Setting the Standard for Automation™

ISA100.11a Principles of Operation Overview

ISA EXPO 2007

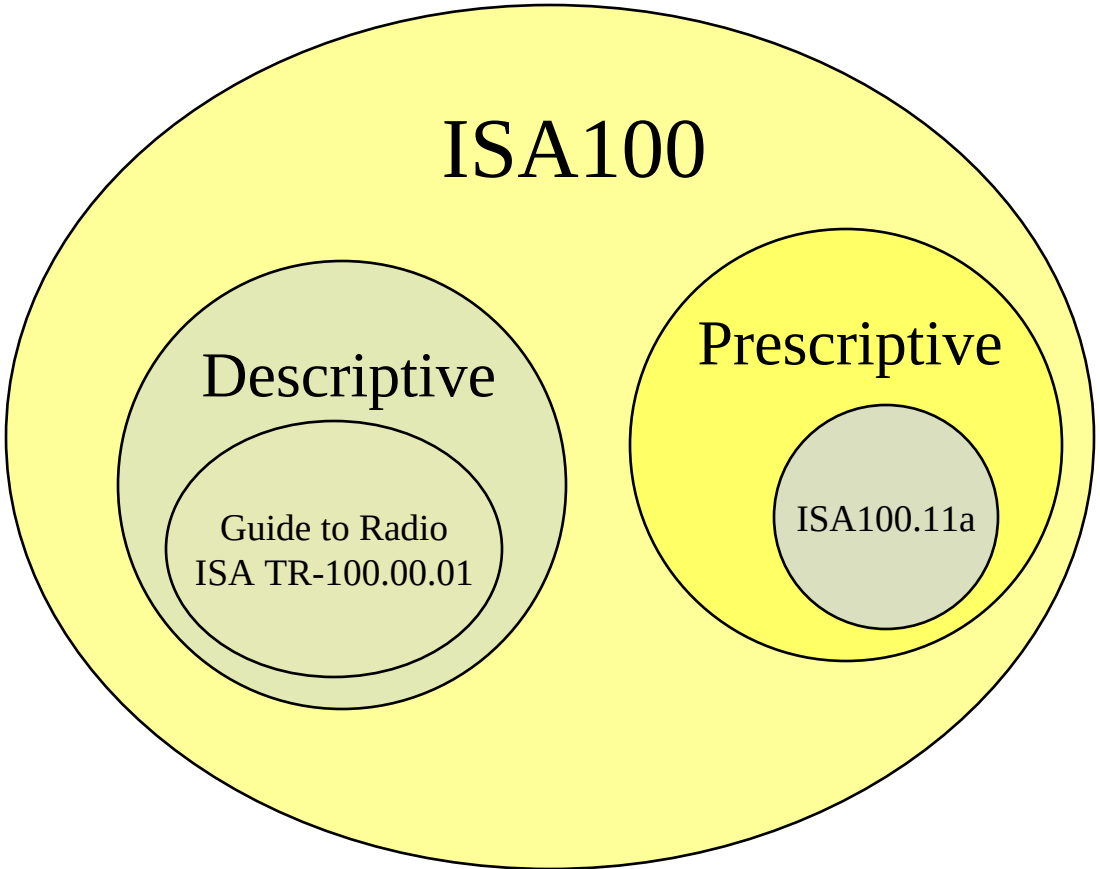
Wayne W. Manges
Oak Ridge National Laboratory

September 11, 2007

Standards
Certification
Education & Training
Publishing
Conferences & Exhibits

Welcome – Why Are We Here?

- Why Me? – ISA100 Co-Chair (with Pat Schweitzer from Exxon); DOE Industrial Wireless lead; etc, etc, etc.
- ISA100 is about announce its first prescriptive (thou shalts) release from the family of standards planned for industrial wireless automation – ISA100.11a



ISA100 creates work products for the community

Webcast For Users Group

- Boundary Conditions – what flexibilities we have, what we don't
- History – What got us to this point?
- Processes – Path to resolution, alternatives considered and yet to be considered
- Critical Issues – PoO details - options, commissioning, life-cycle costs, interoperability vs interchangeability, timelines, tradeoffs
- End-Game – how will we know when we're done?
- Future – Life after ISA100.11a

ISA Webcast Guidelines

- Twenty Minute Segments – I do most (but not all) of the talking
- Q&A – after each 20 minute segment to address questions raised during the session
- Repeat as Necessary – until material is covered
- Final Q&A – Time left at the end for final, no-holds-barred questions and discussion about the Principles of Operation and path to the standard

First Segment – Introduction of Concepts

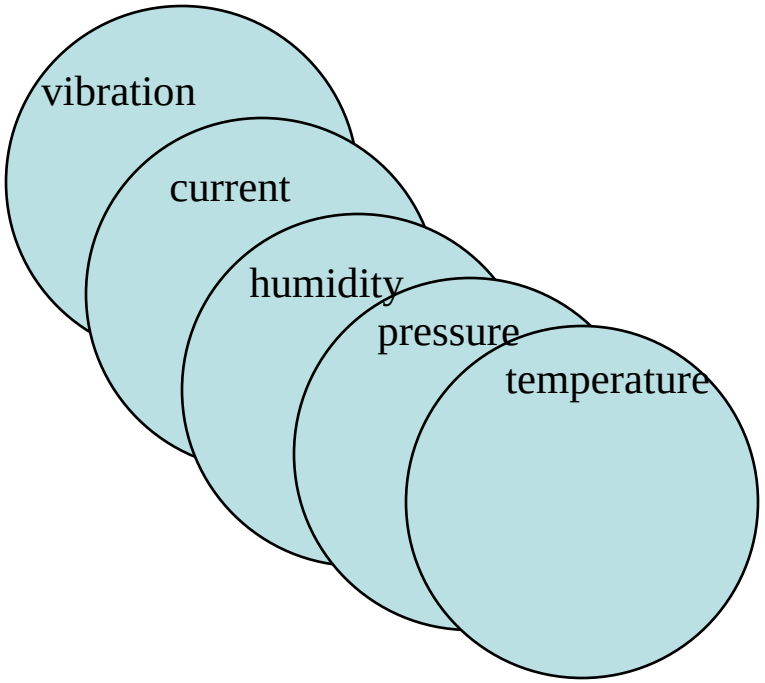
- ISA100 and ISA100.11a – what's the difference?
- Constraints – what drives the inevitable compromises necessary in any standards process
- ISA100.11a Focus – applications, priorities
- Architectures – why? Compromises?

ISA100 – A Family of Standards

- ISA100.11a – Focus on (but not limited to) industrial process automation applications
- Physics of Radio – *Automation Engineer's Guide to Radio* – released as draft in October 2005
- Why?
  - *No one-size fits all*
  - *Market differences*
  - *Culture differences*
  - *Cost sensitivities are different*
  - *Market size limits available options*

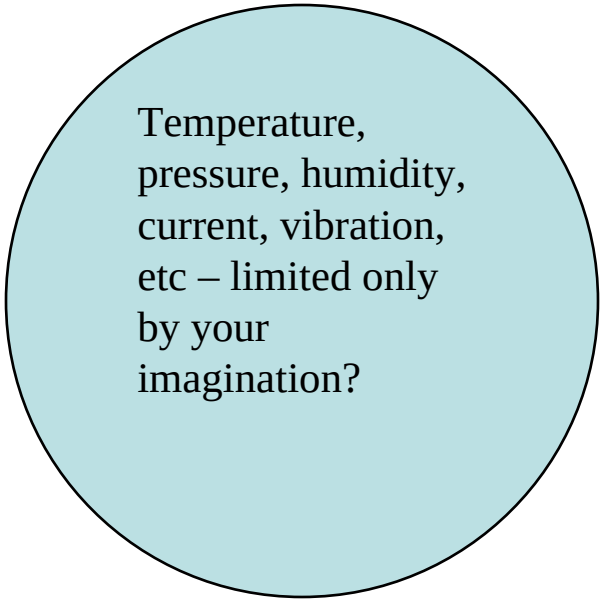
ISA100 – Dealing With Constraints

- *Is Each Application Unique? – then a different standard for each one? At what cost? Maintenance Nightmare!*



