WIRELESS TECHNOLOGY FORUM

Certified Wireless Network Professionals CWNP

WirelessHART®

WirelessHART

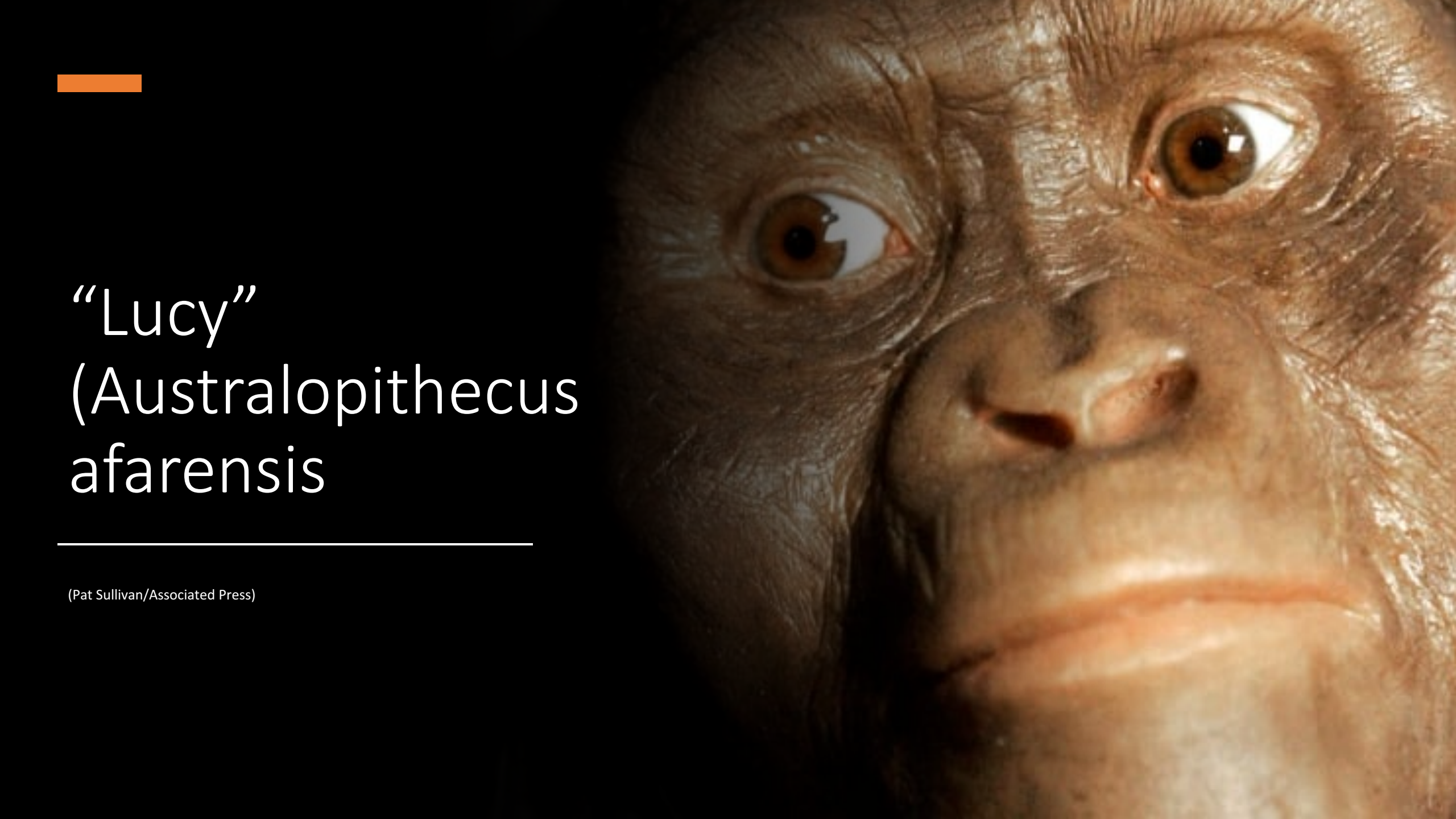
An Overview

@troymart

#WTF20

Lucy

“Lucy” (Australopithecus afarensis



(Pat Sullivan/Associated Press)

Limitless

Who Am I?

Troy Martin P.Eng.

- 20+ years in IT
- Professional Services
- Consulting
- Training

@troymart

Topics

- **Highlights**
- HART history
- Protocol
- Design
- Security

WirelessHART®

WirelessHART Highlights

- Based on IEEE 802.15.4-2006
  - 2.4 GHz ISM DSS (2400 – 2483.5 MHz)
- Low power (battery or scavenger power)
- O-QPSK Modulation
- Secure 128-bit AES based encryption
- Supports mesh and star topologies
- Self-configuring, self-optimizing, and self-healing
- IEC 62591
- Defined by HART v7, maintained by FieldComm Group (fieldcommgroup.org)

IEEE

HART COMMUNICATION PROTOCOL

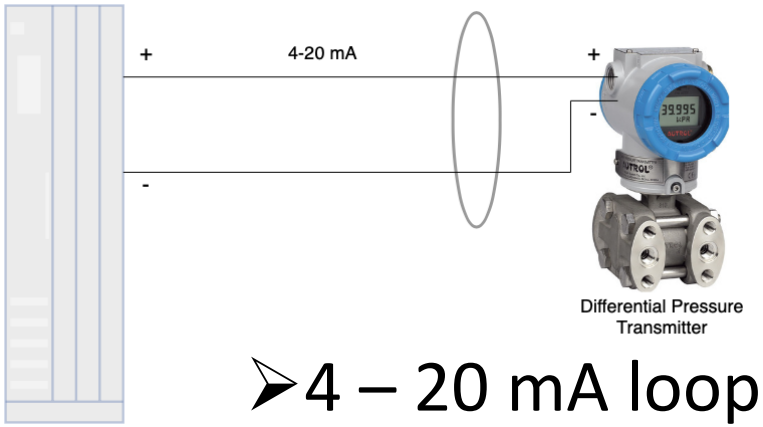
IEC

Topics

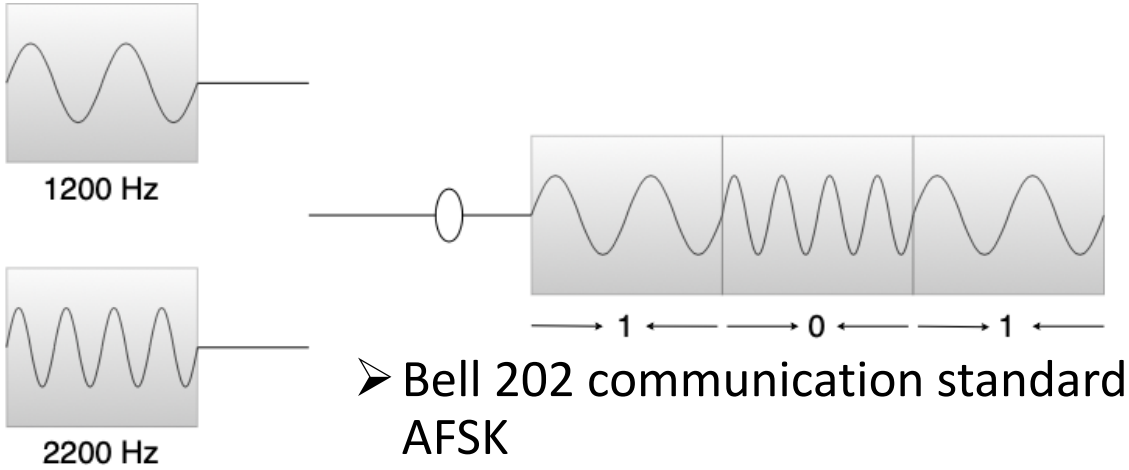
- Highlights
- **HART history**
- Protocol
- Design
- Security

