TeleTrusT-Informationstag

"IT-Sicherheit im Smart Home und der Gebäudeautomation"

Berlin, 12.11.2014

Aktuelle und zukünftige Funktionalitäten in der Gebäudeautomation und notwendige IT-Sicherheitsbetrachtungen

Sascha Remmers, LOYTEC electronics GmbH
Christian Nordlohne, Institut für Internetsicherheit

Vorstellung

Sascha Remmers

- Elektrotechnikermeister und Betriebswirt (HWK)
- Seit 2008 technischer Vertrieb von GA-Systemen
- Seit 2013 bei LOYTEC electronics GmbH mit Sitz in Wien
  - Hersteller von Produkt- und Systemlösungen für alle Bereiche und Protokolle der Gebäudeautomation

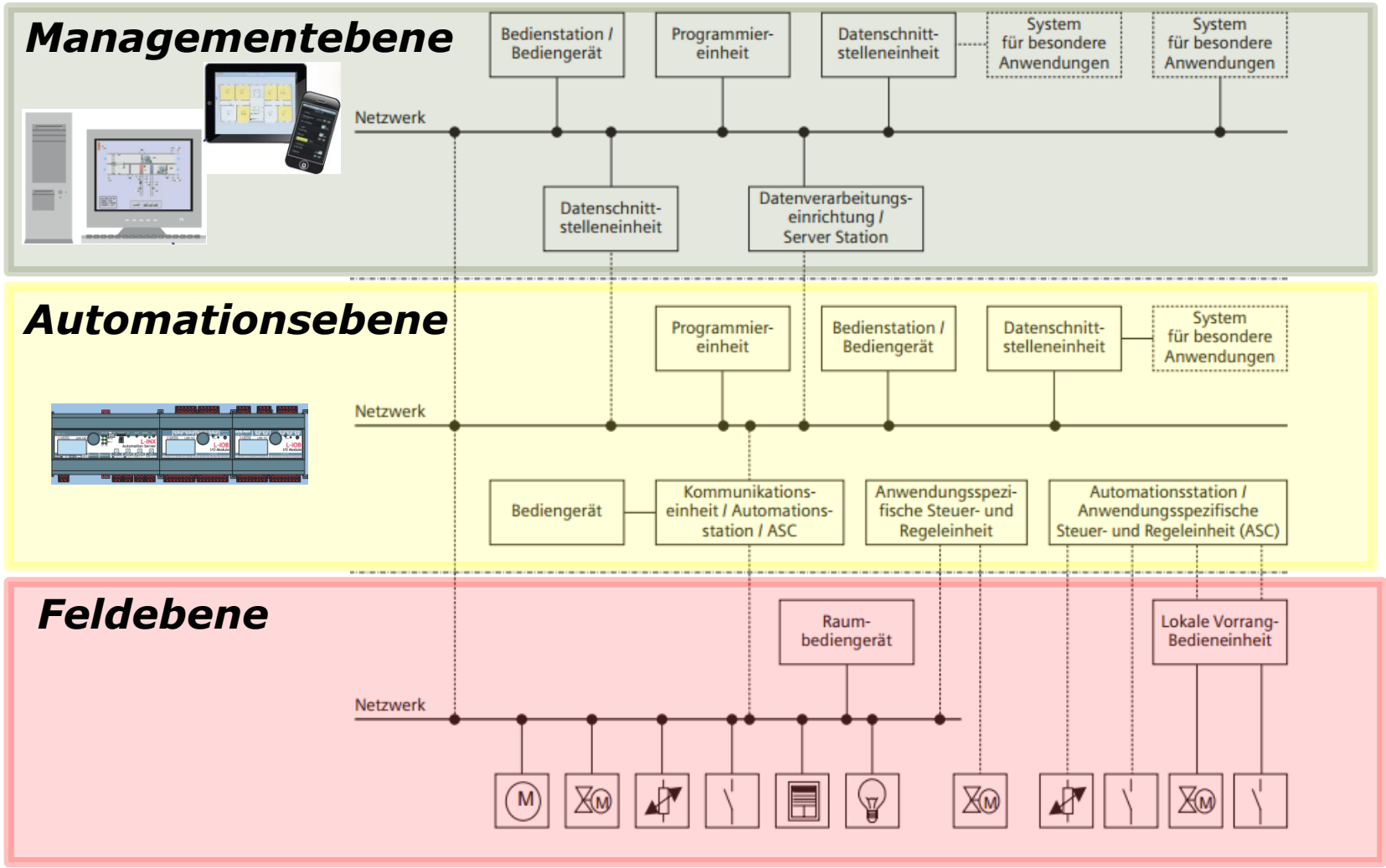
Begriffsdefinition

Gebäudeautomation

Bezeichnung für die 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.

DIN EN ISO 16484-2:2004

Systemmodell nach EN ISO 16484-2



Argumente für die Automatisierung von Gebäuden

- Energieeffizienz

Optimierung des Verhältnisses zwischen eingesetzter Energie und erzieltem Nutzen durch automatische Steuerung und Regelung

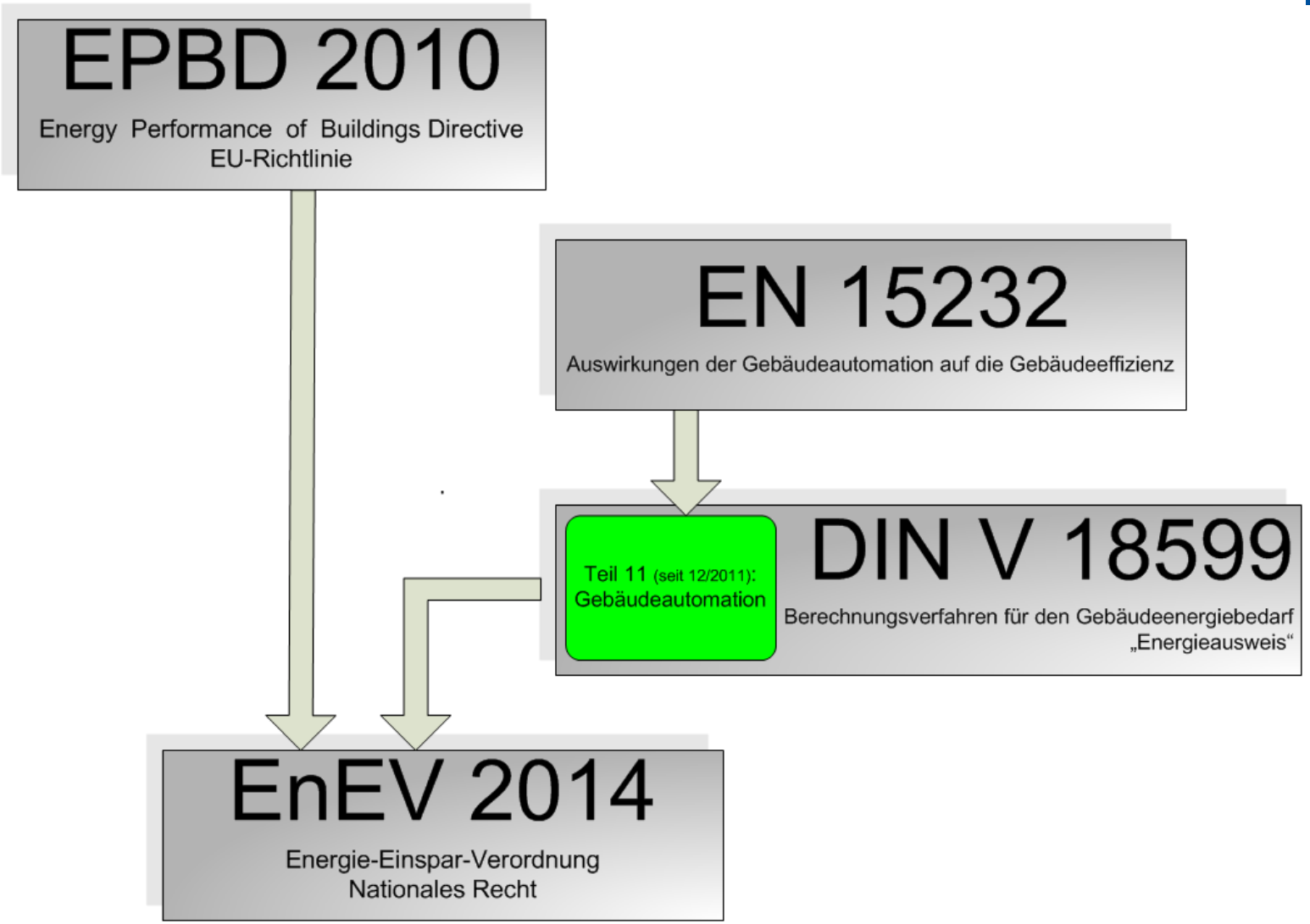
- Komfort

Blendschutz, Optimierung des Raumklimas, der Lichtverhältnisse und der Luftqualität, Bedienkomfort

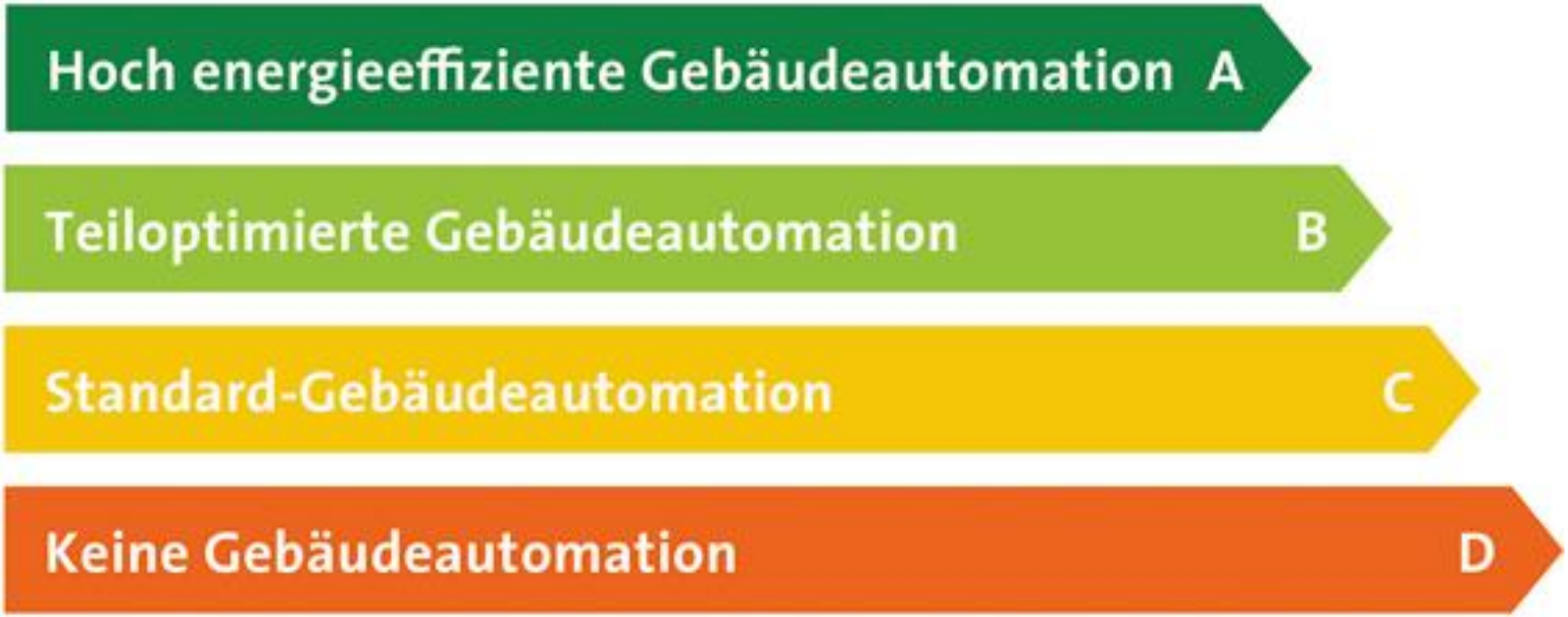
- Flexibilität

Zuordnung von Bediengeräten und Verbrauchern ohne Installationsänderungen, flexible Flächennutzung

