Introduction to ISA100 Wireless

Jay Werb

WCI Technical Director

3 October 2017

Presenter

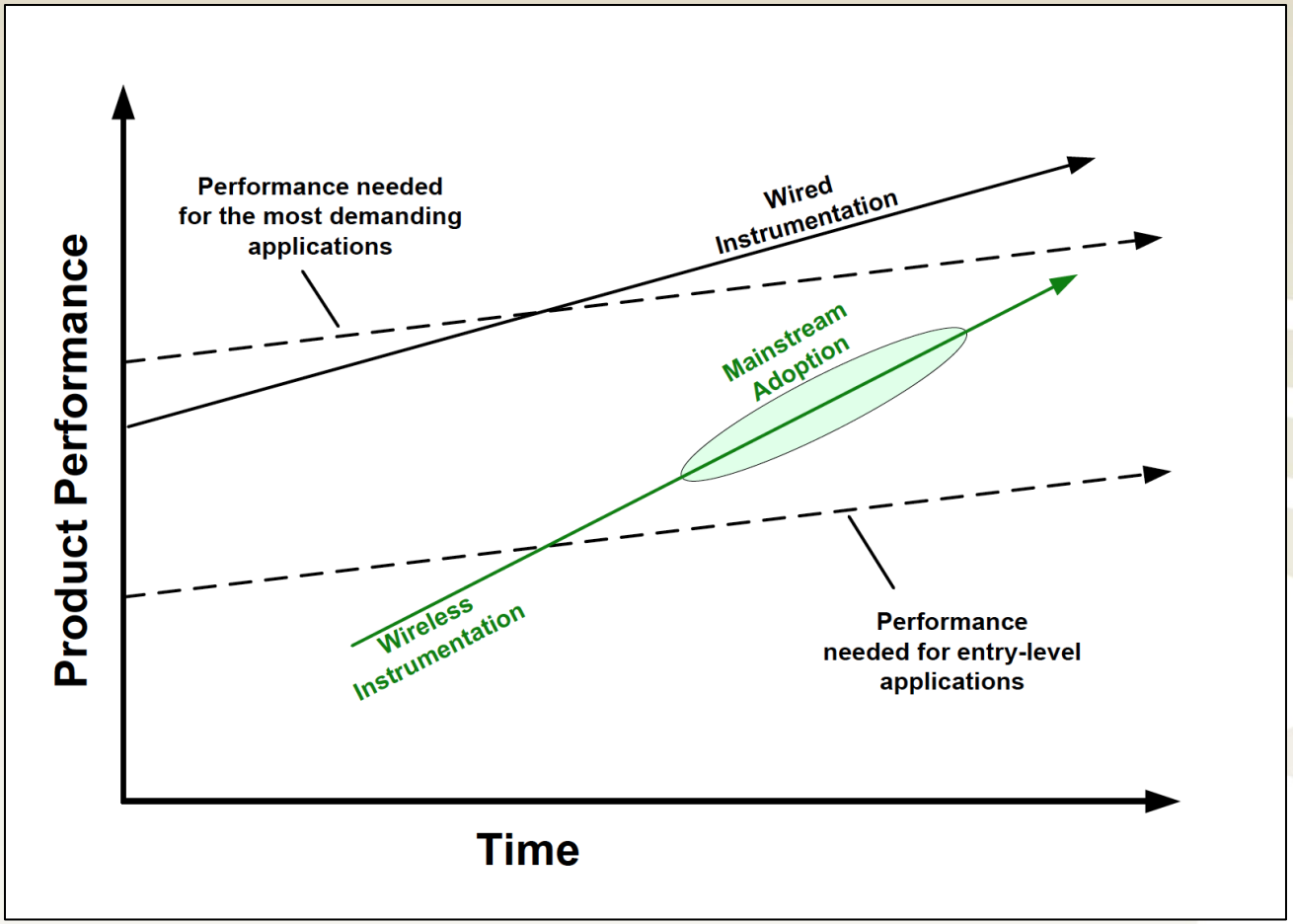
Jay Werb
Technical Director
WCI

Introduction to ISA100 Wireless

- Adoption of Industrial Wireless Instrumentation
  - *Usage Classes*
- Applications
- Network Architecture
- Overview of IEC 62734 standard

- Postscript: Wireless for Safety

Adoption of Industrial Wireless Classic Model



Christensen innovation model adapted for industrial wireless

Courtesy AIW LLC

Commonly Cited Benefits of Wireless Instrumentation

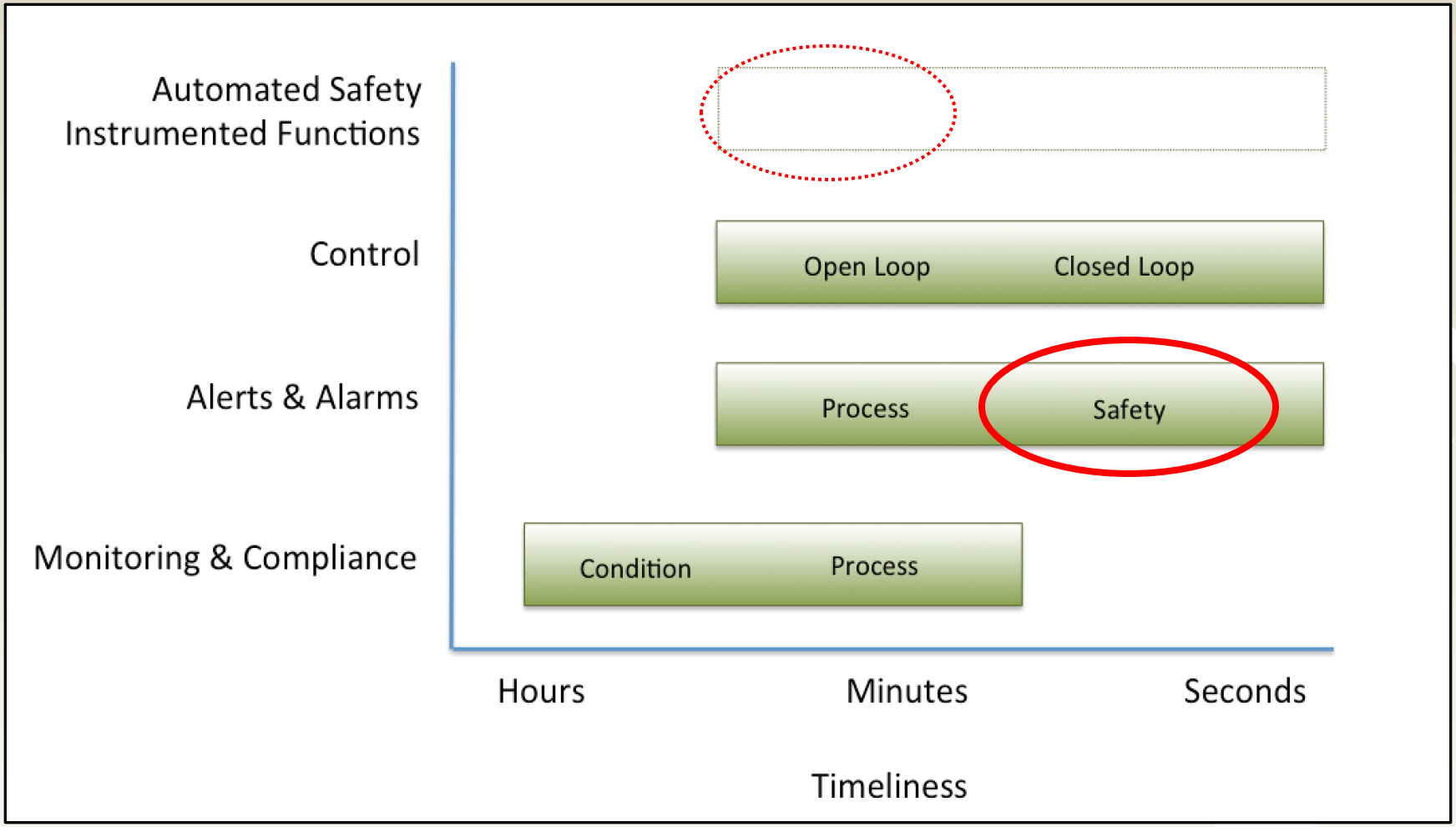
Cost Savings	• Up to 90% of installed cost of conventional measurement technology can be for cable conduit and related construction. • Typically: 1/5 the time, 1/2 the cost. • New and scaled applications are now economically feasible.
Improved Reliability	• Wired sensors may be prone to failure in difficult 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

