

TeleTrust-Informationstag

"IT-Sicherheit im Smart Home und der Gebäudeautomation"

Berlin, 12.11.2014

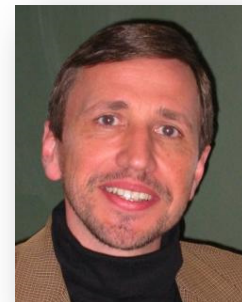
Security und Gebäudeautomatisierung

Wolfgang Kastner

Technische Universität Wien

Automation Systems Group

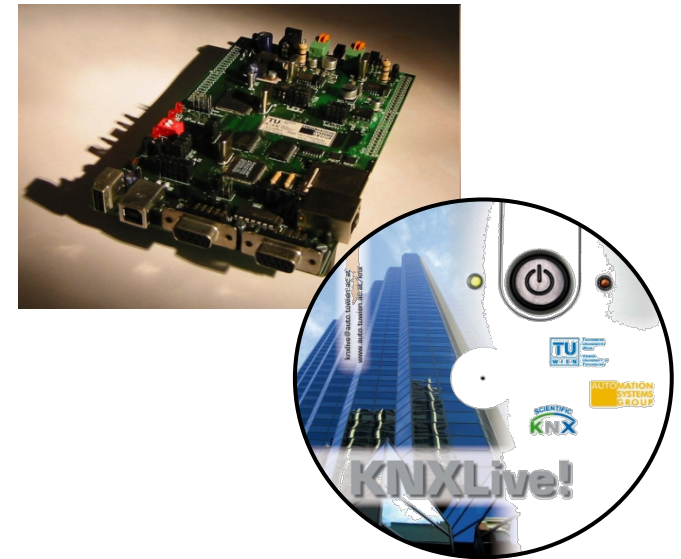
k@auto.tuwien.ac.at, www.auto.tuwien.ac.at



Automation Systems Group

■ Computer Engineering/Software Engineering

- System analysis and system design
- Networked embedded systems
- Information modelling
- (Enterprise) System interfaces
- Advanced control strategies
- Safety AND Security
- International Security Lab (iSecLab)



■ Distributed Automation

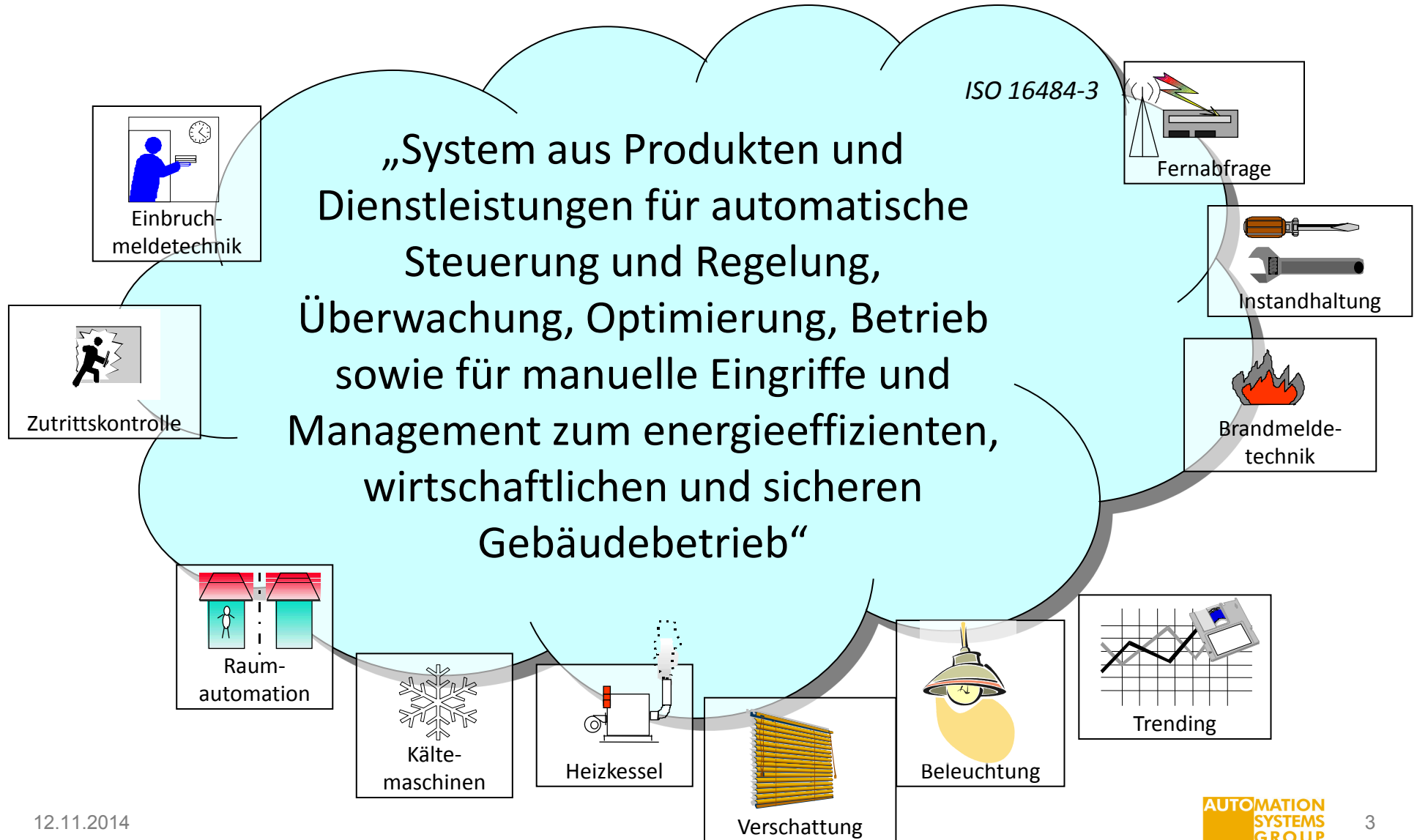
- Building automation (wired/wireless)
- Home automation/Smart homes
- Cyber-physical production systems
- Internet of Things



