

ISA100 Wireless Compliance Institute

The Technology Behind ISA100.11a User Driven Design



Copyright ©2010
ISA100 Wireless Compliance Institute
All rights reserved

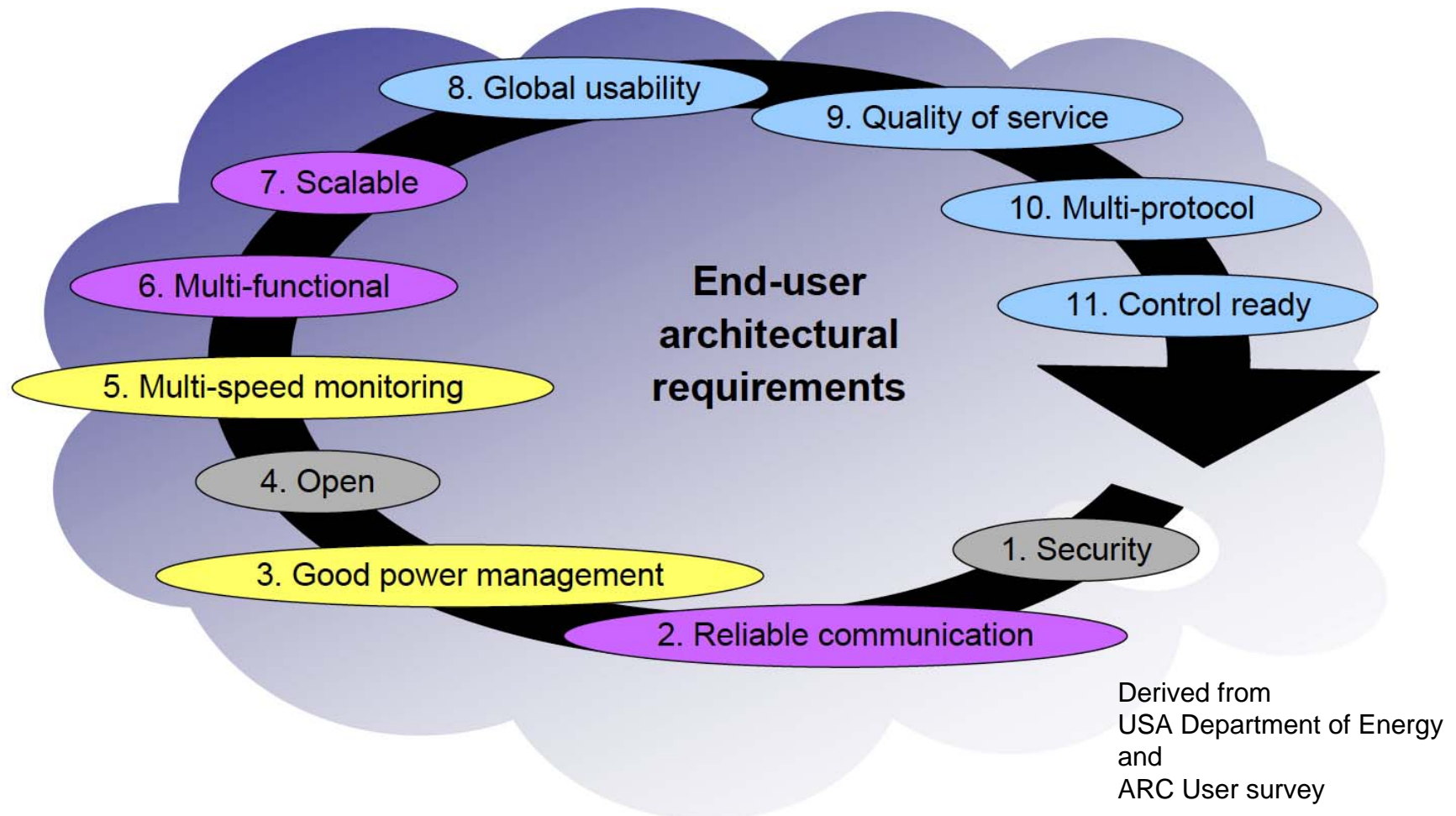
Jay Werb
Technical Director, WCI
jwerb@isa.org