Applications

Industrial Wireless IoT in 2017
Major Applications

- Process Monitoring & Control
- Asset Health Monitoring & Analytics
- Safety Related Alarms

Top Usage Classes for Wireless Instrumentation



Courtesy AIW LLC

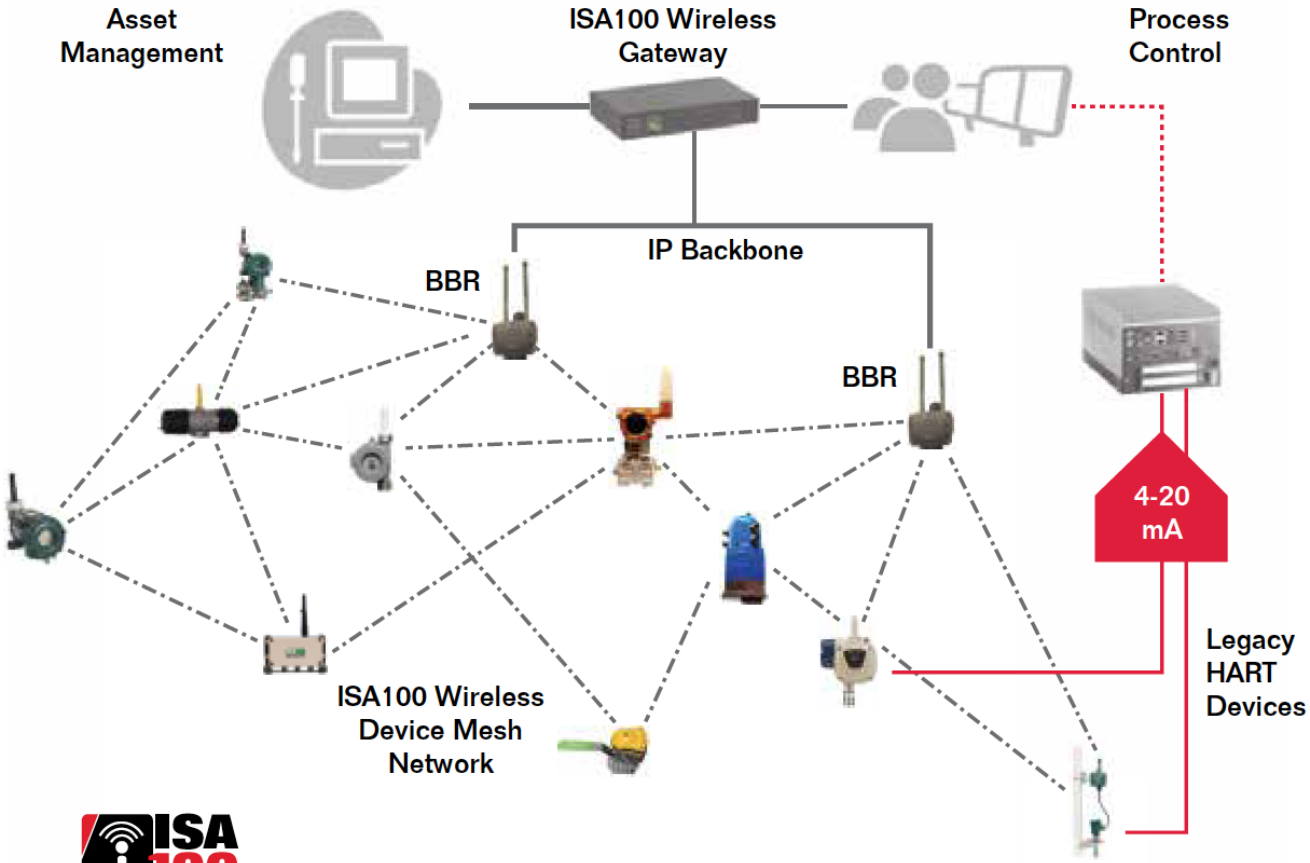
ISA100 Wireless
Major Application Types

- Asset Health Monitoring & Analytics
- Process Monitoring & Control
- Safety Alarms