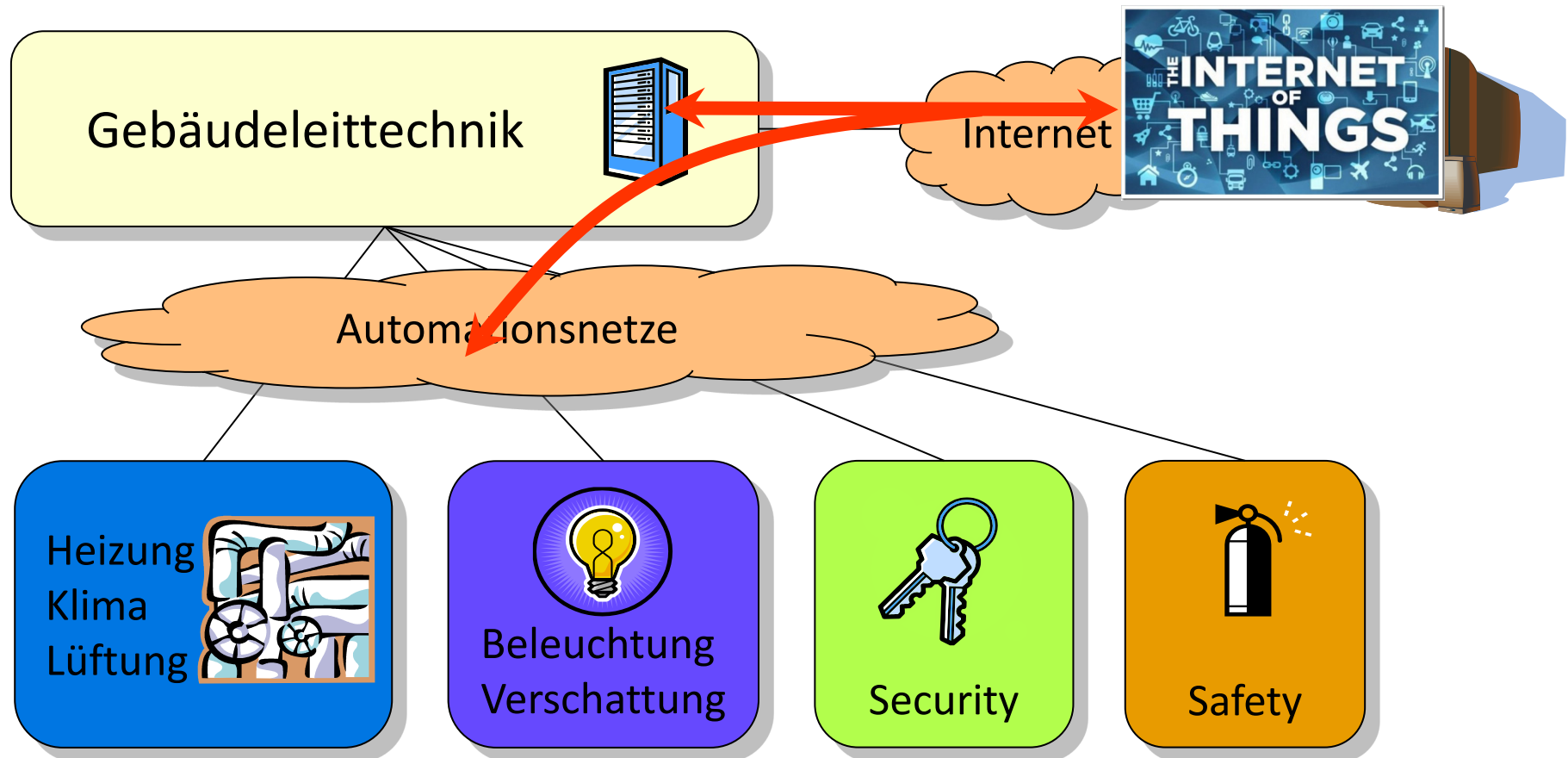
FAKULTÄT
FÜR INFORMATIK

Faculty of Informatics

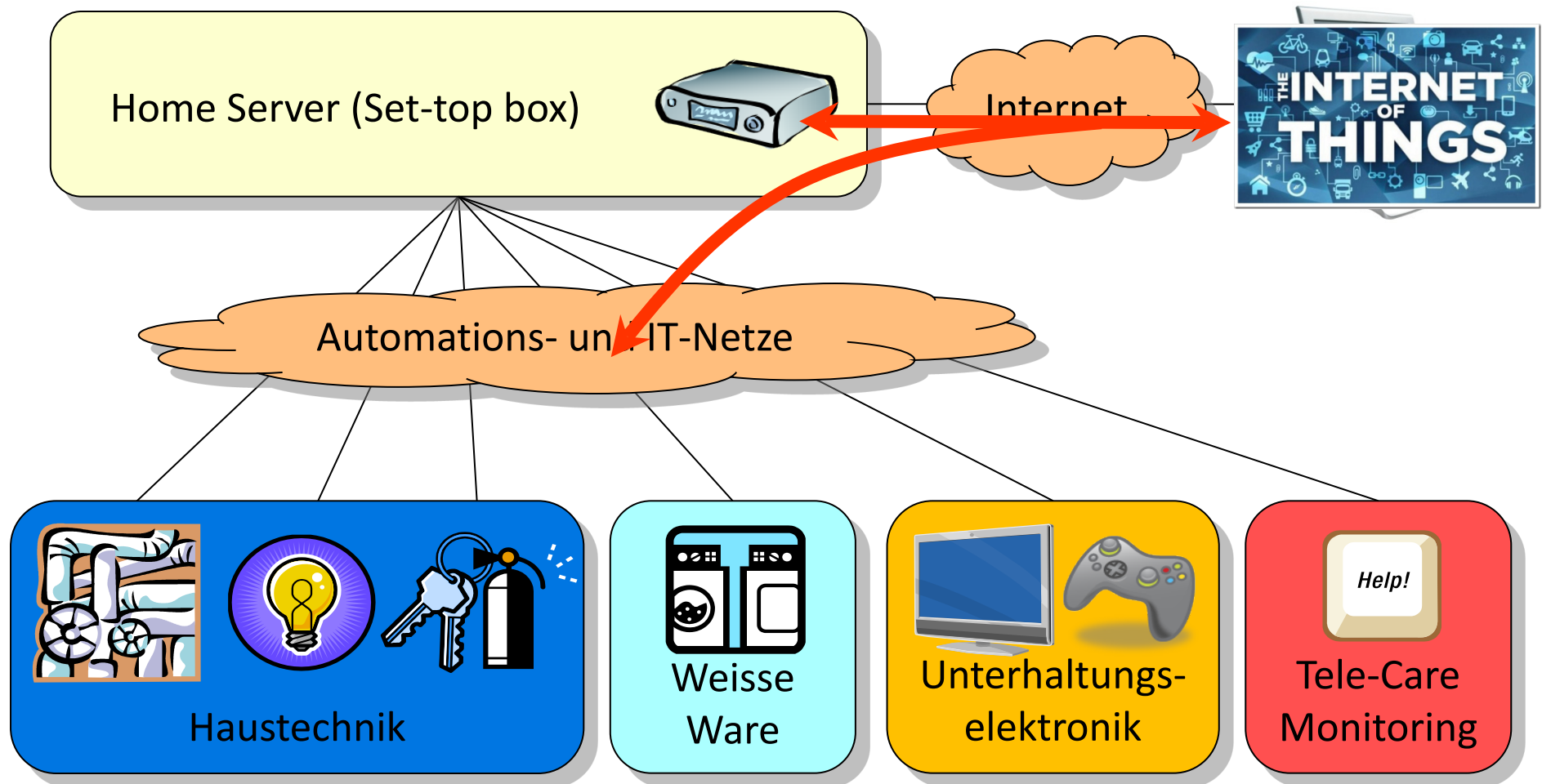
Gebäudeautomation



Systeme der technischen Gebäudeausrüstung



Smart Home Systeme



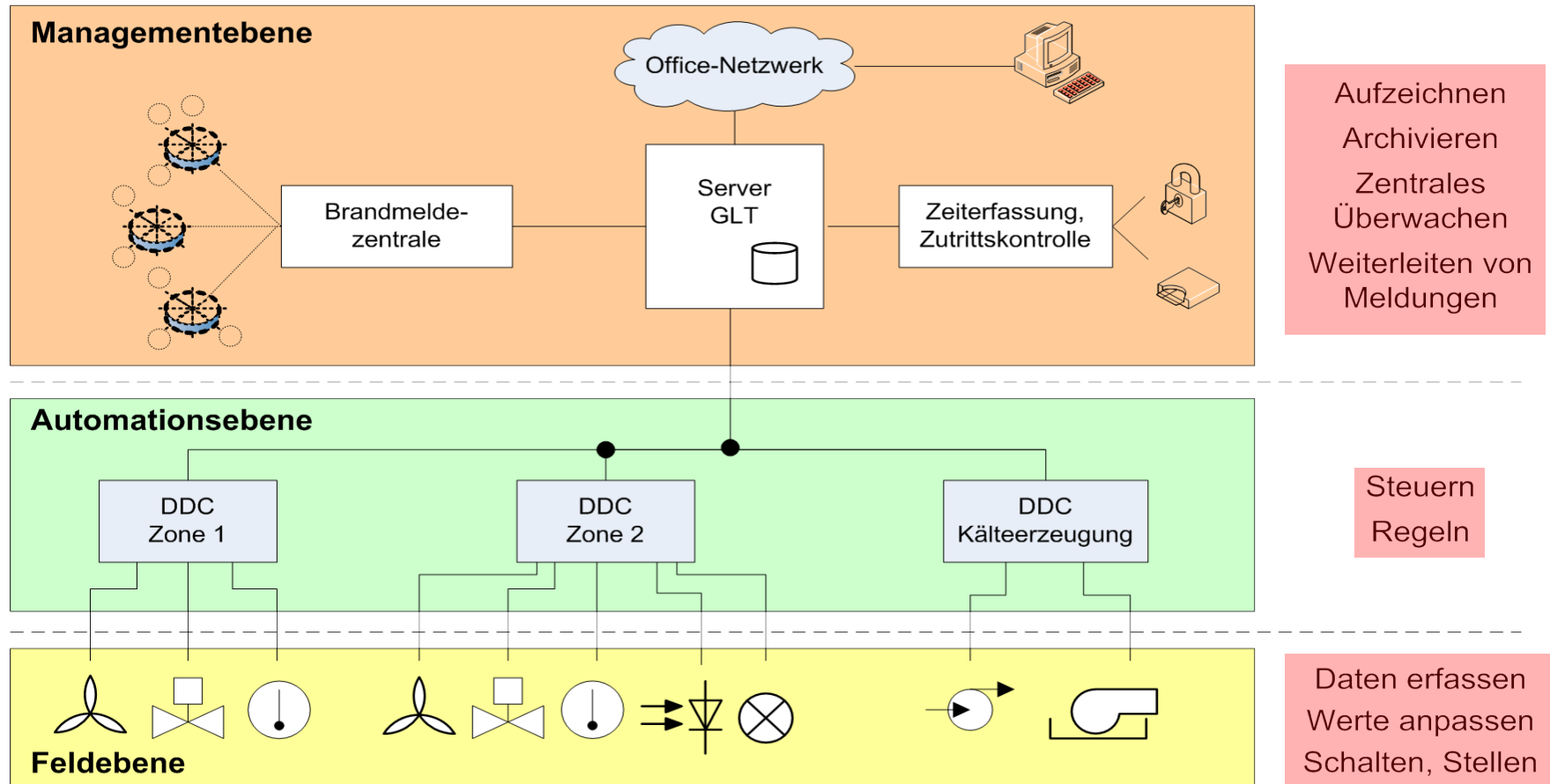
Prozess „Gebäude“

- Gebäudeinneres (und Umfeld)
- Unkritisches Zeitverhalten
 - Keine hochfrequenten Regelkreise
 - Systemträgheit im HLK Bereich groß
 - Ausnahme: Beleuchtungssteuerung
- Verfügbarkeit, Zuverlässigkeit: Mittlere Anforderungen
 - Höhere Erwartung bei Basisfunktionen
 - Maßstab: Dependability der klassischen Installations- und HLK-Technik
 - Graceful Degradation
 - Allerdings sehr hohe Zuverlässigkeit für Safety/Security

