

ISA100.11a, Release 1

An Update on the First Wireless
Standard Emerging from the
Industry for the Industry

21 May 2008

Prepared by Pat Kinney

Presented by Benjamin Rolfe



Setting the Standard for Automation™

ISA100.11a, Release 1

An Update on the First Wireless
Standard Emerging from the
Industry for the Industry

Standards
Certification
Education & Training
Publishing
Conferences & Exhibits

ConnectivityWeek 2008

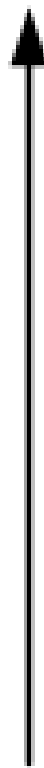
ISA100.11a Working Group Scope

This project will define all specifications including security and management; for wireless devices serving application classes 1 through 5 for fixed, portable and moving devices.

The project's application focus will address performance needs for periodic monitoring and process control where latencies on the order of 100 ms can be tolerated with optional behavior for shorter latency.

ISA100 Usage Classes



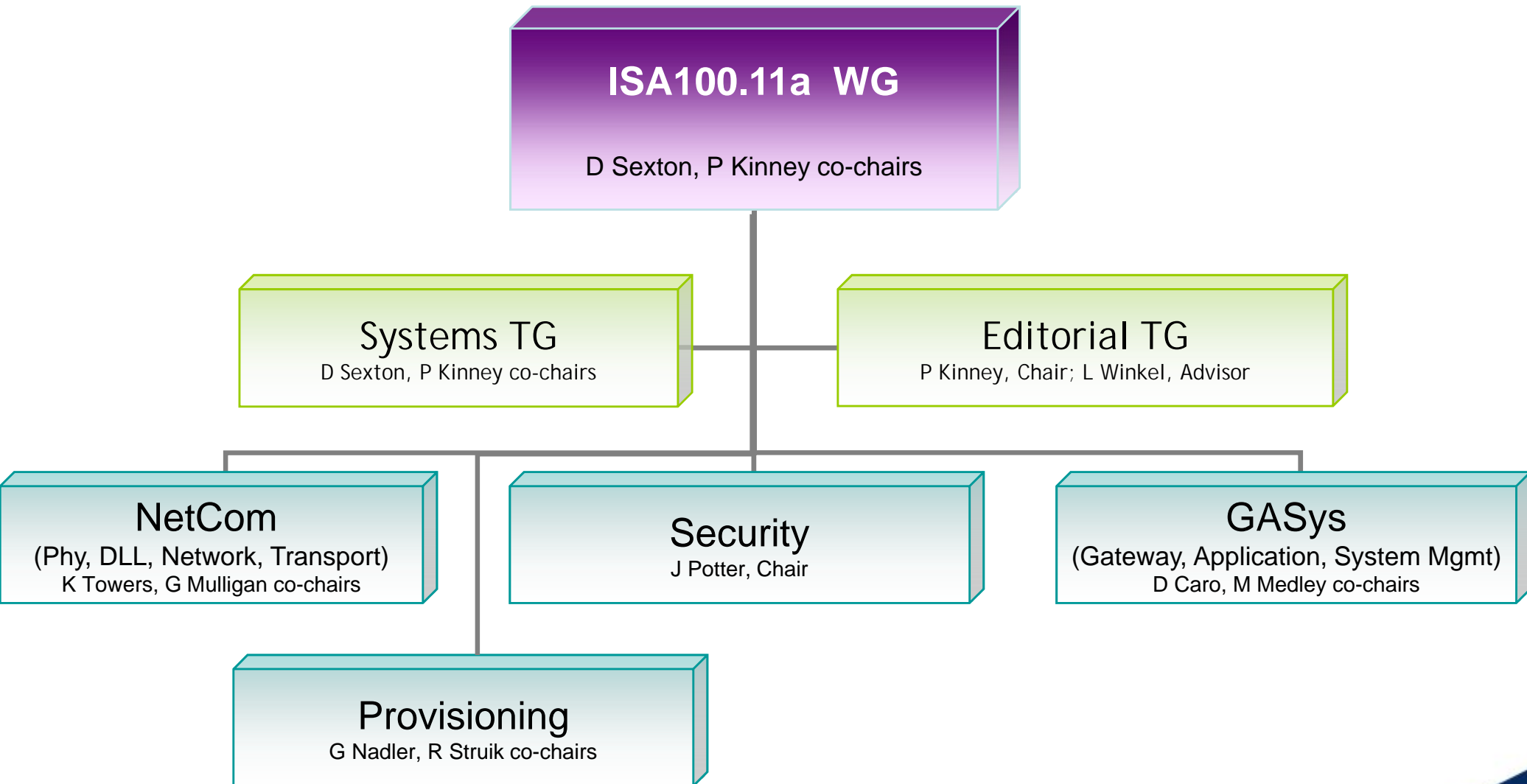
<i>Category</i>	<i>Class</i>	<i>Application</i>	<i>Description</i>	Importance of message timeliness increases 
<i>Safety</i>	0	Emergency action	(always critical)	
<i>Control</i>	1	Closed loop regulatory control	(often critical)	
	2	Closed loop supervisory control	(usually non-critical)	
	3	Open loop control	(human in the loop)	
<i>Monitoring</i>	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)	