User selects appropriate device

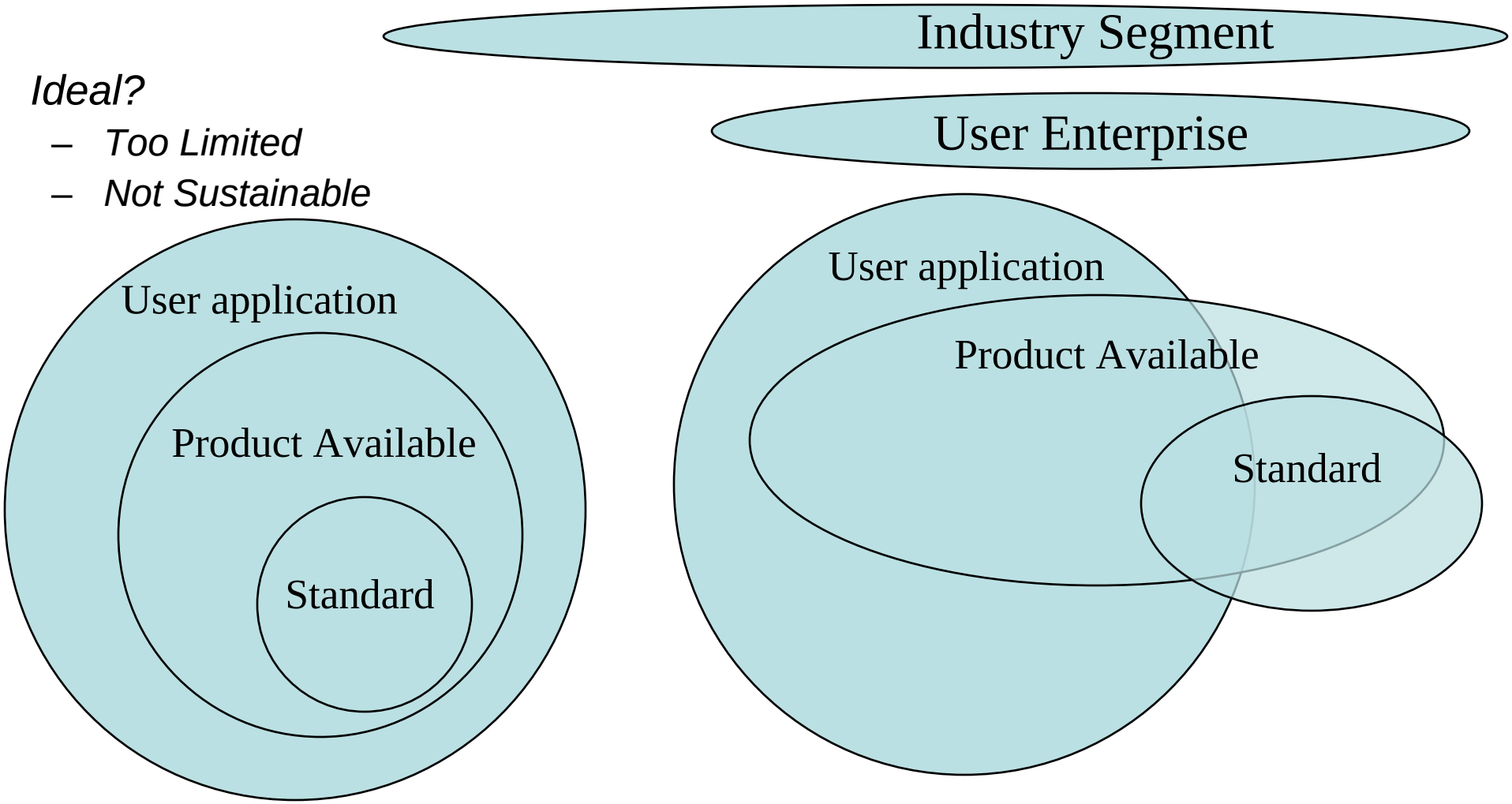
- *Or can a single device do everything? – at what complexity? Reliability?*



User selects appropriate function – microprocessor!

So Where Does a Standard Fit?

- *Ideal?*
  - *Too Limited*
  - *Not Sustainable*



Suppliers struggle if market niche is too small. Users lose supplier base and ultimately can't sustain production. We need a Win-Win!

ISA100.11a – Process Focus

- Chemical – direct target based on early user involvement
- Fresh/Waste Water – recent interest, likely applications
- Petrochemical – direct target based on early user involvement
- Pharmaceutical – some interest but some characteristics may not match up.
- Other? – not precluded but needs to map to existing performance expectations for .11a
  - Throughput – sample intervals at seconds
  - Security – off-the-shelf, best practice, AES encryption
  - Latency – 100ms range
  - Reliability – 99.9% but trades off with latency and throughput
  - Range – about 50m but trades off with reliability, latency, and throughput
  - Expanse – extensible to thousands of nodes (10,000 target) over about 1 square mile footprint

With this background – let's get to the PoO!

Principles of Operation – One Step Away

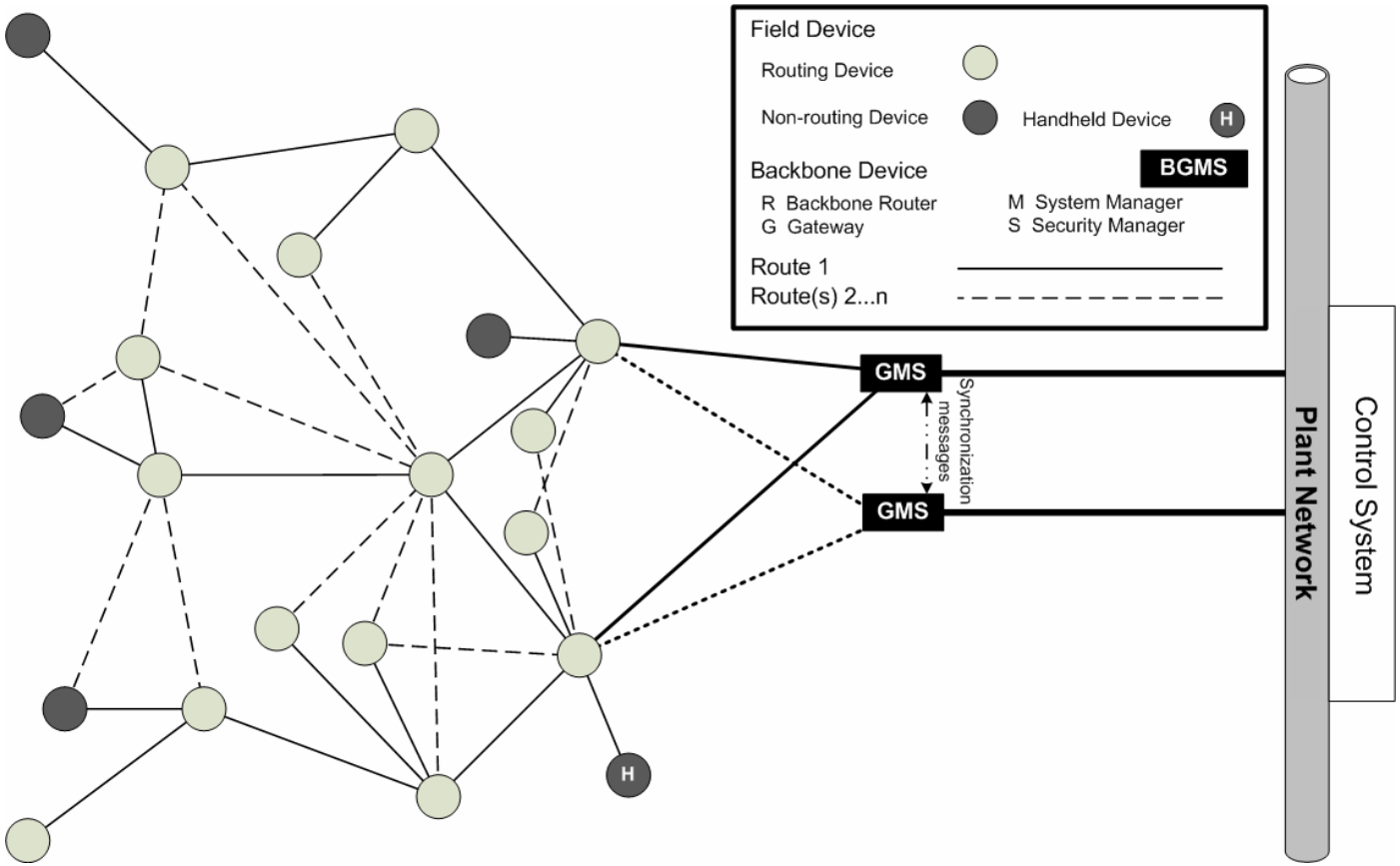
- Detailed – for engineering and operation decisions
- Direct – little room for interpretation and free-lancing but does address options
- Thorough – covers commissioning, configuring, operating, maintaining, and expanding
- Living – Document updated, as required, to augment and correct
- Path to Standard – Superset of possibilities that guides the development of the official release of the standard
- Audience – May not be suitable for end user community

