Smart home and building solutions.
Global. Secure. Connected.

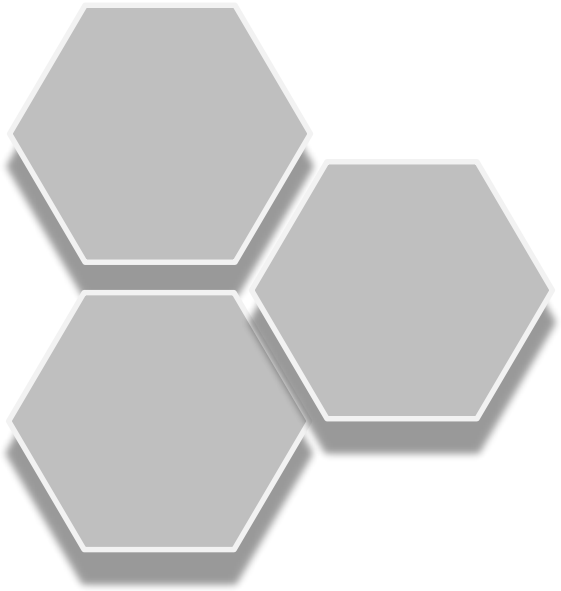
KNX RF - Security Inside

Dr. Thomas Weinzierl
Weinzierl Engineering GmbH
www.weinzierl.de

Join **us**
www.knx.org

Agenda

- About Weinzierl
- KNX System Overview
- KNX RF with ETS
- KNX Data Security
- Implementation



Weinzierl Engineering GmbH

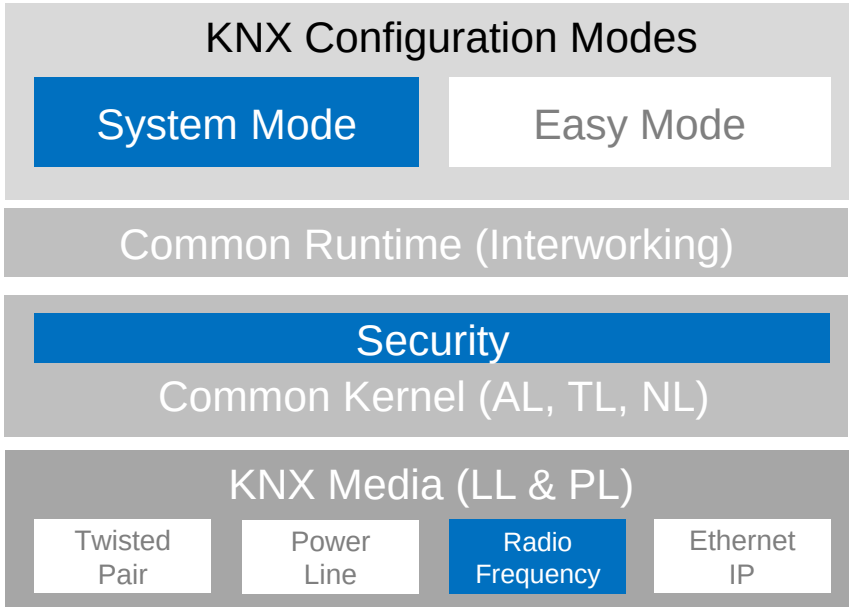
- Founded 2001
- Burgkirchen / Alz
  - South East of Germany
- System solutions for KNX
  - KNX Stacks & Modules
  - KNX Development Tools
- Testing
  - KNX accredited Test Lab
- Production
  - KNX System Devices

KNX RF History

- Since 2002
  - Medium RF specified
  - Mainly for Easy Mode
  - No support in ETS
  - Only a few manufacturers
- Since 2014
  - For System Mode
  - Now in-line with TP, PL, IP
  - Natively integrated in ETS
  - Growing number of products

