Applications in Process Industry

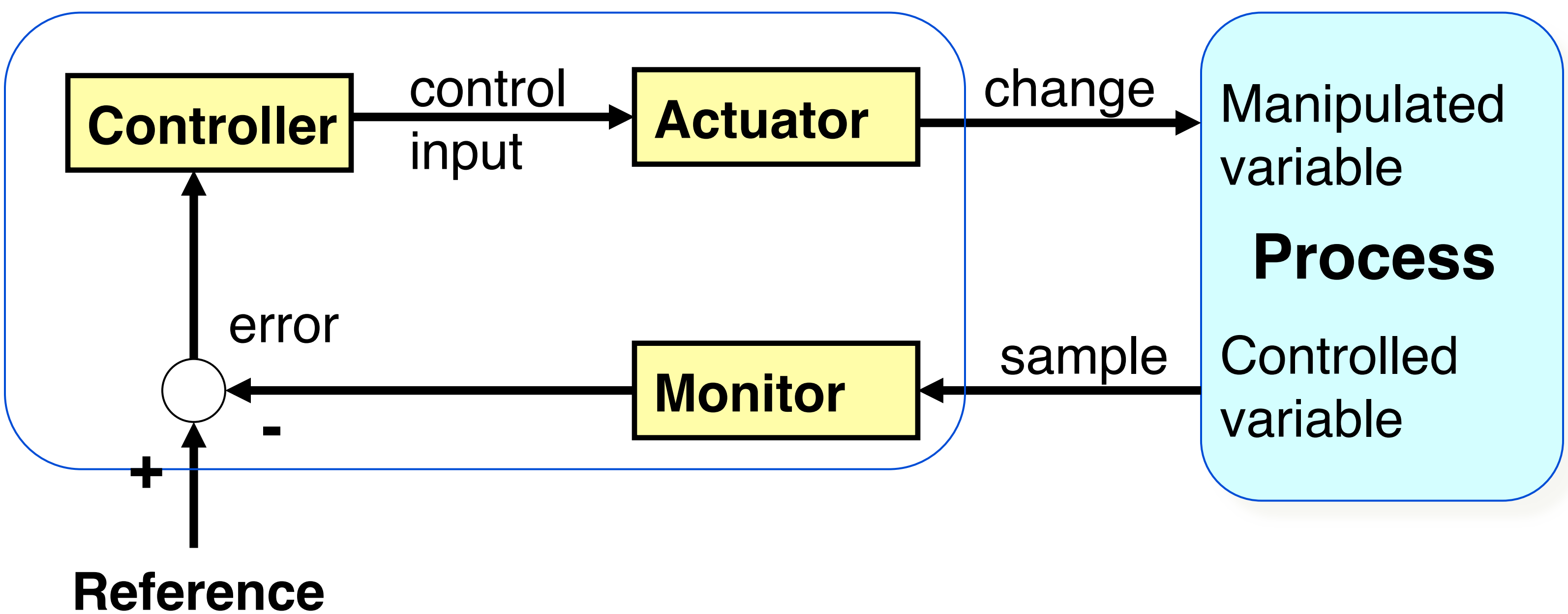
CPSL Cyber-Physical Systems Laboratory

- Enhance safety, optimize process, protect environment
  - Detect leaks before they lead to environmental problems.
  - Monitor the status of manually operated valves.
  - Monitor safety relief valves to detect venting to avoid accidents.

- Health, Safety, and the Environment (HSE) regulations.

Process Control

- Feedback control loop controls a physical process.
  - Example: control temperature by manipulating heat supply.
- Centralized vs. peer-to-peer control.



Why Wireless

CPSL Cyber-Physical Systems Laboratory

- Cost reduction: wiring is economically infeasible
- Easier installation: inaccessible locations
- Easier maintenance
  - Wired networks cannot handle severe heat or exposure of chemicals
  - A wireless infrastructure can remain in place for many years.

