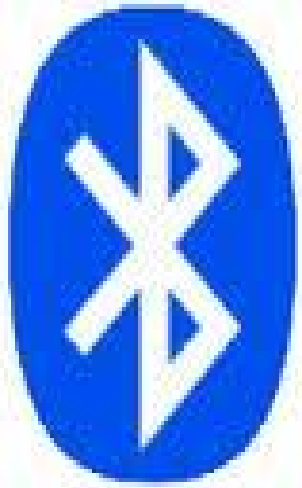
Bluetooth- Theorie

- **Ursprung und Anwendungen**
- **Übersicht der Eigenschaften**
- **Klassen und Reichweiten**
- **Modulation GFSK**
- **FHSS (Frequency Hopping Spread Spectrum)**
- **Paketstruktur**
- **Mechanismen zur Übertragungssicherheit (Authentifizierung, Ecryption, FEC, ARQ)**
- **Profile und Protokolle**
- **Was ist in einem BT-Chip drin ?**

Was ist Bluetooth ?

- Low-Cost, Funkbasierte drahtlose Netzwerk-Technol
- Standardisiert durch die *Bluetooth Special Interest G* (SIG), ein Konsortium, das 1998 von Ericsson, Intel, IBM, Nokia und Toshiba gestartet wurde
- Verwendet das lizenzfreie 2.4 Ghz ISM-Band



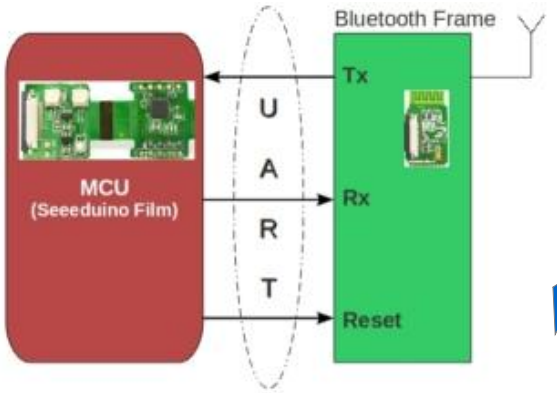
Quelle: http://dramaioldtiden.natmus.dk/vikingetiden/vidensbank/harald_stor.jpg

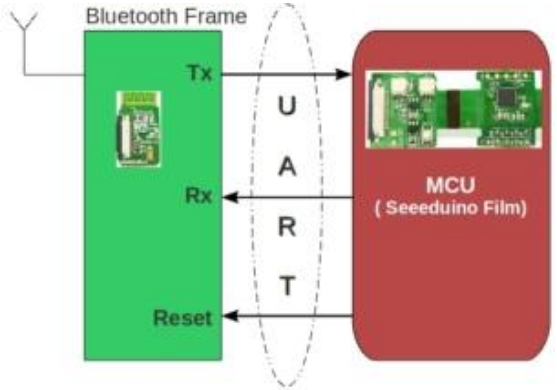
Die Spezifikation wurde nach Harald Blåtand,genannt, einem Dänischen Vikinger-König, der ca. 1000 n.C. Lebte. Blåtand bedeutete dunkle Komplexität und bezog sich vermutlich auf seine dunkele Haut und Haare (und wurde in Englisch zu Bluetooth übersetzt). König Harald wird mit der Christianisierung in Skandinavien und der Einigung von Dänemark und Norwegen in Verbindung gebracht. Der Name wurde adoptiert, weil von Buetooth Wireless Technology eine Vereinigung der Telekommunikations- und Computer-Industie erwartet wurde. Das blaue Logo, das die Bluetooth-Geräte identifiziert ist aus den Runen seines Namens abgeleitet.

.

Kopplung zwischen Bluetooth Geräten

Arduino,
Raspberry Pi
Etc.





Slave

Apple iPAD lässt sich nicht über SPP koppeln wg. fehlender Protokoll-Implementierung

Übersicht der Eigenschaften

- **2.4 GHz ISM-Band (2400-2483,5MHz), 79 HF Kanäle, 1 MHz Kanalabstand**
  - Kanal 0: 2402 MHz … Kanal 78: 2480 MHz
  - Sicherheits-Frequenzabstände Bandende: unterer Rand 2MHz, oberer Rand 3,5MHz
  - Gaussian-FSK Modulation, Hub +/-175kHz (1 MSymbol/s), 1-100 mW Sendeleistung

- **FHSS and TDD**
  - Frequency Hopping mit 1600 hops/s
  - Hopping Sequenz über Pseudo-Random-Generator, Zufallsfolge wird vom Master beeinflusst.
  - Time Division im Duplex-Betrieb zur Sende/Empfangs-Trennung

- **Voice Link**
  - SCO (Synchronous Connection Oriented) kontinuierliche Paketübertragung
  - FEC (forward error correction), keine Sende-Wiederholung, 64 kbit/s duplex,
  - Point-to-Point, circuit switched

- **Data Link**
  - ACL (Asynchronous Connection Less) – Burstübertragung wenn Daten vorliegen,
  - Fast Acknowledge,
  - Point-to-Multipoint, bis zu 433.9 kbit/s symetrisch or 723.2/57.6 kbit/s asymetrisch, packet switched

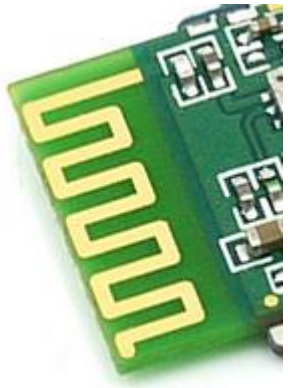
.