WirelessHART®

HART ➢Highway Addressable Remote Transducer

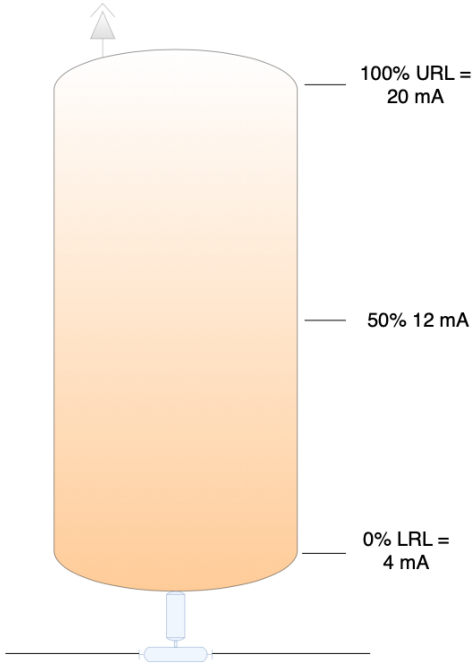


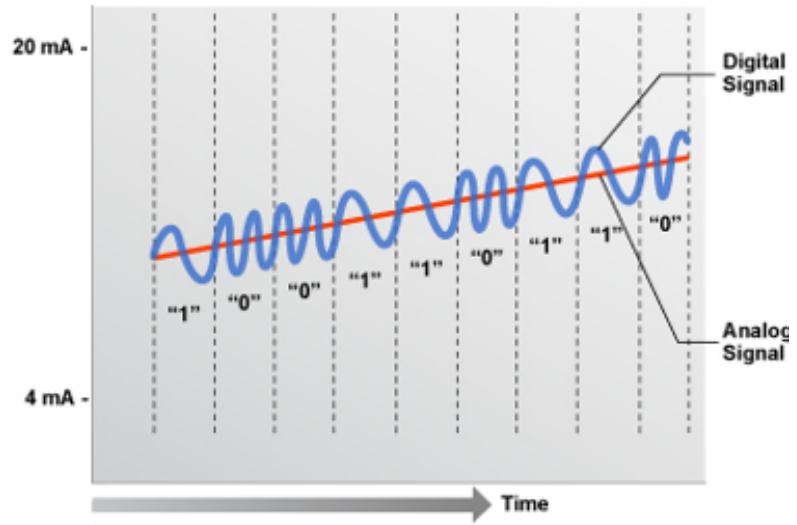
➢4 – 20 mA loop



➢Bell 202 communication standard – uses AFSK

➢A/D conversion with 2^{16} or 65,535 discrete increments





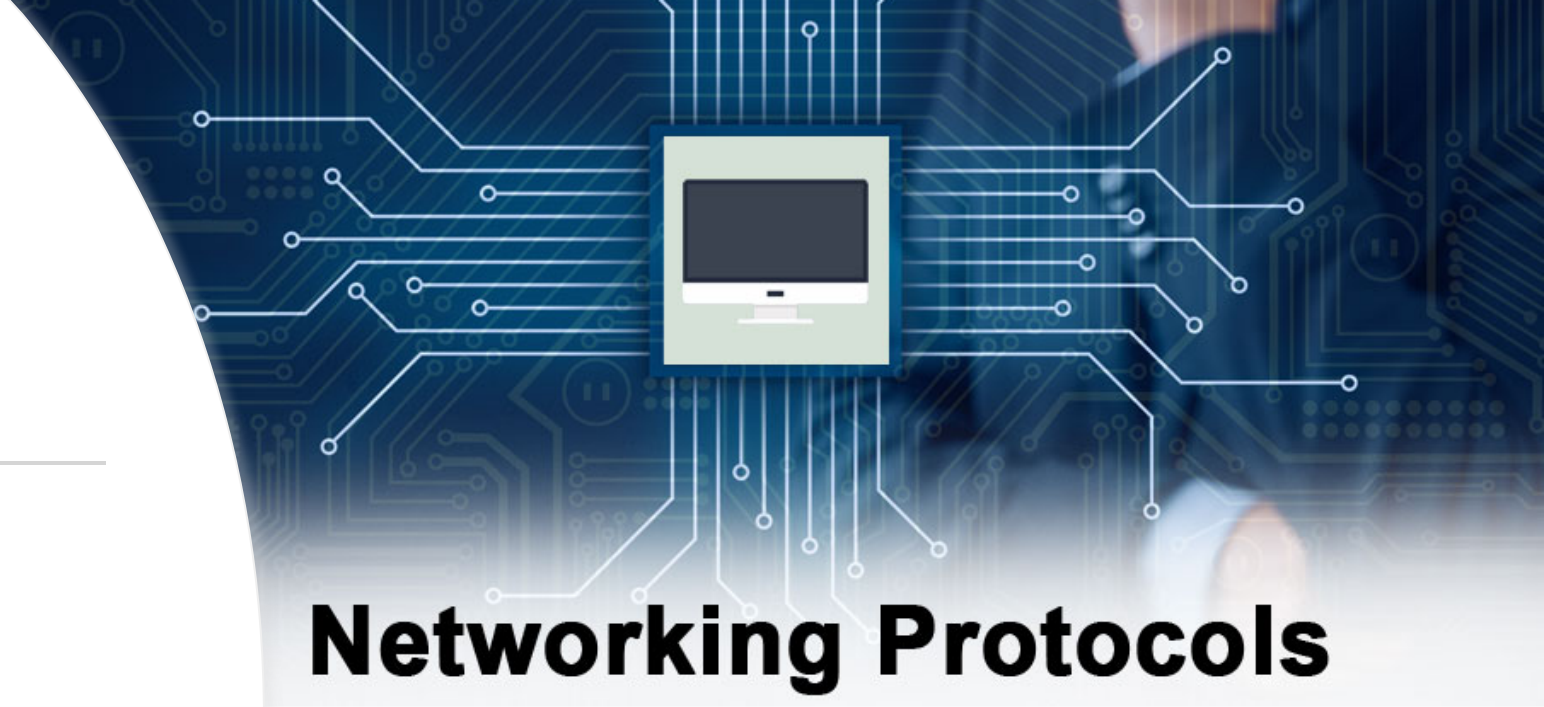
Note: Drawing not to scale

➢Superimposed digital-signal over analog-carrier

Source: HART Technology Detail: HART Communication Protocol (https://fieldcommgroup.org/technologies/hart/hart-technology-detail)

Topics

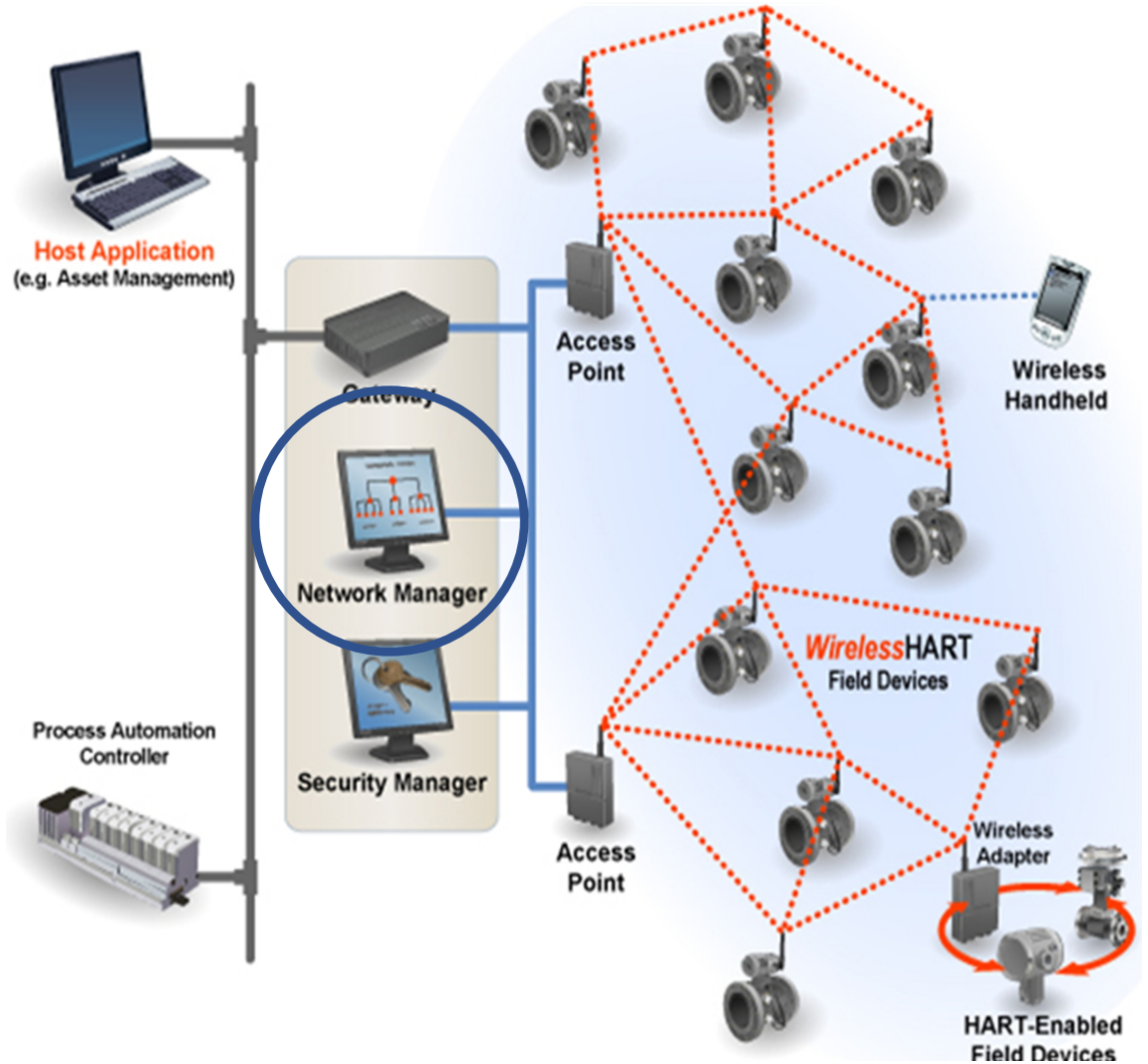
- Highlights
- HART history
- **Protocol**
- Design
- Security



WirelessHART®

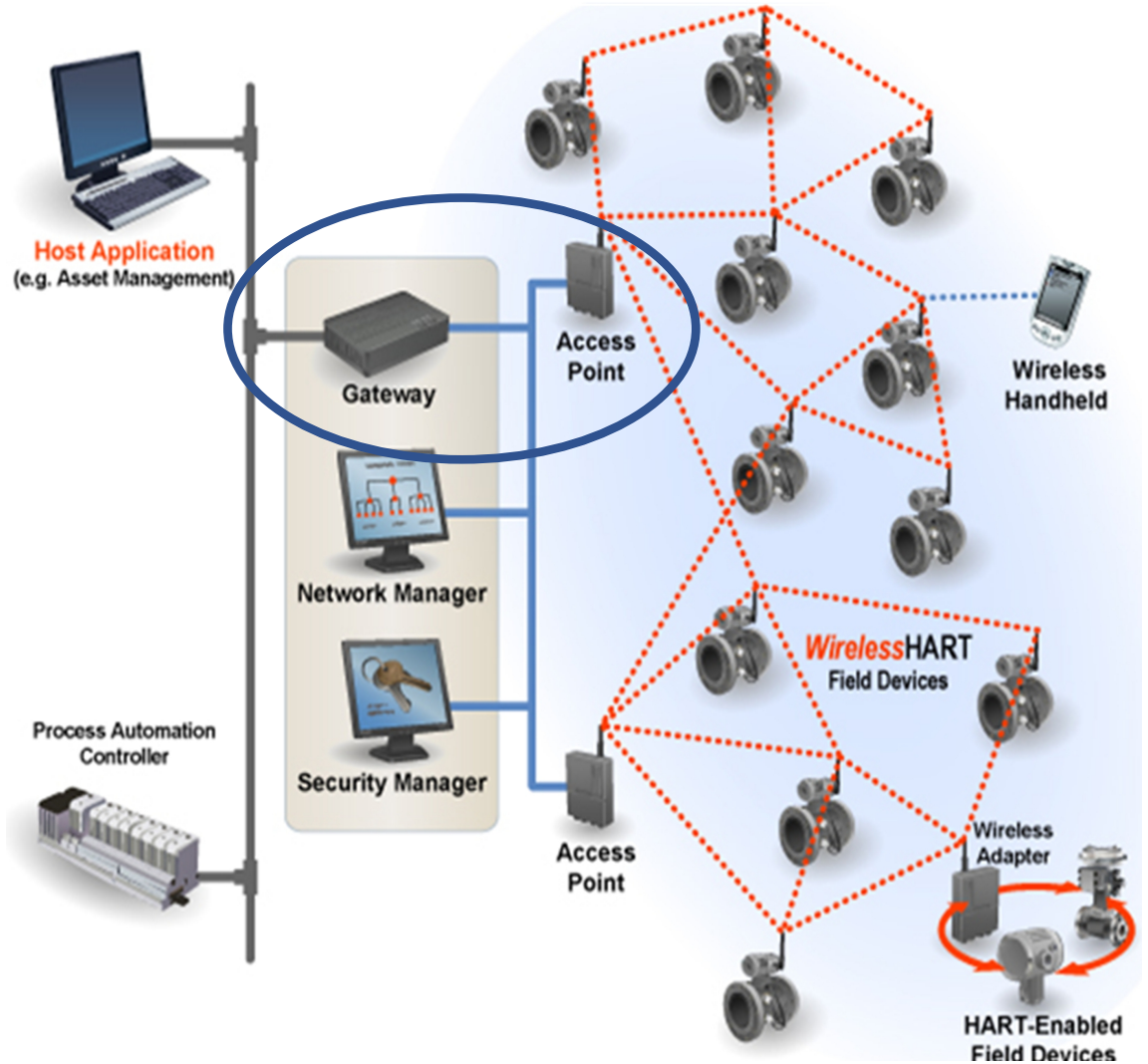
5 WirelessHART Components

- **Network Management**
- Gateway / Access Points
- Wireless Field Devices
- WirelessHART Adapters
- Wireless Handhelds



