ISA100 Wireless Training

Intro and Technology Primer

Jay Werb
ISA100 Wireless Compliance Institute

Robert Assimiti
Centero

For: ISA Saudi Arabia Section
14 November 2022

Presenters

Jay Werb
Technical Director
WCI

email: jay@jwerb.com

Robert Assimiti
CEO
Centero

email:
robert.assimiti@centerotech.com

Agenda

ISA100 Wireless Benefits and Use Cases

Introduction to ISA100 Wireless

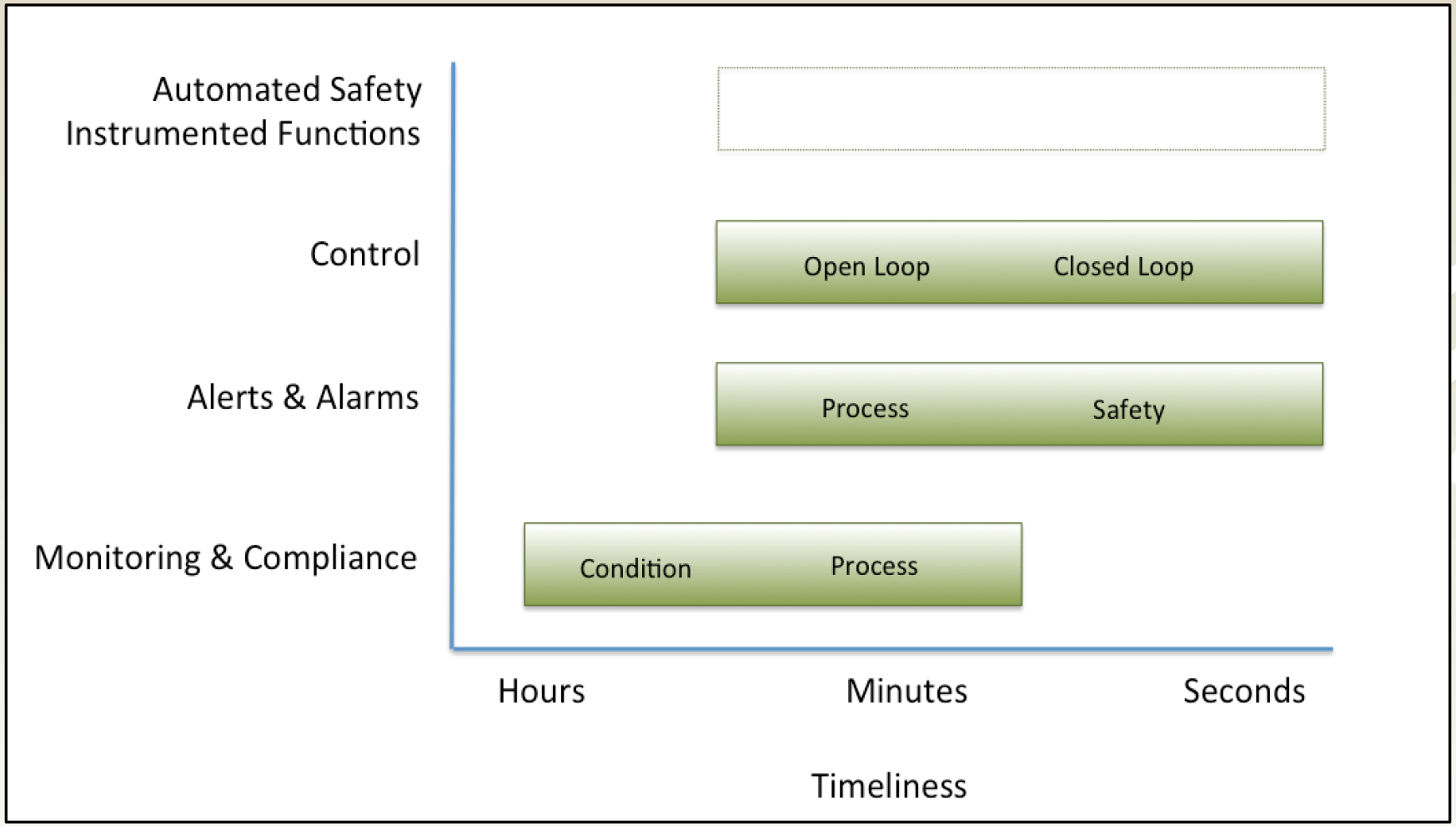
Installation Considerations

ISA100 Wireless Security (time permitting)

Commonly Cited Benefits of Wireless Instrumentation

Cost Savings	• Up to 90% of installed cost of conventional measurement technology can be for cable conduit and related construction. • Typically: 1/5 the time, 1/2 the cost. • New and scaled applications are now economically feasible.
Improved Reliability	• Wired sensors may be prone to failure in difficult environments. • Wireless can add redundancy to a wired solution.
Improved Visibility	• Condition monitoring (equipment) • Process monitoring
Improved Control	• Add wireless to existing processes for more optimal control.
Improved Safety	• Safety related alarms