- **Topology**
  - piconet, Master mit mehreren Slaves
  - Überlappende piconets möglich (Stern), werden scatternet genannt

Klassen und Reichweite

Klasse	Max. Leistung (EIRP)	Max. Leistung	Reichweite allgemein	Reichweite im Freien
Klasse 1	100 mW	+20 dBm	ca. 100 m	ca. 100 m *
Klasse 2	2,5 mW	+4 dBm	ca. 10 m	ca. 50 m
Klasse 3	1 mW	0 dBm	ca. 1 m	ca. 10 m

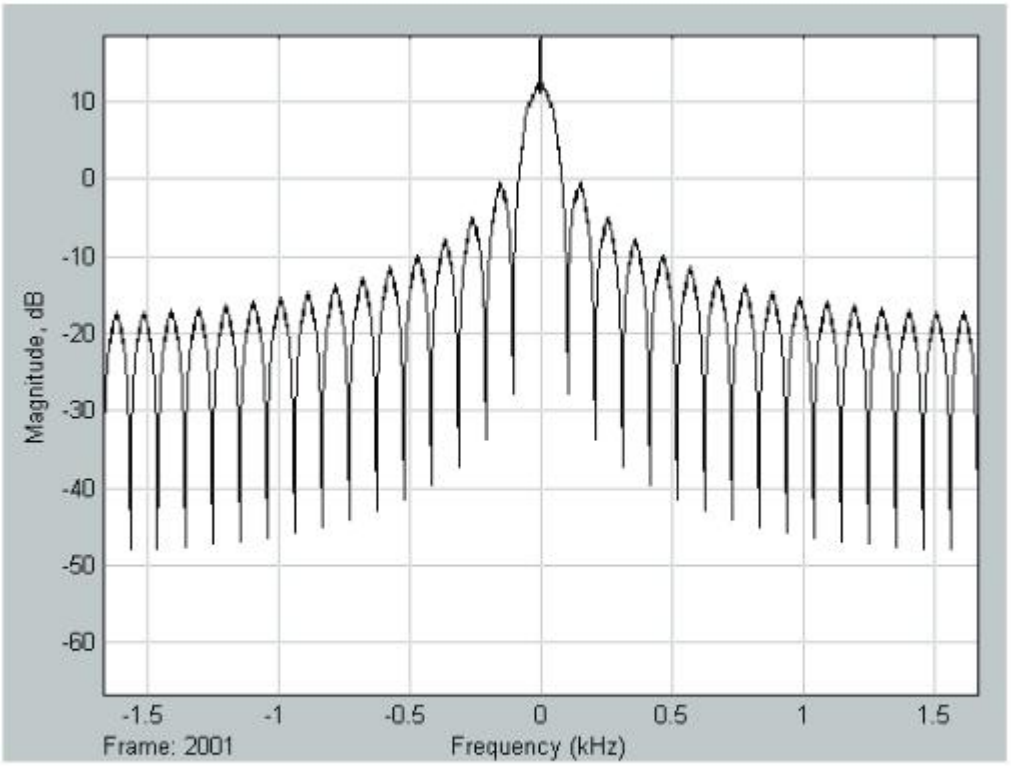
* Bei angepassten Stabantennen (˷λ/4) auch mehrere hundert Meter, wird in der heutigen Fernsteuerungstechnik bis zu 1km verwendet.



Verkürzte Antenne
Auf der Leiterplatte
(Wendelantenne)

λ/4-Stabantenne

GFSK (Gaussian Frequency Modulation)