ISA100.11a Working Group Charter

This project will address:

- **low energy consumption devices, with the ability to scale to address large installations**
- **wireless infrastructure, interfaces to legacy infrastructure and applications, security, and network management requirements in a functionally scalable manner**
- **robustness in the presence of interference found in harsh industrial environments and with legacy systems**
- **coexistence with other wireless devices anticipated in the industrial work space**
- **interoperability of ISA100 devices**

ISA100.11a WG Organization



ISA100.11a Scope for Release 1

Be an open standard for anyone to implement and deploy

- No need to join any group
- Easily available via the internet
- No restrictions on downloads (other than copyrights)

Be simple to use and deploy for end users

- Written in a clear and concise manner
- Easy to navigate through the standard
- Address needs of users ranging from unsophisticated to networking experts

Assure multi-vendor device interoperability

- Standardize the necessary interfaces while leaving other aspects for vendor customization

ISA100.11a Scope for Release 1

Be focused on:

- **serving process industry applications without excluding factory automation**
 - Focus for release 1 is on process industrial applications
 - Architecture of ISA100.11a will support factory automation
- **in-plant/near-plant**
 - Focus on Local Area Networks (LANs) rather than Metropolitan Area Networks (MANs) or Wide Area Networks (WANs)
- **global deployment**
 - Choose radio bands and security techniques that are deployable throughout the world

Provide technology to address Class 1 (non-critical) to Class 5 applications such as monitoring

- Critical and extremely time sensitive applications will be served in later releases

ISA100.11a Scope for Release 1

Adhere to a comprehensive coexistence strategy

- Coexistence is the ability of wireless networks to perform their tasks in an environment where there are other wireless networks that may or may not be based on the same standard
 - Examples of other wireless networks not based upon the ISA100.11a standard are WiFi/IEEE 802.11, Bluetooth, WirelessHART, etc.
- Coexistence strategy includes:
 - Listen before talk
 - Short messages
 - Low duty cycle
 - Adaptive frequency hopping by channel blacklisting
 - Low power operation

ISA100.11a Scope for Release 1

Include only 2.4 GHz 802.15.4-2006 radios

- Single Physical layer to:
 - facilitate vendor interoperability
 - provide a simpler standard
 - expedite release of standard

Use channel hopping to support co-existence and increase reliability

- Channel hopping is where the channel is periodically changed by all nodes
- Hopping is a proven technique to minimize the impact of interference in a congested band
 - Bluetooth and military backpack radios use hopping

Offer field device meshing and star capability

- Star configurations can provide very quick response times that are necessary for some types of critical applications
- Mesh networks can offer increased robustness, enhanced reliability, greater tolerance to interference, etc

ISA100.11a Scope for Release 1

Use a single application layer providing both native and tunneling protocol capability for broad usability

- Native protocols allow efficient use of the bandwidth and provide for longer battery life of nodes
- Tunneling protocol allows the ISA100.11a network to carry existing protocols such as Fieldbus Foundation, HART, Profibus, Modbus, and others.
 - Allows existing installations to be easily converted to wireless

ISA100.11a Scope for Release 1

Provide simple, flexible, and scalable security addressing major industrial threats leveraging 802.15.4-2006 security

- **Security is a major design facet of ISA100.11a**
 - Includes total life cycle such as configuration, operation, maintenance, etc
- **Security is considered throughout the whole system not just at the Phy layer or MAC sub-layer**
 - Leveraging security aspects of the IEEE 802.15.4-2006 standard allows for reduced costs, quicker implementations, and a broad consensus of security experts