Section 2 – .11a Overview – Key Attributes

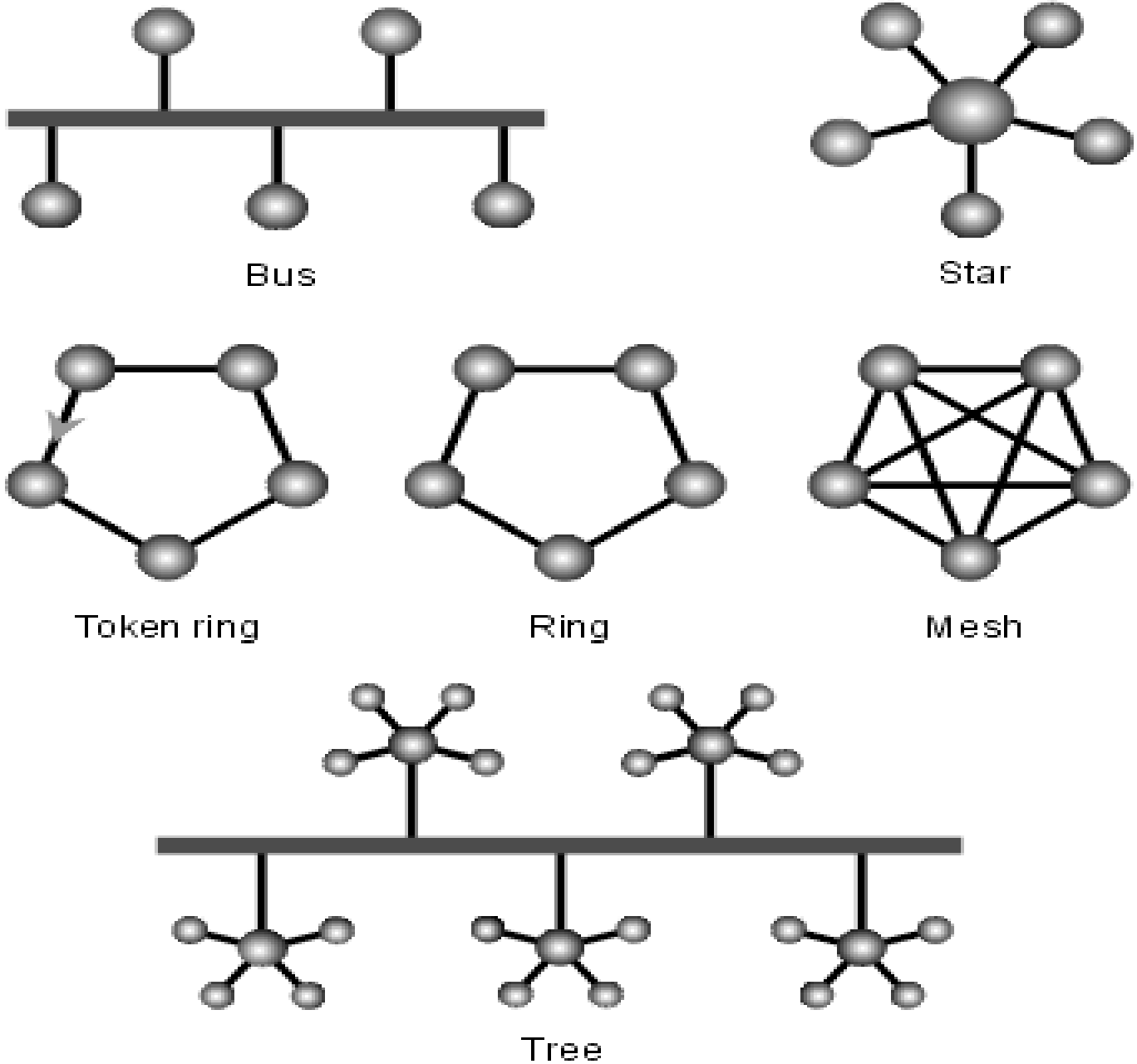
- Non-critical – no lives threatened, little equipment consequence
- Monitor, alert, control – low consequence if communication interrupted
- Low Data Rate – no frame-rate video, vibration problematic
- Mobility – Fixed, portable, moving – but slowly, infrequently
- Very low power – 2-5 year battery life on end devices
- Latency – about 100ms
- Coexistence – with most other standard and non-standard devices
- Interoperability – with ISA100 standard devices

Section 2 – Overview - Architecture

- Mesh, Star, and Star-Mesh (tree) – what's the difference?
- Routing vs non-routing – what about "mesh to the edge"
- Gateway – connecting to the plant network
- Redundancy – measurement to gateway



Networks - Topologies (Wired or Wireless)

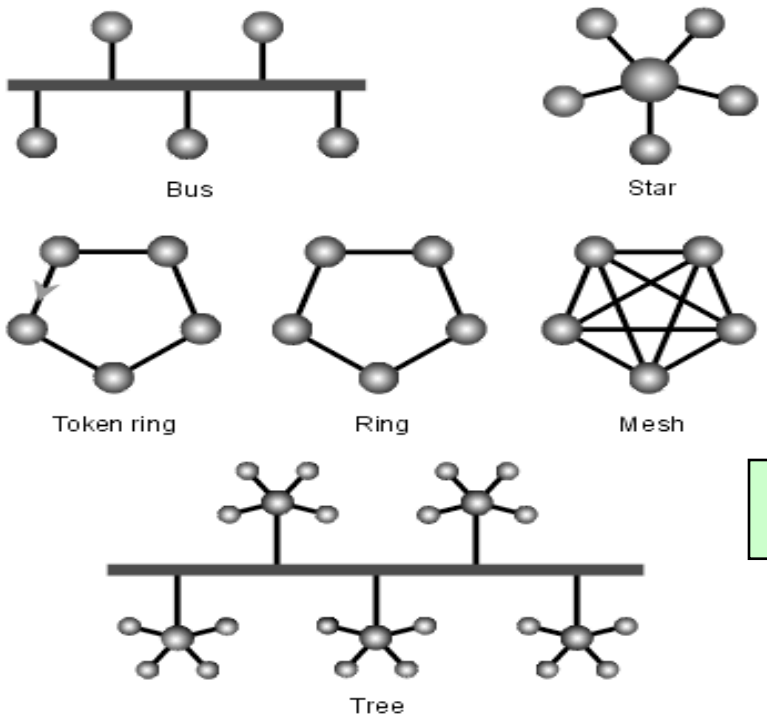


Issues include:

- reliability
- latency
- complexity
- cost
- throughput
- security
- battery life
- determinism
- interchangeability
- range

Mesh-to-the-Edge – Why? Why not?

- Full Mesh - Holy Grail for Mesh Networks – may not be suitable for industrial applications
- All nodes are created equal – full interchangeability
- Routing can be very complex – Bluetooth can take 4 hours to form a network; others take 20 minutes
- Depth of Routing Table – how many failures can you tolerate?



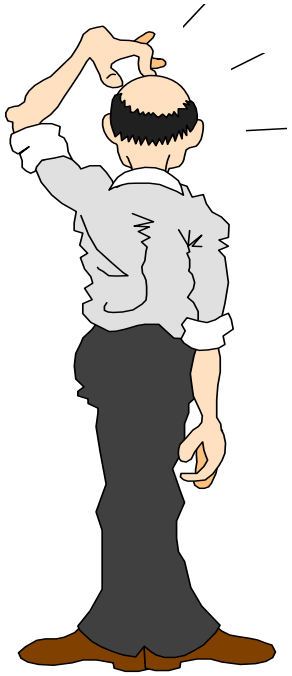
- How many? 10,000?
- Doesn't scale linearly
- Clusters make sense

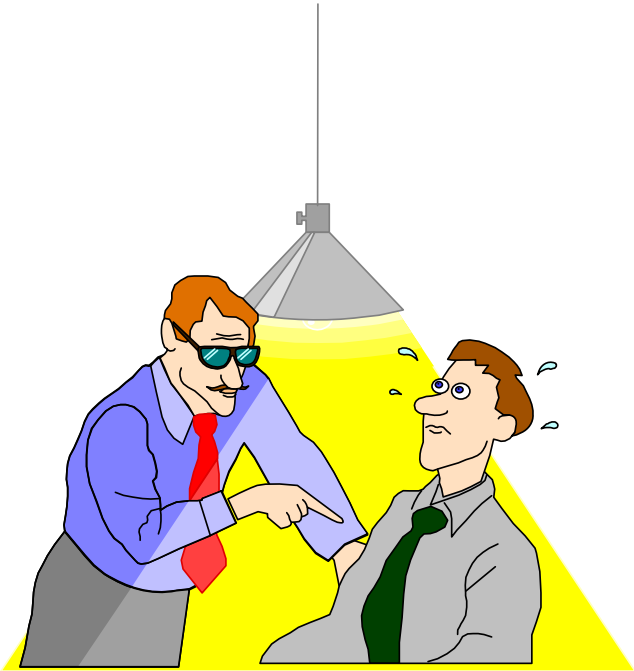
ISA100.11a offers strategic compromise

Review of Key Points

- ISA100 is a Family of Wireless Industrial Automation Standards – not just ISA100.11a
- Constraints – dictate limits to modularity, flexibility, market integration
- ISA100.11a will be first “prescriptive” standard – describes what’s required to be compliant
- Architectures – always trade-offs dictated by constraints, costs, applications
- ISA100.11a will support tree, mesh-to-the-edge, or point-to-point based on configuration

Questions?