Top Usage Classes for Wireless Instrumentation

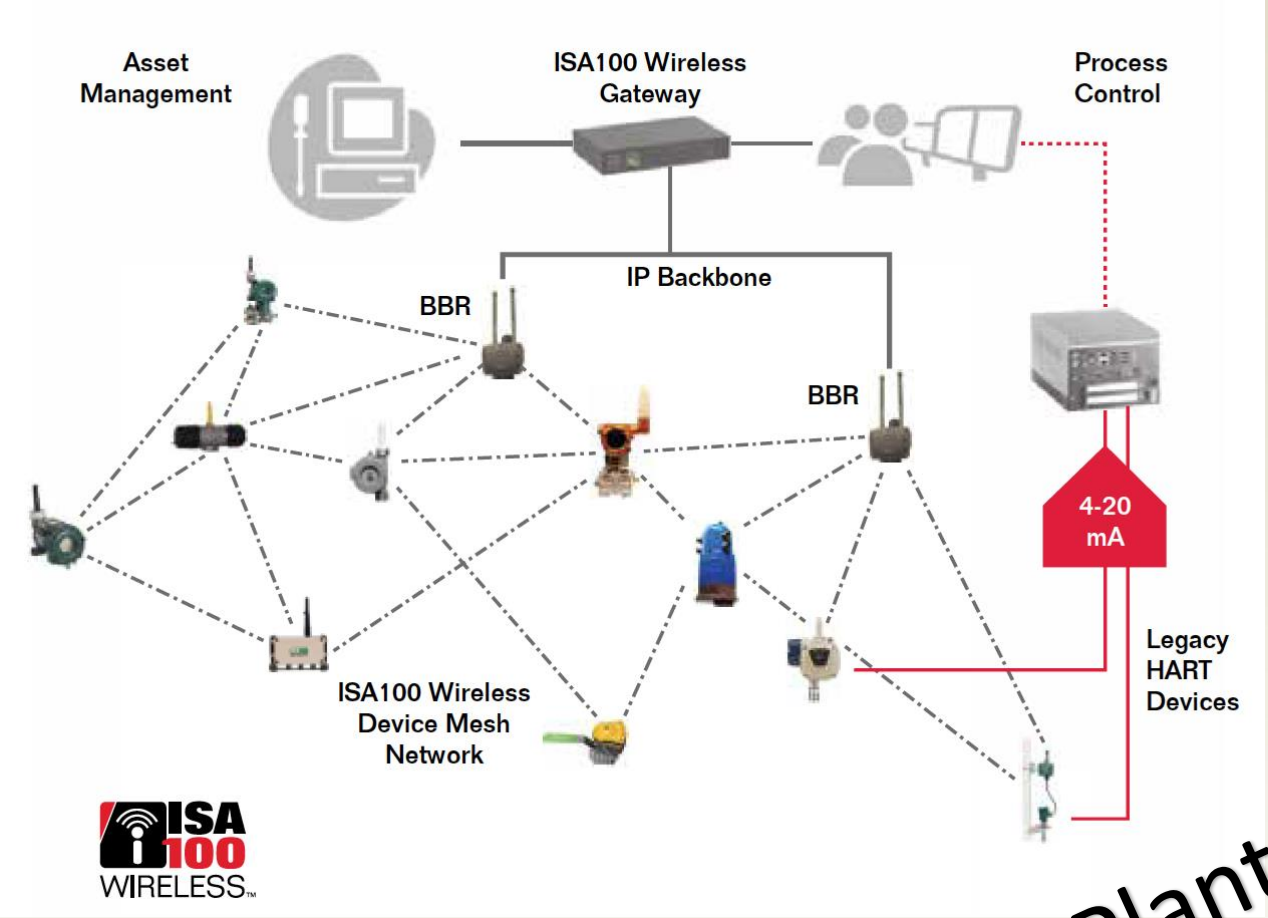


Courtesy AIW LLC

ISA100 Wireless Interoperability

One Plant Network

Introduction to Industrial Wireless



One Plant Network

Applications

Monitoring
- Machine health
- Well head
- Remote process
- Leak detection
- Equipment Condition
- Environmental
- Tank level
- Steam trap

