ISA100 Wireless Compliance Institute

The Technology Behind the ISA100.11a Standard – An Exploration

ISA100 Wireless Compliant

ISA100 WIRELESS

ISA100 WIRELESS

ISA100Wireless Compliance Institute

Welcome From the ISA100 Wireless Compliance Institute Governing Board

Honeywell – Chairman, Dan Sheflin

Yokogawa – Vice Chairman, Penny Chen

GE – Justin Smith

Nivis – Scott Johnson

Yamatake – Hisashi Sasajima

User Representative – ExxonMobil, Pat Schweitzer

The Technology Behind ISA100.11a – User Driven Technology

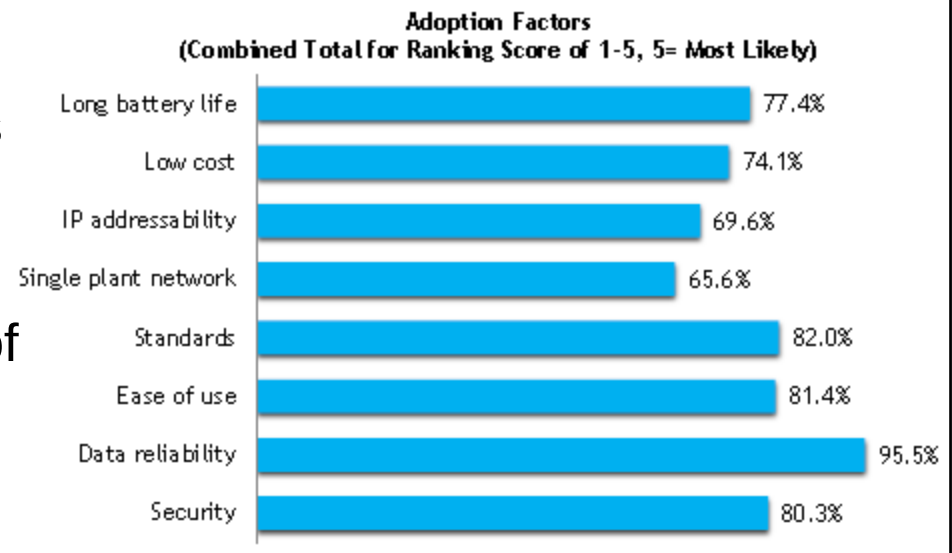
- The ISA100.11a standard was architected based on end user's requirements and feedback
- ISA100.11a based wireless systems incorporate the required underlying technology, architecture and features that address end user desired characteristics
- This webinar offers insights into how these requirements are implemented in the underlying technology foundations

End Users – Wireless Adoption Considerations

- End users voiced their opinions and concerns related to the adoption of wireless sensor networks (WSNs) in industrial applications
- This presentation addresses each and one of the adoption considerations raised by the users by showing how systems based on ISA100.11a address these considerations or concerns
- This is accomplished through an aggregation of technical features and mechanisms that are:
  - ✓ Research based
  - ✓ Empirically field proven
  - ✓ Standards based

Wireless Adoption Considerations

- OnWorld conducted polls and published results based on interviews with 105 plant managers, process integrators and system engineers
- Results are clearly indicative of end user's concerns
- Data reliability ranked as the primary concern for adoption of wireless sensor networks in industrial applications



Source: "Industrial Wireless Sensor Networks," ON World March 2010

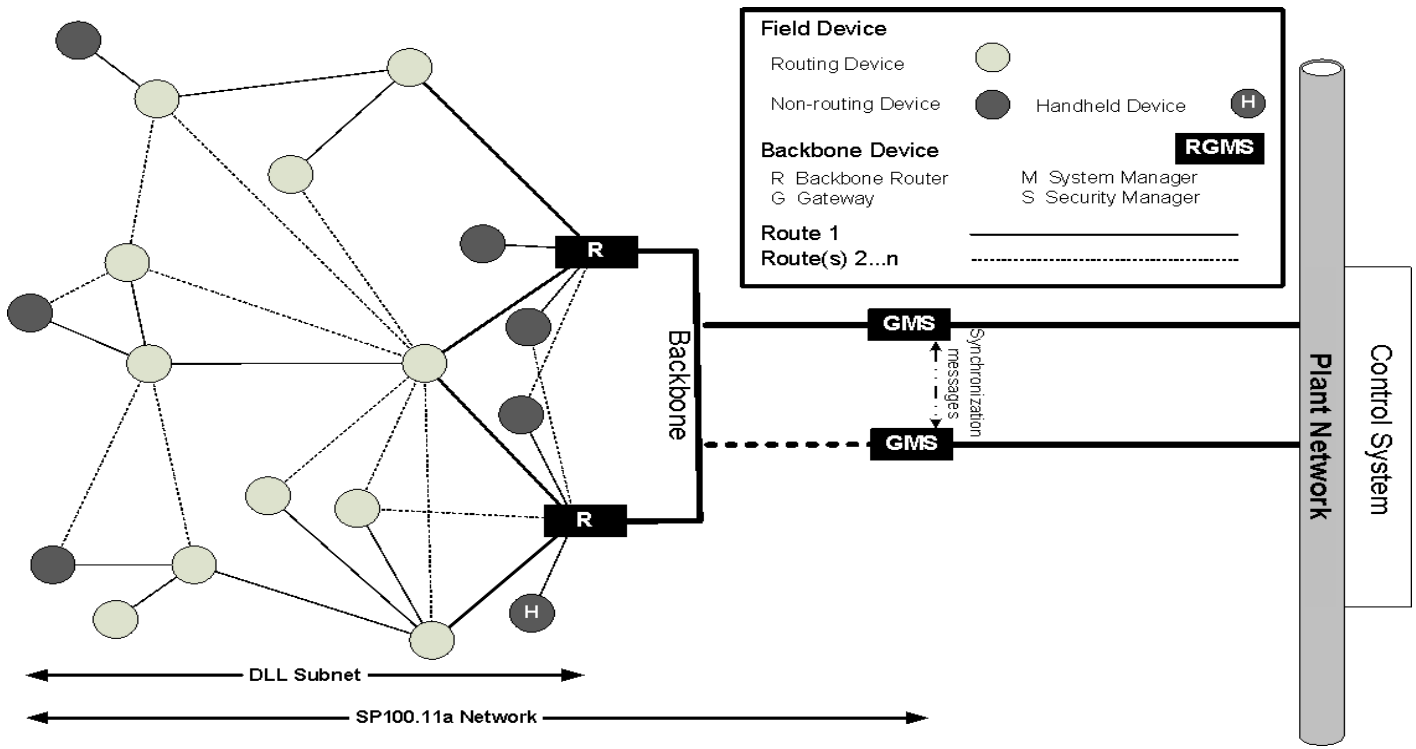
End Users – Wireless Adoption Considerations

In order for end users to deploy wireless sensor networks in industrial applications the wireless network has to be characterized by:

- ✓Highly reliable data communications
- ✓Ease of deployment and utilization
- ✓Extensible in the future
- ✓Vendor interoperability - standards based
- ✓Sound security
- ✓Prolonged battery life
- ✓IP addressability
- ✓Solution needs to operate in a single plant network

Technical Primer – Network Topology Basics

Let's review some technical primers before we delve deeper into ISA100.11a mechanisms and features.



Technical Primer – Logical Roles

Note: Devices operating in the field typically incorporate multiple logical roles.

Role	Role Definition and Responsibilities
Input/Output	Sources or consumes data. Does not route.
Router	Routes messages for other devices operating in the wireless subnet.
Backbone Router	Routes data via the backbone. Mitigates between devices operating in the wireless subnet and devices operating on the backbone.
System Manager	The “brains” of the network. Manages all network devices through policy-controlled configurations based on collection of performance parameters reported.
Security Manager	Enables, controls and supervises the secure operation of all devices present in the network.
Gateway	Provides an application interface between the wireless network and the plant network.
Provisioning	Provisions devices with configurations required for operation within the network.
System Time Source	Responsible for maintaining the master time source of the network.