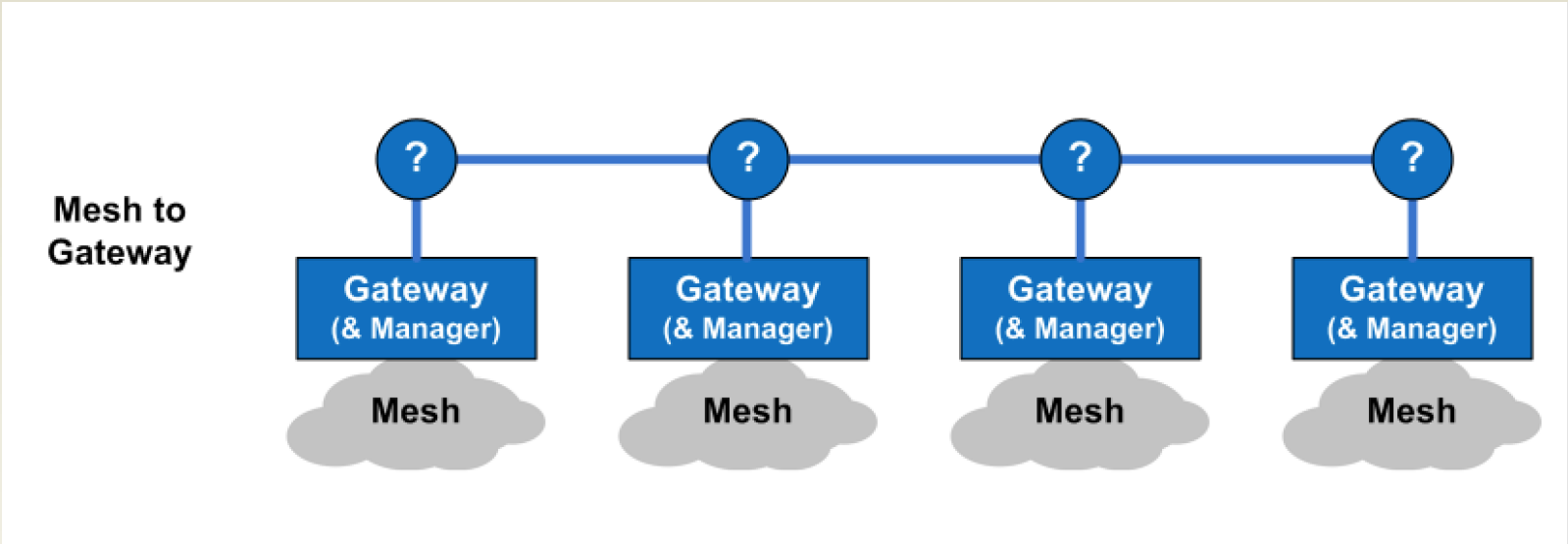
- *One network, all at the same time*

Network Architecture

Example Network

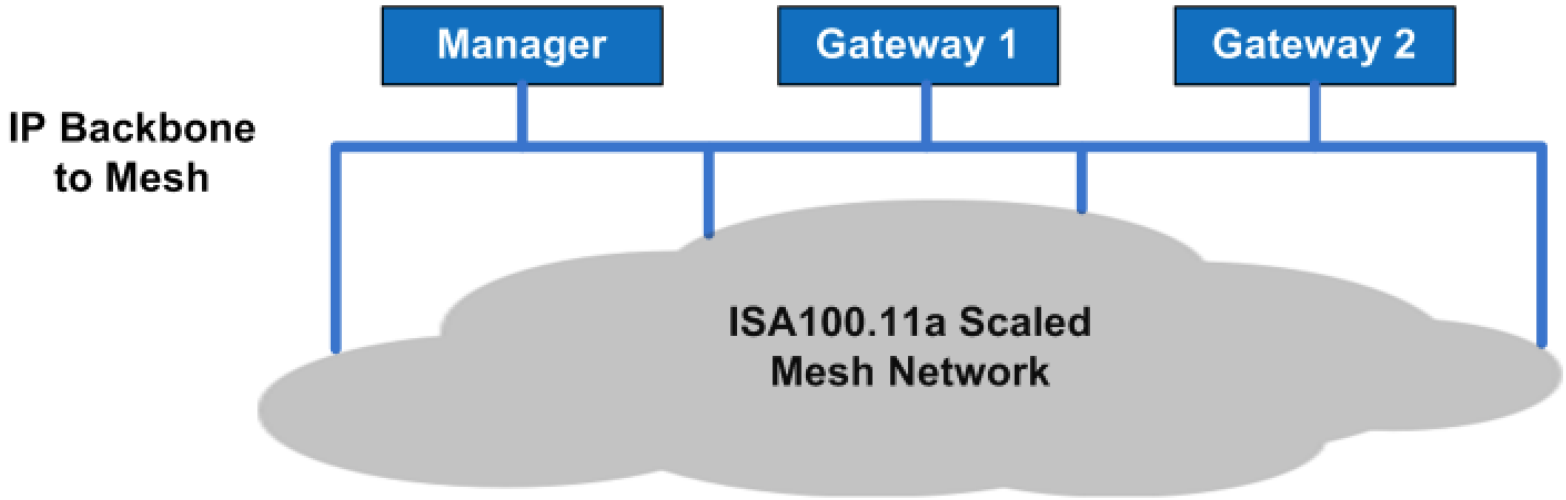


Legacy Network Architectures



Scale by Duplication

ISA100 Wireless IoT Network Architecture



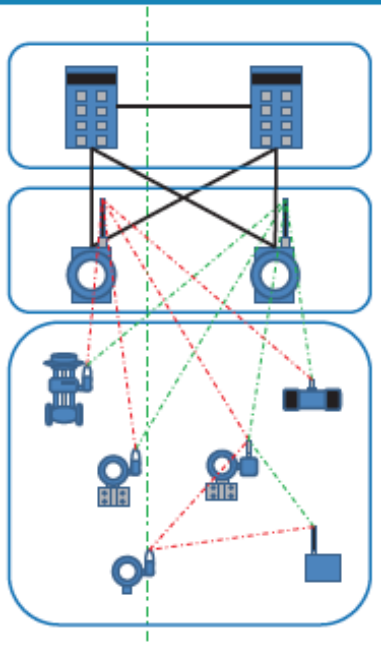
Plant-Wide Network
Scale Through IP

ISA100 Wireless Network Architecture

Redundant Gateway, System Manager, Security Manager

Redundant Access Point (Backbone Router)

Wide variety of Field Devices

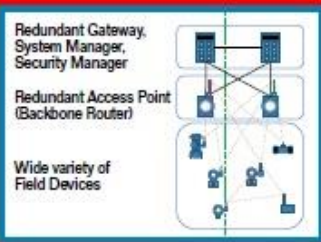


Enterprise Scalability

IPv6 to the Devices

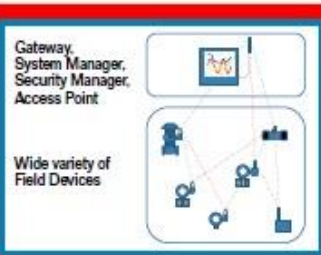
Enterprise Networks

Big Data Aggregation from Multiple Sites



Plant-wide Network

High Reliability and Availability
Duocast for redundancy
Scales to 1000s of devices