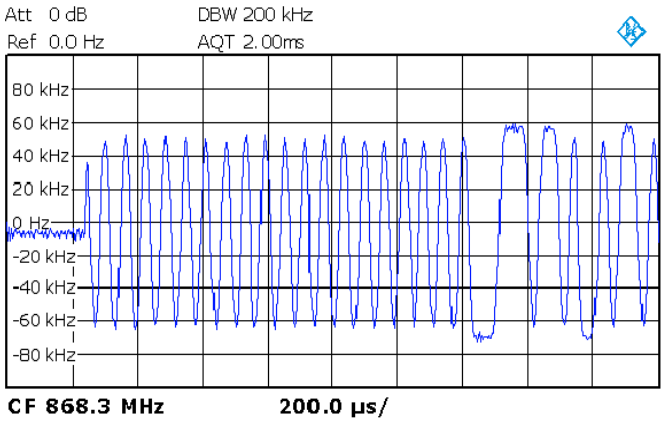
KNX Standard

- Different configuration modes
  - **System Mode (ETS®)**
  - Easy Mode
- One common kernel
  - New: **KNX Security**
- Different media
  - Twisted Pair
  - Power Line
  - **Radio Frequency**
  - Ethernet / IP

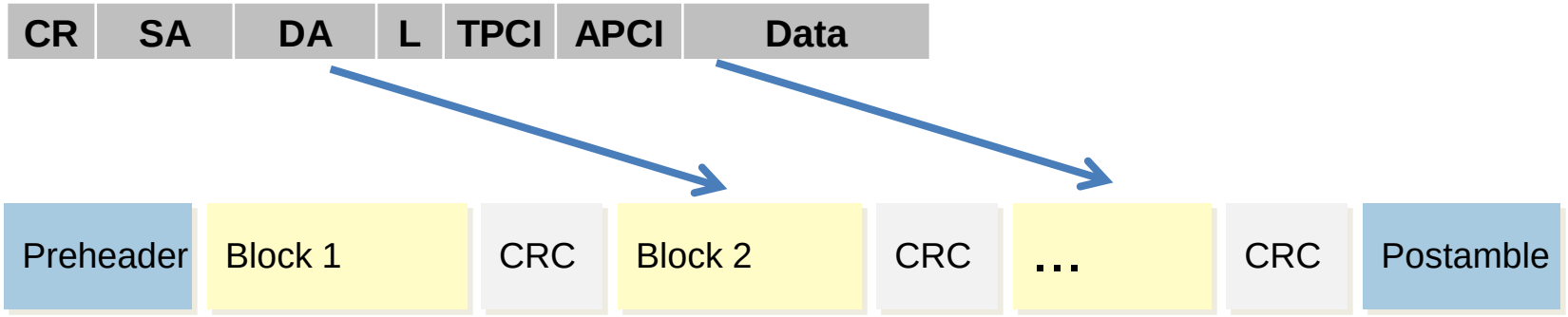


KNX Radio Frequency - RF

- Short range device
  - ISM Band 868 MHz
  - FSK Modulation
- Good range within buildings
  - Very reliable
  - No Mesh required
  - Re-transmitters possible
- No dedicated KNX transceiver required
- Low cost production



Frame format KNX RF ready



IEC870-5-2 (FT3)

- KNX Data in FT3 block format
  - Preheader 176 chips
  - First block 10 bytes (fixed length), RF specific (SN / DoA)
  - Further blocks 16 bytes (variable length), KNX telegram
  - Last block 1 to 16 bytes
  - CRC 2 bytes CRC after each block
  - Postamble 2 to 8 chips, end of frame

Addressing Modes

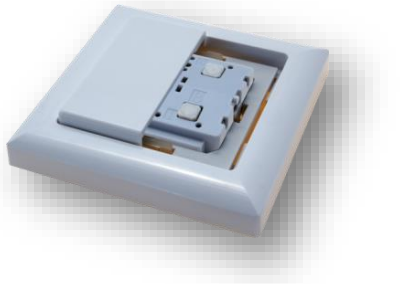
Destination Address		Addressing Mode
IA	DAF = 0	Individual Address
GA	DAF = 1	Group Address
GA = 0x0000	DAF = 1	Broadcast