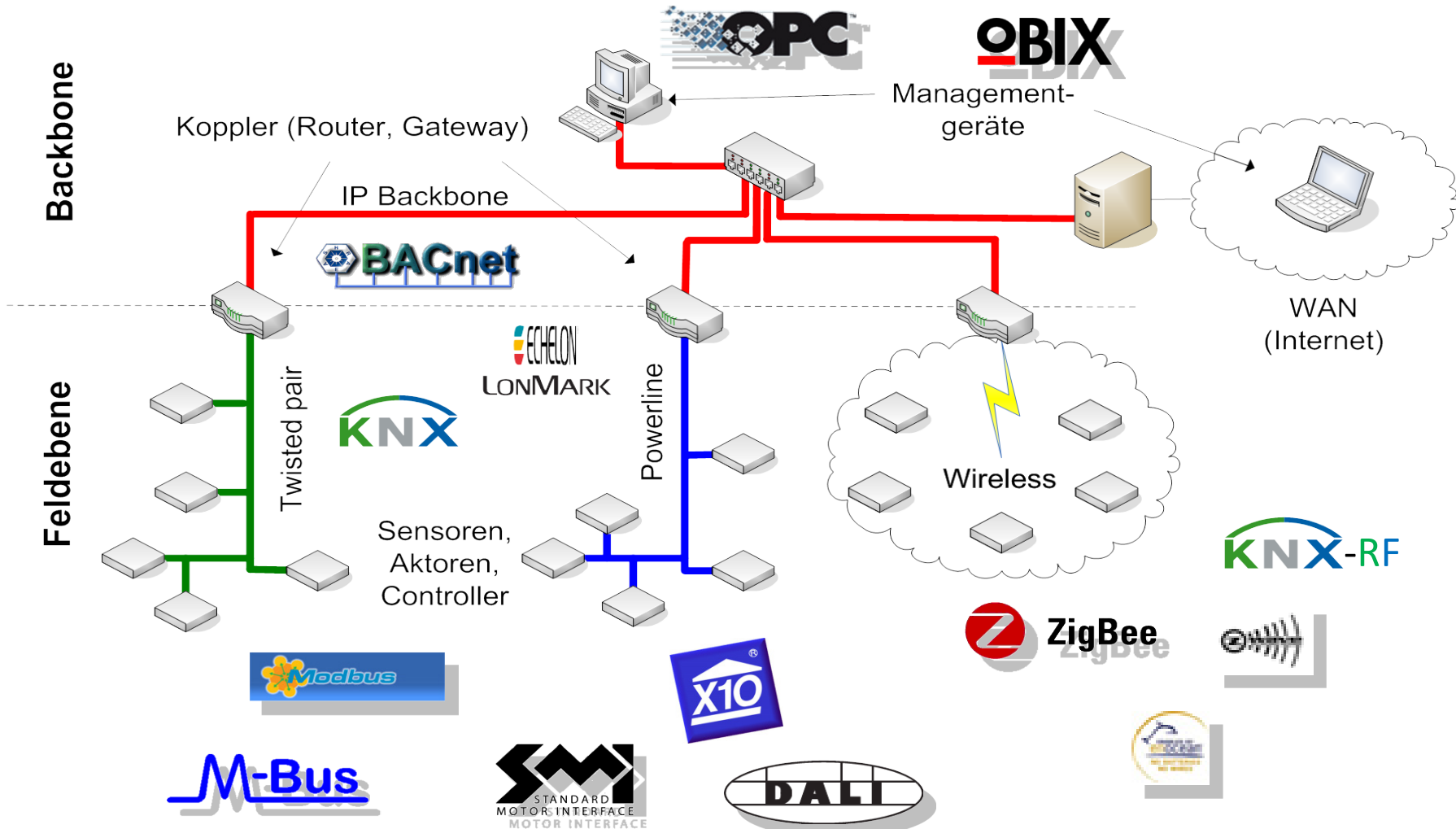
Herausforderungen

- Stochastische Störgrößen
 - Wechselnde Witterungsverhältnisse, Personenanzahl, Verhalten, Geräteabwärme (PCs, Beleuchtung)
 - Oft händischer Eingriff nötig (z.B. Luftumwälzung Hörsaal)
- Kostensensitiv
- Lange Lebenszyklen
 - Technisch konservativ (aber zukunftssicher)
 - Ausschreibungen verlangen oft Normenkonformität
- Potentiell außerordentlich große Ausdehnung
 - Lokalität der Daten hoch → Dezentraler Ansatz

Klassisches 3-Ebenen-Modell



2-stufige Architekturen/Topologien



Sichere Gebäudeautomation?

- Ist Security wirklich wichtig für Gebäudeautomation?
- **Sicherheitskritische Services**
 - Alarmsysteme, Zutrittskontrollsysteme
 - Ja, höchste Wichtigkeit!
- **Traditionelle Gebäudeautomation (HLK, Licht)?**
 - *“Warum sollte es mich stören, wenn jemand mein Licht ein- oder ausschaltet?”*
 - *“Wenn jemand wissen will, wie meine aktuelle Raumtemperatur ist, kein Problem!”*
 - **Aber:** Vandalismus, Massenpanik im öffentlichen Bereich, Attacken im Zweckbau (Bürogebäude, Spitäler, ...), Zugangspunkt zu anderen Netzwerken und Diensten!

Sichere Gebäudeautomation!



Hackers Penetrate Google's Building Management System



The downside of smarter buildings: "If Google can fall victim, anyone can."

Stephen Lacey
May 8, 2013

With more sophisticated controls and software overlays, buildings are getting a lot smarter. Unless there's a hacker out there smarter than your building, in which case your building could become a bumbling, hypnotized fool -- or even dangerous.

Google found that out (the easy way) when two cybersecurity experts hacked into its Wharf 7 office in Sydney, Australia through a building management system controlled by Tridium, a company owned by Honeywell.

According to an account of the hack published yesterday by Billy Rios and Terry McCorkle of the security firm Cylance, the two were able to penetrate Google's facility through an unpatched version of Tridium's Niagara AX, a building management platform that was exposed in February by Rios and McCorkle as having serious security holes.

In this most recent hack, Rios and McCorkle found a login page for

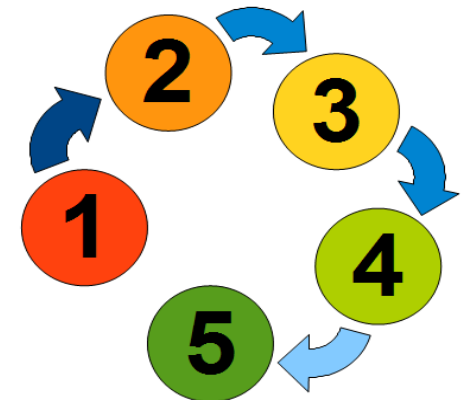
<http://threatpost.com/fbi-memo-shows-hackers-accessed-commercial-hvac-systems-121312/77317>

<http://www.greentechmedia.com/articles/read/hackers-penetrate-googles-building-management-system>

