UNIVERSITÄT SALZBURG

Seminararbeit

Sicherheits-Aspekte in der Gebäude-/Hausautomatisierung

Masterstudiengang Angewandte Informatik
Seminar aus Informatik
Institut für Computerwissenschaften
Universität Salzburg

vorgelegt von
Ulrich Schrittesser

Studiengangs Leiter: Univ.-Prof. Mag. Dr. Helge Hagenauer
Betreuer: Univ.-Prof. DI. Dr.techn. Wolfgang Pree

Salzburg, Juli 2011

Inhaltsverzeichnis

Inhaltsverzeichnis 2

1. Einleitung 3

1.1. Gebäude-/Hausautomatisierung 3
1.2. BA-Protokolle/Standards 4
1.3. Sicherheit allgemein 5

2. Fragestellung/Problematik 7

3. State of the Art 9

3.1. Offene BAS-Protokolle 9
3.2. Sicherheitsbezogene Gegenüberstellung offener BAS-Protokolle 11

4. Ansätze/Lösungen 13

4.1. Vier-Phasen-Ansatz 13
4.2. EIBsec 14
4.3. Multiprotokoll-Ansatz 15

5. Zusammenfassung/Ausblick 18

Literaturverzeichnis 19

1. Einleitung

1.1. Gebäude-/Hausautomatisierung

Building Automation Systems (BAS) bzw. *Home Automation Systems* (HAS) oder auf Deutsch Gebäude- (GBA) bzw. Hausautomation (HA)[1] verbindet alles was im Gebäude/Haus mit Elektrik zu tun hat und gliedert sich im Wesentlichen in 3 Ebenen - namentlich nach Abbildung 1 in Management-, Automatisations- und in die Feldbusebene. Bussysteme werden aber nicht nur in Großgebäuden oder in der industriellen Automatisierung verwendet, sondern finden zunehmend in Ein- bis Mehrfamilienhäusern, zumindest im gehobenen Bereich, Einsatz.

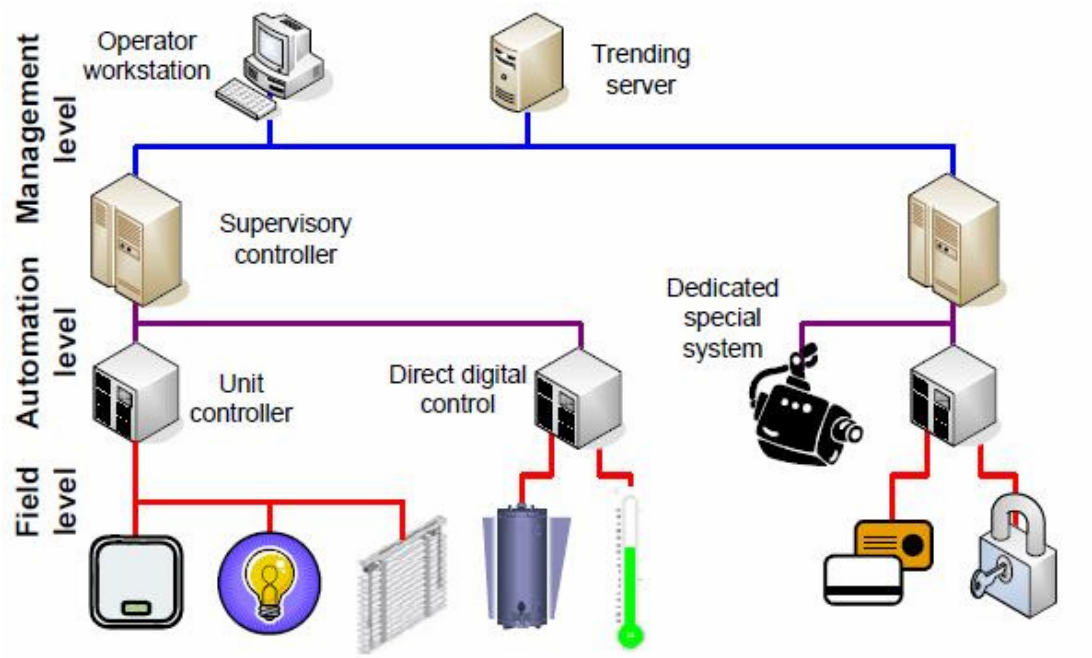

Abbildung 1: BAS-Schichten und Anwendungen [1]

Über diese Schichten verteilen sich verschiedenste Anwendungsbereiche, welche sich wie folgt grob unterteilen:

Energie & Komfort:

Heizung, Lüftung und Klima (HLK), Wasser, Beleuchtung, Jalousie/Sonnenschutz, Energie- und Lastmanagement, Kommunikation, Entsorgung, Gebäudeüberwachung

Safety & Security:

Feuer, Alarm, Einbruch, Zugang, Video, Evakuierung, Notstrom, etc.

Wobei die Heizungs-, Lüftungs-, Klima- und die Licht- bzw. Beschattungstechnik die Hauptanwendungen in der Gebäudeautomatisierung stellen [6].

[1] Im gesamten Dokument wird BA anstelle von GBA verwendet, wobei gleichzeitig GBA = HA gilt

1.2. BA-Protokolle/Standards

Zu den 3 Ebenen gibt es in der BA eine Vielzahl an Protokollen von denen wenige über alle Ebenen hinweg sämtliche Anforderungen erfüllen.

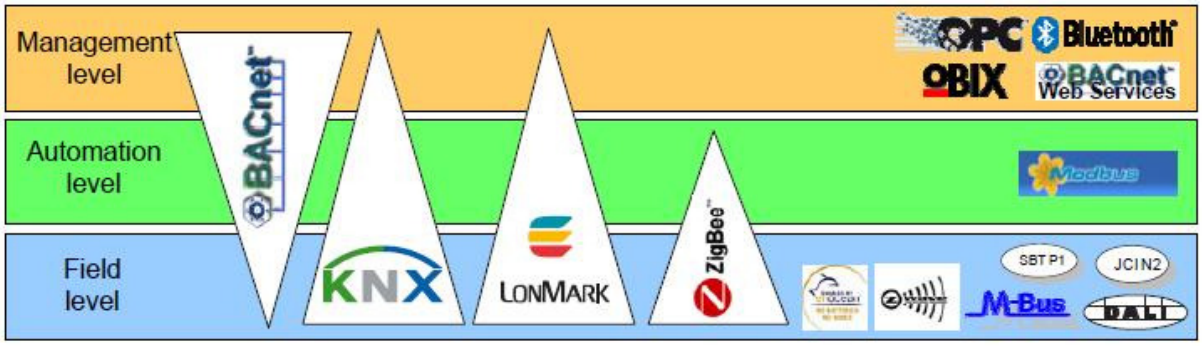

Abbildung 2: BAS-Schichten und Protokolle [1]

Eine grobe Unterteilung kann in Kabelgebunden und Kabellos vorgenommen werden.

