Diplomarbeitspräsentation

HIGHLY AVAILABLE KNX NETWORKS

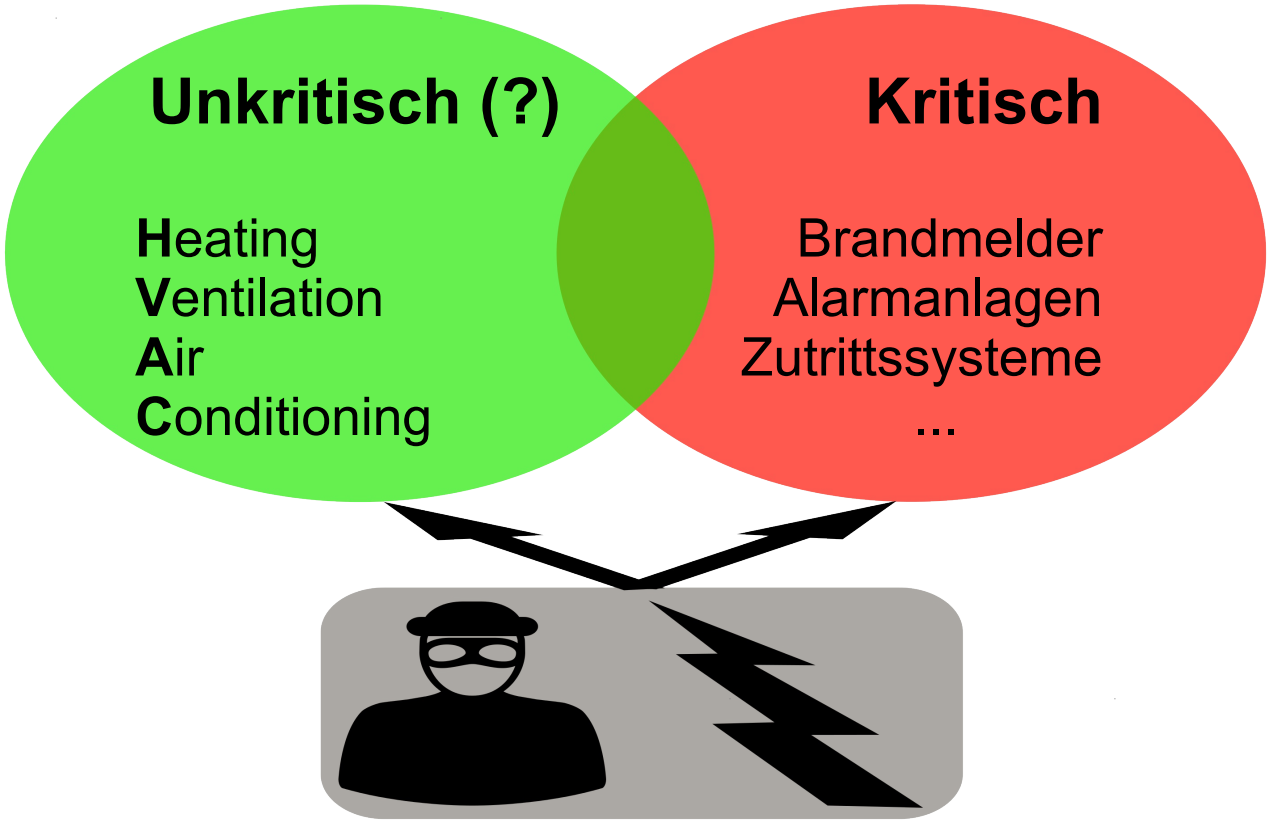
Harald Glanzer

Betreuung

Ao.Univ-Prof. DI Dr. Wolfgang Kastner
DI Dr. Lukas Krammer

Gebäudeautomation

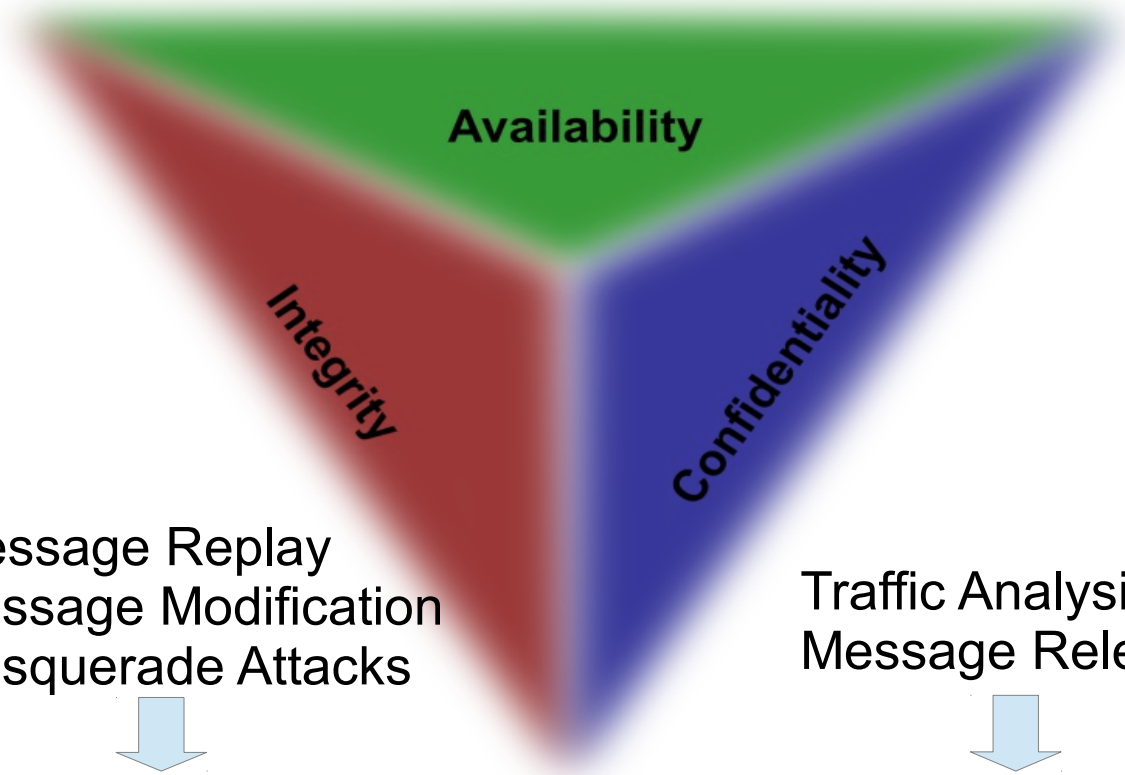
- Energieeffizienz
- Zentrale Steuerung
- Raumkomfort → Produktivität