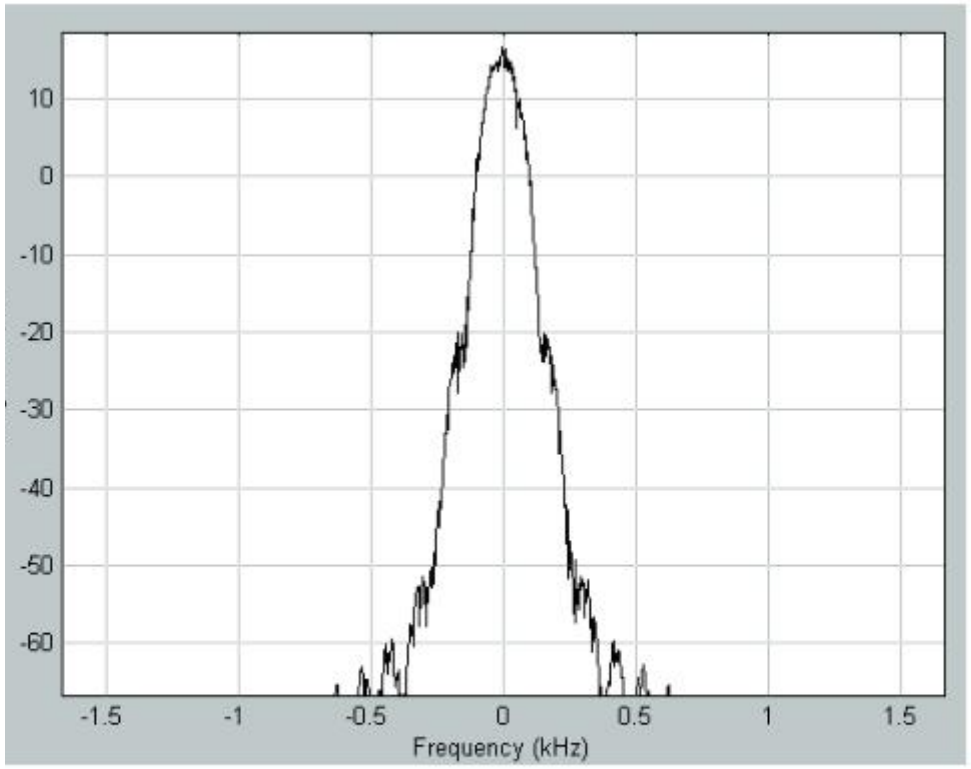
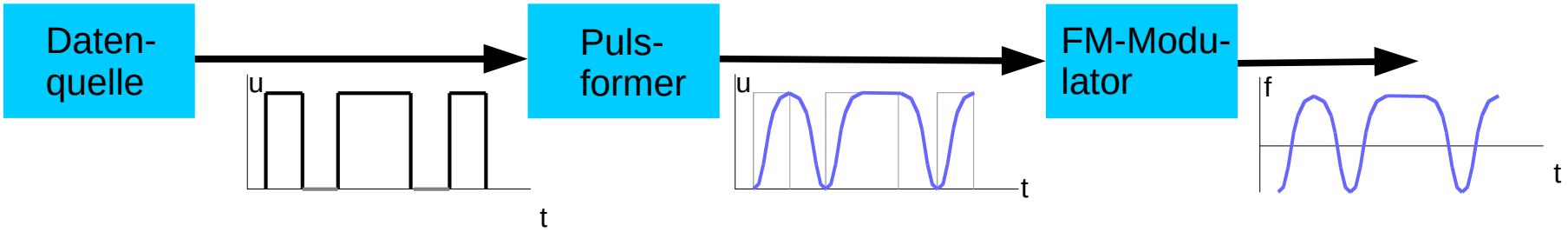


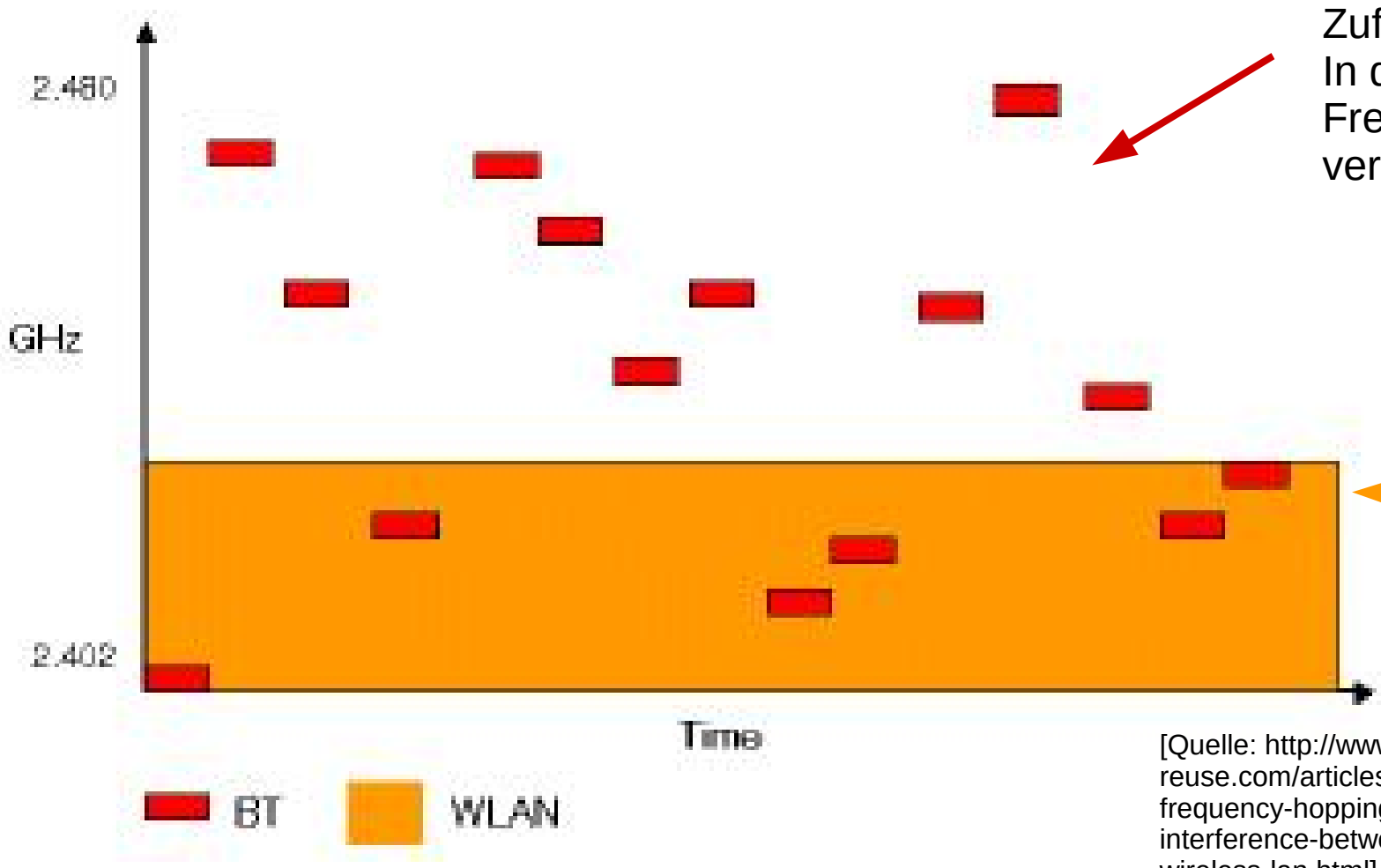
Fig. 2. Power spectrum of the rectangular non-shaped data sequence.

g. 12. Power spectrum of the Gaussian pulse shaped sequence.



