What do we expect from Wireless in the Factory?

And what are we doing about it?

ETSI Wireless Factory Workshop, 15 December 2008

Tim Whittaker
System Architect, Wireless Division

11 December 2008

S4989-P-188 v1.1

What does the Factory, Industrial Control and Automation community want from wireless?

- More data communication to monitor …
  - Equipment condition
  - Secondary processes
  - Environment and emissions
  - Location of assets & tracking
  - Sensors for commissioning
- No new wires
- Reliable communications
- Zero or low maintenance
- Secure
- Low, or at least predictable, latency

Industrial data communication requirements can be categorised

Safety	Class 0: Emergency action *(always critical)*
Control	Class 1: Closed loop regulatory control *(often critical)*
	Class 2: Closed loop supervisory control *(usually non-critical)*
	Class 3: Open loop control *(human in the loop)*
Monitoring	Class 4: Alerting *(short-term operational consequence, e.g. event-based maintenance)*
	Class 5: Logging & downloading/uploading *(no immediate operational consequence, e.g. history collection, SOE, preventive maintenance)*

Source: ISA

- For class 0, even a (single) wired system may not be sufficiently reliable
- The Monitoring classes can be a good fit with wireless communications
- For class 1 and class 2, wireless is generally used only when there's no alternative

In many cases the data rates required are modest

Application area	Likely data volume / frequency
Process temperature sensing	10 bytes / minute
Machinery condition monitoring	1000-50.000 bytes / day
Personal radiation monitor	20 bytes / minute
Portable barcode reader	64 bytes / 10 seconds
Environment alarm	10 bytes / event

Source: ISA

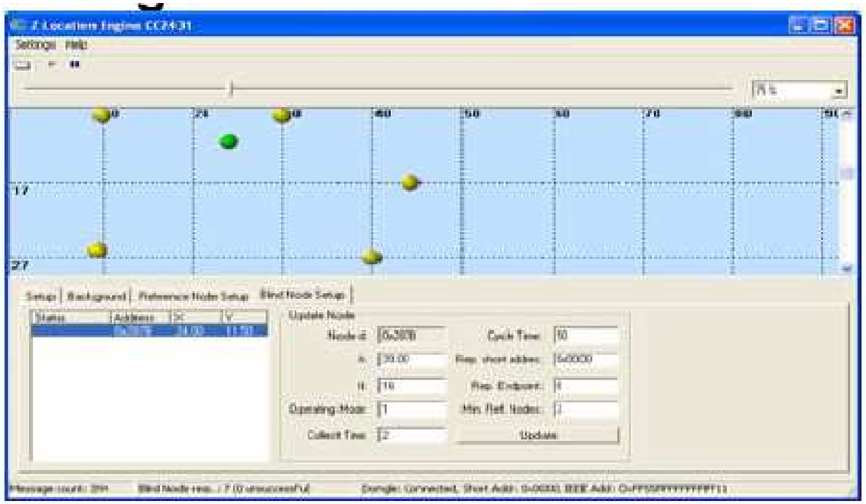
Some of the application areas where wireless provides a good fit include

- Equipment condition monitoring
  - Generally non-critical, replaces a person touring the plant
  - Can monitor vibration, fluid transparency, actuator position, …
  - Aids cost-effective maintenance
- Additional sensors for plant commissioning
  - Temperature, pressure at additional points
  - Environmental monitoring
  - Leak detection in new plant
  - Can be economically removed and re-used after plant is running

What do we want ? – location

As well as communicating with mobile devices, we have the opportunity to locate or track them