Informationssicherheit

Böswillige Angriffe: Denial of Service
Transiente Hardwarefehler

Redundanz



Message Replay
Message Modification
Masquerade Attacks

Message Authentication Codes
Und Digitale Signaturen

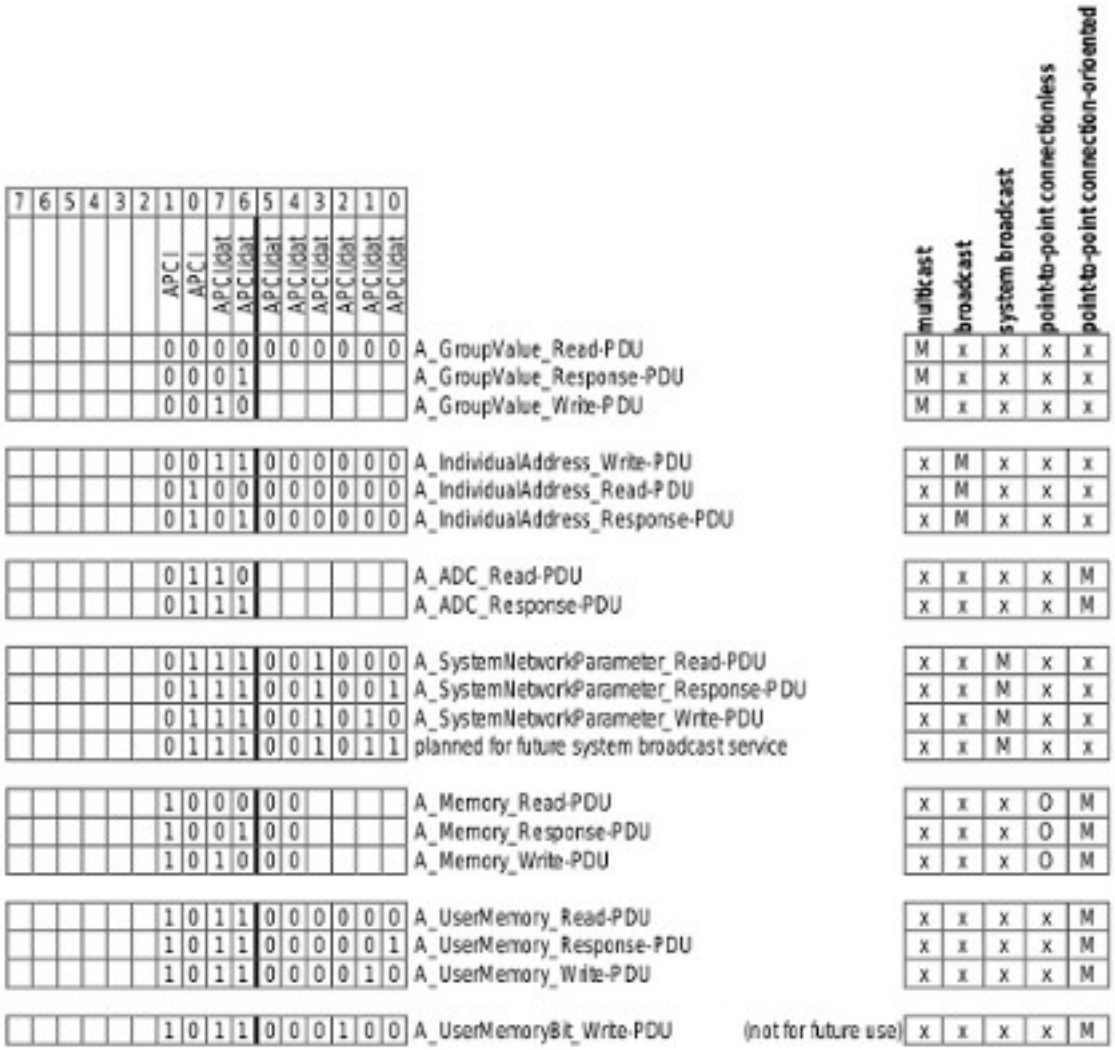
Traffic Analysis
Message Release

Symmetrische / asymmetrische
Verschlüsselung der Daten

- Herausgegeben durch 'KNX Association'
- Zusammenführung von 3 verschiedenen Standards:
  - EIB: European Installation Bus
  - EHS: European Home Systems Protocol
  - BATIBUS
- 'Offener' Standard – Lizenzierung möglich
- ISO OSI Schichtenmodell
- Kommunikation mittels standardisierter 'Data Point Types'

} Herstellerunabhängigkeit

KNX / Layer 7



7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0		multicast	broadcast	system broadcast	point-to-point connectionless	point-to-point connection-oriented
						APCI	APCI	APCIdat	APCIdat	APCIdat	APCIdat	APCIdat	APCIdat	APCIdat	APCIdat						
						0	0	0	0	0	0	0	0	0	0	A_GroupValue_Read-PDU	M	x	x	x	x
						0	0	0	1							A_GroupValue_Response-PDU	M	x	x	x	x
						0	0	1	0							A_GroupValue_Write-PDU	M	x	x	x	x
						0	0	1	1	0	0	0	0	0	0	A_IndividualAddress_Write-PDU	x	M	x	x	x
						0	1	0	0	0	0	0	0	0	0	A_IndividualAddress_Read-PDU	x	M	x	x	x
						0	1	0	1	0	0	0	0	0	0	A_IndividualAddress_Response-PDU	x	M	x	x	x
						0	1	1	0							A_ADC_Read-PDU	x	x	x	x	M
						0	1	1	1							A_ADC_Response-PDU	x	x	x	x	M
						0	1	1	1	0	0	1	0	0	0	A_SystemNetworkParameter_Read-PDU	x	x	M	x	x
						0	1	1	1	0	0	1	0	0	1	A_SystemNetworkParameter_Response-PDU	x	x	M	x	x
						0	1	1	1	0	0	1	0	1	0	A_SystemNetworkParameter_Write-PDU	x	x	M	x	x
						0	1	1	1	0	0	1	0	1	1	planned for future system broadcast service	x	x	M	x	x
						1	0	0	0	0	0					A_Memory_Read-PDU	x	x	x	O	M
						1	0	0	1	0	0					A_Memory_Response-PDU	x	x	x	O	M
						1	0	1	0	0	0					A_Memory_Write-PDU	x	x	x	O	M
						1	0	1	1	0	0	0	0	0	0	A_UserMemory_Read-PDU	x	x	x	x	M
						1	0	1	1	0	0	0	0	0	1	A_UserMemory_Response-PDU	x	x	x	x	M
						1	0	1	1	0	0	0	0	1	0	A_UserMemory_Write-PDU	x	x	x	x	M
						1	0	1	1	0	0	0	1	0	0	A_UserMemoryBit_Write-PDU (not for future use)	x	x	x	x	M