Segment 2 – From Radios to System Issues

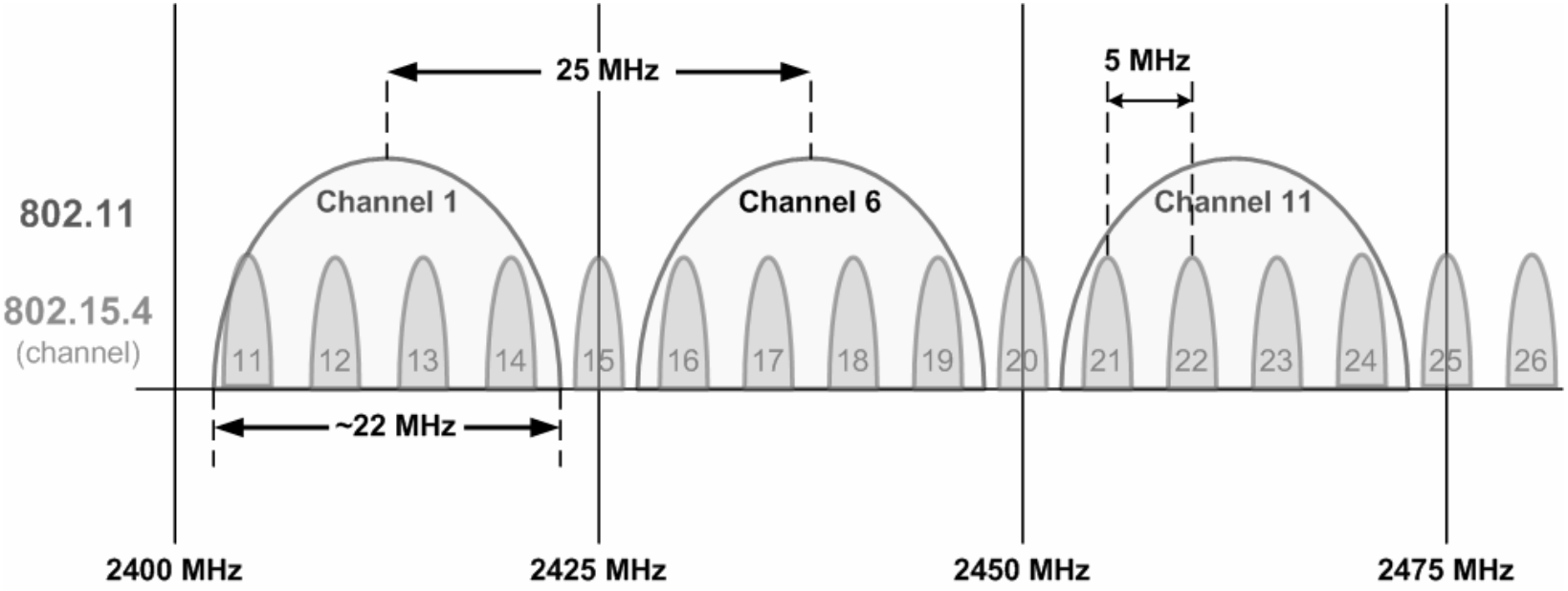
- IEEE 802.15.4 – why, what, how
- Attribute Interplay – reliability, security, coexistence, ease of use
- Structure – synchronization required and why
- Diversity Benefits – frequency, time, space, etc.
- Deployment – self-organizing, security, management, application interfaces
- Device Interfaces and Use classes – class 1 – 5 with an asterisk

Why 802.15.4 Radios?

- IEEE 802.15.4 2006 operating in the 2.4 GHz band offers good compromise:
  - Widely available – hardware suppliers, software suppliers, security options – technological orphans can cause problems!
  - Reliable – well characterized and understood, tested in harsh RF environments
  - Coexistence – options available to address via time, channel, and spatial diversity
  - Security – state-of-the-art solutions readily available and tested
  - Self-organizing – lowers time and cost of commissioning

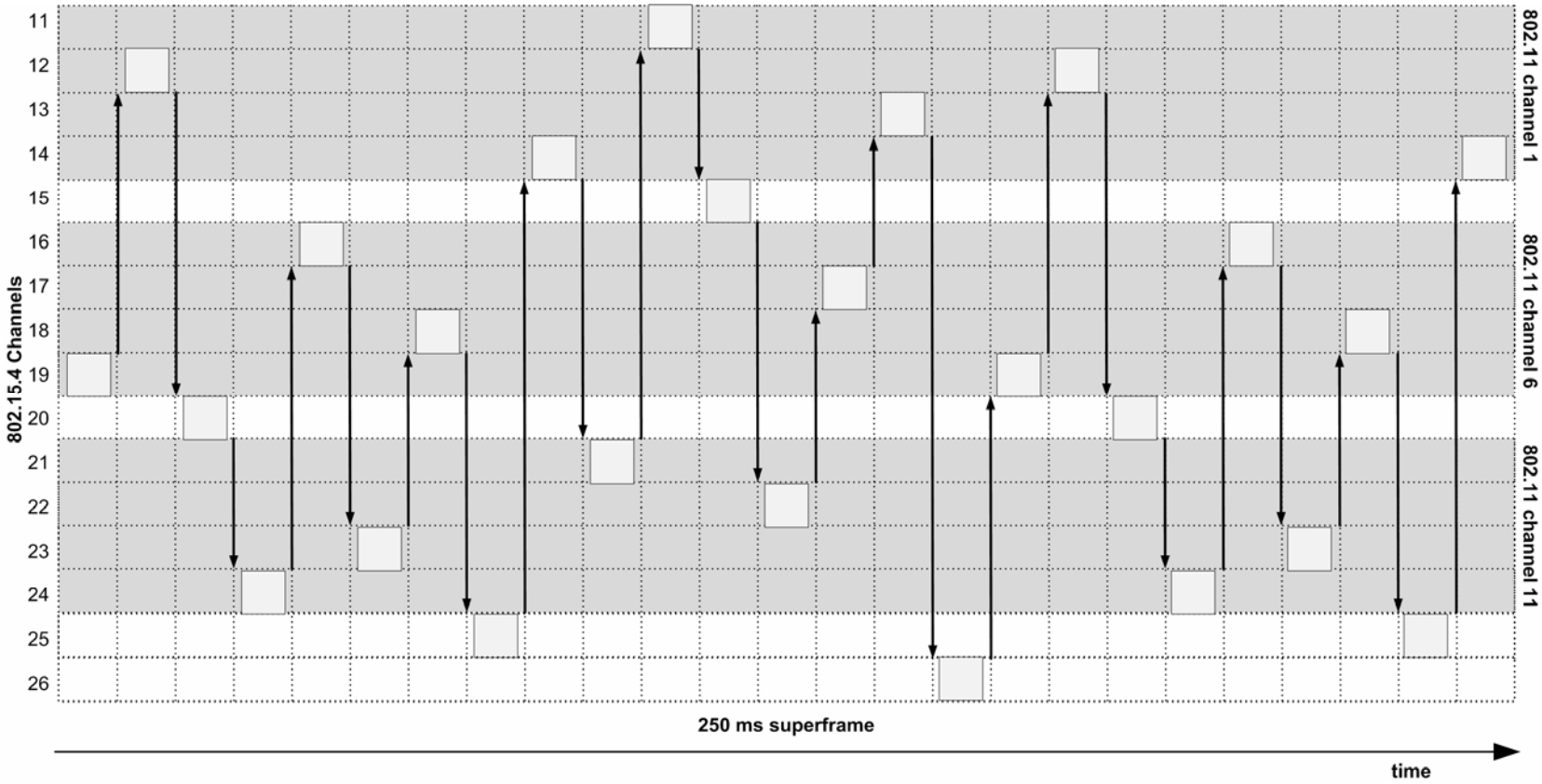
Reliability, Coexistence, Security, Ease of Use All Related