Agenda

- Voice of the customer
- Not just monitoring
- Architecture leverages IP
- State of the art, flexible mesh
- Control ready application layer
- Reprise: Voice of the customer

Voice of the customer

Core user requirements for wireless sensing



ISA100 solutions must meet all requirements simultaneously

Voice of the customer

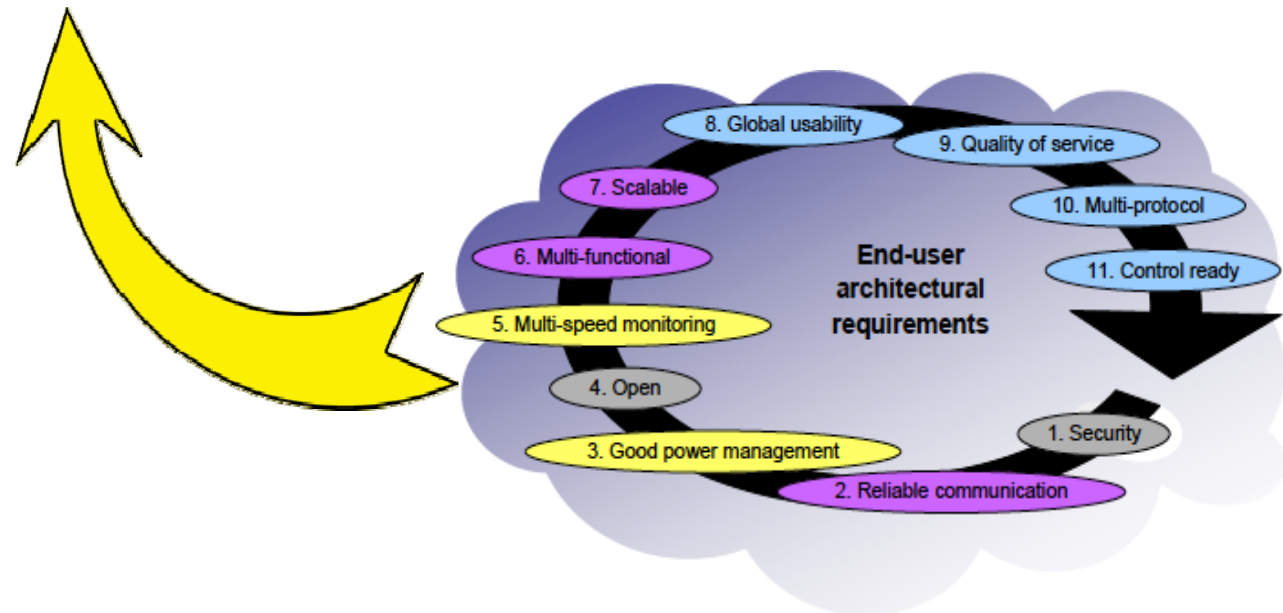
Core user requirements for wireless sensing

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
Global Usability	One technology legal everywhere
Quality of Service	Controlled latency, low error rate
Multi-protocol	Cleanly integrate with wired investment
Control ready	Solves real problems, Day One

Focus for today

ISA100.11a:

- ✓ Covers a broad range of applications, worldwide
- ✓ State-of-the-art mesh fully integrated with standard IP
- ✓ Powerful, flexible, and extensible application layer