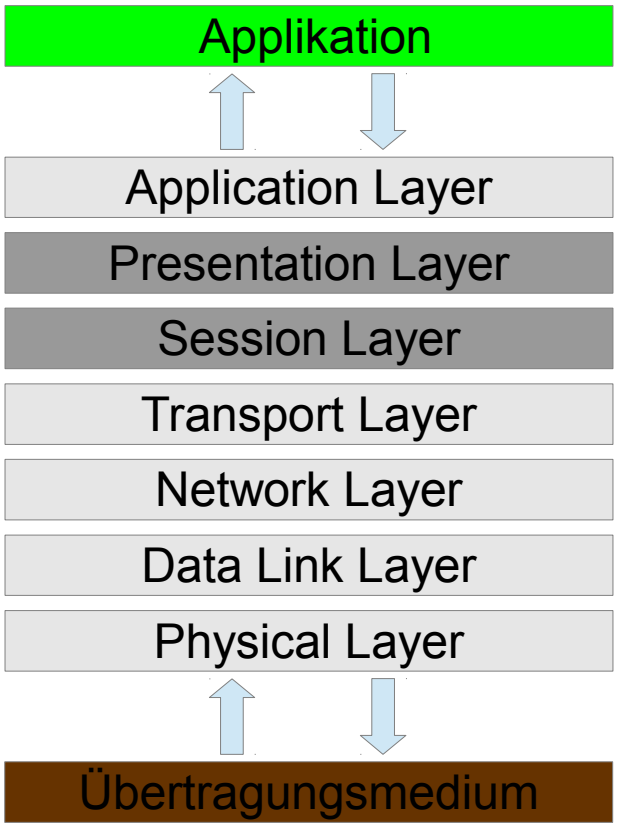
KNX / Layer 5+6

- Data Point Types

  → eindeutige Darstellung
  → L6 nicht notwendig

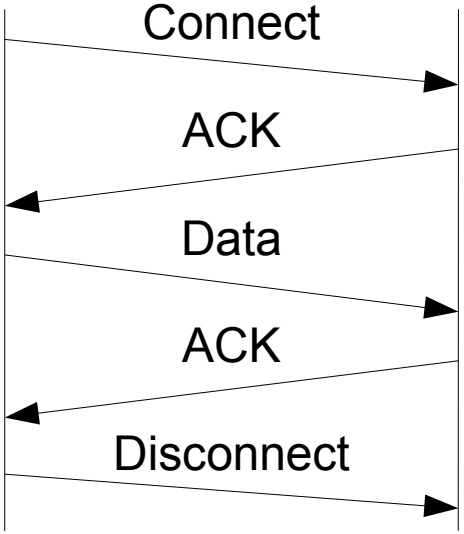
- Zustandsloses Protokoll

  → L5 nicht notwendig

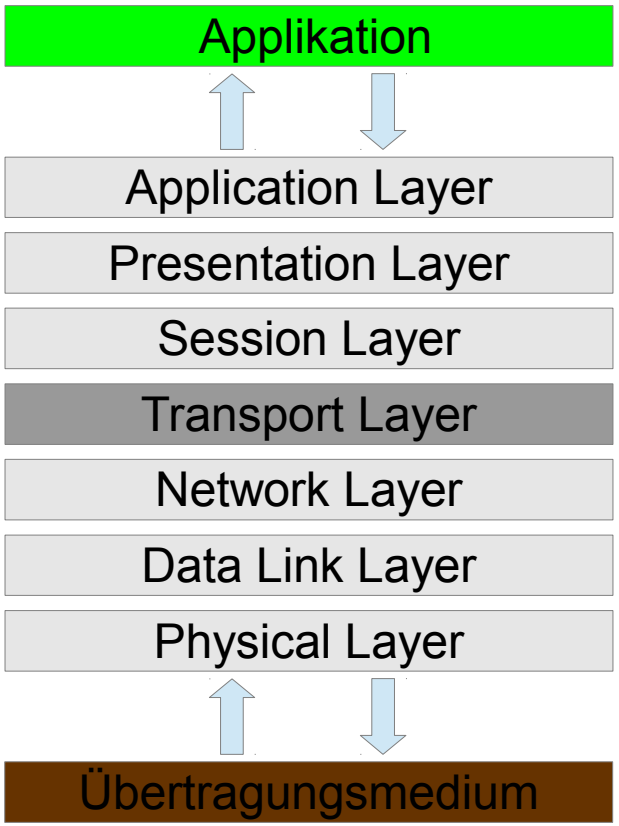


KNX / Layer 4

- Bestätigte Verbindungen
  - Punkt – zu – Punkt



- Unbestätigte Verbindungen
  - Punkt – zu – Punkt
  - Multicast
  - Broadcast



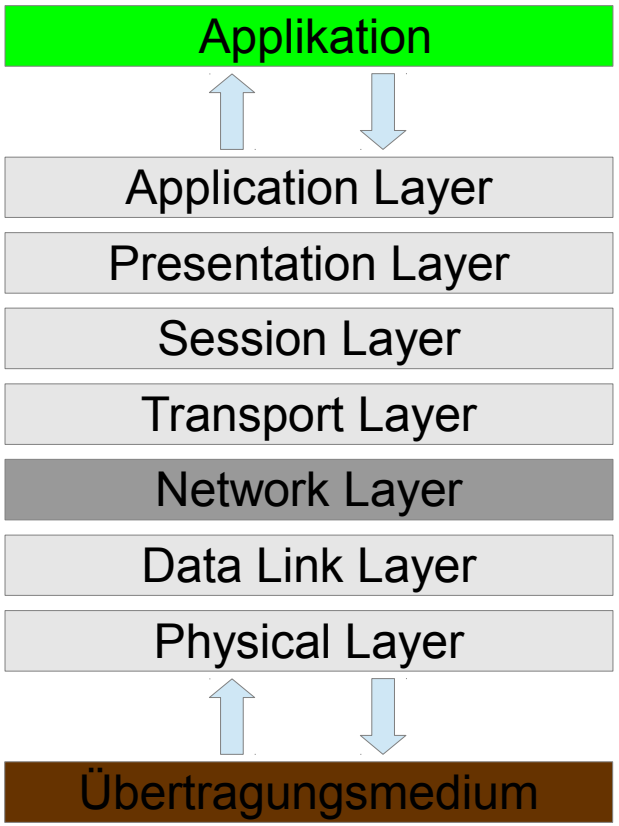
KNX / Layer 3

- 16 Bit Individual Adress
  → eindeutige Geräteadresse

Octet 0								Octet 1							
7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
Area Address				Line Address				Device Address							
Subnetwork Address															

- 16 Bit Group Adress
  → Adresse der Kontrollvariable

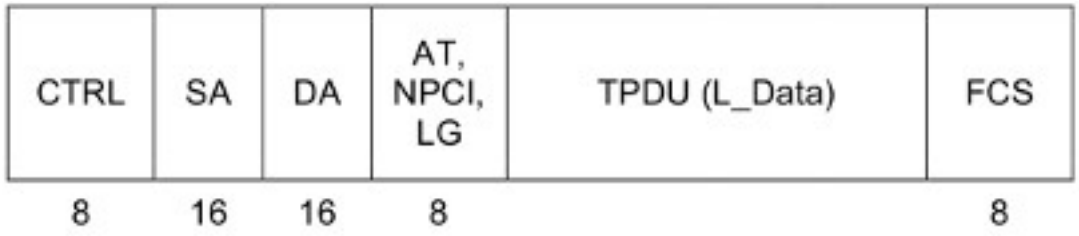
Group Address															
Octet 0								Octet 1							
7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0



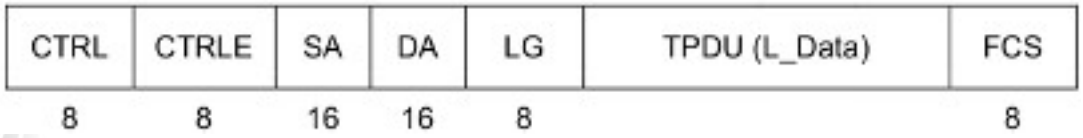
KNX / Layer 2

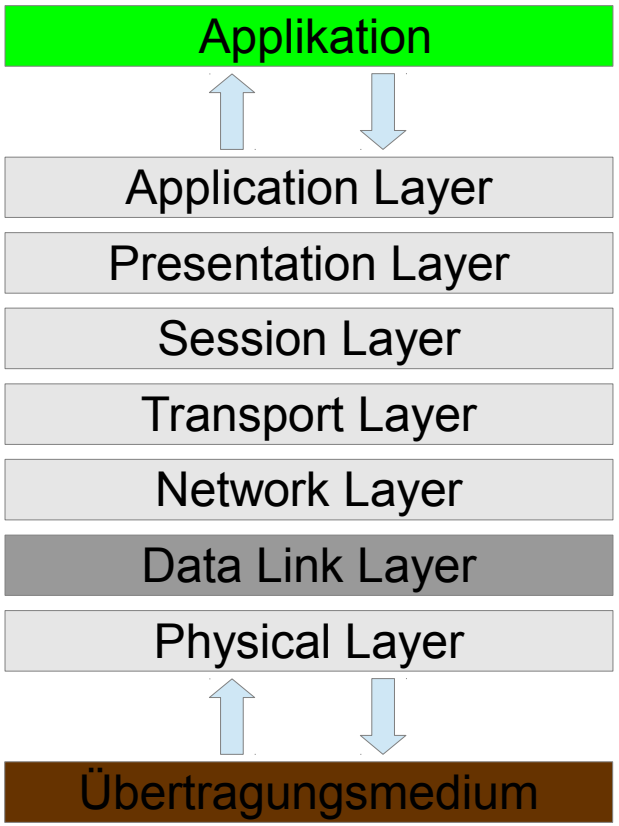
- Verlässliche Übertragung von Frames innerhalb eines Subnetzes
- 2 verschiedene Frame Formate

  - Standard Frames (max. 14 Byte)



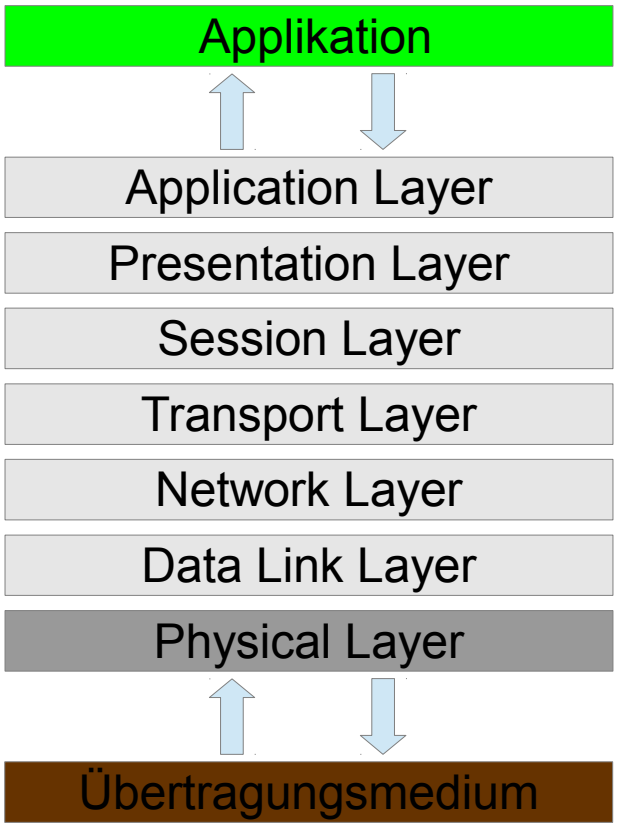
  - Extended Frames (max. 254 Byte)