Kabelgebunden:

Digital Adressable Lighting Interface (DALI) wird rein für Lichtsteuerungen und der *Meter-Bus* (M-Bus) für Strommessung verwendet, während *Modbus* die Kommunikation auf Automationsebene zwischen *Programmable Logic Controllers* (PLCs) und *Direkt Digital Controllers* (DDCs) herstellt. Diese drei Standards berücksichtigen aber keine Sicherheitsmechanismen und werden nicht weiter erläutert.
Sowohl *Building Automation and Control Network* (BACnet), KNX (Weiterentwicklung vom *Europäischen Installationsbus* – EIB) als auch LonWorks (*Local Operating Network* – LON) stellen in der BA offene Protokolle auf allen drei Ebenen dar. KNX als auch die LON-Technologie entstammen aus der Feldbusebene während der BACnet Standard aus der Managementebene bzw. als Klimatechnologie entstand.
Des Weiteren gibt es Powerline Technologien wie den X10 Standard worin BA-Geräte über das Stromkabel angesprochen und gesteuert werden können. Dieser Standard hat sich speziell in Amerika im Smart Home Bereich etabliert und findet zunehmend in Europa Anwendung, hat aber keine Sicherheitsfeatures [2].

Kabellos:

Die *EnOcean GmbH* aus München nutzt für deren Sensoren Energie-Harvesting bzw. Solar Technologien um autark ohne Batterien zu arbeiten. Aufgrund dieser maximalen Energieeffizienzausnutzung werden in der EnOcean-Funktechnologie keine Sicherheitsmechanismen unterstützt.
Z-Wave nutzt ein proprietäres Sicherheitskonzept und Bluetooth wird meist als kabelloses Verbindungsmedium zu Controllern verwendet. Diese Funktechnologien stehen in direkter Konkurrenz zum offenen Zigbee Funkstandard welcher in dieser Arbeit auf dessen Sicherheitsmechanismen näher untersucht wird.

Auf der Management Ebene finden sich Protokolle wie *Object Linking and Embedding* (OLE) *for Process Control* (OPC) bzw. die neueste Spezifikation *OPC Unifed Architecture* (OPC UA), als auch der *Open Building Information eXchange* (oBIX) Standard und BACnet Web Services (BACnet/WS) allesamt als offene Standards wieder. OPC ist in der Industrieautomatisierung weit verbreitet und wird zunehmend in der Gebäudeautomatisierung angewandt.

Aus der Menge an BA-Protokollen wird folglich sicherheitstechnisch rein auf die offenen Standards wie BACnet, LONWorks, KNX, OPC-UA oder auch Zigbee weiter eingegangen, da die meisten geschlossenen/proprietären Systeme derzeit ohnehin nach dem Prinzip „Security by Obscurity“ arbeiten.

1.3. Sicherheit allgemein

Sicherheit, insbesondere die Informations- bzw. Netzwerksicherheit hat zum Ziel die Vertraulichkeit, Verfügbarkeit und die Integrität von Informationen in System in einem ausreichenden Maß sicherzustellen. Nach Tabelle 1 wird in vielen Fällen die Authentizität als Spezialform der Integrität angefügt, welche die Echtheit und Zurechenbarkeit der Daten garantiert.

Sicherheit	**Safety**
Schutz gegen beabsichtigte Angriffe	Schutz vor unbeabsichtigten Ereignissen
Vertraulichkeit • Abhörsicherheit • gegen unbefugten Gerätezugriff • Anonymität Integrität • Übertragungsintegrität • Korrektheit der Daten Authentizität • Spezialform Integrität • Digitale Signatur / Datenurheber • Zurechenbarkeit Verfügbarkeit • Ermöglichen der Kommunikation	Fehlertoleranz Verfügbarkeit • Funktionssicherheit • Technische Sicherheit • Schutz vor Überspannung, Überschwemmung, Temperaturschwankungen etc. • Schutz vor Spannungsausfall Fail Safe / Fail Passive / Fail Operational

Tabelle 1: Sicherheit vs. Safety

Sicherheit ist nicht gleich Sicherheit (Security != Safety). Vielmehr ist Security eine *Precondition* von Safety. Eine systemtechnische Unterscheidung erfolgt in *Safety-critical* (Feuer- oder Alarmsysteme) und *Security-critical* (Einbruchmelde- oder Zutrittskontroll-systeme) Systeme, welche zumeist als proprietäre *stand-alone* Systeme angeboten werden. Zugleich stellt die Integration bzw. Fusion von Security und Safety eine der aktuellsten Forschungsthematiken in der BA dar [3][6].

Grundsätzlich werden notwendige Sicherheitsanforderung in der *Informations- und Kommunikationstechnologie* (*IKT*) Welt von außen nach innen - vom physischen Medium über das Netzwerk auf den Computer, über die Applikation auf die Hardware ausgearbeitet

und entsprechende Sicherheitsstrategien angewendet. D.h. am Beispiel einer Sicherheitsstrategie vom Unternehmen Cisco für die Industrie-Automatisierung beginnend von IPsec Verschlüsselung, *Secure Socket Layer* (SSL) und *Virtuelle Private Netzwerke* (VPNs) über Authentifizierung, *Access Control Listen* (ACL) und *Intrusion Prevention/Detection Systemen* (IPS/IDS), über Applikations-Sicherheit bis hin zur geswitchten Ebene in der die Kommunikation über *Virtual Local Area Network* (VLAN)-Technologien passiert [4].

.

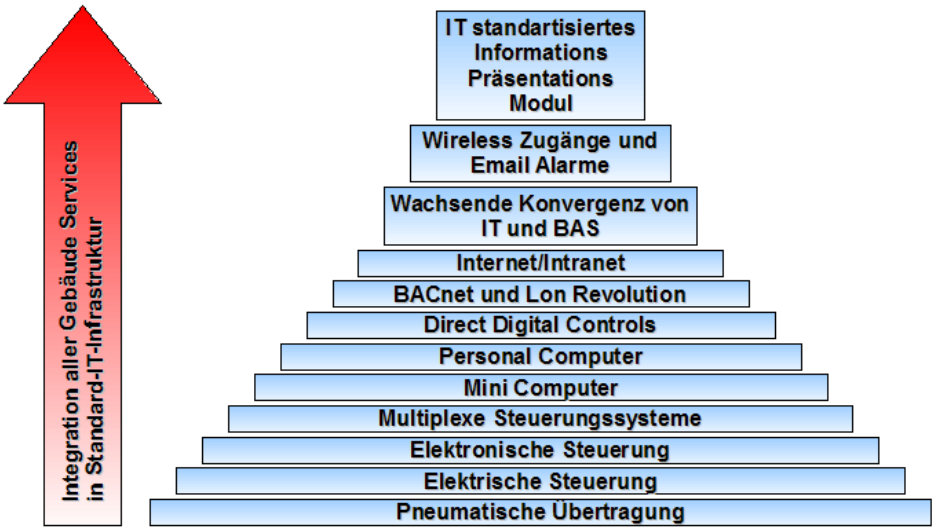

Abbildung 3: BAS Evolution [5]

