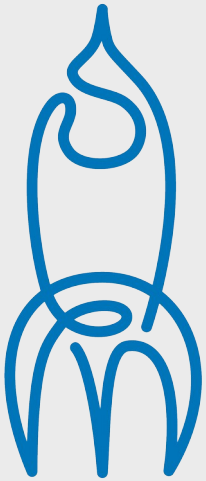
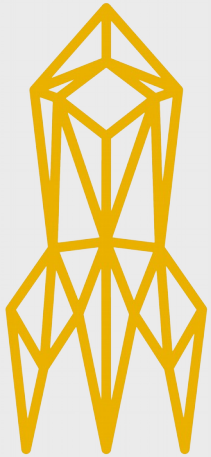
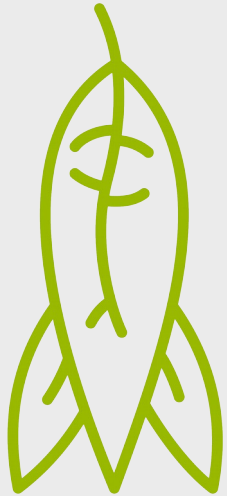
IT-Sicherheit in vernetzten Gebäuden

Was kann man noch retten, wenn langlebigen Strukturen grundlegende Sicherheitskonzepte fehlen?

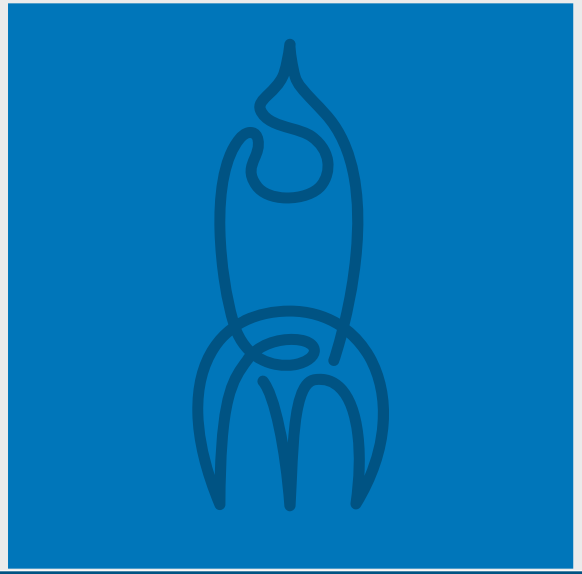
simeon.wiedenmann@uni-rostock.de

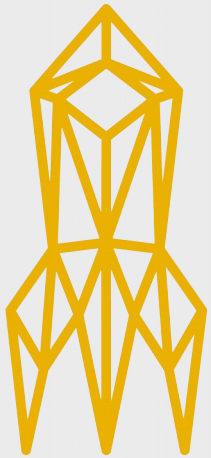


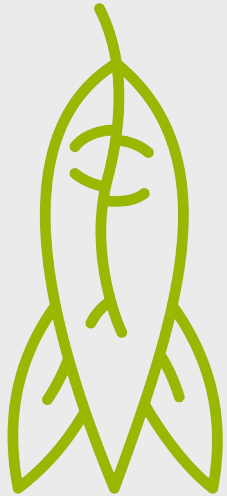




Wie funktionieren vernetzte Gebäude am Beispiel von KNX?	Welche Sicherheitsprobleme bestehen?	Welche Lösungsansätze sind denkbar?







Wie funktionieren vernetzte Gebäude am Beispiel von KNX?

Welche Sicherheitsprobleme bestehen?

Welche Lösungsansätze sind denkbar?

Was macht ein Feldbus

Sensoren

Medium

Aktoren

Mehrere TN – Wer sagt wann was zu wem? → Protokoll

Vor – und Nachteile der Gebäudeautomation

Vorteile

- Komfort
- Flexibilität
- (Lauf)Kosteneinsparung
- geringer Materialaufwand

Nachteile

- hohe Installationskosten
- mangelnde Sicherheit
- weitreichendes Angriffspotential
- Komplexität

