HAFEN DER WISSENSCHAFTEN 1218 ROSTOCK 1419

Lehrstuhl für Informations- und Kommunikationsdienste

„Black Out“ durch unsere GA

Schwachstellenanalyse am Beispiel bestehender Gebäude

GLT-Anwendertagung
25. bis 27. September 2019

Johannes Goltz
Universität Rostock

Aufbau von KNX-Systemen

Abbildung 1: Sensor [2]

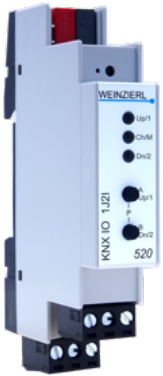
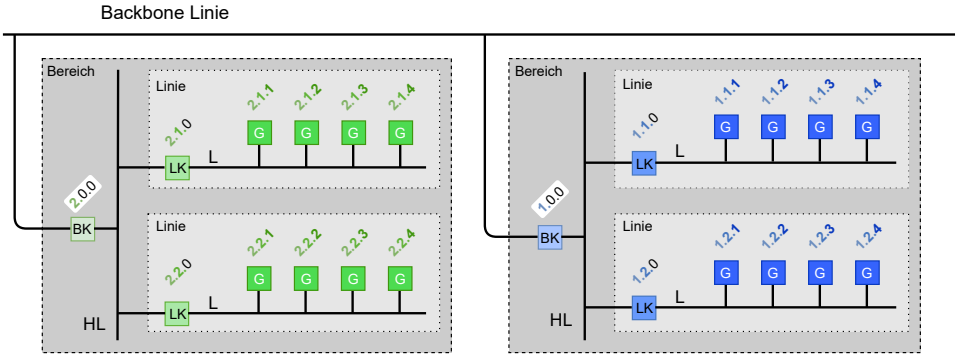


Abbildung 2: Aktor [1]

Abbildung 3: Systemgerät [4]

Aufbau von KNX-Systemen



BK - Bereichskoppler	HL - Hauptlinie	G - Gerät	L - Linie	LK - Linienkoppler

Abbildung 4: Logische Strukturierung des Netzwerkes

Aufbau von KNX-Systemen

- Verbindung von Netzsegmenten durch Koppler
- Jede Linie: Broadcastdomäne
- Kommunikation über Multicasting
- Datenrate bei Twisted Pair: 9,6 kBit/s
- Keine Verschlüsselung
- Keine Authentisierung
- Integrität durch Prüfsummen sichergestellt

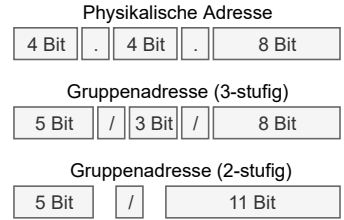


Abbildung 5: Addressierung von KNX-Geräten

Kommunikation bei KNX

Byte	Length	Data
Byte 0	1 Byte	Control Field (see right)
Byte 1+2	2 Bytes	Source Address
Byte 3+4	2 Bytes	Destination Address
Byte 5	1 Bit	Destiantion Address Flag
	3 Bit	Hop Count
	4 Bit	Payload Length
Byte 6-21	2-16 Bytes	Payload
Byte 22	1 Byte	Parity Field (even parity)

Tabelle 1: KNX Standardtelegramm

Bit	Data
Bit 0	Frame Type (1-standard, 0-extended)
Bit 1	Fixed ("0")
Bit 2	Repeat Flag (0-repeated)
Bit 3	Fixed ("1")
Bit 4+5	Priority
Bit 6+7	Fixed ("0")

Tabelle 2: Steuerfeld des KNX-Standardtelegramms

Kommunikation bei KNX

Schnittstellen (Auswahl):

- IP / KNX - UDP: 3671 + Multicast-Adresse + Unicast-Adresse / KNX-Adresse
- USB / KNX
- Seriell / KNX
- KNX RF / KNX TP, USB

Mit Netzen verbinden

Tools & SDKs

- KNXmap (Python)
- knxd (C/C++)
- Calimero (Java)
- kDriveExpress (C/C++/.NET/Python)
- Net'n Node Busmonitor

Abbildung 6: KNX IP Interface 731 [3]

Abbildung 7: KNX USB Interface 332 [5]

Gateways

- KNX IP Interface 731 (Spannungsversorgung über Bus)
- EIB, KNX IP Schnittstelle (Spannungsversorgung über PoE / Netzteil 12-24V DC)
- KNX USB Interface Stick 332