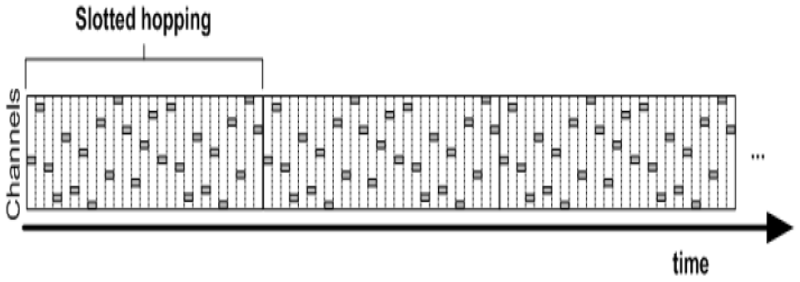
Main Adoption Concern – Data Reliability

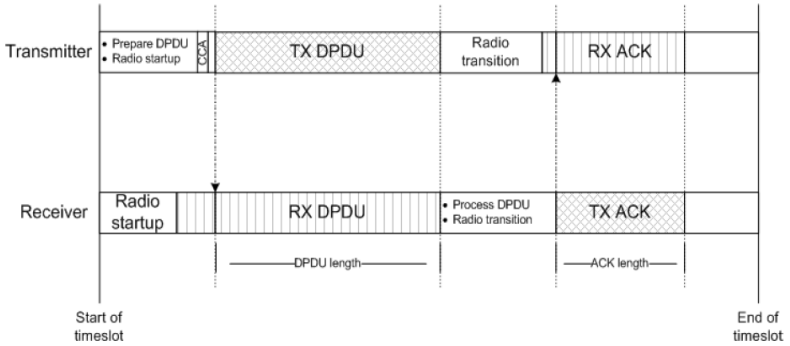
ISA100.11a incorporates a gamut of mechanisms that ensure that communications are highly reliable

- Co-existence mechanisms
  - Time diversity and determinism
  - Collision avoidance
  - Frequency diversity
  - Automatic Repeat-reQuest (ARQ)
  - Spectrum management through channel blacklisting
  - Adaptive hopping
- Path diversity
- Duocast

Time Diversity and Determinism

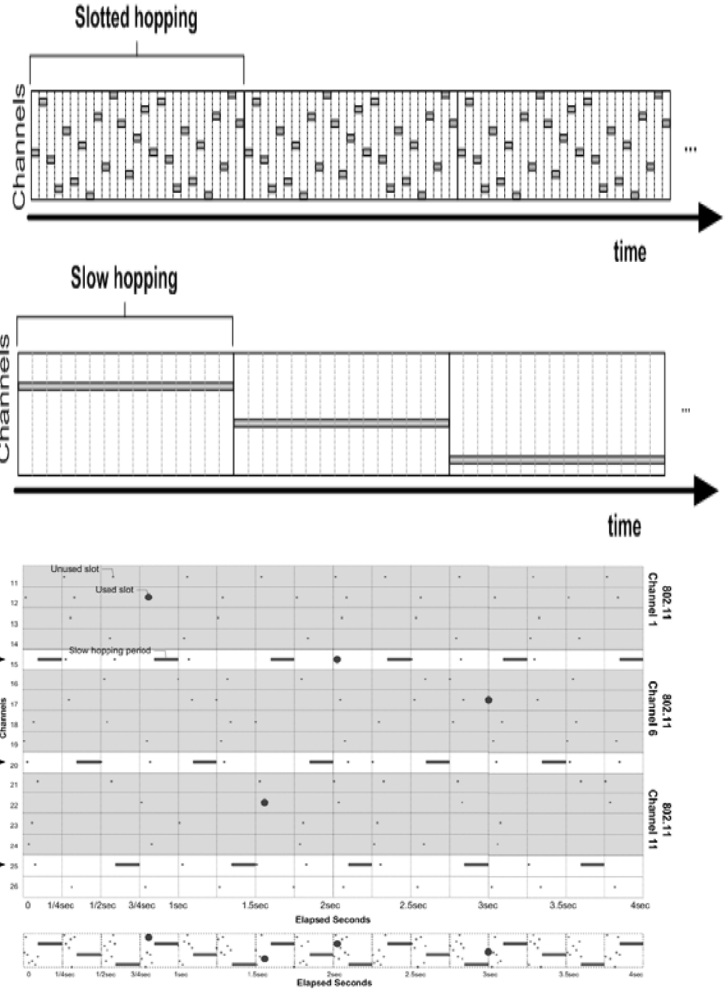
- ISA100.11a systems are fully deterministic
- All devices operating in a wireless subnet communicate at a pre-determined time and pre-allocated frequency channel
- Based on TDMA (time division multiple access) ISA100.11a technology divides time in timeslots of configurable length
- Typical timeslot durations range from10 to 14 ms
- The maximum transmission time of a packet can take approximately 4 ms which results in a 0.004% duty cycle when data is being transmitted once a second
- Therefore wireless transmissions take place in bursts occurring at clearly pre-determined times, increasing robustness to interference and hence data reliability





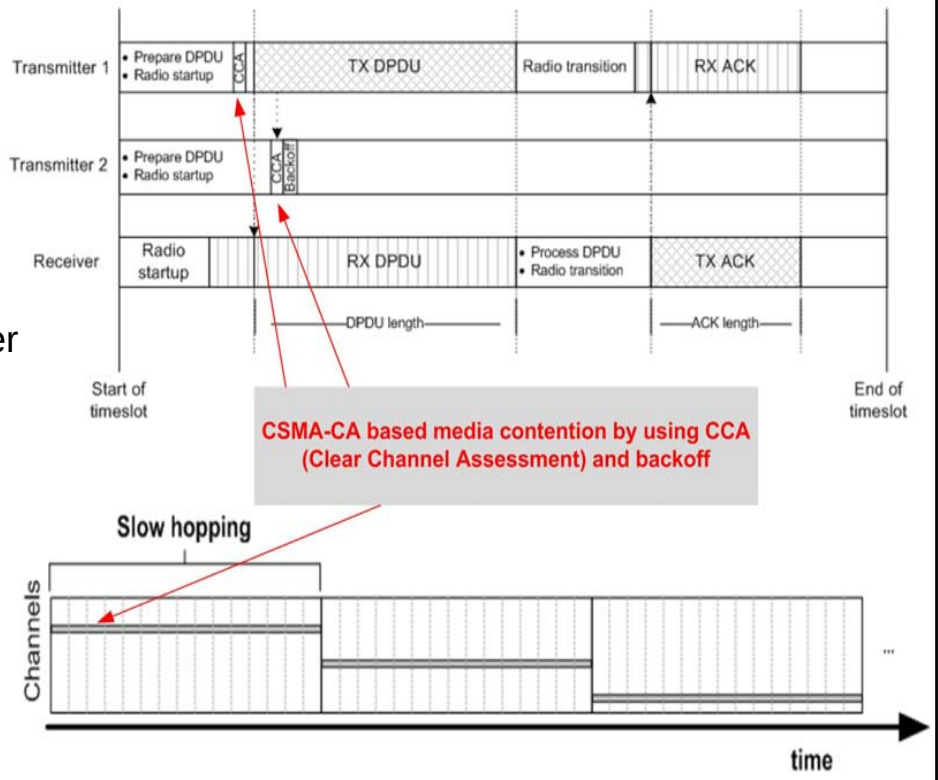
Time Diversity and Determinism

- Configurable timeslot length allow operation using
  - Short timeslots
    - Accommodate predictable, regular traffic
    - Optimized implementations
  - Long timeslots
    - Accommodate extended message wait time
    - CSMA-CA contention at the start of the slot
    - Slow-hopping periods of extended duration by aggregating timeslots
- Not all timeslots are created equal
  - Shared timeslots
    - Accommodate bursty traffic and alarms
    - Utilize CSMA-CA at the beginning of the slot
  - Idle timeslots
    - Accommodate non-periodic traffic
    - Can be activated locally by a neighboring device that needs temporary increased bandwidth



