Adoption of Wireless for Safety

Jay Werb
Technical Director
ISA100 Wireless Compliance Institute
Questions and comments to: jayw@isa100wci.org

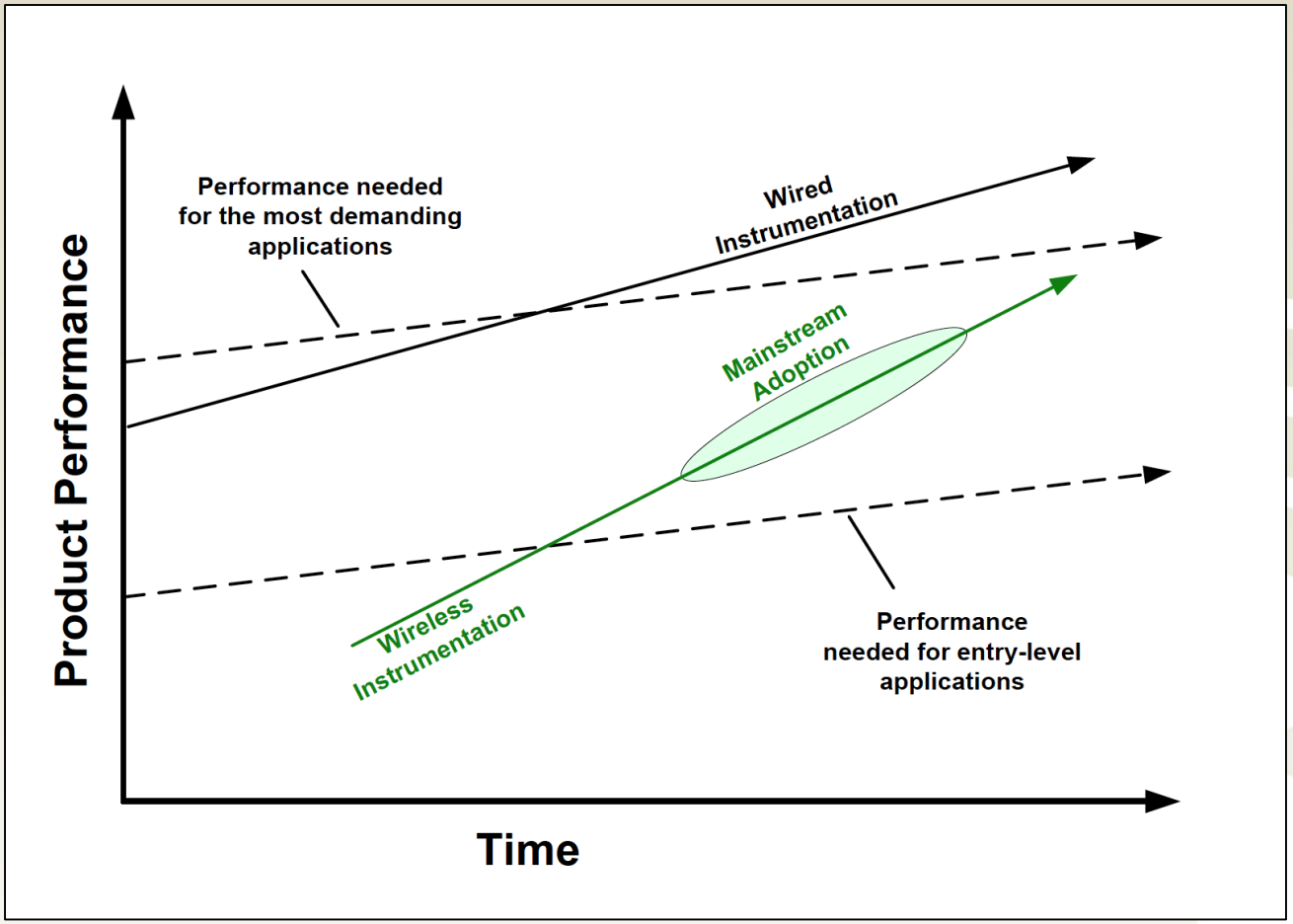
Presenter

Jay Werb
Technical Director
WCI

Adoption of Wireless for Safety Presentation Overview

- **Adoption of Industrial Wireless in General**
  - *Usage Classes*
- **Design Principles for Wireless Safety**
  - *Loosely Derived from ISA84 WG8 Draft*
- **Q & A**