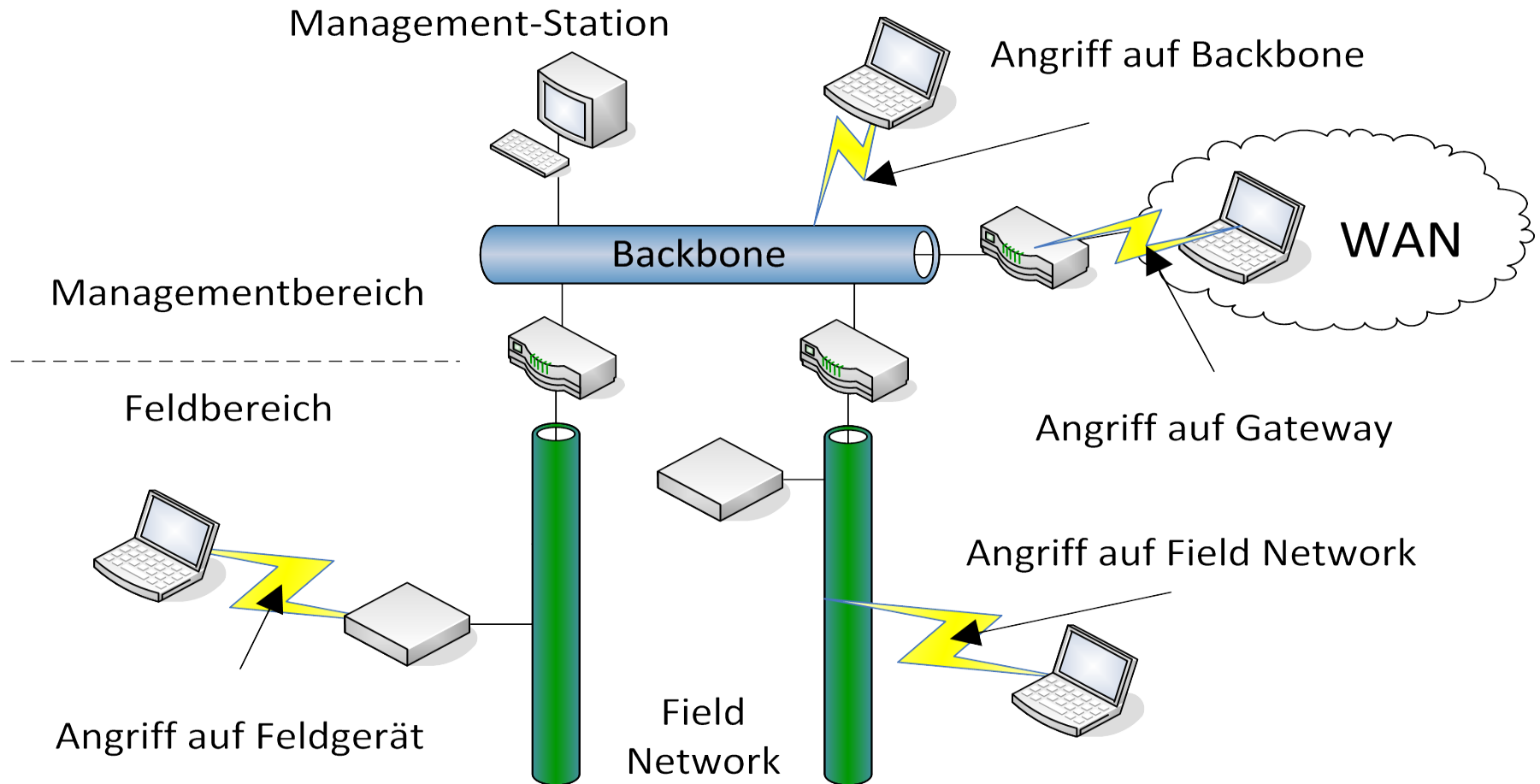
http://mummelie.de/wp-content/uploads/2012/04/gebaeude_tetris_mit.jpg

Methodik

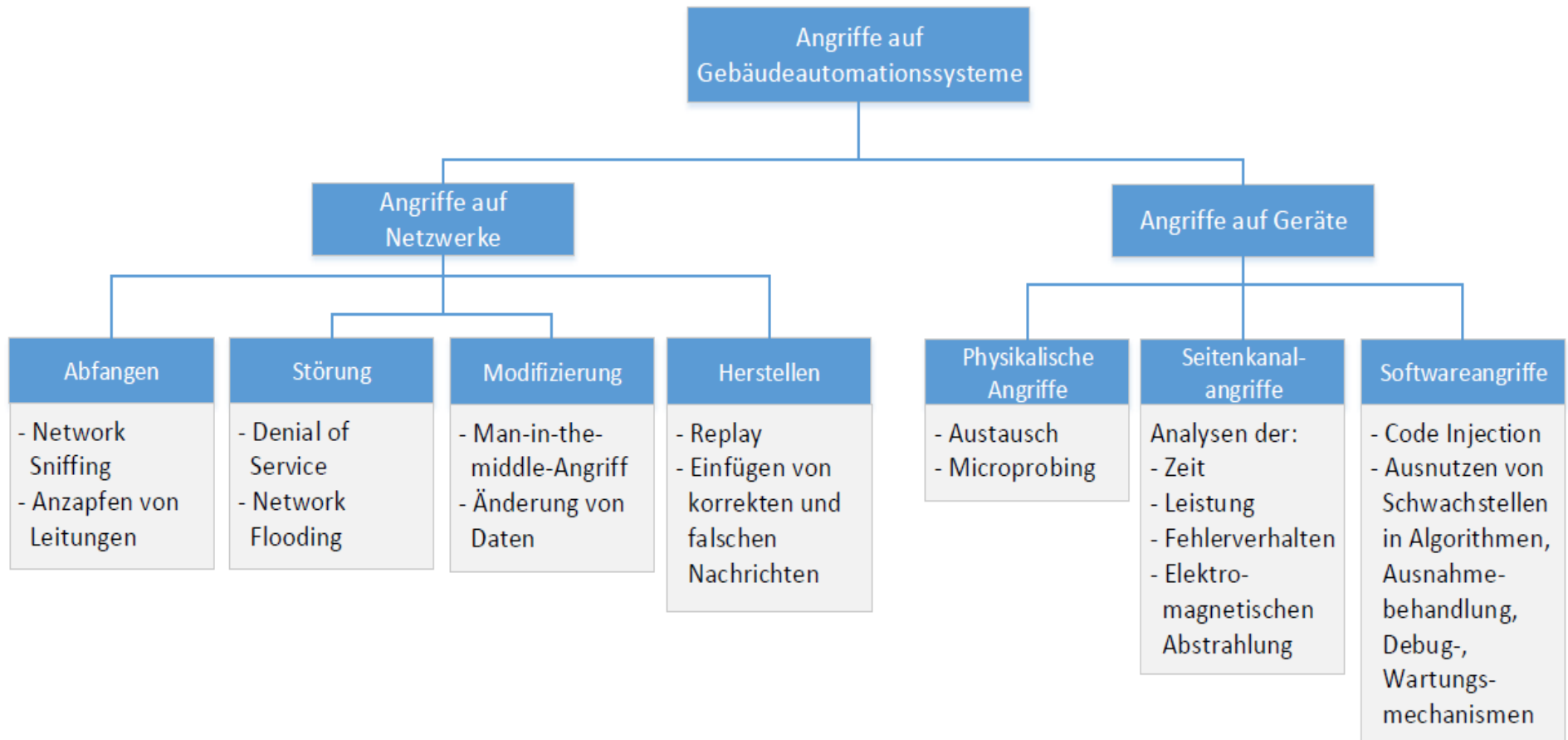
- Target Analyse
 - Welche Systeme/Komponenten sind betroffen
- Angriffsvektoren
 - Welche unterschiedlichen Angriffsszenarien gibt es?
- Anforderungsanalyse
 - Funktionale Anforderungen
 - Domänenspezifische Anforderungen
- State-of-the-art Analyse
 - Sind existierende Technologien sicher?
- Entwurf neuer Sicherheitsmechanismen



Target Analyse



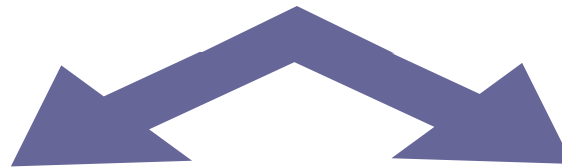
Target Analyse



Wolfgang Granzer: Secure Communication in Home and Building Automation Systems.
 PhD thesis, Vienna University of Technology, Automation Systems Group, 2010