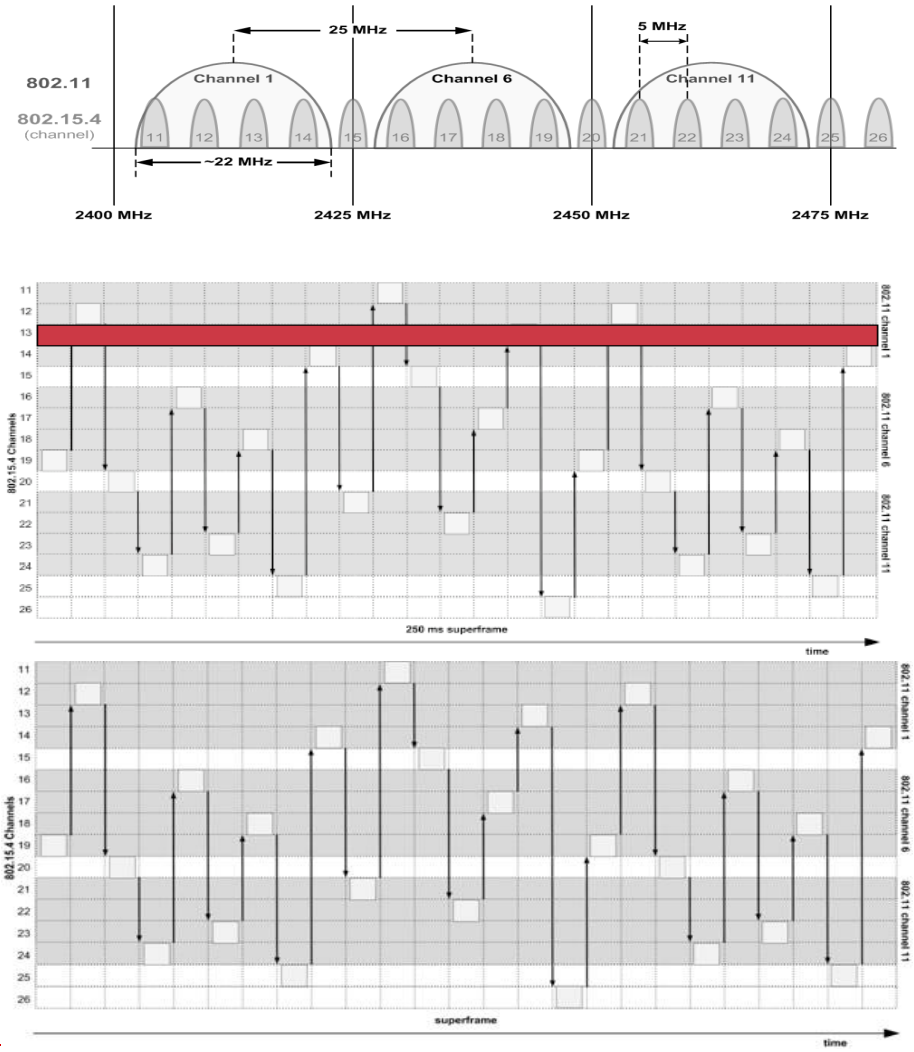
Collision Avoidance

- ISA100.11a allows concurrent media contention based on both TDMA and CSMA-CA resulting in increased data transmission reliability
- ISA100.11a inherits collision avoidance mechanisms from the underlying IEEE 802.15.4 wireless technology such as CCA (clear channel assessment) that allow it to employ CSMA-CA contention
- Before packets are transmitted, the transmitter listens on the channel on which it intends to transmit in order to assess if the channel is clear. If the channel is not clear than the transmitter backs off for a random amount of time after which is attempts to re-transmit the packet
- CSMA-CA contention can be utilized within
  - Dedicated slots
  - Shared slots
  - Slow hopping periods



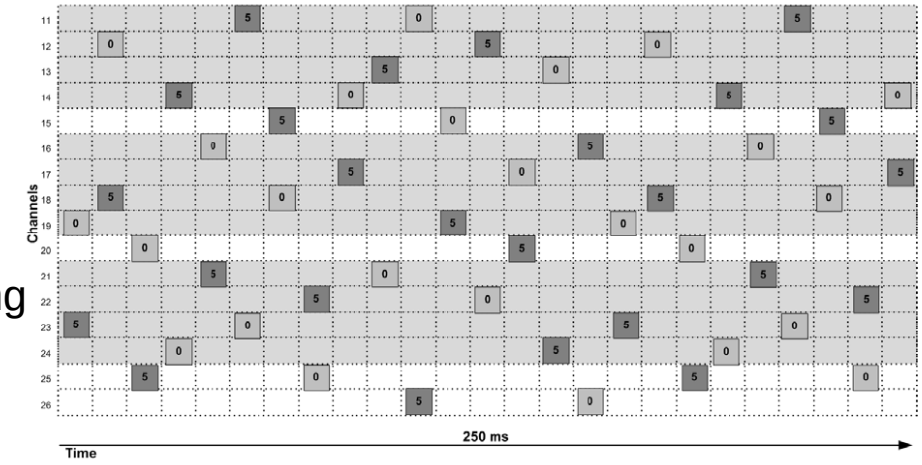
Frequency Diversity

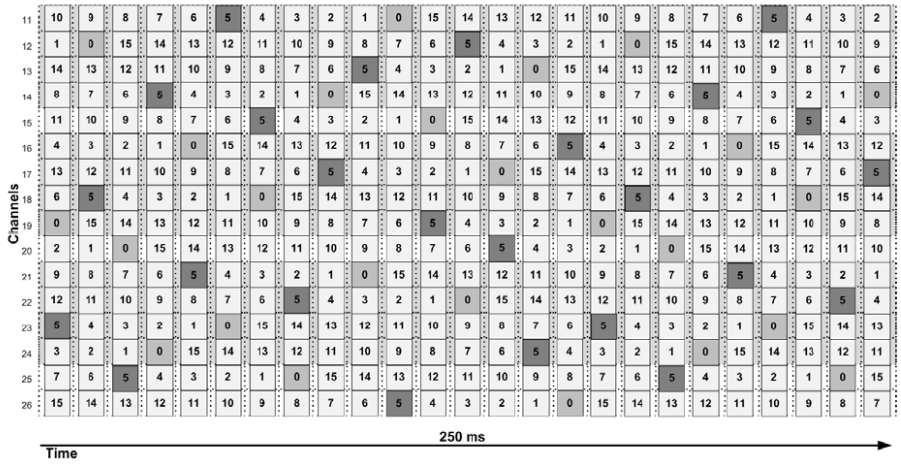
- Frequency diversity tremendously increases data communication reliability by providing
  - Immunity against interference
  - Robustness to mitigate multipath interference effects
- The underlying wireless technology employed by ISA100.11a is IEEE 802.15.4. that organizes the 2.4 GHz unlicensed band into 16 channels
- Devices communicate according to various channel hopping schemes, with each subsequent transmission utilizing the next channel defined in a hopping sequence