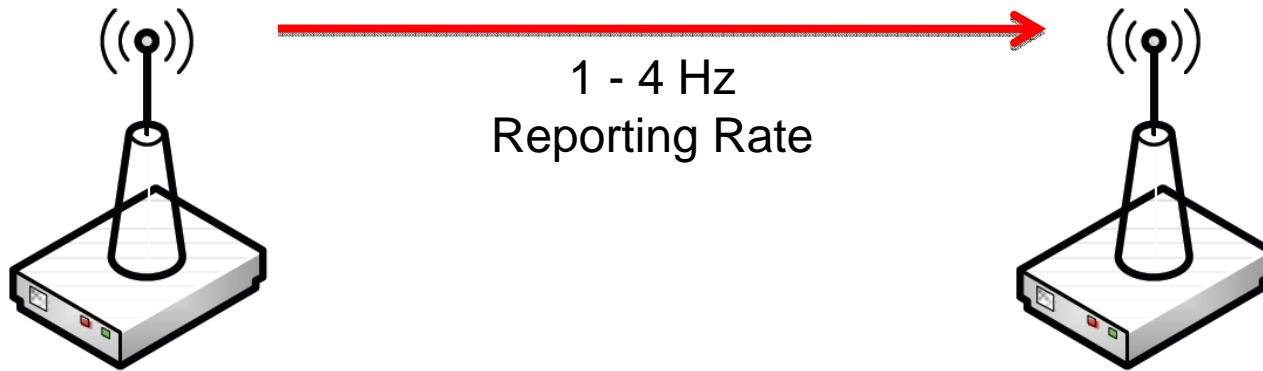
One Network, Multiple Applications



It's never just one thing

ISA100.11a

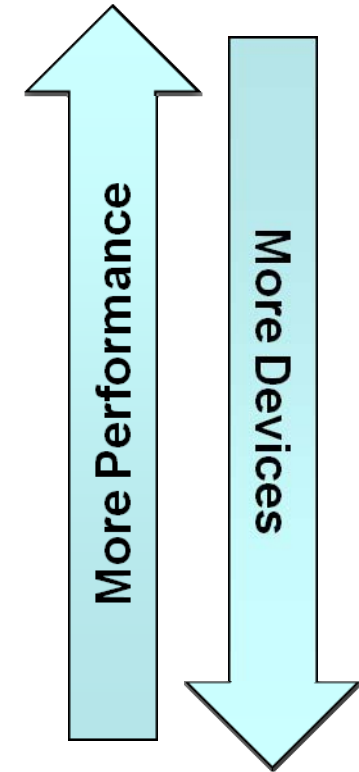
Not just monitoring



ISA100.11a

Usage classes and scalability

Safety	0	Emergency action	Always critical
Control	1	Closed loop Regulatory control	Often critical
	2	Closed loop Supervisory control	Usually non-critical
	3	Open loop control	Human in the loop
Monitoring	4	Alerting	Short-term consequences
	5	Logging Downloading/uploading	No immediate consequences



ISA100.11a

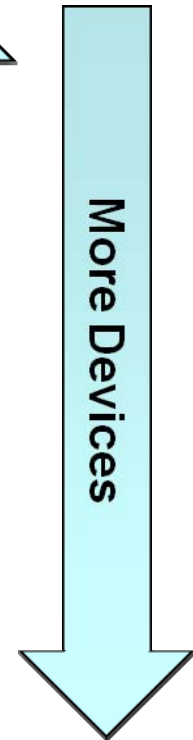
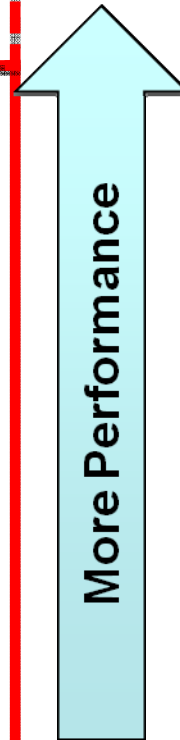
Usage classes, examples listed in standard

Safety	0	Emergency action	Always critical	Safety interlock Emergency shutdown Automatic fire control
Control	1	Closed loop Regulatory control	Often critical	Control of primary actuators High frequency cascades
	2	Closed loop Supervisory control	Usually non-critical	Low frequency cascade loops Multivariable controls Optimizers
	3	Open loop control	Human in the loop	Manual flare Remote opening of security gate Manual pump/valve adjustment
Monitoring	4	Alerting	Short-term consequences	Event-based maintenance Battery low indicator Asset tracking
	5	Logging Downloading/ uploading	No immediate consequences	History collection Preventative maintenance rounds Sequence of events (SOE) reporting

ISA100.11a

Not just monitoring

Safety	0	Emergency action	Always critical
Control	1	Closed loop Regulatory control	Often critical
	2	Closed loop Supervisory control	Usually non-critical
	3	Open loop control	Human in the loop
Monitoring	4	Alerting	Short-term consequences
	5	Logging Downloading/uploading	No immediate consequences



“Classes 1 through 5 and optionally class 0.”