Mit Netzen verbinden

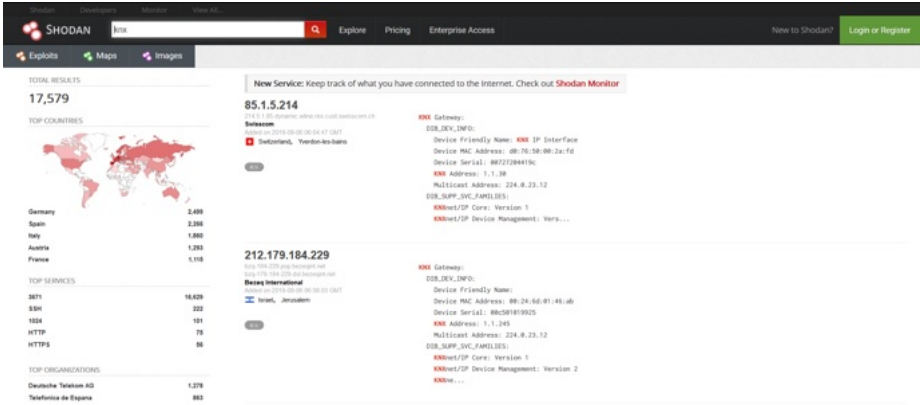


Abbildung 8: Suche nach offen verfügbaren KNX-Gateways

Netzübergange und Gateways

Abbildung 9: LON-IP-Gateway

Abbildung 10: Serielles Gateway

Abbildung 11: USB-Gateway

Abbildung 12: LON-Gateway

Angriffe und Schäden

- Mechanische Überlastung
- Elektrische Überlastung
- Alterung von Bauteilen
- Manipulation von Zugangskontrollsystemen
- Manipulation durch Temperatur
- Reputationsschaden durch Beleuchtung
- Freisetzung gefährlicher Substanzen

Sicherheit vs. Wartbarkeit

Abbildung 13: Schaltschrank

Sicherheit vs. Wartbarkeit

Abbildung 13: Schaltschrank

Abbildung 14: Für jeden zu öffnen

Sicherheit vs. Wartbarkeit

Abbildung 15: Geöffneter Schaltschrank

Sicherheit vs. Wartbarkeit

Abbildung 15: Geöffneter Schaltschrank

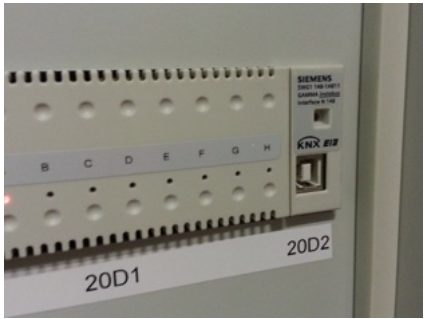


Abbildung 16: Interface direkt verfügbar

Sicherheit vs. Wartbarkeit

Abbildung 17: Abzug in Chemie/Biologie

Sicherheit vs. Wartbarkeit

Abbildung 17: Abzug in Chemie/Biologie

Abbildung 18: Interface direkt verfügbar

Sicherheit vs. Wartbarkeit

Abbildung 19: Zugang zu Feldebene via Gateway

Sicherheit vs. Wartbarkeit

Abbildung 19: Zugang zu Feldebene via Gateway

Abbildung 20: Auch ohne physischen Zugang möglich

Sicherheit vs. Wartbarkeit

Abbildung 21: KNX-Bewegungsmelder

Sicherheit vs. Wartbarkeit

Abbildung 21: KNX-Bewegungsmelder

Abbildung 22: Konfigurationsdaten einfach zugänglich auf dem Gerät

Sicherheit vs. Wartbarkeit

Abbildung 23: Öffentliche IP-Adressen

Sicherheit vs. Wartbarkeit

Abbildung 24: Zugang via VPN

Sicherheit vs. Wartbarkeit

Abbildung 25: Türschild

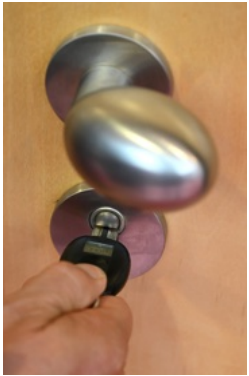


Abbildung 26: Mechatronisches Schloss

Sicherheit vs. Wartbarkeit

Abbildung 27: Blick in die Technikzentrale

Abbildung 28: Informationsschwerpunkt am DDC

Sicherheit vs. Wartbarkeit

Abbildung 29: Kältepumpe

Abbildung 30: Internet nicht mehr verfügbar

Abbildung 31: Telefon nicht mehr verfügbar

Sicherheit vs. Wartbarkeit

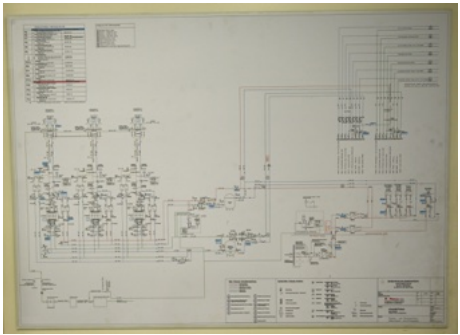


Abbildung 32: Pläne zur installierten Technik

Abbildung 33: Diverse Not-Aus-Schalter

Sicherheit der Protokolle

- Feldebene:
  - Häufigste Vertreter: LON + KNX
  - Verschlüsselung und Authentisierung nicht vorgesehen / nur in aktuellsten Varianten (KNX-Secure)
  - Sehr lange Lebensdauer der Geräte üblich (30+ Jahre), Umstieg/Aktualisierung würde Austausch aller Geräte erfordern.
- IP-Seite:
  - Schutzmaßnahmen vorhanden, aber selten genutzt
  - Ungesicherte Protokolle eher Regel als Ausnahme