[Quelle: http://www.radioeng.cz/fulltexts/2009/09_02_230_237.pdf]

FHSS (Frequency Hopping Spread Spectrum)



Zufallsmuster
In der
Frequenz-
verteilung

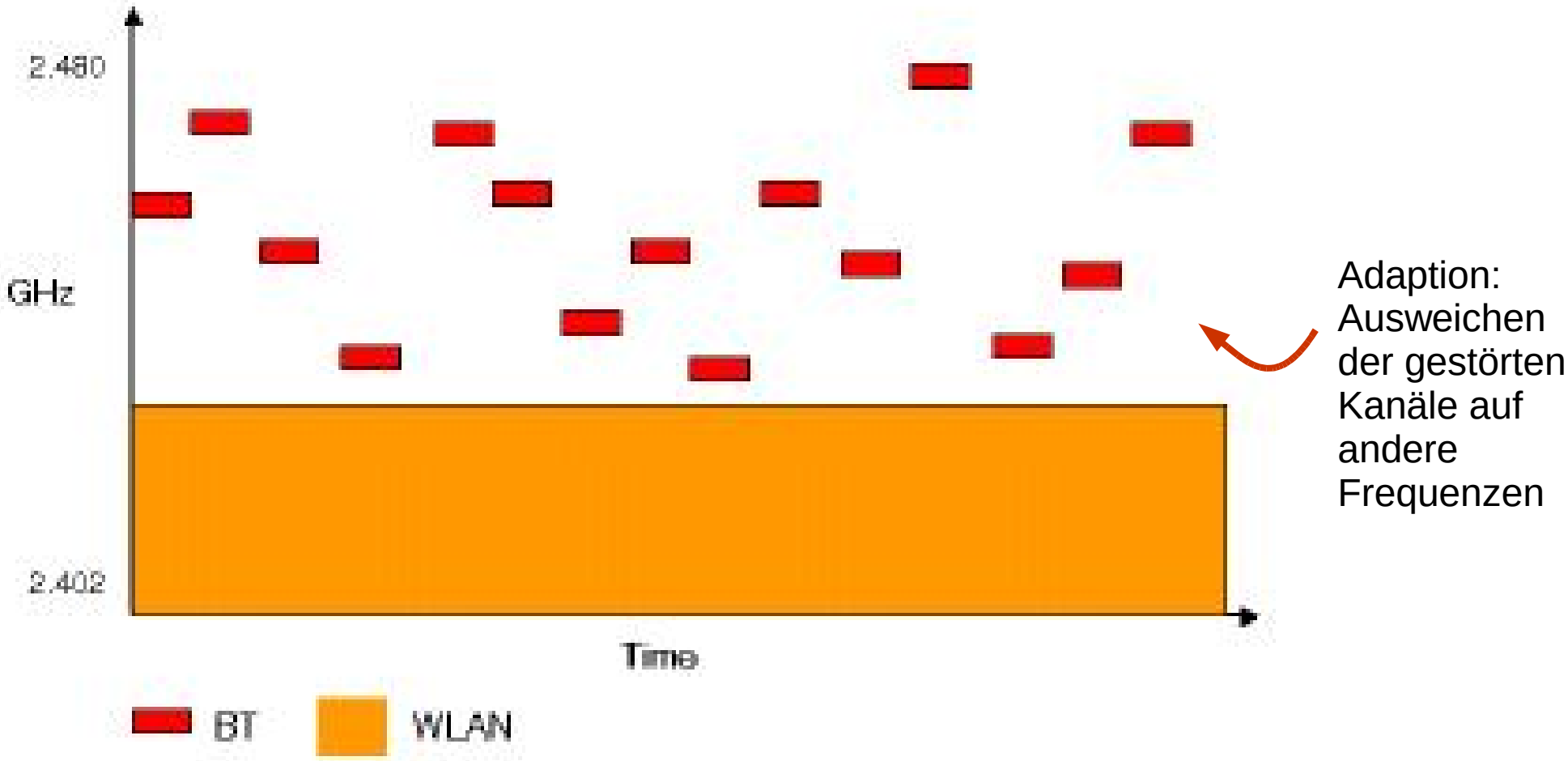
Störung

[Quelle: http://www.design-reuse.com/articles/5715/adaptive-frequency-hopping-for-reduced-interference-between-bluetooth-and-wireless-lan.html]

Die Zufallsfolge wird beeinflusst von Stationsidentifikationsnummer

Übertragung: 1 Paket pro Hop, 625µs zeitlicher Abstand

AFH (Adaptive Frequency Hopping)