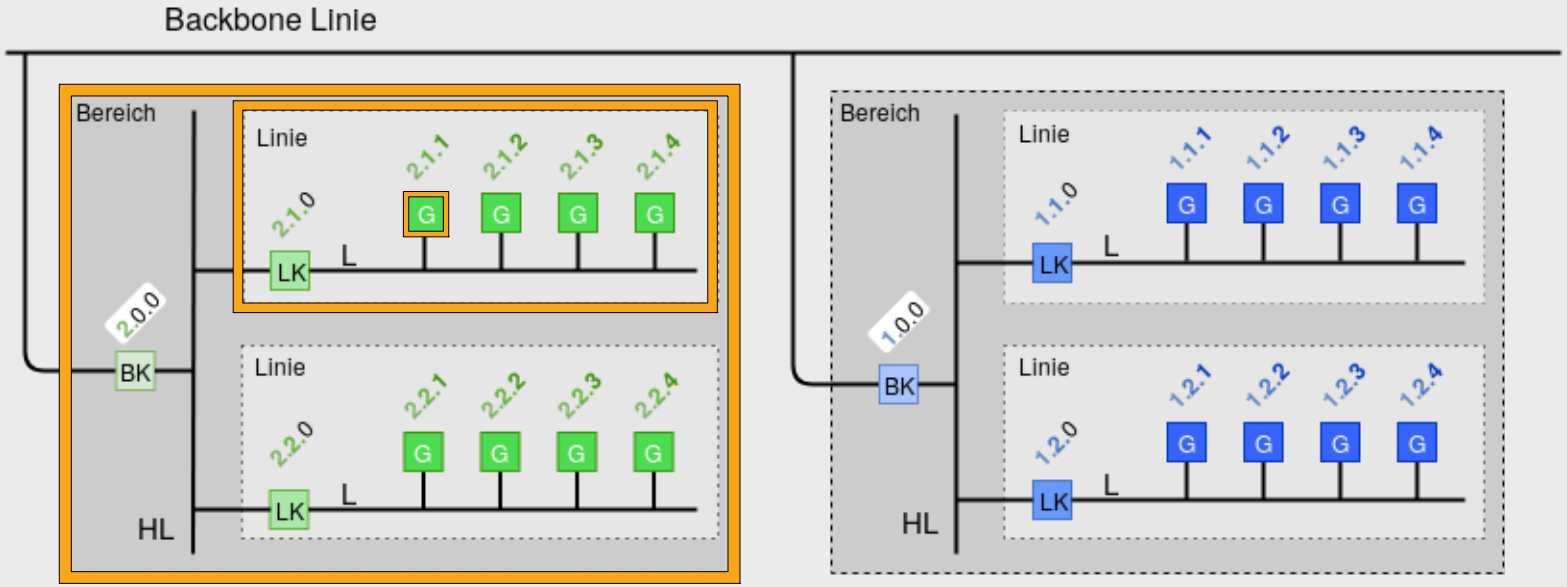
Der KNX Standard

Nachfolger des Europäischen InstallationsBusses (EIB)

- offener Standard
- Spezifikation (2002)
- EN 50090 (2003)
- ISO/IEC 14543-3 (2006)
- herstellerübergreifendes Konsortium
- Zertifizierung durch KNX Association
- Konfiguration – Engineering-Tool-Software (ETS)

Physikalische Adressierung im KNX

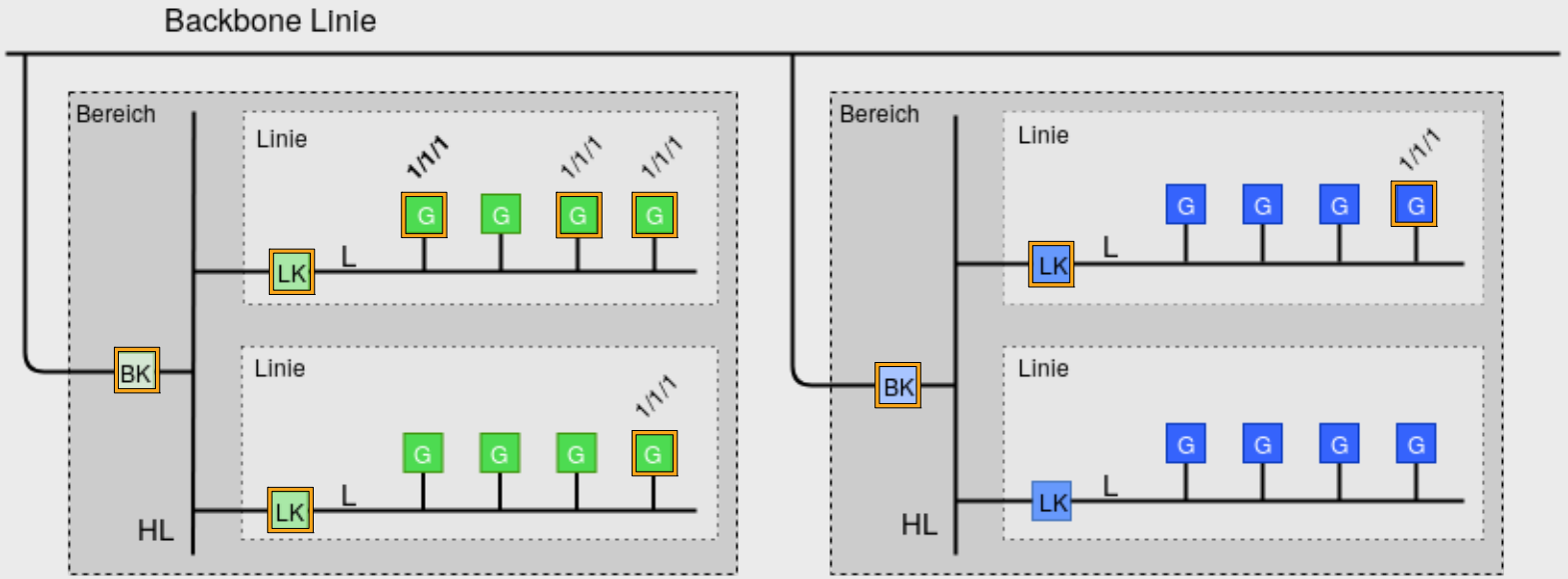
Bereich.Linie.Gerät → 4 bit . 4 bit . 8 bit



Logische Adressierung im KNX

Hauptgruppe / (Nebengruppe /) Untergruppe →

5 bit	/	11 bit		
5 bit	/	3 bit	/	8 bit



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

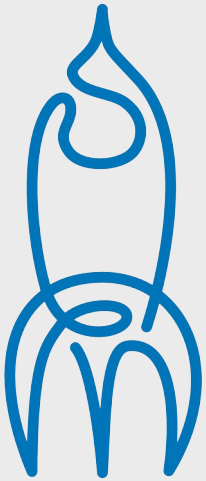
KNX - Telegrammaufbau

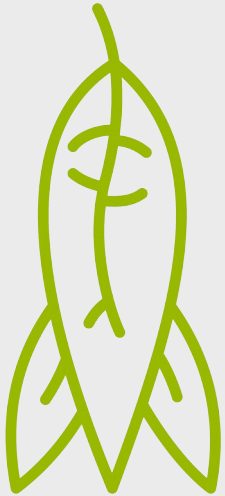
Ctrl (8 bit)	Src (16 bit)	Dest (16 + 1 bit)	RL (7 bit)	Payload (2-16 Byte)	Parity (8 bit)

6	5	4	3	2	1	0
RC2	RC1	RC0	L3	L2	L1	L0

7	6	5	4	3	2	1	0
Type	0	Rep	1	Prio1	Prio0	0	0

KNX für die Gebäudesystemtechnik in Wohn- und Zweckbau, Skollik Helm Seela, ISBN 978-3-8007-4033-8, S.67





Wie funktionieren vernetzte Gebäude am Beispiel von KNX?

Welche Sicherheitsprobleme bestehen?