“Periodic monitoring and process control where latencies on the order of 100 ms can be tolerated, with optional behavior for shorter latency.”

Broad range of applications

Multi-speed and Multi-functional

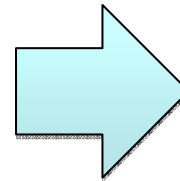
- Major end-users have expressed a need for a coherent, standards-based wireless solution that supports instruments used for:
 1. Manual or automated monitoring where there is not a need for timely data or alarming;
 2. Automated monitoring where timely data and/or alarm reporting is essential;
 3. Automated control; and
 4. Occasionally, safety... because many sites have a combination of the above.

Broad range of applications

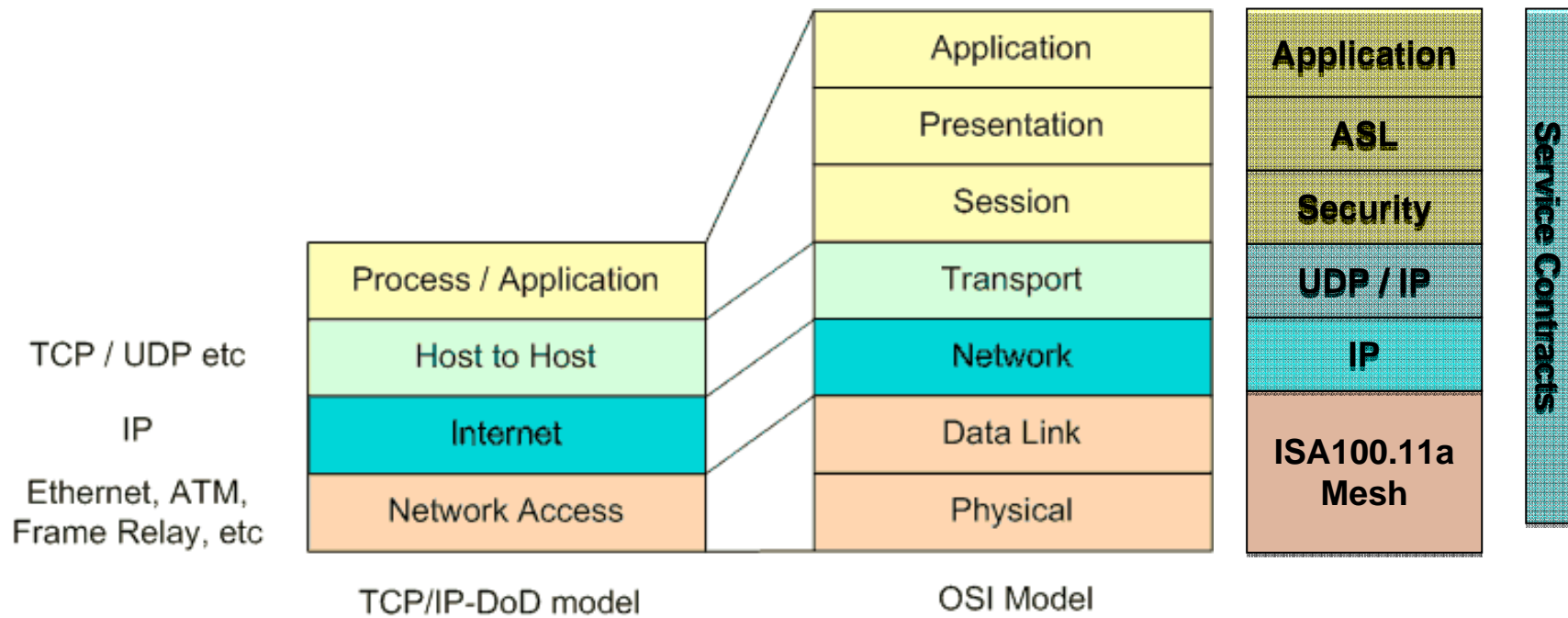
Multi-speed and Multi-functional

- Typically, the number of devices is higher for monitoring, but the architecture needs to accommodate all classes at the same time.