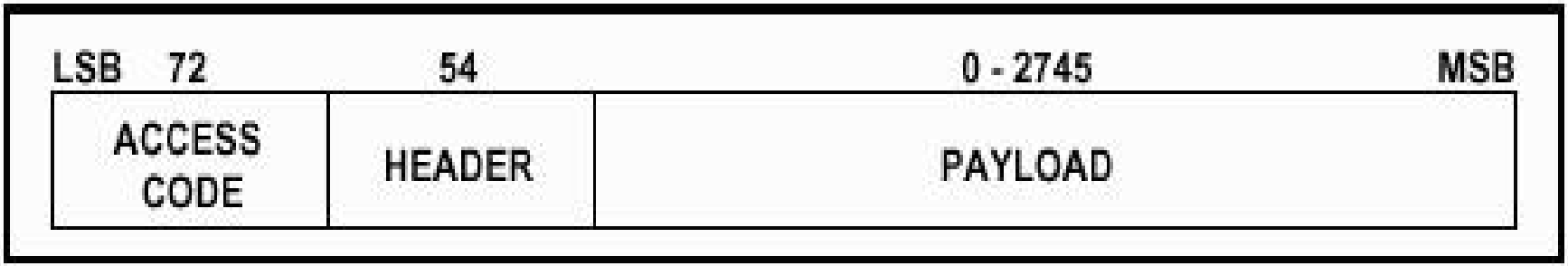
Adaption: Ausweichen der gestörten Kanäle auf andere Frequenzen

Bewertung jedes Kanals, wenn Kanal mehrfach gestört wurde, dann erfolgt Ausweichen

[Quelle: http://www.design-reuse.com/articles/5715/adaptive-frequency-hopping-for-reduced-interference-between-bluetooth-and-wireless-lan.html]

Bluetooth: Generelle Paketstruktur (Frame)

ca. 16 Paketarten !



3 Typen
Access Code:
- Channel Access Code
- Device Access Code
- Inqiry Access Code

Paketbestätigung ACK,
Paketnummer,
Anforderung Paketwiederholung
Flow Control
Slave-Adresse
Header Error Check

Verschiedene interne Strukturen, abhängig von Datencharacteristik (Sprache, Daten,....)

[Quelle: www.palowireless.com]

Authentifizierung / Encryption

Authentifizierung des Slaves:

- Sicherstellen, dass der richtige Kommunikationspartner nach dem Pairing die Daten sendet/empfängt
- Grundlage für Verschlüsselung
- Sender schickt 128bit Challenge
- Empfänger bearbeitet diesen Wert mit 48bit Chip-Adresse und geheimem Link-Key,
  der bei der Initialisierung mit der PIN erzeugt wird
- Die 32 höchsten Bits werden zurückgesendet
- Der Sender kontrolliert das Ergebnis

Verschlüsselung:

- Verschlüsselung des Dateninhalts
- Schlüsselerzeugung mit 128b SAFER+ Verfahren
- Verschlüsselung mit 8-128bit symetrischen Schlüssel
- Einige Bits des Schlüssels können öffentlich sein
  (*Erfüllung staatlicher Auflagen !)*

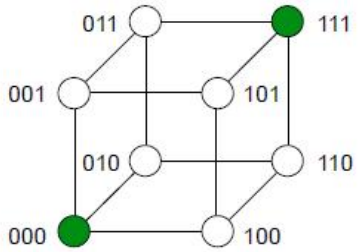
FEC (Forward Error Correction)

Beispiel – Speichern von 1 Bit Information

Speicherzelle 1

Beim Lesen der Speicherzelle kann nicht erkannt werden, ob irgendwann ein Fehler passiert ist

Im Beispiel



$d_{min} = 3$

- Fehlererkennung:
  - Alle 2-Bit Fehler
- Fehlerkorrektur
  - Alle 1-Bit Fehler
- Aber:
  - Mechanismus zur Fehlererkennung und zur Fehlerkorrektur kann nicht gleichzeitig genutzt werden

Fehlererkennende Kodierung

Information	Kodierung
0	00
1	11

1 Bit kippt 01

1-Bit Fehler wird immer erkannt, aber korrekter Speicherinhalt kann nicht bestimmt werden