Obige Strategie muss nach Abbildung 3, welche pyramidenhaft die Entstehungsgeschichte von BAS zeigt, überdacht werden. Zuerst gab es einfache elektrische Geräte die in geschlossenen Systemen miteinander kommunizierten. Wogegen in den letzten Jahren die BA zunehmend mit der IT verschmilzt, welche mittlerweile bis auf die Sensor-/Aktoren-Ebene Einzug hält.
Am optimalsten wäre alles auf den heutigen IT-Standard zu heben oder ein *all-in-one* BAS zu realisieren, das alle Services miteinander auf einen Standard vereint bzw. sämtliche Anwendungsdomänen und Sicherheitsmechanismen beinhaltet. Dies wird in verschiedenen Fällen angewendet, ist aber aufgrund der langlebigen Verwendung von BAS über Dekaden hinweg und der vielfältigen Anwendungsfälle bzw. der Ressourcenverfügbarkeit auf den meisten BA-Geräten nicht durchgängig realisierbar. Darum muss die Sicherheitsstrategie nicht nur von außen nach innen sondern umgekehrt, auch von vermeintlich geschlossenen Systemen von innen nach außen konzipiert und implementiert werden.

Sicherheit ist in jedem Bereich des *System Life Cycle* speziell auch in der Designphase zu berücksichtigen. Es müssen geeignete Maßnahmen getroffen werden, um ein System zu schützen. Z.B. kann die Verwendung eines *Intrusion detection Systems* (IDS) abnormales Systemverhalten erkennen und die Gefahrenquelle lokalisieren, um diese im Anschluss zu isolieren [6]. Andererseits können sogenannte *Building Management Systems* (BMSs) verwendet werden, welche mit den *Supervisory Control and Data Acquisition* (SCADA) Systemen verbunden sind und diese mittels Visualisierungs-, Monitoring-, Wartung- und Alarm-Funktion unterstützen.

2. Fragestellung/Problematik

Wo und wie ist Sicherheit in der BA notwendig bzw. was ist der Nutzen für den Endverbraucher? Warum muss ein Lichtschalter „sicher“ sein?
Die Mehrfachnutzung von Sensoren/Aktoren wie z.B. ein Fensterschließkontakt, welcher im Sicherheitssystem verwendet wird, kann auch für die Aktivierung des Heizung-/Kühlsystem mitverwendet werden. Somit schließen sich mehrere Systeme zu einem Ganzen. Dies spart auf der einen Seite Kosten. Auf der anderen Seite müssen aber Sicherheitsstrategien neu überdacht werden. Im Falle des Lichtschalters könnte die Abwesenheitssimulation in einem Haus über einen Angreifer manipuliert werden. Ebenso könnte durch den Ausfall des Beleuchtungssystemes im Gebäude, verursacht durch schadhafte Manipulation, die anwesenden Personen in Panik geraten und somit Menschenleben gefährdet werden.
Ein zusätzliches Sicherheitsrisiko stellt die Langlebigkeit von BAS und dem damit verbundenen Update-Mechanismus bzw. Kompatibilitätsproblem dar.
Grundsätzlich muss eine gute Balance zwischen benötigtem Security Level und verfügbaren Ressourcen gefunden werden („good enough security“).

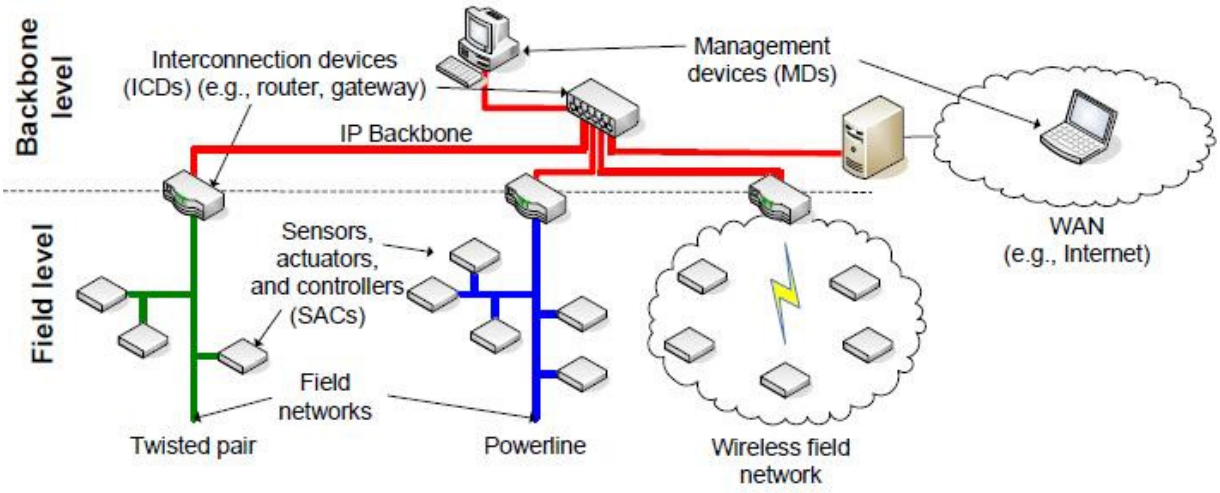

Abbildung 4: BAN – Backbone und Field Level [6]

Durch die zunehmende Konvergenz der IT zu BAS werden die *Building Automation Netzwerke* (BAN) nach Abbildung 4 nur mehr in die Backbone (meist IP-Technologie) und die Feldbusebene unterteilt. In diesen beiden Ebenen finden nach drei Gerätetypen Einsatz:

- SACs *Sensor, Actuators, Controllers*
- MDs *Management Devices*
  Konfiguration, Wartung, Visualisierung, Alarm-Monitoring
- ICDs *Interconection Devices*
  Sind Verbindungsgeräte (z.B. Router) zwischen verschiedenen Netzwerken oder bieten von anderen Netzen aus Remote Zugang an (z.B. Gateway zu einem Wide Area Network)

Diese drei Gerätetypen stellen mit der Field-Netzwerk- und Backbone-Attacke fünf potentielle Attakenziele in BANs dar. Im Unterschied zu üblichen Client-Server bzw. IP-Netzwerkarchitekturen bestehen BANs oft aus wenigen MDs, ein paar ICDs und tausenden (sammelnden) SACs. Hierbei hat der Angreifer grundsätzlich 2 Angriffsmöglichkeiten, den Medium (Netzwerk) und den Geräte Zugriff.