- The architecture needs to be highly scalable to support:
 1. High numbers of devices (1,000s of monitoring points per site)
 2. High performance in a subset of devices (1+ Hz, high QoS)
 3. Economies of scale (“Lick and stick”)
 - Networks need to be manageable, particularly as they scale
- One network performs all functions at scale
 - Leveraging IP

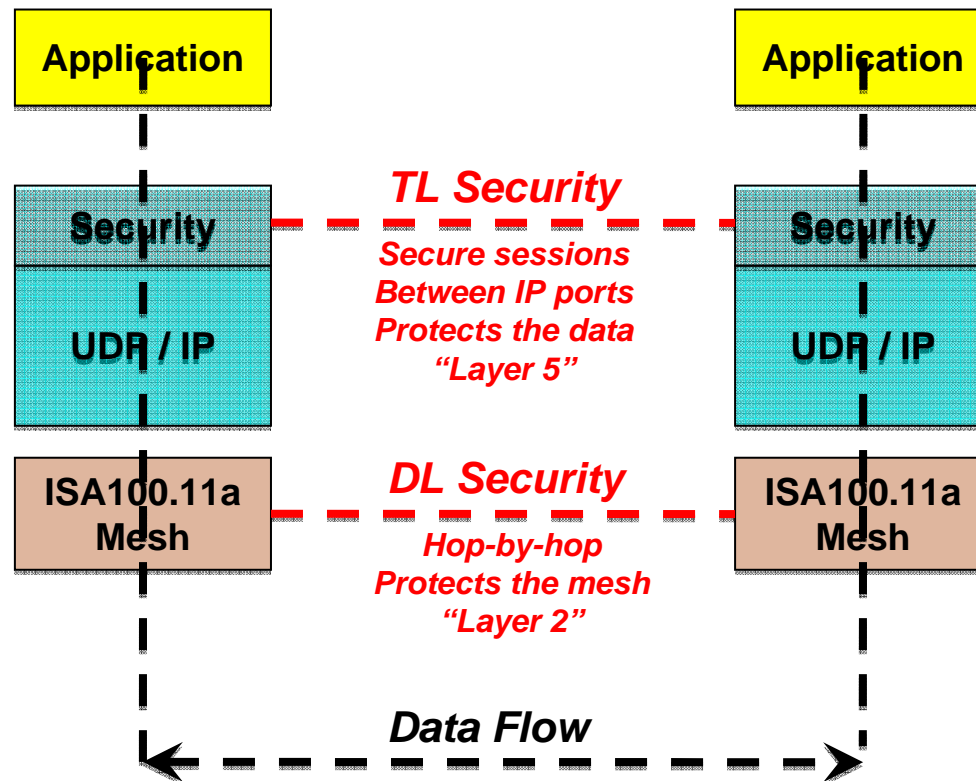
ISA100.11a Communication Architecture



ISA100.11a IP Stack



ISA100.11a Security model



ISA100.11a network architecture

Scaling through IP

IP Backbone
to Mesh



Manager

Gateway 1

Gateway 2

IP Backbone

ISA100.11a Scaled
Mesh Network

Mesh to
Gateway



Mesh

Mesh

Mesh

Mesh

Gateway
(& Manager)

Gateway
(& Manager)

Gateway
(& Manager)

Gateway
(& Manager)

?

?

?