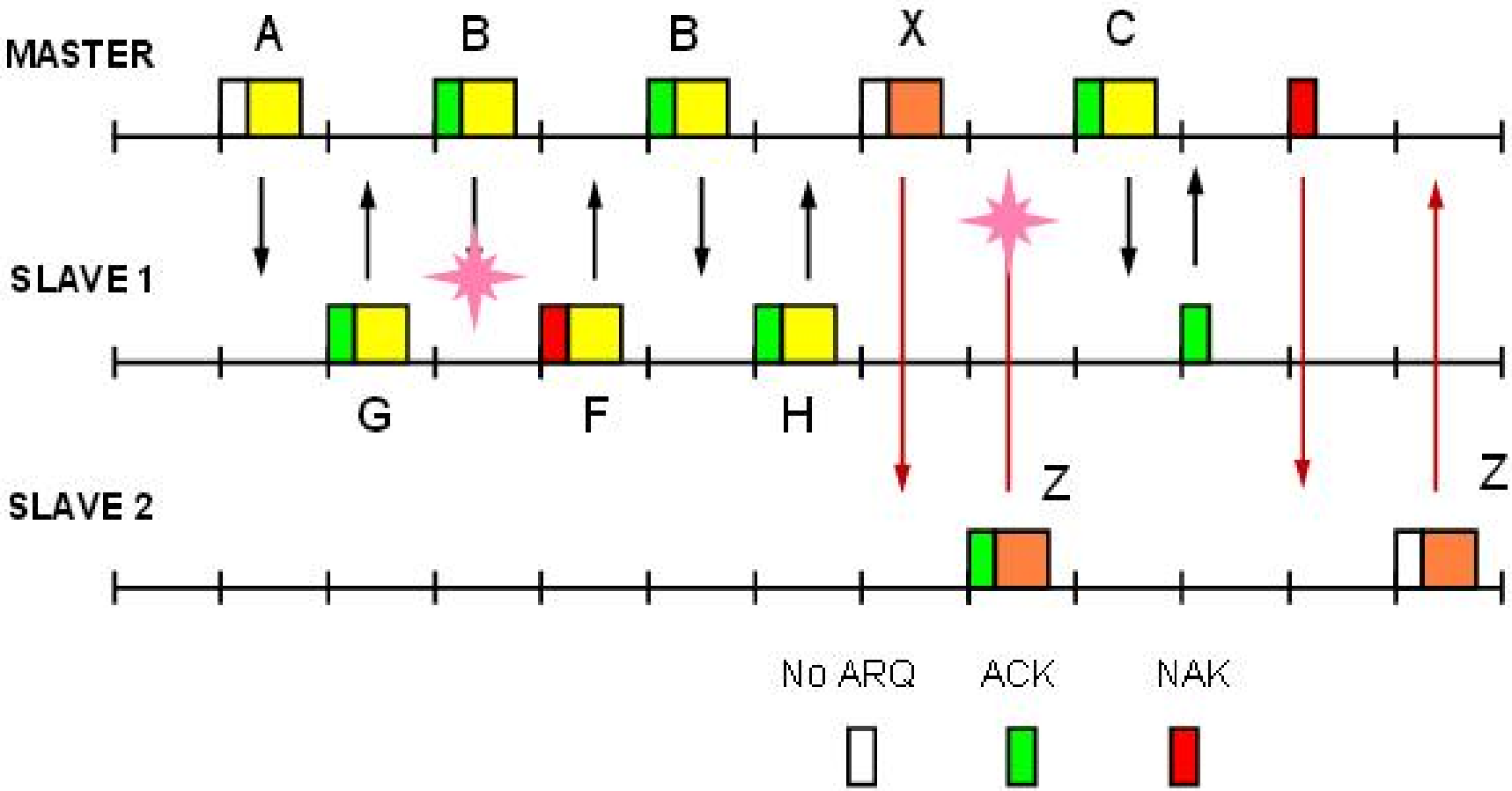
Fehlerkorrigierende Kodierung

Information	Kodierung
0	000
1	111

1 Bit kippt 010

1-Bit Fehler wird immer erkannt, korrekter Speicherinhalt kann eindeutig bestimmt werden

ARQ (Automatic Retransmission Request)