Frequency Diversity and ARQ

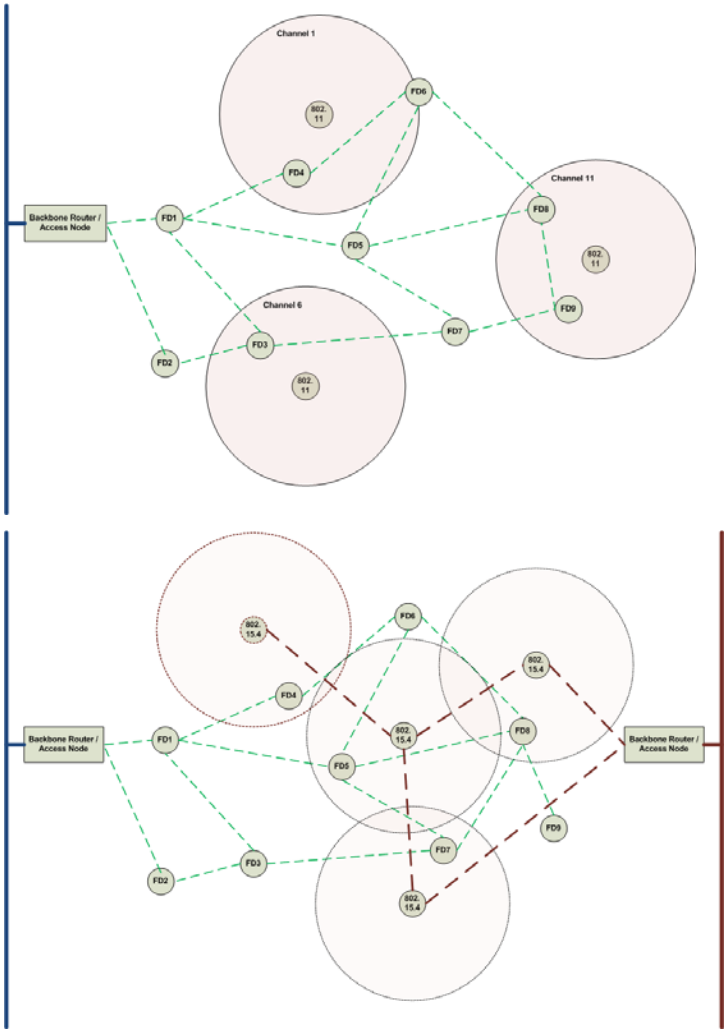
- Frequency hopping significantly increases the probability of successful transmissions throughout the subnet
- Field devices use different offsets into the hopping sequence, resulting in interleaved hopping of devices operating in a wireless subnet
- Every data packet needs to be acknowledged by the receiving device
- ARQ (Automatic Repeat reQuest) ensures that unacknowledged packets are re-transmitted on a different channe over a different frequency
- Frequency hopping used in conjunction with acknowledged communication tremendously increases the reliability of packet delivery





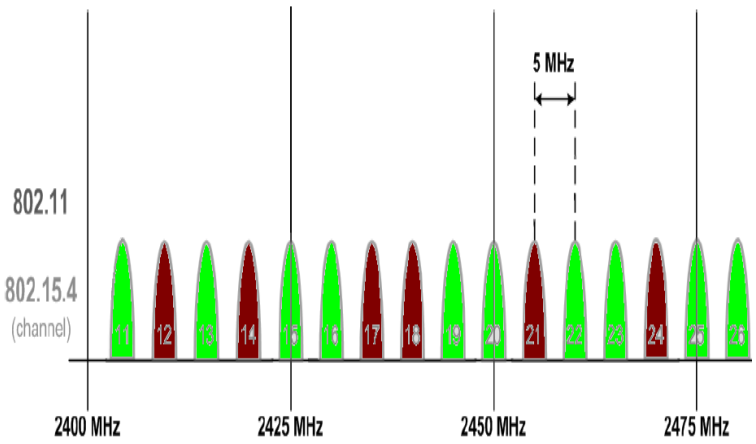
Spectrum Management Mechanisms

- The main purpose of spectrum management mechanisms is to optimize communication reliability by minimizing interference with co-located wireless systems such as:
  - Other 802.15.4 based networks such as ISA100.11a, WirelessHart and Zigbee
  - 802.11 a, b, g, n, LP
  - Bluetooth
  - Microwave ovens
- Spectrum management mechanisms increase reliability by:
  - Continuously assessing how noisy the RF spectrum employed is
  - Continuously assessing the reliability level of the communication among devices
  - Pro-actively adapting usage of the spectrum to existing conditions
- Techniques include
  - Channel blacklisting
  - Adaptive hopping



Spectrum Management through Channel Blacklisting

- ISA100.11a mandates that each wireless device maintains wireless performance statistics indicative of the historical performance of each frequency channel employed
  - CCA back-off counts
  - Number of NACKs received (not ACKs)
  - Count of attempted transmissions
- Channel blacklisting is a technique through which the System Manager (centralized decision) interdicts the usage of particular channel for a period of time based on statistics received from the wireless devices
- These channels are blacklisted from the frequency hopping sequence and devices will only utilize the channels that are clear of external interference
- This mechanism if very effective when wireless devices operates in the vicinity of other wireless equipment that share the same spectrum
- A commonly encountered scenario are co-located 802.11 a,b,g,n wireless routers

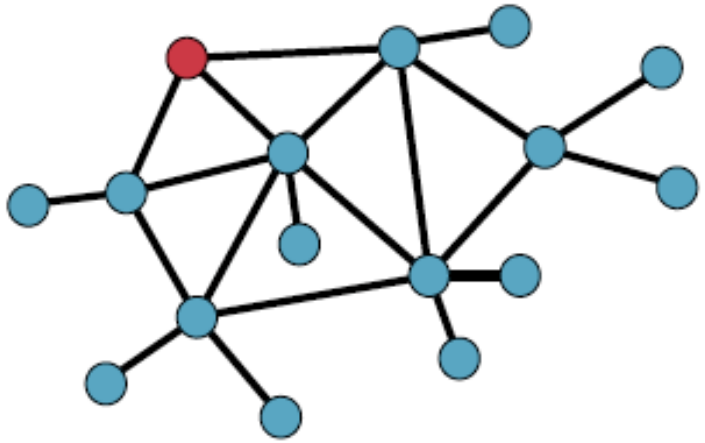


Spectrum Management through Adaptive Hopping

- Adaptive hopping is similar to the channel blacklisting described above except that the decision is made locally based on statistics of wireless parameters collected by the device
- Allows devices to locally manage the spectrum rather than relying on the System Manager to make a decision
- In addition it allows wireless devices to adapt their hopping sequences based on the quality of communication with particular neighbors
- ISA100.11a mandates that devices maintain historical statistics that are indicative of the reliability and quality of communication with particular neighbors
- If device A has poor wireless performance when communicating with device B on a particular channel, it will avoid using that particular channel when communicating with device B
- This gives devices the capability to granularly select the channels they use when communicating with different neighbors and provides robustness to multipath and obstacles that are in the way of communication

Path diversity – Mesh Topologies

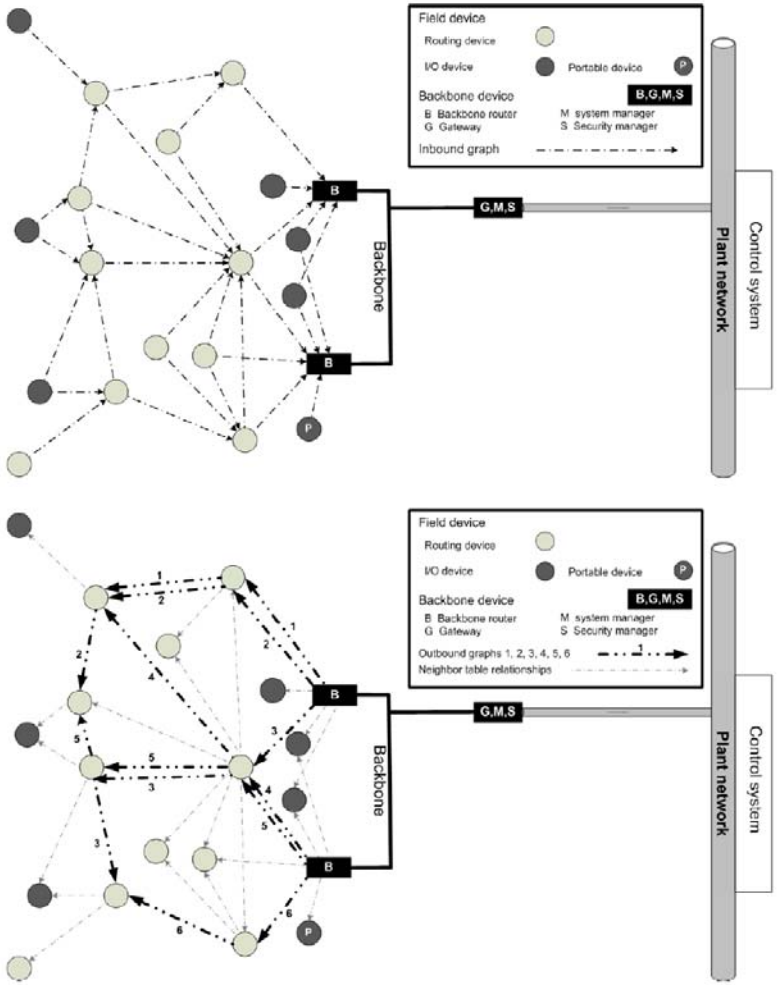
- Mesh topologies based on graph routing support end-to-end network reliability through path redundancy
- Path diversity also mitigates co-existence without user intervention