Adoption of Industrial Wireless Classic Model



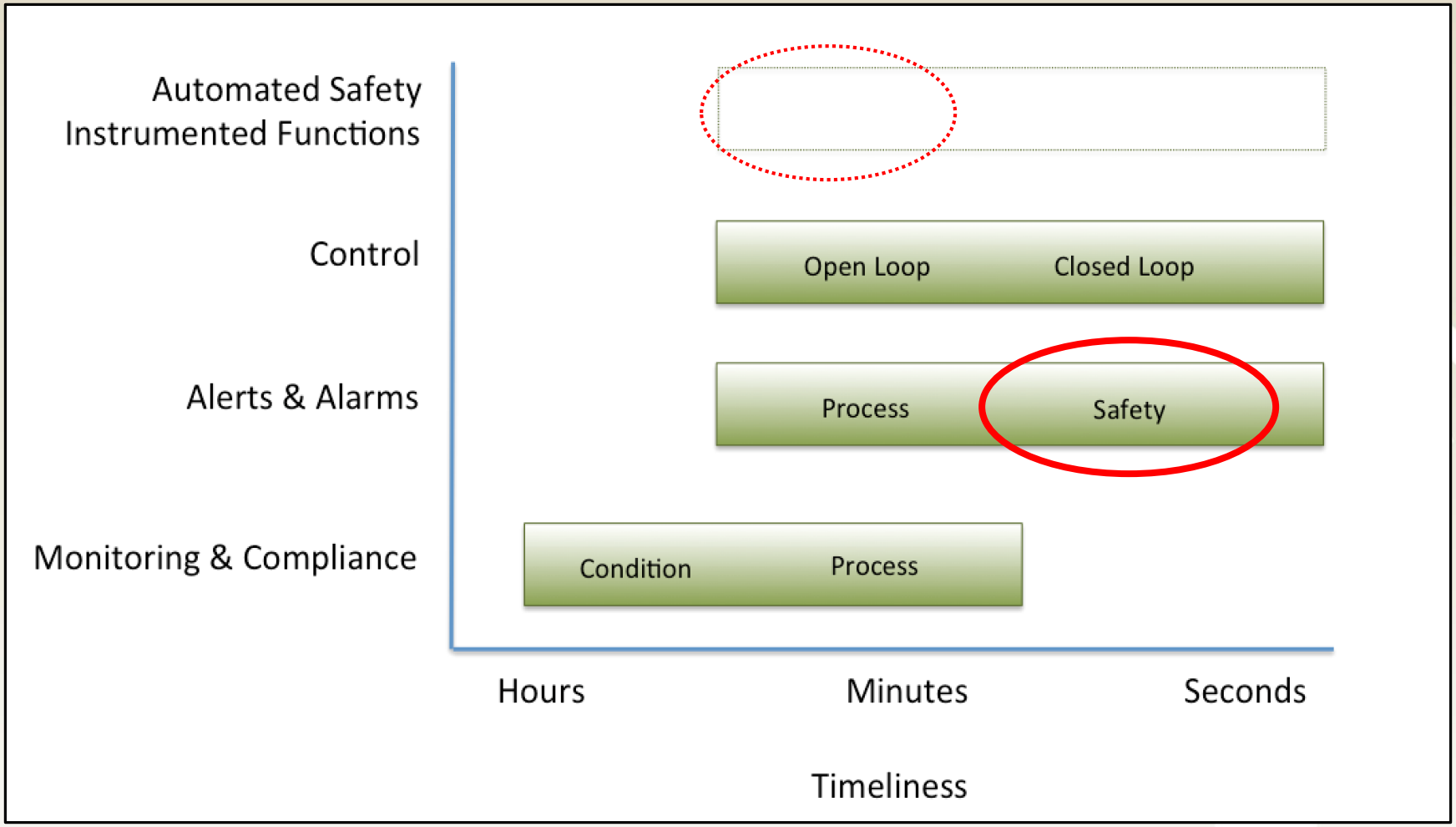
Christensen innovation model adapted for industrial wireless

