch nach Adresstopologie sortieren oder die Gruppenadressen anzeigen. Die rechte Seite stellt detaillierte Informationen zu einzelnen Geräten dar. Dort kann beispielsweise auch die physikalische Adresse eingestellt werden. Im Hauptarbeitsbereich werden alle Geräte innerhalb eines Gebäude- oder Adressbereichs angezeigt. Wenn ein neues Gerät in einem Projekt eingepflegt wird, muss zuerst die KNX-Produkt-Datei vom Hersteller heruntergeladen und importiert werden. Dies ermöglicht es, alle Parameter der Komponente korrekt zu konfigurieren. Die Darstellung dieser Parameter zu einzelnen Geräten kann auch im Hauptfenster erfolgen. In den Parametern für den in Abbildung 6.4 dargestellten 3-fach-Taster kann so beispielsweise gewählt werden, ob „Wippe A“ als „Tastenpaar“, „gesperrt“ oder als „einzelne Tasten“ genutzt werden soll. Bei der Funktion „gesperrt“ haben die Tasten keine Funktion und sind unbelegt. „Tastenpaar“ bildet einen klassischen Schalter nach, wobei eine Seite des Tasters „Ein“ darstellt und die andere Seite entsprechend „Aus“. Werden die Tasten der Wippe A als „einzelne Tasten“ konfiguriert, kann mit beiden Tasten eine völlig andere Aktion ausgelöst werden. Je nach Einstellung der Parameter passen sich auch die entsprechenden Kommunikationsobjekte der Teilnehmer an.

Zuerst bietet es sich an die Struktur des zu planenden Gebäudes abzubilden und die Räume, sowie Schaltschränke dafür anzulegen. Im nächsten Schritt sollten die Gruppenadressen angelegt werden, über die die Kommunikation der einzelnen Komponenten abgewickelt wird. Die Hauptgruppen sollten dabei die unterschiedlichen Gewerke (wie Beleuchtung, Jalousien, Heizung, ...) abbilden. Mittelgruppen können sehr gut für unterschiedliche räumliche Strukturierung genutzt werden, während die Adresse an sich für einzelne Bauelemente benötigt wird. Je nach verwendeten Komponenten müssen unterschiedlich viele Adressen angelegt werden.