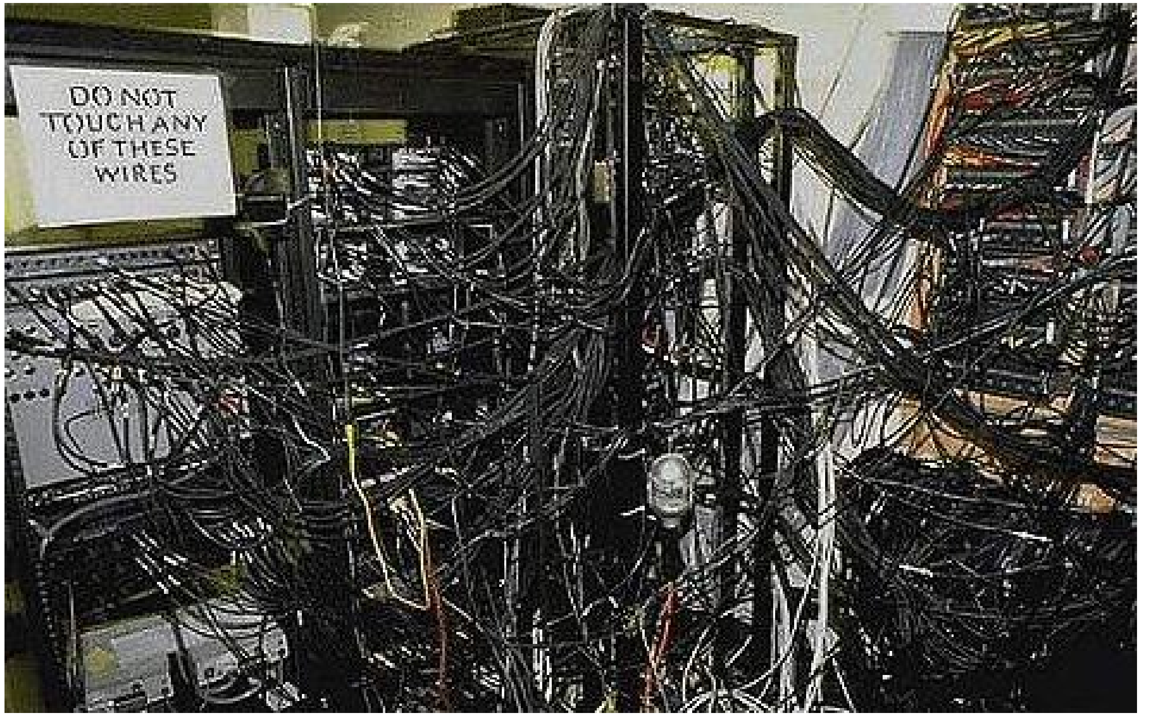
- In all but the smallest facility, the wireless network will have multiple fixed nodes
- A mobile node will hand over communication from one fixed node to the next (cellular operation)
- We can deduce the location of the mobile from
  - The fixed node (base station) serving it
  - Signal strength information from other fixed nodes
  - Time-of-flight information (where the radio system provides sufficient precision)
  - Processing this data with geographical knowledge



Source: Texas Instruments

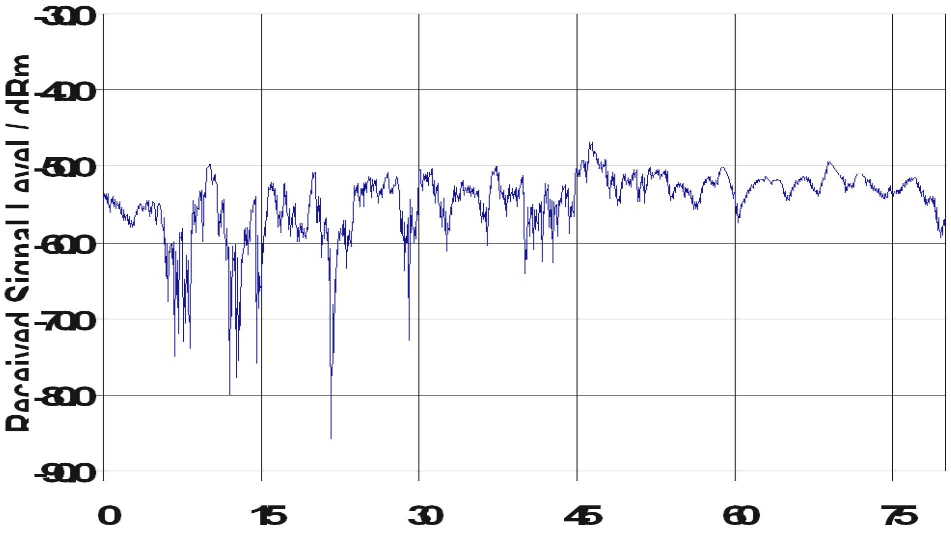
We cannot afford to install any new wires