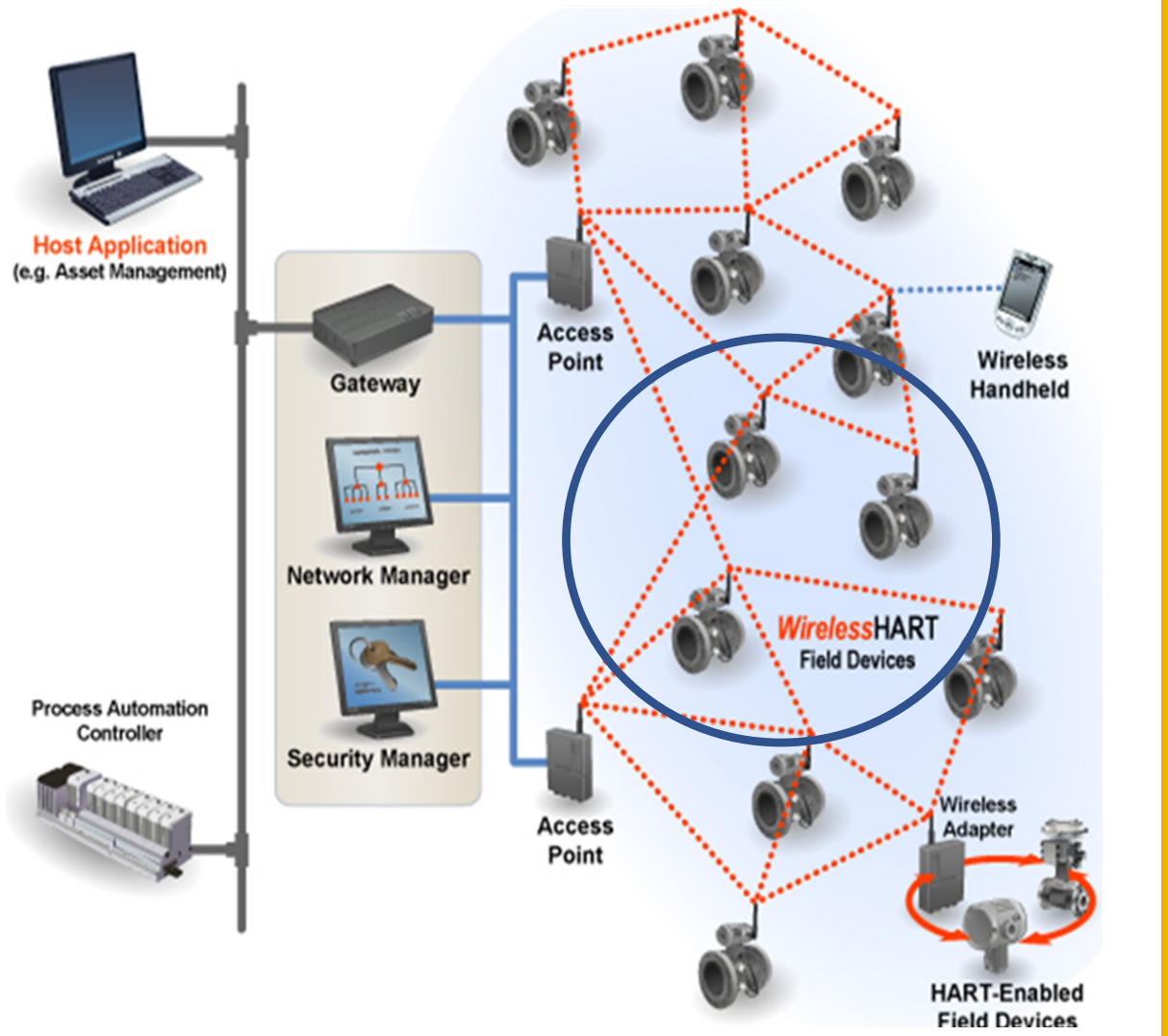
5 WirelessHART Components

- Network Management
- **Gateway / Access Points**
- Wireless Field Devices
- WirelessHART Adapters
- Wireless Handhelds



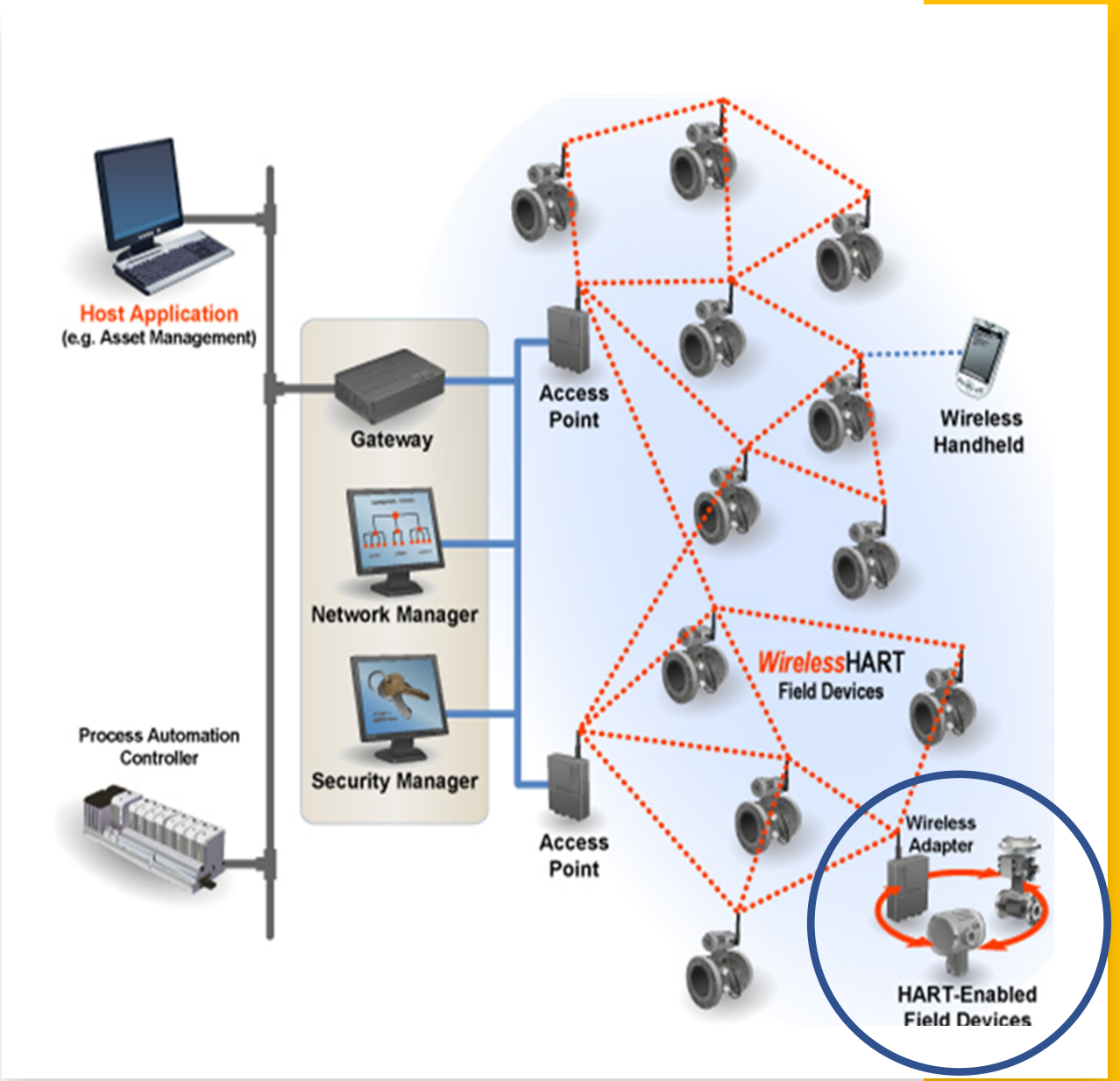
5 WirelessHART Components

- Network Management
- Gateway / Access Points
- **Wireless Field Devices**
- WirelessHART Adapters
- Wireless Handhelds