ISA100.11a Release 2 commitments

ISA100.11a Work Group agreed that release 2 will include:

- **Critical class 1 to 5 applications in addition to monitoring**
 - To address critical and/or time sensitive applications
- **Additional gateway functionality as needed**
 - Release 1 will standardize only basic functionality
- **Additional network manager functionality as needed**
 - Release 1 will standardize only basic functionality
- **Dual/alternate Phys such as narrow band frequency hopping, sub-GHz, licensed bands, high speed, 5 GHz, etc.; driven by user requirements**
 - Release 1 focused on only one radio that may not be appropriate for some applications and/or user needs

ISA100.11a Release 2 Proposed Roadmap



At an ISA100 meeting last year, the Marketing Working Group unanimously approved a motion to recommend development of the following standards for the ISA100 roadmap:

- Factory Automation (Discrete Focus)
- Building Automation (Industrial Facility Focus)
- Transmission & Distribution (Long Distance Focus)
- RFID (.21 - Tagging Focus)
- In collaboration with SP99, Universal Wireless Security (Standard Security Focus for the ISA100 family of standards, Building on .11a)

- To address a diverse marketplace such as industrial, with applications that require significantly different and sometimes incompatible behavior, standards embrace options and configuration settings.
- Options: behavior that while it is not mandated by the standard is totally specified by the standard
 - Example: a standard may not require a device to have a high data rate in addition to the normal one, but if the device does have that higher data rate it must conform to the specifications for that higher data rate
 - Configuration settings: a standard may provide a range of settings that will allow a device to be optimized for an application
 - Example: a standard may provide a range of transmit powers for a device whereas the device would choose one and operate at it

Application Profile: describes functional requirements and points to existing standards, selecting and binding options within those standards. An implementer who then designs a specific module and/or system should be reasonable assured that another designer's (manufacturer's or supplier's) modules will properly function within the same system. This includes all aspects of definition: mechanical, electrical, protocol, environmental, and system considerations

- Application profiles will not be defined by the ISA100.11a standard but could be defined via the Wireless Compliance Institute
- Application profiles allow for additional branding by ISA100.11a equipment suppliers.

Role Profile: A set of one or more role definitions, and where applicable, the identification of chosen classes, subsets, option and parameters of those definitions, necessary for accomplishing a particular role.

An implementer who then designs a specific module for a system role should be reasonable assured that another designer's (manufacturer's or supplier's) modules will properly function within the same system.

Roles include System manager, Gateway, Backbone router, Security Manager, System time source, Provisioning, Non-routing device, and Field router

ISA100.11a Document Deliverables

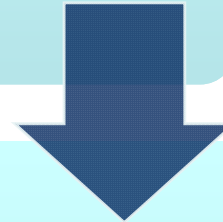
Principles of Operation (“internal” document for WG use)

Overview of how the system works along with explanations of what each ISO layer provides.

Descriptions of configuration and provisioning

Illustrates the architecture of the standard

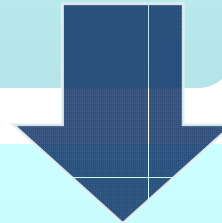
Purpose is to validate the technical direction of editor team



Preliminary Draft (“internal” document for WG use)

Preview of draft standard but with some omissions and TBDs

Purpose is to validate appropriate details of upcoming draft



Release 1 Draft Standard

Includes short descriptions of general operation

States all of the requirements for compliance to the standard

Schedule

- ISA100.11a WG created 18 October 2006
- Principles of Operation 15 August 2007
- Preliminary Draft 21 December 2007
- Draft Standard 5 May 2008
- WG letter ballot start 5 May 2008
- Committee Letter Ballot Start 1 October 2008
- S&P Board Approval of ISA100.11a Standard 9 December 2008