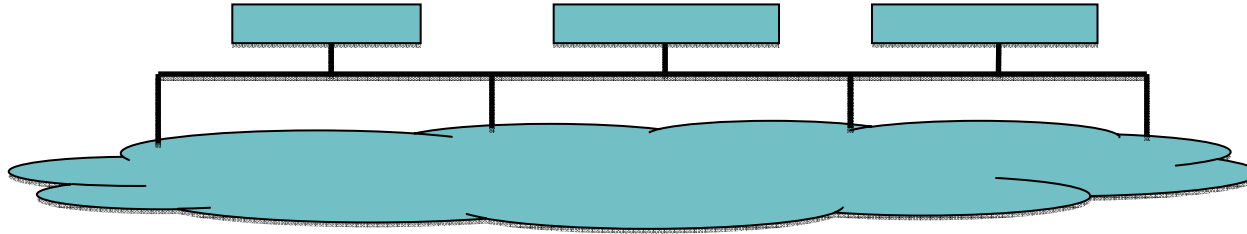
?

ISA100.11a mesh

Ten design principles

1. Leverage the IP backbone
2. Ensure authenticity and integrity
3. Deterministic and long battery life
4. Route adaptively
5. Deterministic, scheduled communication
6. Coexist with 802.11
7. Mitigate multipath
8. Integrate with “adjacent” standards (within reason)
9. Allow user to choose and evolve mesh architecture
10. Leverage the IP backbone

One Plant Network



- ISA100.11a network architecture allows for multiple subnets that operate and co-exist on the same backbone
 - Each subnet can be quite large, up to 30,000 devices.
 - Future ISA100 radios, such as WiFi, and be coherently integrated into the standard and into deployed systems
- Single System and Security Manager is responsible for managing multiple subnets, resulting in
 - Simplified network management
 - Synchronized operation across subnets
 - Shared gateway connections to plant network