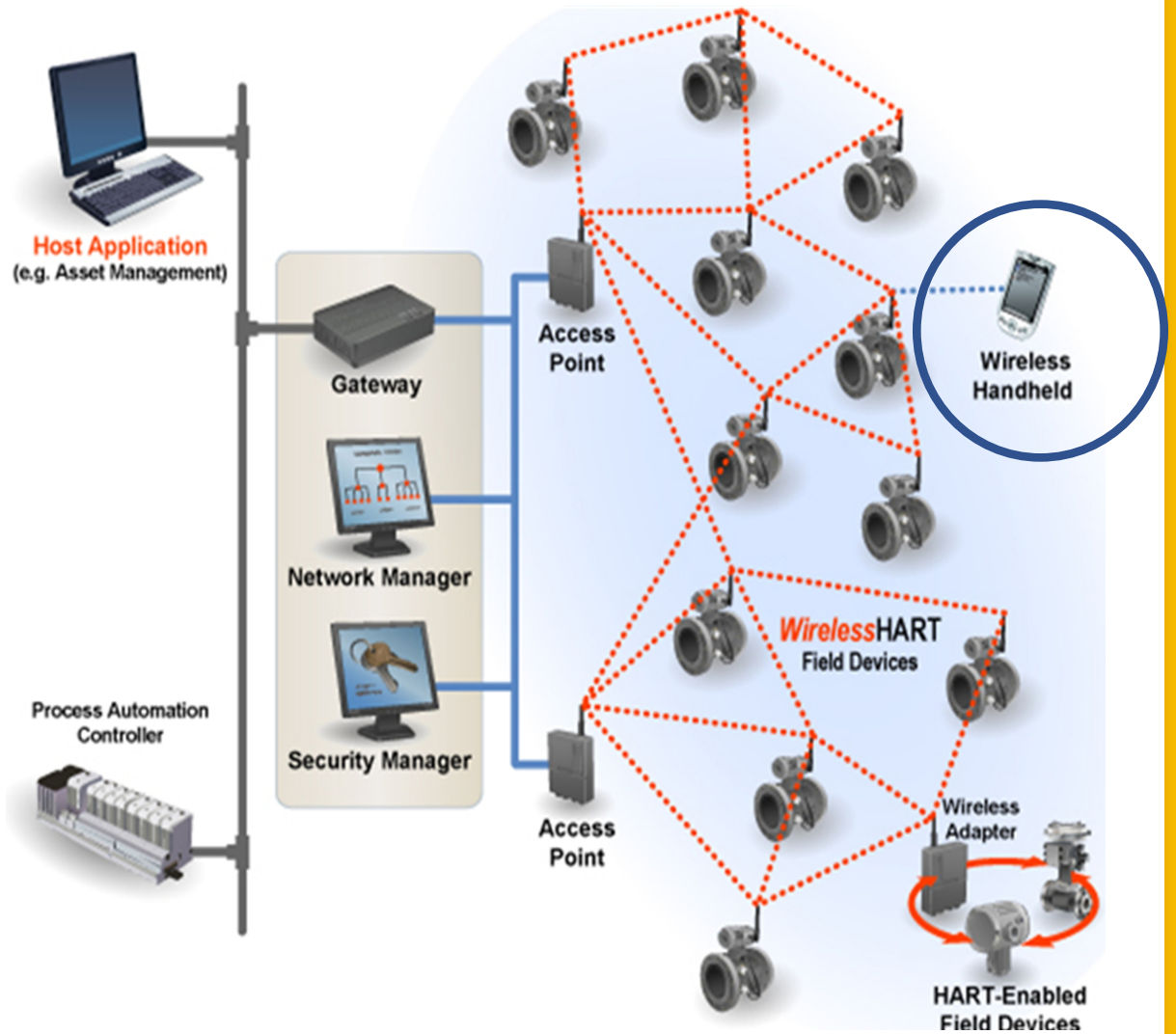
5 WirelessHART Components

- Network Management
- Gateway / Access Points
- Wireless Field Devices
- **WirelessHART Adapters**
- Wireless Handhelds



5 WirelessHART Components

- Network Management
- Gateway / Access Points
- Wireless Field Devices
- WirelessHART Adapters
- **Wireless Handhelds**



Purdue Model

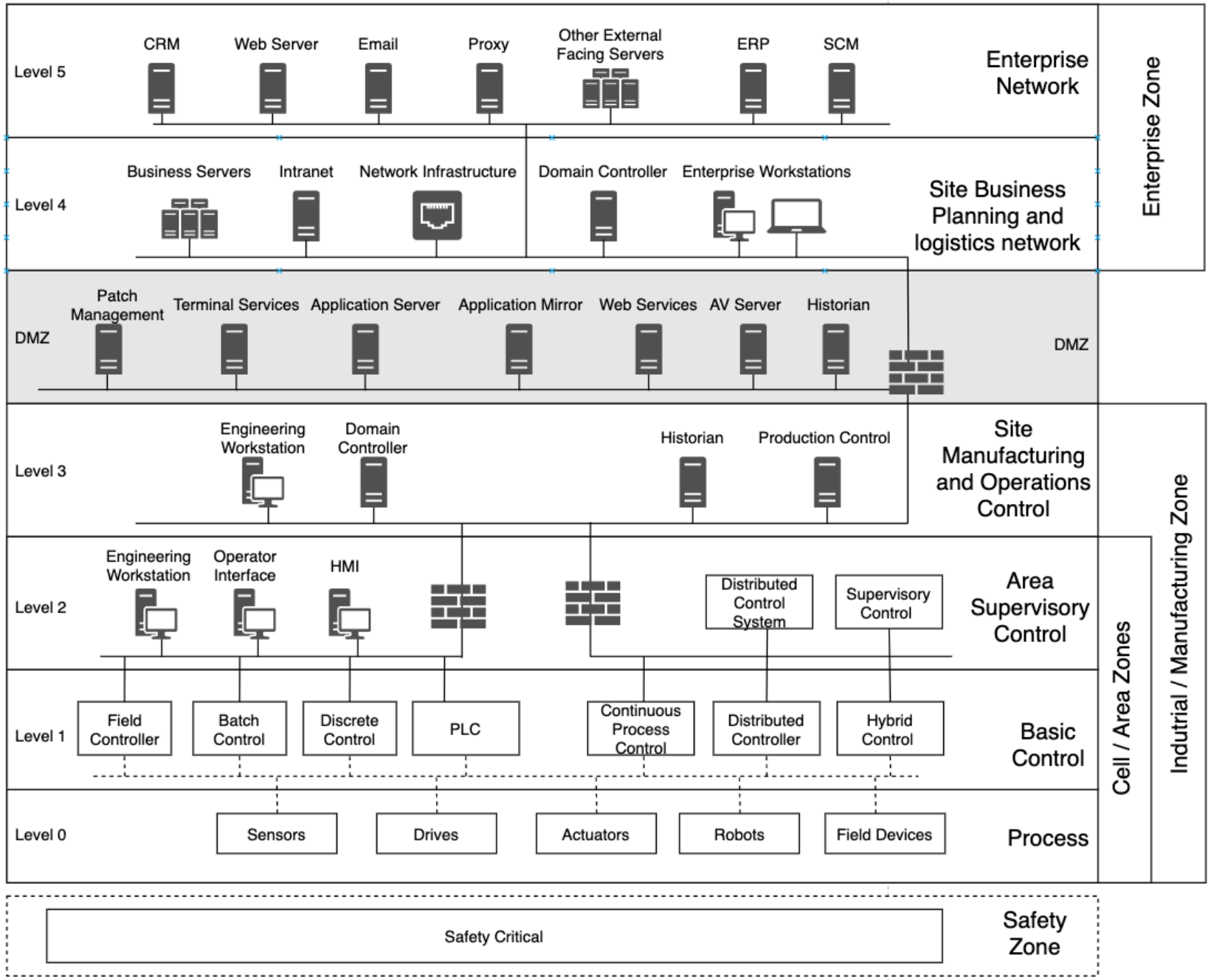
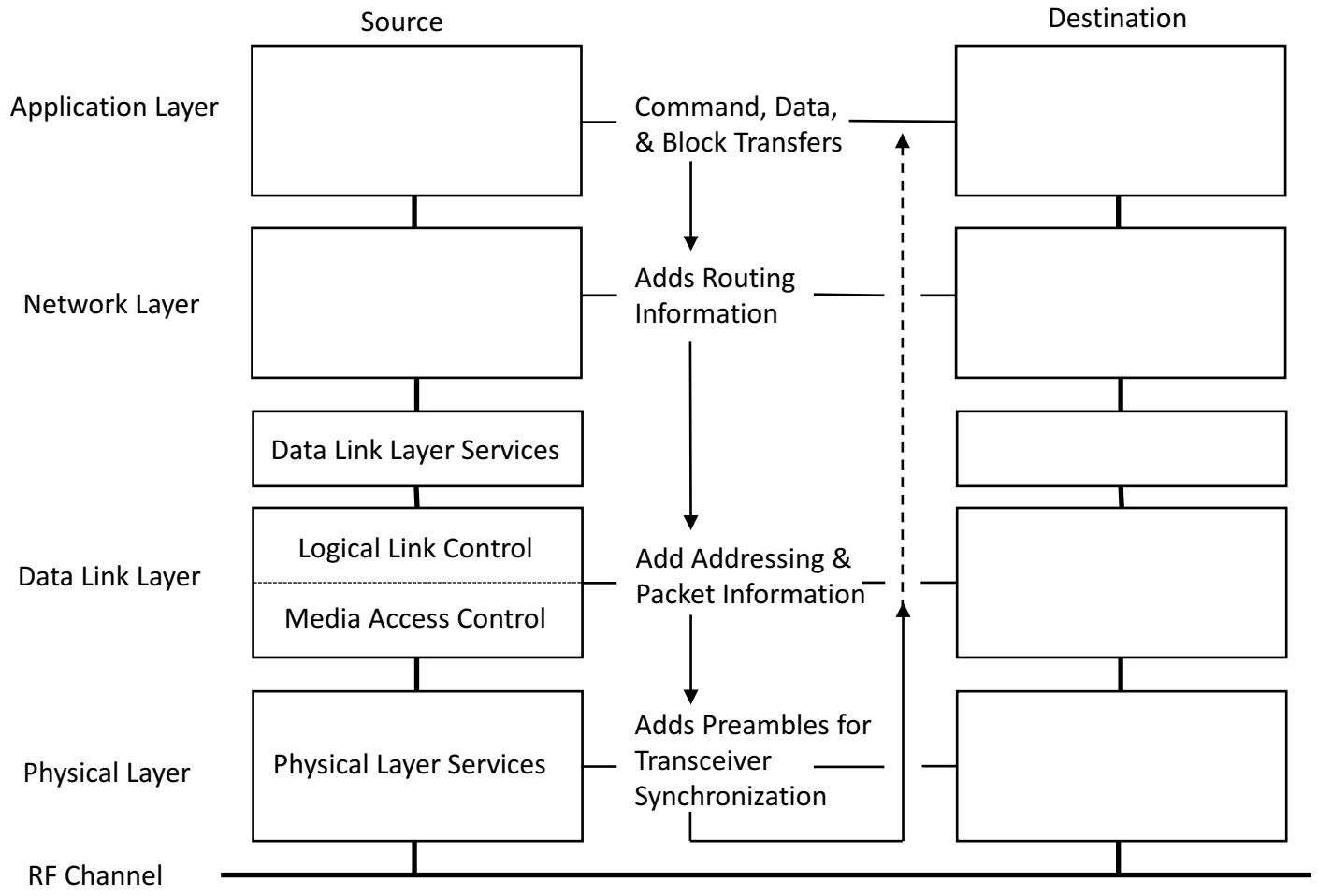