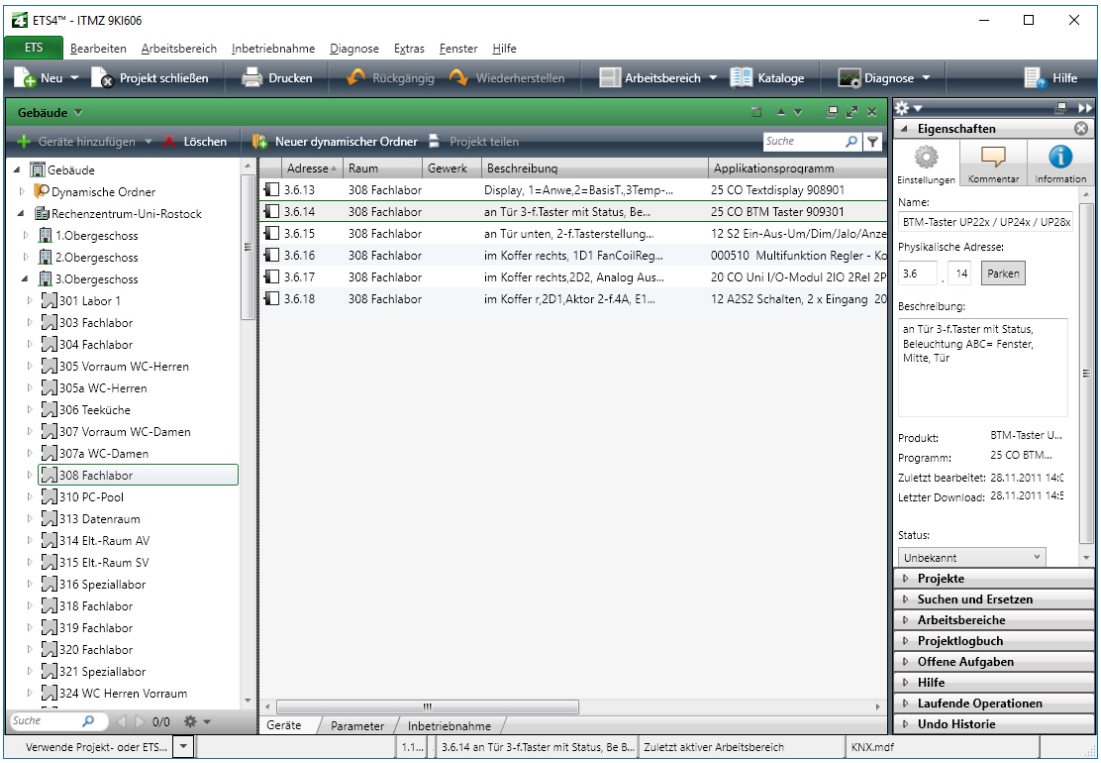

Abbildung 6.3: ETS4 mit geöffnetem Projekt und Darstellung der Geräte in einem zugeordneten Raum

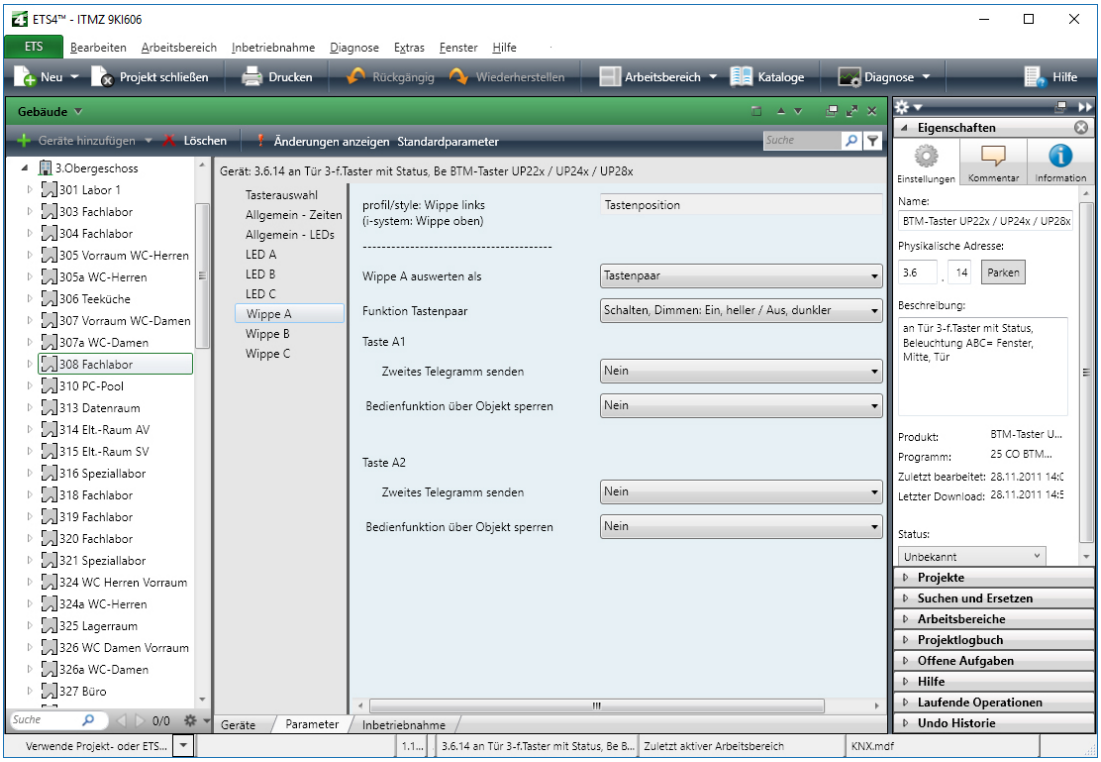

Abbildung 6.4: ETS4 mit geöffnetem Projekt und Darstellung der Parameter eines Gerätes (Taster)

Lampen benötigen zum Beispiel drei bis fünf Gruppenadressen. Diese erfüllen folgende Aufgaben:

- Schalten
- Wert
- Rückmeldung Schalten
- Dimmen
- Rückmeldung Wert

Die letzten beiden Adressen werden nur benötigt, wenn es sich um eine dimmbare Lampe handelt. Grundsätzlich sieht man in den Parametern der Komponenten, welche Kommunikationsobjekte verknüpft werden können, beziehungsweise wird die Menge der vorhandenen Kommunikationsobjekte immer nach der vorgenommenen Parametrisierung angepasst. Bei Schaltern ist es zum Beispiel möglich, diese als Wippe oder einzelne Tasten zu konfigurieren. Mit der Nutzung als Wippe werden immer zwei Tasten zu einem Paar zusammengefasst. Daher muss dann nur ein Kommunikationsobjekt der Gruppenadresse zugeordnet werden. Bei der Konfiguration als Tasten ist dies für jede Taste einzeln nötig, wodurch allerdings die Möglichkeit besteht, mehr Funktionen schalten zu können.