- Frequency Agility – move away from problems
- Time Agility – Reduce impact of burst noise
- Mesh – reduces impact of localized interference



Tight Time Synchronization Provides Benefits

- Battery Life
  - Sleep times – wake up and listen
  - Data rates – lower on-air time
- Security
  - Codes – longer listen time required
  - Depth – multiple approaches



Self-organizing Redundant Networking

- End-to-end Reliability – Redundant paths, dynamically routed based on errors and timing
- Self-Healing – dynamic assessment of path viability
- Coexistence – adjusts frequency and timing to be “good neighbor”
- Time Slots Available
  - Dedicated – predictable, regularly spaced sample intervals
  - Shared – intermittent alarms and other bursty traffic
- Information Models Supported
  - Publish/subscribe – one-to-many
  - Client/Server – point to point
  - Bulk Transfer – allocate channel
  - Alarms – high reliability but low data rate
- Ease of Deployment – “Just Plunk It Down” – take all defaults for time, frequency, and security options

Robust and Flexible Security

- MAC and Transport Layer – media access control (MAC) layer filter reduces impact of “denial of service” attack
- Key Management – drives effectiveness and performance
  - Asymmetric for critical functions – harder to break but slower (knowing one key doesn’t give the other away)
  - Symmetric for high speed requirements – data transfer, lower criticality functions – (single key can be compromised)
- Cryptography – modular to allow for export control issues

• Three Aspects to Security – confidentiality, integrity, and availability (CIA is business default priority)
• What Order of Importance? – Industry says: availability, integrity, confidentiality (AIC)

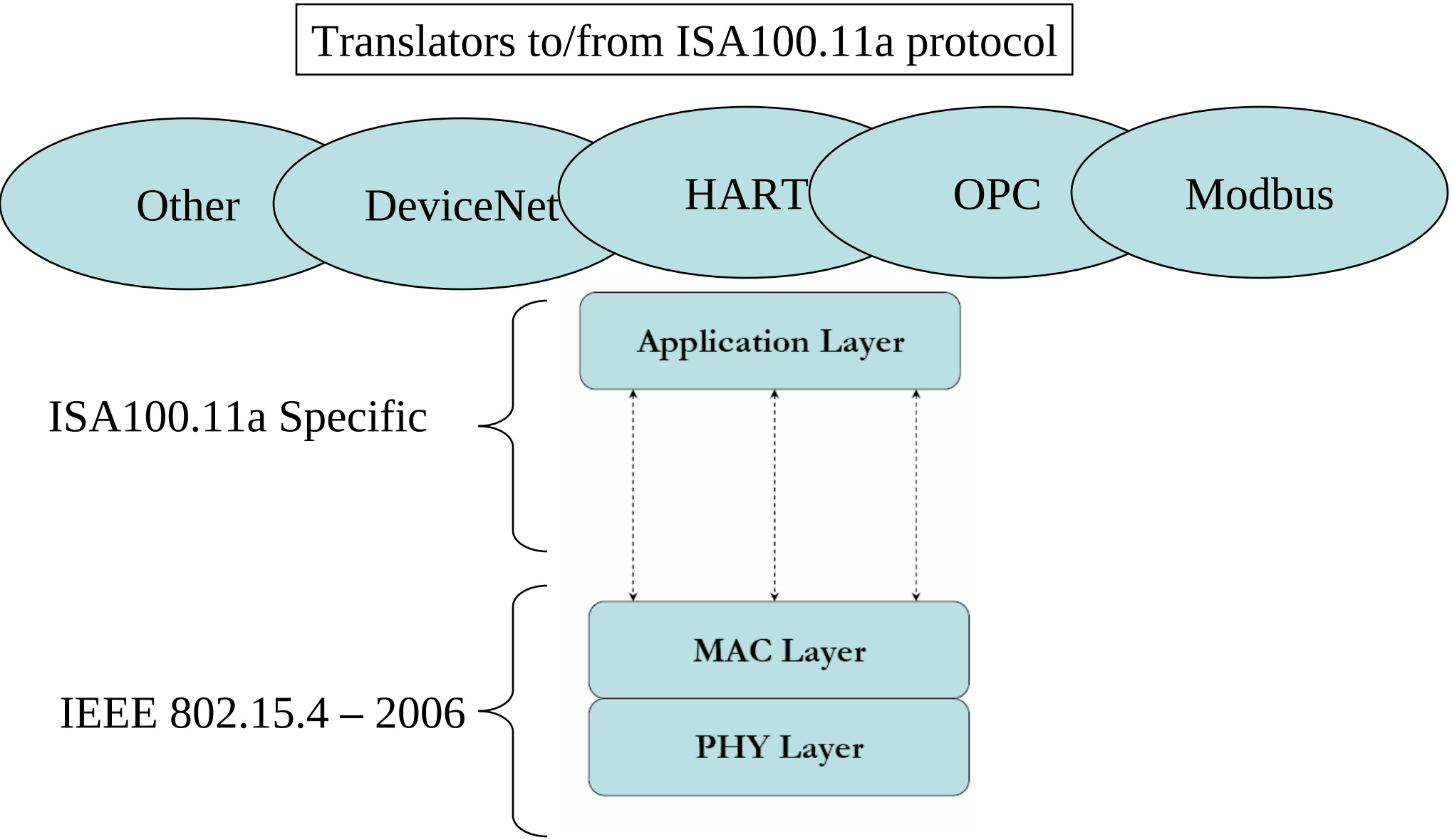
System Management – Allocating Comms Resources

- Fine Tuning – for improving reliability, security, range, throughput, latency
- Policy Based – hierarchical complexity
- Reporting – assess status of configuration, performance, security, non-repudiation, forensic evaluation
- External – enables remote access to security, management features

Application Interface – Key To Deployment

- Object Oriented – encapsulates for re-use and consistency
  - Attributes – detailed setup and runtime data
  - Functionality – methods and internal states, supported commands, etc.
- Maps Legacy Protocols – supports “translators” to/from ISA100 conventions
  - Similar commands re-mapped from lower layers
  - Data attributes – flags, periodicity, etc.
  - Naming conventions – special characters, etc.
  - Addressing – mapping to special protocol needs
- Open, Interoperable Application Environment – suppliers can start early
- Common Integration Point – for multiple host control system (DCS) access
- Alternative to Tunneling – improves performance and transparency

Application Layer – Key to Application Interoperability



Section 3 Systems – Devices & Interfaces

- Device Interfaces – guaranteed interchangeable on default mode – options may move outside total compatibility
- Worldwide Access – Europe, Japan, Canada, US – options available for specific regions
- Device Types and Roles – dictate functionality required
  - Field Devices – exposed to hazards, most primitive communications required
    - Input/Output Devices – Minimum features required for participation in ISA100.11a network
    - Field Router – Maps source data to appropriate sink(s) under field conditions
    - Provisioning Role – allows new devices to join the network
  - Infrastructure Devices – protected from extreme environments, integrates information from floor-level devices
    - Gateway Role – interfaces ISA100.11a field devices to plant network
    - Backbone Router Role – allows ISA100.11a devices to interface to non-ISA100.11a
    - System Management Functions
      - Governs policy based control over resources
      - Enable secure system operation

Note that multiple device types and roles can be implemented in a single package.