Zugriffsmöglichkeiten

- Angreifer kann durch Einsatz eines Gateways von jedem Punkt im Gebäude jeden anderen Punkt erreichen.
- Gateway mit Rasperry Pi und GSM-Modul kann genutzt werden, um Angriffe auch aus der Entfernung auszulösen.
- Bei Untersuchungen wurden in der Regel höchstens Nutzername und Passwort als Zugangssperre gefunden, wenn überhaupt.
- Auf IP-Seite dient das Abschotten der Netze per VLAN und das Verschließen der Räume als Schutzmaßnahme. Durch die Vielzahl an wichtigen Räumen und Berechtigten und die Vielzahl der Netzzugänge + der zahlreichen Möglichkeiten für Fehlkonfigurationen ist dies eine fragliche Praxis.

Mögliche Auswirkungen

- Sehr hohes Risiko für beträchtliche Schäden.
- Angriffe mit dem Ziel von Chaos und Aufmerksamkeit sind einfach durchführbar.
- Ansteuerung beliebiger Aktoren auf der Feldebene möglich.
- Aufzeichnung von Sensordaten ist sehr einfach möglich. Auswertungen dieser erlauben auch komplexe Rückschlüsse.

Welche Auswertungen sind möglich?

1. Wie viele Mitarbeiter sind im Gebäude? ✓
2. Wann ist der letzte Mitarbeiter gegangen? ✓
3. Wann, wie oft und wie lange Max M. arbeitet, Pausen macht, ...? ✓
4. Beziehung zwischen verschiedenen Mitarbeitern? ✓
5. Ob ein Mitarbeiter die öffentlichen Verkehrsmittel nutzt? ✓

Strategien für mehr Sicherheit

Zonenbildung mit Fokus auf Erhöhung der Sicherheit

- Quantifizierung des Risikos
- Einstufung von Geräten, Zugänglichkeit von Geräten/Leitungen und Erreichbarkeiten in Klassen
- Daraus resultierende Abschätzung der Risiken
- Menge und Art der Pakete zur dynamischen Beobachtung
- Möglichkeit zur Unterstützung schon bei der Erstellung solcher Systeme

Weiterführend dazu: Sicherheitsanalyse von Gebäudeautomationsnetzen auf Feldbusebene am Beispiel von KNX

Intrusion Detection System mit Netflows

- Umsetzung eines Intrusion Detection Systems in KNX
- Netflows zur Verdichtung der Daten
- Übertragung In-Band
- Auswertung mittels verschiedener Machine-Learning-Ansätze

Weiterführend dazu: Analysis of Distributed In-Band Monitoring Messages for Field Bus Networks in Building Automation Systems

Deep Packet Inspection

- Umsetzung eines Whitelisting-Konzepts
- Extraktion von Filterregel aus der Datenbank der ETS
- Konzeption von neuen Kopplern mit zusätzlichen Filterregeln
- Verbesserte Abschottung der Netzsegmente

Weiterführend dazu: Deep packet inspection in field busses

Ist der Blackout unausweichlich - Nein, aber...

- Wer Netzwerk schützen möchte, muss seine Struktur, seine Geräte und seine Schnittstellen kennen.
- Lösungen für Sicherheitsprozesse liegen auf der Hand.
- Erfahrungen sind vorhanden.
- Bewusstsein muss wachsen.

Fragen

Vielen Dank für die Aufmerksamkeit

Fragen?

Kontakt

Johannes Goltz

E-Mail:
johannes.goltz@uni-rostock.de
Telefon: +49 381 498 7503
Web: Mitarbeiterprofil

Quellen

[1] KNX Aktor - Weinzierl KNX IO 520 Jalousieaktor. https://weinzierl.de/images/products/520/KNX_IO_520_small.png, 19.08.2019 um 12:55 Uhr.

[2] KNX Bewegungsmelder - Busch-Jaeger Präsenzmelder 220. https://www.voltus.de/out/pictures/generated/product/1/665_665_100/BJ_f_6847agm-204.jpg, 19.08.2019 um 11:19 Uhr.

[3] KNX IP Interface - Weinzierl KNX IP Interface 731. https://weinzierl.de/images/development/download/products/731/KNX_IP_731_final_small.png, 23.08.2019 um 08:37 Uhr.

[4] KNX Netzteil - Weinzierl KNX Power Supply USB 367. https://weinzierl.de/images/products/367/KNX_PS_367_USB_display_ON_small.png, 19.08.2019 um 11:10 Uhr.

[5] KNX UBS Interface - Weinzierl KNX USB Interface 332. https://weinzierl.de/images/332_KNX_USB_Stick1_small.png, 23.08.2019 um 08:52 Uhr.