Nach dem Hinzufügen der Geräte und der Verknüpfung über die Gruppenadressen müssen die entsprechenden Daten noch auf die Geräte geladen werden. Neben einem USB-Gerät kann dazu auch eine KNX/IP-Schnittstelle genutzt werden. Um die physikalischen Adressen zu programmieren, muss der Programmierknopf auf dem Gerät gedrückt werden. Applikationsprogramme können auch ohne die Betätigung dieser Taste auf das Gerät geladen werden. Wurden alle Geräte erfolgreich eingerichtet, kann die Zusammenstellung getestet werden.

Neben der Einrichtung von Komponenten und der Konfiguration eignet sich die ETS auch zum Auffinden von Fehlern in bestehenden Installationen. Dazu kann Busverkehr aufgezeichnet und auch erneut abgespielt werden, um eventuelle Fehler aufzudecken.

Im Demonstrator wurden Linienkoppler vom Hersteller Weinzierl (KNX Line-Coupler 650) verbaut. Diese bieten jeweils einen Taster zur zeitweisen Abschaltung

der Filterung und damit Weiterleitung der Gruppentelegramme oder auch von Telegrammen mit individuellen Adressen. Dies war auch bei der Programmierung nötig. Die Einstellung der Koppler wurde so gewählt, dass physikalisch adressierte Telegramme nicht weitergeleitet werden. Damit konnte zwar die Adresse auf die Teilnehmer geladen werden, danach konnte die ETS allerdings die Teilnehmer nicht mehr erreichen, da der USB-Zugang auf Linie 1.1.0 genutzt wurde. Eine Deaktivierung mit den Tastern zur Weiterleitung der Telegramme mit physikalischen Adressen sorgte für eine problemlose Programmierung der Teilnehmer.

Durch den Demonstrator ist es möglich Testdaten eines KNX-Bussystems zu sammeln, die ohne Personenbezug entstanden sind. Diese Daten können daher für Experimente genutzt werden, ohne dass Rückschlüsse auf personenbezogene Daten möglich sind.

Kapitel 7

Zusammenfassung und Ausblick

Dieses Kapitel fasst abschließend die Ergebnisse der Arbeit zusammen. Weiterhin werden offenen Forschungsfragen aufgezeigt, welche sich während der Bearbeitung des Themas ergeben haben.

7.1 Zusammenfassung

In der Arbeit wurden neben den Grundlagen zum Bussystem KNX auch die Techniken der IP-Welt zur Sicherung von Infrastrukturen betrachtet. Dies liegt vor allem daran, dass die Sicherheitsansprüche in IP-basierten Netzen im Normalfall deutlich höher sind, da diese großflächiger vernetzt sind, während Bussystem in der Regel wenig bis keine Netzübergänge bieten sollten. Die dort vorhandenen Techniken und Methoden müssen für die Nutzung in den Bussystemen angepasst und adaptiert werden. Dabei wurden vor allem die Bildung von Netzzonen und die Einschätzung von Risiken in dieser Arbeit näher betrachtet.

Um diese Bereiche allerdings genauer zu beleuchten, sollte vorab auch die Seite der Angreifer untersucht werden. Hierbei wurde zuerst eine Auswahl an möglichen Angriffen gesammelt und im weitere wurden Möglichkeiten vorgestellt, diese entsprechend zu klassifizieren. Das Problem dabei besteht vor allem darin, dass eine allgemeingültige Klassifizierung nur sehr schwer zu erreichen ist und es nicht möglich ist, alle Seiten eines Angriffs genau zu betrachten. Häufig ist eine spezifischere Betrachtung nötig. Ein kurzes Beispiel soll dies verdeutlichen. Betrachtet man den Angriff des Mitschneidens von Telegrammen näher, so kann dies als ein

Angriff mit geringem bis mittlerem Schadpotenzial betrachtet werden, da der Angreifer lediglich abstrakte Daten gewinnt. Sollte der Durchführende des Angriffs jedoch über entsprechendes Hintergrundwissen verfügen, um Adressen konkrete Orte zuordnen zu können, so kann er mit dem Mitschnitt aus den Telegrammen sogar Bewegungsprofile ableiten. Dies stellt ein sehr hohes Schadpotenzial dar, da diese Daten beispielsweise das Verhalten von einzelnen Personen offenbaren, was unbedingt schützenswert ist.