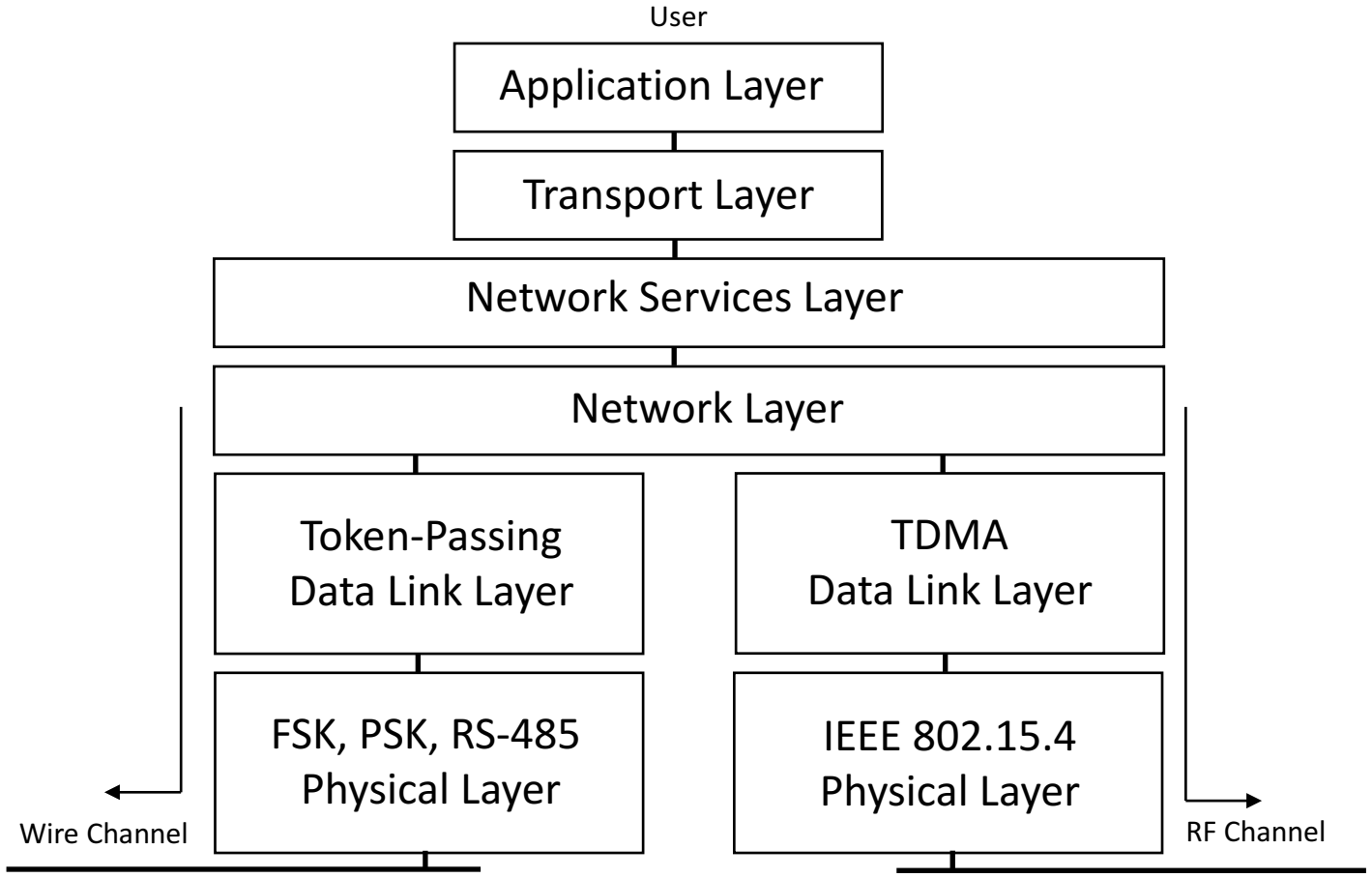
Image source: CWIIP Study Guide

Data-Link Layer Scope



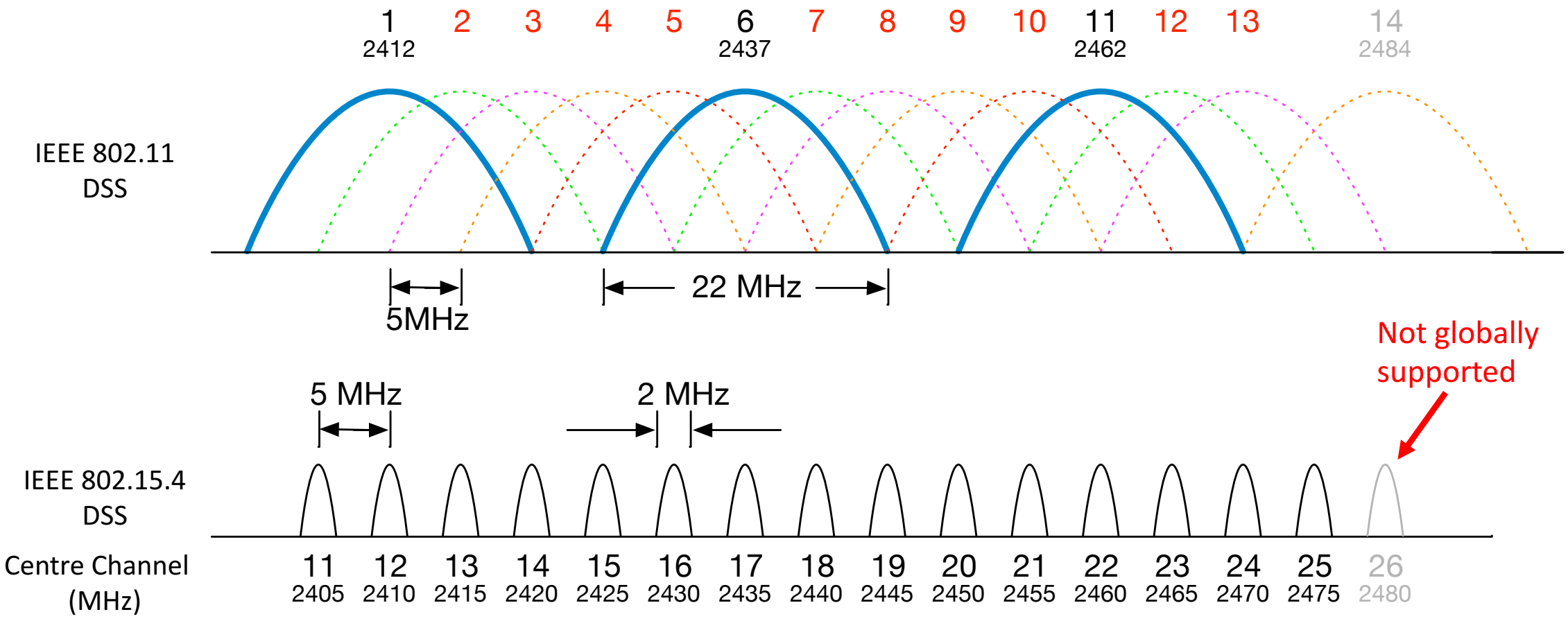
Source: D. Chen et al., WirelessHART: Real-Time Mesh Network for Industrial Automation Figure 3.1

Network Layer Scope



Source: D. Chen et al., WirelessHART: Real-Time Mesh Network for Industrial Automation Figure 4.1

Operates in the 2.4 GHz ISM band



Fc = 2405 + 5 (k – 11) in MHz, for k = 11, 12, …, 26

WirelessHART Modifications

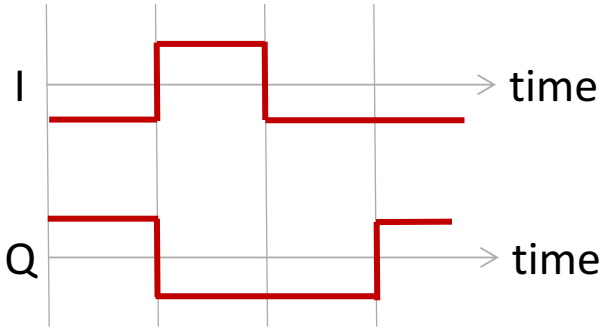
- 2.4 GHz PHY (IEEE)
  - **250 kb/s** (4 bits/symbol, 62.5 kBaud/s)
  - Data modulation is 16-ary **OQPSK** modulation
    - 16 symbols are ~orthogonal set of 32-chip PN codes
  - Chip modulation is MSK at 2.0 Mchips/s

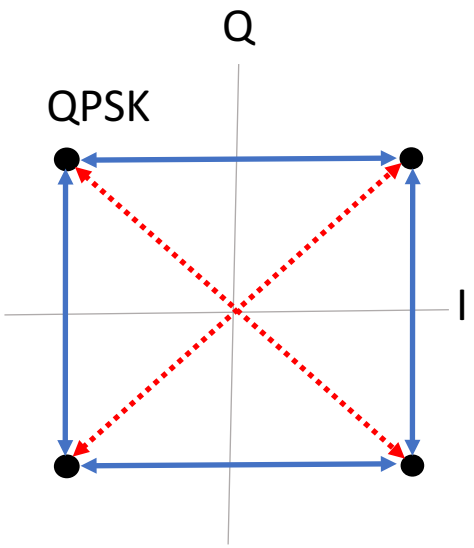
- WirelessHART modification
  - Max Layer 2 payload is 127 bytes (DLPDU)
  - Multichannel TDMA MAC
  - Slot times fixed at 10ms
  - All 15 channels could be used simultaneously
  - Same channel is NOT used consecutively

Data symbol (decimal)	Data symbol (binary) ($b_0\ b_1\ b_2\ b_3$)	Chip values ($c_0\ c_1 \cdots c_{14}\ c_{15}$)
0	0000	00111110001001 01
1	1000	01001111100010 01
2	0100	01010011111000 10
3	1100	10010100111110 00
4	0010	00100101001111 10
5	1010	10001001010011 11
6	0110	11100010010100 11
7	1110	11111000100101 00
8	0001	01101011011100 00
9	1001	00011010110111 00
10	0101	00000110101101 11
11	1101	11000001101011 01
12	0011	01110000011010 11
13	1011	11011100000110 10
14	0111	10110111000001 10
15	1111	10101101110000 01