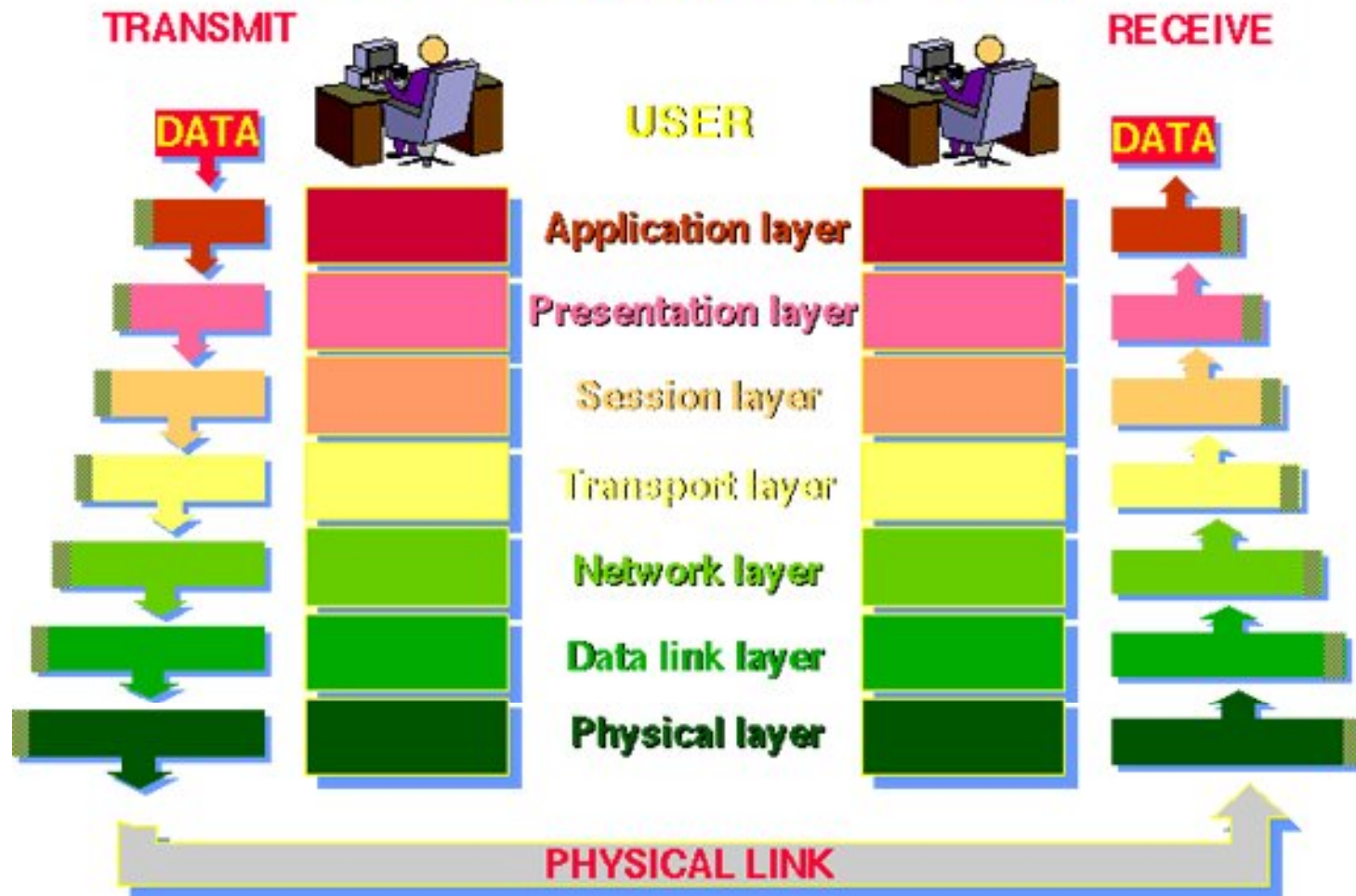
Technical Overview

1. Background
2. Objectives
3. System
4. System Management
5. Physical layer
6. Data Link Layer
7. Network Layer
8. Transport Layer
9. Application sub-Layer
10. Gateway
11. Security

Technical Overview: Background Information



THE 7 LAYERS OF OSI



The Abdus Salam International Centre for Theoretical Physics
(http://users.ictp.it/~radionet/1998_school/networking_presentation/index.html)

Technical Overview: Objectives

- Release 1 provides reliable and secure operation for non-critical monitoring, alerting, supervisory control, open loop control, and closed loop control applications.
 - defines the specifications for low data rate wireless connectivity with fixed, portable, and moving devices supporting very limited power consumption requirements
- Application focused on needs for monitoring and process control
 - where latencies on the order of 100 ms can be tolerated
 - with optional behavior for shorter latency
- Provides robustness in the presence of interference found in harsh industrial environments and with legacy systems.
- Coexists with other wireless devices anticipated in the industrial work space as well as providing interoperability of ISA100 devices.
- Open standard that is intended to be of low complexity for end users to use and deploy