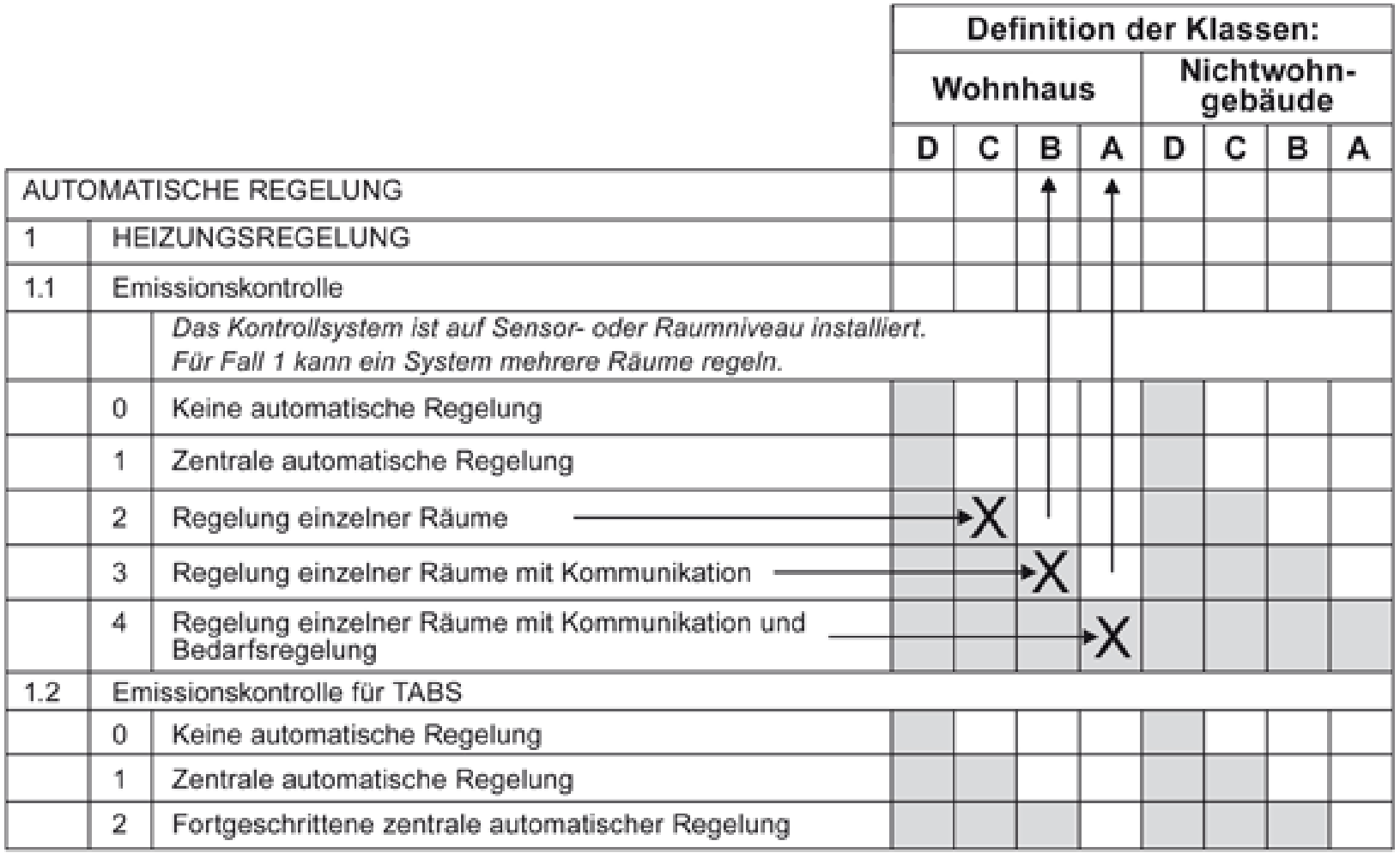
Normen und Richtlinien



EN 15232: Energieeffizienzklassen



EN 15232: Bewertungsmatrix



			Definition der Klassen:							
			Wohnhaus				Nichtwohn-gebäude			
			D	C	B	A	D	C	B	A
AUTOMATISCHE REGELUNG										
1	HEIZUNGSREGELUNG									
1.1	Emissionskontrolle									
		Das Kontrollsystem ist auf Sensor- oder Raumniveau installiert. Für Fall 1 kann ein System mehrere Räume regeln.								
	0	Keine automatische Regelung								
	1	Zentrale automatische Regelung								
	2	Regelung einzelner Räume		X						
	3	Regelung einzelner Räume mit Kommunikation			X					
	4	Regelung einzelner Räume mit Kommunikation und Bedarfsregelung				X				
1.2	Emissionskontrolle für TABS									
	0	Keine automatische Regelung								
	1	Zentrale automatische Regelung								
	2	Fortgeschrittene zentrale automatischer Regelung								

EN 15232: Übersicht

Heizen/Kühlen	Sonnenschutz	Beleuchtung	Belüftung
Einzelraumregelung mit **präsenzabhängiger** Regelung und Kommunikation zu Primäranlagen zur **lastabhängigen** Regelung der Wassertemperatur	Kombinierte Regelung des Sonnenschutzes, der Beleuchtung und der HLK-Anlagen **entsprechend der Belegung**	Automatisches Ausschalten **bei Abwesenheit** mit automatischer Regelung entsprechend dem Tageslichteinfall	**Bedarfsabhängige** Regelung mit freier Kühlung durch Außenluft
Einzelraumregelung mit Kommunikation zwischen Regeleinrichtungen und GA-System (z.B. Zeitprogramme) und Kommunikation zu Primäranlagen zur lastabhängigen Regelung der Wassertemperatur			Anwesenheitsabhängige Regelung mit freier Nachtkühlung
Einzelraumregelung durch Thermostatventile oder elektronische Regeleinrichtungen und witterungsabhängige Regelung der Wassertemperatur	Motorbetrieben mit automatischer Regelung	Manueller Ein-/Ausschalter mit automatischem Ausschaltsignal und manueller Steuerung nach Tageslichteinfall	Zeitabhängige Regelung mit Nachtkühlbetrieb
Keine automatische Regelung	Motorbetrieben mit manueller Regelung/ manuelle Betätigung	Manueller Ein-/Aus-Schalter	Keine automatische Regelung

EN 15232: Einsparpotenziale

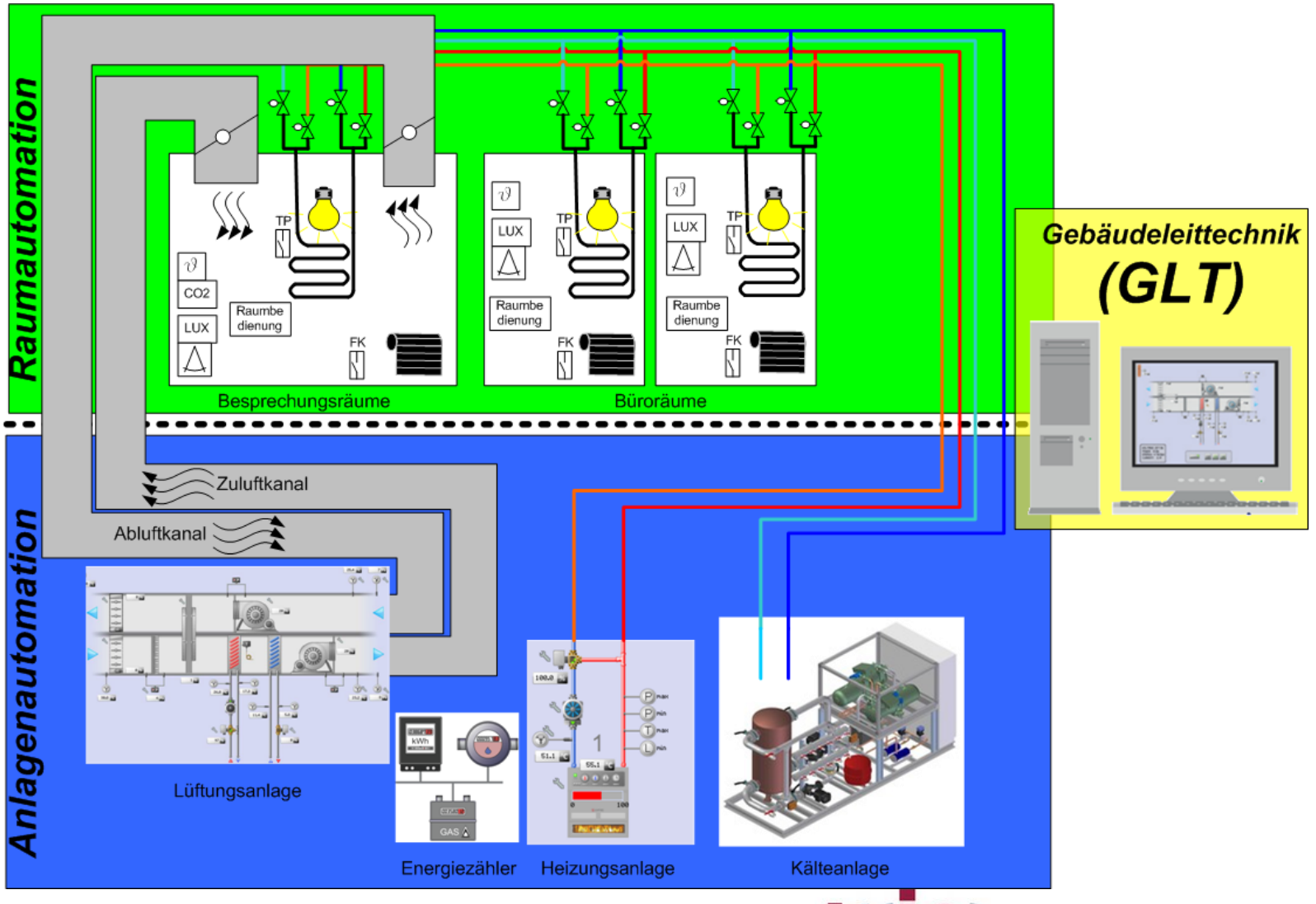
Gebäudetypen	BACS-Effizienzfaktoren $f_{BSCS,th}$				
	D	C (Referenz)	B	A	
	Nicht energieeffizient	Standard	Erweitert	Hohe Energieeffizienz	
Büros	1,51	1	0,8	0,7	thermisch
Hörsaal	1,24	1	0,75	0,5	
Schule	1,20	1	0,88	0,8	
Hotel	1,31	1	0,85	0,68	
Büros	1,10	1	0,93	0,87	elektrisch
Hörsaal	1,06	1	0,94	0,89	
Schule	1,07	1	0,93	0,86	
Hotel	1,07	1	0,98	0,96	