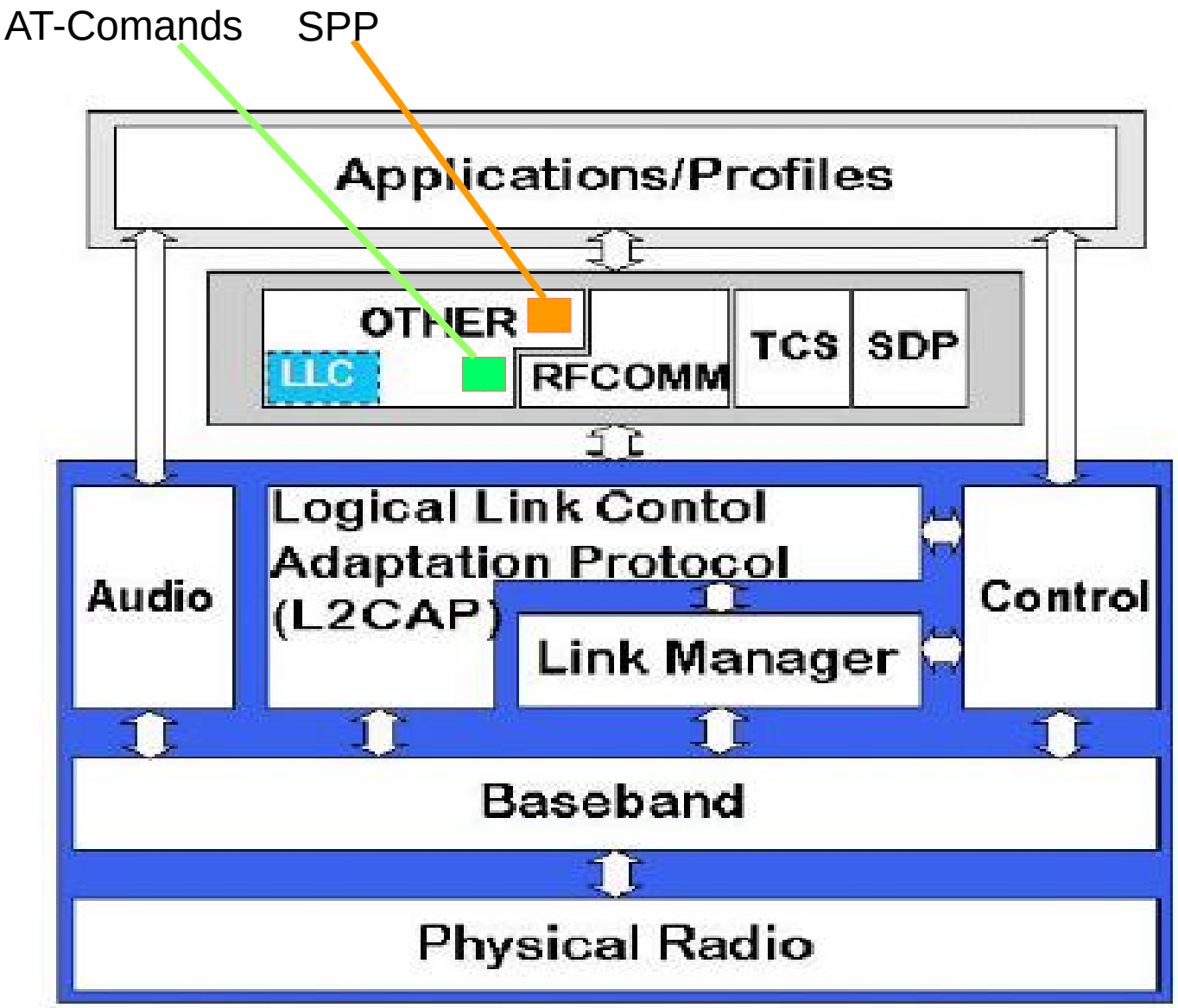


Bluetooth Protokolle.....beliebig kompliziert !

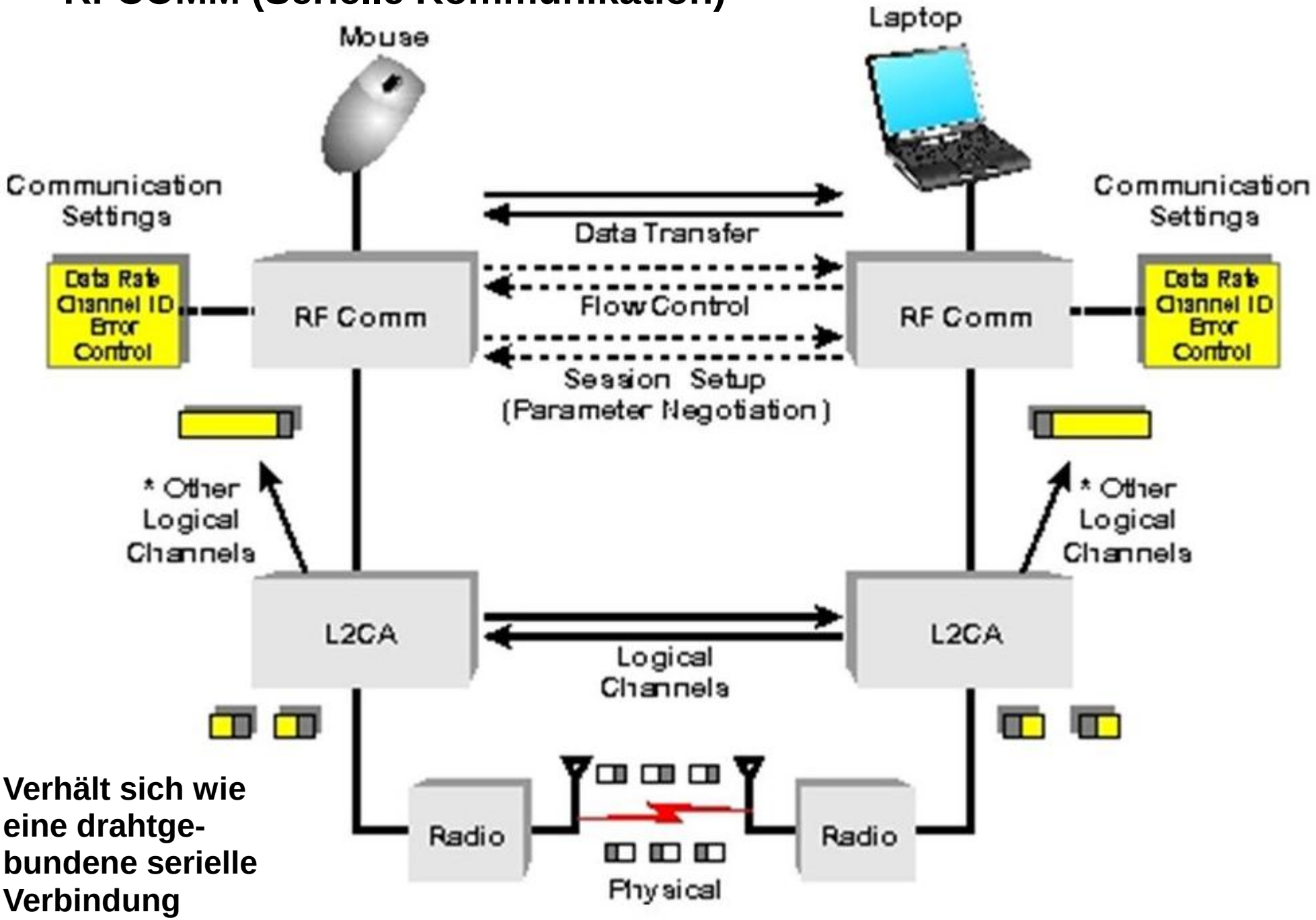
Akronym	Bluetooth-Profile	Funktion
A2DP	advanced audio distribution profile	Übertragung von Audiodaten
AVRCP	audio video remote control profile	Audio/Video-Fernbedienung
BIP	basic imaging profile	Übertragung von Bilddaten
BPP	basic printing profile	Druckfunktion
CIP	common ISDN access profile	ISDN-CAPI-Schnittstelle
CTP	cordless telephone profile	Schnurlose Telefonie
DNP	dial-up networking profile	Einwahlverbindung
DUNP	dial-up networking profile	Einwahlverbindung für Internet
ESDP	extended service discovery profile	Erweiterte Diensteerkennung
FaxP	fax profile	Fax-Funktion
FTP	file transfer profile	Übertragung von Dateien
GAP	generic access profile	Zugriffssteuerung mit Authentifizierung
GAVDP	generic AV distribution profile	Übertragung von Audio/Videodaten
GOEP	generic object exchange profile	Objektaustausch
HCRP	hardcopy cable replacement profile	Drucken
HDP	health device profile	Medizindaten
HID	human interface device profile	Schnittstelle zum Menschen
HFR	hands free profile	Übertr. zwischen Handy und Freisprecheinr.
HSP	headset profile	Schnurloses Headset
IntP	intercom profile	Sprechfunk
LAP	LAN access profile	PPP-Netzverbindung
OPP	object push profile	Übertragung von Terminen und Adressen
PAN	personal area networking profile	Netzwerkverbindung
SAP	SIM access profile	SIM-Karten-Zugriff
SDAP	service discovery application profile	Auffindung von Geräten
SP	synchronisation profile	Dateisynchronisation
SPP	serial port profile	Serielle Datenübertragung