Challenges in Wireless

CPSL Cyber-Physical Systems Laboratory

- Strict timing requirement
- High security concerns
- Reliable communication despite wireless deficiencies
- Plant environments are inherently unreliable
  - Interference, obstacles, power failures, lightening, storms…

Wireless Technologies

- Existing standards fail in industrial environments
  - ZigBee: static channel
  - Bluetooth: quasi-static star network

- WirelessHART
  - For process measurement and control applications
  - First open and interoperable wireless standard to address the critical needs of real-world industrial applications

History

- HART (Highway Addressable Remote Transducer Protocol)
  - Most widely used field communication protocol
  - 30 million devices worldwide

- WirelessHART released in Sep 2007 (as a part of HART 7)
  - Adds wireless capabilities to the HART protocol while maintaining compatibility with existing devices, commands and tools.

Wireless for Process Automation

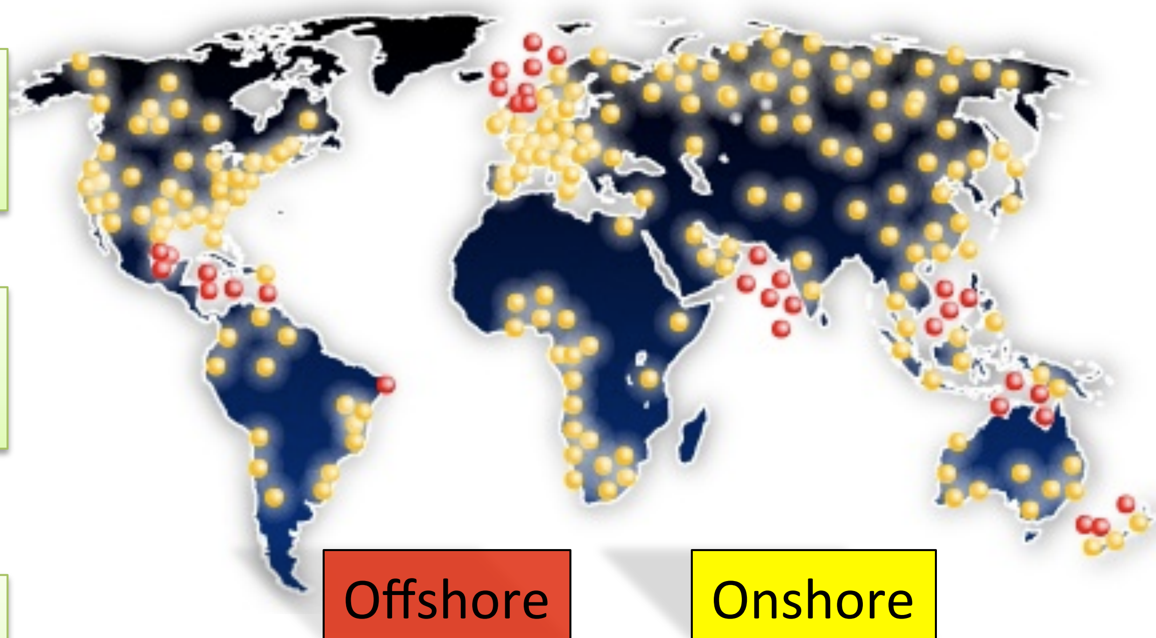
CPSL Cyber-Physical Systems Laboratory

- World-wide adoption of wireless in process industries

1.5+ billion hours operating experience

100,000s of smart wireless field devices

10,000s of wireless field networks



Courtesy: Emerson Process Management

Killer App of Sensor Networks!