EN 15232: Einsparpotenziale

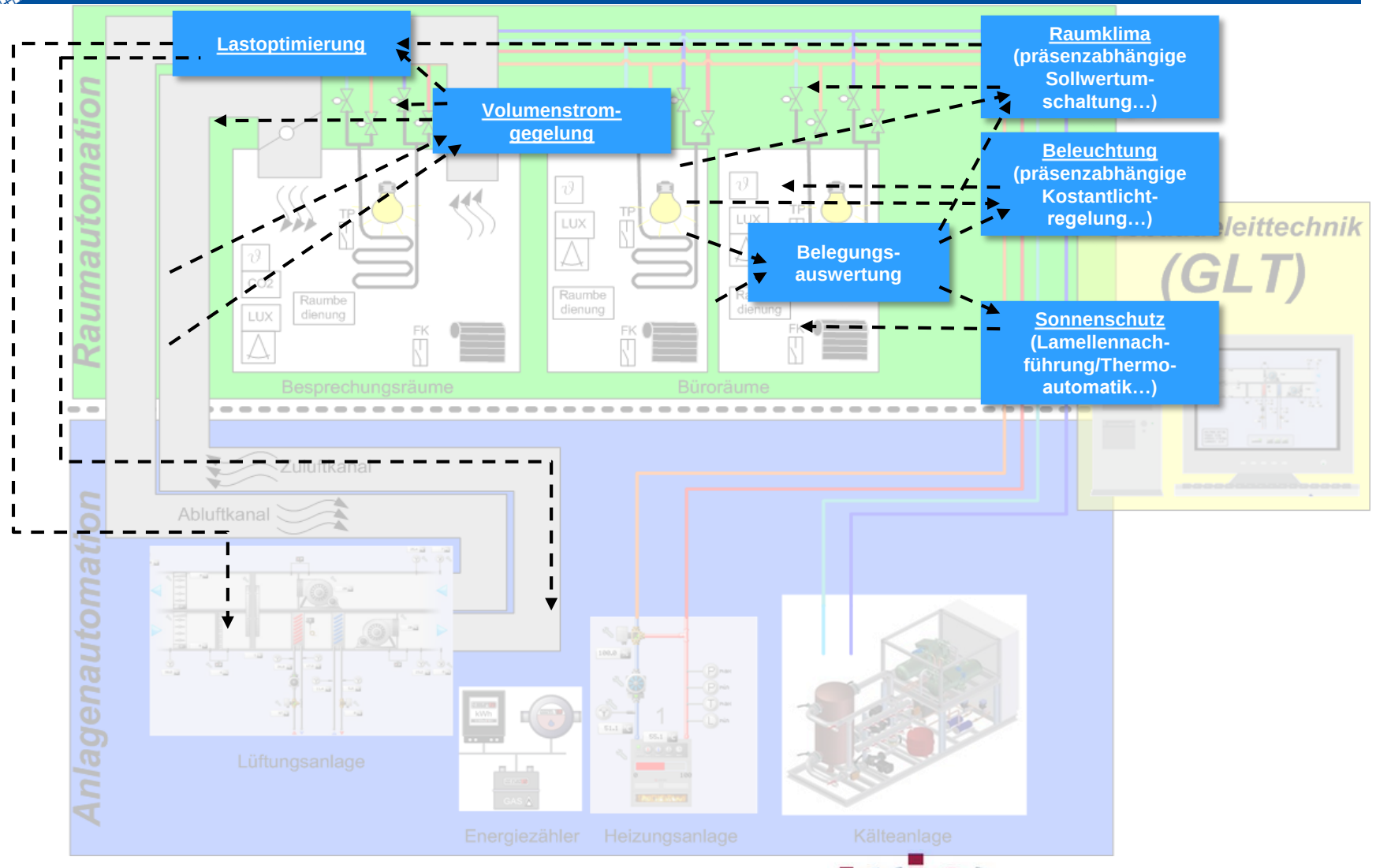
	Einfamilienhaus	Mehrfamilienhaus
Thermisches Einsparpotenzial	6%-7%	3%-4%
Elektrisches Einsparpotenzial	20%-24%	18%-22%

(Quelle: S. Sander, M. Krödel, H. Krause: "Ermittlung des Energieeinsparpotenzials durch Gebäudeautomation in Wohngebäuden anhand verschiedener Wohnsituationen")

Umsetzung am Beispiel Bürogebäude



Umsetzung am Beispiel Bürogebäude



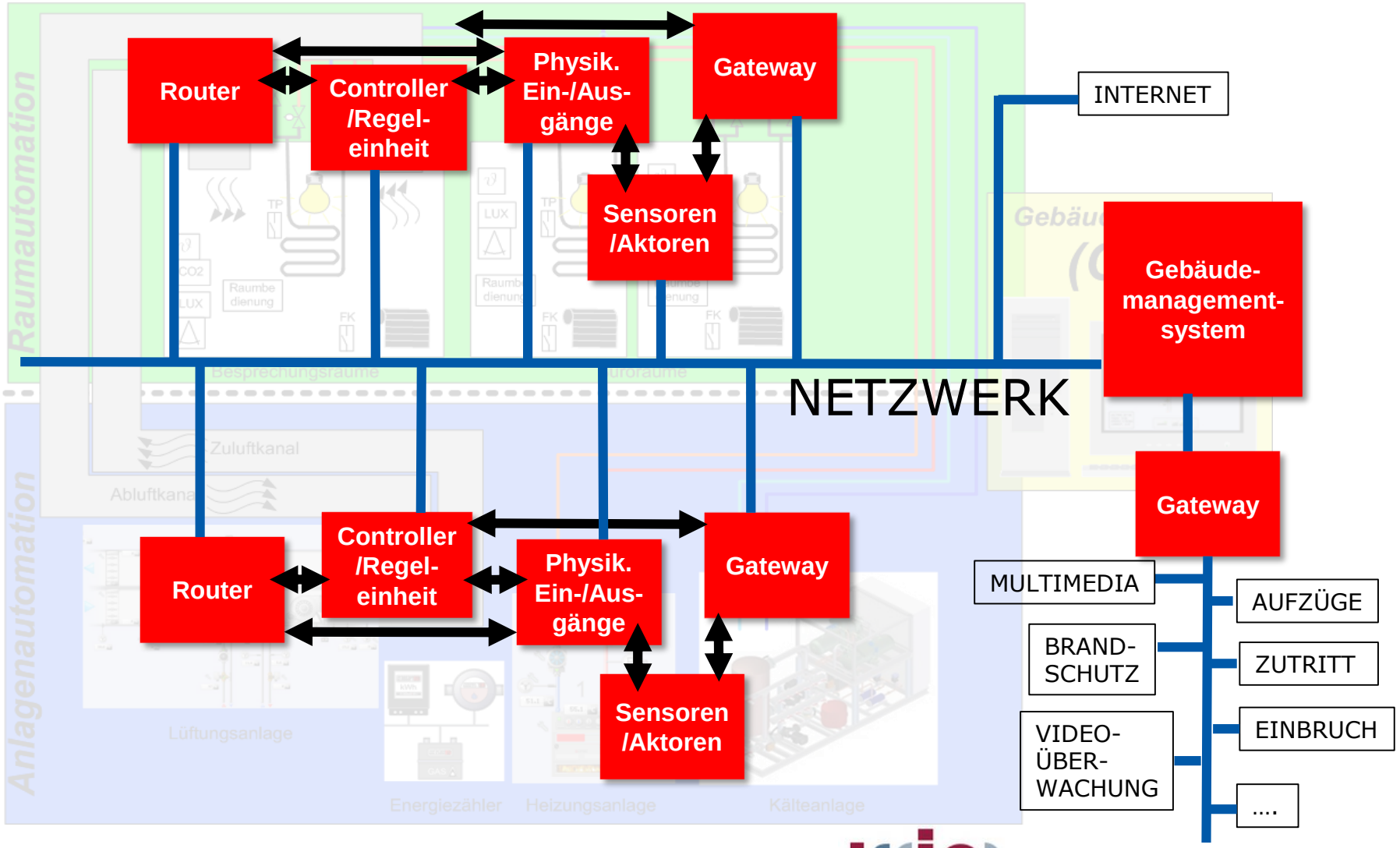
Umsetzung am Beispiel Bürogebäude

			Physikalisch		Kommunikativ		
			Digital	Analog	drahtgebunden	Funk	
SENSOREN		Fensterkontakt	X			X	
		Taupunkt	X		X		
		Lichtstärke		X	X	X	Licht+Präsenz meist gemeinsam in einem Multisensor
		Präsenzerkennung	X		X	X	
		Luftqualität		X	X	X	Luftqu.+ Raumtemp.meist gemeinsam in einem Multisensor
		Raumtemperatur		X	X	X	
	Raumbedienung	Anwesenheit manuell	X		X	X	
		Bedienung Licht	X		X	X	
		Bedienung Jalousien	X		X	X	
		Sollwertverstellung	X		X	X	
AKTOREN		Ventilstellantriebe	X	X	X	X	
		Leuchten	X	X	X		
		Jalousiemotor	X	X	X		
		Volumenstromregler	X	X	X	X	

Umsetzung am Beispiel Bürogebäude

Protokoll	Varianten	Typischer Einsatzzweck
BACnet	BACnet MS/TP, BACnet-IP	Managementebene/Automationsebene
OPC	OPC XML/DA, OPC UA	Managementebene/Visualisierungen
LON	LON-FT10, LON-IP	Raumautomation/Feldebene
KNX	KNX TP1, KNXnet IP	Raumautomation/Feldebene
Modbus	Modbus RTU, Modbus TCP	Feldebene
DALI		Beleuchtung/Feldebene
SMI		Jalousiemotoren/Feldebene
Enocean		Drahtlose Anbindung von Sensoren/Feldebene
MP-Bus		HLK/Feldebene
M-Bus		Energiezähler

Umsetzung am Beispiel Bürogebäude



Wer bin ich?