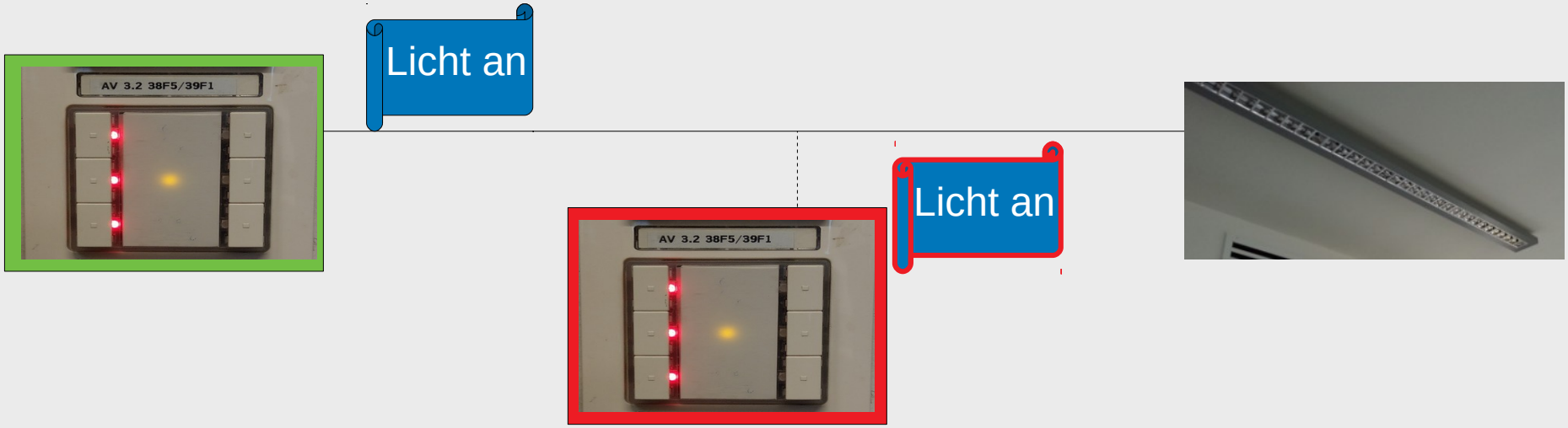
Welche Lösungsansätze sind denkbar?

Schutzziel Vertraulichkeit

„Vertraulichkeit ist die Eigenschaft einer Nachricht, nur für einen beschränkten Empfängerkreis vorgesehen zu sein.“ – Wikipedia

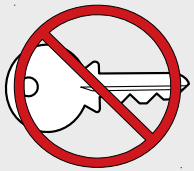
Schutzziel Authentizität

„Die Eigenschaften der Echtheit, Überprüfbarkeit und Vertrauenswürdigkeit.“ – Wikipedia



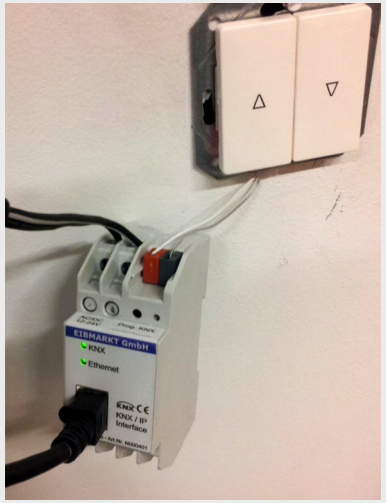
Sicherheitsprobleme bei KNX

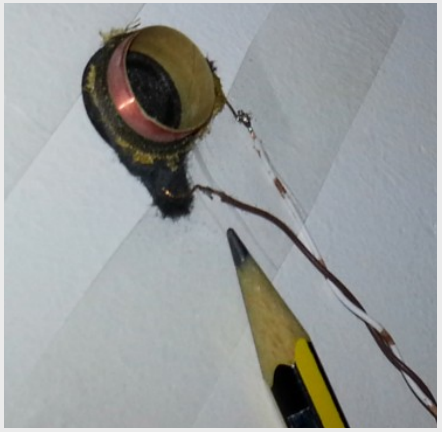
- keine Verschlüsselung (de Facto)
- keine Autorisierung
- Angriffsreichweite & Schadenspotential
- langjährige Laufzeiten der Systeme



SHODAN
Computer Search Engine

Angriffsmöglichkeiten auf KNX

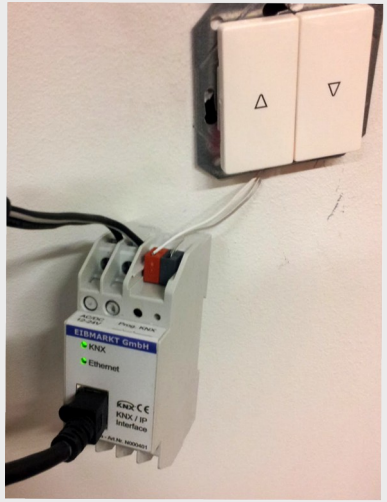




DOS

Licht,
Heizung,
Klimaanlage,
...

Angriffsmöglichkeiten auf KNX

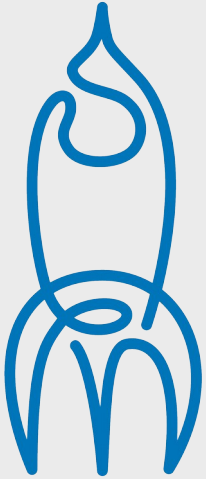


DOS

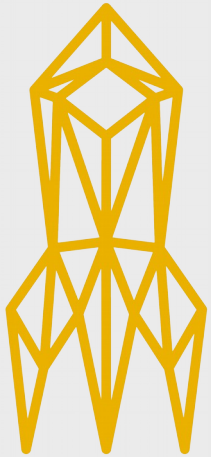
Licht,
Heizung,
Klimaanlage,
...