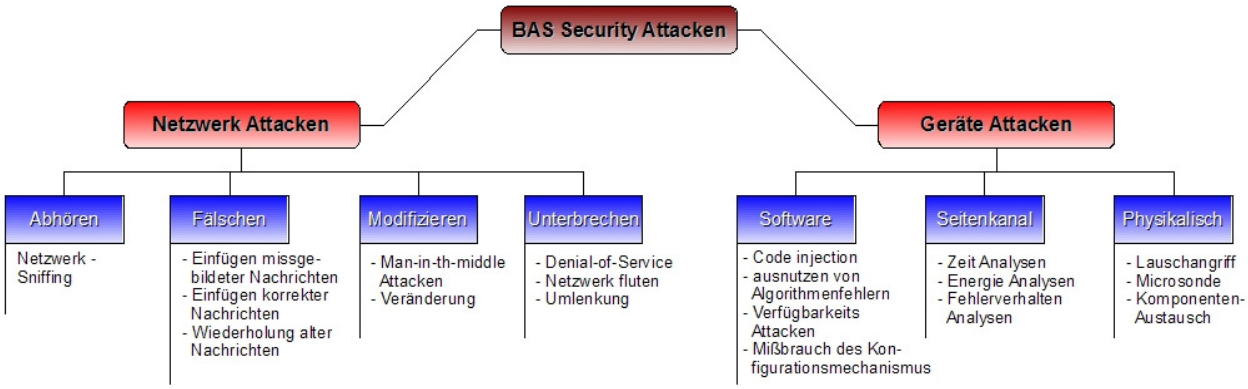

Abbildung 5: GBA Attacken [6]

Die Netzwerkattacken unterteilen sich wiederum in Abhör-, Fälschungs-, Manipulations- und Unterbrechungsattacken. Neben sicheren Netzwerkeigenschaften zählen sichere Geräteeigenschaften und die Absicherung von Angriffspunkte gegen Software- (Exploits, etc.), Side-Channel-Angriffe (Angreifer überwacht Geräte um Informationen zu erhalten) oder auch einen Angriff auf physikalischer bzw. invasiver Ebene, zu den wichtigsten Punkten. Des Weiteren ist eine korrekte, zuverlässige bzw. zeitnahe, geordnete Übermittlung von Daten in BANs unerlässlich.
Ziel ist es nun sowohl einen Angriff von außen, als auch von innen abzuwehren und die Prozessdaten bzw. die Management-Kommunikation zu sichern. In dieser Arbeit wird auf Strategien zur Netzwerksicherheit und weniger auf die Softwaresicherheit eingegangen.

3. State of the Art

Im Folgenden werden einzelne offene Standards in BAS beschrieben, auf deren Sicherheitsmechanismen untersucht und gegenübergestellt.

3.1. Offene BAS-Protokolle

BACnet

Der *Building Automation Control Network* (BACnet) Standard ist in Amerika aus der Klimatechnik entstanden und wurde 1995 für HVAC Systeme verabschiedet. Seit 2003 ist die BACnet Protokoll Definition in der internationalen Gebäudeautomatisierungsnorm ISO 16484 verankert. Im Vorgängerstandard wurden die Daten noch mit einem kurzen Schlüssel nach dem symmetrischen *Data Encryption Standard* (DES) mit 56 Bit verschlüsselt. Der BACnet Normungsausschuss veröffentlicht je nach Bedarf Protokoll-Erweiterungen in so genannten Addendums. 2008 wurde Addendum g, in der eine sichere Kommunikation in Netzwerken einschließlich Verschlüsselungs- und Authentifizierungstechnologien beschrieben ist, verabschiedet. Hierin sind 6 Keys und 8 sichere Services, als auch eine stärkere Verschlüsselung über AES definiert.
Sowohl der alte, wie auch neue Standard beschreiben einen trusted Key Server, aber nicht dessen Implementierung.

LONWorks

LONWorks ist ein offenes durchgängiges Feldbuskonzept in der das *Local Operational Network* (LON) Protocol, welches in den 90er Jahren in Amerika für Automation & Control im Gebäude-, Transport-, Industrie- und Haus-Bereich entwickelt wurde, Einsatz findet. Der Focus dieser Bustechnologie liegt in der dezentralen Automatisierung und auf Energie-effizienz in der Gebäude- und Raumtechnik. Diese BA-Technologie wurde 2008 in die Norm IEC/ISO 14908 dokumentiert. Die Protokollentwicklung, mitunter auch LONTalk wird vom internationalen LONMark Konsortium mit ihren rund 200 Controller Mitglieder Firmen vorangetrieben.
Zur Verbesserung der Sicherheit wird ein vier Stufen Challenge-Response Mechanismus genutzt, welcher Schwachstellen, wie der schwachen Verschlüsselung mit 48 Bits Länge, aufweist. Dazu gibt es keinen Key-Verteilungsmechanismus und die Netzwerkteilnehmer teilen sich nur einen gleichen Authentifizierungskey. Des Weiteren werden auch keine Broadcast-Funktionen unterstützt.

KNX/EIB

Die KNX Feldbustechnologie gilt seit 2002 als Nachfolger vom *Europäischen Installations Bus* (EIB) und wurde 2006 unter der Norm ISO/IEC 14543-3 standardisiert.
Hierin bildet ein Kontrollschema mit Klartext übertragenem Passwort den Basiszugang in einer KNX Umgebung. Dazu werden bis zu 255 verschiedene Access Level mit je einem 4 Byte langen Passwort verwendet. Als Programmier- bzw. Managementtool ist eine Engineering Tool Software (ETS) verfügbar. Es gibt jedoch keine standardisierten Sicherheitskonzepte. Einzig Ansätze wie Secure EIB (SEIB) oder EIBsec (Kapitel 4.2.) bieten mögliche Lösungen für sichere EIB/KNX-Netzwerke.
Als offener BA-Standard unterstützt KNX die meisten Kommunikationsmedien (Twisted Pair, Powerline, Wireless, Internet Protokoll). Aber selbst bei KNXnet/IP wird nach dem Prinzip „Security by Obscurity“ vorgegangen. KNX hat keinen Key-Mechanismus und es werden keine Parallelverbindungen erlaubt, welches sich schlecht auf die Datenverfügbarkeit auswirkt.

OPC

Der Vergleich zu OPC (OLE-for Processcontrol; OLE: *Objekt Linking und Embedding*) soll den grundsätzlichen Unterschied zu etablierten Feldbustechnologien aufzeigen. *OPC Unified Architecture* (OPC-UA) definiert volle Sicherheitsmechanismen, ist aber nach Abbildung 2 rein auf der Managementebene angesiedelt. Dafür werden Sicherheitsanforderungen wie Integrität, Aktualität und Vertraulichkeit über einen Sicheren Kanal und die Entität Authentifizierung über Zertifikate realisiert. Die OPC-Foundation ist eine Non-Profit Organisation und der erste OPC-DA Standard (lesen, schreiben, monitoren von Steuerungsdaten) ist 1996 aus der Automatisierungstechnik entstanden und war auf Windows-Systeme beschränkt. Der Nachfolger OPC-UA ist seit 2006 in der Norm IEC 62541 verankert und auch für Linux/Unix Geräte verfügbar. Die Datenübertragung erfolgt zum einen über Webservices oder binär über das *Transmission Control Protocol* (TCP).