Technical Overview: System

How each ISO layer works together to accomplish system functionality

- ISA100.11a covers networks of wireless devices connected to an application.
- To accomplish this, a full specification from the physical layer to the application layer is required.
- ISA100.11a defines suitable interfaces to allow for those components typically used in a complete system but are not within the scope of ISA100.11a
- The network configuration has a series of wireless field devices, some of which can and will route messages, and some of which may not have routing capabilities or may not be configured to use routing capabilities.
- The network is attached to a user application at a gateway.
 - The gateway provides the transition from ISA100.11a into the users' application.

Technical Overview: Provisioning

Provisioning includes those efforts required to prepare a device to be able to join a network

- At the end of the Provisioning process, the device must have the following information:
 - Network Secured with Symmetric keys
 - A 128-bit join key
 - The 64-bit EUI of the security manager that generated the join key.
 - Network Secured with Public keys (asymmetric keys)
 - Certificate signed by a certificate authority trusted by the target ISA100.11a network.
 - Non-secure Network:
 - well-known, published, non-secret 128-bit key common to all ISA100.11a networks

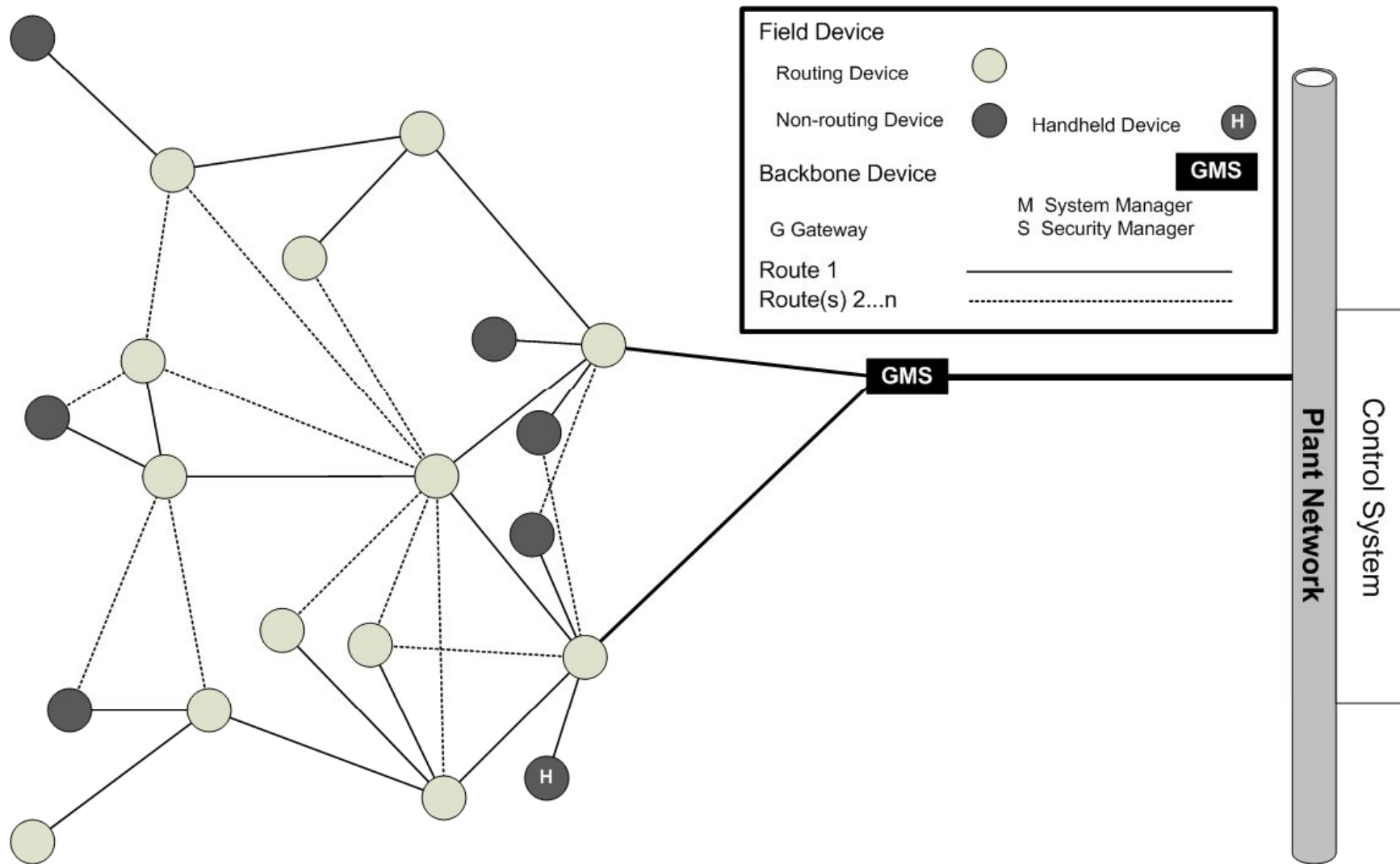
Provisioning can be accomplished via the device's radio and by other means such as infrared, connectors, etc.