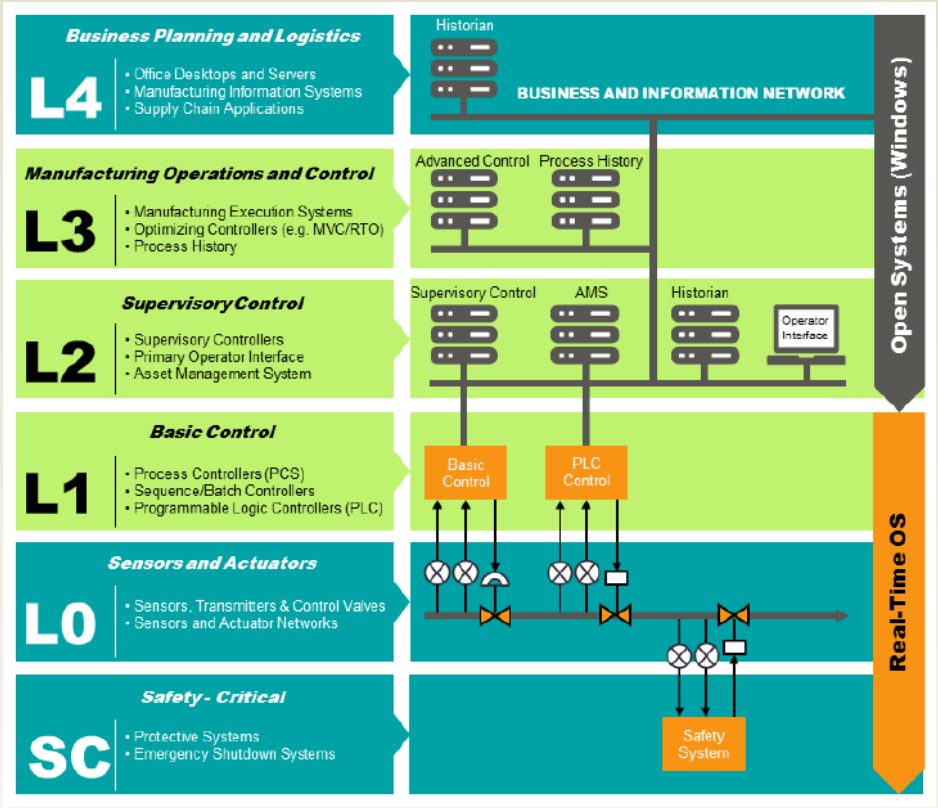


Stand Alone Network/Point Solution

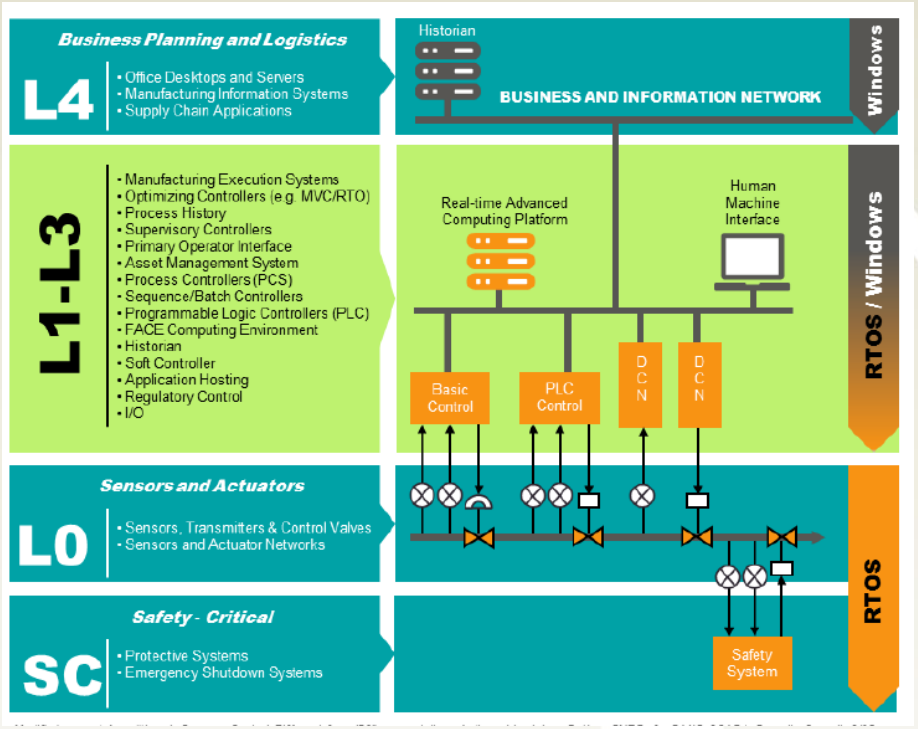
Simple and Easy
Able to Grow

Internet of Things Enables Next Generation Automation Systems

Systems Today

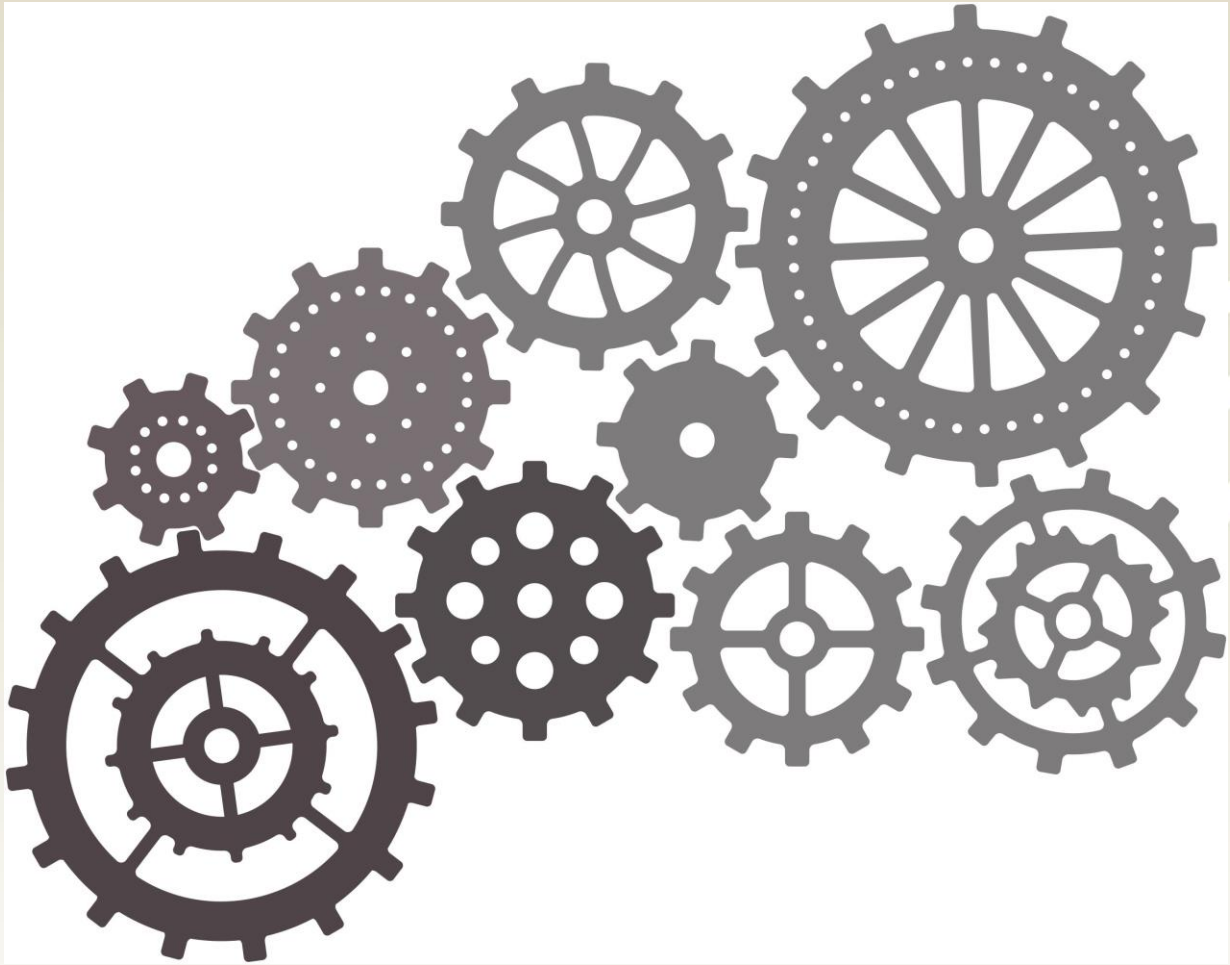


Systems Tomorrow



XOM diagrams from Lockheed Martin PIRA#OWG20161002

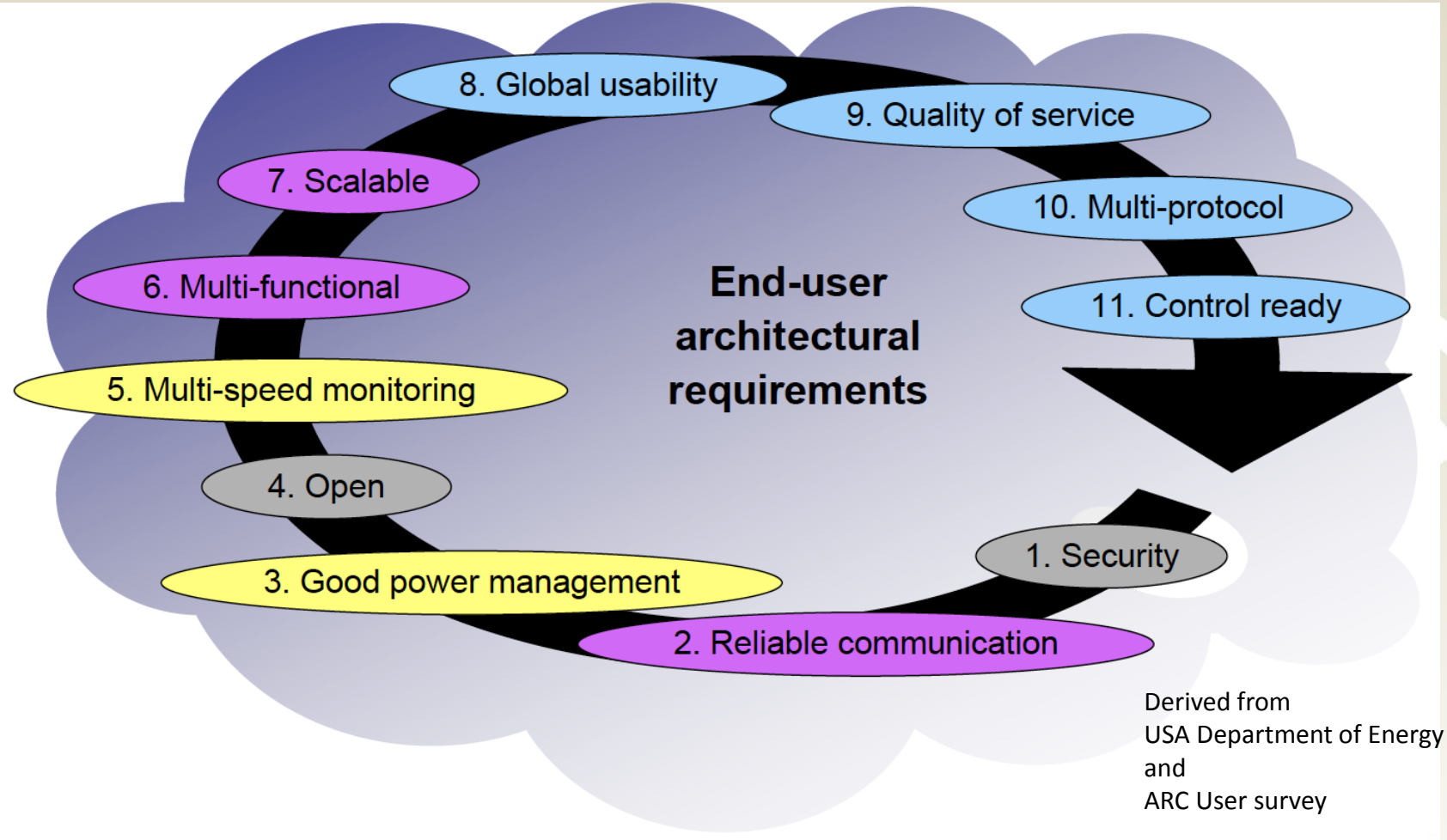
ISA100 Wireless Standard



Main Features of ISA100 Wireless

IEEE 802.15.4 Radio	• Available from multiple high quality sources.
ETSI Compliant	• Compliant to new ETSI 300.328 v1.8.1 • Various modes of compliance, described in the standard
Robust	• Advanced coexistence and resiliency mechanisms at all levels
Secure	• Two layer AES 128 cryptography
IP based	• Future Proof
Object based	• Compact and Extensible • Supports Tunneling
International Standard	• Standardized as IEC 62734