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

Top Usage Classes for Wireless Instrumentation



Courtesy AIW LLC

Industrial Wireless in 2016
Major Applications

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

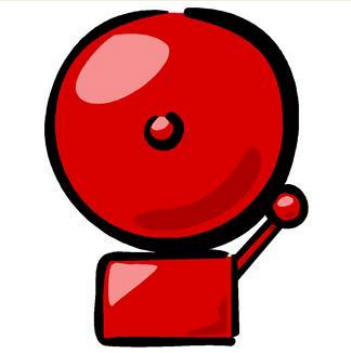
Safety Related Alarms

Applications

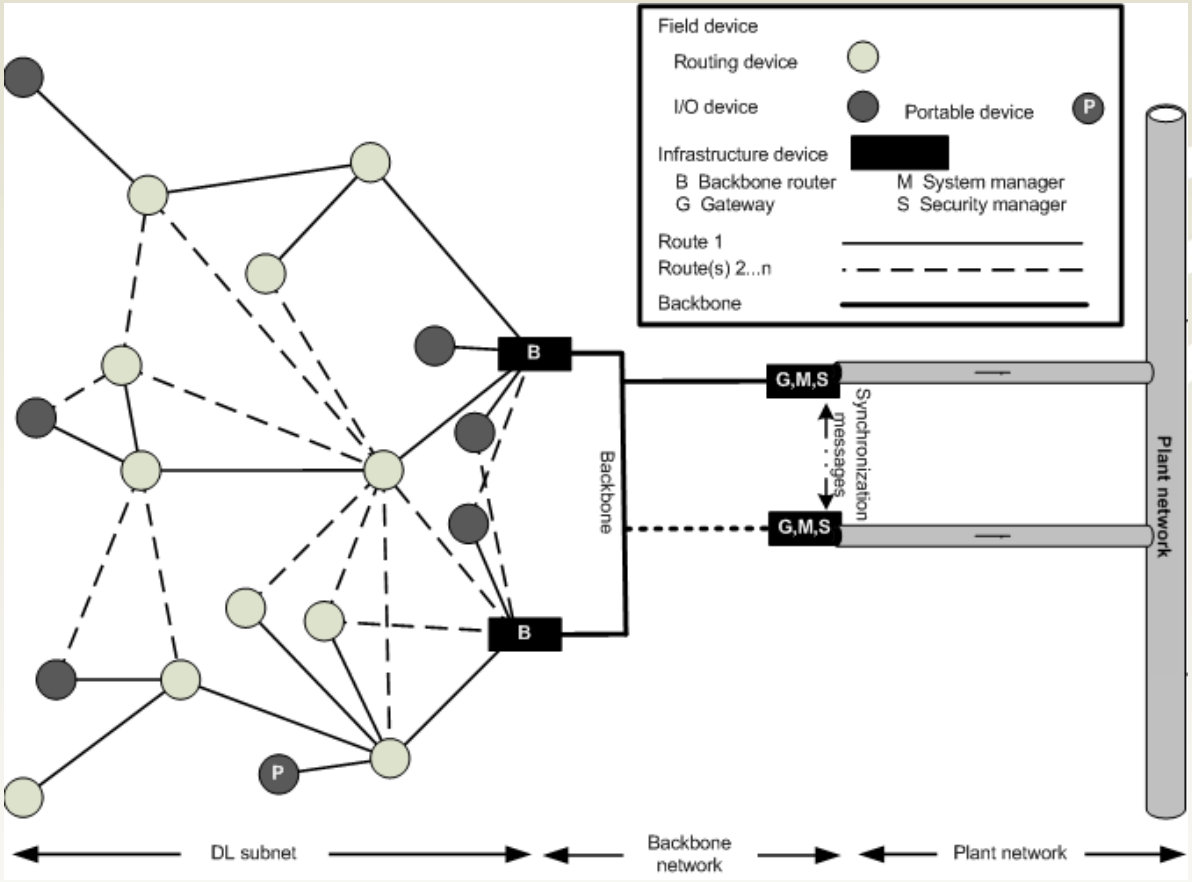
- Gas Detection
- Fire Prevention
- Level Detection
- Safety Showers
- Etc…

Wireless Requirements

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



Adoption of Wireless for Safety Design Principles



Adoption of Wireless for Safety Design Principles

- ISA84 WG8 (Draft)
  Purpose and Focus of the Technical Report
- Latency and Availability
- Network Design Common Best Practices
- Security Matrix
- Denial of Service
- Some Other Considerations

The following slides are derived from recent ISA84 WG8 drafts, and other materials.
This is not intended as a summary of ISA84 WG8.
Emphasis and summaries might not match WG intent.