Technical Overview: Security – Joining

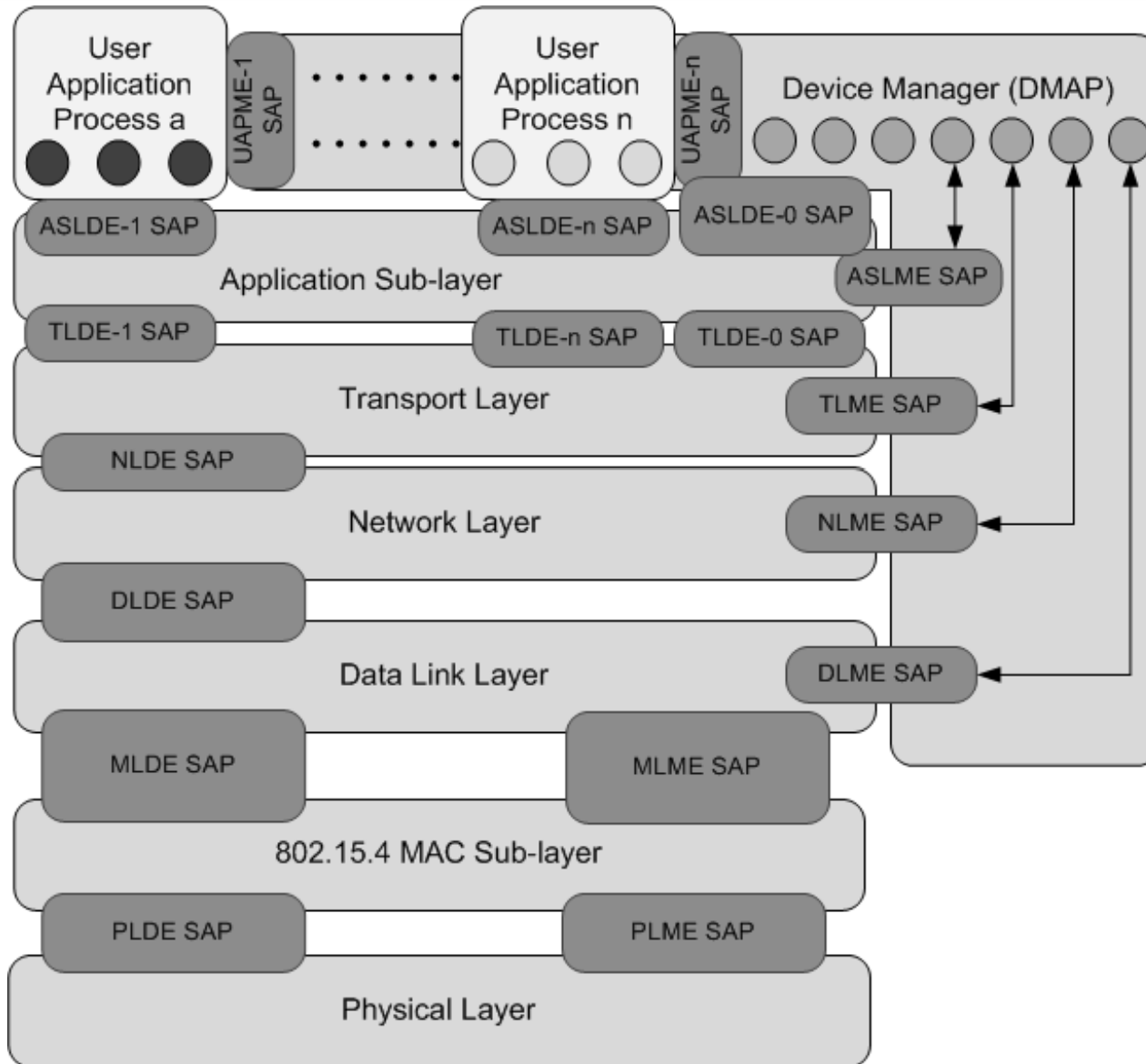
Join process is how a new node is admitted into the network