Funktionale Anforderungen

Management- und Prozessdaten



Authentication

- Sender
- Receiver(s)
- Key Management



Secure Channel

- Confidentiality
- Integrity
- Freshness



Domänen-spezifische Anforderungen

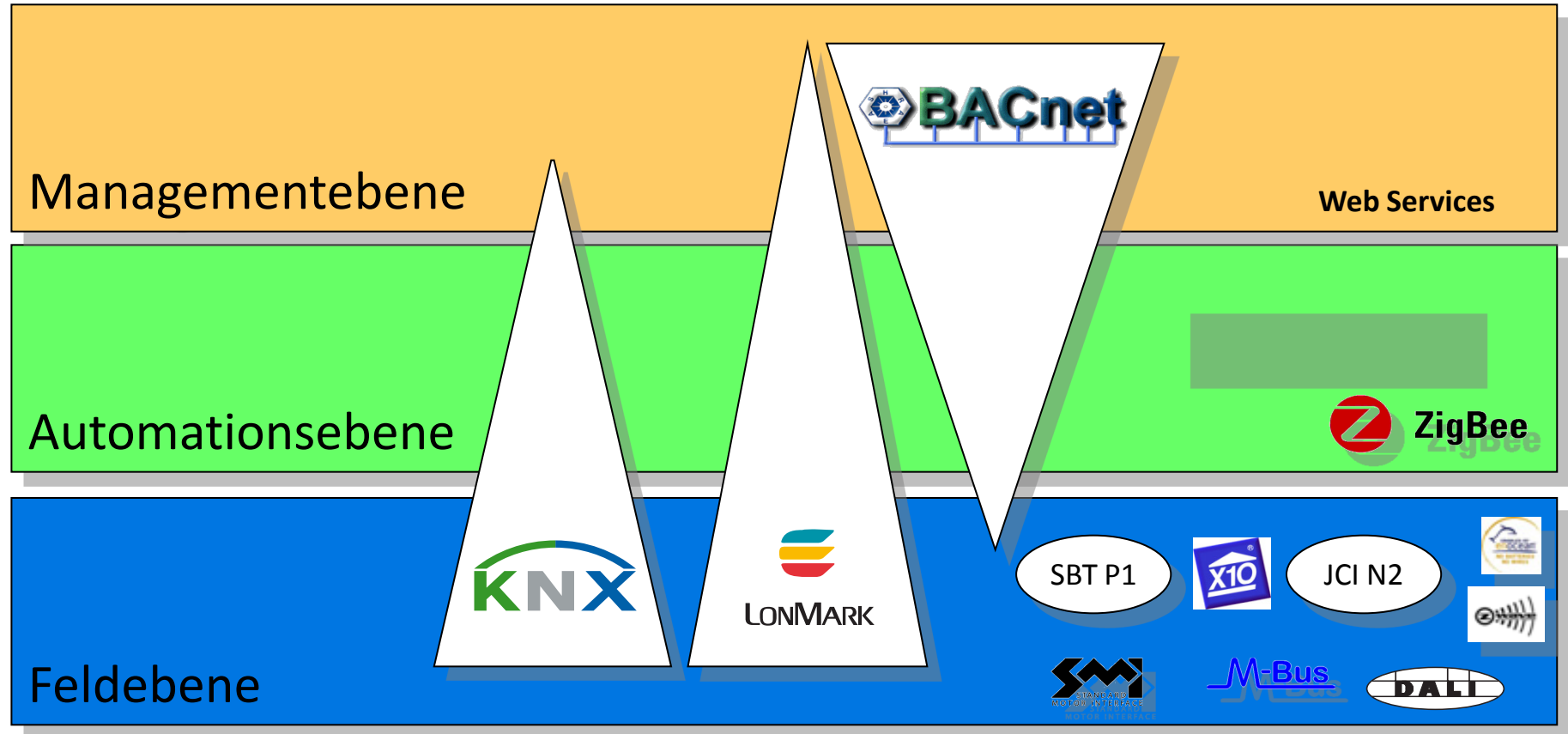
- **Eingeschränkte Ressourcen**
 - Wenig Rechenleistung
 - Limitierter Speicherplatz
 - → Anwendbarkeit von IT Technologie?
- **Skalierbarkeit**
 - Tausende Knoten
 - Installation und Updates
 - → Anleihen bei Wireless Sensor Networks (WSN) Technologie?
- **Kompatibilität!**



Weitere Anforderungen

- Kommunikationsmodelle
 - Unicast (client/server)
 - Multicast (producer/consumer, publish/subscribe)
- Non-IP Automationsnetze
 - Feldbussysteme sind nicht IP basierend
- QoS Parameters
 - Zuverlässigkeit (integrity, no duplicates, liveness)
 - Message ordering (single source FIFO, causal, total)

Offene Systeme



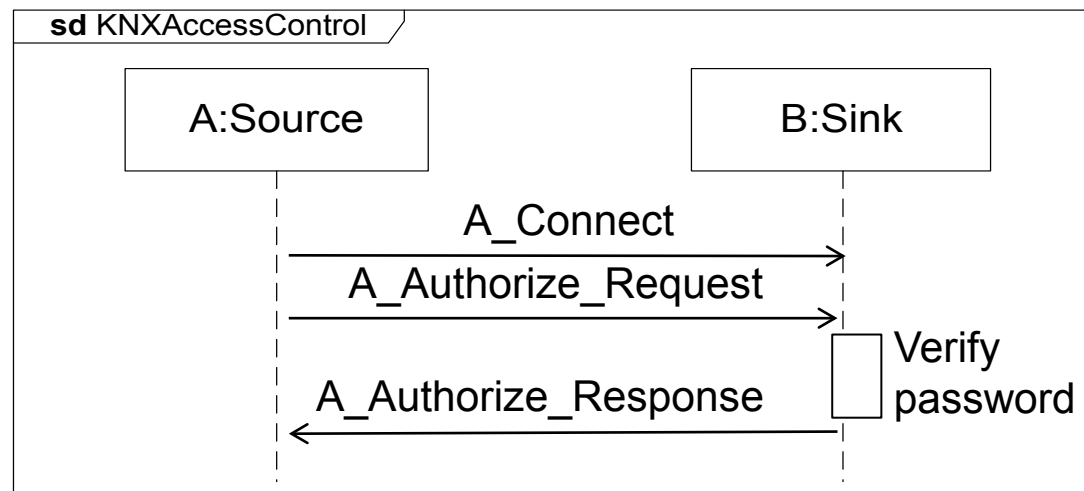
KNX

- Batibus (Batiment bus)
 - Elektrische Installationstechnik, HLK
 - **EIB (Europäischer Installationsbus)**
 - Installationsbus (Insta, Siemens, Merten), populär in D-A-CH
 - Elektrische Installationstechnik, HLK
 - EHS (European Home System)
 - Integration von weißer und brauner Ware
 - KNX (EN 50090, ISO/IEC 14543)
-
- Typisch: Automations- und Feldfunktion integriert
 - Einheitliches Konfigurationstool;
interoperable „Easy-Modes“ ohne PC



Security in KNX

- Ursprünglich keine sicheren Kommunikationsdienste
- (Rudimentärer) Zugriffsschutz für das Management von Geräten (Engineering)
- 4 Byte (unverschlüsseltes) Passwort