- Routes are configured by the System Manager based on diagnostics and statistics received from the wireless field devices
- Redundant routes are continually adapted to the spectrum conditions
- Devices also make instantaneous adaptive routing decisions

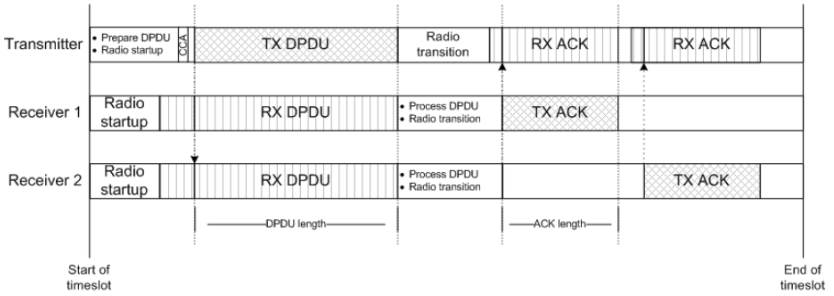
Path diversity – Graph Routing

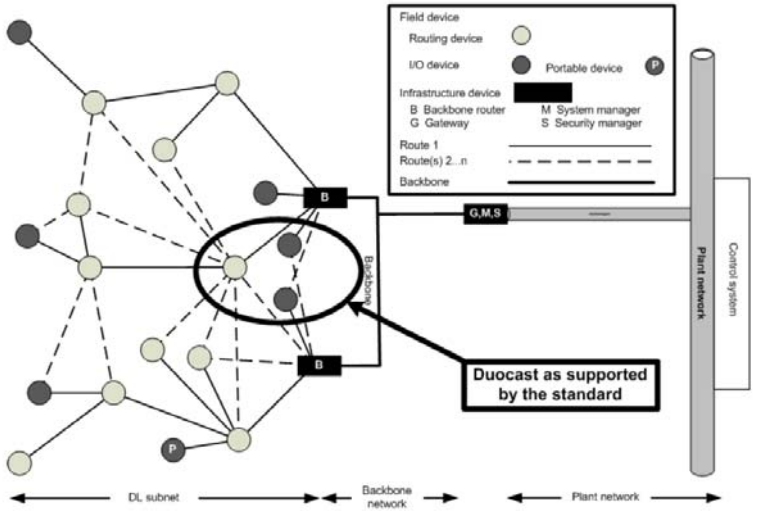
- Graphs are sets of directed links used to carry data packets throughout the wireless subnet
- Graphs are configured by the System Managers
- Data packets “follow” inbound or outbound graphs depending on the final destination of the packet
- Graph routing inherently improves reliability of communication through path redundancy



Duocast

- Duocast is a mechanism through which a device sends a packet that is received and acknowledged by multiple devices within the duration of the same timeslot
- It is typically targeted at wireless field devices that communicate directly with backbone routers but can also be applied for devices that operate deeper within the wireless subnet
- Probability of a successful communication (and hence reliability) increases exponentially when employing duocast (or n-cast)





Ease of Deployment and Use

- Path diversity is accomplished through self-forming and self-healing graph routing that swiftly and continuously adapts to dynamic conditions
- Mechanisms that ensure reliability are transparently configured and operated by the wireless field devices in conjunction with the System Manager
- Mechanisms that ensure secure communication are transparently configured and operated by the wireless field devices in conjunction Security Manager
- ISA100.11a natively supports firmware upgrades with configurable cutover

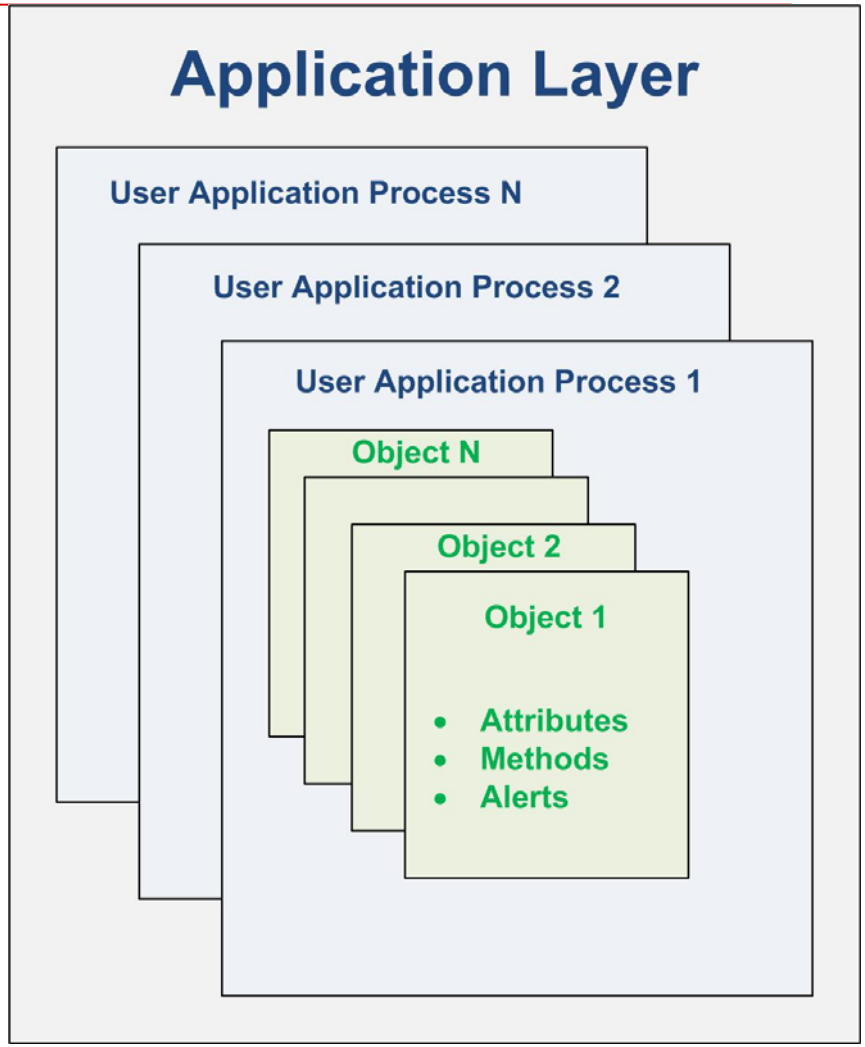
Ease of Deployment and Use

- Native support in the Gateway high side interface (Gateway Service Access Point) for
  - Services
  - Reports
  - Alerts
  - Configuration primitives
- These services give users full visibility into the ISA100.11a network facilitating swift and painless deployments as well as smooth day-to-day operation of the network

Service	Service subtype	Primitive	Description
Session		G_Session request	
		G_Session confirm	
Lease		G_Lease request	
		G_Lease confirm	
Device_List_Report		G_Device_List_Report request	
		G_Device_List_Report confirm	
Topology_Report		G_Topology_Report request	
		G_Topology_Report confirm	
Schedule_Report		G_Schedule_Report request	
		G_Schedule_Report confirm	
Device_Health_Report		G_Device_Health_Report request	
		G_Device_Health_Report confirm	
Neighbor_Health_Report		G_Neighbor_Health_Report request	
		G_Neighbor_Health_Report confirm	
Network_Health_Report		G_Network_Health_Report request	
		G_Network_Health_Report confirm	
Time		G_Time request	
		G_Time confirm	
Client/Server		G_Client_Server request	
		G_Client_Server indication	
		G_Client_Server response	
		G_Client_Server confirm	
Publish/Subscribe	Publish	G_Publish request	
		G_Publish indication	
		G_Publish confirm	
	Subscribe	G_Subscribe request	
		G_Subscribe confirm	
	Publish_Timer	G_Publish_Timer indication	
	Subscribe_Timer	G_Subscribe_Timer indication	
	Watchdog_Timer	G_Watchdog_Timer indication	
Bulk_Transfer[1]	Open	G_Bulk_Open request	Allows upload and download of large items such as firmware images and sample buffers
		G_Bulk_Open confirm	
	Transfer	G_Bulk_Transfer request	
		G_Bulk_Transfer confirm	
	Close	G_Bulk_Close request	
		G_Bulk_Close confirm	
Alert	Subscribe	G_Alert_Subscription request	Allows subscription and receipt of specific alerts
		G_Alert_Subscription confirm	
	Notify	G_Alert_Notification indication	
Gateway_Configuration	Read	G_Read_Gateway_Configuration request	
		G_Read_Gateway_Configuration confirm	
	Write	G_Write_Gateway_Configuration request	
		G_Write_Gateway_Configuration confirm	
Device_Configuration	Read	G_Read_Device_Configuration request	
		G_Read_ Device_Configuration confirm	
	Write	G_Write_ Device_Configuration request	
		G_Write_ Device_Configuration confirm	