KNX / Layer 1

- Twisted Pair
  - 9600bps
  - CSMA/CA
  - alle Topologien ausser Ringe
- Power Line
  - 1200bps
  - Übertragung über Stromnetz
- Radio Frequency
  - kabellose Übertragung
- KNX/IP
  - Routing Mode
  - KNXnet/IP
  - KNX IP

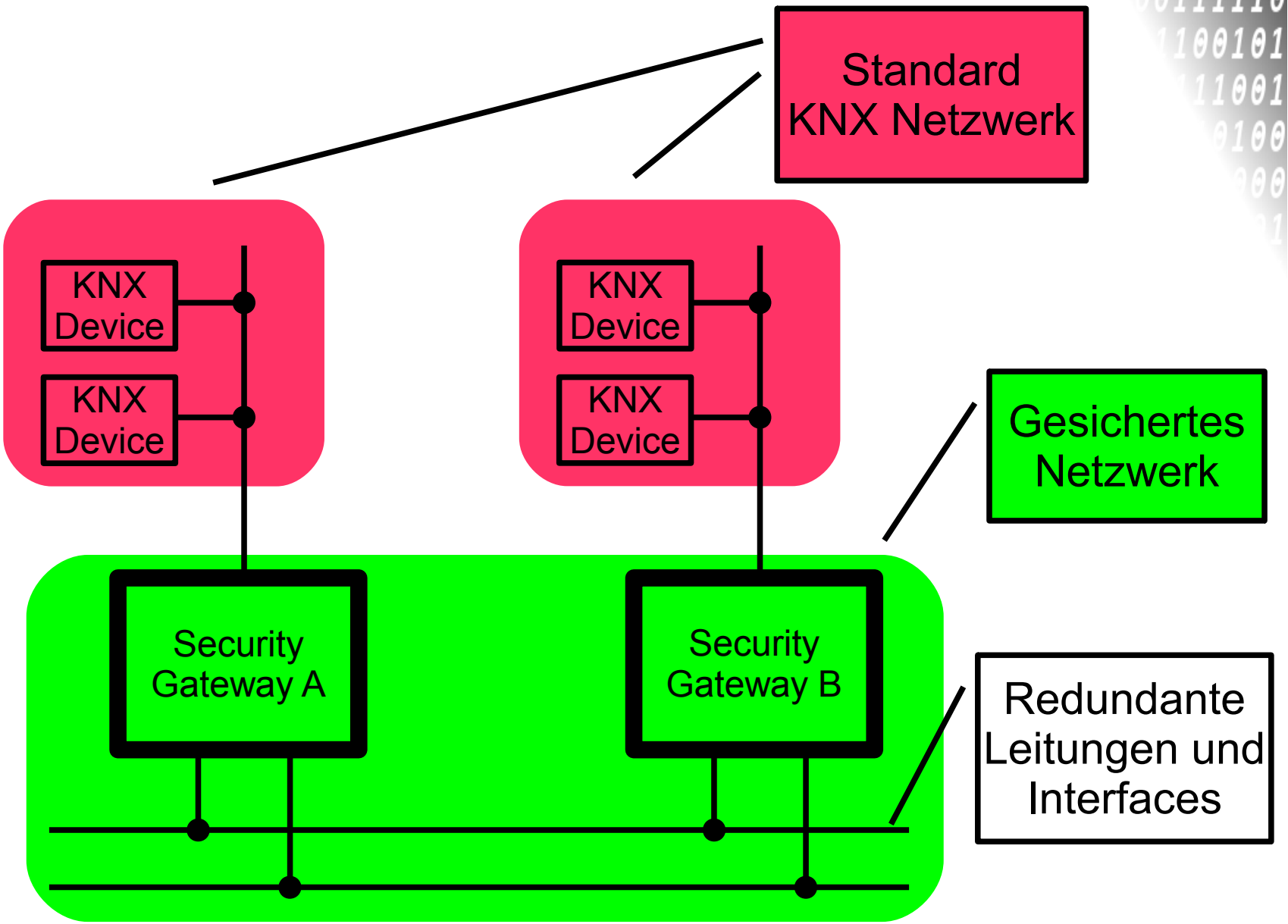


KNX / Sicherheitsmassnahmen

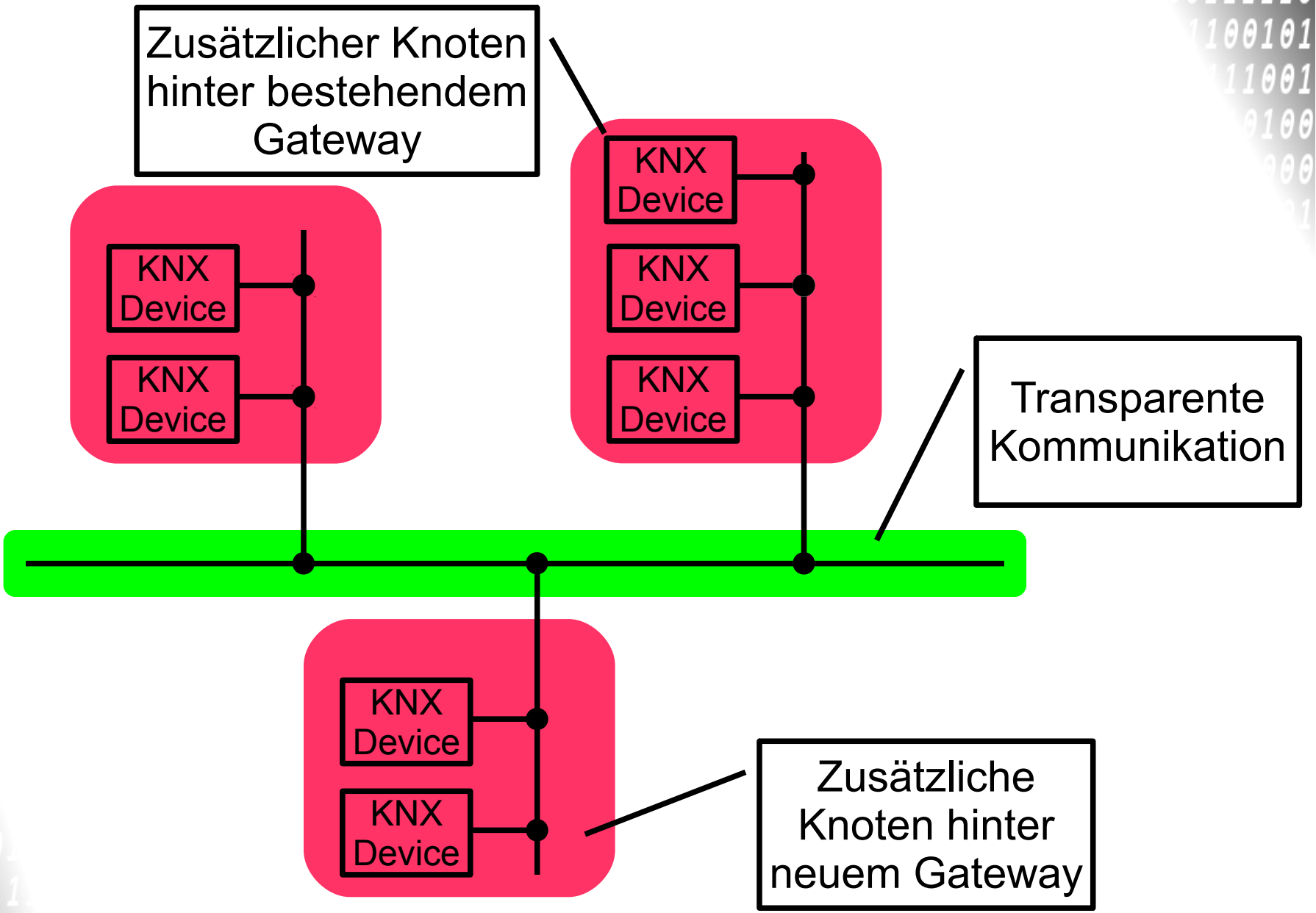
- 'Basic' KNX
  - Cleartextkeys für Managementnachrichten
  - Cleartext für Kontrollinformation
- KNX Data Security
- EIBsec
- KNX IP Security