Persönlichkeitsbezug von KNX-Daten

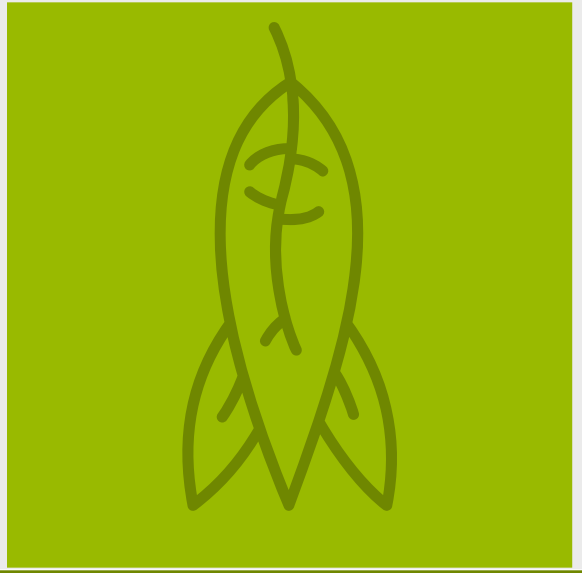
https://opsci.informatik.uni-rostock.de/index.php/Washroom_Behaviour
https://ieeexplore.ieee.org/document/6363068?arnumber=6363068&tag=1



Wie funktionieren vernetzte Gebäude am Beispiel von KNX?



Welche Sicherheitsprobleme bestehen?



Welche Lösungsansätze sind denkbar?

Risikoanalyse

- Klassifikation von Angriffen

Wissen	**Ort des Angreifers**	**Möglicher Schaden**	**Sichtbarkeit des Angriffs**
kein Spezialwissen nötig	entfernt	vernachlässigbar	nicht sichtbar
Grundlagenwissen	Gebäudeumfeld	finanziell	sichtbar (bekannte Adresse)
Spezialwissen erforderlich	innerhalb des Gebäudes	Personenschaden	sichtbar (unbekannte Adresse)

https://ieeexplore.ieee.org/document/8718149

Risikoanalyse

Statische Faktoren

- Geräteklasse
- physikalischer Zugriff Geräte
- physikalischer Zugriff Busmedium
- Reichweite zu anderen Geräten

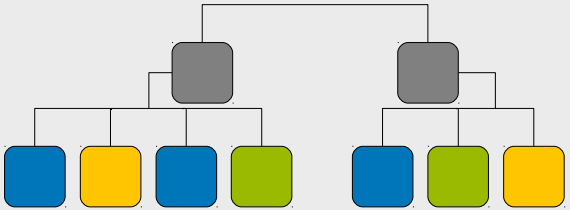
Dynamische Faktoren

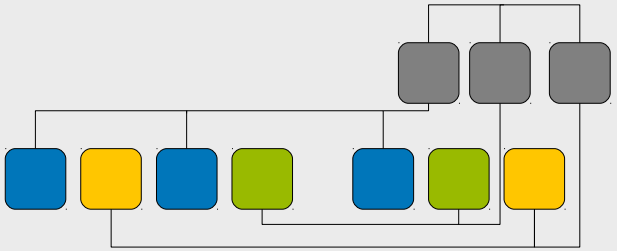
- Telegrammtyp
- # Telegramme / Zeitslot

$$Risiko_{statisch} = \left| \begin{pmatrix} c_{endangerment} \\ c_{accessibility\,(device)} \\ c_{accessibility\,(wire)} \\ c_{reachability} \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{3} \\ \frac{1}{2} \\ \frac{1}{3} \\ \frac{1}{2} \end{pmatrix} \right| \cdot \left(\frac{1}{2}\right)$$

https://ieeexplore.ieee.org/document/8718149

Zonenkonzept



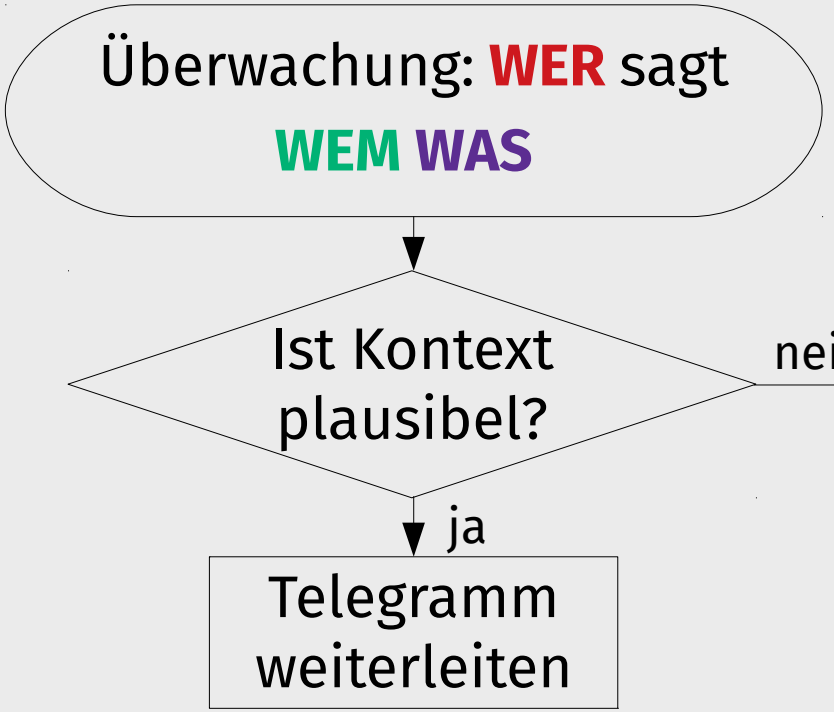


+ weniger Kabel
+ günstig
- hohe Angriffsfläche

- mehr Kabel
+ getrennte Bereiche
+ Sicherheit

http://eprints.iuk.informatik.uni-rostock.de/689/1/Masterarbeit_Goltz.pdf

Filter und Deep Package Inspection



\+ verhindert unplausible Weiterleitung
\- schützt nicht vor Spoofing
\- nur Broadcastübergreifend

http://eprints.iuk.informatik.uni-rostock.de/707/1/deep-packet-inspection-in-fieldbusses-georg-ehrke-ma-2019.pdf