- Installed industrial wiring can cost between €100 and €10.000 per metre
- This cost can increase substantially where the factory or process cannot be operated during installations
- With wiring, every measurement or control has to justify its installation cost
  - Temporary (commissioning) instrumentation can be hard to justify



Radio is inherently an unreliable medium, so we need various measures to deliver a reliable service

- Signal processing for better immunity to interference, etc.
- Various types of diversity to avoid poor link performance:
  - Space diversity combats reflections and multi-path
  - Path diversity combats shadowing or excessive propagation loss
  - Frequency diversity combats interference
- Send / acknowledge / retry ensures that the end devices know whether the message has got through or not
- Listen before send improves co-existence with other systems
  - Increases chance of first-time success
  - Improves throughput



Radio nodes need a source of power, without significant additional maintenance

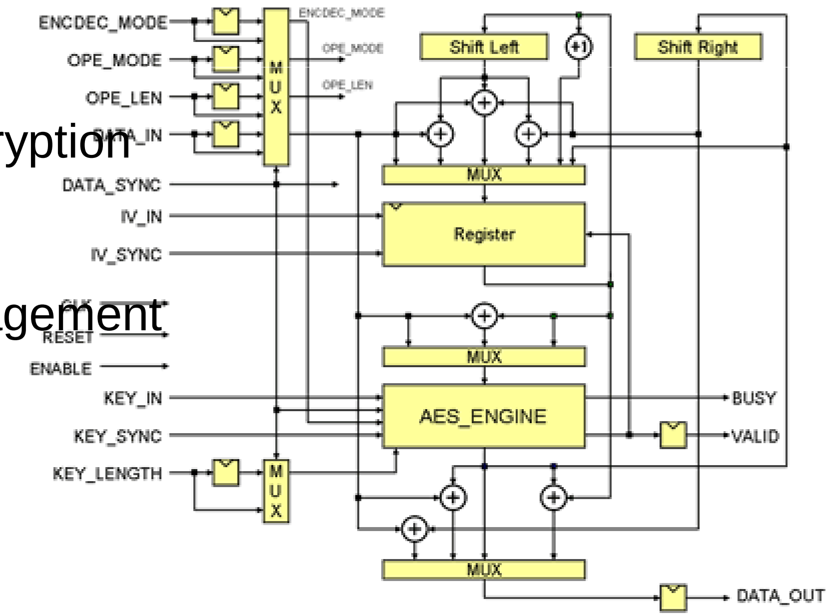
- Batteries will need to be charged or replaced
  - Battery lifetime must be at least a year, and preferably more
  - Places a heavy demand on the system design to achieve this
- Electrical energy can in some cases be harvested from external sources
  - Solar (or other) light
  - Vibration of motors etc.
  - Temperature difference
- Otherwise a power supply needs to be available for the node, which can increase its cost

Source: Perpetuum Ltd.

A radio system must be *at least as secure* as the wired system would have been

- Must ensure that transmitted data is correct – integrity
- Must avoid spoof instrument readings or control actuation – authentication
- May need to keep data secret – confidentiality

- All radio systems achieve these objectives by encryption
  - AES 128 is a popular coding scheme
  - Different methods are specified for key management



What wireless communications standards and products are used now?