End-user requirements for Industrial wireless sensing

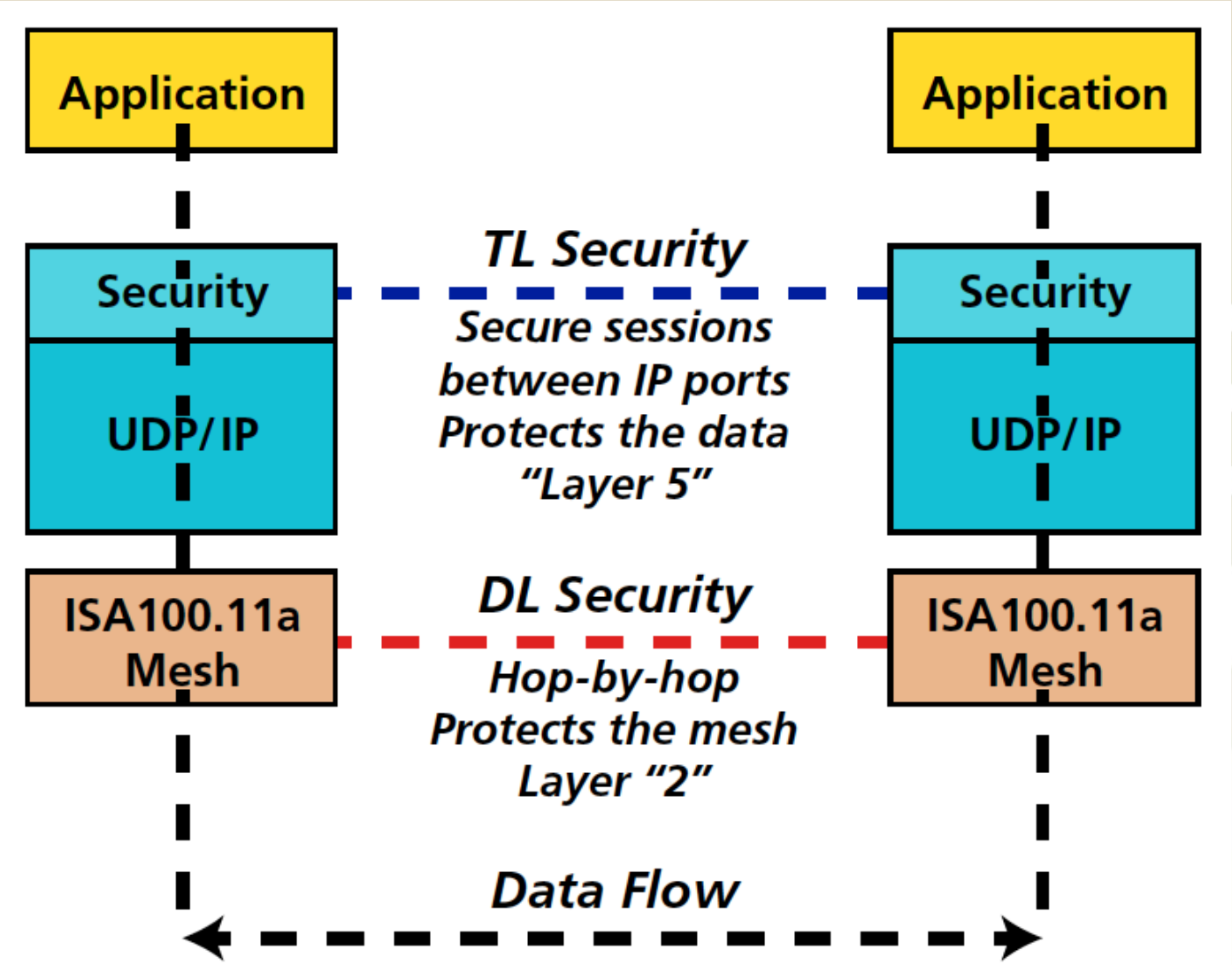


ISA100 solutions must meet all requirements simultaneously

Technical requirements for Industrial wireless sensing

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

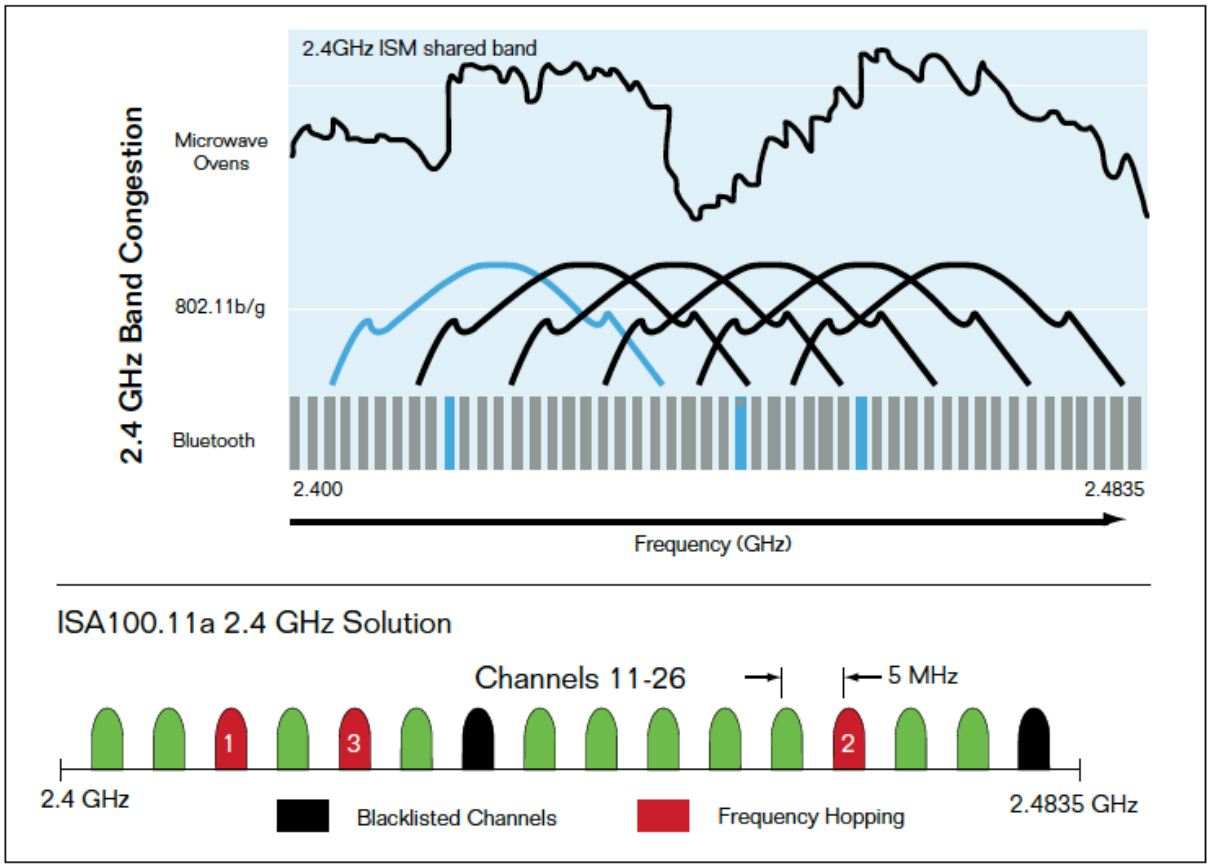
Two Levels of Security



Robust Communications

Spectrum Analysis → **System Management** → **Policy Enforcement**

Spectrum Analysis	System Management	Policy Enforcement
Identifying Interferers	Device Configuration	Channel Allocation
Monitoring Saturation	Element Provisioning	Rules Creation
	Performance Monitoring	Blacklisting