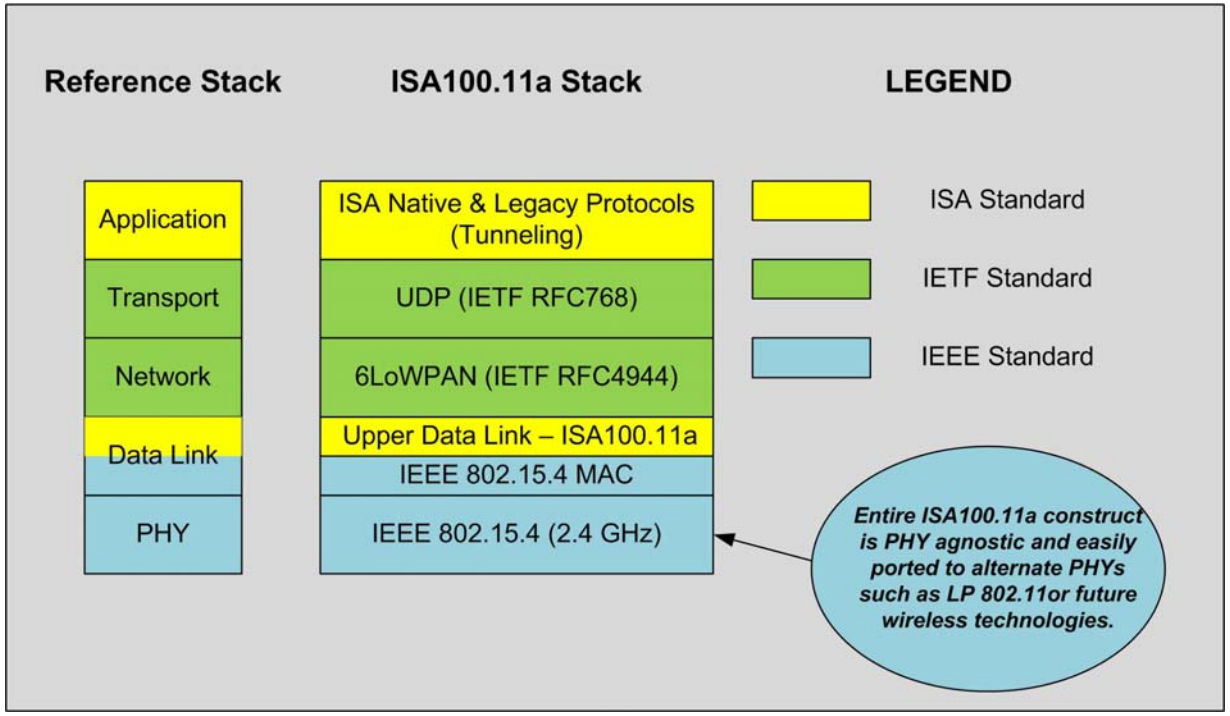
Extensible in the Future

- The Application layer is
  - Flexible
  - Modular
  - Extensible
  - Object based
  - Future proof
  - Easily customizable
  - Accommodates a wide variety of applications
- Building blocks
  - UAPs
    - Objects
      - Attributes
      - Methods
      - Alerts
- Multiple applications are supported by the same device through UDP port addressing



Standards Based Solution

- The entire ISA100.11a stack is constructed employing widely industry accepted and proven standards
- Stack architected in strict adherence to the reference ISO model



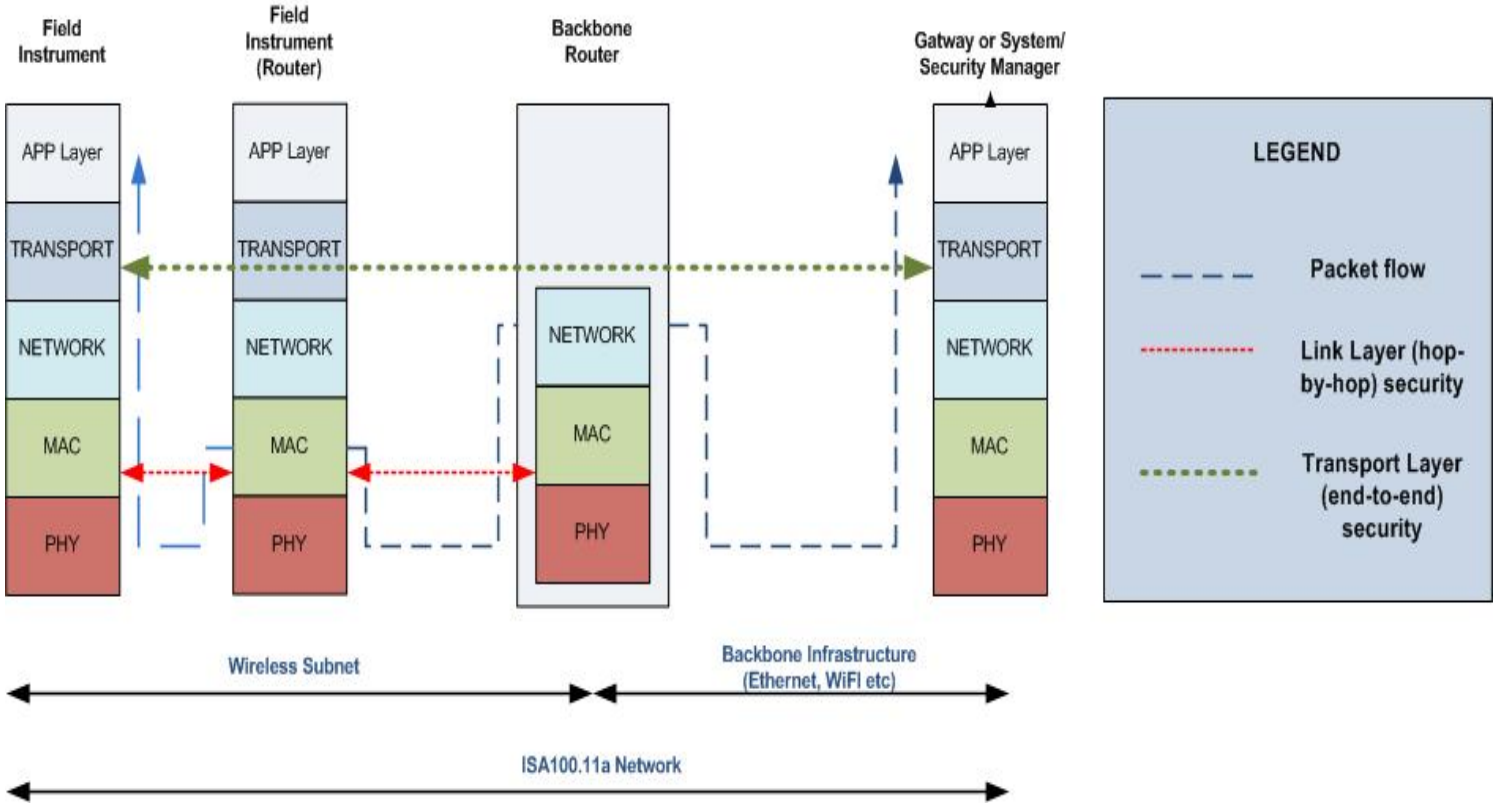
Sound Security

The security mechanisms incorporated in the ISA100.11a standard were designed to meet the following requirements and constraints:

- Message authenticity ensures that messages received are originated by an authorized device and have not been modified by an outside, rogue entity
- Guaranteed data confidentiality through state-of the art encryption
- Ensure data integrity of data transferred over the wireless network
- Provide protection against replay and delay attacks, a vital aspect for industrial applications

Two-layered Security

The ISA100.11a standard incorporates a two-layered security methodology as depicted in the figure below



Two-layered Security

- **Link Layer** security is associated with hop-to-hop authentication and encryption
  - ISA100.11a wireless subnets are multi-hop, mesh enabled subnets with packets of data being routed over multiple devices to the subnet extraction point
  - Each router authenticates and encrypts/decrypts the packet that it routes
- **Transport Layer** security is associated with end-to-end authentication and encryption of data messages
  - The originating device authenticates and encrypts the packet at the transport layer, and only the destination authenticates and decrypts the packet
  - This is accomplished through sessions that are established between pairs of devices that communicate at the transport layer

Policy Based Security

- Various levels of authentication and encryption can be enabled for both layers. These levels are inherited from the security policies supported by IEEE 802.15.4, the underlying wireless technology on which ISA100.11a is based
- Policies distributed with cryptographic material, permit application specific security levels
- The Security Manager controls the policies for all the cryptographic materials it generates
- The ISA100.11a standard uses state-of-the-art encryption based on AES-128 block ciphers.

Security Policy	Authentication Message Integrity Code (MIC) length	Encryption
MIC-32	4 bytes	Off
MIC-64	8 bytes	Off
MIC-128	16 bytes	Off
ENC-MIC-32	4 bytes	On
ENC-MIC-64	8 bytes	On

Time-stamped Security

- In order to provide protection from a variety of attacks, the ISA100.11a standard employs time stamps in its security by including it in the nonce needed for the AES-128 encryption engine
- ISA100.11a networks operate based on a tightly synchronized sense of time. The time basis used in ISA100.11a networks is based on TAI (atomic international time) and all devices within the network are continuously synchronized to TAI
- Transport layer security uses a time stamp in the nonce that indicates when the data packet was created. The final recipient of the device attempts to authenticate the data packet, but if the packet was created more than N seconds ago (configurable), the recipient will discard the packet. This provides protection against replay attacks which is vital for industrial applications where a malicious attack can disrupt operations

The Key is the Key

- Symmetric keys are used for data encryption and authentication
- Asymmetric keys can be used for the join process
- Each key has an expiration time and can be updated
- Asymmetric-key security certificates are optional

Symmetric keys used include:

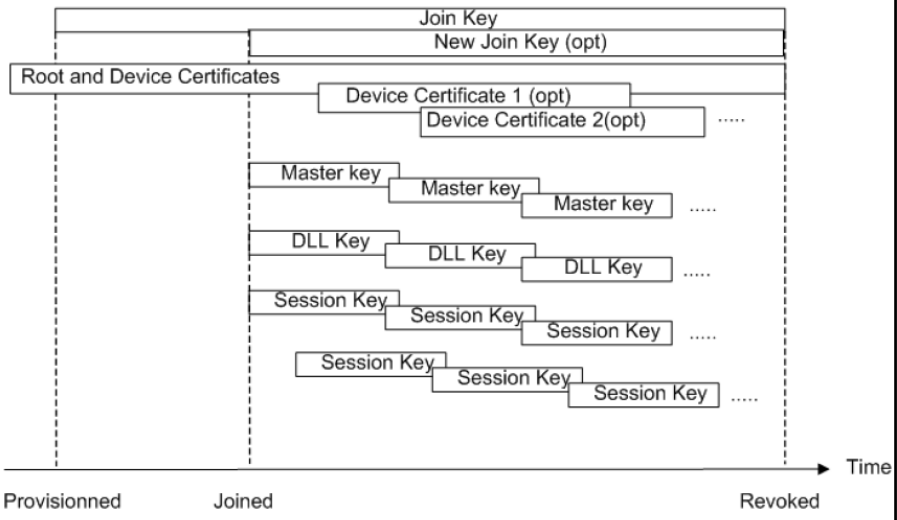
Global Key - a well known key that shall not be used to guarantee any security

Join Key **-** a key received at the conclusion of the symmetric key provisioning. It is used to join the network and to receive the Master Key.

Master Key **-** a key first derived at the conclusion of the key agreement scheme, and used for communication between the Security Manager and devices. It expires and needs to be periodically updated

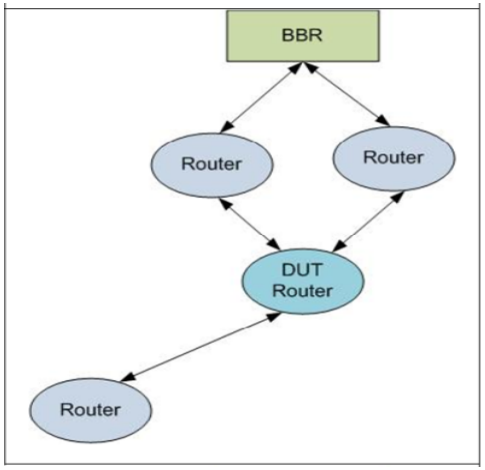
DL Key **-** a key used to compute the MIC at the link layer. It expires and needs to be periodically updated

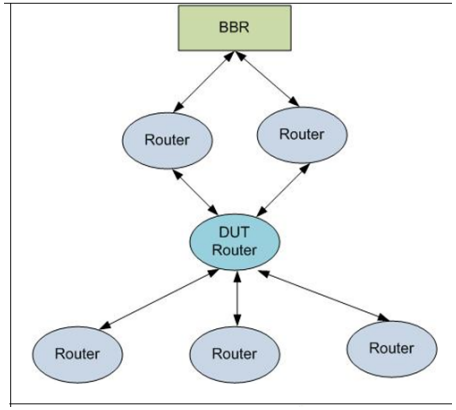
Session Key **-** an optional key used to encrypt and/or authenticate PDUs at the transport layer. It expires and needs to be periodically updated



Prolonged Battery Life

- User generated requirements indicate that field instruments need to have a 3-5 year battery life
- Coordinated network scheduling (determinism) allows for prolonged battery life
- Devices are allocated precise timeslots when they need to communicate (Tx/Rx)
- The rest of the time is spend in deep sleep mode operation followed by synchronized wake-ups