Zigbee

Zigbee (Allianz seit 2002) als kabellose Technologie definiert den Netzwerk und Applikations-Layer und setzt auf dem IEEE 802.15.4 (seit 2004) Standard auf. Erste Zigbee Geräte kamen 2006 auf den Markt. Mittlerweile sind unterschiedliche Profile wie das *Home Automation Public Application*, das *Smart Energy Public Application* oder auch *Health Care Profil*, sowie verschiedene Standards wie *IPv6 over Low power Wireless Personal Area Networks* (6LoWPAN) oder auch *WirelessHART,* welches speziell im Automatisations Bereich eingesetzt wird, erhältlich.
Die Sicherheitsmechanismen vom IEEE 802,15.4 Standard (Data Link Layer) werden in Zigbee nicht genutzt. Die kleinste Security Einheit ist das Device. Das Sicherheitskonzept basiert auf symmetrischer Verschlüsselung (AES). Zigbee unterscheidet 3 Arten von Schlüssel (Link, Network, Master), welche zur Laufzeit über ein einzelnes *Trust Center* verteilt werden können. Bezüglich dem Key Management sind drei verschiedene Möglichkeiten beschrieben aber deren Implementierung nicht genau definiert.

3.2. Sicherheitsbezogene Gegenüberstellung offener BAS-Protokolle

Im diesem Kapitel werden die in 3.1. beschriebenen Protokolle in zwei Tabellen, zum einen auf deren konkrete Sicherheitsmechanismen verglichen. Die zweite Tabelle stellt vier offene BA-Standards und zwei IT-Mechanismen im Bezug zu Sicherheitsanforderungen gegenüber. Auf den OPC-UA Standard wurde wegen der reinen Verwendung auf der Managementebene verzichtet.

	BACnet	LONWorks	KNX/EIB	Zigbee
Authentifizierung	DES	64 bit MAC (48 bit key)	32 bit Passwort	AES-128
Integrität	DES	64 bit MAC (48 bit key)	-	FCS
Vertraulichkeit	DES	-	-	AES-128
Aktualität	Random Nummer (64 bit)	Random Nummer (64 bit)	-	Freshness Timer

Tabelle 2: Sicherheitsmechanismen-Vergleich offener BAS-Protokolle [9]

Sowohl BACnet, unter Verwendung der neuen Erweiterung Addendum g samt der stärkeren AES Verschlüsselung, als auch Zigbee bilden eine solide Basis für sichere BAS.

Gängige Sicherheitsstrategien für IP-Netzwerke ist die Verwendung von *IPsec* (inkl. Internet Key Exchange Protokoll), SSL bzw. dessen Nachfolger *Transport Layer Security* (TLS) welche nur Unicast aber kein Multi- oder Broadcast unterstützen oder auch die Nutzung von VPNs. All diese Technologien bieten eine gute Möglichkeit um den Netzwerkverkehr zu verschlüsseln, nutzen aber einerseits einen zentralisierten Server an den alle Clients hin verbunden und damit schlecht bezüglich Skalierung sind, und auf der anderen Seite bieten sie wenig Möglichkeiten für das Key Management und sind zudem zu komplex für Embedded Geräte.

	BAS				IT Mechanismen	
	BACnet	LONTalk	KNX	Zigbee	IPsec	TLS
Entität Authentifizierung	+	-	-	+	+	+
Autorisierung	~	-	~	~	+	+
Datenintegrität	+	~	-	+	+	+
Datenursprungsauthentifizierung	~	-	-	+	+	+
Datenaktualität	+	~	-	+	+	+
Datenvertraulichkeit	+	-	-	+	+	+
Datenverfügbarkeit	-	-	-	-	-	-
Embedded Geräte	+	+	+	+	-	~
Kommunikationsmodelle	-	~	-	-	~	-
Skalierbarkeit	-	-	-	-	-	-
Non IP Netzwerke	+	+	+	+	-	+
QoS Parameter	-	~	-	~	~	~

Tabelle 3: Funktional/Domain spezifische Gegenüberstellung offener BAS-Protokolle [12]

Nach [12] werden sieben *funktionale Anforderrungen* (FR),

FR1.) Entität/Objekt Authentifizierung (sind die Teilnehmer die richtigen Teilnehmer?)
FR2.) Autorisierung (prüfen der Berechtigung, verschlüsselt/unverschlüsselt)
FR3.) Datenintegrität (Daten wurden nicht verändert)
FR4.) Datenursprungsauthentifizierung
FR5.) Datenaktualität (Freshness; Daten aktuell und gültig)
FR6.) Datenvertraulichkeit (nur aut. Personen haben Zugang zu vertr. Informationen)
FR7.) Datenverfügbarkeit (Zugang zu Daten ist ungestört vorhanden)

und fünf Domain spezifische Herausforderungen (*Domain Specific Challenges*, DC)

DC1.) Embedded Geräte (Gute Balance zw. Security Level und verfügbaren Ressourcen)
DC2.) Kommunikationsmodelle (Standard: Client/Server; in BAS: Multicast oder Broadcast)
DC3.) Skalierbarkeit (100e bis 1000e Geräte)
DC4.) Non IP Field Netzwerke (robuste, flexible und kosteneffiziente Field-Netzwerke)
DC5.) *Quality-of-Service* (QoS) (in der IT Mega-Giga Byte ohne Realtime Anforderungen im Vergleich zu wenigen Byte in BAS mit soft Realtime Anforderungen)

definiert und die einzelnen offenen Standards nach Tabelle 3 verglichen. Wie in Tabelle 2 bilden die BACnet als auch die Zigbee Variante eine gute Grundlage für eine sichere Kommunikation. Jedoch ist keines der genannten BAS Protokolle für sicherheitsrelevante (Safety) Anwendungen geeignet [12].
Eine direkte Spiegelung der IT-Mechanismen wie IPsec oder TLS, die nahezu alle funktionalen Sicherheitsanforderungen nach Tabelle 3 erfüllen, auf die BAS, ist aufgrund von Ressourcenverfügbarkeit bzw. Kompatibilität zu vorhanden System nicht durchgängig möglich. Aber auch die IT-Mechanismen können, wie die BAS-Protokolle nur bedingt bzw. gar nicht die Punkte Verfüg- oder Skalierbarkeit bedienen.

4. Ansätze/Lösungen

4.1. Vier-Phasen-Ansatz

Nach [6] wird eine Vorgehensweise für sichere BANs aufgezeigt, welche genügend Sicherheit für die Datenübertragung gewährleisten soll:

1. Initiale Konfiguration
   Jedes Gerät ist zur Installationszeit vorkonfiguriert. Die Konfiguration am Gerät enthält generelle Informationen über das BAN (z.B. Adressinformation) und ein so genanntes *Initial Security Token Set* (ISTS). Das ISTS wird später für das „Sichere Verbinden“ benötigt. Der Upload bzw. die Aufspielung der initialen Konfiguration muss physikalisch gesichert sein [9]!