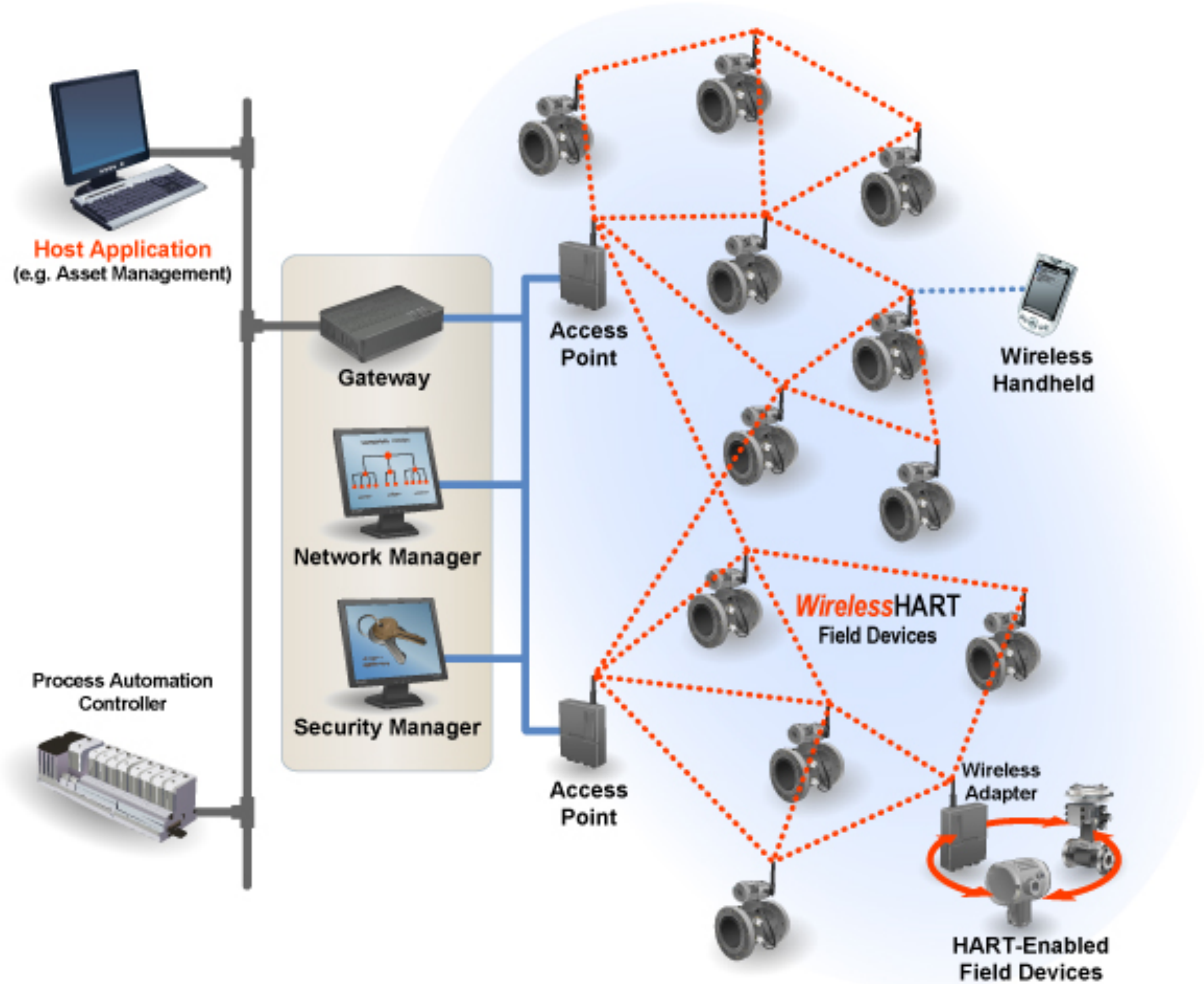
WirelessHART Use Cases

- Improved control of plant steam supply by detecting "cool spots" in cross plant steam lines
- Reducing risk of overfilling tanks by adding redundant level measurements (in oil and petroleum refineries)
- Monitor and control safety valves
- Monitor and control pressure and temperature of process fluids and gases

What is special?