ISA84 WG8
Draft Technical Report

Title

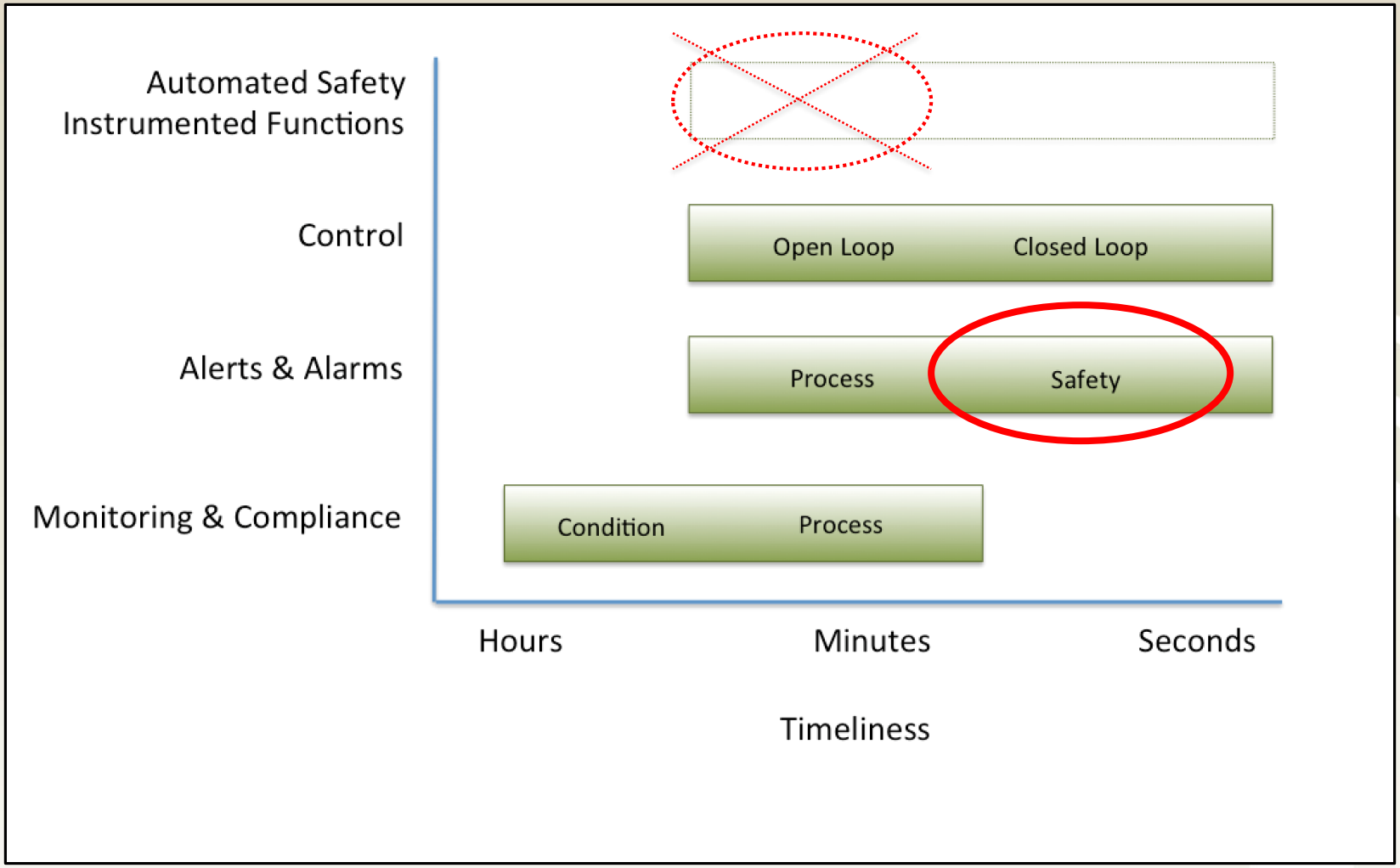
Guidance for Application of Wireless Sensor Technology
To ***Non-SIS Independent Protection Layers***