Im weiteren wurde eine Möglichkeit der Messung des Risikos vorgestellt. Das Risiko wurde dabei in statisch und dynamisch eingeteilt, um neben der Betrachtung zum Installationszeitpunkt auch die Live-Situation einschätzen zu können. Selbstverständlich ist auch eine Kombination beider Teilwerte nötig. Damit soll beispielsweise die einfache Darstellung von Risiken in Form einer Heatmap möglich sein. Dies bringt den Vorteil, besonders gefährdete Bereiche schnell visuell erkennen zu können und auch Veränderungen im laufenden Betrieb einfach einzusehen. Problematisch könnte allerdings sein, dass eventuell Angriffe auftreten, die so vorher gar nicht bedacht wurden und daher auch ein möglicher Vektor bei der Betrachtung des Risikos nicht mit eingeflossen ist. Die Verknüpfung der Teilnehmer über die Gruppenadressen wurde bei der Einschätzung ebenfalls bisher noch nicht berücksichtigt. Angreifern ist es daher aktuell möglich eine Absenderadresse eines Teilnehmers zu spoofen und damit Telegramme unbemerkt an andere Teilnehmer zu senden, die mit diesem Gerät verknüpft sind. Derartige Angriffe werden auch von Linienkopplern nicht verhindert, da dieser Kommunikationsweg regulär vorgesehen ist. Zumindest wenn die gestohlene Absenderadresse an die entsprechenden Gruppenadressen senden darf. Eine Aussendung von Telegrammen an physikalische Adressen kann trotzdem unterbunden werden. Es können also weiterhin Angriffe auftreten, die so nicht detektiert werden können. Das statische Risiko soll dies teilweise abfedern, indem eine gute Netzsegmentierung und enge Einstellung der Filter für Linienkoppler mit einem geringeren Risiko einhergehen. Wie bereits beschrieben ist hier allerdings die Verknüpfung mit den Gruppenadressen noch nicht beachtet worden.

Ebenfalls zu bedenken ist, dass bei der Neukonfiguration von Komponenten oder der Installation neuer Teilnehmer im Bussystem auch die Werte für die statischen Risiken wieder angepasst werden müssen. Dabei gilt es zu beachten, dass dies auch

bei der Änderung von Zugangskontrollsystemen beachtet werden muss.

Neben der Einschätzung von Angriffen und der Möglichkeit ein Risiko in einem Bussystem messbar zu machen wurden in Kapitel 5 zusätzlich Möglichkeiten vorgestellt sich gegen derartige Angriffe zu schützen. Beachtung fand vor allem die Erstellung von neuen Bussystemen im Sinne einer sinnvollen Segmentierung des Netzes und des Schutzes von sensiblen Leitungen. Hierfür wurde auch ein Demonstrator entworfen und die entwickelten Konzepte praktisch umgesetzt. Dabei wurde eine Segmentierung in verschiedene Linien mit unterschiedlichen Teilnehmern betrachtet. Somit ist es möglich, die Filterung von Telegrammen genauer untersuchen zu können. Die praktische Umsetzung von KNX-Projekten mit der ETS wurde durchgeführt, um weitere Probleme in der Praxis aufdecken zu können.

Über den Kern der Arbeit hinaus wurde die Feststellbarkeit von Angriffen durch die Überwachung vom Busverkehr angedacht. An den entsprechenden Stellen verweist die vorliegende Arbeit auf relevante und weiterführende Literatur.

7.2 Offene Fragestellungen

Dieses Kapitel zeigt weiterführende Forschungsfragen auf, die im Zuge der Arbeit entstanden sind.

Eine wichtige Fragestellung bezieht sich auf die Zusammenstellung und Katalogisierung von Angriffen. Hierfür kann beispielsweise die Bewertung der Angriffe nach dem Common Vulnerability Scoring System (CVSS) genutzt werden. Der Vorteil wäre dabei, dass dieses System bereits in der IP-basierten Netzwelt etabliert ist und so auch die Anbindung an entsprechend weitere Tools gegeben wäre. Eine zentrale Sammlung von Angriffen wäre wichtig um Angriffe anhand von Mustern erkennen zu können. Damit könnten Intrusion Detection Systeme nicht nur anhand von Machine-Learning-Algorithmen Anomalien detektieren, sondern auch nach bekannten Angriffssignaturen suchen.