- Reliable: 99.9%
- Secure
- Self-organizing, self-healing
- Interoperable
- Supports both star and mesh topologies
- Built-in time synchronization

Network Architecture



Network Manager

- Centralized brain

- Manages the network and its devices
  - Routing, scheduling
  - User/administrator interacts with the Network Manager
  - Generates network management packets to devices

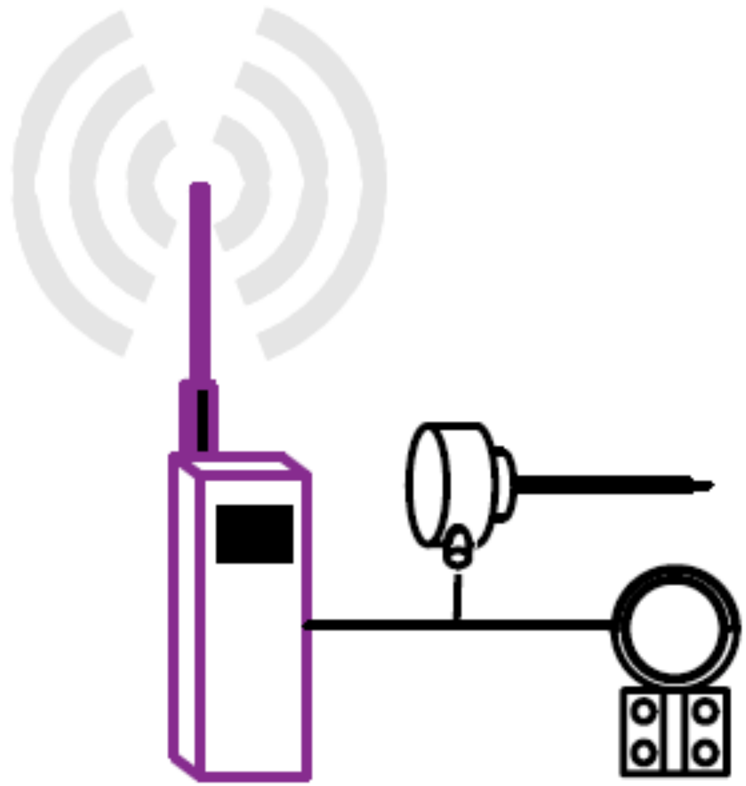
- Redundant Network Managers supported (only one active)

Field Devices

- Sensor/actuator/both
- Connected to the process or plant equipment
- Combines wireless communication with traditional HART field device capabilities
- May be line or battery-powered

WirelessHART Adapter

- Enables communication with a non-native device through a WirelessHART Network. .



Gateway

- One gateway can support up to 80 devices

- A Gateway provides
  - One or more Access Points providing the physical connection into the WirelessHART network
  - One or more Host Interfaces connecting the Gateway to backbone networks (e.g., the plant automation network)
  - A connection to the Network Manager
  - Buffering and local storage for publishing data, event notification, and common commands
  - Time synchronization sourcing

Other Devices

CPSL Cyber-Physical Systems Laboratory

- Handheld devices
  - Portable applications used to configure, maintain or control plant assets.
  - Typically belong to networks of different standards
- Plant Automation Network
  - Connects client applications to the gateway
- Security Manager
  - Industry standard AES-128 ciphers/keys

WirelessHART PHY

- Adopts IEEE 802.15.4
  - Same 16 mutually orthogonal channels
  - Operates in the 2.4GHz ISM band
  - Data rate of up to 250 Kbps

- Radio transceivers
  - Omni-directional
  - Half-duplex
  - 100 meters LOS @ 0 dB
  - Time to switch between channels: 0.192 ms
  - Radio turn-on time: 4 ms

How to achieve reliability?