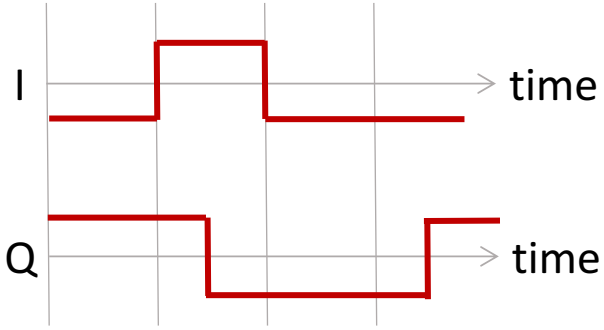
O-QPSK

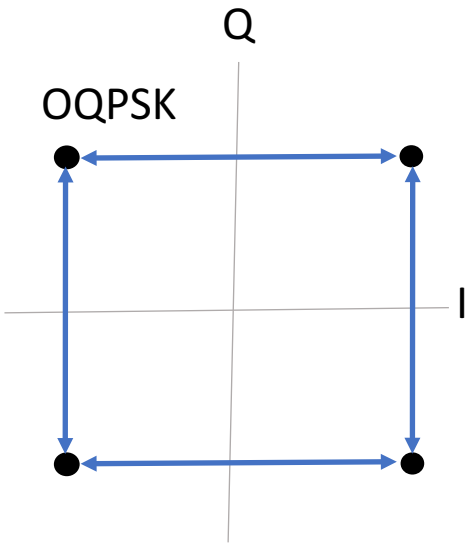
Symbol Boundaries





Symbol Boundaries





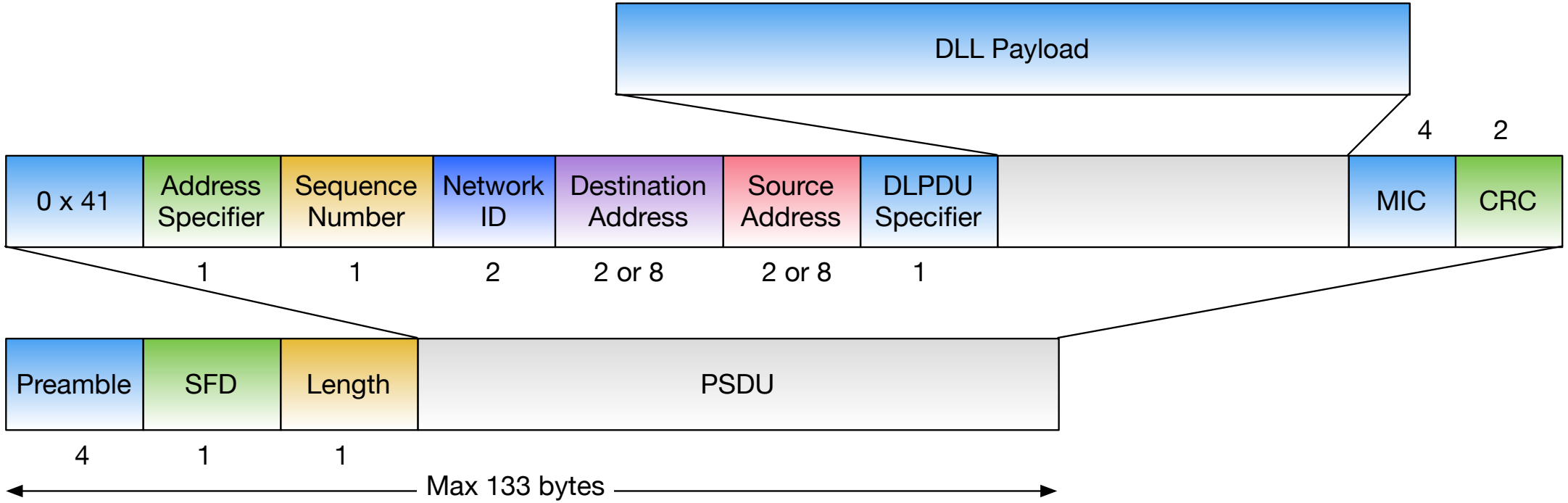
Offset–QPSK – attempts to prevent signal transitions through ’zero’ by reducing total variation in waveform

Constant switching through ‘zero’ at high rates can cause spectral regrowth at power amplifier output

Offset-QPSK – reduces peak to average power

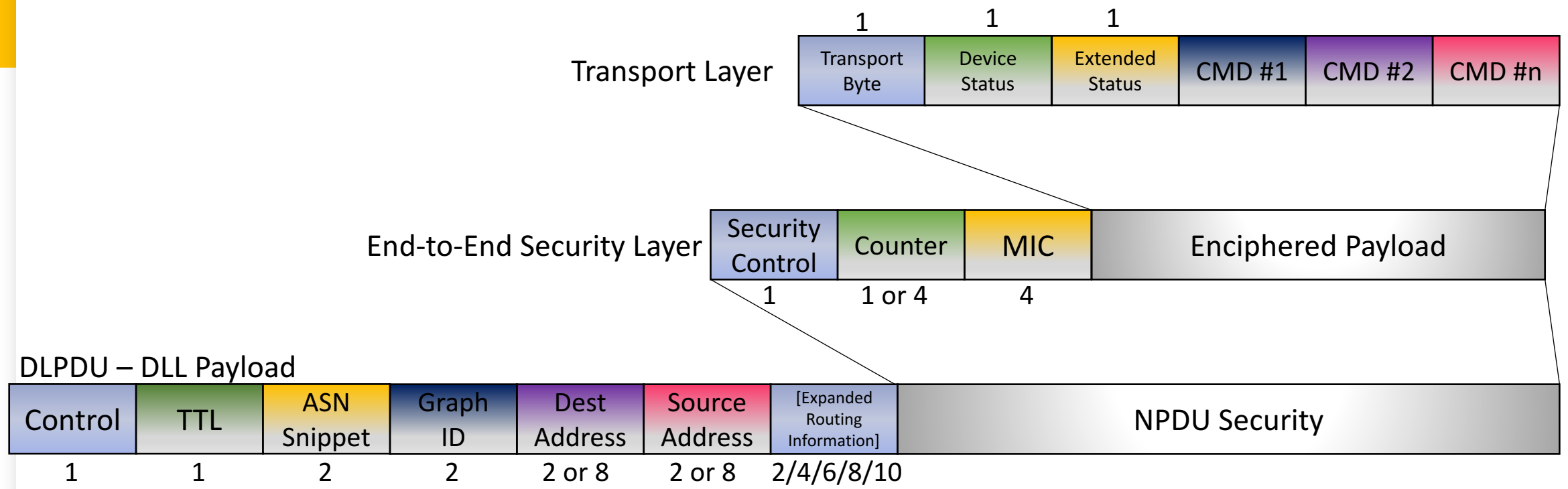
Types of Datalink PDU (DLPDU) Frames

- Advertisement (Periodic)
- Keep-Alive (Periodic)
- Data
- Acknowledgement
- Disconnect



Datalink Packet Data Unit (DLPDU)

- 4 types of MAC frame
  - Beacon frame
  - Data frame
  - Acknowledgement frame
  - MAC command frame
- PHY Packet Fields
  - Preamble (32 bits) – synchronization
  - Start of Frame Delimiter (8 bits)
  - PSDU length (8 bits)
  - PSDU (0 to 1016 bits) – Data field

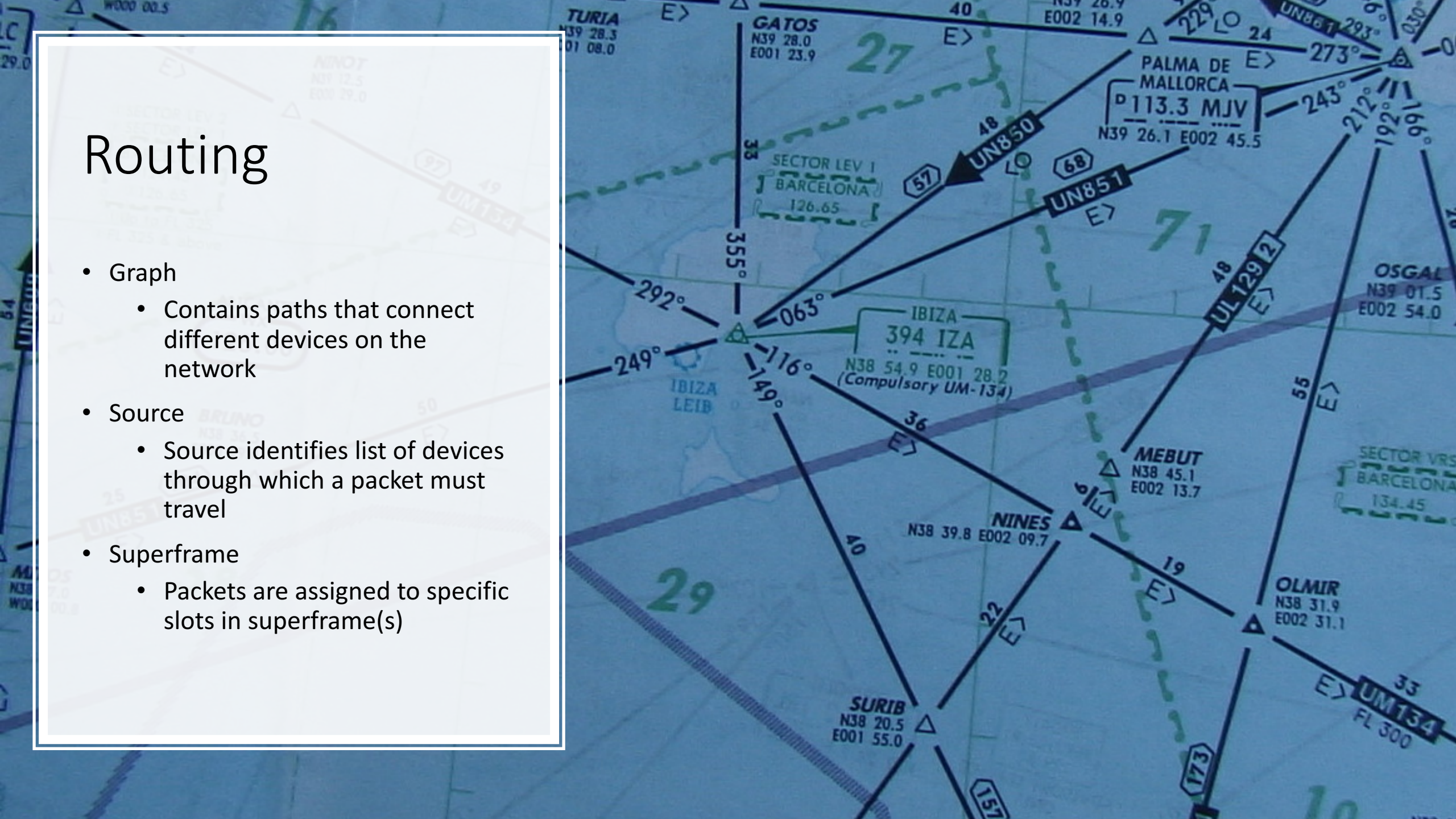


Network Packet Data Unit (NPDU)