- Christian Nordlohne
  - Wissenschaftlicher Mitarbeiter am Institut für Internet-Sicherheit
  - Projektleiter für den Bereich Botnetze und Malware

Smart aber unsicher?

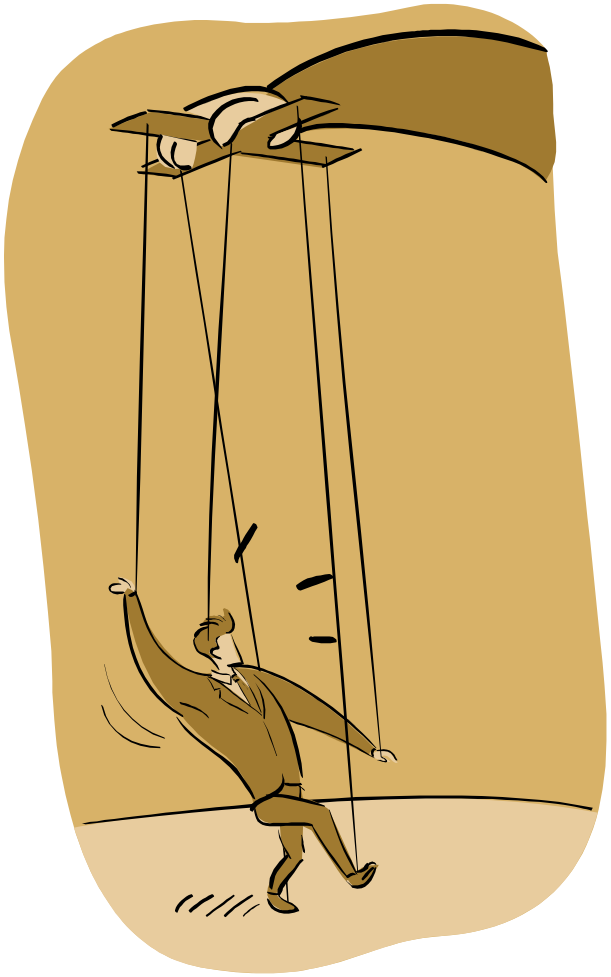
- Alles wird „smart“
- Welche Risiken bestehen für smarte Haushalte und Gebäude?
- Lassen sich gewonnene Erkenntnisse aus dem Bereich der IT-Sicherheit übertragen?
- Wo liegen die Herausforderungen für ein sicheres Smart Home?

Risiken

- Ausspähung
  - Mitlesen von Daten ermöglicht es Angreifern Informationen über Strukturen und Nutzer zu erhalten

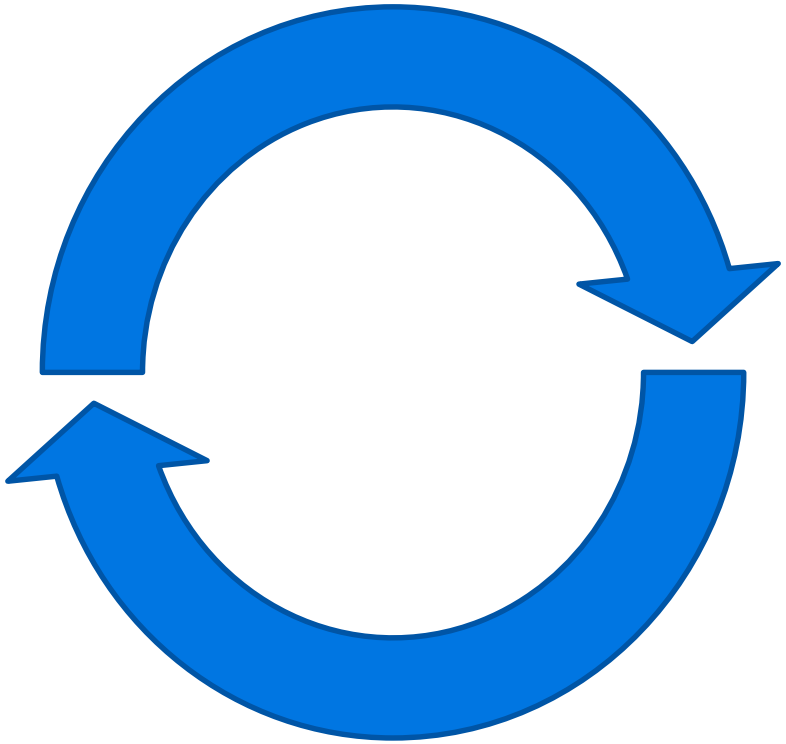
Risiken

- Manipulation
  - Das gezielte Verändern von Steuerungsdaten ermöglicht direkte Angriffe auf die Infrastruktur



Risiken

- Wiedereinspielen von Befehlen
  - Das Wiedereinspielen von Befehlen in Steuerungsnetze ermöglicht z.B. das Öffnen einer Tür