- Time diversity
- Channel diversity
  - Channel hopping
  - Channel blacklisting
- Route diversity
  - Graph routing
- Power Diversity

TDMA Data Link Layer

CPSL Cyber-Physical Systems Laboratory

- 10 ms time slot
  - Transmission starts at a specified time after the beginning of a slot
    - Source & destination set channel
    - Allows receiver to begin listening
  - Enough time for transmission + ACK

- Superframe: a series of time slots defining the communication schedule of a set of devices

Time Synchronization

- Gateway is the root source of time

- When a device receives a packet
  - Δ t = time of arrival – expected arrival time
  - sends Δ t to the sender via ACK

- Sender adjusts time

Shared vs. Dedicated Time Slots

- A time slot may be shared or dedicated
- Dedicated slot: only one sender sends to a receiver
- Shared slot: multiple senders attempt to send to a receiver

Shared Time Slots

- Devices contest for access using a contention-based scheme.
  - Behave similar to Slotted Aloha
  - Use collision-avoidance (backoff).
- Using shared links may be desirable when
  - Throughput requirements of devices are low
  - Traffic is irregular or comes in bursts
- May reduce latency since devices do not need to wait for dedicated slot
  - True only when chances of collisions are low

Channel Hopping

- Enhances reliability
  - Avoid interferers
  - Reduce multi-path fading effects
- Blacklisting restricts hopping to some channels
- Each device has a channel map (logical to physical)
- ActiveChannel = (ChannelOffset + ASN) % #Channel

Routing

- WirelessHART supports both Graph and Source routing
- Graph routing: provides redundant paths
- Routing graphs
  - Uplink graph: upstream communication
  - Downlink graph: Downstream communication
  - Broadcast graph

Scheduling

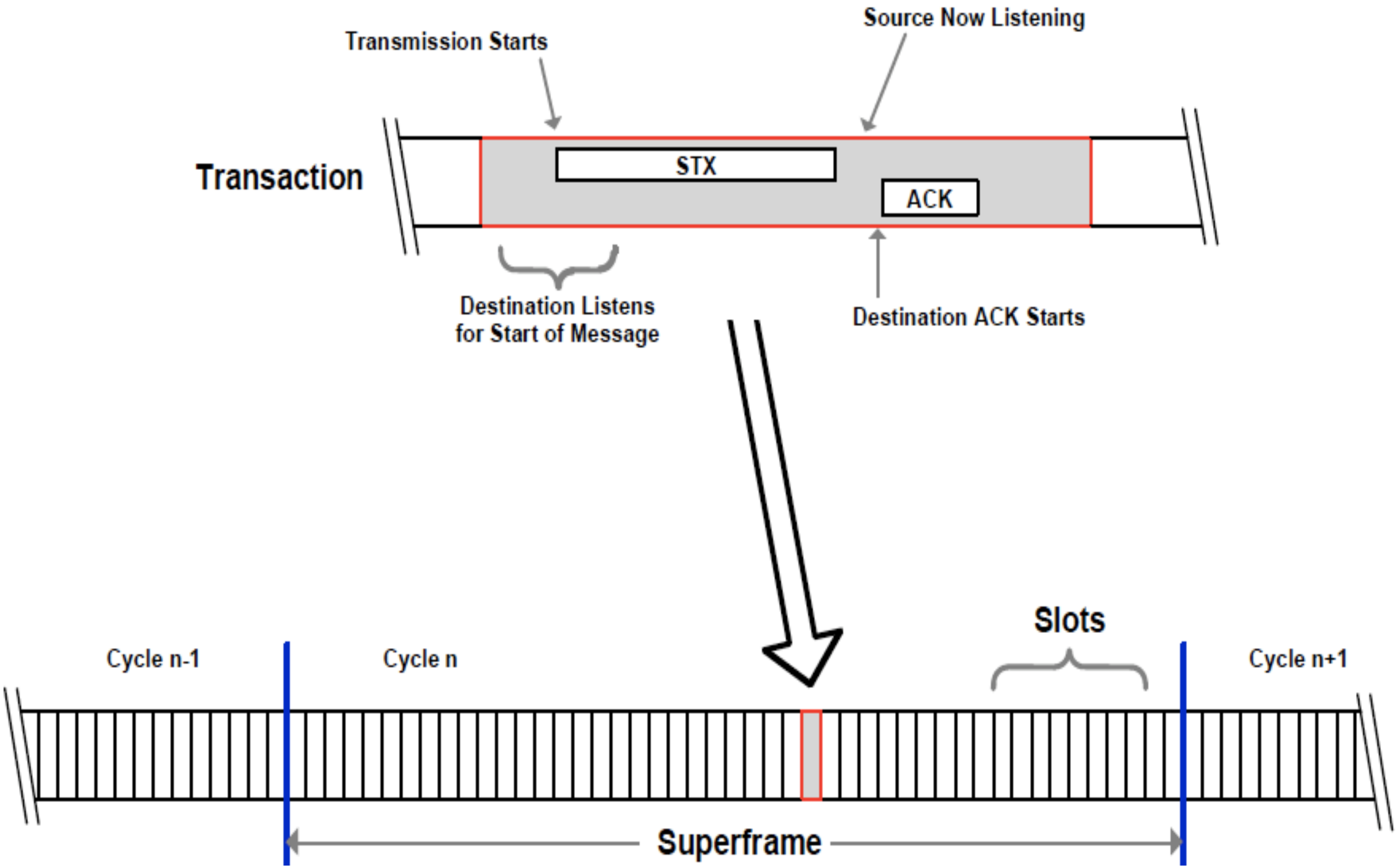
- Slots and channel assignment
  - Each receiver uses a separate channel for reception
  - A transmission is followed by a retransmission on the same link on a dedicated slot, then again on another link on a shared slot