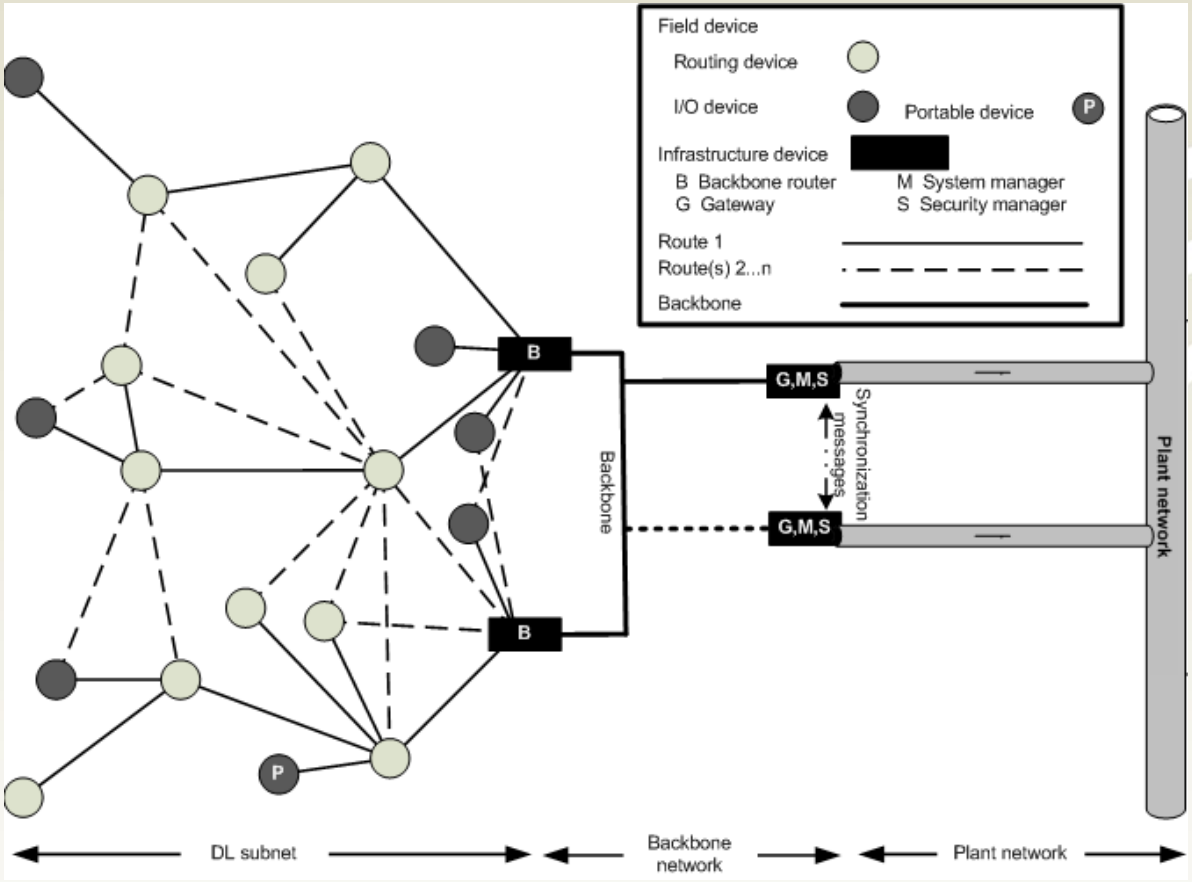


ISA100 – Ensured Coexistence with Many Wireless Networks

Conclusion

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

Postscript: Adoption of Wireless for Safety Design Principles



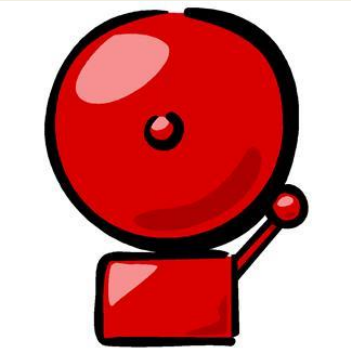
Safety Related Alarms

Applications

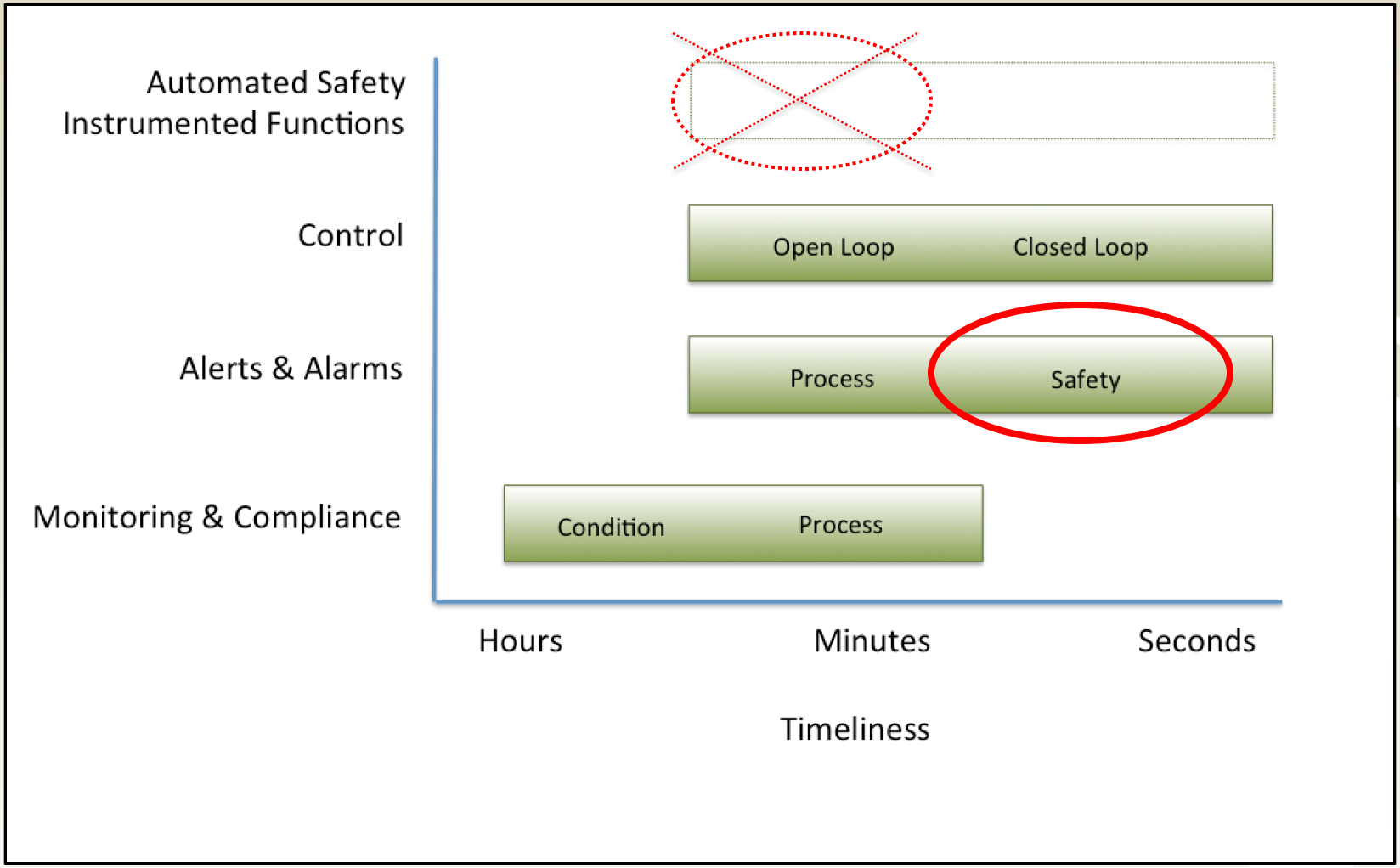
- Gas Detection
- Fire Prevention
- Level Detection
- Safety Showers
- Etc…

Wireless Requirements

- Controlled Quality of Service
  - Diagnostics!
- Low and Deterministic Latency
- Layered Open Architecture
  - e.g. ProfiSAFE



Industrial Wireless Safety Today



Courtesy AIW LLC

Adoption of Wireless for Safety Design Principles

- Latency and Availability
- Network Design Common Best Practices
- Security Matrix
- Denial of Service
- Some Other Considerations

Typical Wireless Safety Application

- *"…it is assumed that the risk analysis team has already determined that the protection layer comprised of an **alarm with operator action generated from a wireless transmitter** meets the specificity and independence criteria."*

- *"…**Risk reduction claimed is less than or equal to 10**."*

From ISA84 WG8 draft.