(will consider local area systems, as wide area / public services are well understood)

- Wi-Fi has been available for some time in various ‘hardened’ forms
- Bluetooth has been deployed in some industrial systems
- ZigBee was originally targeted at factory automation …
- Wireless HART has recently been released
- ISA 100.11a is in a near-final draft

Source: Cisco Systems

- Specialist standards have been created, e.g. Wireless M-BUS, KNX-RF
- ‘Ex-proprietary’ standards are gaining traction
  - Z-Wave
  - Wavenis
  - …

IEEE 802.15.4 is a very popular PHY/MAC standard for industrial use

- 16 channels, 5 MHz spacing, in the 2.400 – 2.485 GHz licence-free band, peak data rate of 250 kbit/s (also defined for 868 and 902MHz)
- Direct sequence spread spectrum transmission, with a chip rate of 2 MHz, gives a processing gain against interference of 9dB
- 16-bit ‘local’ address allows compact messages
- Operable at very low duty cycles for long battery life
- Encryption engine (invariably hardware) gives 128-bit AES CCM*
- Implemented in silicon in volume now, from many vendors

freescale semiconductor

OKI

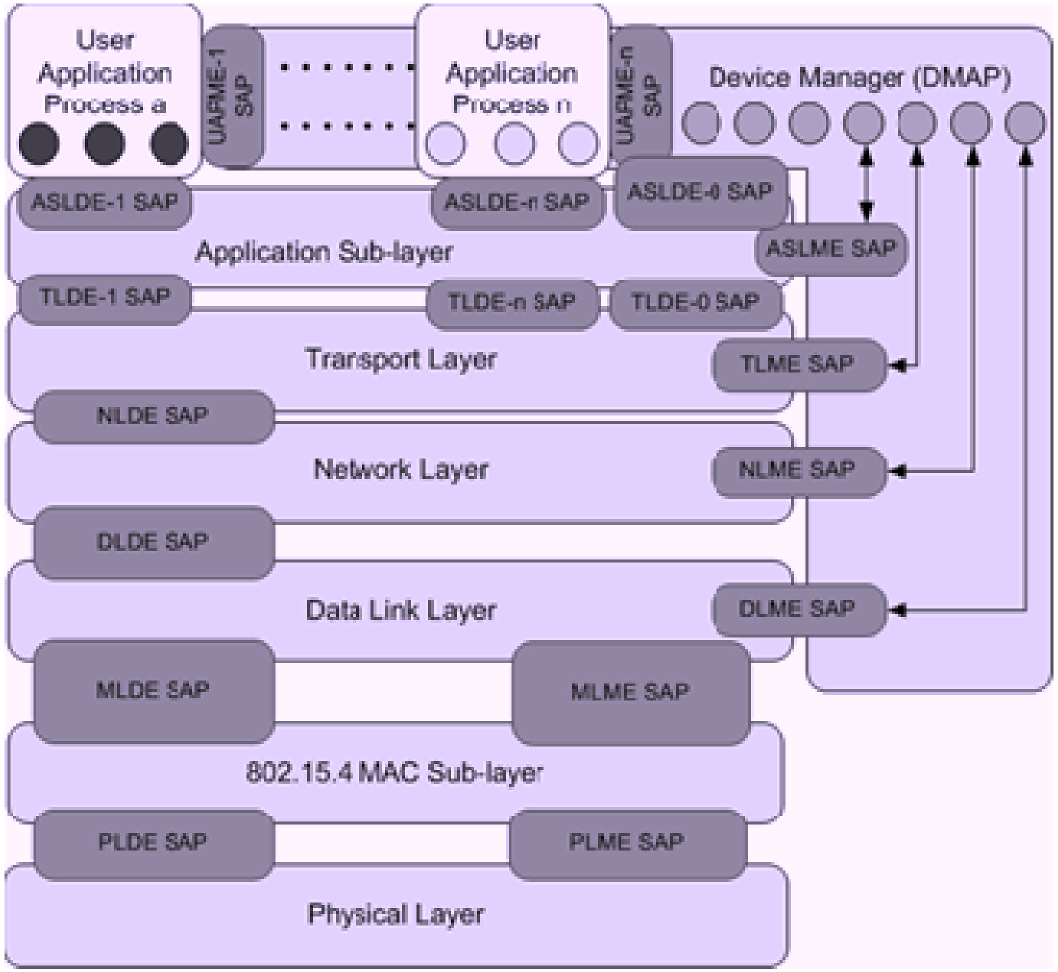
ember

SAMSUNG

TEXAS INSTRUMENTS

Jennic

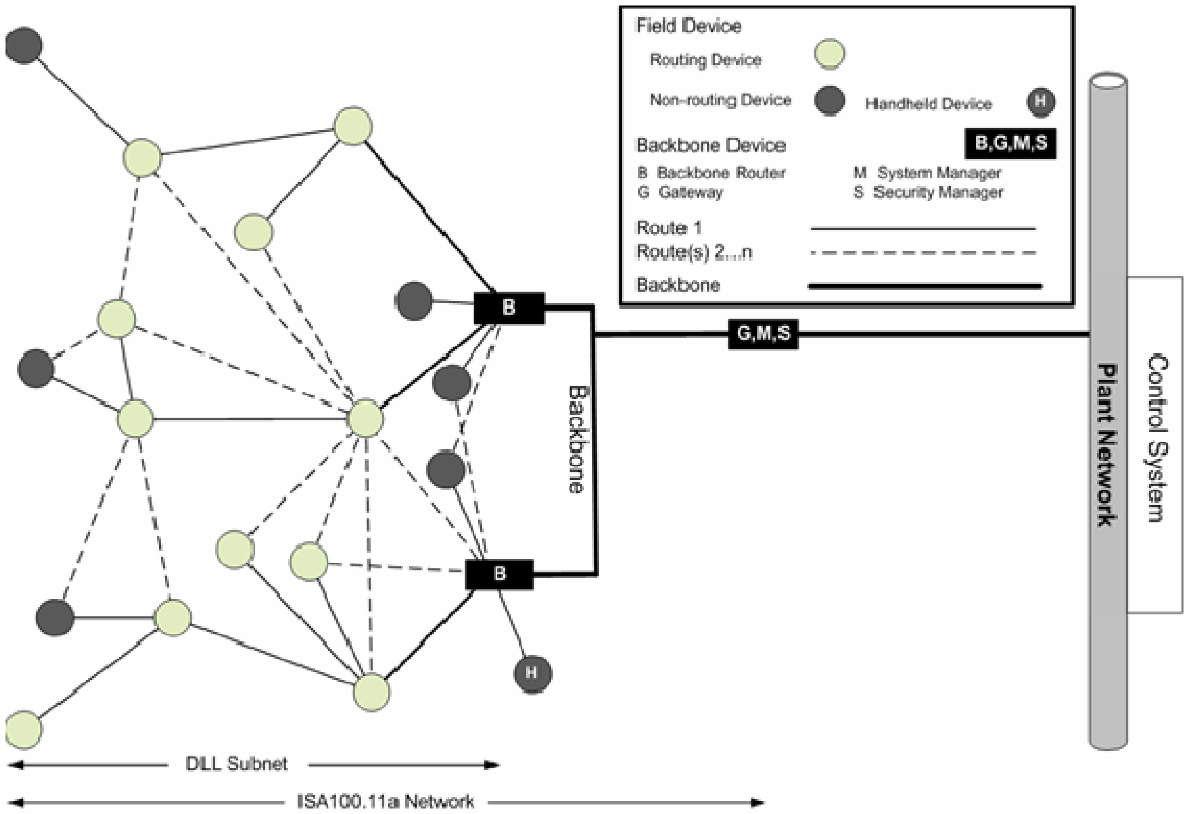
ISA 100 is designed to support native and tunnelled application layers