Gas detection

Fuel tank gauging

Basic process control

Open loop control

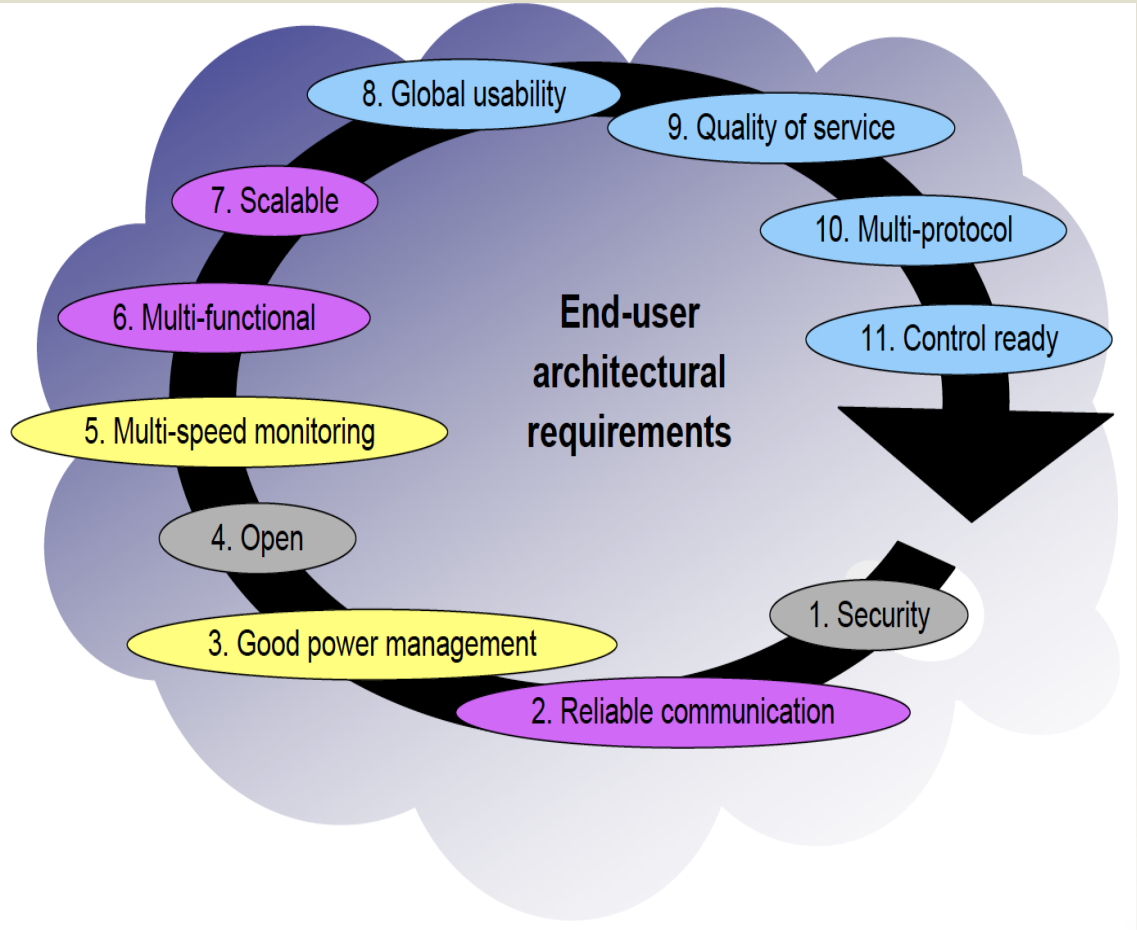
Stranded data capture

Diagnosis of field devices

… and more

Technical requirements for Industrial wireless sensing and control

(Voice of the customer, ~2005)



Security	Flawless application of proven cryptography
Reliable communication	24x7 operation; High data integrity
Good power management	Long and deterministic battery life
Open	Buy instruments from multiple suppliers
Multi-speed	Some devices report frequently, other not
Multi-functional	One network, many applications
Scalable	Scalable in numbers, space, and rate. Scale through IP, not by duplication.
Global Usability	One technology legal everywhere
Quality of Service	Controlled latency, low error rate
Multi-protocol	Cleanly integrate with wired investment
Control ready	Not just monitoring

Technical requirements for Industrial wireless sensing and control

(Voice of the customer, ~2005)

1. Rate and Latency	• Publication rates 1-2 seconds • Capable of 100 ms latency • Controlled latency, ~50% publication rate • 4 Hz publication in constrained configurations
2. Mesh Networking	• IP Backbone: Engineered and scalable • Mesh and non-mesh topology; access points and field devices • Peer-to-peer communication • Objects = Function blocks at device level • Long and deterministic battery life
3. Reliability	• Wireless transmission is deterministic • Wireless transmission is received • Wireless transmission is accurate • Redundant communication paths to process control network
4. Security	• Wireless transmission is secure; prevention & detection

Radio Reliability Strategies in ISA100 Wireless

Leverage the Infrastructure	Messages to the backbone minimizing wireless transmissions
Mesh networking	Alternative routes available for retries
Time Slotted Operation	Avoid collisions and retries, deterministic message delivery
Radio selection	Widely available IEEE radio designed for WiFi coexistence
Low duty cycle	Transmit a small amount of data only when necessary
Staccato operation	Short messages allow other radios in network to quickly recover
Time diversity	Retries configurable, backoff on longer timeframes than WiFi etc
Channel diversity	Retries using a different radio channel
Spectrum management	Detect and blacklist problematic radio channels
Collision avoidance	Listen before send (configurable!)
Security	Strong checks at the link level , immediate detection of unsuccessful transmission
Diagnostics	Measure and report performance of radio links

Generally, messages are short, radio connections stable, retries on different time/channel/route.