Whitelisting

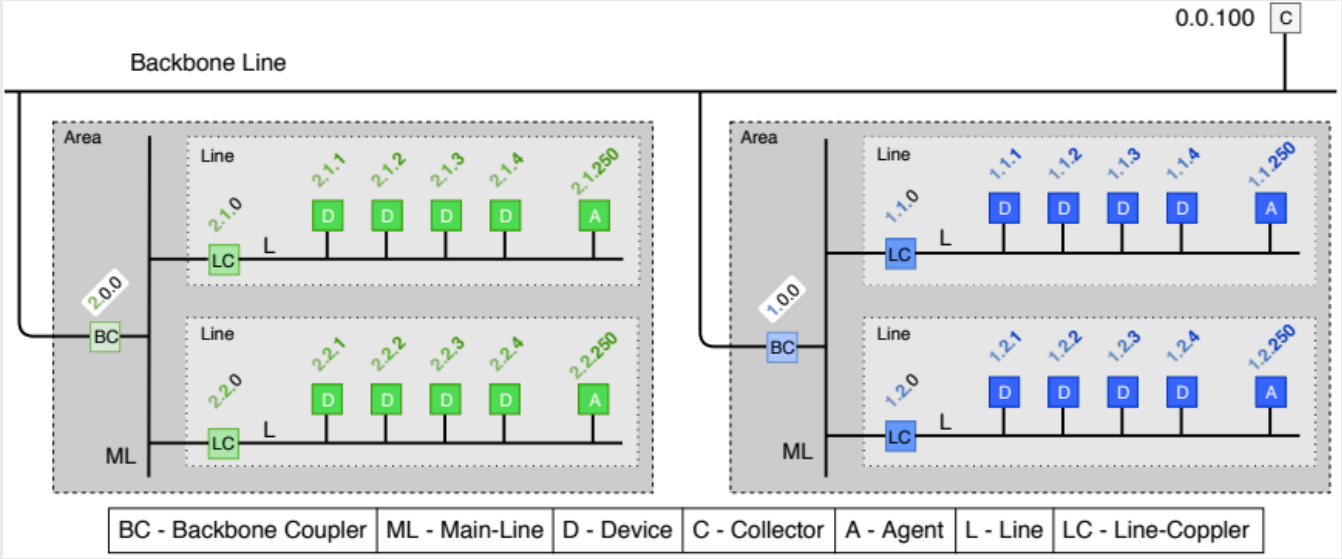
Projektierung [ETS] kennt

- alle autorisierten Kommunikationsteilnehmer
- Empfängerkreise
- Kommunikationsobjekte
- logische Position im Netz

→ entsprechende Filter schlucken alles, was nicht erlaubt ist

http://eprints.iuk.informatik.uni-rostock.de/689/1/Masterarbeit_Goltz.pdf

NetFlow – Analyse des Busverkehrs

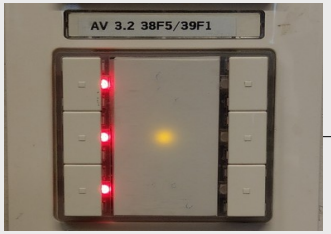


- Agents im Netz verteilen
- Kollektor sammelt Infos
- aggregierte Infos an Warnsystem → Alarm bei Intrusion

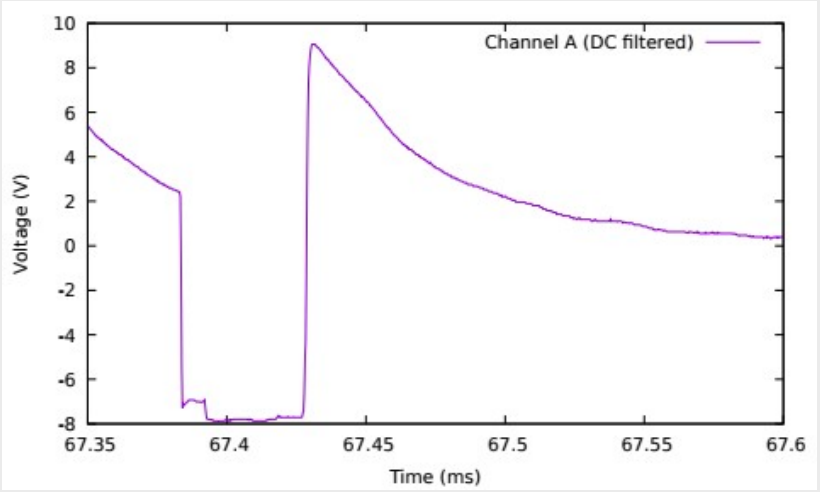
\+ skaliert (kostengünstig) - ggf. Überlastung/ Ziel (Inband)

https://doi.org/10.1007/978-3-030-24907-6_26 ,https://github.com/FreakyBytes/master-thesis
https://github.com/IuK-Uni-Rostock/agent-mirror

Physical-Layer-Beobachtung



2 m / 50 m



+ potentieller Schutz vor ‚Dazuklemmen‘

+ Gerätefingerabdrücke denkbar

- Anfälligkeit für elektromagnetische Störungen

- aufwendige, individuelle Konfiguration pro Installation/ Änderung

Testdaten für Experimente

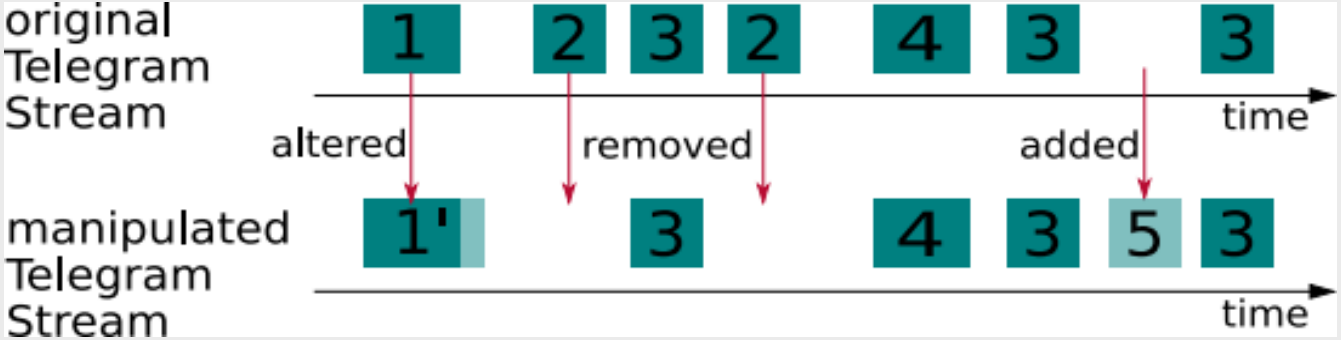
- hochsensible Daten
- Image & Reputation schützen
- kein Risiko eingehen
- reale Daten derzeit nicht verfügbar
- Ansätze bewerten können, Experimentieren benötigt Testdaten