- Destination Address on KNX RF

Block 1	Block 2, Dest. Address		Addressing Mode
SN	GA	DAF = 1	Ext. Group Address (PB Mode)
DoA	GA	DAF = 1	Group Address
DoA	IA	DAF = 0	Individual Address
DoA	GA = 0x0000	DAF = 1	Broadcast
SN	GA = 0x0000	DAF = 1	System Broadcast

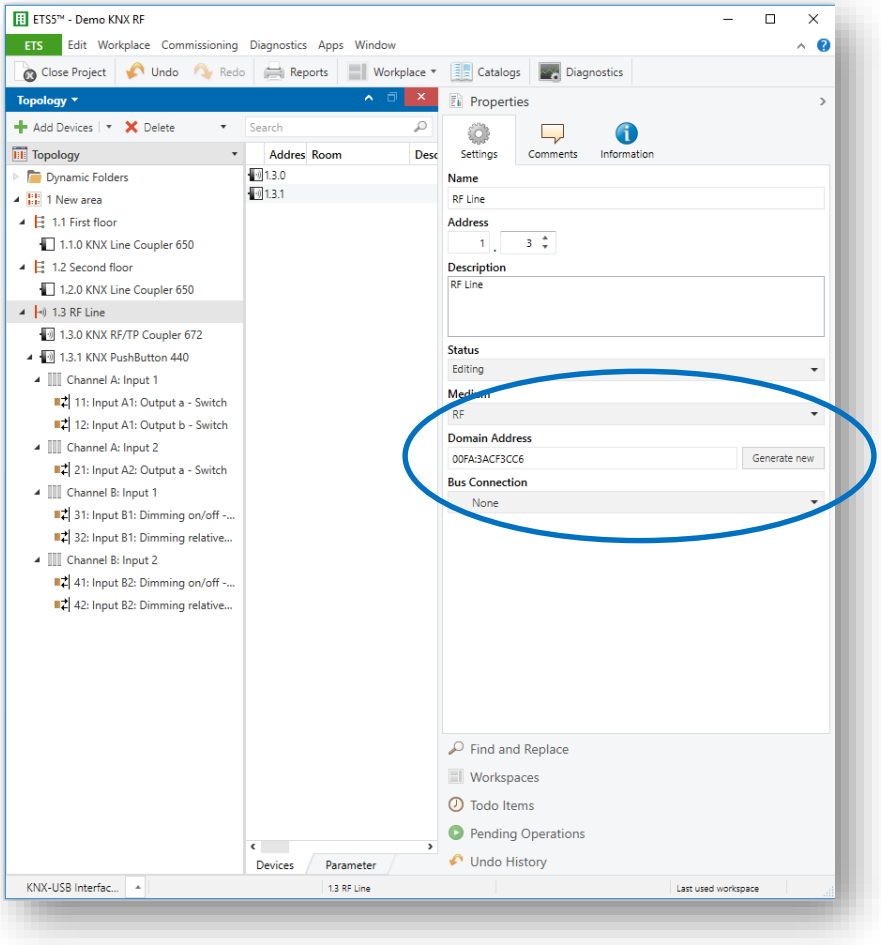
Application Area

- KNX wireless devices
  - Sensors
  - Actuators
  - Remote control
  - …
- RF-only Installations
  - Renovation market
- Hierarchical Installations
  - RF combined with TP and IP
  - In one ETS project



