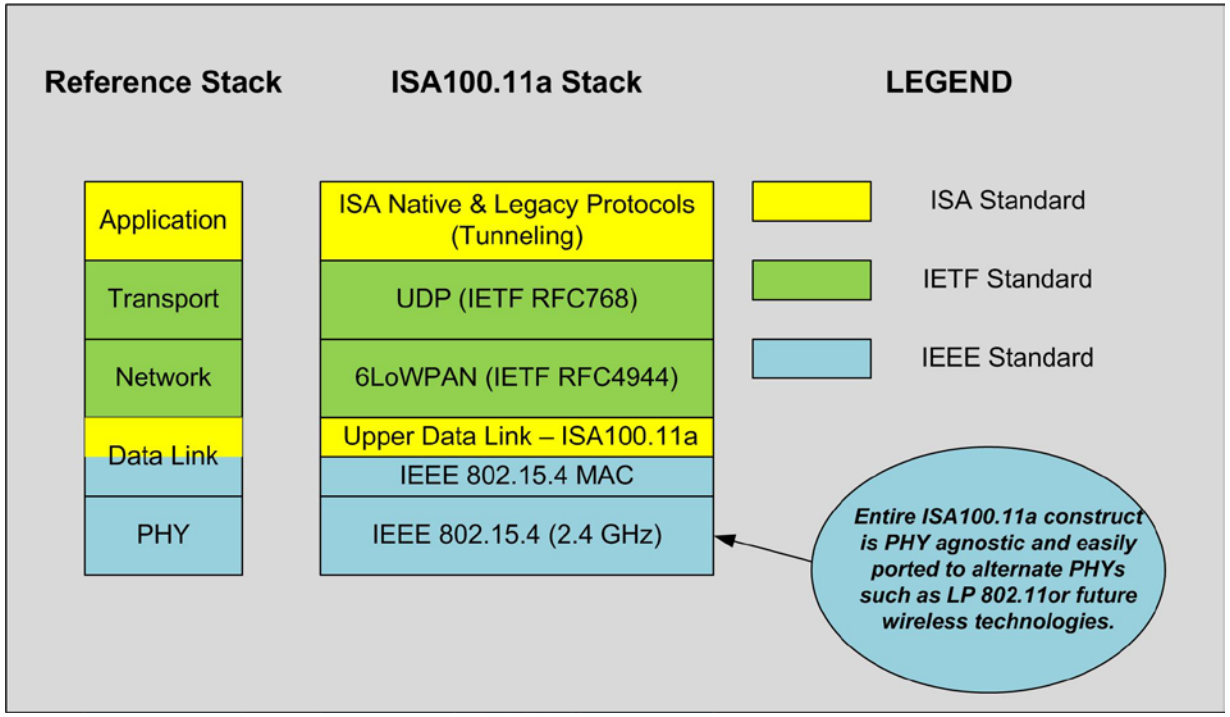
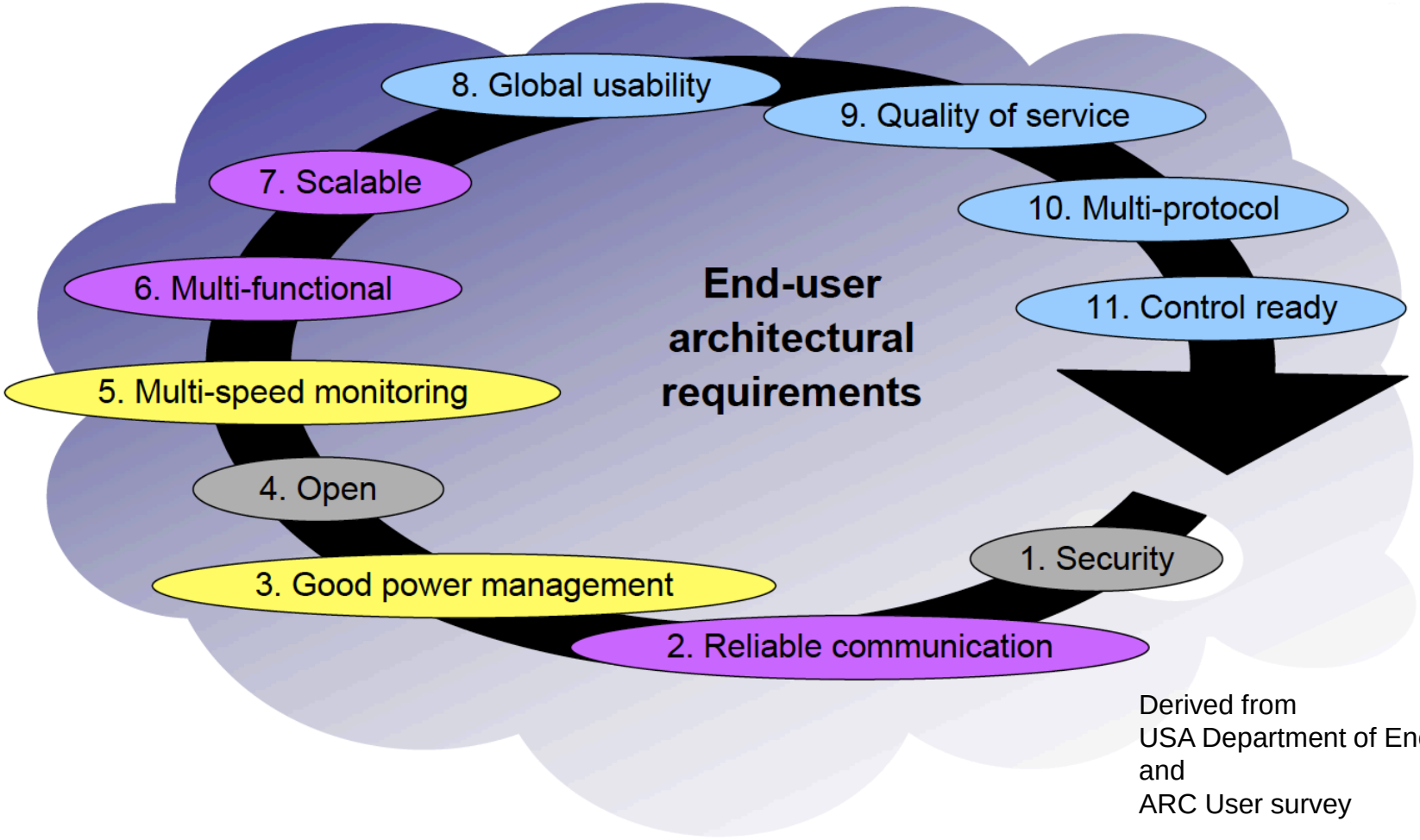
# Standards Based Solution