ISA100 Wireless
"Native" Application Layer

WCI Extensions

Device Information
- Identification & Certification
- NAMUR NE107 Diagnostics

Unified Field Objects (Process)
- Tag
- Filter/Hysteresis
- Alarms
- Simulate (Test)

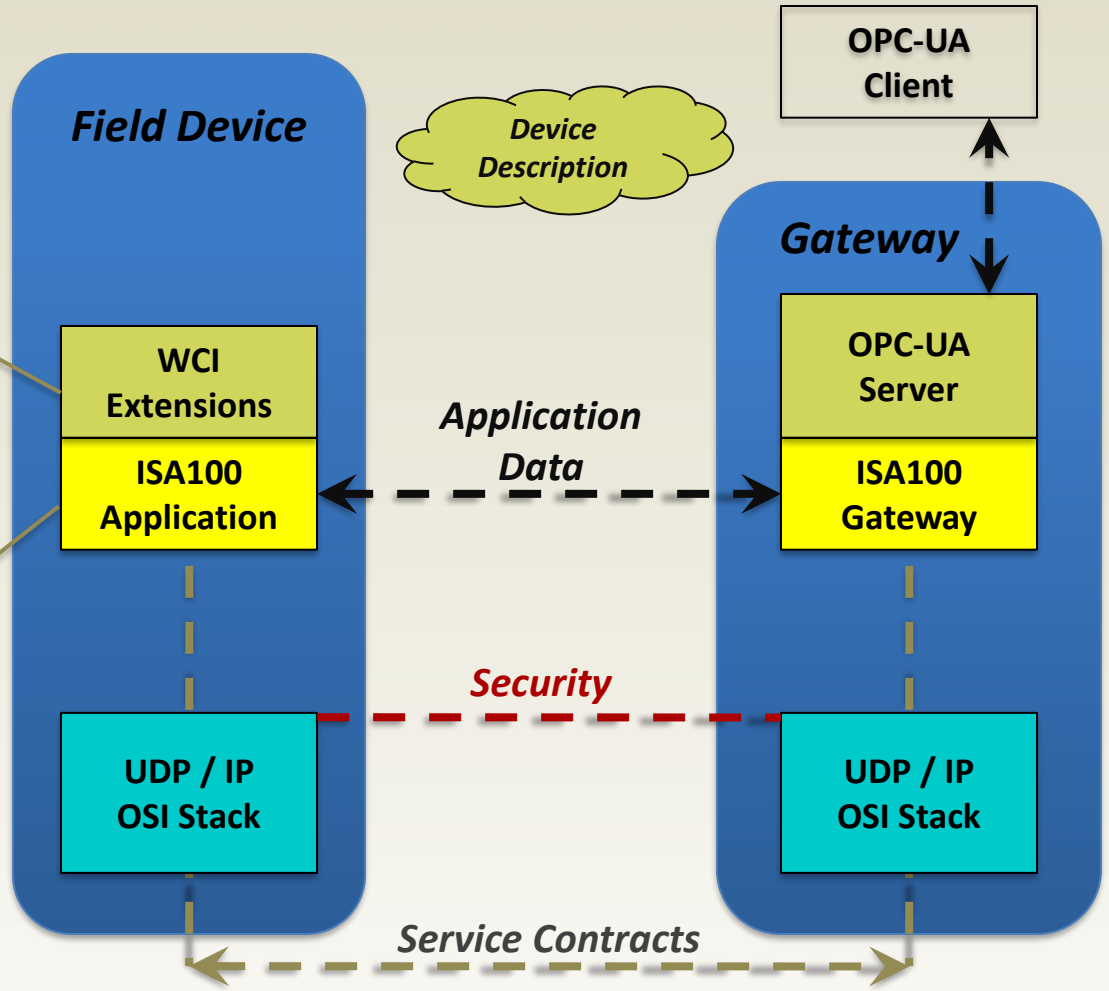
Profiles (Process)
- Temperature
- Pressure
- Positioner
- Custom