Latency, Availability

Latency

- *"Wireless sensor network data latency is the time between the acquisition of a measurement value and the delivery of that data via the wireless network to a gateway." (ISA84 WG8 draft)*

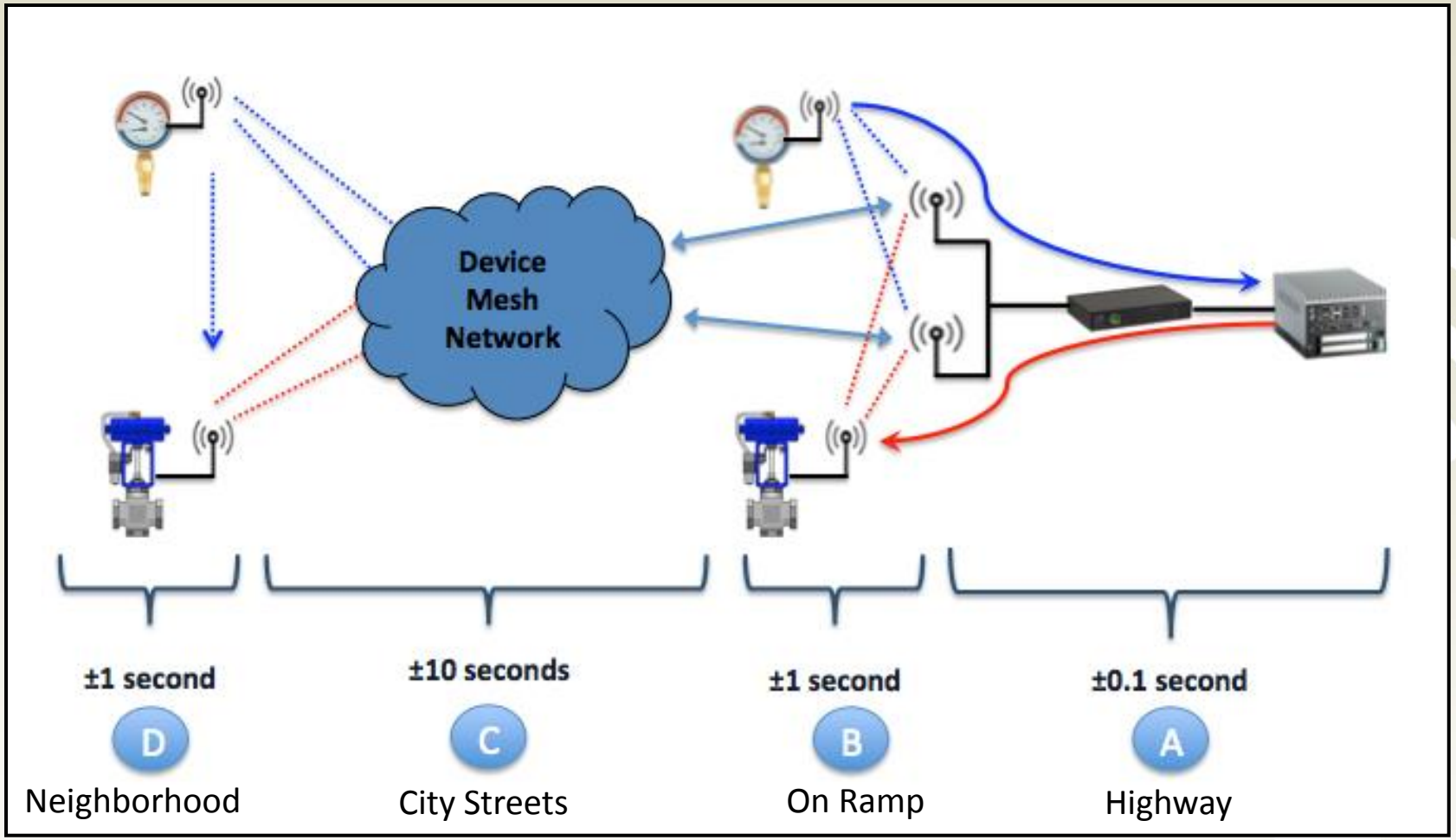
Availability

- Percentage of values received within the required response time. Can be measured per device or for an overall system.

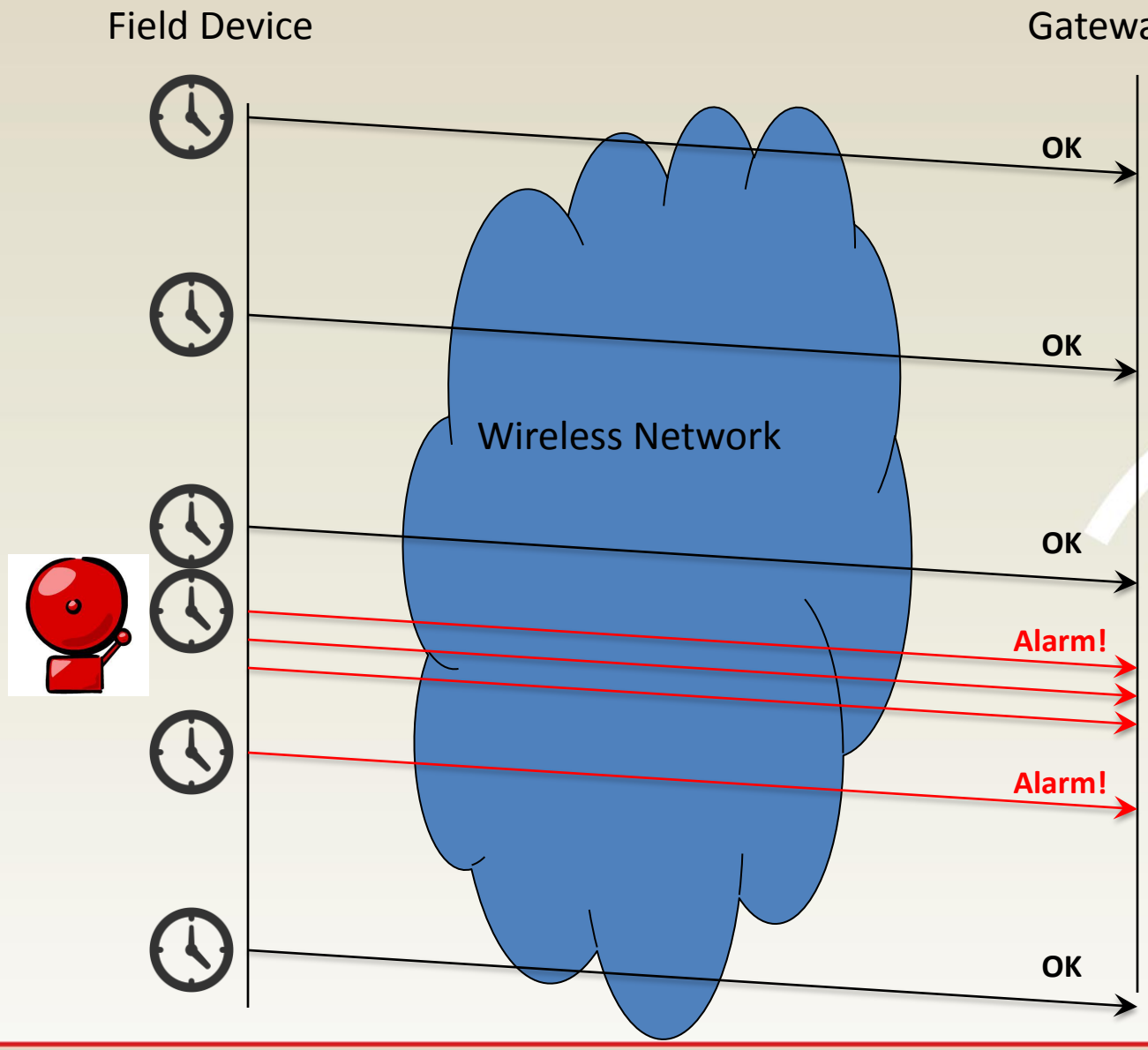
Sidebar

- An exception may be a late-arriving alarm, or a stale state.
- Be alert for freshness requirements at times when there is no alarm.