Das Problem mit dem persönlichen Bezug der aufgezeichneten Daten erschwert es, ebenfalls einen öffentlichen Testdatensatz bereitzustellen. Dieser könnte neben

dem regulären Busverkehr auch um Angriffe angereichert werden, sodass es möglich wird, Intrusion Detection Systeme zu trainieren, zu testen und einen Benchmark zu entwickeln. Für die Veröffentlichung von gesammelten Daten aus einer realen Automationsanlage könnte eine Anonymisierung der Daten untersucht werden. Es reicht allerdings nicht aus einfach die Adressen auf OSI-Layer 3 zu verwerfen, wenn man annimmt, dass User oder Geräte darüber identifizierbar seien. Dadurch könnte es dazu kommen, dass die Daten für die Auswertungen nicht mehr sinnvoll nutzbar sind. Ein besserer Ansatz könnte der Crypto-PAn-Algorithmus sein. IP-Adressen können darüber beispielsweise zu anonymen Subnetzen zusammengefasst werden. Dadurch wird die Privatheit erhöht und zugleich fallen nur möglichst wenig Daten für eine Auswertung weg [HCT+14]. Zu untersuchen ist dabei, ob die Anonymisierung auf der einen Seite ausreicht um die Erstellung von Bewegungsprofilen oder die Ableitung von Nutzerverhalten vereitelt und auf der anderen Seite noch genügend Raum gibt, um Verteidigungssysteme zu testen und entsprechend sinnvoll einzusetzen.

Durch die starke Verbindung zur ETS und der im Hintergrund arbeitenden Datenbank ist eine Verbindung der Analyse schon zum Zeitpunkt der Projektierung denkbar. So könnte der Ersteller bereits während der Arbeit auf eventuell sicherheitskritische Planungen hingewiesen werden. Alternativ ist eine Prüfung am Ende der Projektierungsphase denkbar. Sollte es hier auch die Möglichkeit geben, Gebäude und Netzpläne einzubinden, könnte eine ganzheitliche Planung von Sicherheitszonen ermöglicht werden, die auch eine gute Visualisierung für den Planer erlaubt. Dies bietet vor allem den großen Vorteil, dass die Erstellung eines Zonenkonzepts auch von Personen ohne umfangreiche Fachkenntnisse in diesem Bereich umgesetzt werden kann.

Ein weiteres interessantes Problem könnte die Untersuchung sein, ob sich das Problem der Planung eines derartigen Bussystems auf ein Graphenproblem abbilden lässt. Die Lösbarkeit des Problems, und auch das Finden einer optimalen Lösung, ist mit der Einschränkung einiger Parameter eine interessante Fragestellung. Vor allem mit dem Hintergrund die Planung der Zonen und Filterregeln nach Sicherheitsaspekten zu optimieren.

Literaturverzeichnis

[Ass13] Association, K. N.X.: *Grundlagenwissen zum KNX Standard.* https://www.knx.ch/knx-chde/wdownload-d/Flyer/Endkunden/Grundlagenwissen_zum_KNX_Standard_German.pdf, 2013. zuletzt aufgerufen am 23.04.2018 - 12:56 Uhr.

[BSI17] BSI: *Risikoanalyse auf der Basis von IT-Grundschutz (BSI 200-3).* Standard, 2017. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/standard_200_3.pdf?__blob=publicationFile&v=5.

[Bun16] Bundesamt für Sicherheit in der Informationstechnik (Herausgeber): *IT-Grundschutz-Kataloge.* Bonn, 15. Auflage, 2016. zuletzt aufgerufen am 29.03.2018 - 16:00 Uhr.

[DIN04a] DIN: *Elektrische Systemtechnik für Heim und Gebäude (ESHG) - Teil 4-1: Medienunabhängige Schicht - Anwendungsschicht für ESHG Klasse 1; Deutsche Fassung EN 50090-4-1:2004, Text Englisch*, Juni 2004.

[DIN04b] DIN: *Elektrische Systemtechnik für Heim und Gebäude (ESHG) - Teil 4-2: Medienunabhängige Schicht - Transportschicht, Vermittlungsschicht und allgemeine Teile der Sicherungsschicht für ESHG Klasse 1; Deutsche Fassung EN 50090-4-2:2004, Text Englisch*, Juni 2004.

[DIN04c] DIN: *Elektrische Systemtechnik für Heim und Gebäude (ESHG) - Teil 5-2: Medien und medienabhängige Schichten Netzwerk basierend auf ESHG Klasse 1, Zweidrahtleitungen (Twisted Pair);Deutsche Fassung EN 50090-5-2:2004, Text Englisch*, September 2004.