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



# Fundamental requirements for Industrial wireless sensing




Derived from
USA Department of Energy
and
ARC User survey

***ISA100 solutions must meet all requirements simultaneously***

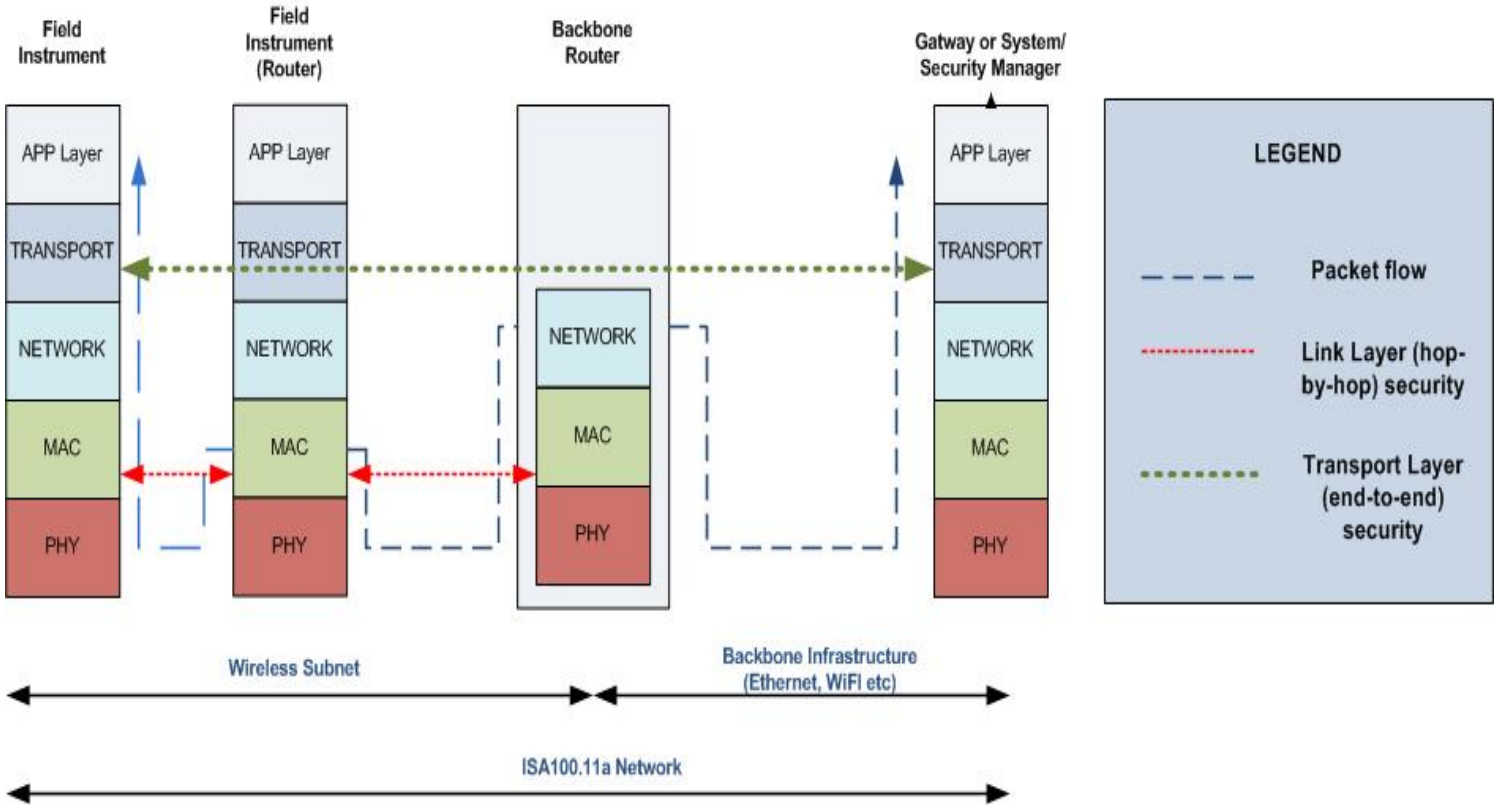
# Sound Security

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