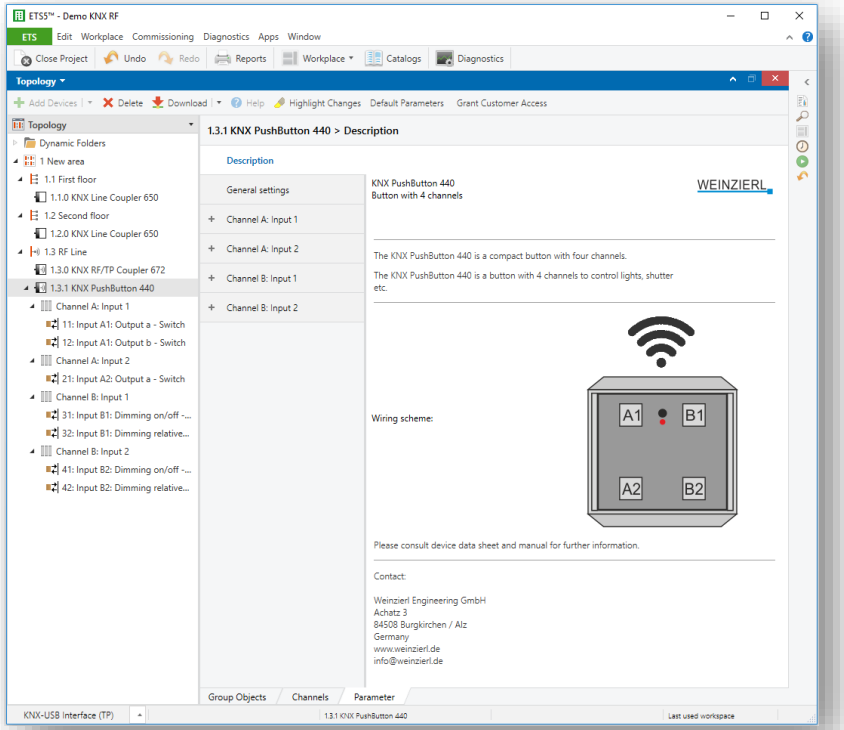
ETS5 & RF

- What's new
  - Lines for RF
  - Domain addresses
  - Connection via USB / RF Interface
  - RF / TP Coupler
- What's unchanged
  - Group Objects
  - Group Addresses
  - Parameters
  - Download



ETS – Group Objects & Parameters

- Group Objects
  - Linked via group addresses
  - Configured by flags
- Parameters
  - Device configuration
  - Set in parameter dialog
- Download
  - Via KNX network
  - Via USB / RF Interface
  - Via TP and RF / TP Coupler
  - Local USB connection



Topology: RF-only Installation

- Minimal RF Setup
  - KNX RF Devices
    - 2..255
  - KNX Interface to PC
    - USB, optional
    - For commissioning only