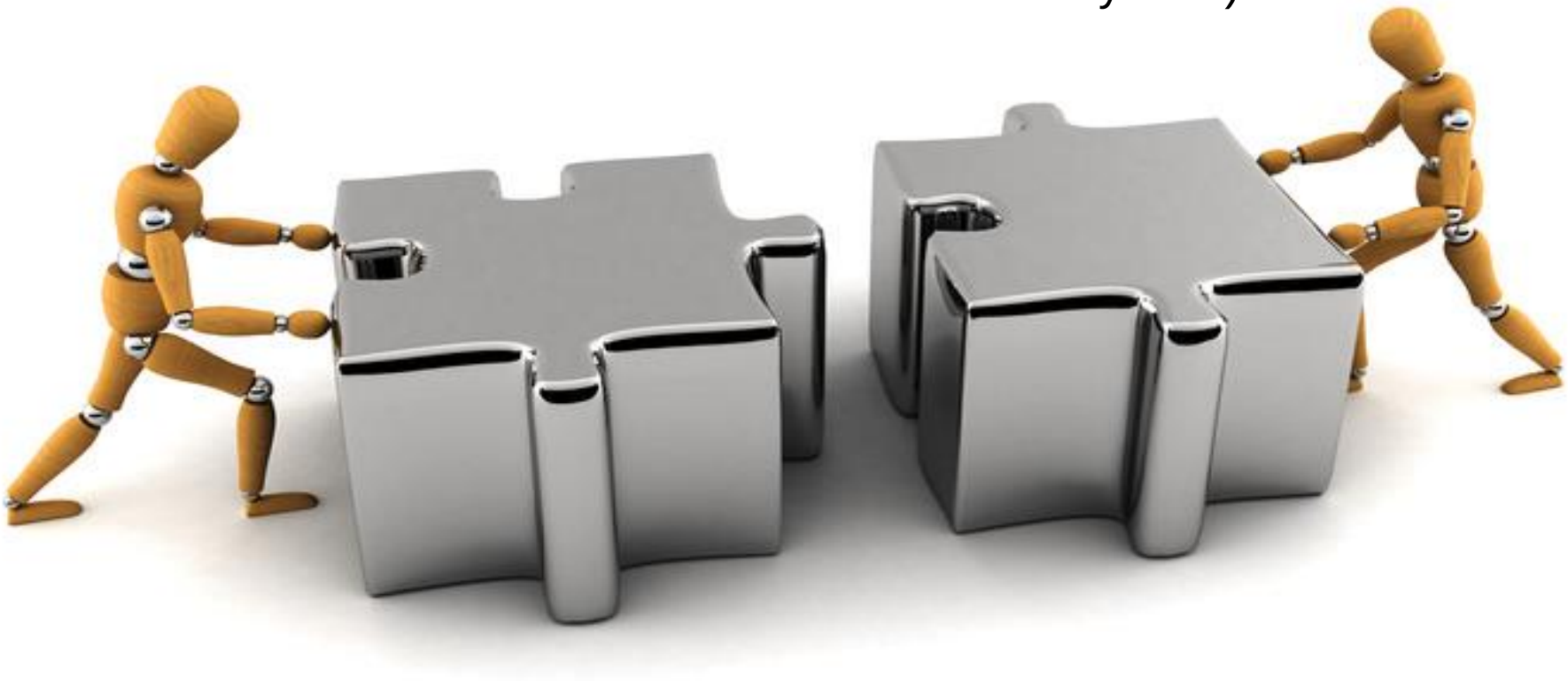
Schutzmaßnahmen kategorisieren

Externe Sicherheit

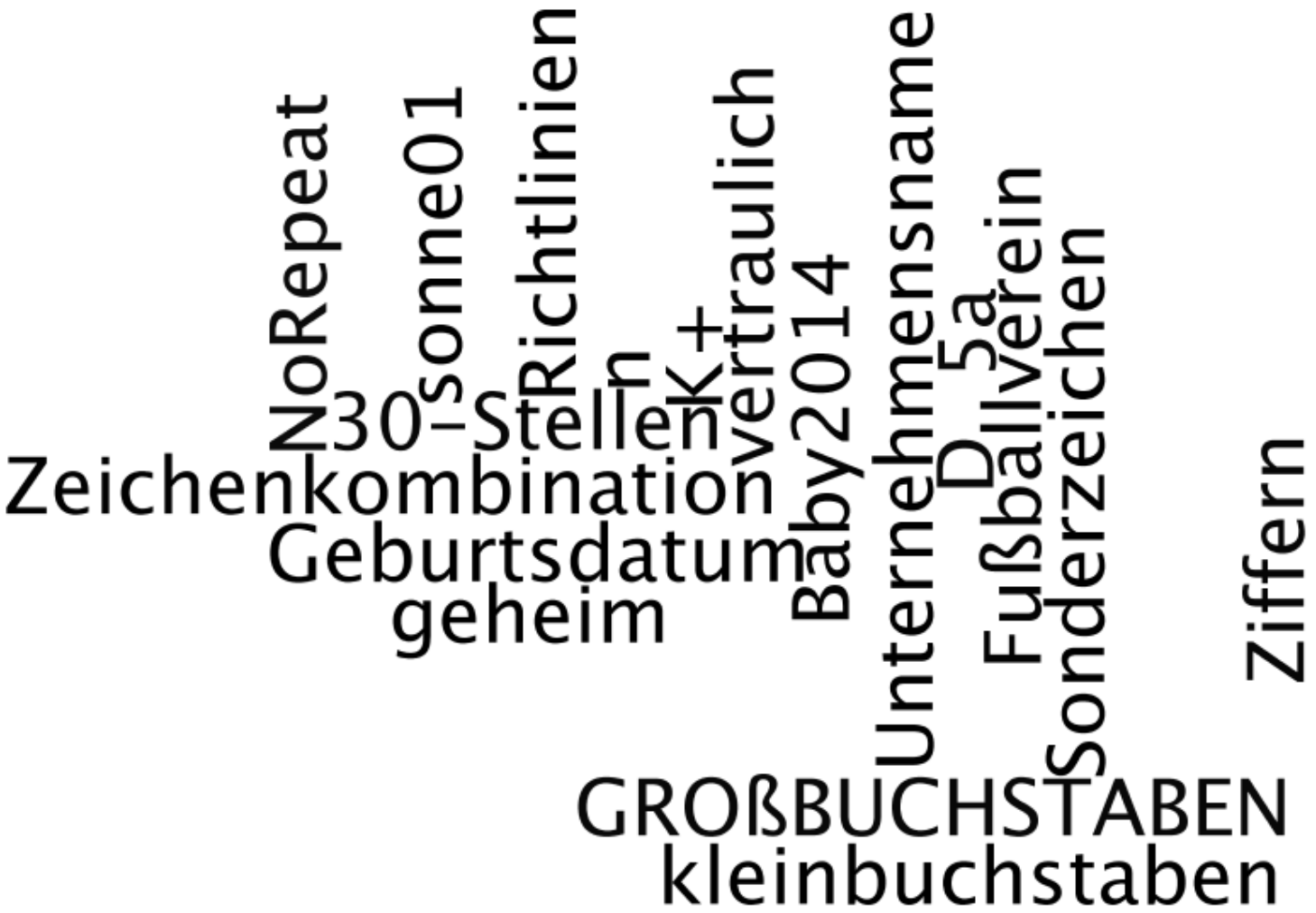
- Sicherheit gegen Angriffe übers Internet

Interne Sicherheit

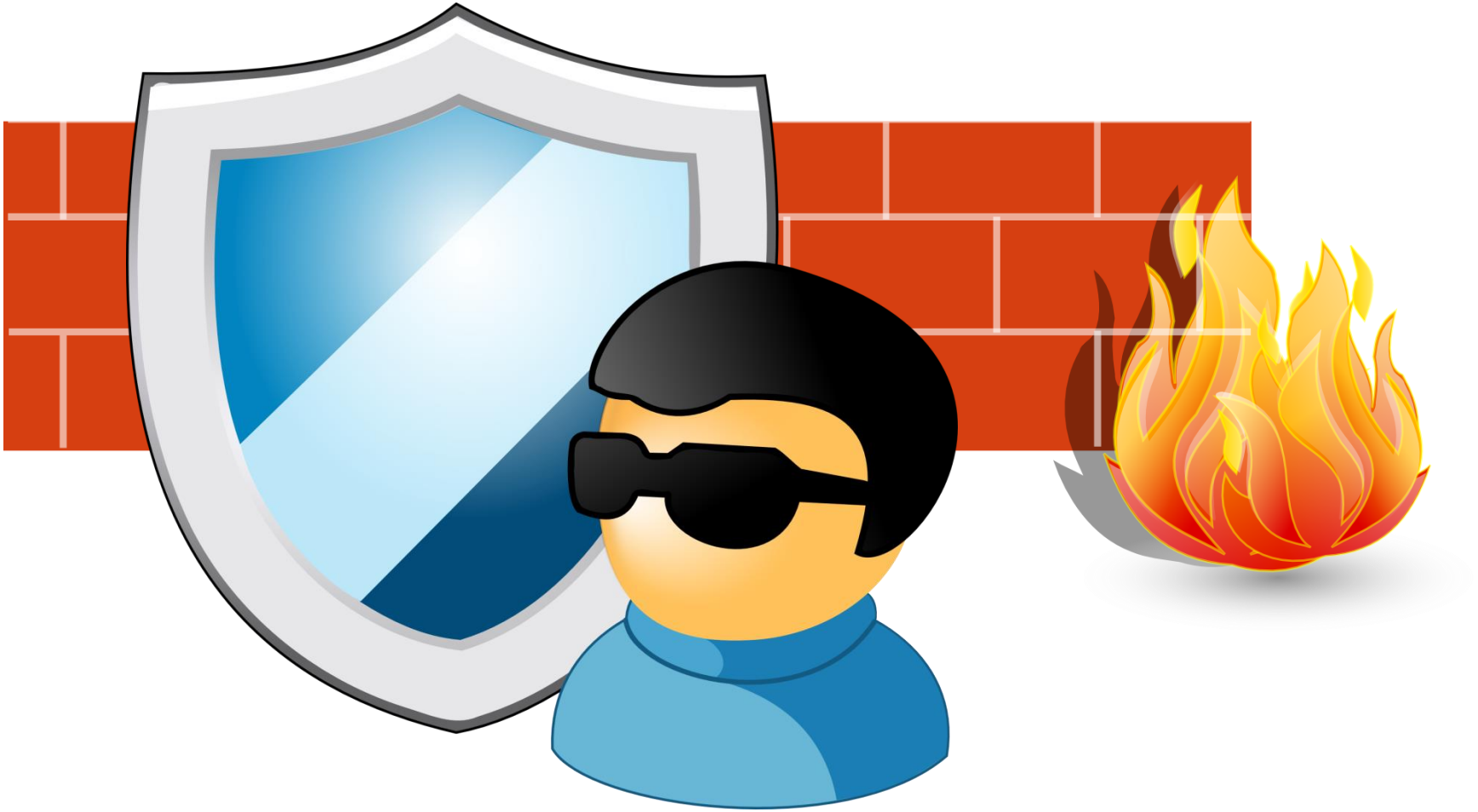
- Sicherheit des internen Netzes (LAN und Bussystem)