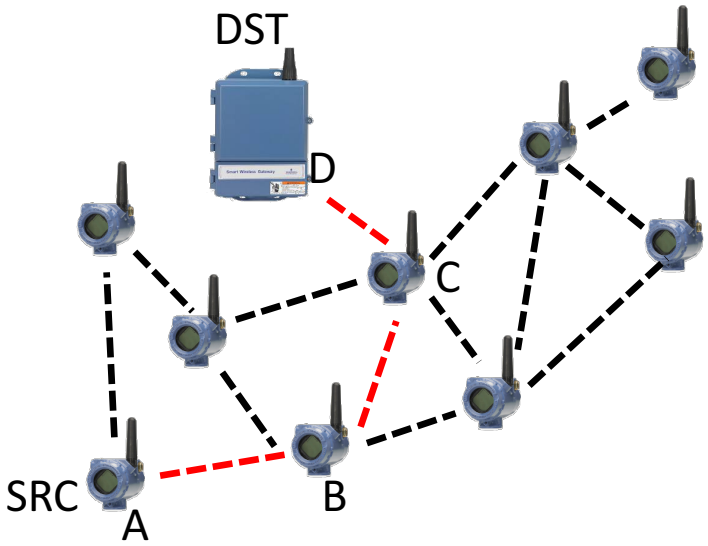
- Network & Transport Layer
  - Control defines remaining fields
  - Address use Nickname (2) or EUI-64 (8)
  - TTL decremented each hop until reaching 0, then discarded
  - Graph ID used to route packet to final destination
- Security Layer
  - Counter is NONCE used for encryption algorithm
  - Encrypts TPDU

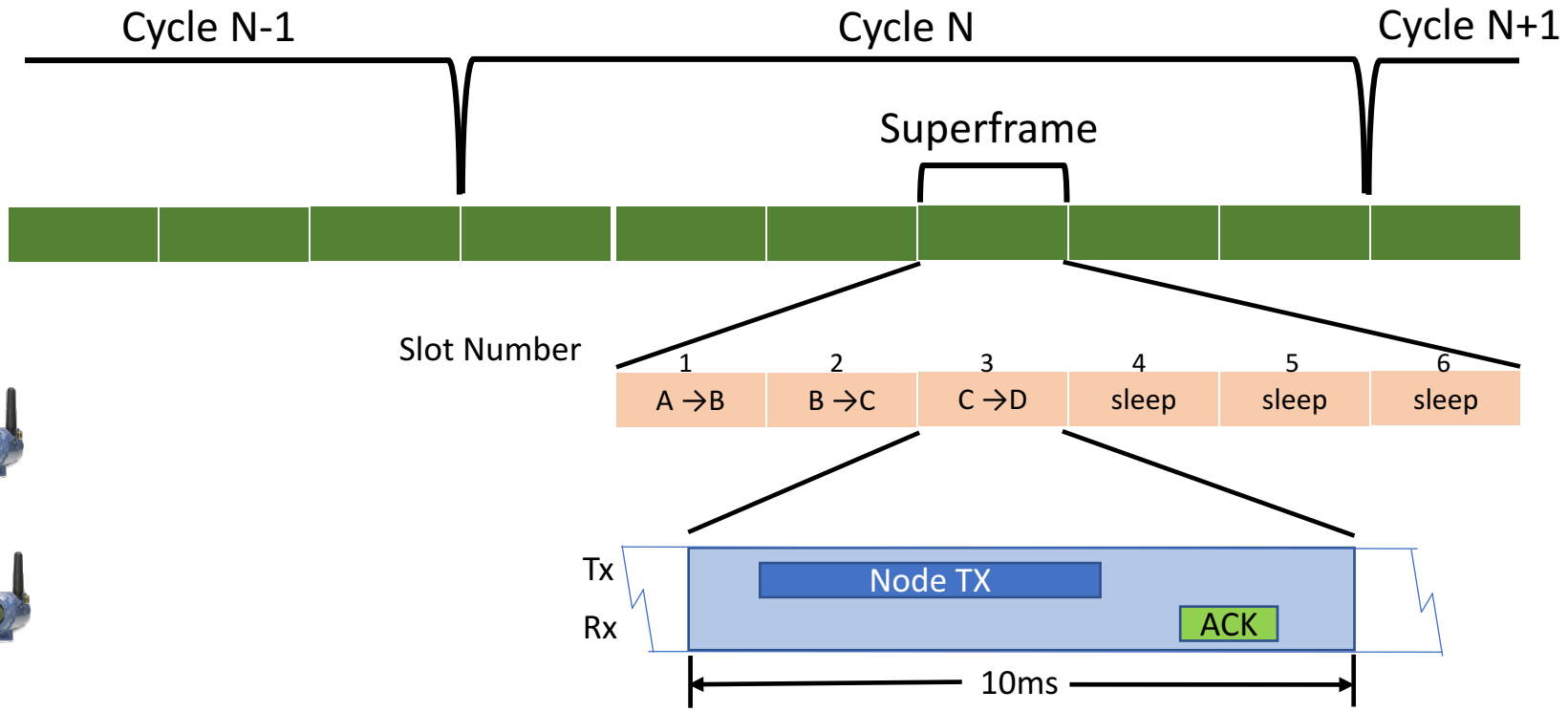
Routing

- Graph
  - Contains paths that connect different devices on the network
- Source
  - Source identifies list of devices through which a packet must travel
- Superframe
  - Packets are assigned to specific slots in superframe(s)

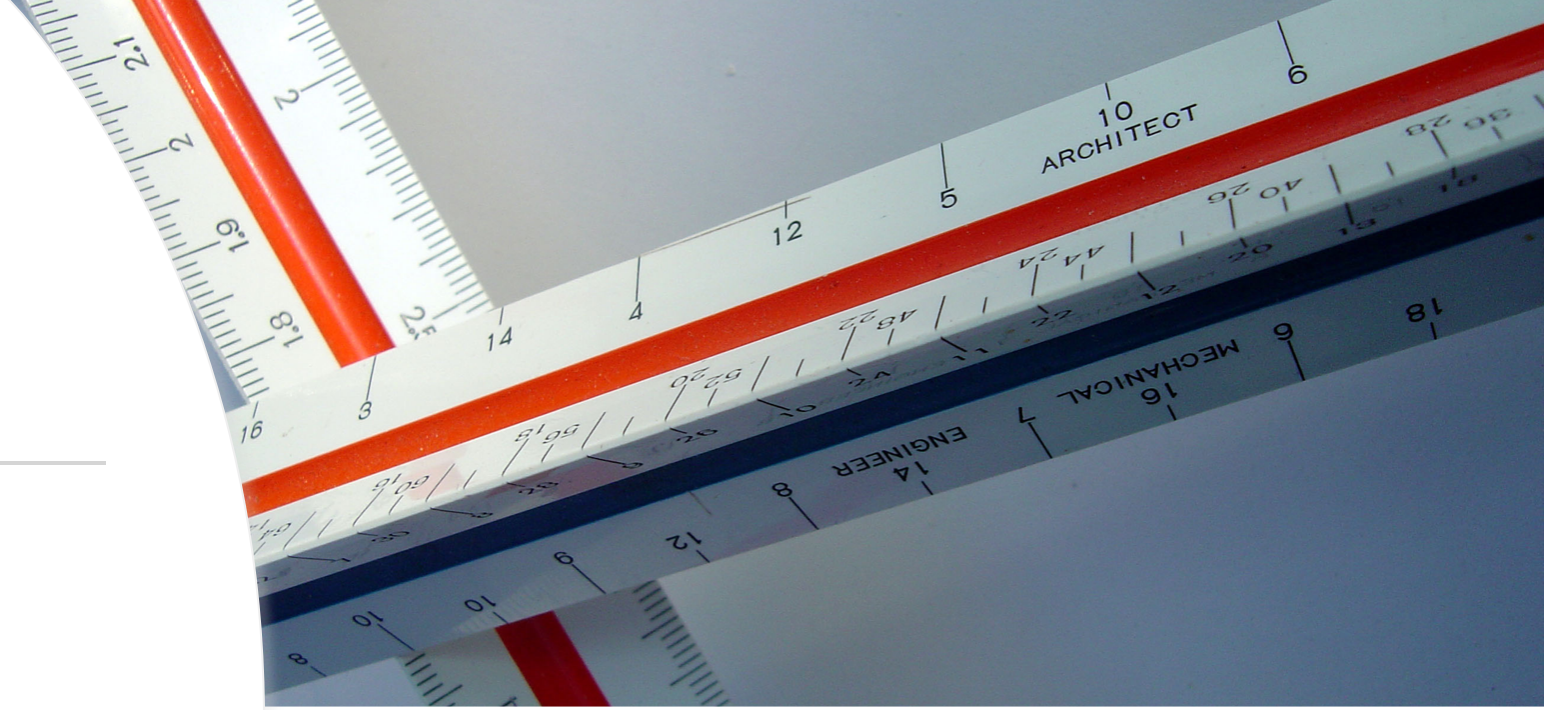


Superframe


DST
D
C
SRC
A
B


Cycle N-1
Cycle N
Cycle N+1
Superframe
Slot Number
1
2
3
4
5
6
A →B
B →C
C →D
sleep
sleep
sleep
Tx
Rx
Node TX
ACK
10ms

Topics



- Highlights
- HART history
- Protocol Overview
- **Design**
- Security

WirelessHART®

WirelessHART Design Philosophy

- Nodes/Motes/Field Devices are
  - self-configuring, self-healing, self-optimizing
- Site surveys are costly and take too much time
  - Challenging RF environment
  - Difficult to accurately model dense process plant environment(s)
  - Not possible to survey greenfield sites
  - 1000s of sensors could be deployed
- No need to develop complicated frequency/channel plans

Rule #1 - Rule of 5 (minimum)

- Minimum of 5 devices within range for Gateway

Rule #2 - Rule of 3

- Every device should have minimum of three neighbours
- Ensures at least two connections