DVC **KNX RF Device**

Topology: TP line + RF line

Line 1

RF / TP

PS / Ch

DVC 1

DVC 255

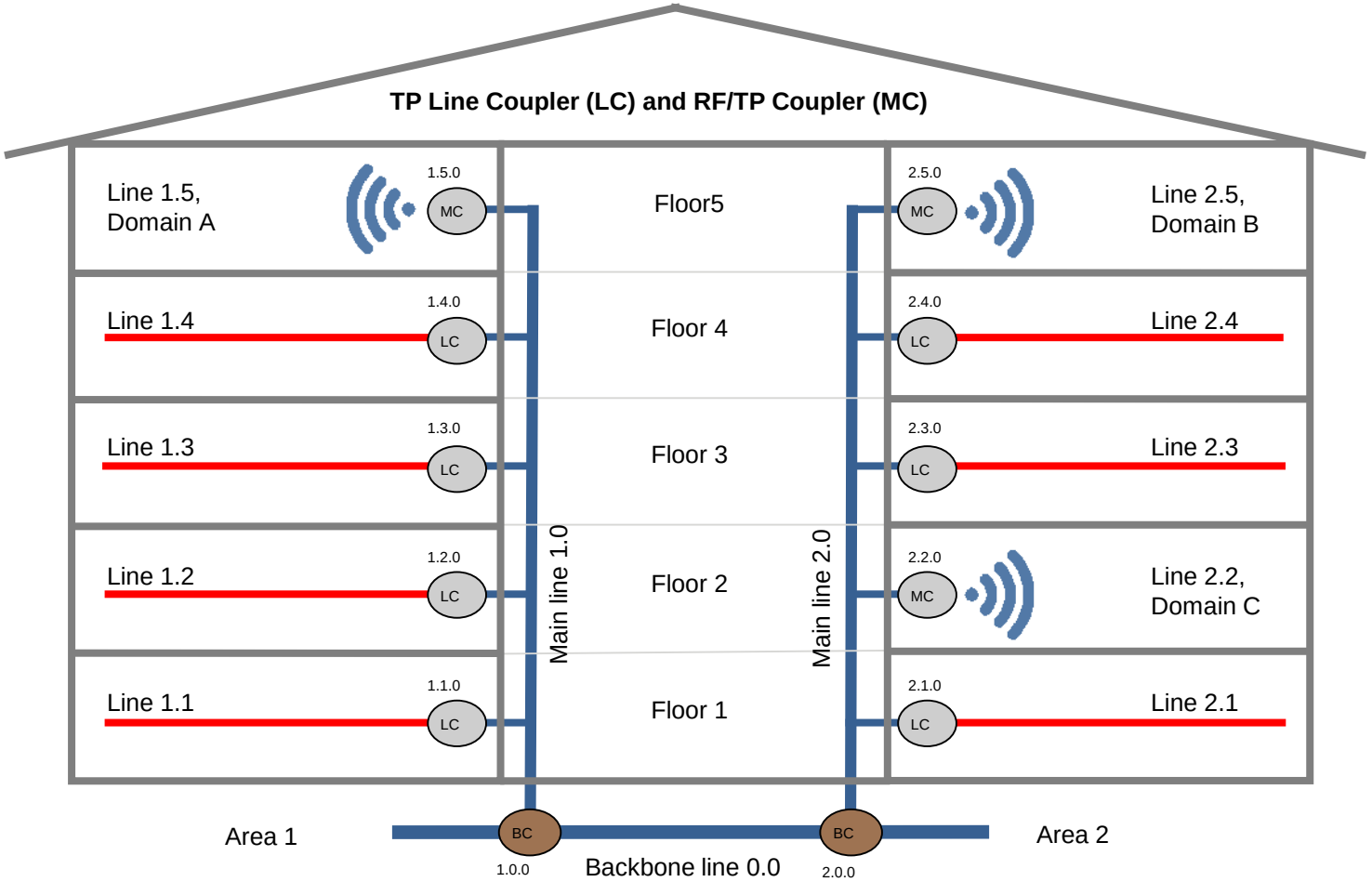
Line 2

DVC 1

DVC 255

DVC **KNX Device**

Topology: Structure in building



Further aspects about KNX RF

- Semi-bidirectional devices
  - For battery driven sensors
  - Bidirectional for commissioning
  - Unidirectional during runtime
- KNX RF Multi
  - Usage of different channels
  - Fast ACK
  - High effort for implementation
  - Support by ETS in preparation
- KNX Data Security
  - Required for many applications
  - Available: NOW!