Erhöhung der Verfügbarkeit
durch zusätzliches Einführen
von Redundanz

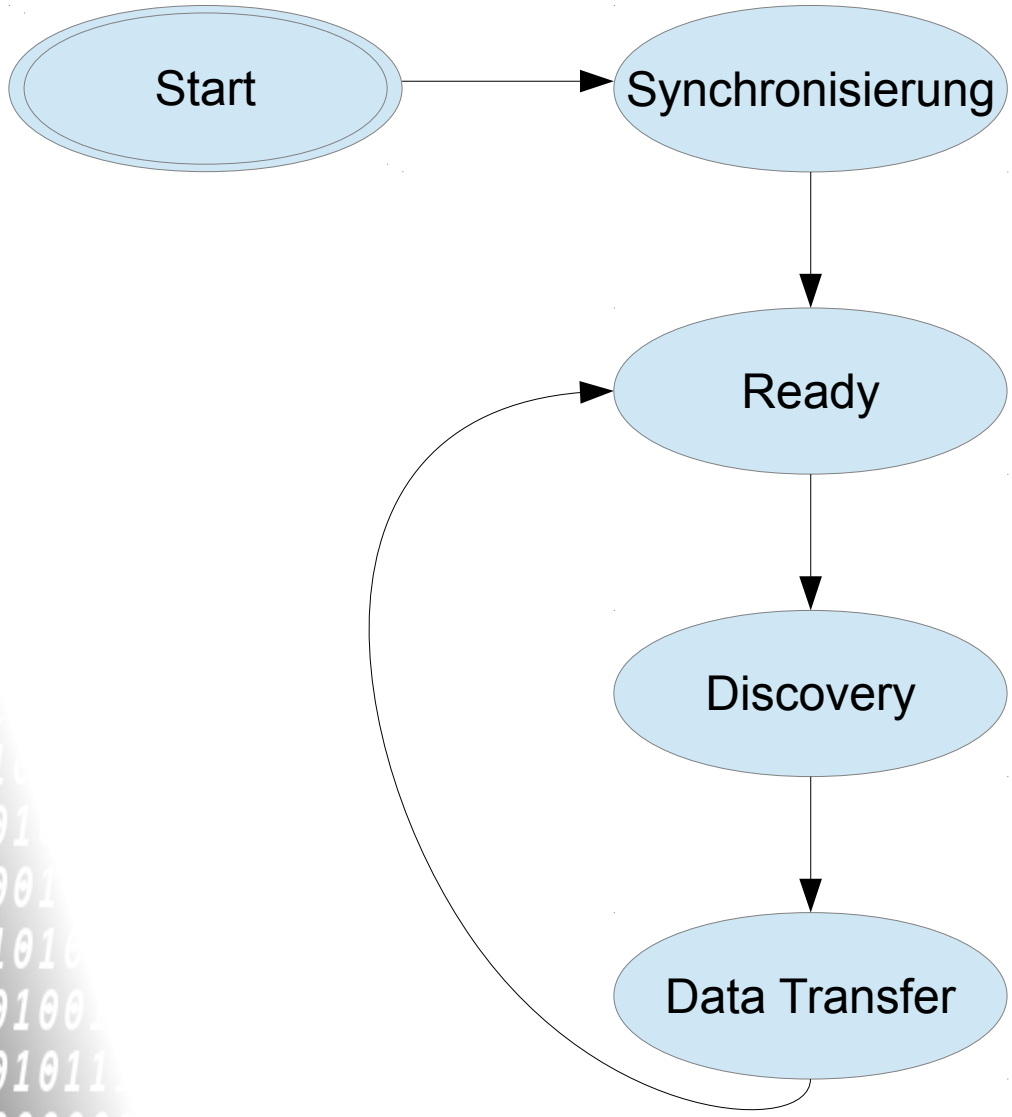
Security Gateways



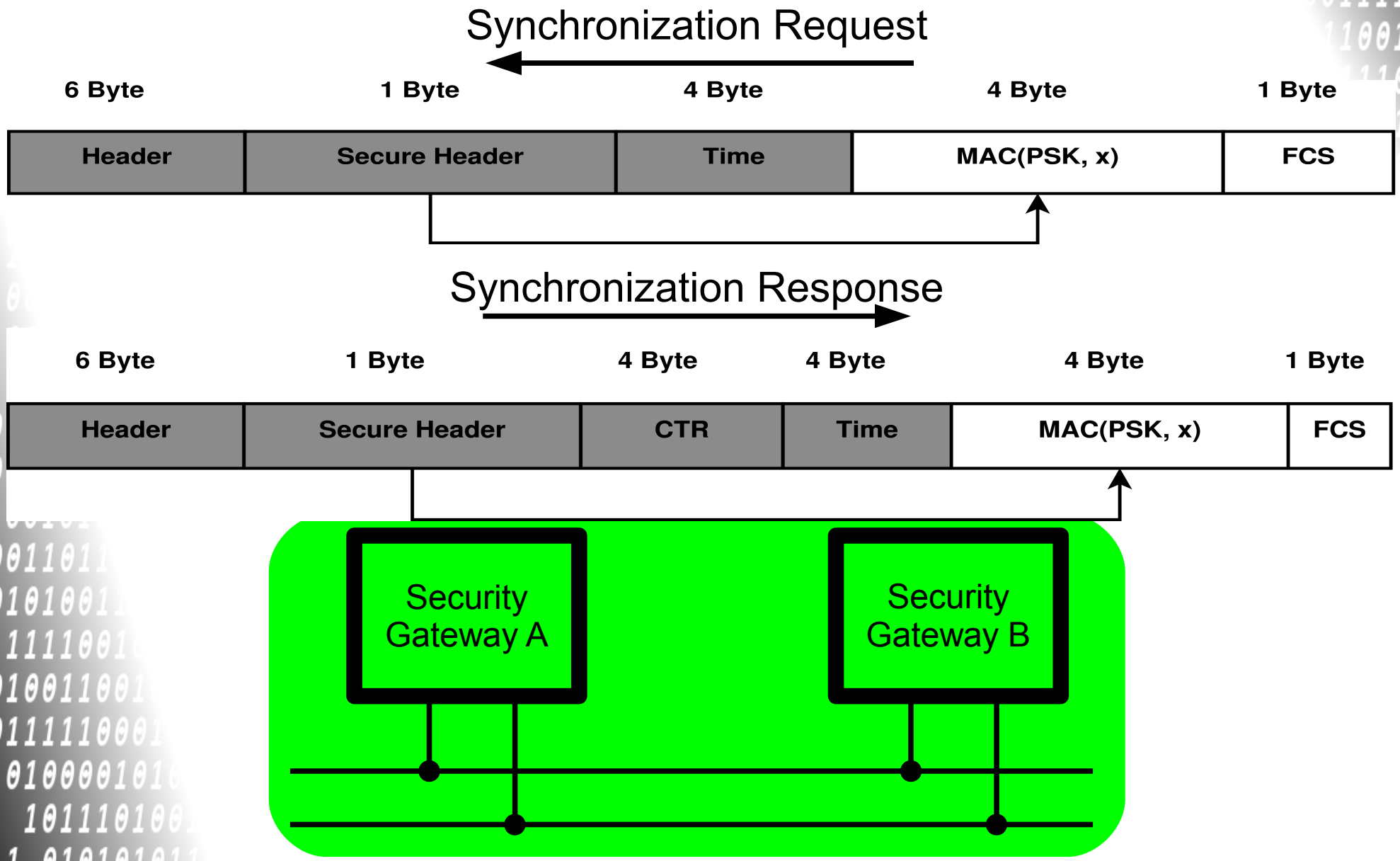
Transparenz & Flexibilität



Protokollphasen

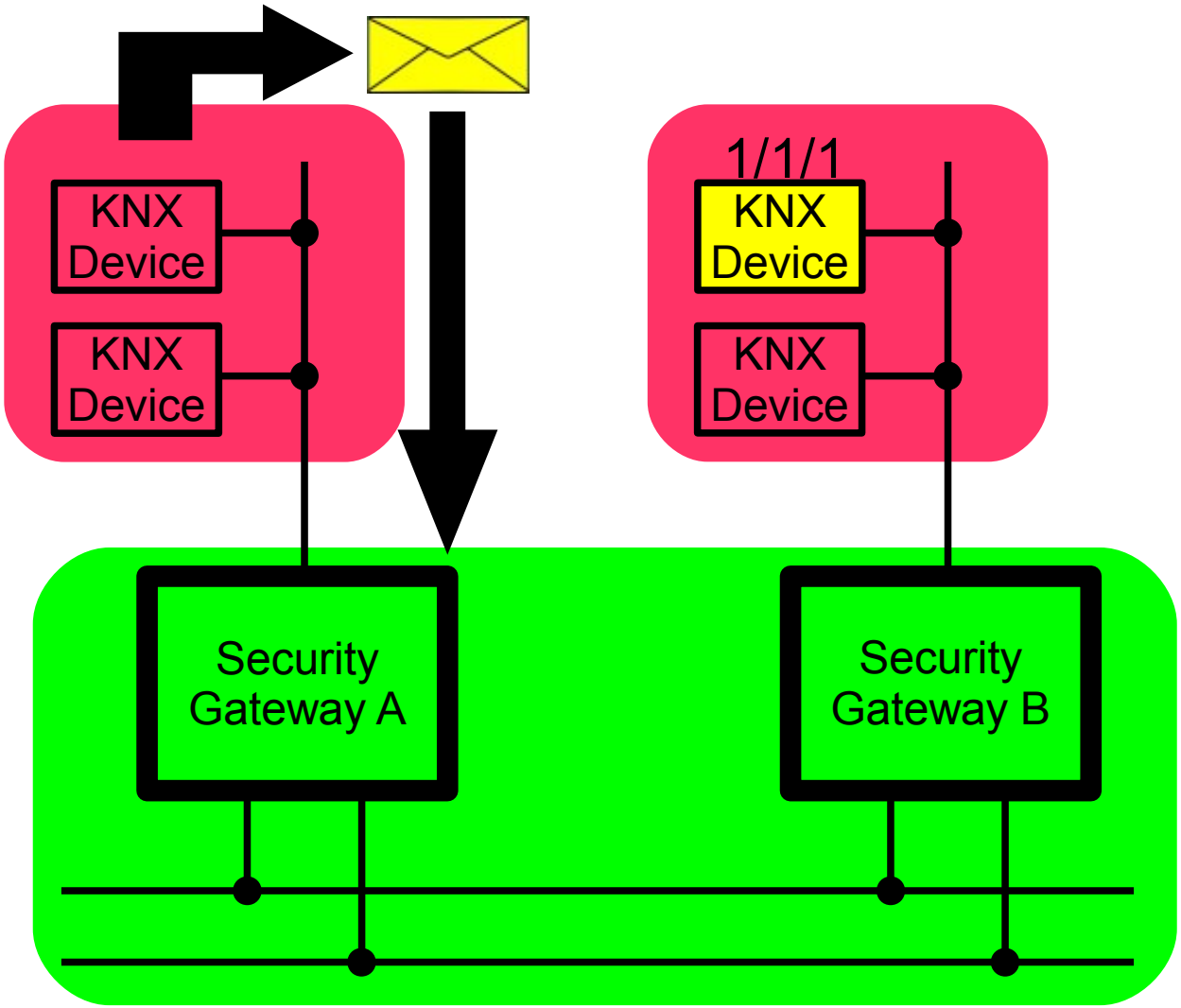


1. Synchronisierungsphase

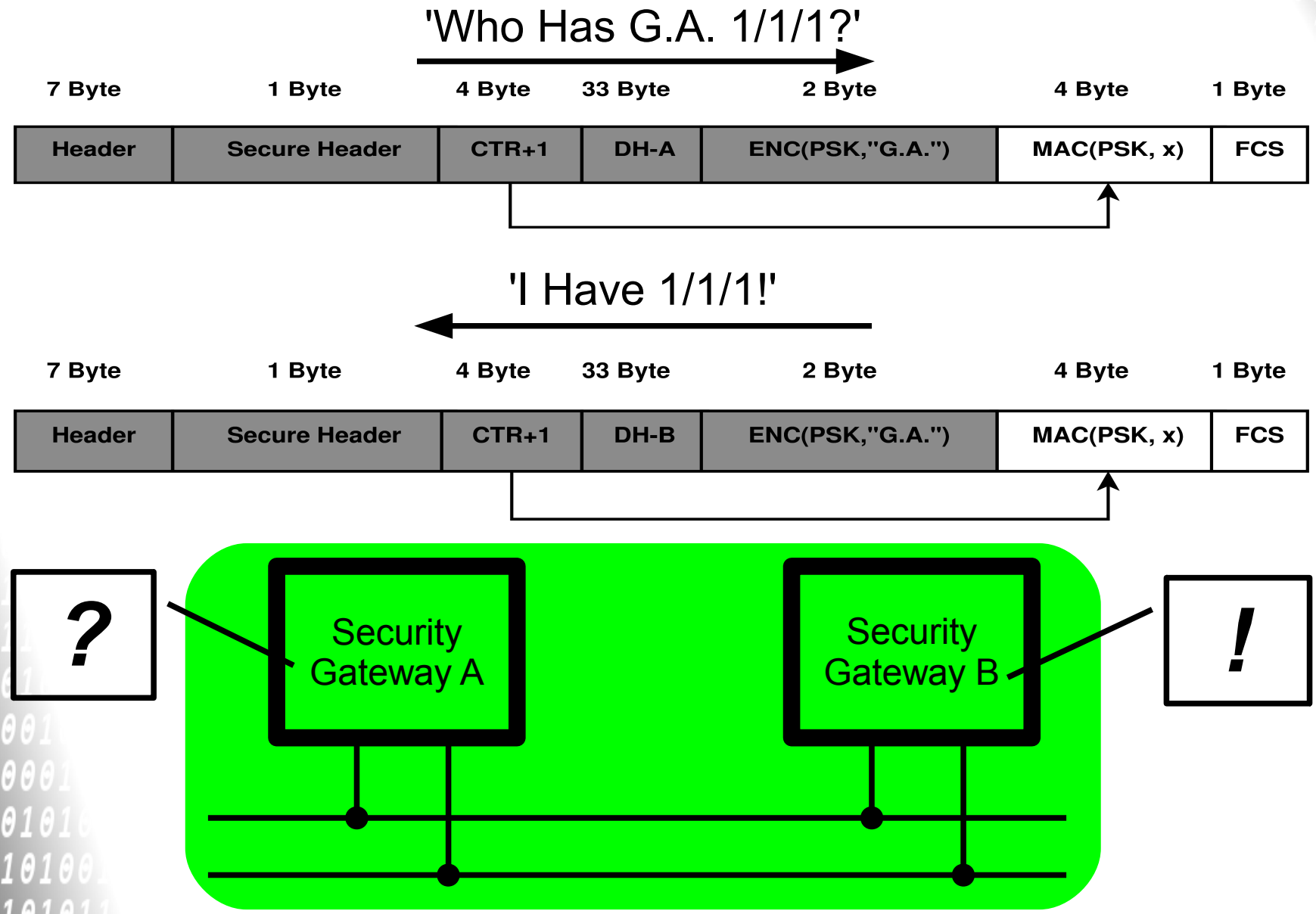


Highly Available KNX Networks

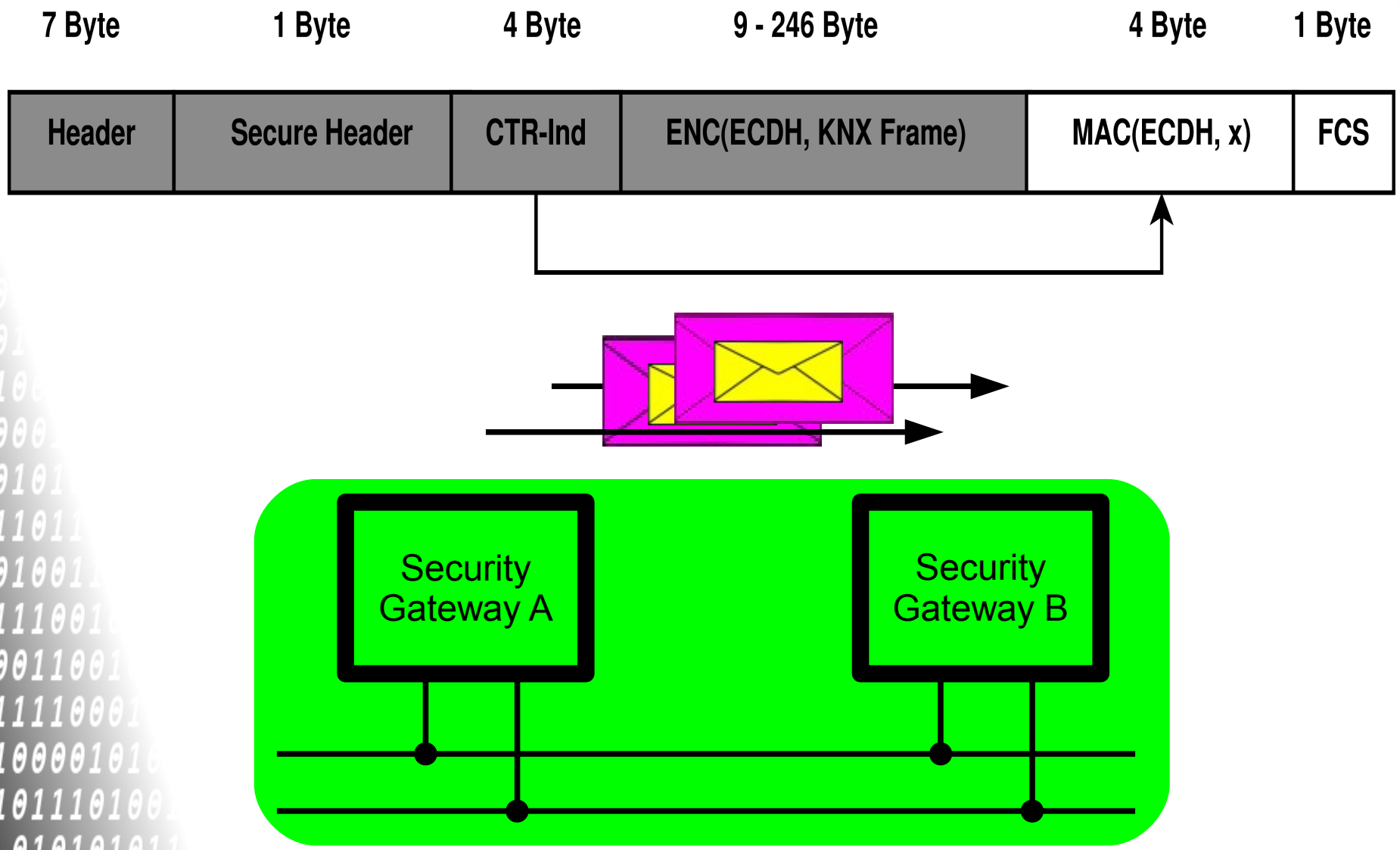
2. Nachricht an Gruppenaddresse 1/1/1



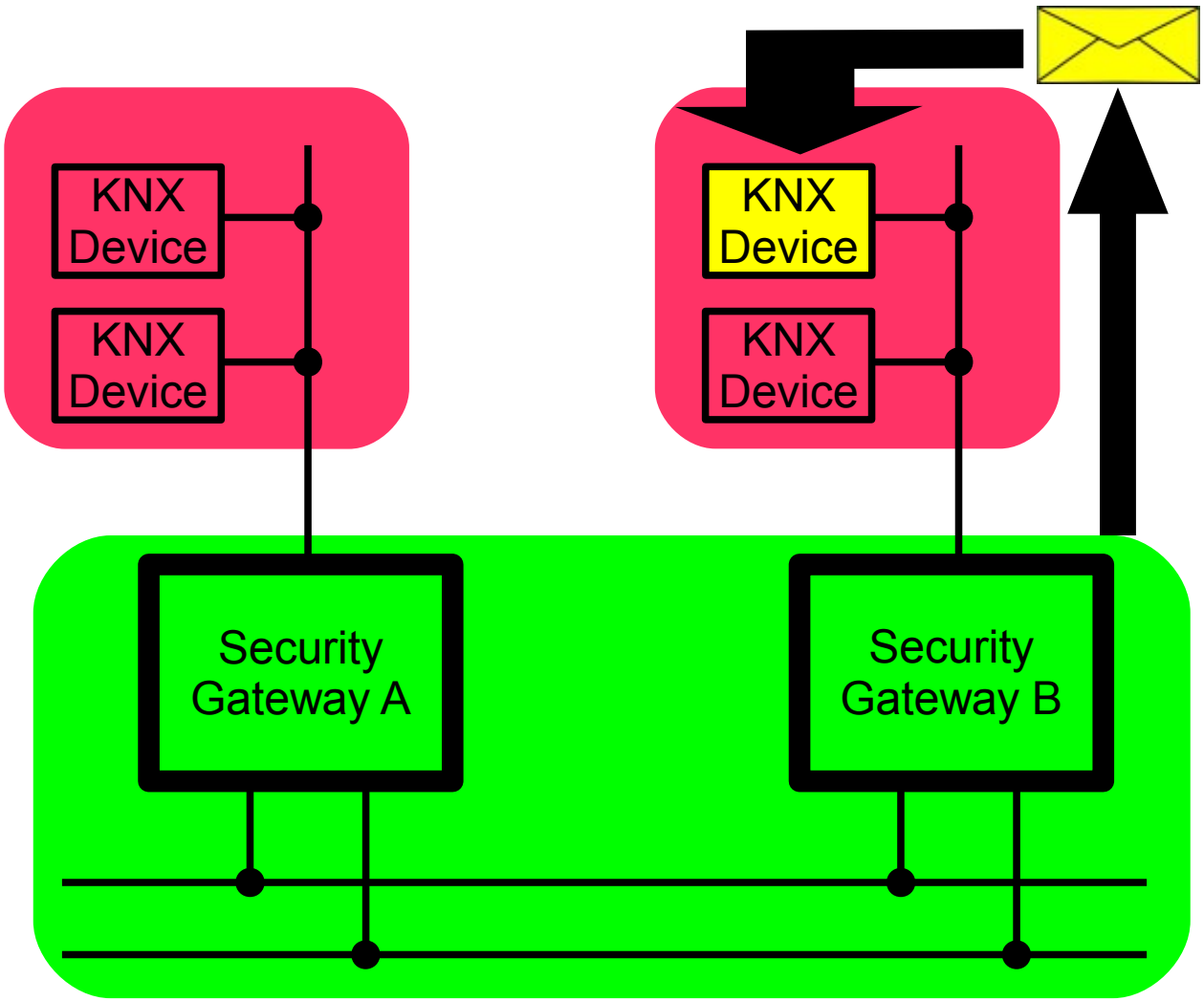