➔ CC BY-SA 4.0 Feldbusverkehr Simulation Log 

https://opsci.informatik.uni-rostock.de/index.php/Fieldbus_traffic_simulation_logs

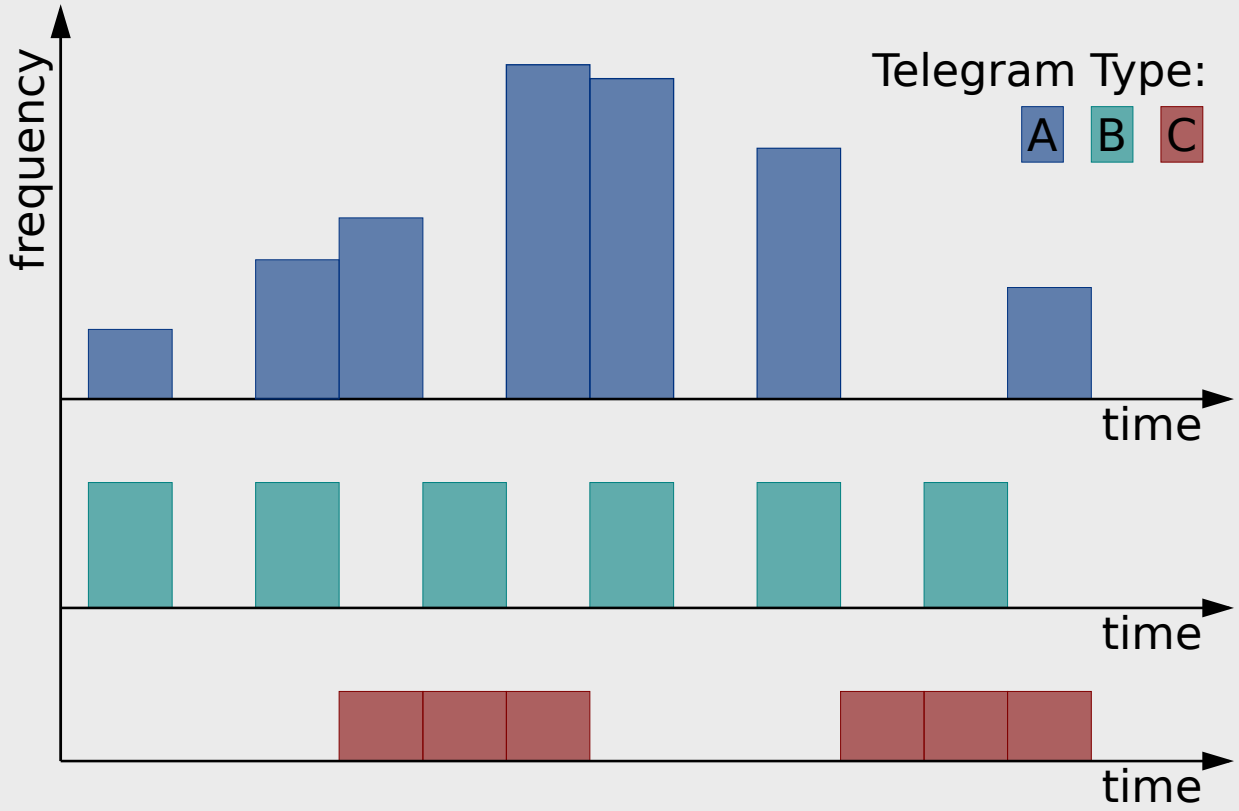
Testdaten für Experimente

- Aufzeichnung realer Daten (angriffsfrei)
- Telegrammtypen beschreiben
- aufgezeichnete Telegrammtypen klassifizieren
- zeitliche Ordnung der Telegramme beschreiben



https://ieeexplore.ieee.org/document/8631474

Zeitliche Verteilung von Telegrammtypen



Angriffe in künstlichen Testdaten

- manipulierte Parameter
- unbekannte Absenderadressen
- zeitlich verschobene Telegramme
  - 1s, 12h, 2d, -1h
- Replay-Angriffe
- Negationsangriffe
- Entfernen von Telegrammen

https://opsci.informatik.uni-rostock.de/index.php/Fieldbus_traffic_simulation_logs

Warum ist es schwierig Sicherheit nachzurüsten?

- Sicherheit vs. Freiheit/ Kosten → komplexe Güterabwägung
- Komplexitätssteigerung → Installations- & Wartungsaufwand
- Keymanagement → ungelöste Problematik
- Adressraum Brootforceable → auch wenn verschlüsselt
- IDS etc. auch missbrauchbar → Personenbezug
- Klassifikation lernt „Normalfall“ → Was ist normal?

Problembewusstsein schaffen

- nicht jeder ist IT-Experte
- öffentliche Ausschreibungen sollten grundlegende IT-Sicherheitsmerkmale einfordern
- Hersteller gesetzlich in Verantwortung integrieren
- Finden sich vergleichbare (problematische) Situationen auch in anderen Gebieten?