- User application processes are standardised, with hooks for extension
- Various transport services, including ‘reliable,’ ‘best effort,’ ‘real-time’ are offered
- Network and transport layers are based on TCP or UDP / IPv6
- Separate Data Link layer adds
  - Frequency hopping
  - Mesh routing
- MAC and Physical layer are defined in IEEE 802.15.4

The scope of standard ISA 100.11a includes

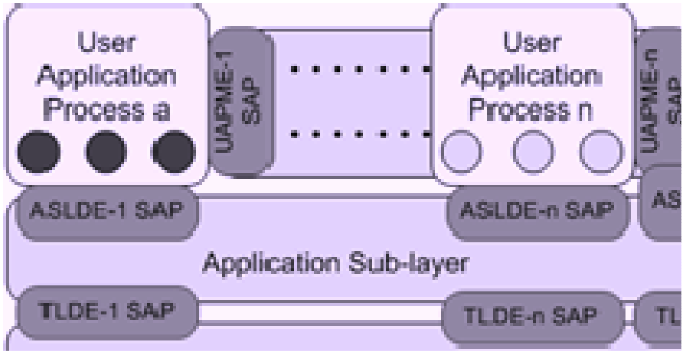
- Permitted networks
  - Radio link
  - ISA 100.11a over Ethernet and field buses
- Topologies
  - Star / tree
  - Mesh
  - Alternative routing
- Security architecture and specification
- Gateways and backbone routers
- System management functions



Example ISA 100.11a network

Application Support Layer delivers communications services to user and management processes

- Data from the transport layer is de-multiplexed and sent to the peer UAP (or MP)
- Can pass objects (methods, attributes) natively within the ISA 100.11a protocol
  - Standard objects defined
  - Standard profiles defined per application
  - Manufacturers also free to define their own
- A tunnelling mode is available to pass legacy data
- Adaption modes supports legacy field protocols:
  - Foundation FieldBus
  - ProfiBus
  - HART …



Industry Independent Objects defined in ISA 100.11a

- UAP management object – 1 per UAP – facilitates common UAP management.
- Device management object.
- Alert reporting management object.
- Alert receiving object(s) – up to four per device, supporting the four alert reporting categories (device related, communication related, security related, and process related).
- UploadDownload object.
- Concentrator object – represents an assembly of data at a publisher.
- Dispersion object – represents an assembly of data at a subscriber.
- Gateway cache object – represents local cache in the gateway.
- Tunnel object – supports encapsulation of non-native ISA100.11a messages.

Security is fully built-in to the standard

- Authentication and confidentiality services are independently available
- A security manager in the network manages and distributes keys
  – Asymmetric keys, or (provisioned) secret master keys for session key distribution
- Each node can secure data at two places
  – Data Link layer encryption, secures each hop
  – Transport layer encryption, secures peer-to-peer comms
- Default device policy sets the minimum security available to an application:

Security requirements for packets transmitted by device		**Outgoing protection of packet requested by device**		
		Unsecured	**Authenticated**	**Authenticated and confidential**
Device's Policy	**Unsecured**	Allowed	Allowed	Allowed
	Authenticated	Not allowed	Allowed	Allowed
	Authenticated and confidential	Not allowed	Not allowed	Allowed

Thank you for your attention

Any questions ?

MAKING TECHNOLOGY WORK

Our 300+ engineers and scientists offer wireless product design across the spectrum

Contact details:

Cambridge Consultants Ltd
Science Park, Milton Road
Cambridge, CB4 0DW
England

Cambridge Consultants Inc
101 Main Street
Cambridge MA 02142
USA

Tel: +44(0)1223 420024
Fax: +44(0)1223 423373

Tel: +1 617 532 4700
Fax: +1 617 737 9889

Registered No. 1036298 England

Tim.Whittaker@CambridgeConsultants.com
www.CambridgeConsultants.com