Purpose

- *"This Technical Report was developed to document guidance and considerations to users for application and implementation of wireless sensor technologies for fully non-Safety Instrumented System (SIS) process Independent Protection Layers (IPL).* ***The guidance provided is not intended for the use of wireless as a Safety Instrumented Function (SIF).****"*

- *"This TR provides guidance to demonstrate the wireless system is sufficiently robust to support meeting the requirements of a Non-SIS Independent Protection Layer."*

Scope of ISA84 WG8



Courtesy AIW LLC

ISA84 WG8 Focus

- *"For the purposes of this Technical Report 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. Instead the Technical Report will focus on providing information on **how to establish a design that satisfies the dependability and auditability criteria** for an alarm with operator action that is generated from a wireless transmitter. "*

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

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."*

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.

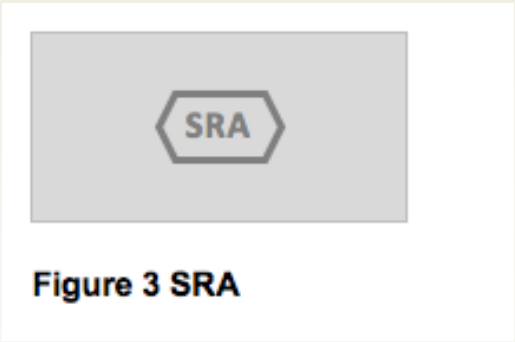
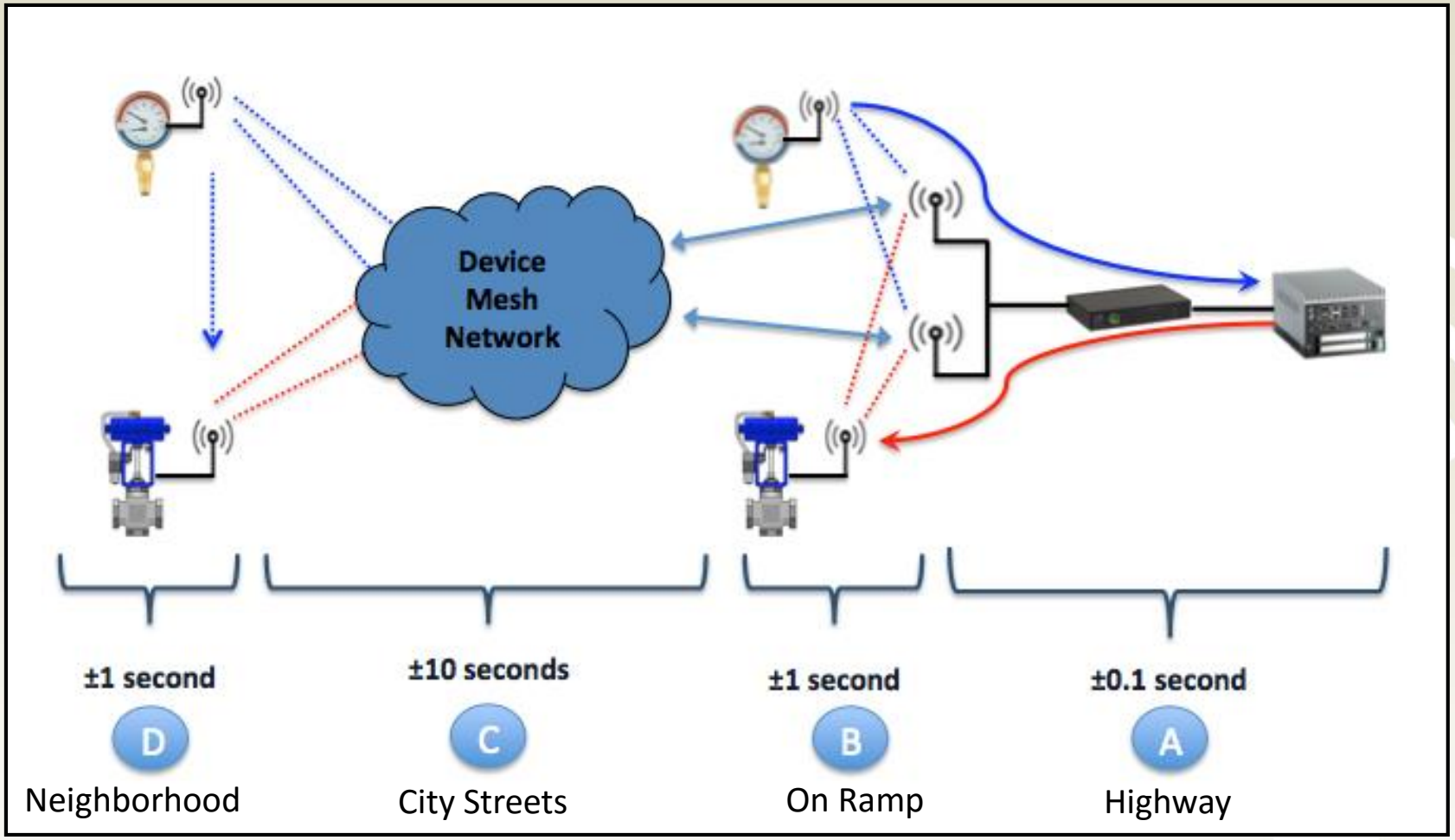