2. Sicheres Verbinden
   Im Gegensatz zur initialen Konfiguration, welche nur einmal ausgeführt wird aber die Daten für das sichere Verbinden liefert, kann danach eine/mehrere sichere Verbindung/en beliebig oft zur Laufzeit zu anderen Teilnehmern aufgebaut werden. Über den Entitäts Authentifizierungs Prozess wird der *joinenden Entität* (JE) ein sogenanntes *Dynamic Security Token Set* (DSTS) vom Verbindungspartner bzw. nach gegenseitiger Überprüfung, von einer *vertrauenswürdigen Entität* (*Trusted Entity*, TE) übermittelt. Ein von einer TE gesendetes Daten Set ist auf eine Kommunikations-beziehung einmalig zugeteilt und wird später für die sichere Kommunikation für den Datenaustausch verwendet. Um sowohl die Authentifizierung, als auch die erhaltenen DSTS zu sichern werden für die Verschlüsselungsalgorithmen Inputparameter aus dem ISTS verwendet.
   Damit die JE die TE bzw. deren Adressen finden und die TE im Besitz der DSTS sind, gibt es zwei Möglichkeiten:

   - Vordefinierte TE
     Vordefinierte Koordinatoren werden als TE verwendet. Dessen Adressen, die einzelnen Keys (gemeinsamen, geheimen oder öffentliche/private) und Zertifikate sind im ISTS der JE enthalten. Um ein *Single Point of Failure* (SpoF) zu vermeiden empfiehlt es sich vordefinierte redundante Koordinatoren zu verwenden [7].

   - Dynamische TE
     Erfolgt über demokratischen Ansatz welcher sinnvollweise nur mittels asymmetrischen Algorithmen (z.B. *Elyptic Curve Cryptographic* - speziell für Embedded Geräte) realisiert werden kann [8]. Hierbei enthält der jeweilige Teilnehmer bzw. das ISTS nur das Zertifikat der zentralen Autorität, die jeweiligen Entitäts-Zertifikate und sein eigenes öffentliche/privates Schlüsselpaar. Im Falle der Nutzung symmetrischer Algorithmen müssen die TEs alle gemeinsamen Schlüssel von allen JEs bevorraten. Zur dynamischen TE Einbindung muss ein Mechanismus (service to discover) zur Auffindung der Entitäten verfügbar sein.

3. Sichere Kommunikation
   Nachdem das DSTS empfangen wurde, kann eine sichere Kommunikation erfolgen. Um Speicher- und Rechenaufwand zu minimieren sollte es möglich sein, individuelle Sicherheitsstufen für eine Übertragung wählen zu können.

   I.) Geschützter Kanal
   Datenorginalität und Datenintegrität z.B. MAC-Algorithmus
   II.) Zuverlässiger Kanal
   I + Datenaktualität über monoton steigenden Zähler
   III.) Vertrauenswürdiger Kanal
   II + Verschlüsselung mittels AES

   Für die Zuordnung in den 3 Sicherheitskategorien ist ein DSTS auf eine Kommunikationsbeziehung beschränkt. Zusätzlich ist die Lebensdauer des Schlüsselsets limitiert.

4. Sicheres Trennen
   Zum einen kann eine Netzwerk Entität von sich aus die Verbindung beenden, z.B. wenn ein MD nur wenige Management Daten austauscht, und zum anderen können Netzwerkteilnehmer selbst entscheiden ob sie eine Entität aus Sicherheitsgründen von Kommunikationsbeziehungen ausschließen. In beiden Fällen muss gewährleistet sein, dass die Entitäten nicht mehr an der Kommunikation teilhaben können. Dies wird über den *Widerruf-Prozess*, indem ein neues DSTS generiert wird, realisiert. Die Koordination erfolgt über die zuständigen TEs.

4.2. EIBsec

Aufgrund von Ressourcenverfügbarkeit können keine gängigen ICT-Sicherheitsmechanismen auf den KNX/EIB Feldgeräten genutzt werden. *EIBsec* [9] als Sicherheitsextension ist eine Weiterentwicklung des *Secure EIB* (SEIB) Ansatzes, der aus einer Doktorarbeit an der TU München resultiert [10]. SEIB basiert auf dem *Sensor Network Encryption Protocol* (SNEP), welches Teil des *Secure Protocol für Sensor Netzwerke* (SPINS) ist und stellt bereit.
In EIBsec sind zwei Verschlüsselungsmodi „normal mode“ und „counter mode“ (Sicherung von Management- und Prozessdaten) möglich.

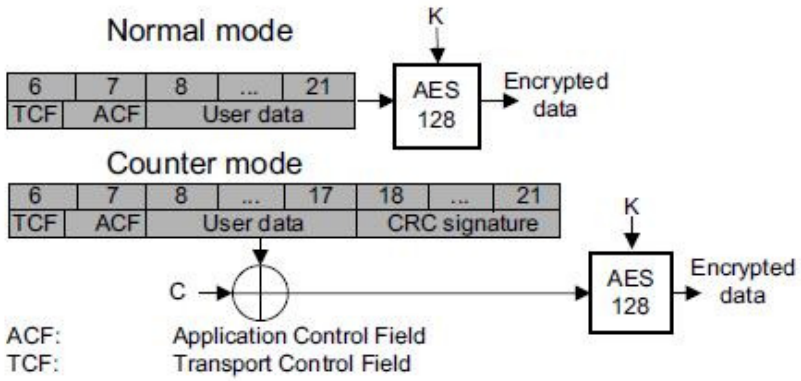

Abbildung 6: EIBsec Verschlüsselung [9]

Hierbei werden die Daten mittels AES verschlüsselt, wobei die Adressierung unverändert bleibt um die Kompatibilität zum alten EIB zu gewährleisten. Hinzu kommt eine 32 Bit *Cylcic Redundancy Check* (CRC) Checksumme, die gegen unautorisierte Modifikationen schützt. Ein 128 Bit Counter soll gegen Replay-Angriffe helfen.
Je nachdem in welchem Netzwerksegment eines hierarchisch aufgebauten EINB/KNX Netzwerkes eine sichere Kommunikation notwendig ist, kann ein sogenanntes *Advanced Coupler Unit* (ACU) Modul mit EIBsec Funktion verwendet werden.
Des Weiteren werden nach [9] ein Key-Management für den Bus, Local und Direct Mode inklusive Key-Wiederverwendung und Key-Lifetime beschrieben. Der EIBsec Entwurf soll eine sicheres Datenmanagement inklusive -kommunikation ermöglichen, wurde auf einem „KNXcalibur“ Embedded Board implementiert und auf Netzwerktauglichkeit getestet [9]. Die beschriebenen EIBsec Ergebnisse von der Forschergruppe an der TU Wien trugen fortwährend zur Weiterentwicklung des aktuellen KNX-Standards der KNX-Assoziation [11] mit bei.