Quelle: www.itwissen.info

Bluetooth Layer Struktur

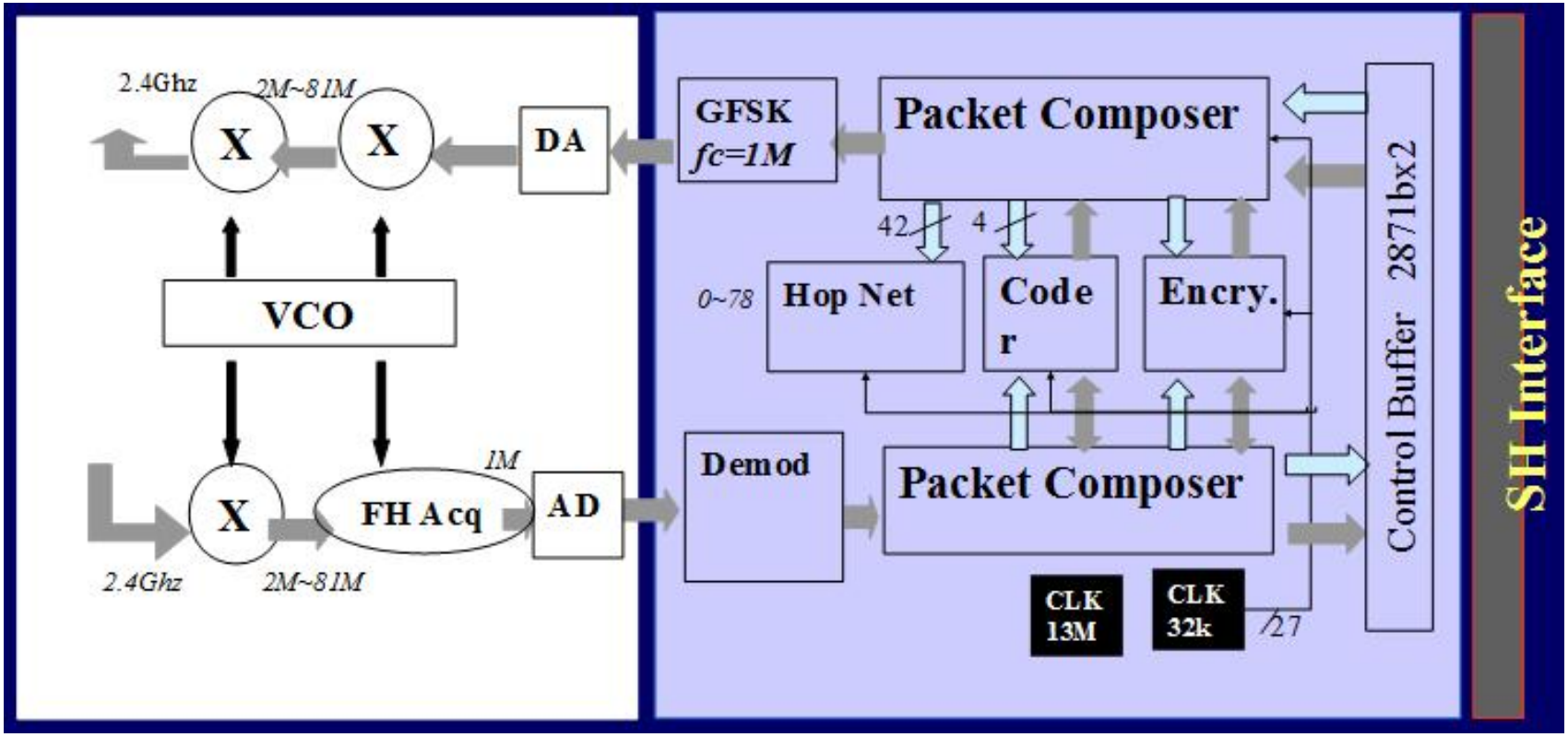


RFCOMM (Serielle Kommunikation)



Verhält sich wie eine drahtge-bundene serielle Verbindung

Was ist in einem BT-Chip drin ?



HF-Technik Digital-Technik