Baseline Application Layer

Services
- Client/Server
- Publish/Subscribe
- Alerts
- Contracts

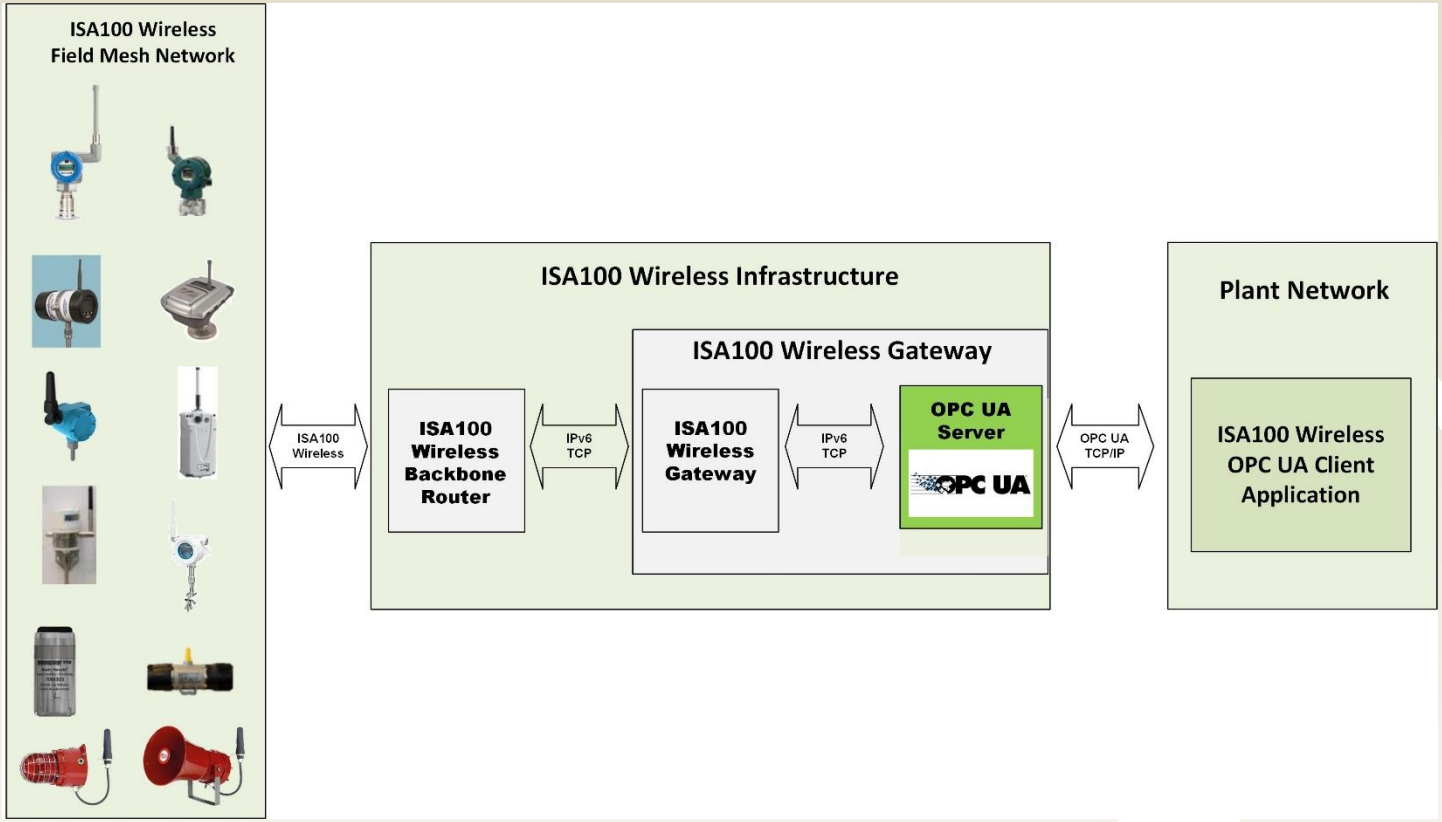
Unified Field Objects (Generic)
- Analog Input Object
- Binary Input Object
- Analog Output Object
- Binary Output Object