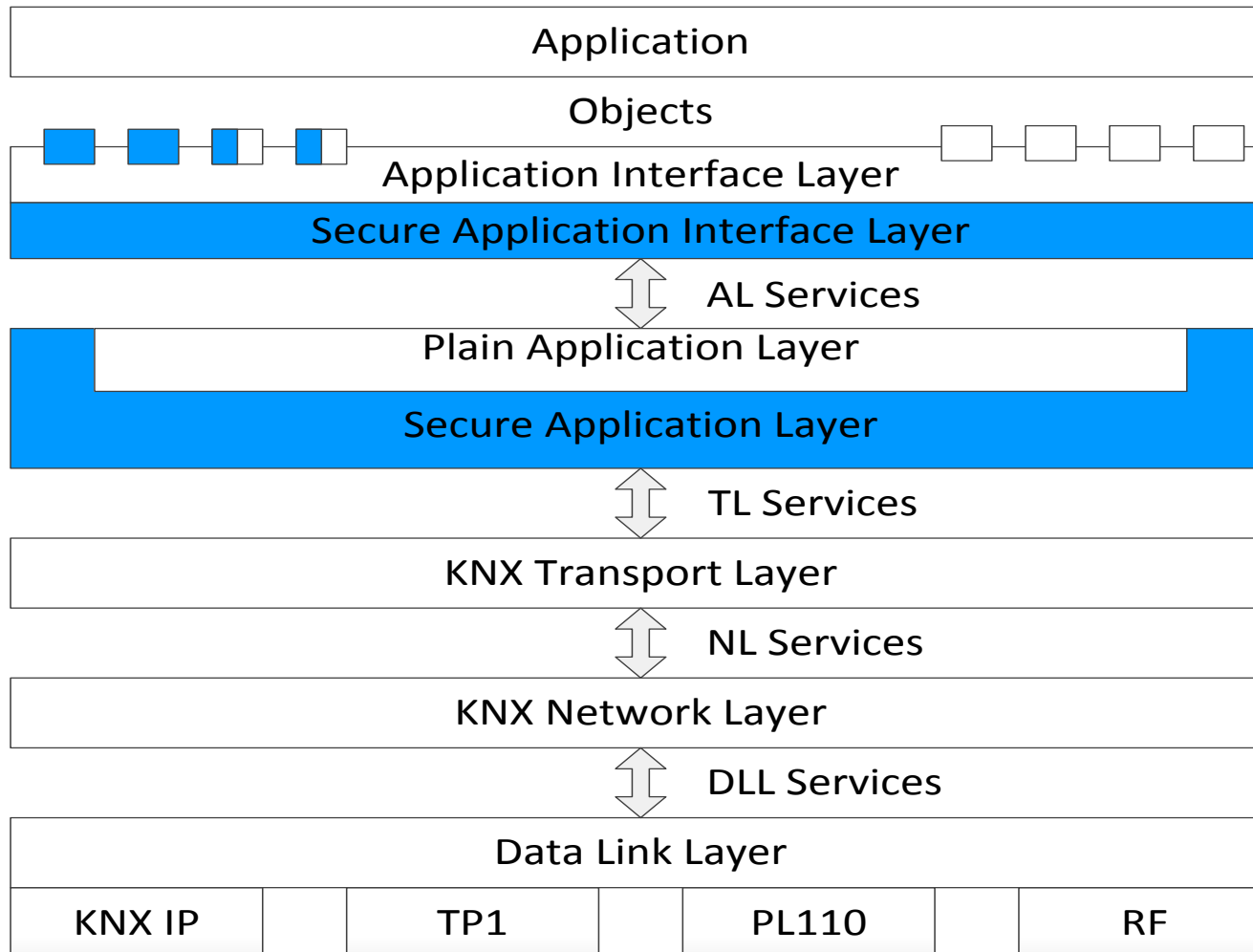


KNX Sicherheitskonzept

Basierend auf zwei Säulen

- **KNX Data Security**
 - Verschlüsselung und Authentifizierung auf Applikationsschicht
 - Medien-unabhängige Verschlüsselung
 - Feingranulare Autorisierung auf Datenpunktebene
- **KNX IP Secure**
 - Verschlüsselter und authentifizierter Übertragungskanal
 - Berücksichtigt spezielle Anforderungen IP-basierter Systeme
 - Sichert KNXnet/IP Konfigurations- und Managementdienste

KNX Data Security

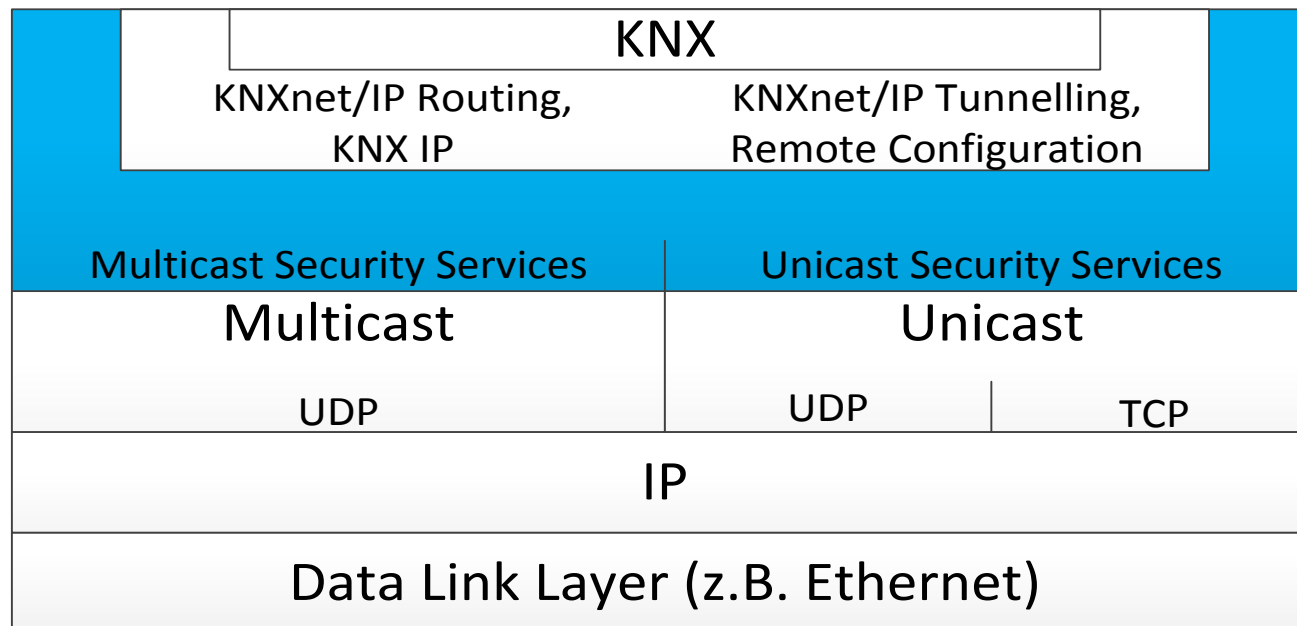


**Autorisierung auf
Objektebene**

**Authentifizierung &
Verschlüsselung**

KNX IP Secure

- Sichere Kapselung von KNXnet/IP Paketen
 - Authentifizierung & Verschlüsselung (AES+CCM)
 - Unicast via TCP oder UDP (KNXnet/IP Tunnelling)
 - Multicast via UDP (KNXnet/IP Routing)



LonWorks

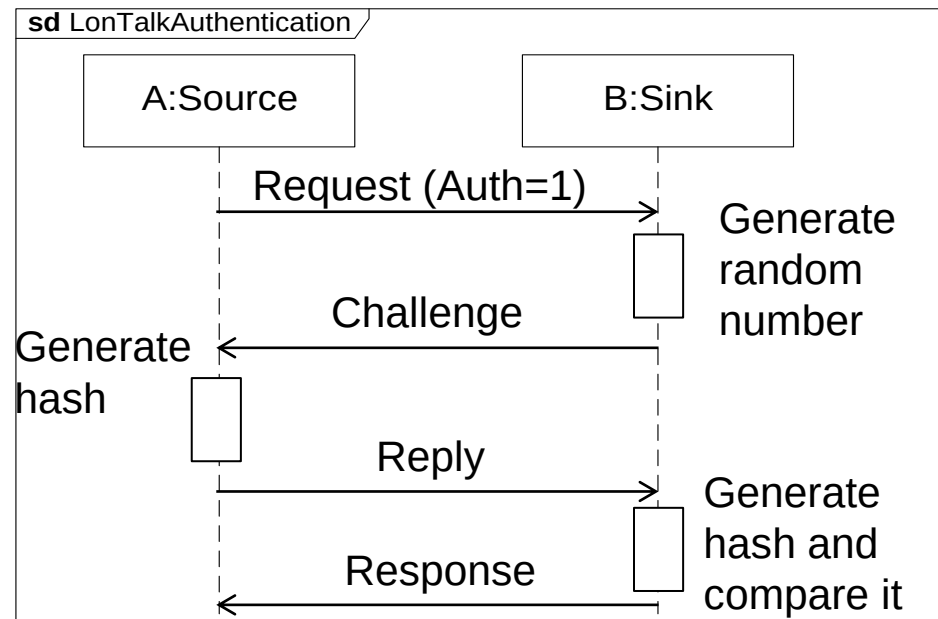
- Entworfen von Echelon Inc. als allgemein anwendbares, ereignisgesteuertes Embedded-Netzwerk für Steuerungszwecke
- LonTalk-Protokoll (ANSI/EIA/CEA-709, EN 14908): „CNP“
- „Neuron“-Chip
- Network Management Tool (LNS); ISI (Interop. Self Install.)
- Netzwerkvariablen
- Interoperabilität: LonMark



LONMARK

Security in LonWorks

- Four step challenge-response protocol
 - Überprüfung des Senders
 - Data integrity
 - Data freshness



BACnet

- „Building Automation and Control Network“
- American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE)
- ANSI/ASHRAE 135 ► ISO 16484-5
- BACnet Interest Groups, BACnet International, Testing Labs
- Kann lizenzfrei implementiert werden
- Netzwerkneutral (auch IP)
- Objekte und Dienste