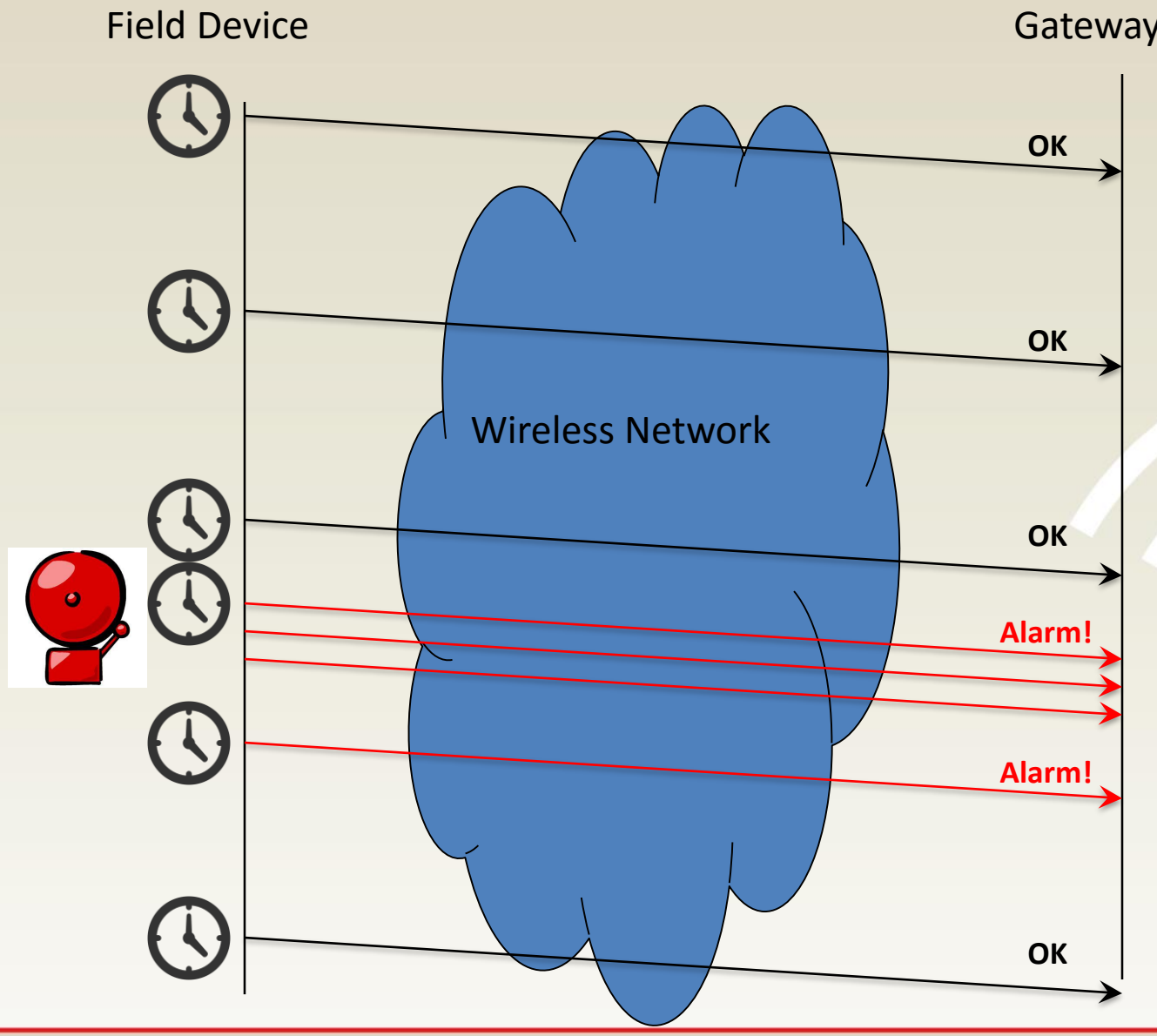
Figure 3 SRA

Figure 4 Unavailable SRA

Mesh Networks
Latency Considerations



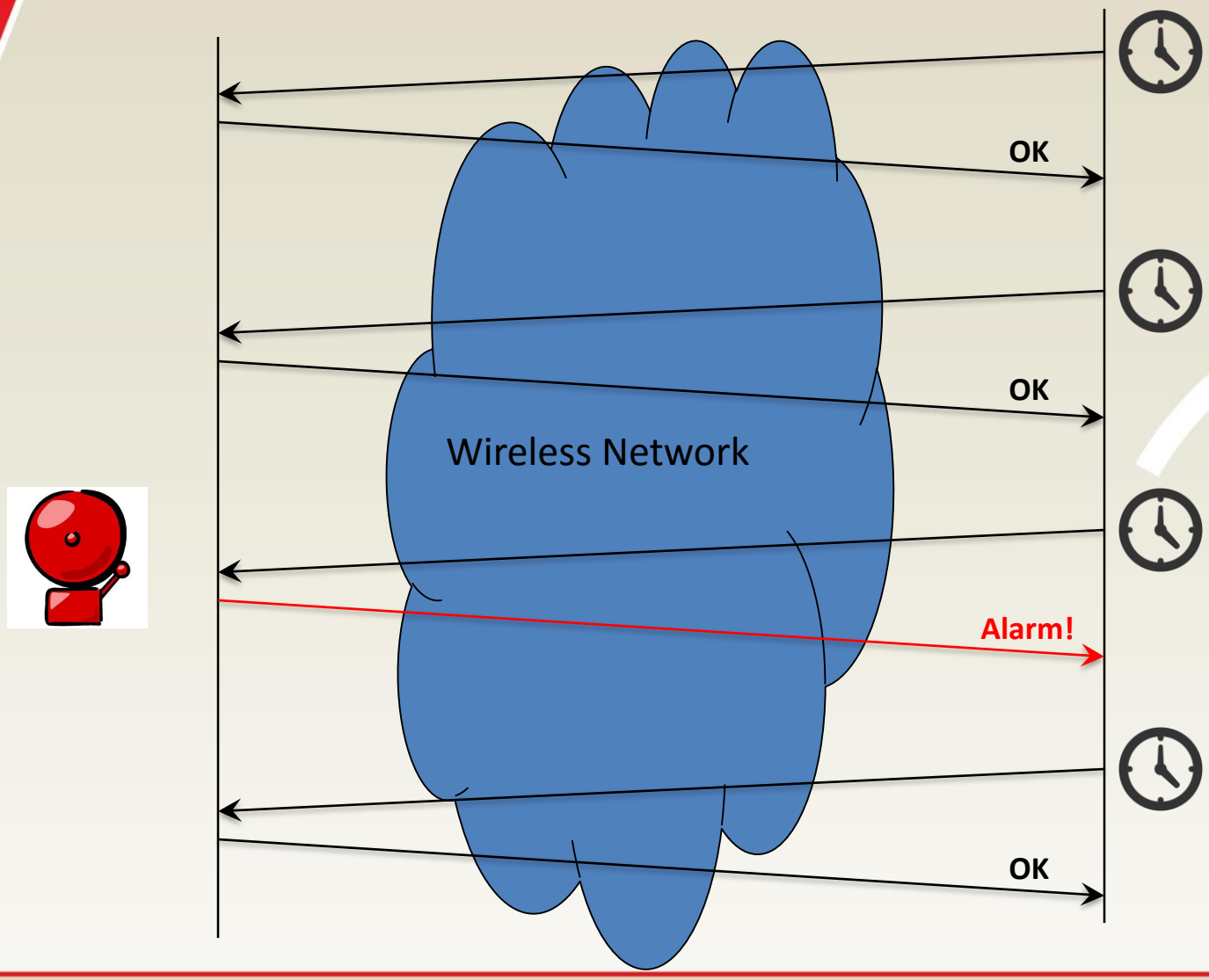