- Each network contains exactly one overall schedule that is created and managed by the Network Manager.

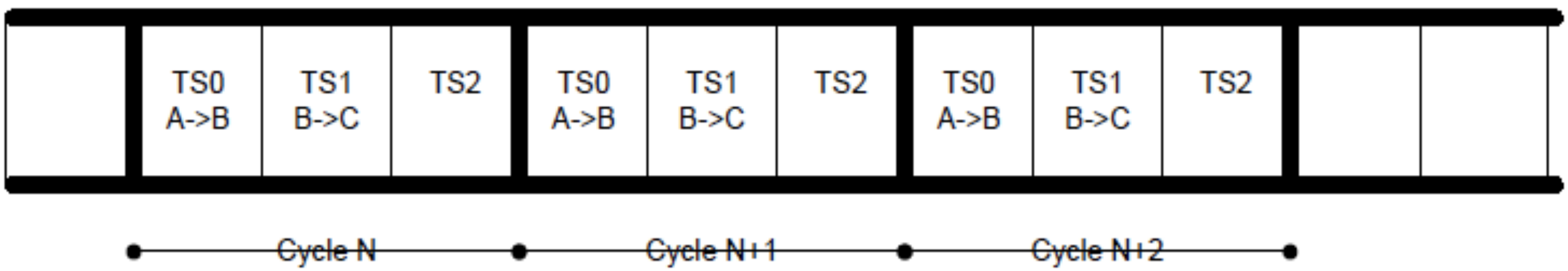
- The schedule is organized into superframes