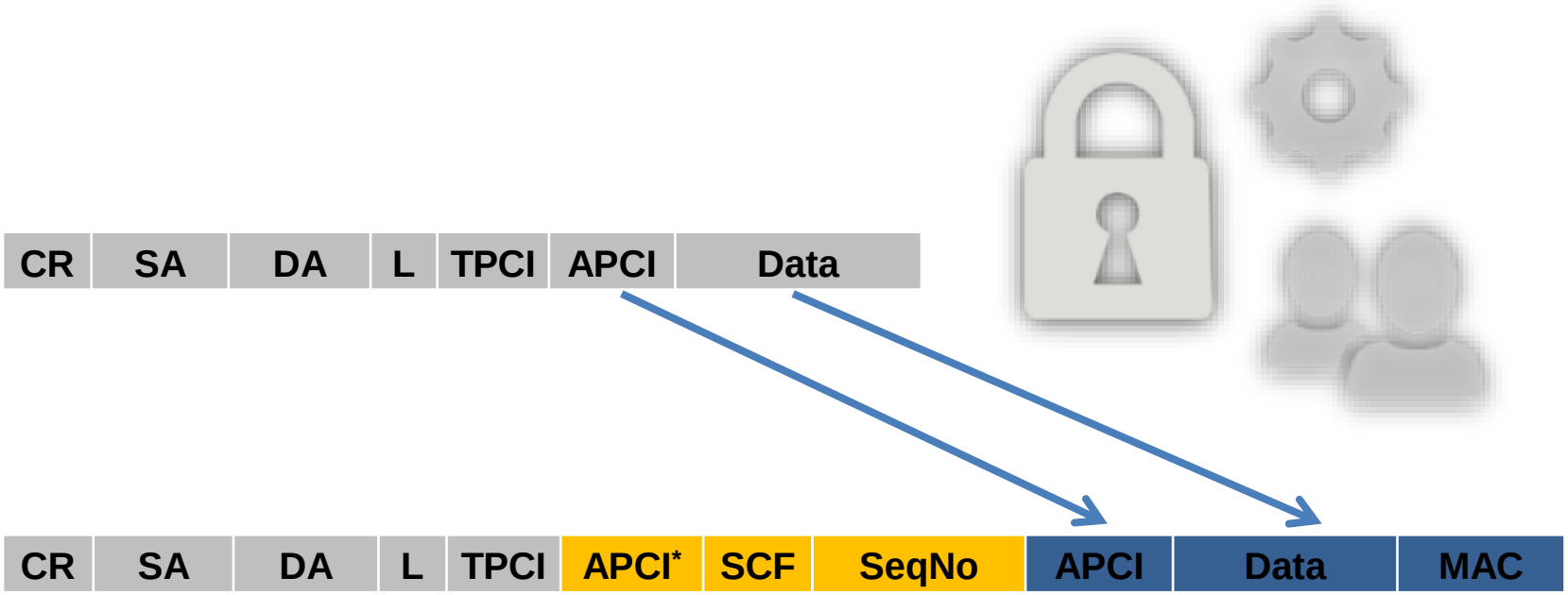
KNX Security

- Based on standard security technologies
- Based on AES
  - Advanced Encryption Standard
  - Since 2000 “de facto” standard for symmetric encryption
  - Block length: 128 bits
  - Key length: 128 bits
- Challenge: KNX System aspects
  - E.g. group addressing

Security Goals in General

- Data Integrity
  - Prevents an attacker from manipulating the data (MAC = Message Auth. Code)
- Freshness
  - Prevents data from being recorded and replayed (Sequence No.)
- Confidentiality
  - Prevents the data from being monitored; Data is encrypted (AES)

KNX Data Security: Frame Format



KNX Frame with Authentication and Encryption

KNX Data Security: Keys

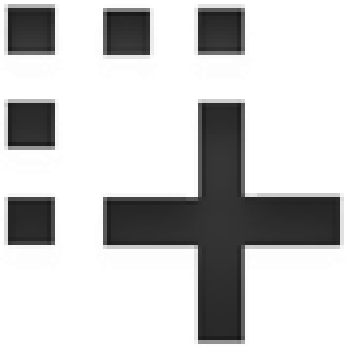
- FDSK (Factory default setup key)
  - Set by manufacturer, shown as QR-Code
  - Reactivated after master reset
- Tool key
  - Replace FDSK
- P2P keys
  - Point-to-point communication
- Group keys
  - Runtime communication

KNX Data Security: Sequence counter

- 48-bits long
- Sending
  - One per device
  - Continuously incremented on sent message
- Receiving
  - One per communication partner (device)
  - Accept only higher values
- Tool access
  - Accept only higher values
  - Non-readable / non-writable
  - Synch-Service required

- Persistency required!