- Join process follows the provisioning process
- Provides the device with information required to communicate with:
 - direct neighbors
 - system manager
 - security manager
- At the end of the join process, the system shall have the following state:
 - The new node and the security manager share a symmetric long-term master key
 - The new node has the required cryptographic information and non-cryptographic information to talk to its direct neighbors
 - The new node has a contract with the system manager.

Technical Overview: System



Technical Overview: System



Technical Overview: System Management

Supports management of the various communications resources across the ISA100.11a network and across all layers of the architecture

- The purpose of the ISA100 management functions is to support management in the following five areas:
 - fault
 - configuration
 - accounting
 - performance
 - Security
- The primary components of the management service include a device management application process that resides on every ISA100.11a device, as well as one or more system manager applications that reside on a small subset of devices.

Technical Overview: Phy & DLL Layers

Physical layer: Radio layer

- Defined as compliant to IEEE 802.15.4-2006 2.4 GHz DSS

Data Link Layer: defines the format of data on the network

- Consists of:
 - IEEE 802.15.4-2006 MAC sub-layer
 - Upper DLL sub-layer
 - Shim layer between MAC and Upper DLL
- Upper DLL provides:
 - TDMA
 - Channel Hopping
 - Mesh routing

Technical Overview: Network Layer

Provides inter-networking routing

- The functions offered by the network layer are divided into:
 - addressing
 - routing
 - quality of service
 - management functions
- Provides inter-networking routing; i.e. provides mesh to mesh routing
- Frame format in accordance with IETF RFC 4944

Technical Overview: Transport Layer

In the five layer ISA100.11a model, transport is the fourth layer, sitting right under the application layer and on top of the network layer.

- The transport layer responds to service requests from the application layer and issues service requests to the network layer.
- The transport layer is responsible for end-to-end communication and operates in the communication endpoints (as opposed to the routing devices).
- The ISA100.11a transport layer performs datagram services with optional security
 - A datagram is an independent, self-contained data packet that does not rely upon earlier data exchanges

Technical Overview: Application sub-Layer

Provides capabilities and services to enable an open interoperable ISA100.11a application environment.

- provide support for wireless field devices and to enable a gateway to integrate an ISA100.11a wireless network and its devices with a host control system
- object-oriented modeling concepts support both ISA100.11a native and non-ISA100.11a native (legacy) protocol tunneling applications.
 - An object model is a protocol-, platform-, and language-neutral means of describing and distinguishing components (system elements) that have a unique identity

Technical Overview: Gateway

- Provides portal between ISA100.11a and another system
- ISA100.11a provides support for protocol translation. The support includes a tunneling object that fits within the application layer structure and provides generic services for protocol translation.
 - ISA100.11a does not provide the actual protocol translators, only the supporting mechanism.

Technical Overview: Security

Provides authentication, encryption, authorization services

- The communications security functionality for ISA100.11a release 1 is primarily transmission security with authorization based primarily on device identity and configured plant communications relationships
- Transmission security is provided for the DLL layer and for the transport layer
 - DLL security defends against attackers who are outside the system and do not share system secrets
 - Transport security defends against attackers who may be already inside the system and have co-opted (i.e., Trojaned) some devices
- Types of keys supported include both symmetrical keys and non-symmetrical (i.e. public) keys

Conclusion

- The ISA100 committee continues to be committed to rapid development to satisfy the expressed needs of the user community
- “Family of Standards” approach allows a succession of releases focused on market segments
 - Consensus among a balanced membership allows the committee to rise above special interests and do what is right for the industry
 - Ultimate goal is a quality standard that will stand the test of time by adapting to changes within the industrial environment