Upload/Download

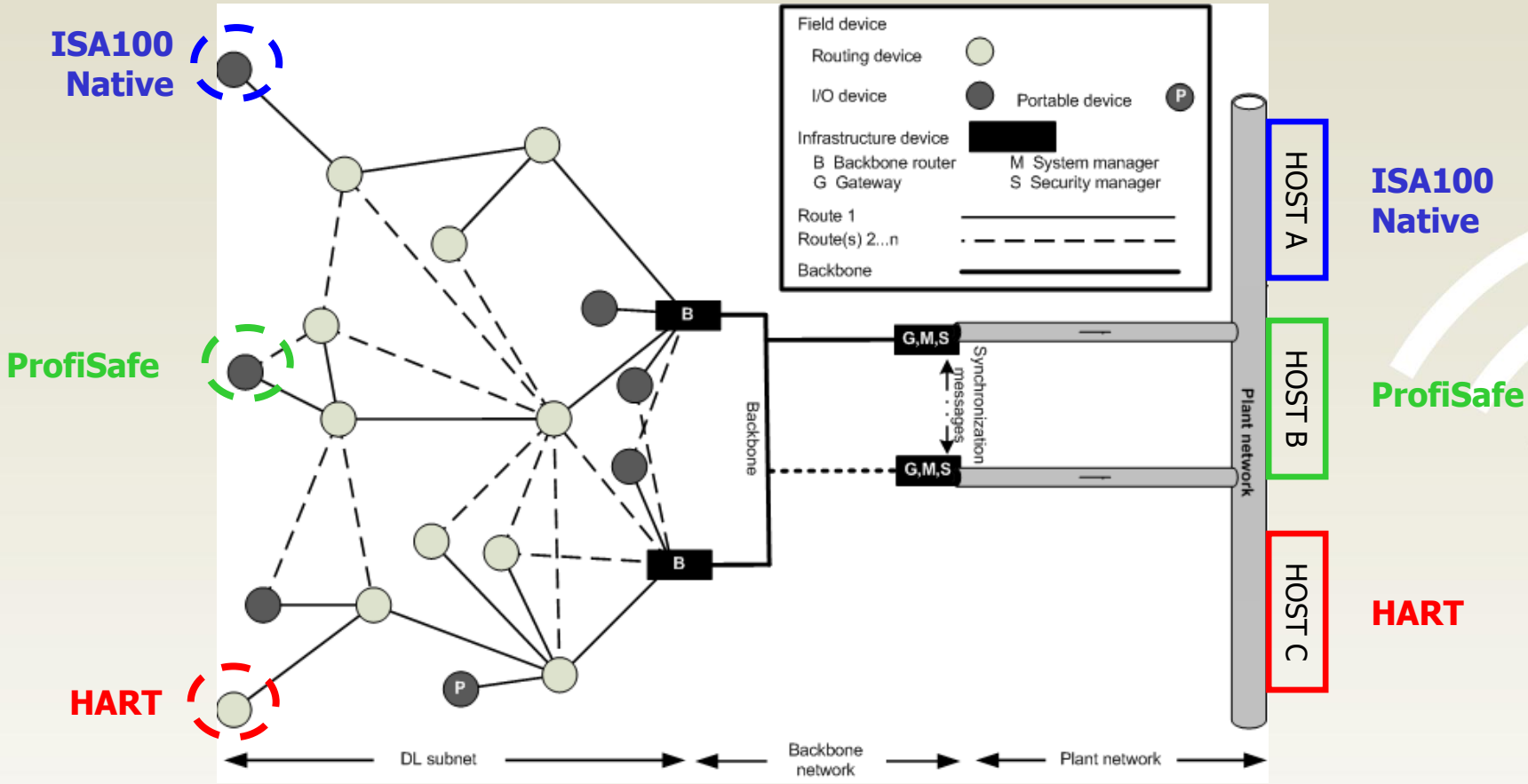


ISA100 Wireless
OPC UA Information Model

- WCI standard document that defines an OPC UA Information Model to represent and access ISA100 Wireless devices
- Standardization was a cooperative effort between the WCI and the OPC Foundation
- Includes the following OPC UA models
  - ISA100 Field Devices – extension of PA-DIM model (OPC 30081)
  - ISA100 Access Point
  - ISA100 Network information model



ISA100 Wireless
One Network, Multiple Application Layers



ISA100 Wireless Solutions

Infrastructure

- **Independent Gateway**
  - Honeywell, Yokogawa


- **Access Point (AP)**
  - Honeywell, Yokogawa


- **Integrated Gateway/AP**
  - Honeywell, Yokogawa, CDS, Nexcom

- **GW/AP + Recorder**
  - Yokogawa

- **Adapter (HART, etc.)**
  - Honeywell, Yokogawa


Measurement & Control

- **Temperature**
  - Honeywell, Yokogawa

- **Pressure / Flow**
  - Honeywell, Yokogawa

- **Level**
  - Honeywell, Yokogawa

- **DI/DO, AI**
  - Honeywell, Yokogawa


- **Valve Position**
  - Eltav, Flowserve, Honeywell


Energy Efficiency, HSE & Asset Management

- **Corrosion**
  - RCS , Honeywell


- **Steam Trap**
  - Spirax Sarco, TLV, Armstrong, Bitherm


- **Vibration**
  - Bently Nevada

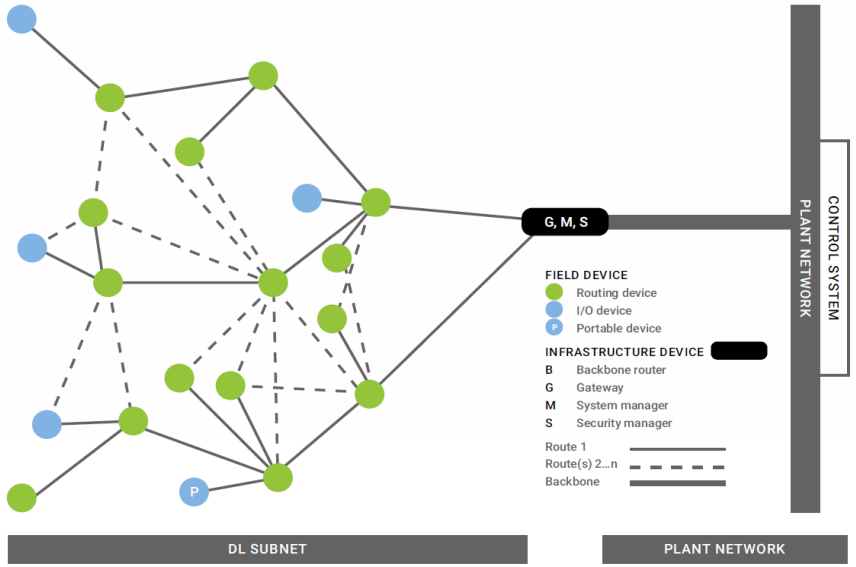
- **Gas**
  - GasSecure, Scott Safety, New Cosmos, Riken Keiki