3. Discovery - Phase



4. Redundante Datenübertragung

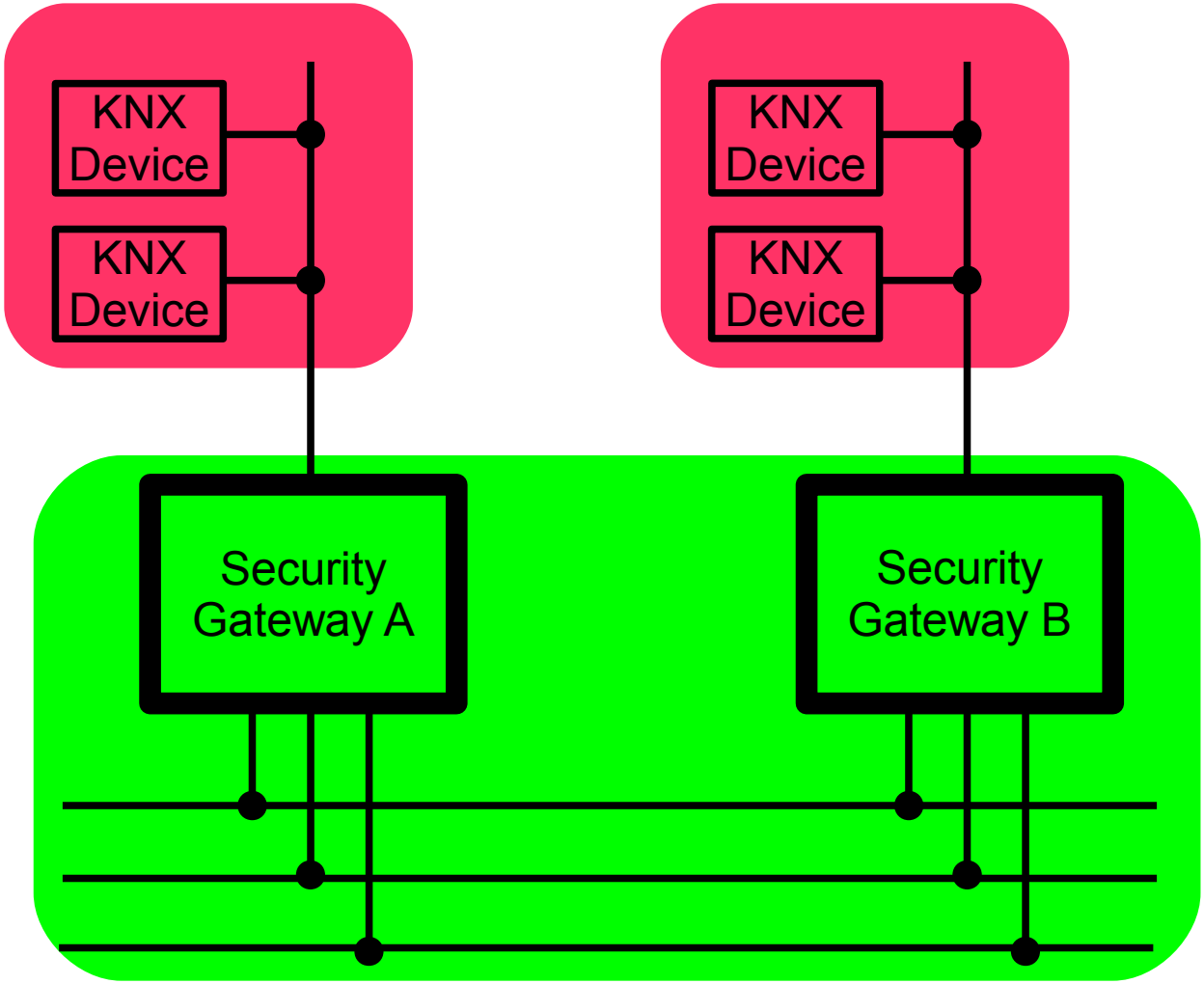


5. Zustellung

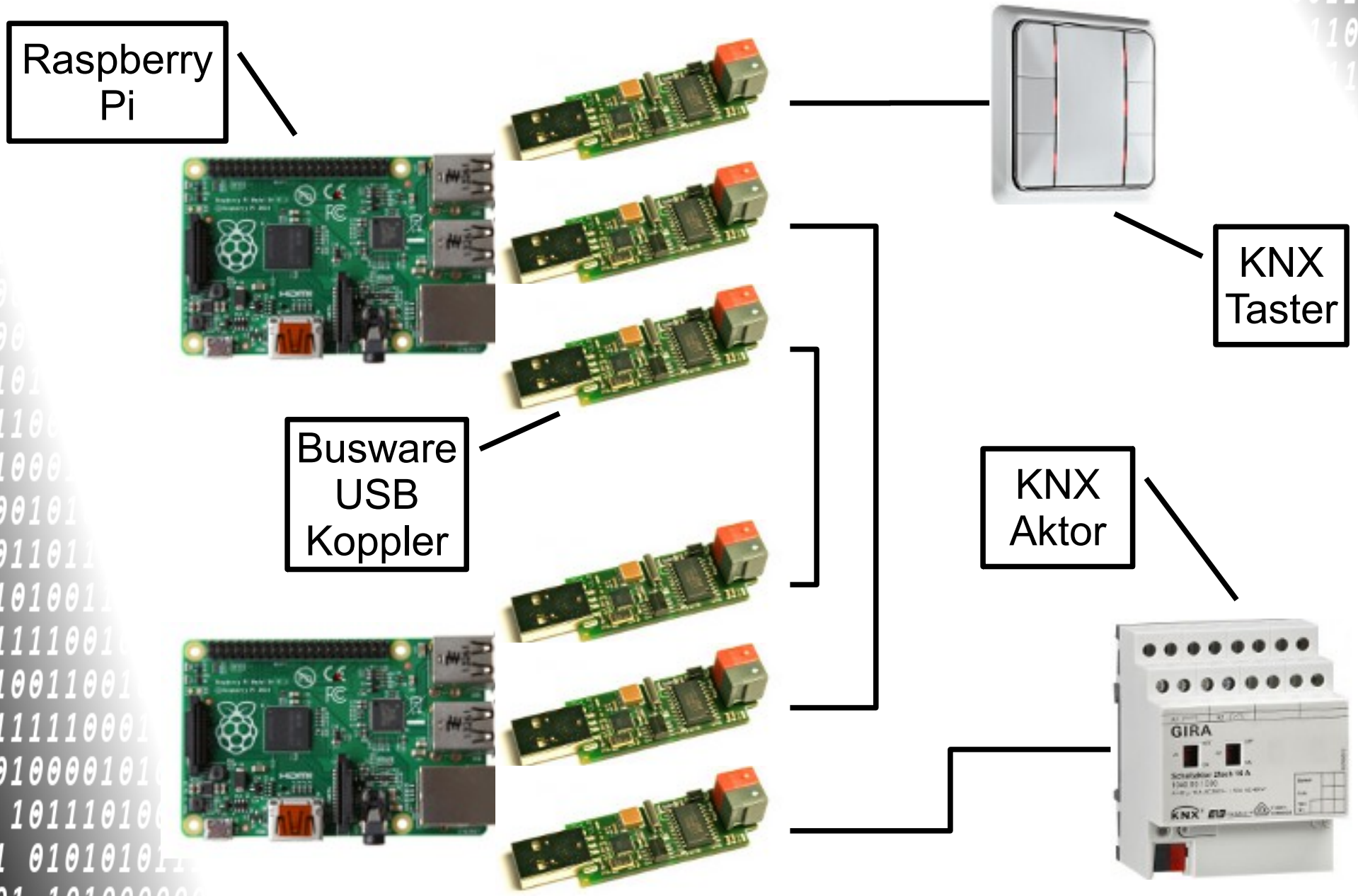


Highly Available KNX Networks

Zusätzliche Redundanz → Verfügbarkeit erhöhen



Evaluierung / Test Setup



Verschlüsselung & Authentifizierung

- MAC: Authentifizierung & Ingetrität
  - HMAC Konstruktion
  - Hash Function: SHA256

- AES: 256 Bit Blockcipher
  - symmetrische Verschlüsselung
  - Counter Mode
  - 2 Keys:
    1x Pre-Shared Authentication Key
    1x Abgeleiteter Key

- Diffie Hellman (DH): Key Negotiation

OpenSSL™
Cryptography and SSL/TLS Toolkit

Elliptic Curves (EC)

- Ursprüngliches Diffie-Hellman (DH) über Finite Fields
  gegeben y,g,p: finde Exponenten x sodass y = g^x mod p
  → Discrete Logarithm Problem (DLP)

- DH über EC:
  gegeben EC, P, Q: finde Integer k sodass P = k * Q
  → Elliptic Curve Discrete Logarithm Problem (ECDLP)

- Allgemeine Form der Kurve: $y^2 = x^3 + a*x + b$
  Definierte Operationen: 'Punkt-Addition', 'Punkt-Verdopplung'

- 'Gleiche' Sicherheit wie DH mit kürzeren Keys

RSA/DH	ECDH
1024	160
2048	224
3072	256
7680	384
15360	512

Source: NIST recommendation

Ergebnisse

- Schutz gegen aktive Angreifer
- Schutz gegen passive Angreifer
- Schutz gegen Transiente Hardwarefehler
- 'Plug – and Play' Funktionalität
  → Erweiterung bereits bestehender KNX Netze möglich
- EIBD API erweitern
- USB Buskoppler: instabiles Verhalten