4.3. Multiprotokoll-Ansatz

Warum sollen mehrere Protokolle zu einem zusammen gefügt werden?
Wie im Kapitel 2 erwähnt reduzieren sich durch Kombination von verschieden BAS sowohl Investitions- als später auch Wartungskosten und erhält somit einen Mehrwert [6].
Z.B. kann ein Fensterkontakt-Sensor, der sicher über BACnet angeschlossen und im Security System eingehängt ist auch für das Heizungs/Kühlungs System, welches womöglich über EIB/KNX angeschlossen ist, genutzt werden. Zusätzlich können die einzelnen Sicherheitsmechanismen der verschiedenen Protokolle in einem Netzwerk miteinander kombiniert werden.
Üblicherweise werden die einzelnen heterogenen BA-(Sub)netze horizontal nebeneinander integriert und über verschiedene Gateways miteinander verbunden.

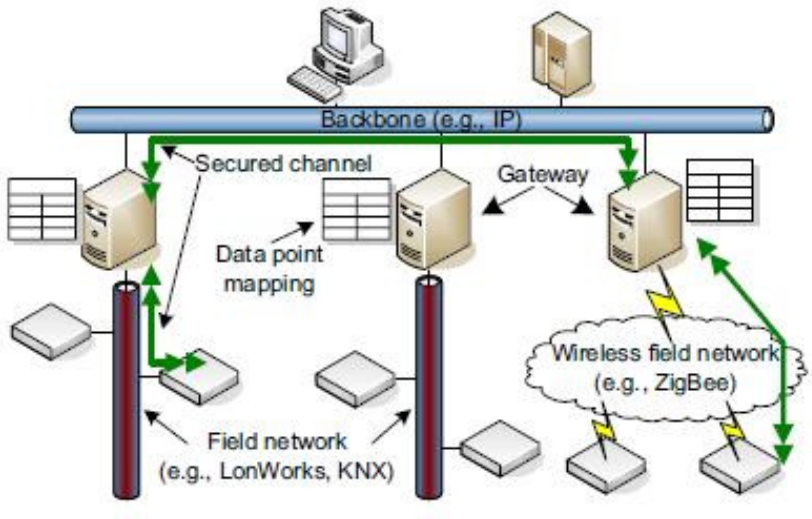

Abbildung 7: Horizontale Integration für BAN [15]

Die horizontale Integration in Abbildung 7 stellt zwei prinzipielle Nachteile. Zum einen das Mappen von Datenpunktabellen (Datenpunkte: Temperatur, Füllstand, Lichtschalter, Relais,

Fensterschließer, etc.) und zum anderen, die Gateways zwischen den einzelnen Netzwerken, die potentielle Angriffspunkte darstellen und somit voll (sicherer Kanal, Datenintegrität, -vertraulichkeit, -aktualität und Authentifizierung) abgesichert werden müssen.

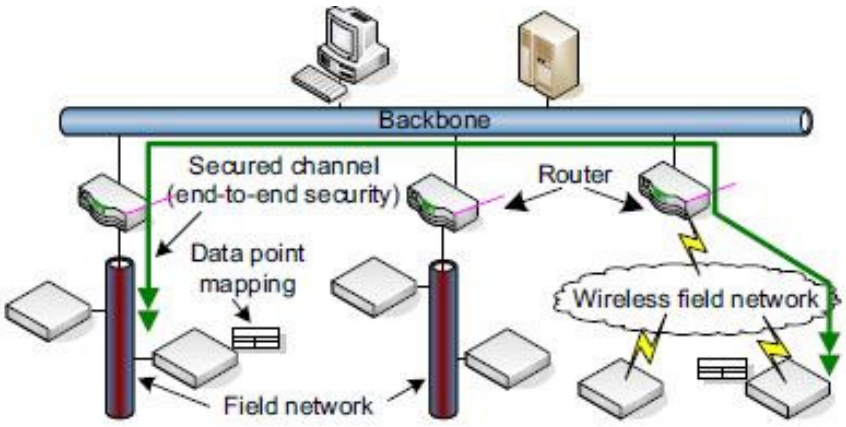

Abbildung 8: Vertikale Integration für BAN [15]

Eine vertikale Integration für BAN nach Abbildung 8 samt Multiprotokoll-Ansatz ermöglicht die Verwendung von simplen Routern im Vergleich zu dedizierten Gateways und ein Datenpunkt-Mapping direkt am Gerät. Wobei nur Geräte die über heterogene Netzwerke hinweg kommunizieren mit der Multiprotokoll-Funktion ausgerüstet werden müssen.

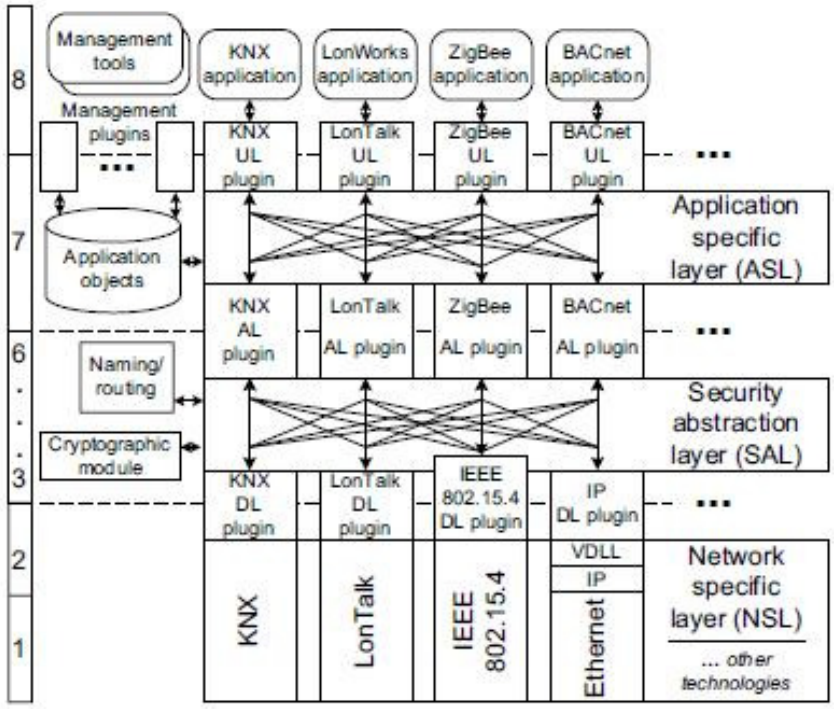

Abbildung 9: Multiprotokolllayer-Ansatz [15]

Der Mutliprotokoll-Ansatz in Abbildung 8 verfolgt prinzipiell das *Open Systems Interconnection-Referenzmodell* (OSI-Schichtenmodell). Im Wesentlichen werden diese 7 Schichten und die Funktionalität von BAS in eine dreistufige Hierarchie unterteilt und um einen Layer erweitert.