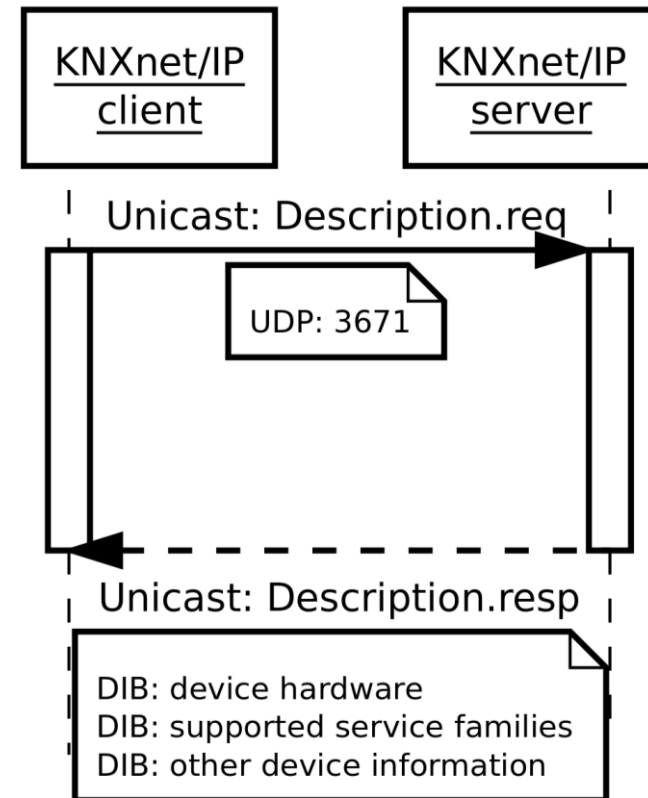
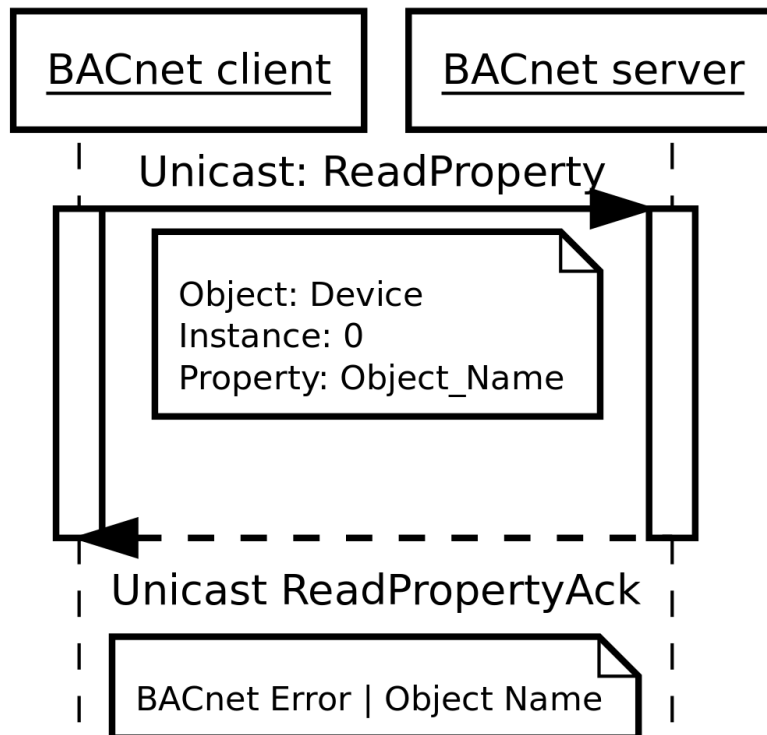


Security in BACnet

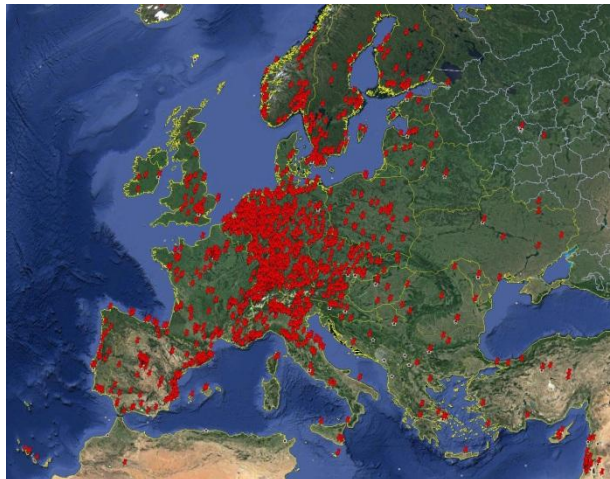
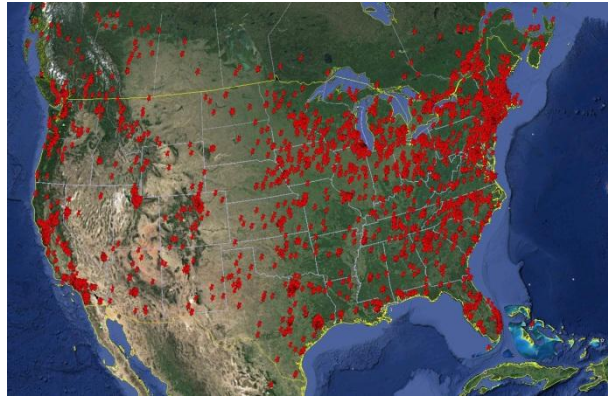
- Verwendet AES und HMAC in Kombination mit MD5 und SHA
- Trusted Keyserver zur Schlüsselverteilung
- 6 verschiedene Schlüssel werden unterschieden:
 - General-Network-Access, User-Authenticated, Application-Specific, Installation, Distribution, Device-Master
- Dienste für sicheren Datentransfer und Schlüsselaustausch
 - Plain-Non-Trusted; Plain-Trusted, Signed-Trusted, Encrypted-Trusted
- Definition von Vertrauensstufen (Trust Levels) und Sicherheitsrichtlinien (Security Policies)

Sichere Installationen?

■ Angriffsvektor



Ergebnisse



Country	BACnet	Country	KNX
US, United States	8989	DE, Germany	627
CA, Canada	2296	NL, Netherlands	522
FI, Finland	282	ES, Spain	332
AU, Australia	271	FR, France	244
ES, Spain	231	AT, Austria	220
FR, France	148	CH, Switzerland	204
SE, Sweden	138	IT, Italy	173
GB, United Kingdom	131	NO, Norway	129
DE, Germany	118	SE, Sweden	120
KR, Korea, Republic of	110	BE, Belgium	119
NO, Norway	103	IL, Israel	109
IT, Italy	101	PL, Poland	67
CZ, Czech Republic	98	GB, United Kingdom	56
TW, Taiwan	97	GR, Greece	42
NL, Netherlands	89	CZ, Czech Republic	30
NZ, New Zealand	47	RU, Russian Federation	24
HK, Hong Kong	45	VN, Vietnam	23
JP, Japan	44	TR, Turkey	21
AT, Austria	42	LT, Lithuania	20
CH, Switzerland	39	PT, Portugal	20
worldwide	13964	worldwide	3295

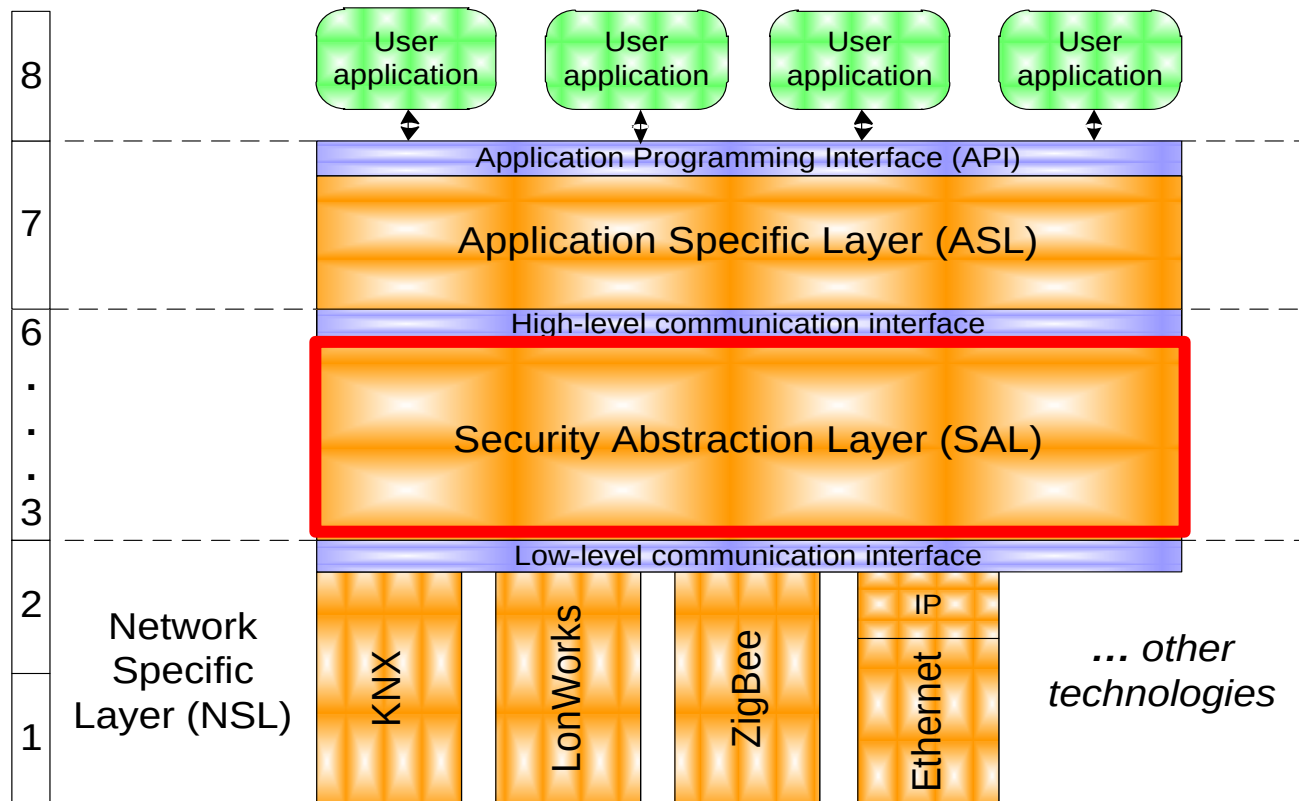
Maßnahmen

- Attack prevention
 - Integration von Security in den Lebenszyklus
 - Definition von Security Policies
 - Firewalls, Datenverschlüsselung, ...
- Attack detection
 - Falls präventive Maßnahmen nicht möglich sind, müssen Attacken zumindest erkannt werden
 - Intrusion Detection Systems
- Hybride Ansätze