Usage Classes 1 through 5 – not designed for critical, emergency responses

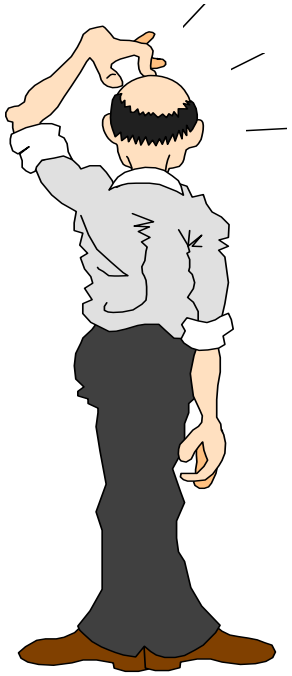
Category	*Class*	*Application*	*Description*
Safety	0	Emergency action	(always critical)
Control	1	Closed loop regulatory control	(often critical)
	2	Closed loop supervisory control	(usually non-critical)
	3	Open loop control	(human in the loop)
Monitoring	4	Alerting	Short-term operational consequence (e.g., event-based maintenance)
	5	Logging and downloading/uploading	No immediate operational consequence (e.g., history collection, sequence-of-events, preventive maintenance)

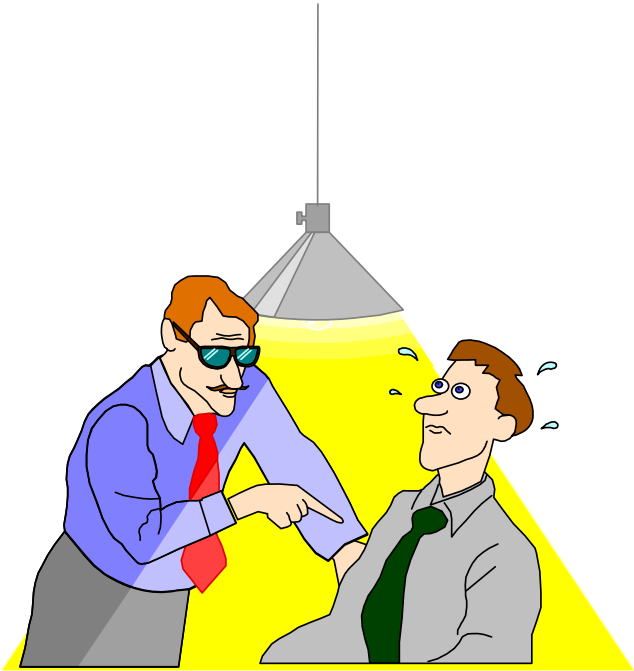
Importance of message timeliness increases

Segment 2 Review – From Radios to Systems

- IEEE 802.15.4 – A good compromise, slam dunk choice (for now)
- Attribute Interplay – reliability, security, coexistence, ease of use
- Structure – synchronization improves battery life and security
- Diversity Benefits – Improves reliability and security
- Deployment – Ease of deployment to ease of integration
- Device Interfaces and Use classes – class 1 – 5 with an asterisk

Questions?