Mesh Networks
Latency Considerations



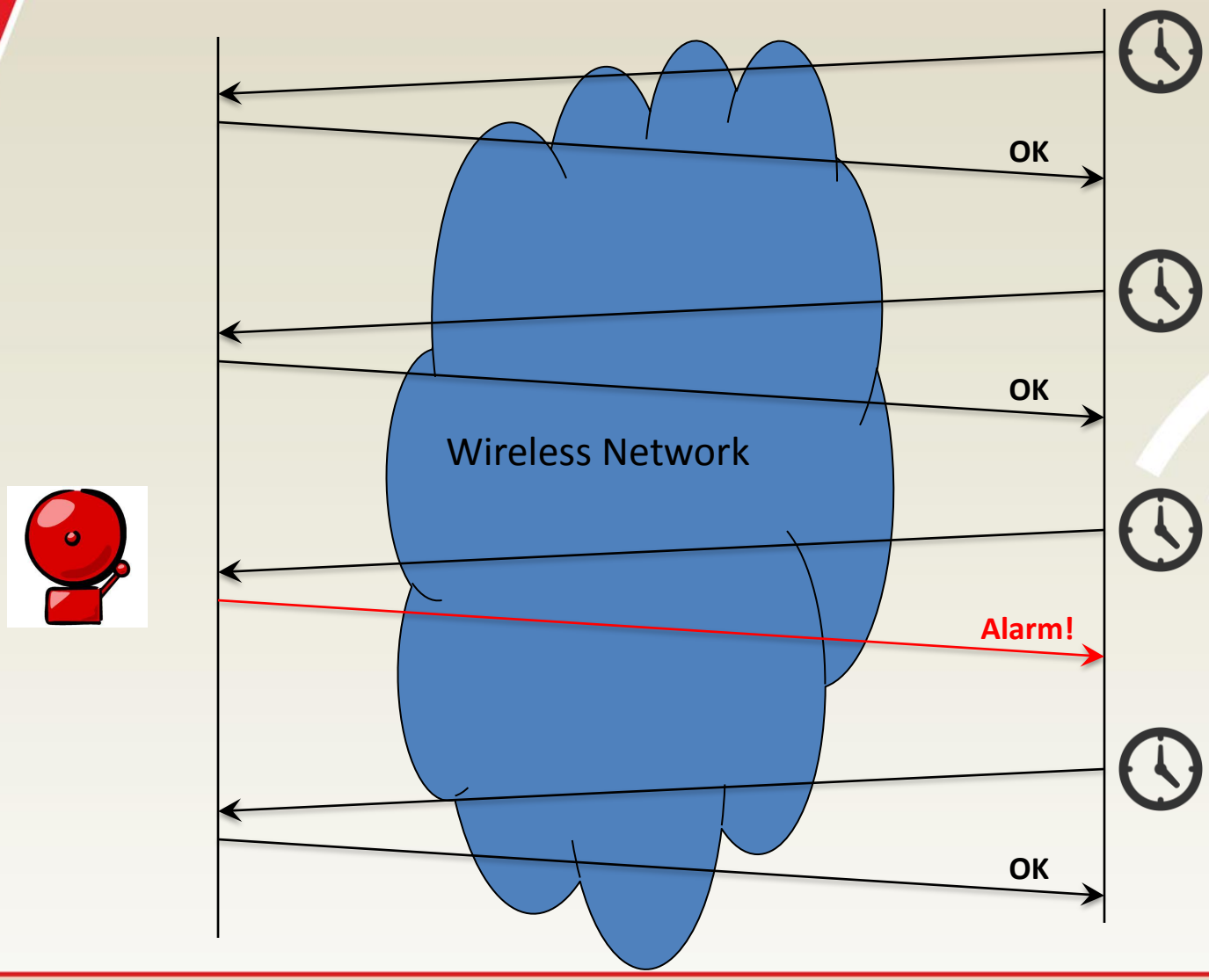
Publication



Wireless publications are commonly acknowledged hop-to-hop, but not end-to-end.

Rely on field device's clock for timestamp, freshness, etc.

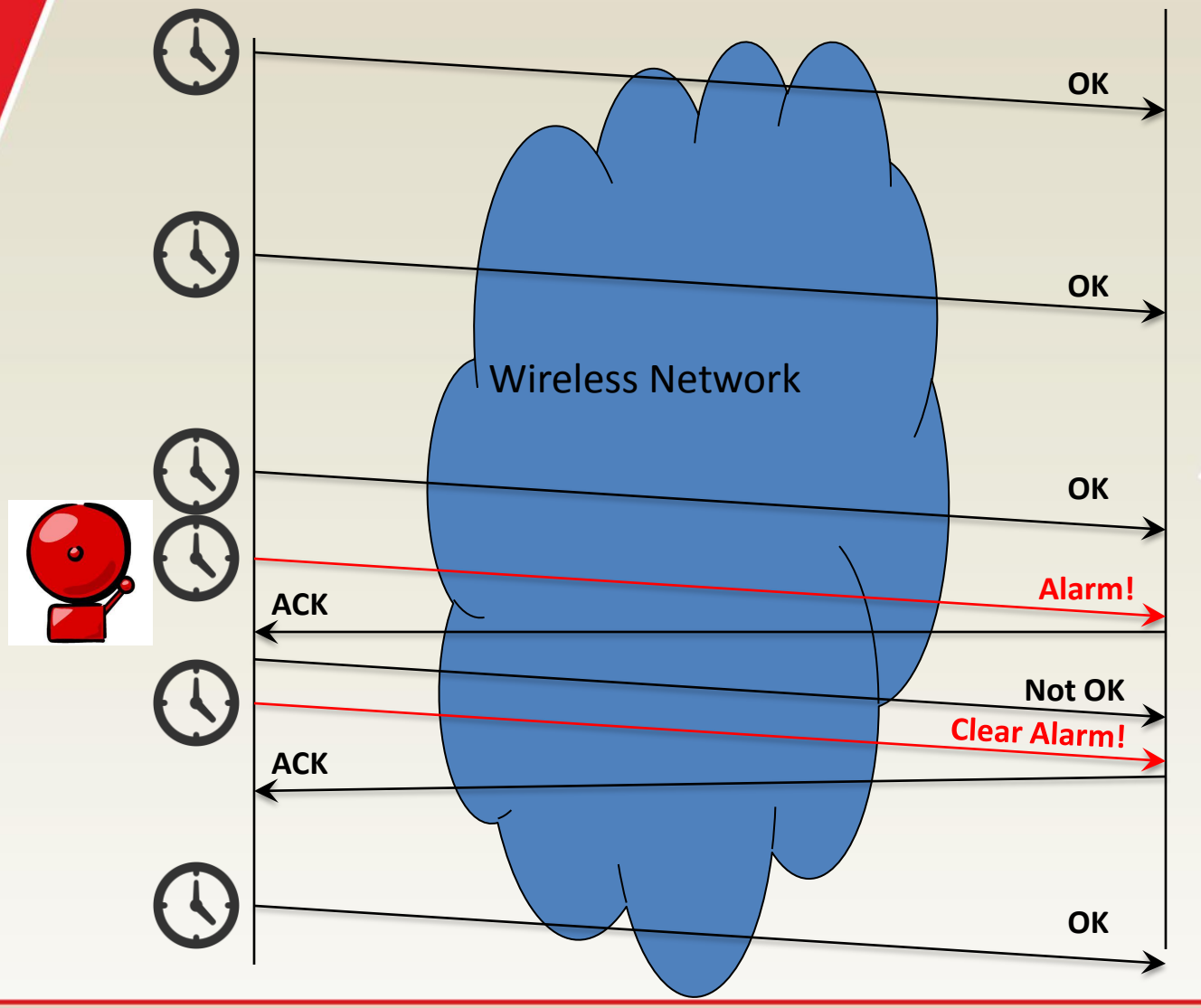
Request-Response



Wireless may be considered a black channel.

Timestamp, freshness, etc are based on interrogation clock in this diagram.

Hybrid (Example)



Publish heartbeat periodically.

Alarms are transmitted immediately. Acknowledged by gateway to squelch re-transmission.

Network Design
Common Best Practices

*"… it is critical to closely **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.

Derived from ISA84 WG8 draft.

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 generally features of an interoperable communication standard such as ISA100 Wireless. User should not be able to disable or mis-apply these features.

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

Similar table is in ISA84 WG8 draft.

Denial of Service

Radio standards and implementations should 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.*

Adoption of Wireless for Safety Summary

Cost savings from wireless enable scaled adoption of safety applications

ISA100 Wireless is commonly used today for safety related alarms

Proven in use, following manufacturer best practices

(Not covered here: SIL-2 ratings should accelerate integration with safety systems)

Questions?