Interne Sicherheit: Passwörter

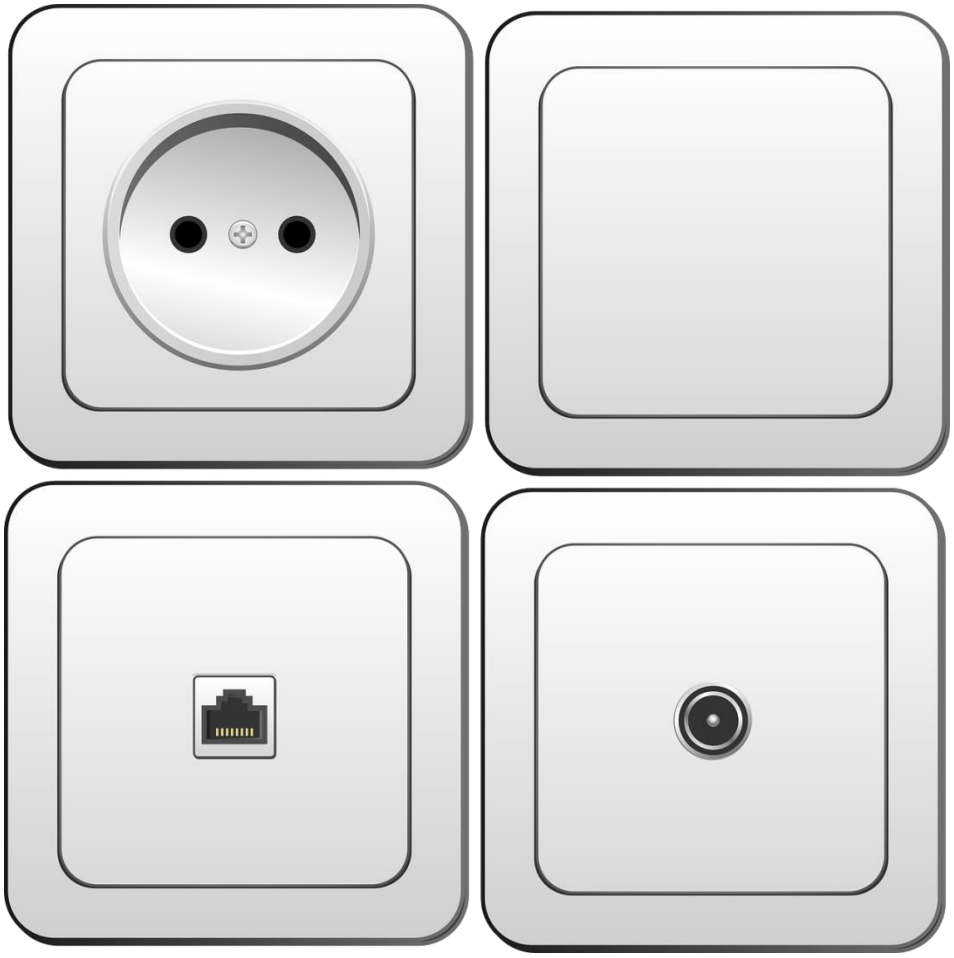


Interne Sicherheit:
Firewall und Anti-Malware

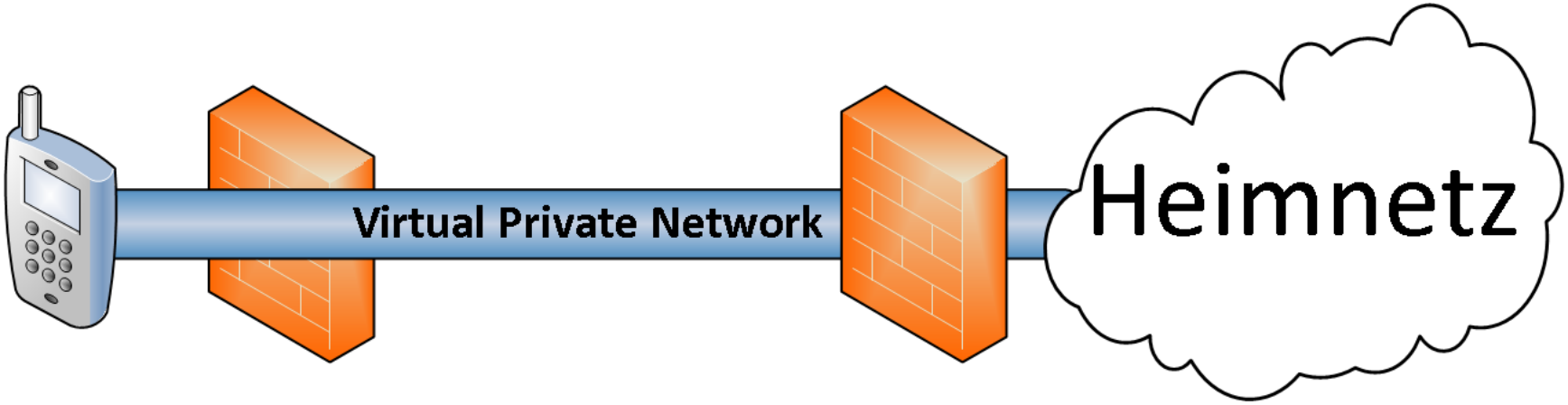


Interne Sicherheit: Verschlüsselung

Interne Sicherheit: Physikalischer Zugriff

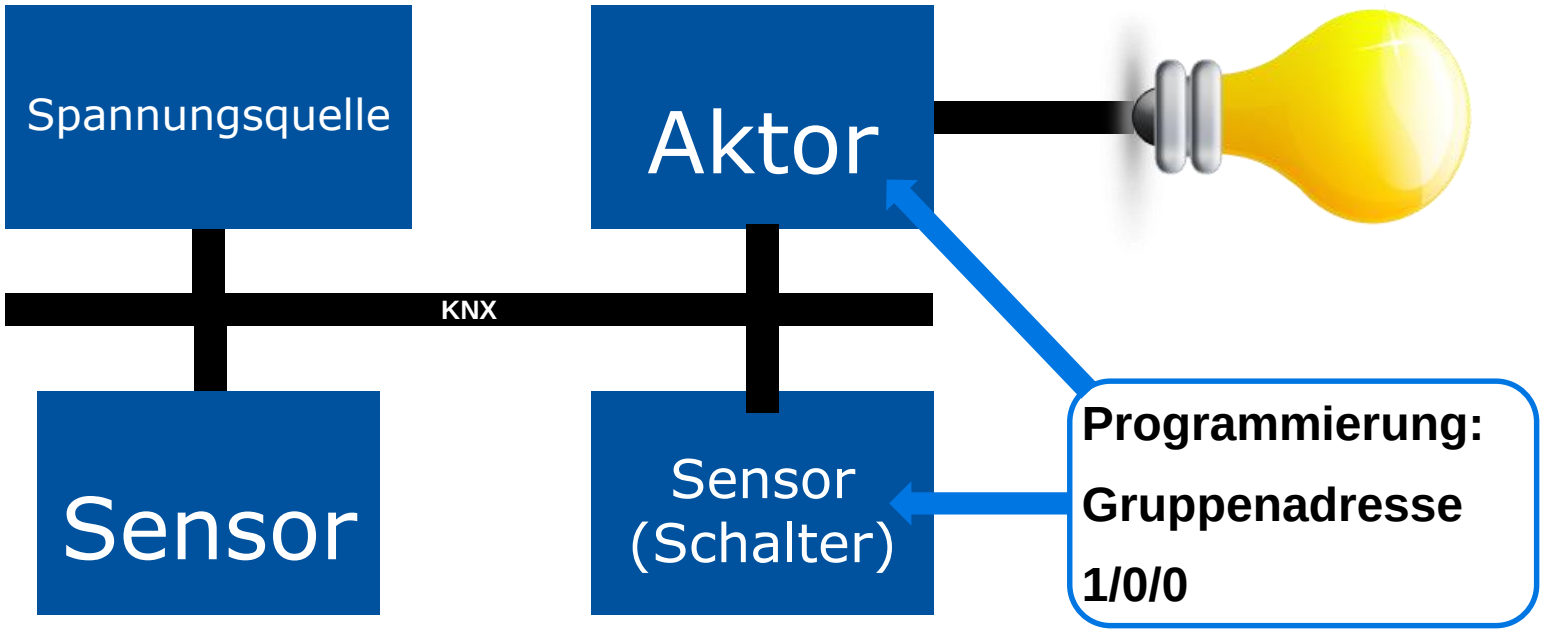


Externe Sicherheit: Virtual Private Network

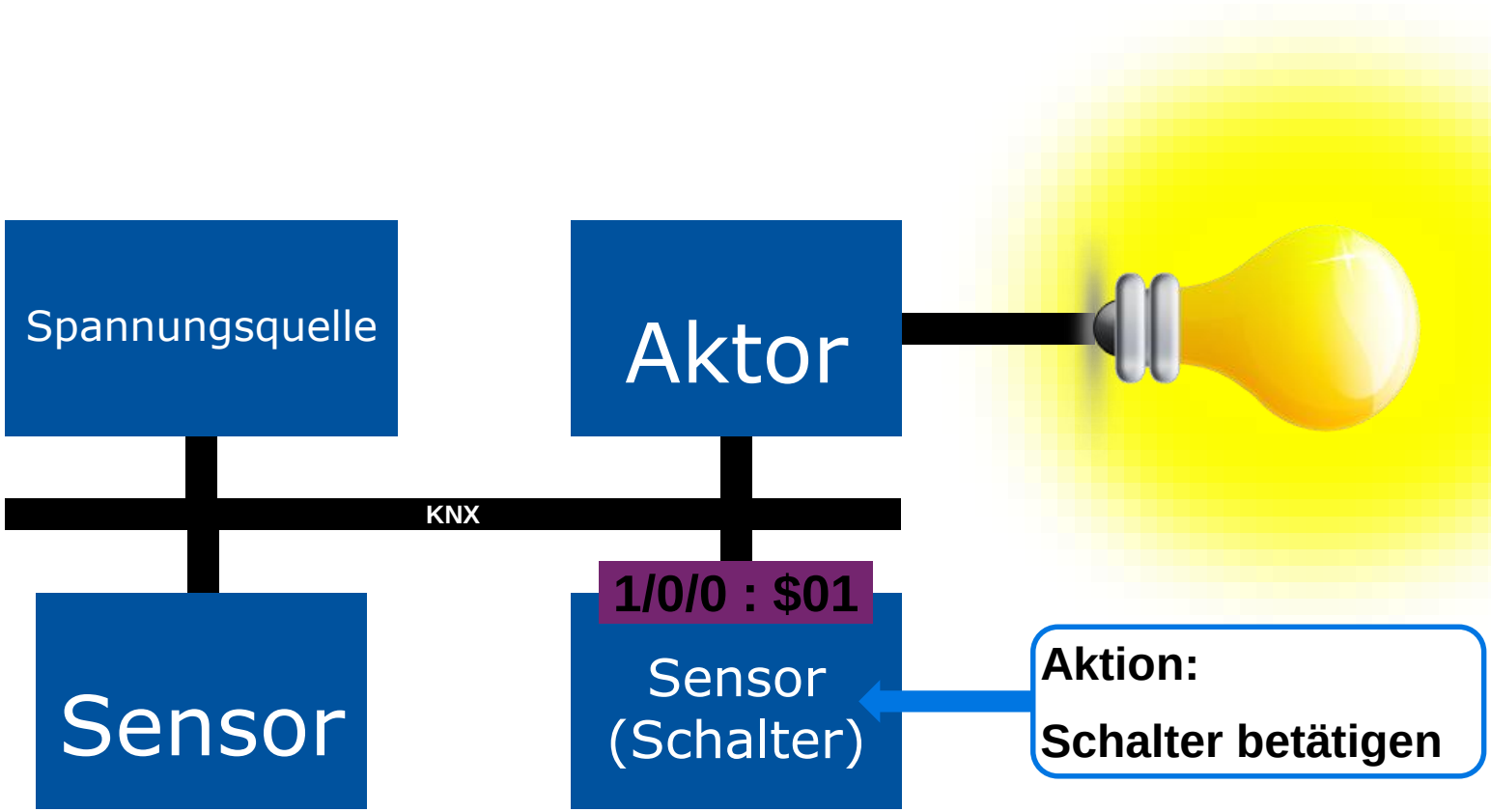


Externe Sicherheit: Updates

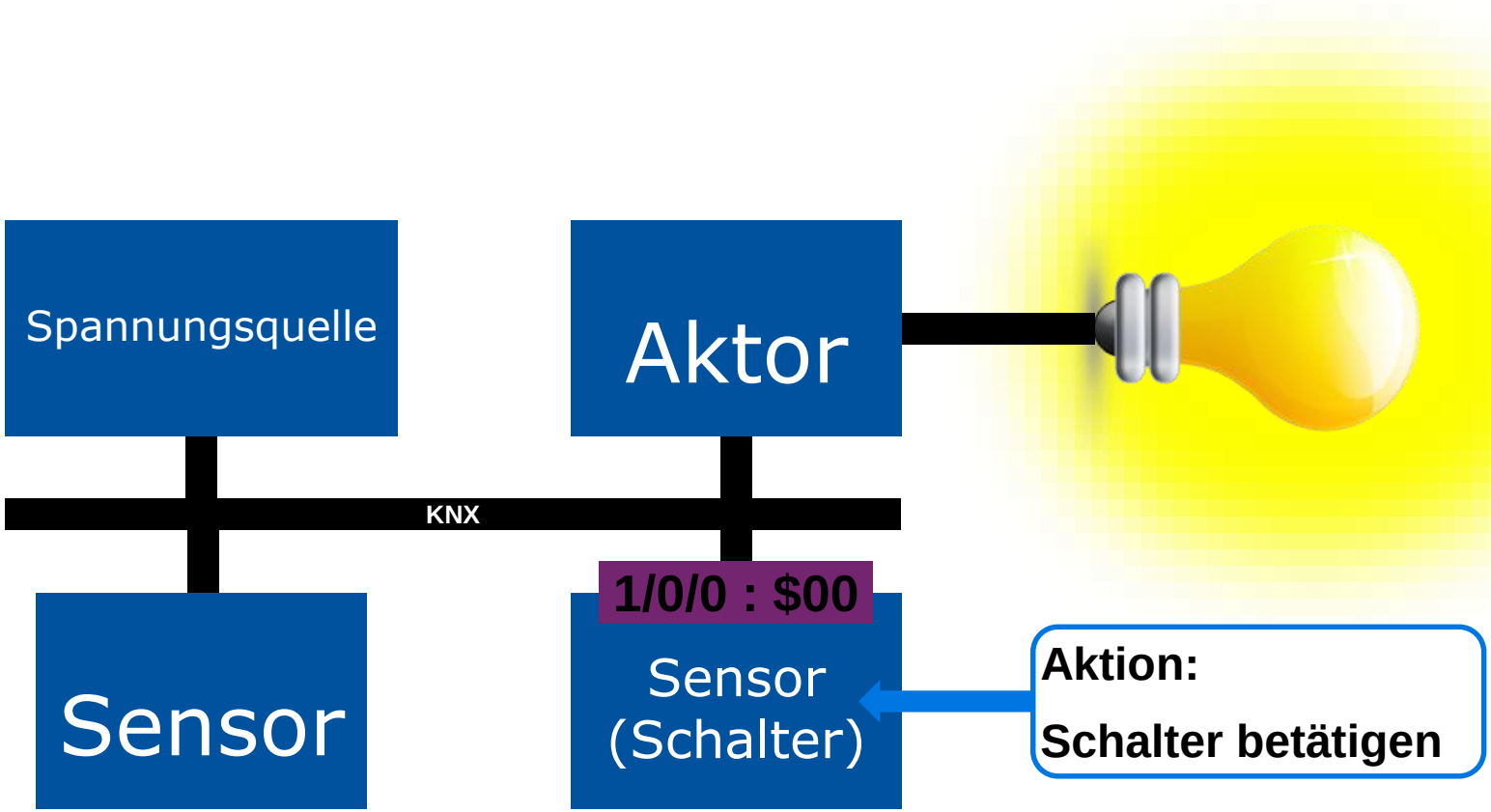
Angriffe in der Praxis: Einspielen von Befehlen