  Kraftwerke, Krankenhäuser, Fabriken, Häfen, Boote, Autos, …

Experimente mit KNX

Tools und SDKs:

- KNX Virtual https://my.knx.org/shop/product?product_type=knx-virtual
- https://www.weinzierl.de/index.php/de/alles-knx1/software-tools/net-n-node
- https://github.com/takeshixx/knxmap (Python)
- https://github.com/knxd/knxd (C/C++)
- https://github.com/calimero-project/calimero-core (Java)
- https://www.weinzierl.de/index.php/en/all-knx/software-tools-en/kdriveexpress-en (C/C++/.NET/Python)

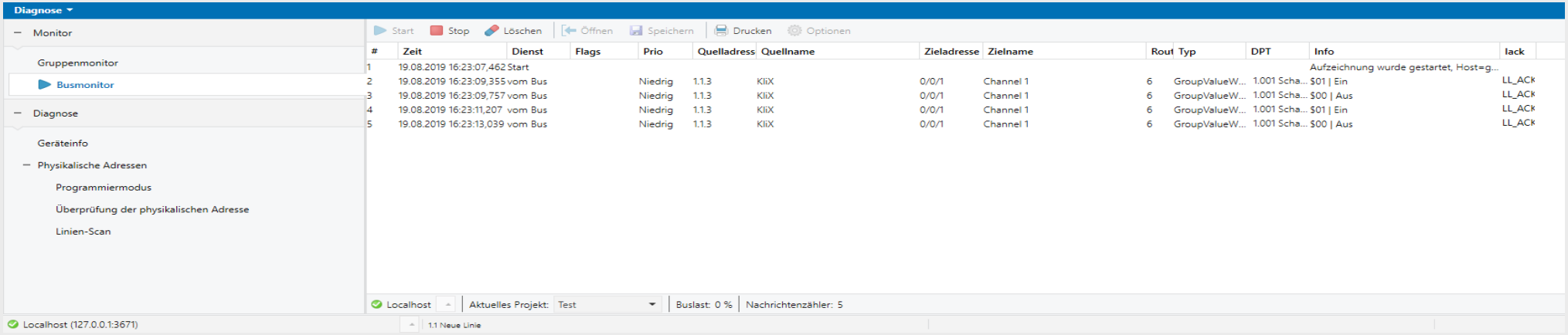
Gateways:

- https://www.weinzierl.de/index.php/en/all-knx/knx-devices-en/knx-usb-interface-332-en (USB Gateway)
- https://www.weinzierl.de/index.php/en/all-knx/knx-module-en/knx-baos-module-838-en (Serielles Gateway für Raspberry Pi)
- https://www.eibmarkt.com/de/products/EIBMARKT-EIB-KNX-IP-Schnittstelle-PoE-mit-bis-zu-5-Tunneling-Verbindungen-N000401.html (IP Gateway)

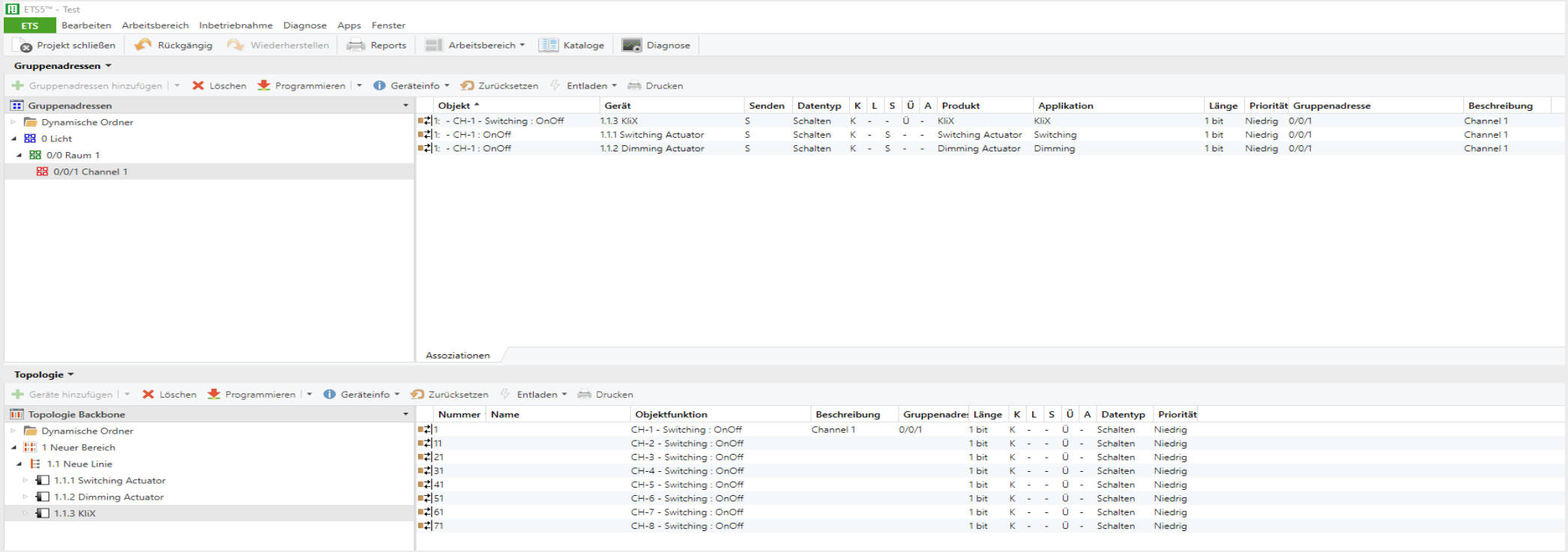
KNX Virtual


KNX Virtual
View
Help
Push Buttons
0
1
0
1
0
1
0
1
0
1
0
1
0
1
0
1
Lamps
ch1
ch2
ch3
ch4
ch5
ch6
ch7
ch8
Dimmable Lamps
ch1
ch2
ch3
ch4
ch5
ch6
ch7
ch8
Blinds
ch1
ch2
ch3
ch4
ch5
ch6
ch7
ch8