[DIN09] DIN: *Elektrische Systemtechnik für Heim und Gebäude (ESHG) - Teil 3-3: Anwendungsaspekte - ESHG-Interworking-Modell und übliche ESHG-Datenformate; Englische Fassung EN 50090-3-3:2009*, September 2009.

[DIN16] DIN: *Gebäudeautomationssysteme - Teil 2: Hardware (ISO/DIS 16484-2:2016); Deutsche und Englische Fassung prEN ISO 16484-2:2016*, 2016.

[GKNP06] Granzer, Wolfgang, Wolfgang Kastner, Georg Neugschwandtner und Fritz Praus: *Security in Networked Building Automation Systems*. Factory Communication Systems, Seiten 283–292, 2006.

[GW17] Gregory-Brown, Bengt und Doug Wylie: *Securing Industrial Control Systems 2017*. `https://www.sans.org/reading-room/whitepapers/analyst/securing-industrial-control-systems-2017-37860`, 2017. zuletzt aufgerufen am 27.03.2018 - 9:40 Uhr.

[HCT+14] Hofstede, Rick, Pavel Celeda, Brian Trammell, Idilio Drago, Ramin Sadre, Anna Sperotto und Aiko Pras (Herausgeber): *Flow Monitoring Explained: From Packet Capture to Data Analysis With NetFlow and IPFIX*, Band 16. IEEE, 2014.

[Jun18] Jung, Maximilian: *Aufzeichnung und Analyse von Netflows in Feldbus-Netzwerken*. Bachelorarbeit, Universität Rostock, März 2018.

[KNX] KNX Association: *KNX Grundkurs - 02_ Bus-Teilnehmer*. `http://knx-prog.de/files/02_Bus-Teilnehmer_G1213b.pdf`. zuletzt aufgerufen am 04.04.2018 - 11:00 Uhr.

[MDS14] Mundt, Thomas, Andreas Dähn und Stephan Sass: *An Intrusion Detection System with Home Installation Networks*. In: *University of Bahrain : Scientefic Publishing Center (Hg.) 2014 – International Journal of Computing*, Band 3, Seiten 13–20. 2014.

[MHH09] Merz, Hermann, Thomas Hansemann und Christof Hübner: *Gebäudeautomation: Kommunikationssysteme mit EIB/KNX, LON und BACnet*. Carl-Hanser-Verlag, München, 2. Auflage, 2009.

[MW16] Mundt, Thomas und Peter Wickboldt: *Security in building automation systems - a first analysis*. In: *2016 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, Seiten 1–8, Piscataway, NJ, 2016. IEEE.

[Nor05] Northcutt, Stephen: *Inside network perimeter security*. Sams Pub, Indianapolis, Ind, 2. Auflage, 2005.

[Pet18] Peters, Martin: *Analysis of Distributed In-Band Monitoring Messages for Field Bus Networks in Building Automation Systems.* Masterarbeit, Universität Rostock, März 2018. `https://github.com/FreakyBytes/master-thesis/releases/download/handing-in/master-thesis-peters.pdf`, zuletzt aufgerufen am 03.04.2018 - 10:45 Uhr.

[QZCZ04] Quittek, J., T. Zseby, B. Claise und S. Zander: *Requirements for IP Flow Information Export (IPFIX).* RFC 3917, RFC Editor, Oktober 2004. `https://www.ietf.org/rfc/rfc3917.txt`.

[SHS17] Sokollik, Frank, Peter Helm und Ralph Seela: *KNX für die Gebäudesystemtechnik in Wohn- und Zweckbau.* VDE Verlag GMBH, Berlin und Offenbach, 6. Auflage, 2017.

[SSS+10] Sperotto, Anna, Gregor Schaffrath, Ramin Sadre, Cristian Morariu, Aiko Pras und Burkhard Stille: *An Overview of IP Flow-Based Intrusion Detection.* IEEE Communications Surveys and Tutorials, 12(3):343–356, 2010.

Anhang A

Datenträger

Selbständigkeitserklärung zur Masterarbeit

Ich, Johannes Goltz, erkläre, dass ich die vorliegende Arbeit zum Thema „*Sicherheitsanalyse von Gebäudeautomationsnetzen auf Feldbusebene am Beispiel von KNX*“ selbständig und nur unter Vorlage der angegebenen Literatur und Hilfsmittel angefertigt habe.

Rostock, 26. April 2018

Ort, Datum

Unterschrift