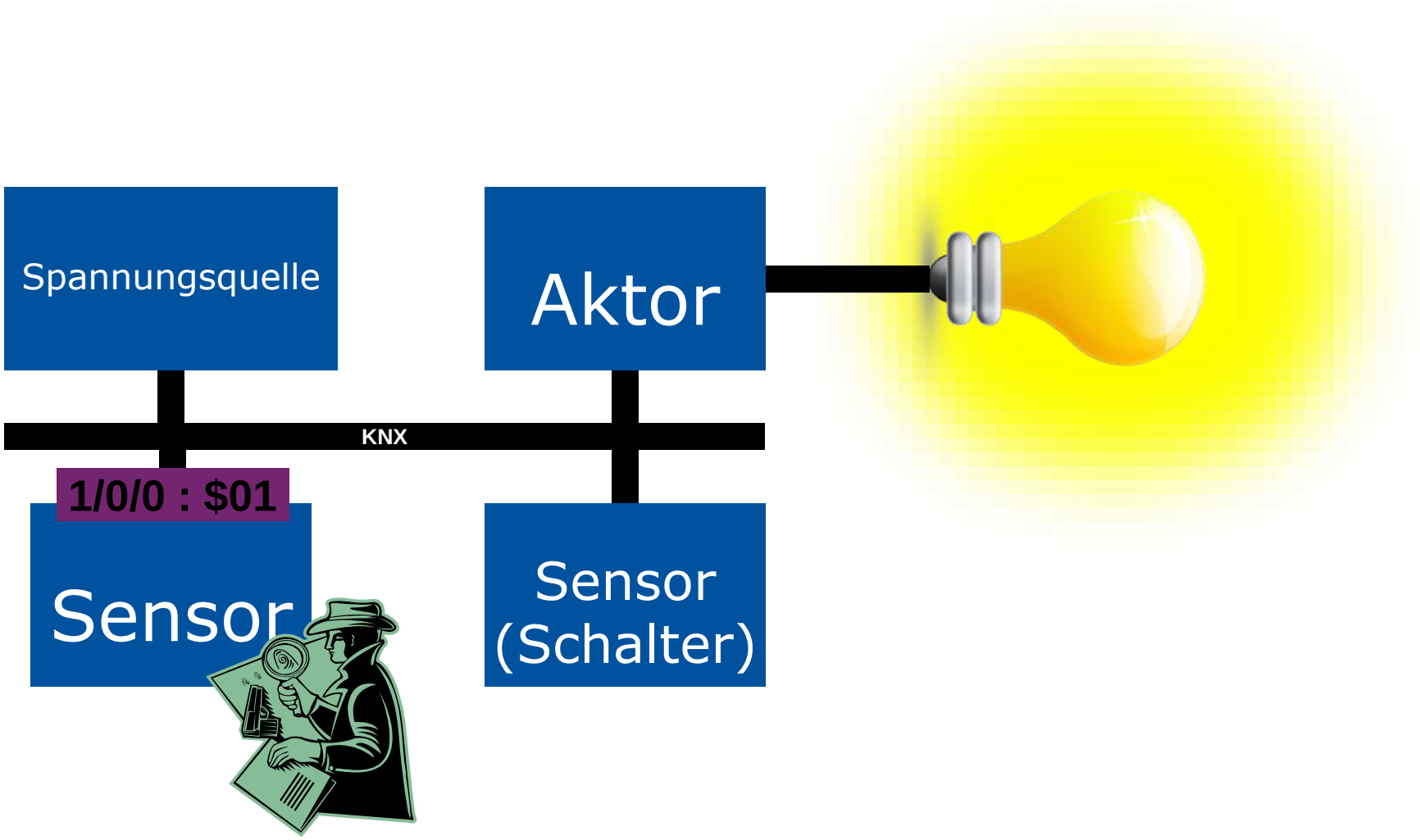
Angriffe in der Praxis: Einspielen von Befehlen



Angriffe in der Praxis: Einspielen von Befehlen



Angriffe in der Praxis: Einspielen von Befehlen



Angriffe in der Praxis: Mitlesen

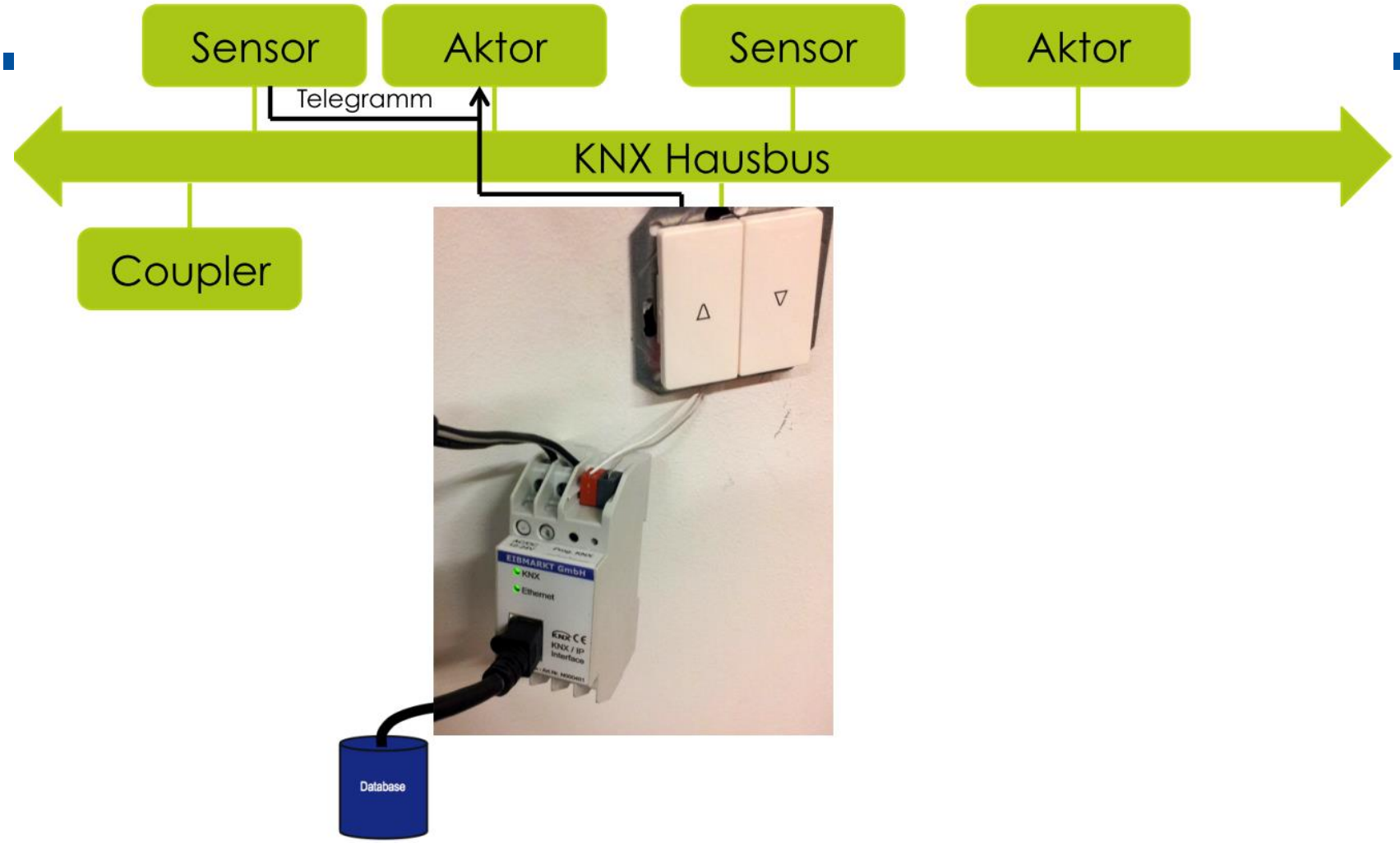
- Mitlesen von Daten
- Erstellen von Bewegungsprofilen
  - Vielen Dank an Dr.-Ing. Thomas Mundt von der Universität Rostock

Angriffe in der Praxis: Mitlesen

Etagengrundriss des Zielgebäudes

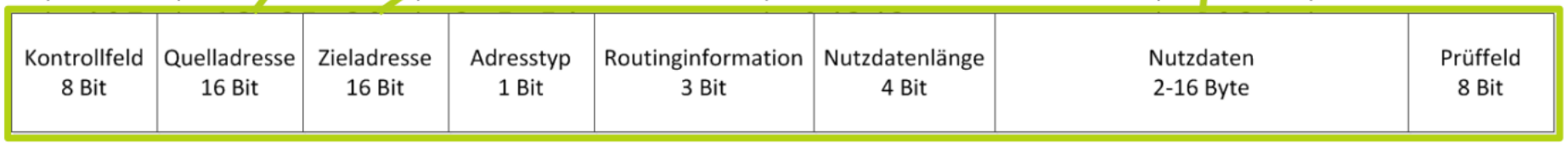
Untersuchung eines KNX-Netzwerkes in einem Bürogebäude