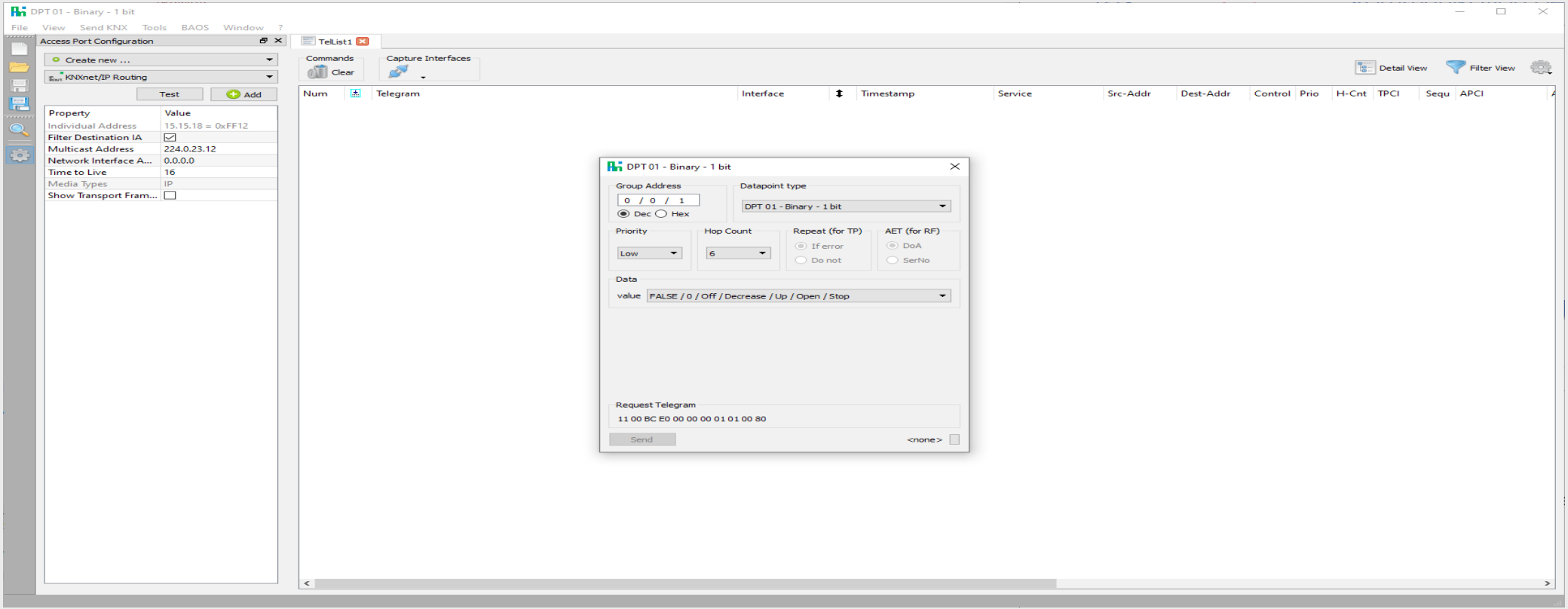
Engineering-Tool-Software (ETS)



Engineering-Tool-Software (ETS)



Net'n Node

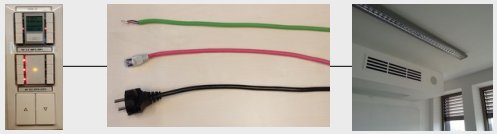

DPT 01 - Binary - 1 bit
File View Send KNX Tools BAOS Window ?
Access Port Configuration
Create new ...
KNXnet/IP Routing
Test
Add
Property
Value
Individual Address
15.15.18 = 0xFF12
Filter Destination IA
Multicast Address
224.0.23.12
Network Interface A...
0.0.0.0
Time to Live
16
Media Types
IP
Show Transport Fram...
TelList1
Commands
Clear
Capture Interfaces
Detail View
Filter View
Num
Telegram
Interface
Timestamp
Service
Src-Addr
Dest-Addr
Control
Prio
H-Cnt
TPCI
Sequ
APCI
DPT 01 - Binary - 1 bit
Group Address
0 / 0 / 1
Dec Hex
Datapoint type
DPT 01 - Binary - 1 bit
Priority
Low
Hop Count
6
Repeat (for TP)
If error
Do not
AET (for RF)
DoA
SerNo
Data
value
FALSE / 0 / Off / Decrease / Up / Open / Stop
Request Telegram
11 00 BC E0 00 00 00 01 01 00 80
Send
<none>

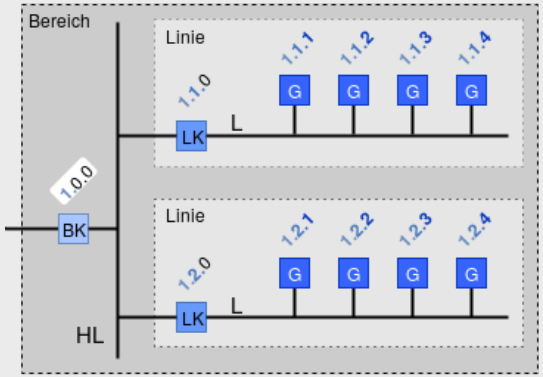
Credits

Thomas Mundt, Johannes Goltz, Johann Bauer, Andreas Zdziarstek, Maximilian Jung, Martin Peters, allen (ehemaligen) Mitarbeitern am Lehrstuhl für Informations- und Kommunikationsdienste der Uni Rostock

Publicdomainvectors.org
Wikipedia

Wie funktionieren vernetzte Gebäude am Beispiel von KNX?

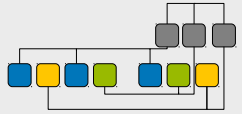


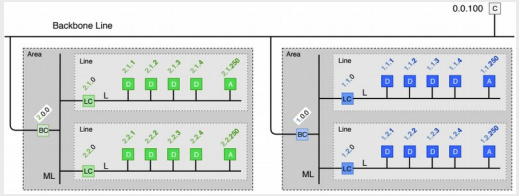


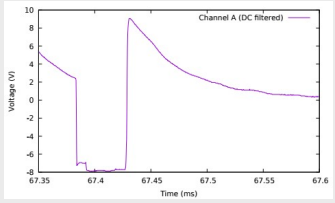
Ctrl	Src	Dest	RL	Payload	Parity

Welche Sicherheitsprobleme bestehen?

Welche Lösungsansätze sind denkbar?







Fragen, Feedback und Tipps sind willkommen → simeon.wiedenmann@uni-rostock.de