KNX Data Security: Resources

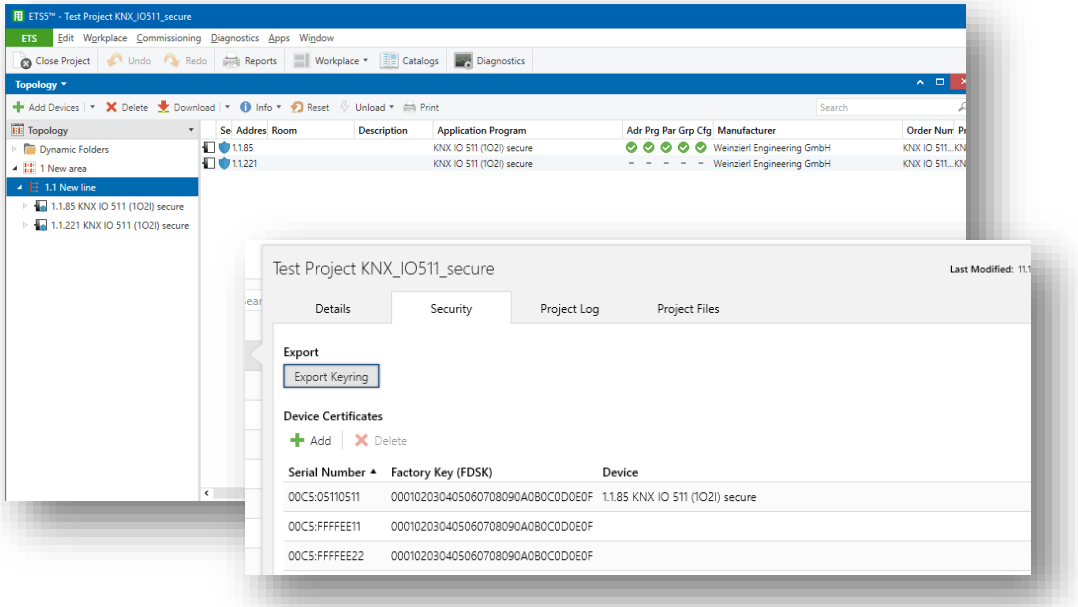


- 18 bytes per group address
  - Key
  - Index
- 8 bytes per communication partner (device)
  - Individual Address
  - Counter
- 20 bytes per communication per p2p link
  - Index
  - Key
  - Roles

- Significantly more memory required!