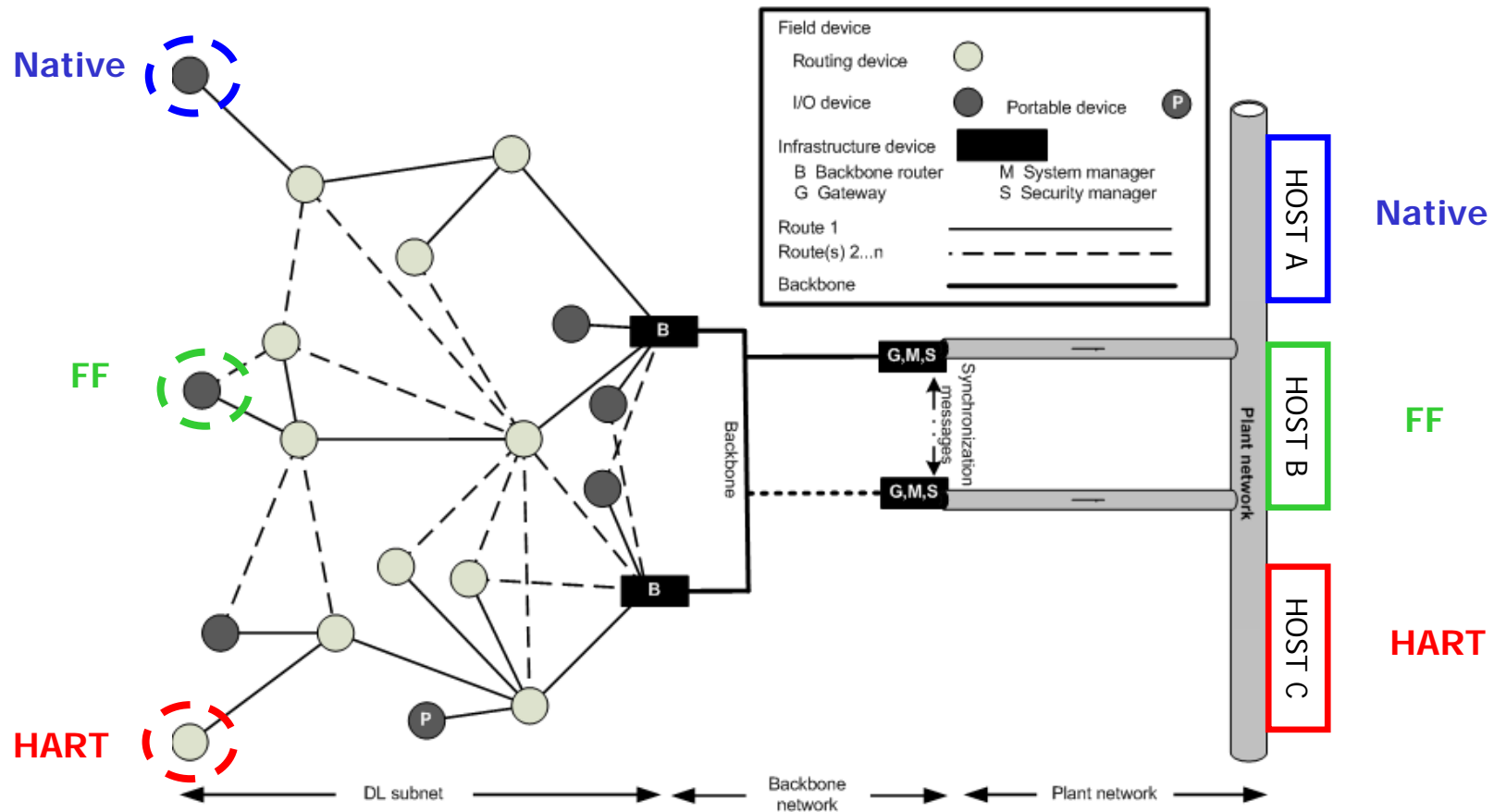
ISA100.11a

Control-ready application layer



ISA100.11a

Multi-protocol application layer



ISA100.11a Application Layer

Powerful, flexible, and extensible

1. Native mode

- Basic function blocks supported by standard
 - Analog input/output, binary input/output
- Publish (input) / Subscribe (output)
- Alerts (events and alarms)
- Bulk transfer

2. Tunneling

- Non-native (e.g. legacy) fieldbus commands/services over ISA100.11a
 - Example: HART commands can be tunneled through ISA100.11a

3. Extensions to native mode

- ISA100.11a native mode uses an extensible object model
- New WCI specifications build on that base
 - Profiles (temperature, pressure, tunneling, more to come)
 - Extensible device descriptors (ISA104 and XML)
 - Capability File: Additional information about device (capabilities, constraints)