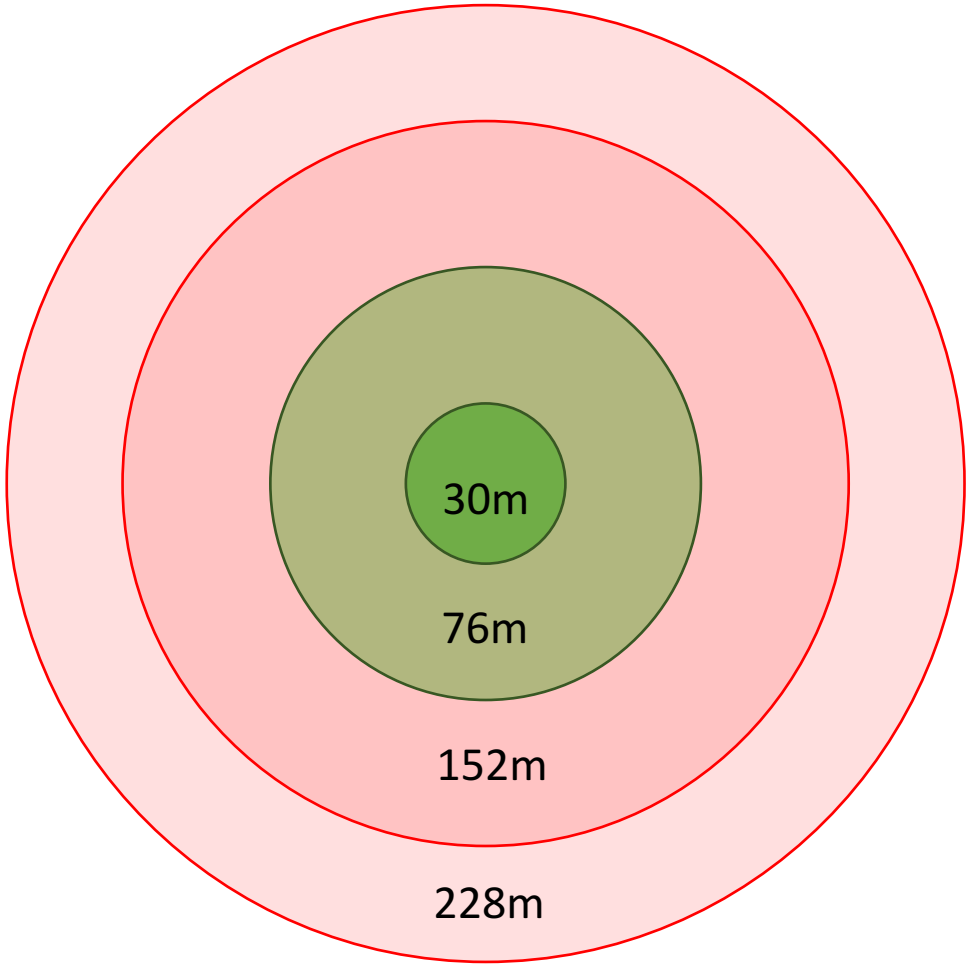
Rule #3 - Rule of Percentages

- Networks with more than 5 devices should have 25% within effective range of Gateway
- Networks with greater than 20% updates faster than 2 seconds should increase the percentage of devices within effective range of the Gateway from 25% to 50 %

Classification	Distance (m)	Distance (feet)	Description
Heavy Obstruction	30	100	Dense plant environment; where vehicle cannot pass.
Medium Obstruction	76	250	Less light process areas with lots of space. Drive a vehicle within space.
Light Obstruction	152	500	Typical tank farm. Lots of space between allows good RF propagation
Clear LoS	228	750	Antenna above obstructions with angle of terrain change < 5 degrees

Rule #4- Rule of Maximum Distance

- ✓wireless devices with updates faster than two seconds should be within two times the effect range of wireless devices from the Gateway



WirelessHART Design Philosophy Summary

1) Rule of 5 (minimum)
   - min 5 devices with range for Gateway
2) Rule of 3
   - every device should have minimum of three neighbours
   - ensures at least two connections
3) Rule of Percentages
   - Networks with more than 5 devices should have 25% within effective range of Gateway
   - Networks with greater than 20% updates faster than 2 seconds should increase the % of devices within effective range of the Gateway from 25 to 50 %
4) Rule of Maximum Distance
   - wireless devices with updates faster than two seconds should be within two times the effect range of wireless devices from the Gateway

Mounting Best Practices

- Antenna should be mounted
  - > 1m (3ft) from any large structure, building, or vertical surface
  - 4-8m (15-25ft) above ground
  - 2m (ft) above obstructions or major infrastructure

- Position antennas vertically, either straight up or straight down
- Always check weather proofing
- Follow lighting arrestor requirements

Topics

- Highlights
- HART history
- Protocol Overview
- Design
- **Security**

WirelessHART®

Security

- **Network ID** (‘think’ SSID)
  - Integer between 0 and 65535
- **Network Key**
  - Hop-by-hop datalink integrity
- **Join Key** (‘think’ PSK) – 32 hex characters
  - Global or unique per device
- **Broadcast Session Key** (‘think’ SSL)
  - Encrypt between endpoints
- **Unicast Session Key** (‘think’ SSL)
  - Encrypt between endpoints

- AES CCM* (CBC-MAC with counter mode)
  - Datalink layer(hop-by-hop) -> Integrity ONLY
  - Transport layer (end-to-end) -> enciphered

Default Vendor Keys

Default Join Keys

- **445553544E4554574F524B53524F434B** – Used by Multiple vendors “DUSTNETWORKSROCK”
- **E090D6E2DADACE94C7E9C8D1E781D5ED** – Used by Pepperl+Fuchs
- **24924760000000000000000000000000** – Used by Emerson
- **456E6472657373202B20486175736572** – Used by Endress+Hauser

“Endress + Hauser”

Default Network Key

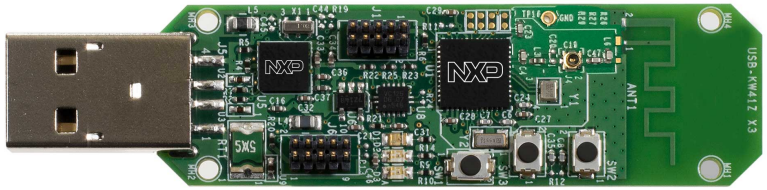
- **7777772e68617274636f6d6d2e6f7267** –Used by Multiple Vendors

www.hartcomm.org

Security Best Practices

- Never use default keys
- Use robust key management
- Practice physical security

WirelessHART - Packet Capturing

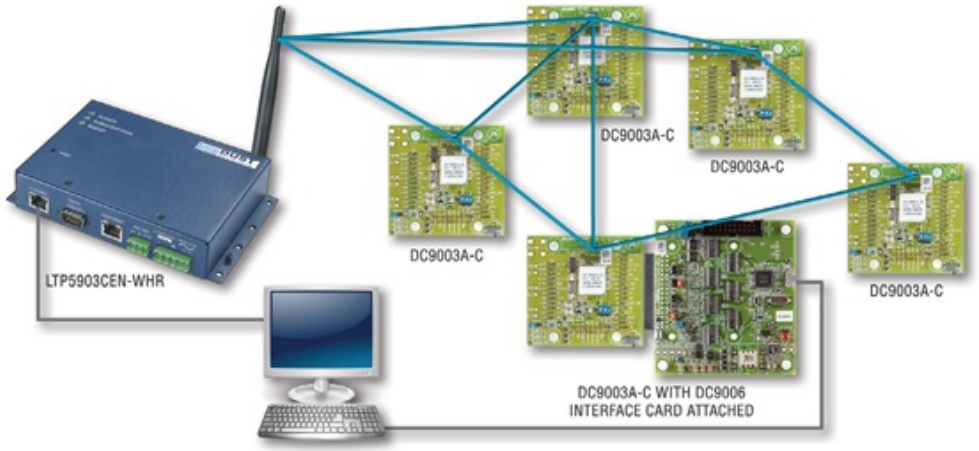


NXP KW41Z

- ZigBee sniffer (potential to modify firmware to capture WirelessHART)
- Requires 15 units
- Windows based software

Wi-Analysis

- Capture all 16 channels simultaneously
- Windows based software



DC9007A (analog.com)

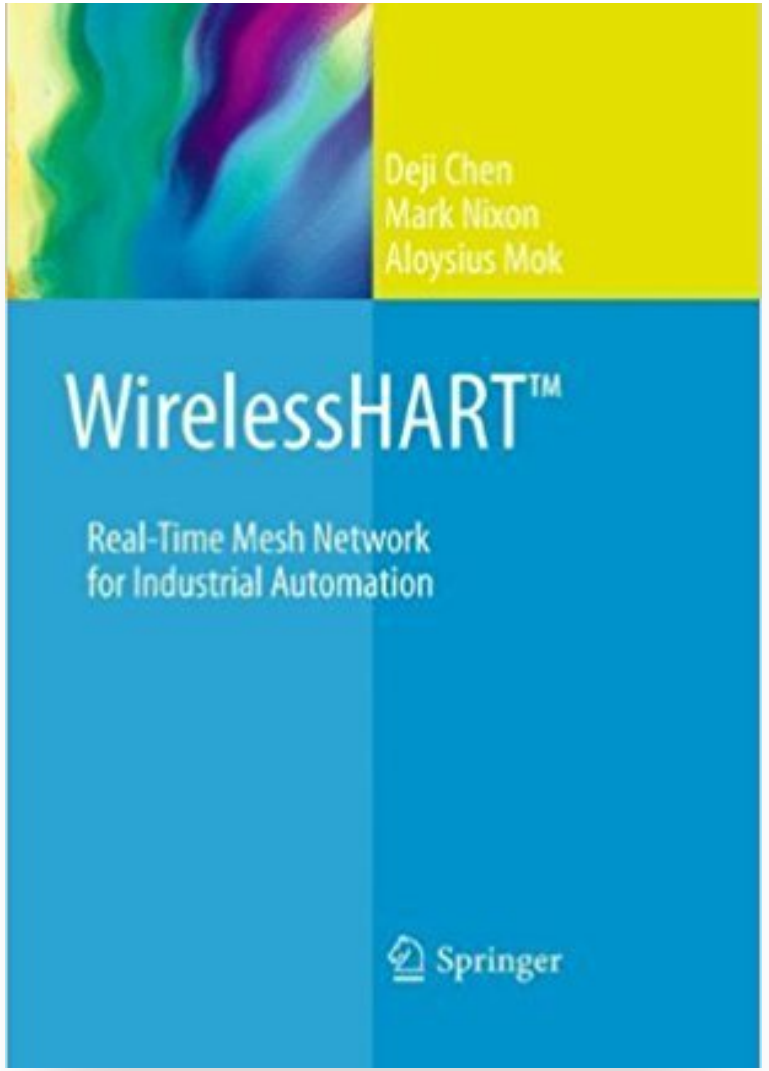
- SmartMesh WirelessHART Starter Kit
- Software development kit used to interact with the devices' Application Programming Interface (API)
- GitHub Repository

Additional **WirelessHART** Resources

- WirelessHART - defined by HART Communication Foundation (now called FieldComm Group- https://fieldcommgroup.org/
- Emerson Design Guide http://www2.emersonprocess.com/siteadmincenter/PM%20Central%20Web%20Documents/EMR_WirelessHART_SysEngGuide.pdf
- IEEE 802.15.4-2006 specification http://standards.ieee.org/getieee802/download/802.15.4-2006.pdf
- IEC 62591

https://webstore.ansi.org/RecordDetail.aspx?sku=IEC+62591+Ed.+2.0+b%3a2016

- **WirelessHART(TM): Real-Time Mesh Network for Industrial Automation**



Questions?

WirelessHART®

@troymart