- *Network specific Layer* (NSL)
  Je nach Bedarf kann die hohe Bandbreite von Ethernet oder die Topologien von KNX oder LonWorks können genutzt werden.
- *Security Abstraction Layer* (SAL)
  Der SAL stellt generische sichere Kommunikations-Services zum ASL bereit.
  - Kommunikations Service Typen
    Management-, Prozessdaten
    Sporadische, frequentielle Daten
  - Kommunikations Modelle
    BACnet: Client/Server
    KNX: Producer/Consumer
    oder Publisher/Subscriber Model
  - Global Naming
    Mappt die globalen Adressen auf den *Data Link Layer* (DLL)
- *Application specific Layer* (ASL)
  In diesem Layer können beliebige Applikation über das *Applikations Layer Plugin* implementiert und auch mehrere Applikationsfunktionen der darunter liegenden unterschiedlichen Technologien gemeinsam zu einer Anwendung genutzt werden. Der ASL ist verantwortlich für das Datenpunkt-Management auf den einzelnen Geräten. Hierzu werden *Applikation Objekte* (AOs) in einer generischen *Applikations Objekt Datenbank* abgespeichert.

Zwischen dem NSL und dem SAL befindet sich der *Virtual Data Link Layer* (VDLL), welche die Layer 3 Schnittstelle (z.B. IP, derzeit angewendet bei BACnet/IP mit UDP) zum DLL bildet. Hierin kann in Zukunft je nach Ressourcenverfügbarkeit auf den Geräten das IPv6 [11] mit den Sicherheitsmechanismen aus der IP-Welt verwendet werden.
Der Hauptvorteil des Multiprotokoll-Ansatzes liegt in der Flexibilität der Nutzung, als auch der Kompatibilität zu existierenden Installationen. Die einzelnen Sicherheitsmechanismen der jeweiligen Technologien können je nach Einsatzfall vom NSL über den SAL bis hin zum ASL genutzt bzw. miteinander kombiniert werden, wobei der SAL alleine volle end-to-end Sicherheit über jegliche Entitäten und auch Gerätegruppen hinweg bereitstellt. Im ASL können nach [14] neue sichere Kontrollapplikationen softwaretechnisch implementiert und genutzt werden.
Ein weiteres verbesserungswürdiges Themengebiet ist die Multi-, Uni- und auch Broadcast-Fähigkeit der einzelnen BAS Protokolle bzw. deren jeweilige anwendungsbezogene Nutzung im SAL.

5. Zusammenfassung/Ausblick

Wie aus dieser Arbeit ersichtlich gibt es mehrere Möglichkeiten auf verschiedenen Ebenen BAS bzw. deren Geräte sowohl von außen als auch von innen her abzusichern. Eine optimale Lösung wäre eine All-In-One Lösung in der ein Protokoll alle Protokolle ersetzt. Dies ist jedoch in den meisten Fällen aus Kompatibilitäts bzw. aus Kostengründen nicht realistisch. Derzeit verfügbare offene BAS-Standards bieten eine solide Grundlage für sichere BANs.
Neben modernen, handhabbaren Security Frameworks bzw. Regelwerken stellen, wie in dieser Arbeit zusammengefasst, sowohl eine definierte, überdachte Sicherheitsstrategie als auch die Nutzung mehrerer, jeweils auf die Anwendung angepassten Protokolle zu einem Multiprotokoll-Ansatz, wie auch die Realisierung konkreter Sicherheitsmechanismen auf Feldbusebene mehr Angriffssicherheit in modernen BAS.
Die genannten Technologien bzw. Ansätze erhöhen Sicherheitsfaktoren wie Authentifizierung, Integrität, Aktualität und Vertrauenswürdigkeit der Daten als auch der BA-Netzwerkteilnehmer und schützen gegen deren Modifikation, Verfälschung und Unterbrechung.
Zusätzlich benötigen moderne BAS-Mechanismen um Datenverfügbarkeit zu garantieren oder auch geeignete IDS, die Unterbrechungs-Attacken erkennen und somit Dos-Attacken abwehren können. Unter Verfügbarkeit fallen die Nutzung von redundanten Netzwerkpfaden, die Mehrfachübertragung von Daten, wie auch das Testen der Netzwerkstrukturen, welches in BANs noch nicht zufriedenstellend gelöst ist.
Die Fusion der einzelnen BAS-Protokolle zu einem All-In-One Ansatz sowie die Verschmelzung von Security zu Safety Eigenschaften benötigen innovative Methoden und bilden die Forschungsthemen für zukünftige BAS bzw. BANs.

Literaturverzeichnis

[1] W. Granzer: *Secure Communication in Home and Building Automation Systems*. Dissertation, Technische Universität Wien, 2010.

[2] J. R. Rosslin and K. Tai-hoon: *A Review on Security in Smart Home Development*. International Journal of Advanced Science and Technology, Vol. 15, February, 2010.

[3] T. Novak, A. Treytl and P. Palensky: *Common Approach to Functional Safety and System Security in Building Automation and Control Systems.* University of Technology Vienna, 2007.

[4] Cisco, Rockwell Automation: *IACS Network Security and the Demilitarized Zone*, Chapter 6, 2010.

[5] http://www.frost.com/prod/servlet/market-insight-top, 2011.

[6] W. Granzer, F. Praus, and W. Kastner: *Security in building automation systems.* IEEE Transactions on Industrial Electronics, 3622-3630, November 2010.

[7] W. Granzer, C. Reinisch, and W. Kastner: *Key set management in networked building automation systems using multiple key servers*. In Proc. IEEE Int. Workshop Factory Commun. Syst., pages 205–214, 2008.

[8] W. Granzer, D. Lechner, F. Praus, und W. Kastner. *Securing IP backbones in building automation networks*. In Proc. IEEE Int. Conf. Ind. Informat., pages. 410–415, 2009.

[9] W. Granzer, W. Kastner, G. Neugschwandtner, and F. Praus: *Security in Networked Building Automation Systems*. In Proc. 6th IEEE International Workshop on Factory Communication Systems (WFCS '06), pages 283-292, June 2006.

[10] W. Westermeir: *Diversitäre Zugangs- und Sichermechanismen angewendet in automatisierten Gebäuden*. Dissertation, Technische Universität München, 2004.

[11] http://www.knx.org/ 2011.

[12] W. Granzer and W. Kastner: *Security Analysis of Open Building Automation Systems*. In Proc. 29th International Conference on Computer Safety, Reliability and Security (SAFECOMP '10), pages 303-316, September 2010.

[13] M. Kovatsch, M. Weiss and D. Guinard: *Embedding Internet Technology for Home Automation.* Institute for Pervasive Computing ETH Zurich, 2010.

[14] F. Praus and W. Kastner: *Secure Control Applications in Building Automation using Domain Knowledge*. In Proc. 8th IEEE International Conference on Industrial Informatics (INDIN 2010), pages 52-57, jul 2010.

[15] C. Reinisch, W. Granzer, and W. Kastner: *Secure Vertical Integration for Building Automation Networks.* In Proceedings of 7th IEEE International Workshop on Factory Communication Systems (WFCS '08), pages 239-242, May 2008.