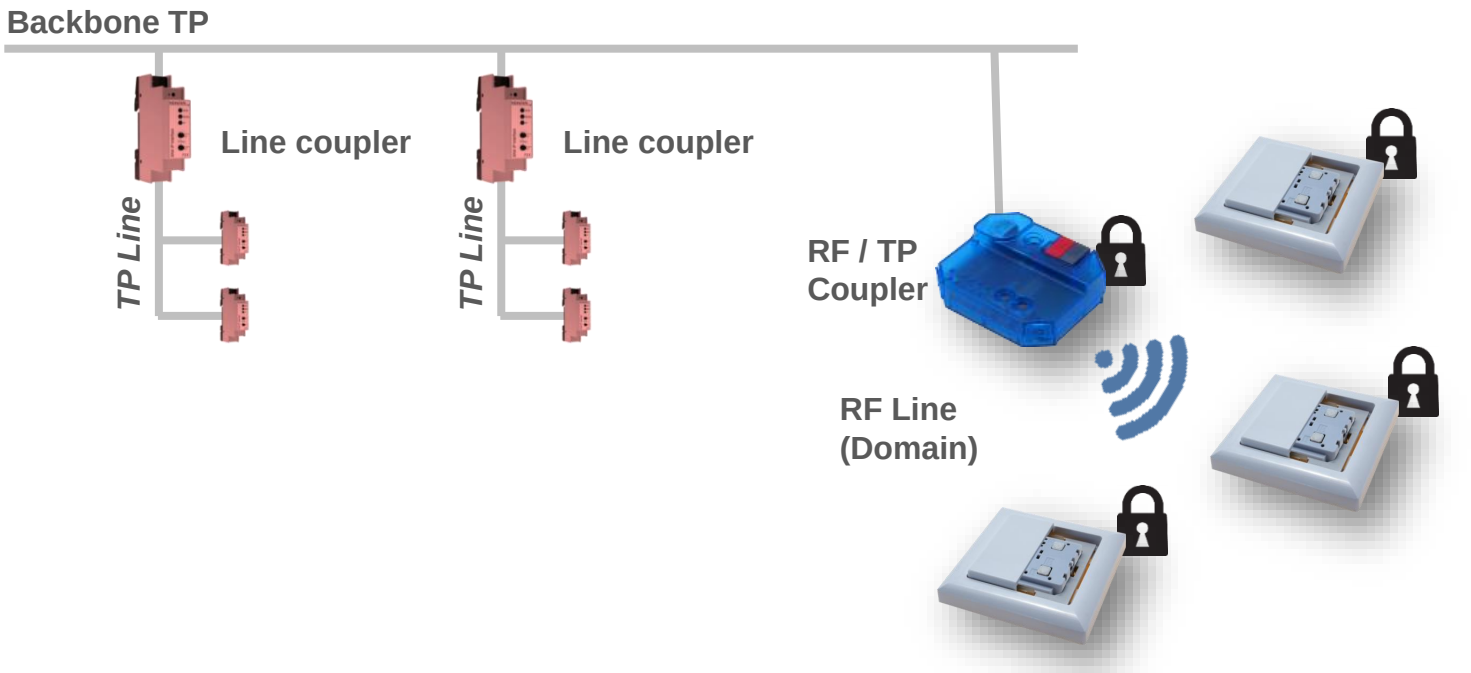
KNX Security in ETS

- Fully Integrated
- Using camera for QR-Code
- Secure configuration
- Secure Download



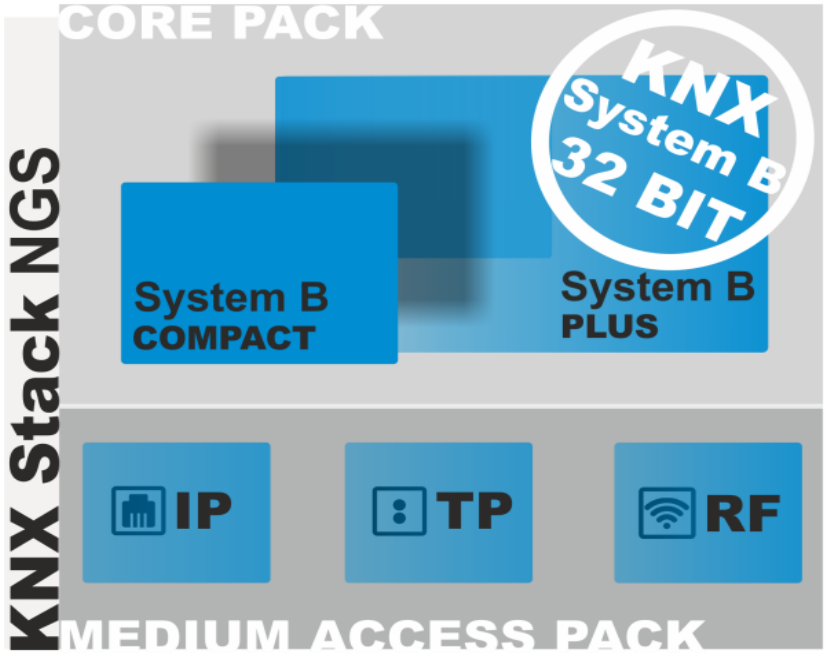
Mixing secure and non-secure Communication

- Security per link
- Security in sub-systems
  - KNX Secure Proxy
  - In preparation for ETS



KNX Stack Implementation NGS

- Professional solution
  for high volume products
- KNX Security integrated
- Modular
  - Twisted Pair TP
  - Radio Frequency RF
  - Ethernet / IP
- Scalable
  - Compact
  - Plus
- Development HW
- Tools



KNX Development Tools

- Net'n Node
  - Bus Monitor and Analyzer
- TraceMon
  - Optimized debug support
- kScript
  - Model driven design
  - Script based system
  - Automated generation of ETS product entries
- kDrive SDK
  - For tool development
  - Bus access and services
  - Free and commercial versions

net'n'node
kScript
kDrive

Conclusion

- KNX RF
  - Fully integrated in the KNX System
  - One tool fits all: ETS5
  - Potential for complex topologies
  - Security enables new applications

- Technology available
  - Specification, ETS, EITT
  - KNX Stack and Modules
  - Development tools

Let it fly...

Thanks.

KNX RF - Security Inside

For general questions:
info@knx.org – www.knx.org

Weinzierl Engineering GmbH
DE-84508 Burgkirchen / Alz
+49 (0)8677 916 36 – 0
info@weinzierl.de
www.weinzierl.de

Smart home and building solutions.
Global. Secure. Connected.