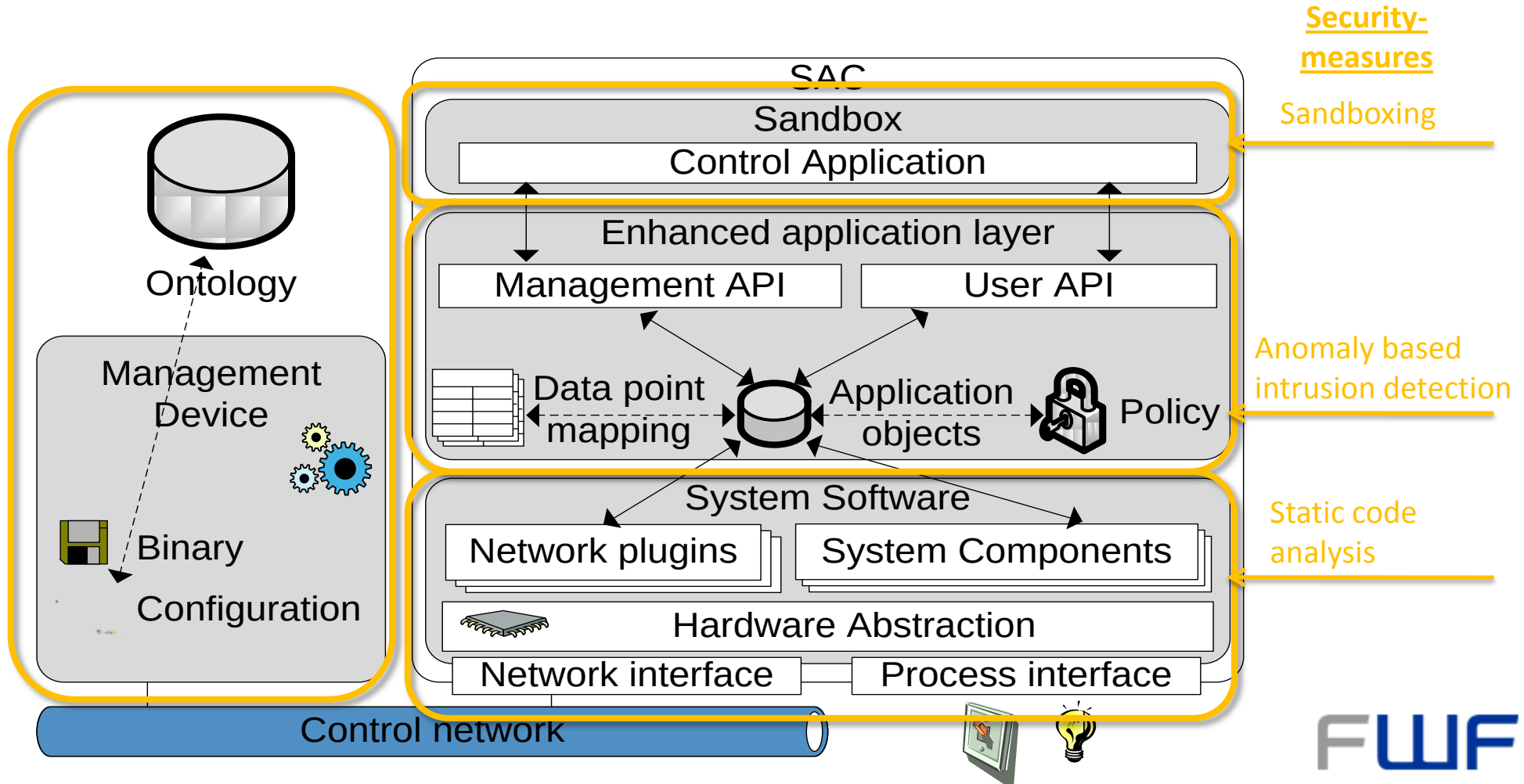


Sichere Gebäudeautomation

■ Generisches Konzept zur sicheren Datenübertragung

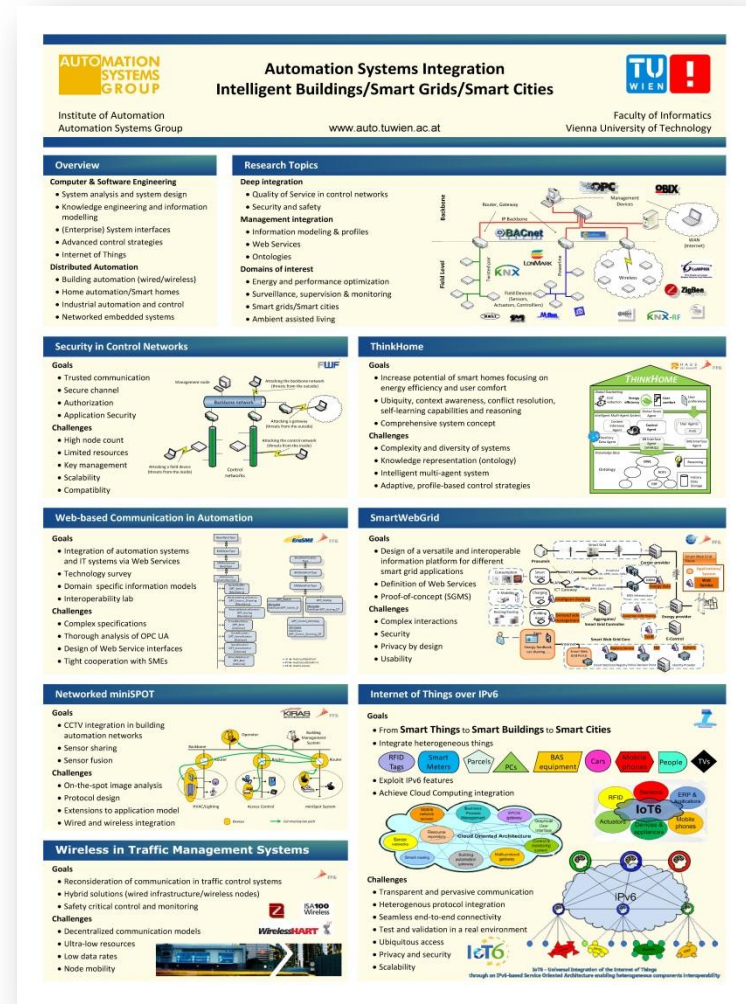


Sichere Gebäudeautomation



Zusammenfassung

- Sicherheit betrifft das ganze „System“ Gebäude!
- Netzwerk- UND Gerätesicherheit
- Integrative Ansätze!
- Ausbildung?
- Awareness?
- Safety & Security!



Referenzen

- Security in Building Automation, FWF (P19673) <https://www.auto.tuwien.ac.at/seBAS/>
- Wolfgang Kastner, Lukas Krammer, and Andreas Fernbach. *State of the Art in Smart Homes and Buildings*, CRC Press, 2014.
- Wolfgang Kastner, Markus Jung, and Lukas Krammer. *Future Trends in Smart Homes and Buildings*, CRC Press, 2014.
- Fritz Praus, and Wolfgang Kastner. Identifying unsecured building automation installations. *Proc. 19th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA'2014)*, 1-4, September 2014.
- Aljosha Judmayer, Lukas Krammer, and Wolfgang Kastner. On the security of security extensions for IP-based KNX networks. In *Proc. of the 10th IEEE International Workshop on Factory Communication Systems (WFCS 2014)*, 1-10, May 2014.
- Lukas Krammer, Steven De Bruyne, Wolfgang Kastner, and Wolfgang Granzer. *Security Erweiterung für den KNX Standard*, innosecure, 1-10, September 2013.
- Wolfgang Granzer, Fritz Praus, and Wolfgang Kastner. Security in Building Automation Systems. *IEEE Transactions on Industrial Electronics*, 57(11):3622-3630, November 2010.
- Wolfgang Granzer and Wolfgang Kastner. Security Analysis of Open Building Automation Systems. *Proc. 29th International Conference on Computer Safety, Reliability and Security (SAFECOMP '10)*, 303-316, September 2010.