- **pH**
  - Honeywell, Yokogawa

And more…

Common Network Architectures

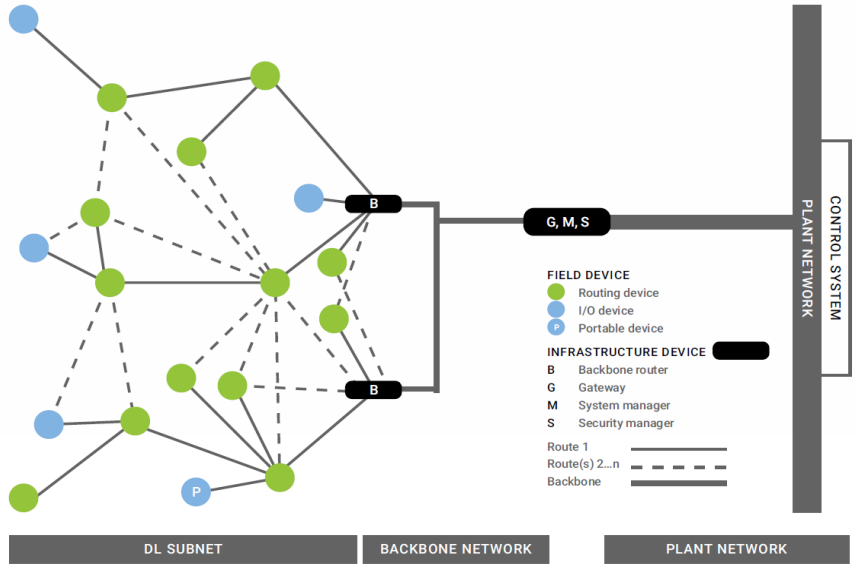
All-in-One Network Topology



KEY CHARACTERISTICS

- Single subnet – no backbone infrastructure
- Typically scales to <100 field instruments
- Instruments deployed are in close proximity
- Cover smaller deployment areas
- Simplified network deployment