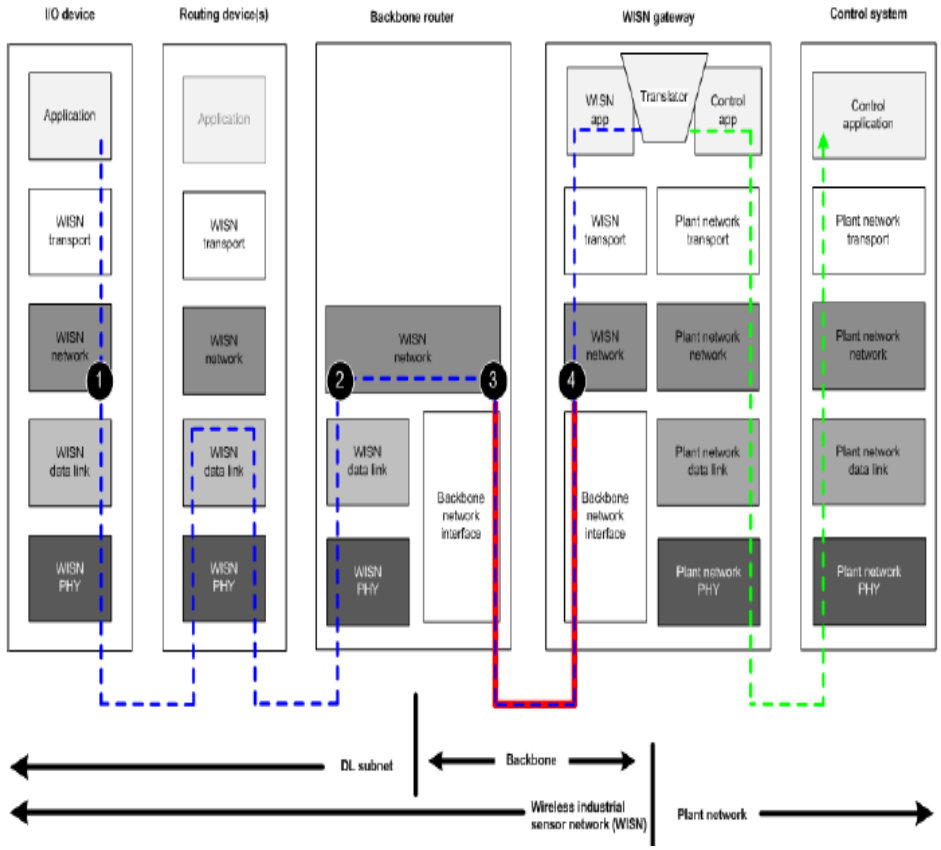
Prolonged Battery Life

- ISA100.11a mandates that each device report its estimated battery life and energy capacity related attributes to the System Manager
- System Manager allocates communication links to devices based on their reported energy capabilities

Energy Attribute	Description	Unit
Energy Life	Estimation of the remaining battery life	Positive number for months and negative number for days
Listen Rate	Capacity of the device to operate its receiver	Seconds/hour
Transmit rate	Capacity of the device to transmit data	Packets/minute
Advertisement rate	Capacity of the device to transmit advertisements	Advertisements/minute

IP Addressability

- Network layer is based on IETF RFC4944 (6LoWPAN)
- IP connectivity to the field device through compressed IPv6 and UDP packets
- Addressing scheme
  - EUI-64 (64 bits)
  - IPv6 (128 bits)
  - Short address (16 bits IEEE 802.15.4)

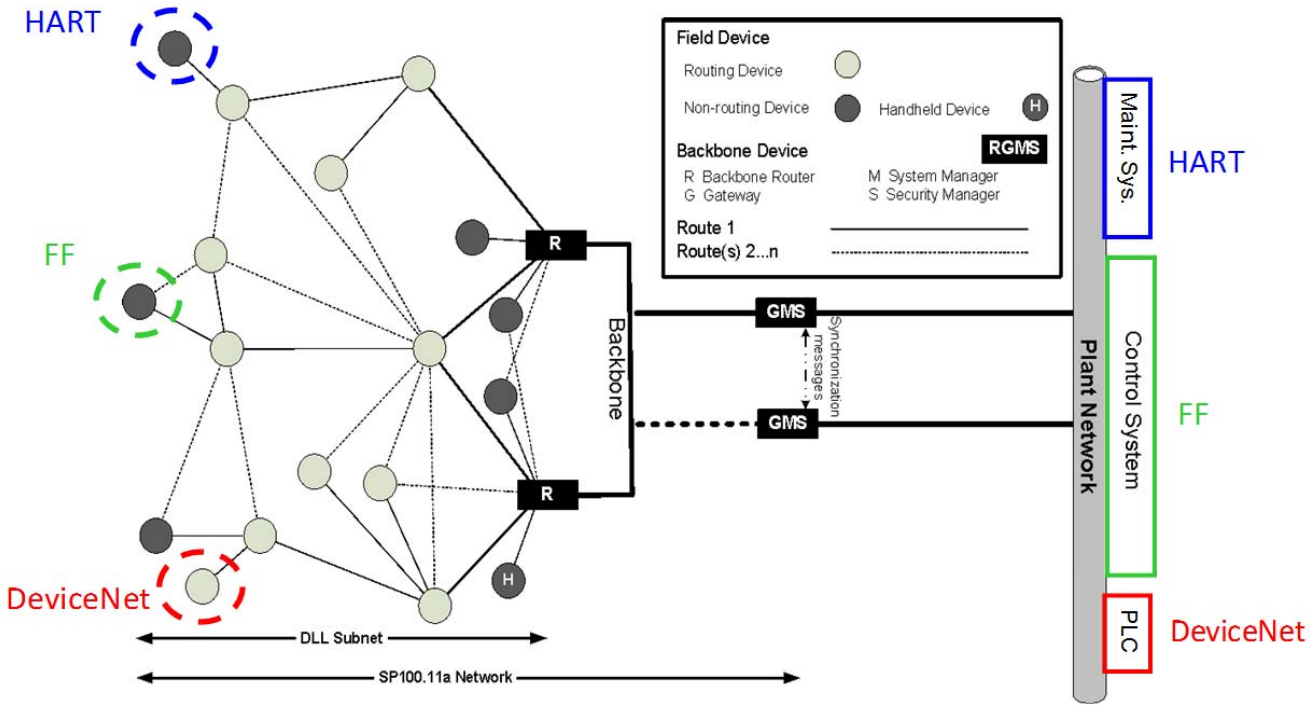


IP Addressability (continued)

- Backbone router responsible for:
  - Address translation
  - Packet expansion
  - Routing on the backbone
- ISA100.11a allows for Application PDUs as large as 1280 bytes
- Fragmentation/de-fragmentation mechanism with optional packet recovery mechanism
- Does not imply that backbone needs to be IP based

Single Plant Network

- Architected to concurrently accommodate multiple protocols at the device and host level
- Applications run in an interoperable manner over a common network infrastructure



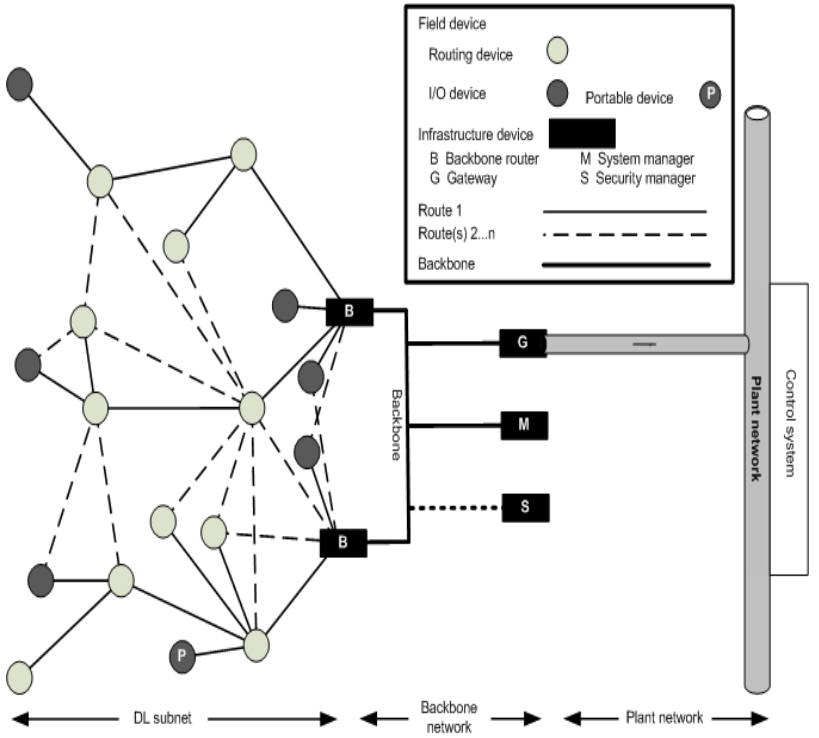
Single Plant Network

Technology employed on the backbone is not mandated allowing for combinations of:

- Wired and wireless systems
- IP based or non-IP based technologies
- Proprietary or standardized technologies
- Low-bandwidth (sensor data) or high-bandwidth (video, voice)

Single Plant Network

- ISA100.11a network architecture allows for multiple subnets that operate and co-exist on the same backbone
- Single System and Security Manager is responsible for managing multiple subnets, resulting in
  - Simplified network management
  - Synchronized operation across subnets
  - Better airtime utilization due to synchronized operation



Q & A

Questions?