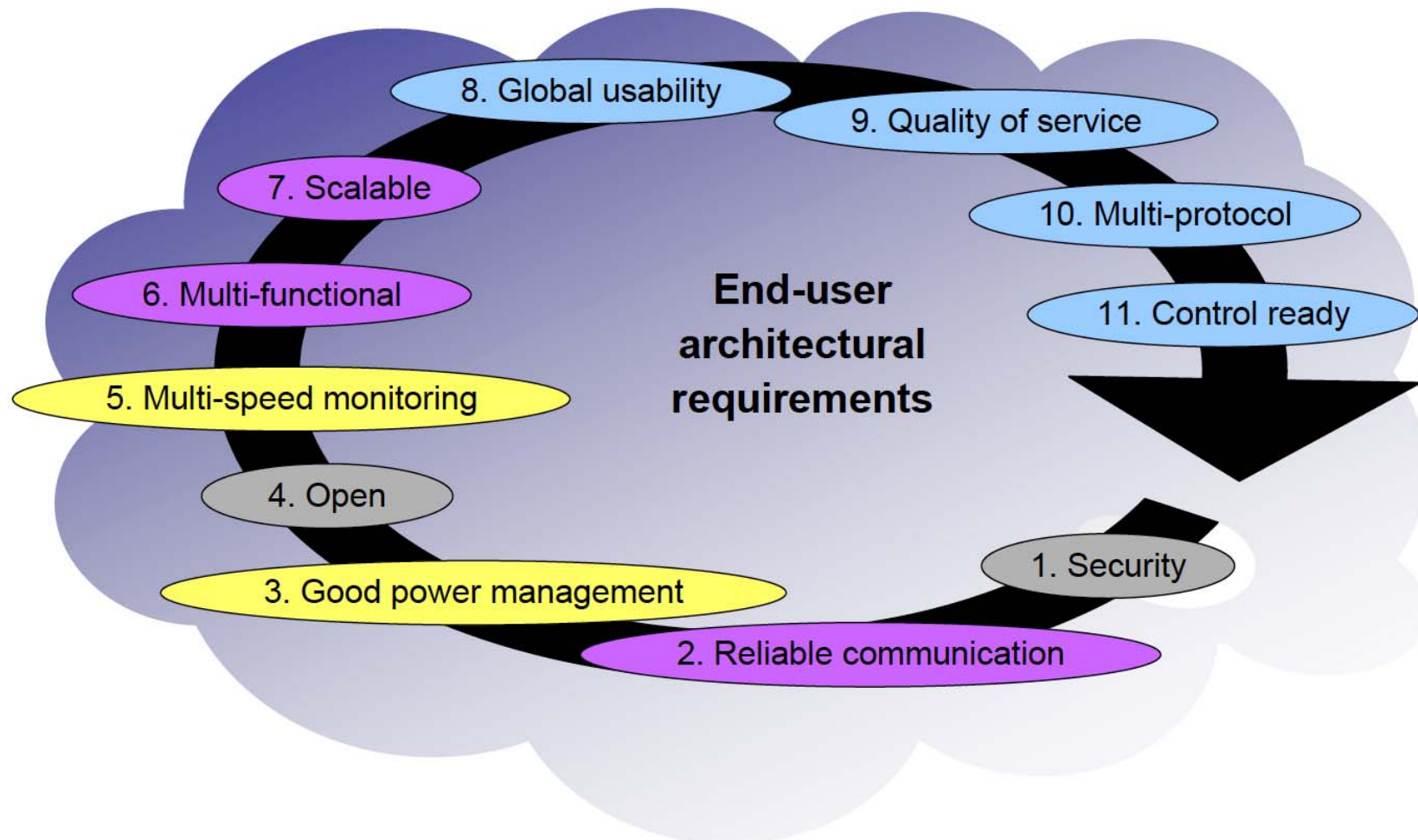
ISA100.11a Application layer

Control ready

- Lightweight native application layer derived from FF, HART and Profibus
 - Suitable for wireless monitoring and control.
- Process data has value + status, similar to FF, HART, Profibus
 - Baseline features can be mapped at the gateway
 - Tunneling of commands and services at the device level if needed
- Jitter in loop deadtimes is minimized
 - Scheduled, latency-controlled, phased, periodic messaging
 - Full peer-to-peer supported
 - Direct, controlled latency communication between neighbors.
- Full alert and alarm mechanism, derived from FF, HART, Profibus
- Typical fieldbus communications and support services API
 - Periodic, phased data publication and subscription
 - Event report and acknowledgement
 - Client-server read/write

Reprise: Voice of the customer

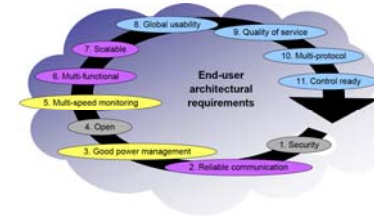
Core requirements for wireless sensing



ISA100 solutions must meet all requirements simultaneously

Voice of the customer

Technical requirements



	Secure, Reliable, Scalable		Flexible, Extensible Application Layer
	IP Architecture	Wireless Mesh	
Secure	☑	☑	☑
Reliable	☑	☑	☑
Low energy	☑	☑	☑
Open	☑	☑	☑
Multi-speed	☑	☑	☑
Multi-function	☑	☑	☑
Scalable	☑	☑	☑
Global	☑	☑	☑
QOS	☑	☑	☑
Multi-protocol	☑	☑	☑
Control Ready	☑	☑	☑

Thank you!



ISA100.11a – A framework for innovation