Distributed Network Topology



KEY CHARACTERISTICS

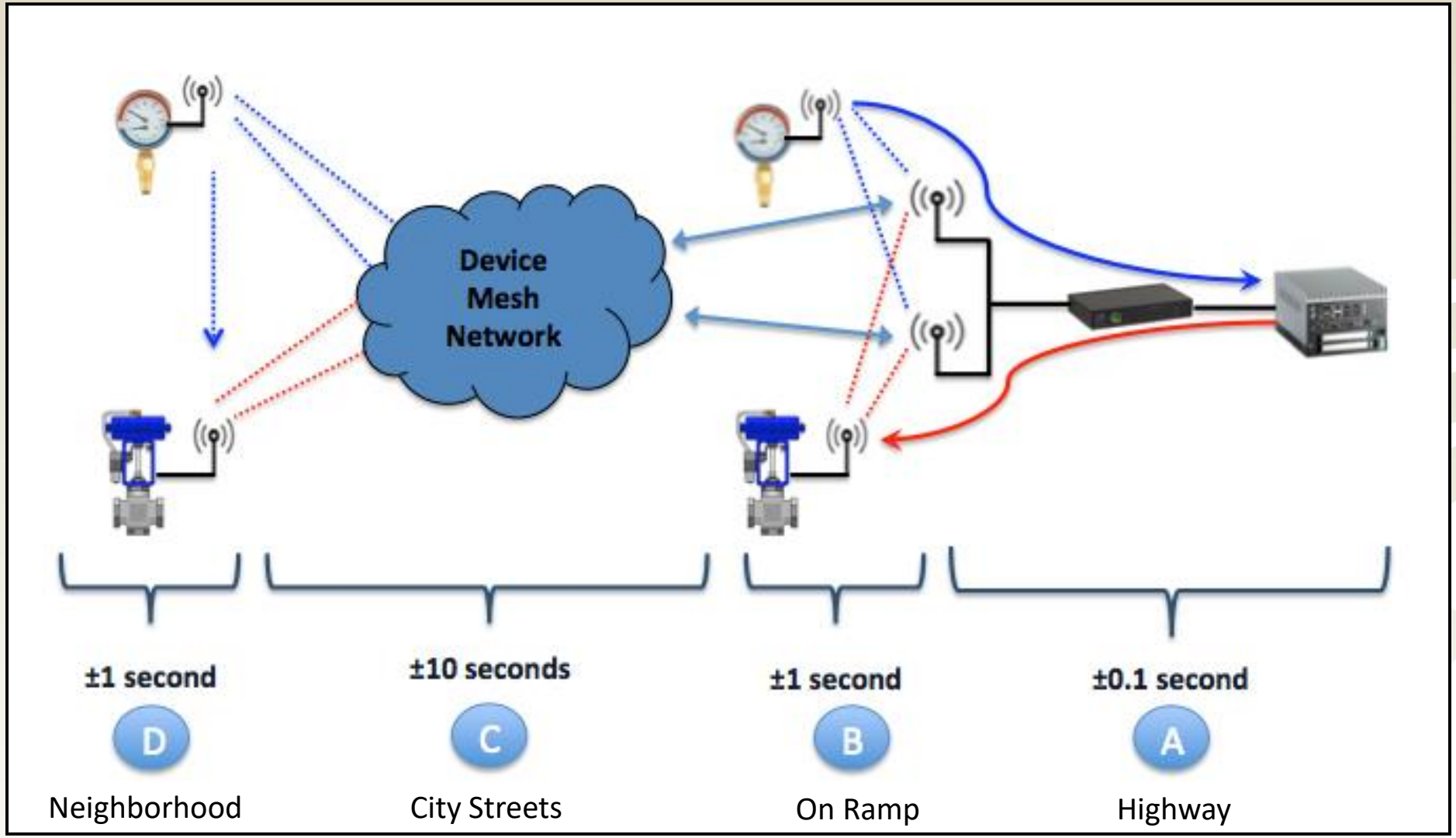
- Multiple ISA100 Wireless mesh subnets connected via Wi-Fi Mesh backbone
- Typically scales to hundreds of field instruments
- Instruments are scattered throughout the facility
- Extended geographic coverage (miles/kilometers)
- Plant wide wireless canopy

Centero Examples

ISA100 Wireless
Installation Considerations

- Latency
- Network Design
- Security Matrix
- Denial of Service
- Some Other Considerations

Mesh Networks – Latency Considerations



Network Design

*Please **adhere to manufacturer's best practices** when designing and laying out a wireless sensor network.*

- Conservative communication range
- Reporting Rates
  - *Device and router battery capacity*
  - *Wireless channel capacity*
  - *Infrastructure capacity*
- Centrally located infrastructure
- Control hop depth
- Path redundancy (Infrastructure and/or mesh)
- Avoid bottlenecks
- Use network layout and simulation tools
- Documentation!!!

Design network with plenty of margin and monitor that margin carefully.

Security Matrix

	Authentication	Verification		Encryption	Access Control	Key Management
		Integrity Check	Time			
Sniffing			✓	✓		✓
Tampering		✓	✓			✓
Spoofing	✓		✓	✓	✓	
Replay Attack		✓	✓			✓
Routing Attack	✓			✓	✓	✓
DoS Attack	See Next Slide					

Authentication, Integrity Check, TAI, and Encryption are built into the ISA100 Wireless standard. Systems ensure that users cannot not disable or mis-apply these features.

Access Control and Key Management involve adherence to manufacturer's best practices.

Denial of Service

The ISA100 Wireless standard and implementations apply a variety of techniques to operate reliably in the presence of interference.

- *Unintentional interference ≈ coexistence*
- *Intentional interference ≈ denial of service attack*

Common strategies

- *Spread spectrum modulation*
- *Redundant routing*
- *Channel blacklisting*
- *LBT Disable (Listen Before Talk)*
  - *LBT may be required due to regulations, policies, or coexistence with other systems*
  - *LBT is configurable in ISA100 Wireless*
  - *Regulations and/or policies may allow LBT to be disabled only at reduced power*
- *Diagnostics!!!*
  - *For example, LBT backoff counts*
- *Proven in Use*

Some Other Considerations

Gateway-Host Communications

- *Use well-known standards for Gateway-Host communications*
- *Security considerations for Gateway (ISA99)*

Alarm Management

- *General ISA18 considerations apply*
- *Large numbers of wireless devices may raise concerns about alarm floods*

Battery Management

- *Battery life should exceed instrument's natural service interval*
- *Avoid network configurations and processes that randomize battery life*

Data Quality Diagnostics

- *Early detection and prevention of stale data conditions*
- *Include information about health & timeliness of wireless sensor data*
- *General device diagnostics*

Network Diagnostics

- *Include ample margin in the wireless design.*
- *Real-time recovery from reduced margin, while meeting availability targets.*
- *Diagnostics, HMI, processes for systematic loss of margin.*

Questions and Discussion