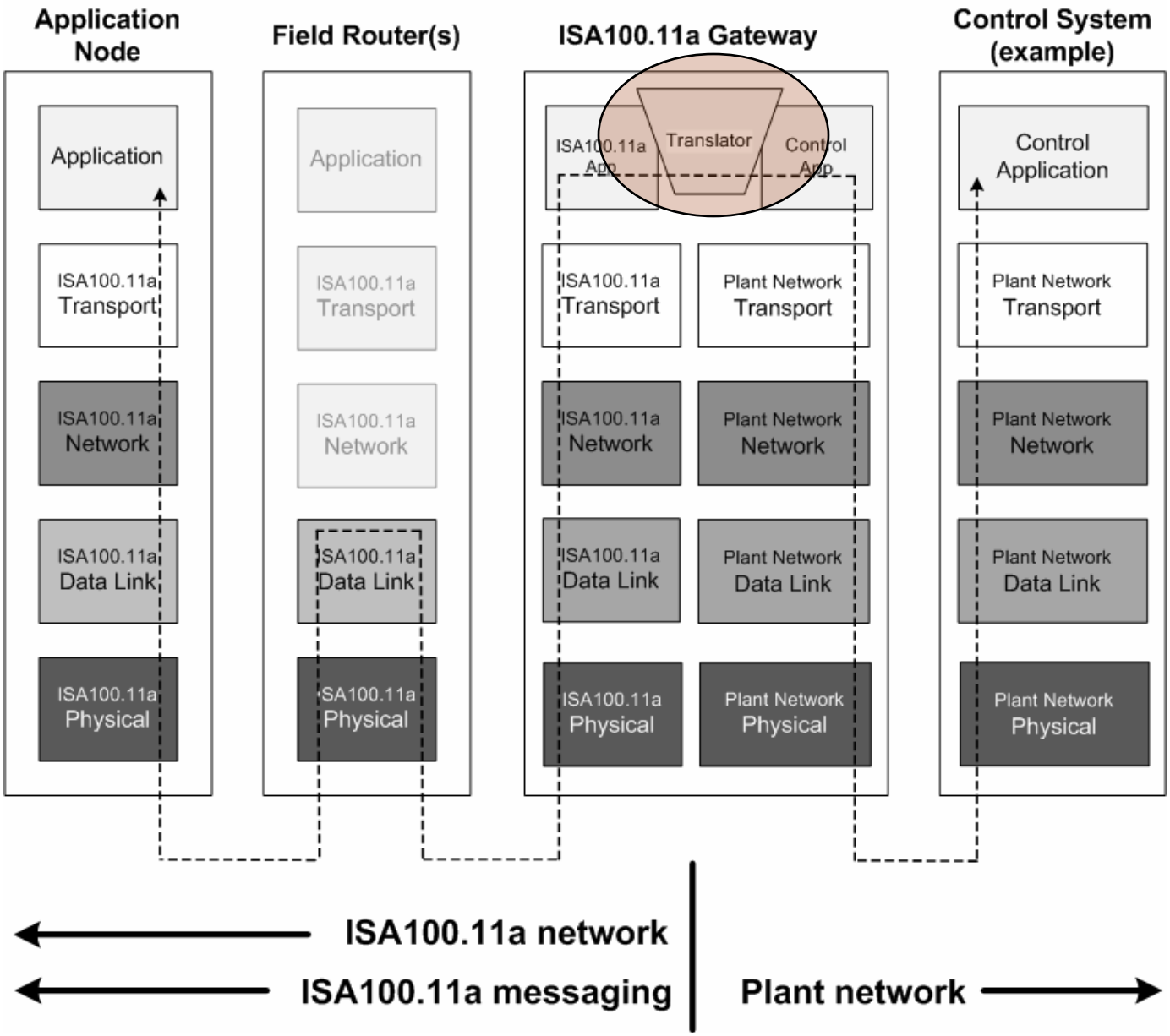




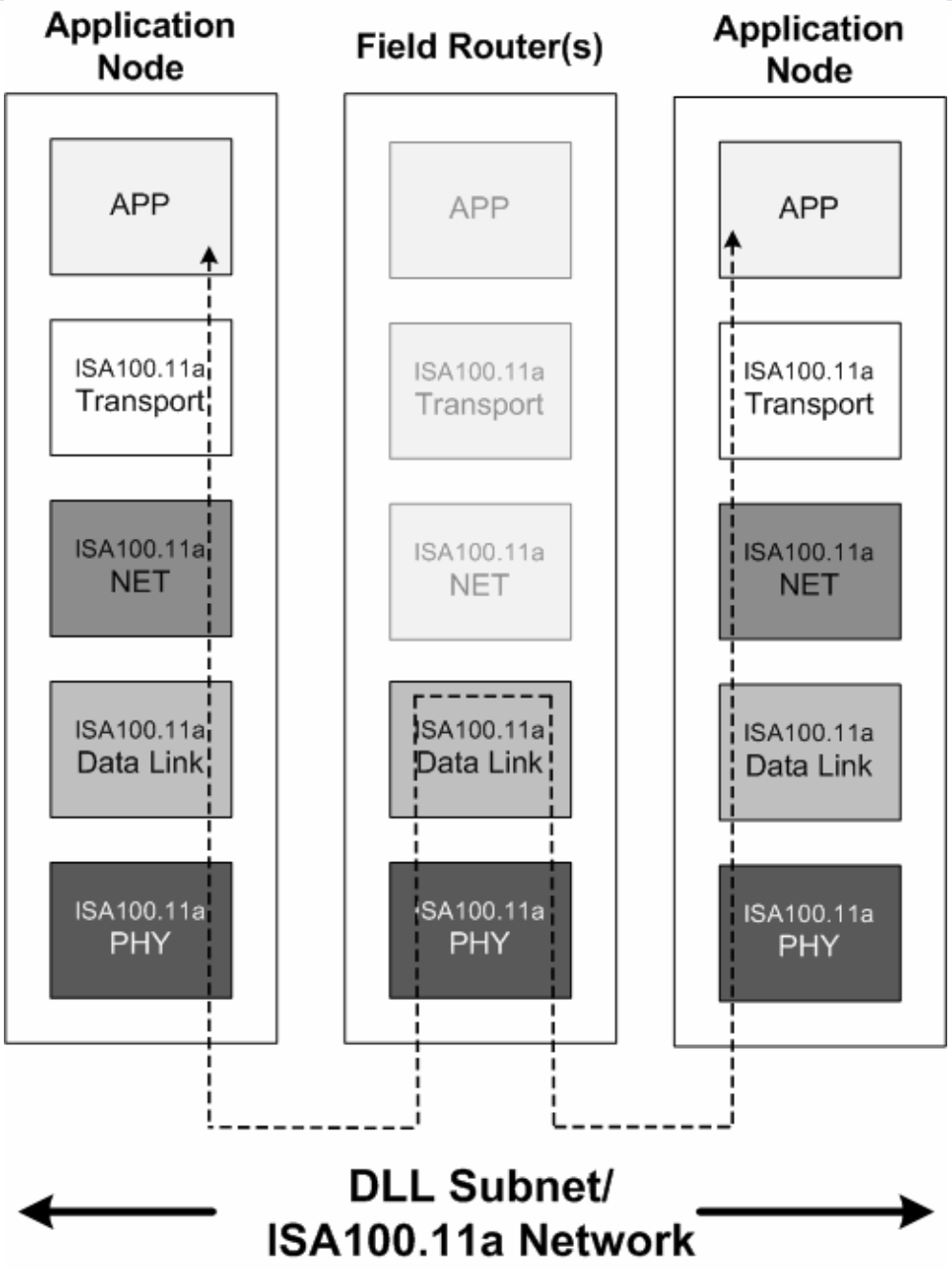
Segment 3 – Processes and Modes

- Translators – Application layer and PHY layer
- Joining – commissioning and de-commissioning devices
- Quality of Service – choices and impacts
- Security – choices and impacts
- User Input – most needed issues needing user input

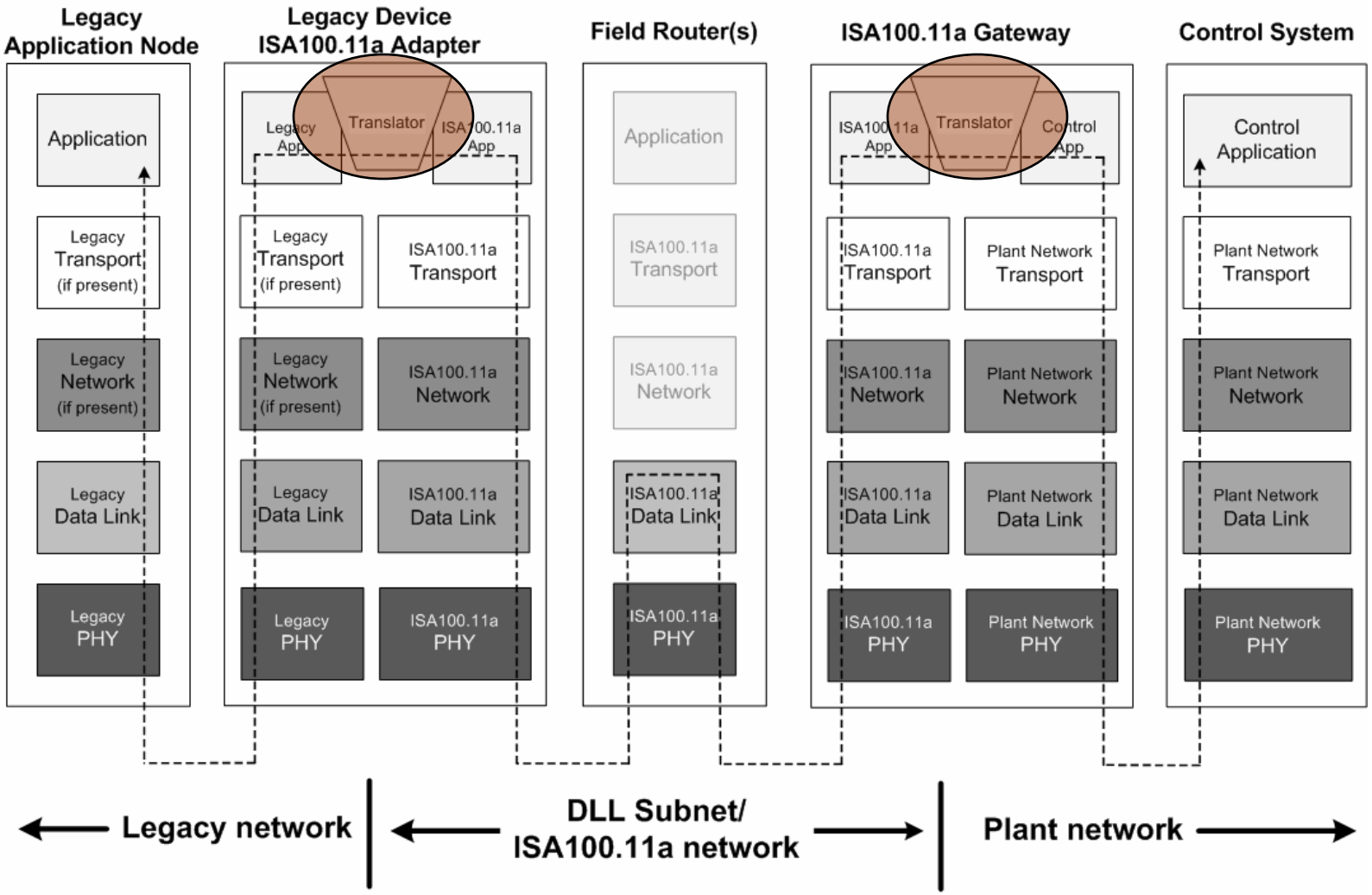
Communication Details Hidden From Most



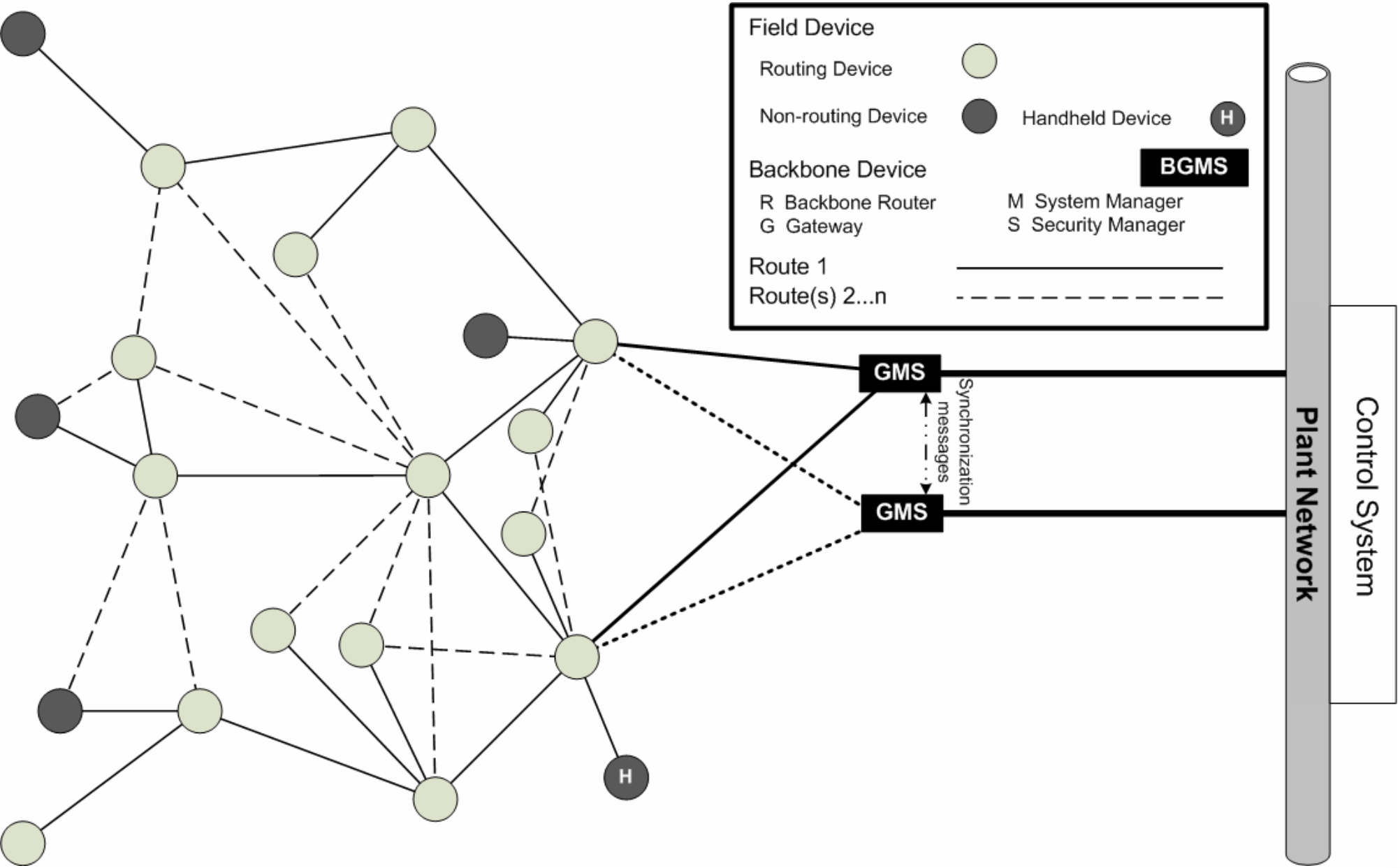
Simplest Case – No Gateway!