- Kann man erkennen, ob sich innerhalb des Gebäudes Menschen befinden?
- Kann man erkennen, wo diese Leute sich befinden?
- Kann man erkennen, wie viele Leute am Tag bestimmte Räume nutzen?
- Lässt sich feststellen, was in den Räumen vor sich geht (z.B. Vorträge o.ä.)?
- Wie viele Leute befinden sich im Gebäude?
- Welche Personen laufen gerade durch den Flur?
- Und letztlich: **Wer wäscht sich nach dem Toilettengang die Hände und wer nicht?**



„Anzapfen" des KNX-Datenverkehrs

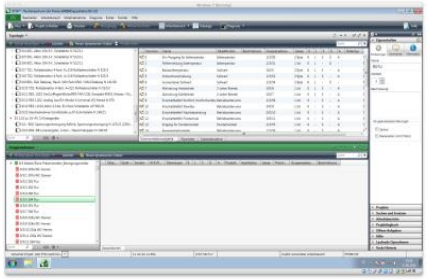
```
mysql> select * from knxlog limit 10;
+-----+----------+---------------+------------------+------+
| id  | Time     | SourceAddress | DestinationAddr  | Data |
+-----+----------+---------------+------------------+------+
| 155 | 13:31:21 | 3.6.4         | 1/1/60           | 0080 |
| 196 | 13:31:58 | 3.6.7         | 1/1/64           | 0080 |
| 264 | 13:33:24 | 3.6.12        | 1/1/73           | 0080 |
| 265 | 13:33:24 | 3.6.12        | 1/1/74           | 0080 |
| 392 | 13:35:19 | 3.5.57        | 0/3/4            | 0081 |
| 393 | 13:35:19 | 3.6.12        | 1/1/73           | 0081 |
| 394 | 13:35:19 | 3.6.12        | 1/1/74           | 0081 |
| 402 | 13:35:25 | 3.5.58        | 0/3/4            | 0081 |
```



Abgehörte Telegramme

Angriffe in der Praxis: Mitlesen

- ***Physikalische Adressen werden benötigt, um Telegramme einem Gerät zuordnen zu können.***
- Adressen-Sammeln durch Ausprobieren oder Zugucken.
- Adressen aus der Konfigurationssoftware (ETS) entnehmen.
- Adressen bei Wartungsarbeiten notieren.



Angriffe in der Praxis: Mitlesen

Etagenplan mit eingezeichneten Gerätepositionen

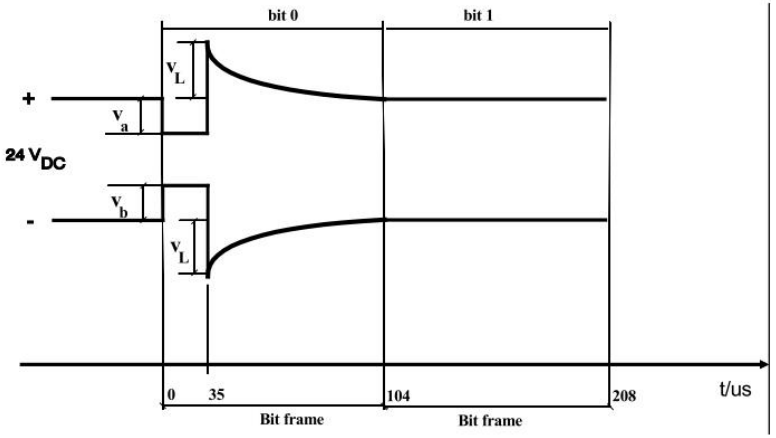
Angriffe in der Praxis: Mitlesen

Scores durch Zuordnung der Waschraum-Verweildauer zu Zielen oder Ursprung der Sensorevents.

Angriffe in der Praxis: Mitlesen

- ***Maßnahmen zur Verbesserung des Datenschutzes***
- Verbot durch Verwaltung, Lichtschalter auszubauen
- Rekonfiguration der Linienkoppler, damit nicht alle Telegramme des 3. OG mitgelesen werden konnten

Neues Abhörgerät



Angriffe in der Praxis: Mitlesen

+

+

=

Angriffe in der Praxis: Shodan

- Suchmaschine
- „Wie google nur anders“
  - Speichern der Antworten von IP-Adressen
- Ermöglicht das Auffinden von Geräten die „öffentlich zugänglich sind“

Beispiel International

128.171 [redacted]
University of Hawaii
Added on 12.07.2014
Honolulu
Details

Instance ID: 60000
Object Name: BIO-BOILER-VND
Vendor ID: /
Firmware: 1.13.29
Location: Biomed Basement
Application Software: 1.13.29
Model Name: 460 EDX
Description: Biomed Boiler System **BACnet** IP

Part # 460MXT-Ascon

Modbus TCP Client / BACnet/IP Server

Revision 1.13.29

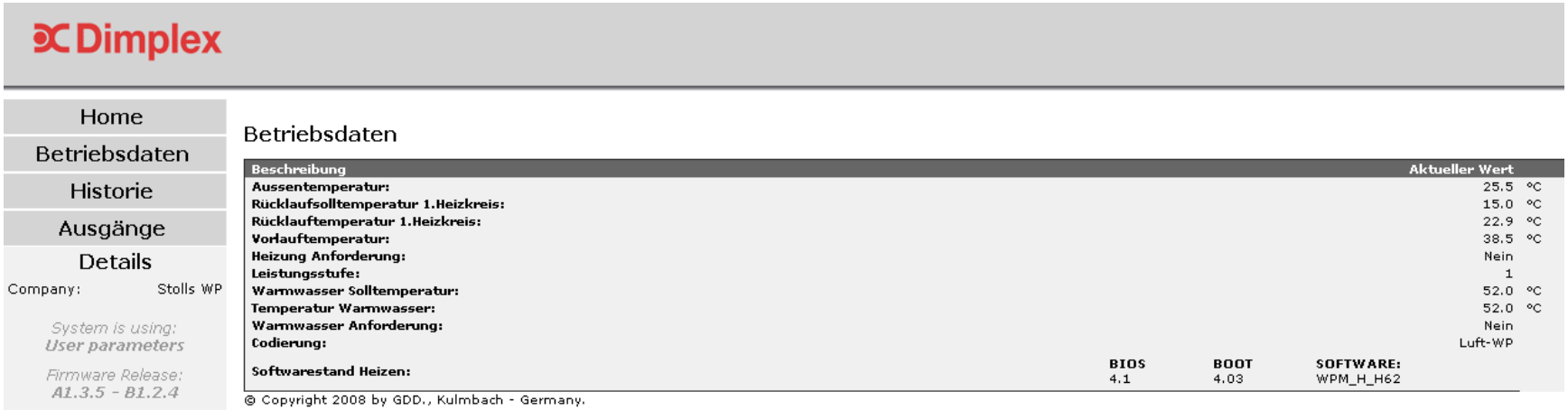
Status and Summary

Utilities

Description	Enter an application description.	Edit
460MXT-Ascon Network Settings	IP address: 128.171 [redacted] Subnet mask: 255.255.255.0 Default gateway: 128.171.246.1 MAC address: 00-03-F4-06-18-FF	Edit
Selected Communication Modules	**Modbus TCP Client** TCP Connect Timeout: 5 Response Timeout: 1000 Delay Between Polls: 10 **BACnet/IP Server** Device Instance: 60000 Device Name: BIO-BOILER-VND Description: Biomed Boiler System BACnet IP Location: Biomed Basement Number of Objects to Expose: AI: 20, AO: 20, BI: 20, BO: 20	Edit
Server Module Configuration	**BACnet/IP Server** No configurable parameters	Edit
Client Module Configuration	**Modbus TCP Client** 1 device configured	Edit
460MXT-Ascon Application Parameters	460MCBS Mapping — Click the Edit button to see the information	Edit

Compatible with Internet Explorer Only

Beispiel Deutschland



Beispiel Nachrichten

heise Security

News Hintergrund Erste Hilfe

Security > News > 7-Tage-News > 2013 > KW 16 > Vaillant-Heizungen mit Sicherheits-Leck

15.04.2013 13:00 « Vorige | Nächste »

Vaillant-Heizungen mit Sicherheits-Leck

vorlesen / MP3-Download

Die Vaillant-Heizungsanlagen des Typs ecoPower 1.0 enthalten ein hochkritisches Sicherheitsloch, durch das ein Angreifer die Anlage über das Internet ausschalten und potenziell beschädigen kann. In einem Informationsschreiben rät der Hersteller seinen Kunden daher zu einem drastischen Schritt: Sie sollen den Netzwerkstecker ziehen und auf den Besuch eines Servicetechnikers warten.

http://www.heise.de/security/meldung/Vaillant-Heizungen-mit-Sicherheits-Leck-1840919.html

Beispiel Nachrichten

golem.de IT-NEWS FÜR PROFIS

HOME TICKER VIDEO ABO ✓ Suchen

TOP-THEMEN: Android Apple Google Windows 10 Linux Wearable mehr

INTELLIGENTE STROMZÄHLER

Gehackte Smart Meter machen Lichter aus

Black Hat Europe 2014

Sicherheitsexperten ist es gelungen, in Spanien eingesetzte intelligente Stromzähler zu hacken. Damit könnten sie den Strom abschalten, den Zähler manipulieren oder dort Malware installieren.

Die Sicherheitsforscher Alberto Garcia Illera und Javier Vazquez Vidal haben sich Zugriff auf einen intelligenten Stromzähler verschafft, der in Spanien weit verbreitet ist. Dort entdeckten sie schwere Sicherheitslücken, über die nicht nur der eine Smart Meter manipuliert werden könnte, sondern auch weitere des gleichen Herstellers. Die beiden Sicherheitsexperten präsentierten ihre Ergebnisse auf der Sicherheitskonferenz Black Hat Europe 2014.

Spanischen Sicherheitsexperten ist es gelungen, intelligente Stromzähler zu manipulieren. (Bild: CC BY-SA 3.0)

Datum:	17.10.2014, 16:28
Autor:	Jörg Thoma
Themen:	Security, Black Hat, Black Hat Europe 2014, Malware, Smart Grid, Technologie, Applikationen,

Quelle: http://www.golem.de/news/intelligente-stromzaehler-gehackte-smart-meter-machen-lichter-aus-1410-109923.html

Maßnahmen

- Zugriffe absichern
  - VPN
  - https (SSL/TLS)
- Physikalischen Zugang absichern
  - Verschlüsselte Technologien einsetzen
- Heimnetzwerk sichern
  - Firewall & Anti-Malware
  - Verschlüsselung
  - Updates

TeleTrusT
Pioneers in IT security.

TeleTrusT-Informationstag

"IT-Sicherheit im Smart Home und der Gebäudeautomation"

Berlin, 12.11.2014

Vielen Dank für Ihre Aufmerksamkeit!

Fragen?