Publication



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

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

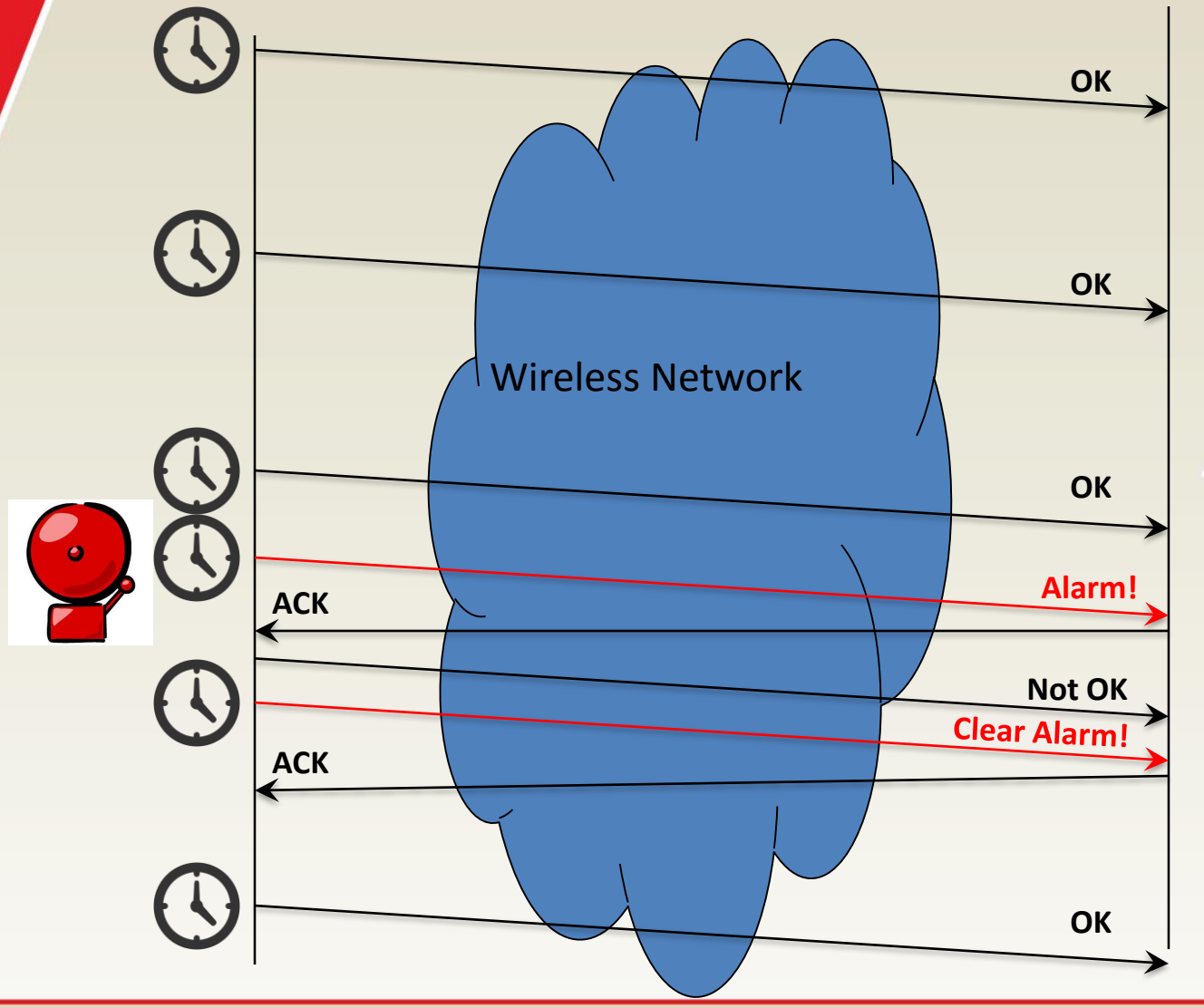
Request-Response



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.*

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?