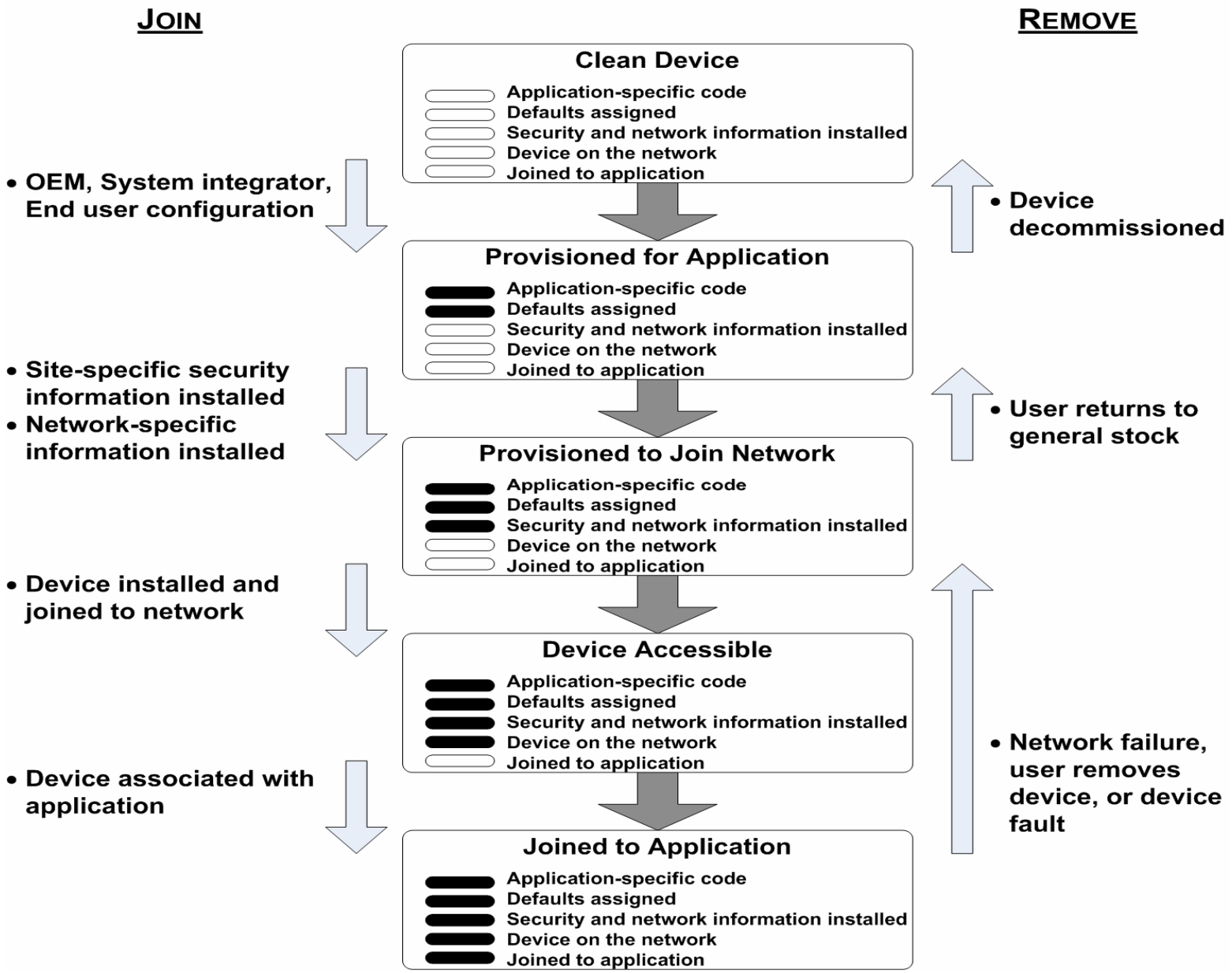
Legacy Device Adds One More Translator



Remember – Canonical .11a Architecture



It's A Process!



Application Requests Vs Default Quality Of Service

Application flow type	*Periodic*	*Unicast*	*Multicast*	*Reliable*	*Unacknowledged*	*Enhanced security*	*Basic security*	*Priority*
Periodic publish/ subscribe (buffered)	✓	✓	**(possible future use)**		✓	✓	✓	**Minimum AL need: High / Medium/Low**
Client/ server (queued)		✓			✓	✓	✓	**Minimum AL need: High/ Medium/Low**
Source/sink (queued)		✓	**(possible future use)**		✓	✓	✓	**Minimum AL need: High / Low**
Bulk transfer unicast (stream)		✓	**(possible future use)**	✓		✓	✓	**Minimum AL need: High / Low**

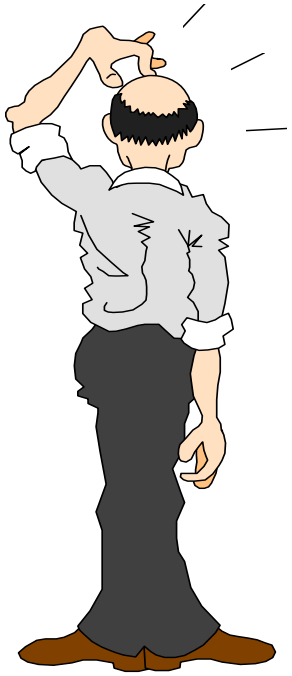
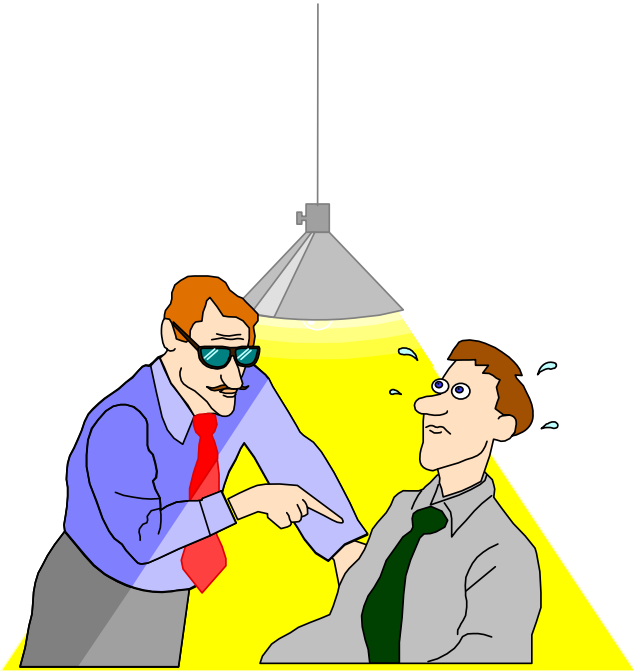
Security Must Not Be Degraded During Transport

		Outgoing security level		
		Unsecured	***Authenticated***	***Authenticated and confidential***
Incoming security level	***Unsecured***	**Allowed**	**Allowed**	**Allowed**
	Authenticated	**Not allowed**	**Allowed**	**Allowed**
	Authenticated and confidential	**Not allowed**	**Not allowed**	**Allowed**

ISA100.11a Principles of Operation Review

- Based on Current Status – security, joining and several other issues have details yet to be worked out
- Options – yet to be determined how options will be implemented and how they will impact interchangeability
- Flexibility – required at this stage but will be managed as the process moves toward the standard
- Future – is there a .11b, .11c, … - Who Knows?

User Input Most Needed

- Options – how many? At what cost to ease-of-use? When do we stop and create new standard?
- Defaults – base requirements for latency, throughput, range, security, reliability
- Future – What is needed? .11b, .11c, etc. or a new ISA100.12, .13, .14, etc.
- Security – What minimum is acceptable? None? What maximum is acceptable? Hardware provisioning?
- Metrics – what on-line performance assessment is required?
- Non-Communications Properties – how do we deal with ruggedness requirements?

Final Questions?