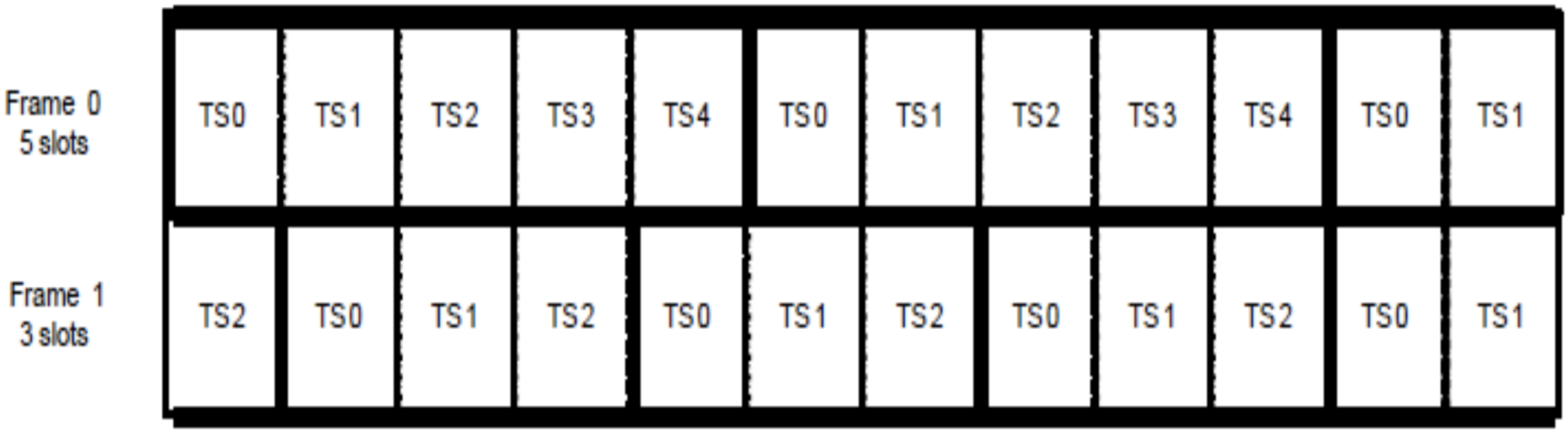
Superframe

CPSL Cyber-Physical Systems Laboratory



Superframe


TS0
A->B
TS1
B->C
TS2
TS0
A->B
TS1
B->C
TS2
TS0
A->B
TS1
B->C
TS2
Cycle N
Cycle N+1
Cycle N+2


Frame 0
5 slots
Frame 1
3 slots
TS0
TS1
TS2
TS3
TS4
TS0
TS1
TS2
TS3
TS4
TS0
TS1
TS2
TS0
TS1
TS2
TS0
TS1
TS2
TS0
TS1
TS2
TS0
TS1

Superframe

- All devices must support multiple superframes
- At least one superframe is always enabled while additional superframes can be enabled or disabled
- Slot sizes and the superframe length are fixed and form a network cycle with a fixed repetition rate

Data Link Protocol Data Unit (DLPDU)

CPSL Cyber-Physical Systems Laboratory

- Five DLPDU types:
  - Data
  - Keep-Alive (periodic)
  - Advertise (periodic)
  - Disconnect
  - ACK

- Devices receiving a packet with an unknown packet type must not acknowledge the packet and shall immediately discard it.

Network Initialization

- WirelessHART Network automatically starts up and self-organize.
- Before a network can form, a Network Manager and a Gateway must exist.
- The Network Manager activates the first superframe. This establishes the system epoch – ASN 0.
- Once the Network Access Point starts to advertise, devices can begin to join the network.
- As devices join, the network forms.

Network Maintenance

- Advertise and Keep-Alive DLPDUs assist in building and maintaining the device's neighbor list
- A Keep-Alive must be transmitted to the neighbor if Last Time Communicated > Keep Alive Interval.
- Keep-Alive transmissions are repeated until a new DLPDU is received from the neighbor
- Keep-Alive no more often than once per 30 seconds (if temperature varies 2° C per minute or less).

Network Maintenance

CPSL Cyber-Physical Systems Laboratory

- Path failures are reported to the Network Manager when devices lose connectivity to neighbors.
- After the Path Fail Interval lapses, a Path-Down Alarm is generated (by both the sender and the receiver).
- As each device's Health Report Timer lapses, the devices generate health reports, which include indications of any problems the device is having with a neighbor.
- Default period of each devices health report is 15 minutes.

Network Maintenance

CPSL Cyber-Physical Systems Laboratory

- Devices continue trying to reestablish communication until the links between them are deleted by the Network Manager.
- It is common for broken paths to be restored after a temporary environmental effect passes.
- If the disruption persists, additional Path-Down Alarms will be generated when the Path Fail Interval lapses again.

Best Practices

- Each field device should have at least three neighbors
  - The 3rd neighbor will act as a backup if one of the two primary paths is obstructed or unavailable.
- Devices (antenna) mounted >0.5m from any vertical surface.
- Devices mounted >1.5m off the ground.
- 25% of the network devices should have a direct connection to the gateway in large networks.