Introduction

Remote Control and Monitoring

An industrial facility typically comprises a relatively small control room, surrounded by a relatively large physical plant. The control room is equipped with panels that depict the state of the plant as captured by sensors and input devices that control the actuators, affecting the state of the plant. The actuators and sensors are often relatively inexpensive when compared with the cost of the cable that needs to be used to connect them. The difference becomes even greater when considering the high installation and maintenance costs, the high failure rate of connectors and the difficulty of troubleshooting them.

The information being communicated in industrial environments is typically state information and as such in normal operation it takes the form of repeated streams of small packets. At the same time, these packets are associated with critical tasks having strict timing requirements in harsh environments. The latter may include extremely high or low temperatures, high humidity levels, intense vibrations, explosive atmospheres, corrosive chemicals and excessive electromagnetic noise caused by large motors and conductors. Thus, in general, the required data throughput of the network is relatively low, but its reliability needs to be very high.

In recent years, the desire for connectivity and physical mobility has caused an exponential growth in wireless communication systems. Wireless telephony has entered our daily lives and wireless local area networks increasingly serve as a means to access business and private data. In industrial environments, apart from lower installation and maintenance costs, wireless systems can offer ease of equipment upgrading and practical deployment of mobile robotic systems and micro-electromechanical systems (MEMS).

The rest of this introduction is organized as follows. The next two sections provide an overview of the evolution in wired control and monitoring and present solutions in cable replacement along with examples of successful deployments. The introduction continues with the hybrid wired/wireless fieldbus and mesh networking approaches. Finally, the results of study on how wireless technology is expected to impact industrial control and monitoring are presented in the form of a technology roadmap.

Wired Control and Monitoring

One may identify three main paradigms in wired communication for industrial control and monitoring:

***a)** parallel wiring,*
***b)** fieldbusses and*
***c)** industrial Ethernet.*

According to the first paradigm, each of the field devices is connected with parallel wires to the I/O module of a control or monitoring system. Such a point-to-point wiring approach became obsolete following the introduction of fieldbus technology, which allowed the use of only one two-wire line to provide power, control and configuration functions to devices. Fieldbusses allow many devices to be connected on the same wire and provide the necessary addressing mechanism to support communication with them. The open standardization approach adopted by main fieldbus technologies such as Profibus has facilitated interoperability among systems from multiple vendors and has been proven in many factory, process and building automation applications worldwide.

*Several fieldbus manufacturers have more recently recognized the advantages of Ethernet, which is the established standard bus system in the office world, for industrial applications. The advantages are related to the physical layer, particularly in terms of bandwidth, which can be higher than 100Mb/s rather than up to 12Mb/s for fieldbusses. The higher bandwidth can be utilized by larger packets e.g., for computer vision systems. In the past, the main disadvantage of Ethernet was the **Carrier Sense Multiple Access / Collision Detection** (**CSMA/CD**) contention protocol which does not guarantee time-critical communication. However, by splitting up the network in multiple collision domains using switches (or bridges), the prices of which have dropped dramatically as a result of the Internet revolution, every port on a switch is in its own collision domain and as such no more collisions between devices attached to the switch take place. Ethernet-based solutions offer also improved information sharing between manufacturing and backoffice systems such as asset management and inventory control applications. The data can also be made easily available via a Web server for remote control and monitoring purposes.*

Cable Replacement

Cable replacement is used here to denote the elimination of wires as the physical layer to carry data without requiring any physical changes to the machinery/instrument, the control panel or the underlying software involved. Industrial devices using traditional serial interfaces such as RS232, RS422 and RS485 are good candidates for cable replacement. This is because serial interfaces are typically connected to standard PCs and the connecting software is application dependent or device specific. Apart from serial point-to-point connections, cable replacement has found applications into master/slave multi-point connections, wireless parameterization and diagnosis particularly to do with moving/rotating subsystems, e.g., robotic arms. There are limitations to what cables can be replaced, though, due to the error characteristics of wireless links. When deterministic communication with latency (the time it takes for a packet of data to get from one designated point to another) under 10ms is essential, wireless transmission should be avoided.

*Wireless transmission can take place in various frequency bands and the transmission power is often restricted by law. The 2.4GHz **Industrial Scientific and Medical (ISM**) band is the most widely used. The 900MHz band, which is characterized by lower throughput but better*

range and wall penetration, is only available in a few countries and used by proprietary protocols. The 5.8GHz band holds a lot of potential in terms of higher throughput, better noise immunity and smaller antennas, but products are yet to be proved in the market.

Infrared (IrDA) can also be considered for cable replacement but has the shortcoming of requiring line of sight which limits its applicability.

Standard (Market Name)	802.11 (Wi-Fi)	802.15.1 (Bluetooth)	802.15.4 (Zigbee)
Application focus	Web, e-mail, video	Cable replacement	Control and monitoring
Bandwidth (Kbps)	11000	1000 – 3000	20 – 250
Transmission range (m)	100+	20 (Class 2) 100+ (Class 1)	20-70, 100+ (ext. amplifier)
Nodes supported	32	7	2^{64}
Battery life (days)	0.5 – 5	1 – 7	100 – 1000+
Power consumption (transmitting)	300 mA	45 mA (Class 2) <150 mA (Class 1)	30 mA
Suitability for low duty-cycle applications	Poor (Slow connection time)	Poor (Slow connection time)	Good
Spread spectrum technology	DSSS	FHSS	DSSS
Memory footprint (KB)	70+	50+	40
Success metrics	Speed flexibility	Cost, convenience	Power, cost

Table 1 Summary of different wireless standards.

Table 1 compares three main wireless transmission technologies. These technologies are complementary rather than competing to each other, as they address different needs and have different strengths. Bluetooth requires a low-cost transceiver chip in each device to be connected. Each device has a unique 48-bit address and the transceiver transmits and receives in the ISM band. Connections can be point-to-point or multipoint with a range of 20-100m. Data can be exchanged at a rate of 1-3Mbps and a ***Frequency Hopping Spread Spectrum*** *(****FHSS****) scheme allows devices to communicate even in areas with a great deal of electromagnetic interference. However, this makes it extremely difficult to create extended networks without large synchronization cost. Built-in encryption and simple verification is also provided by Bluetooth.*

ZigBee moves data only a quarter as fast as Bluetooth but can handle orders of magnitude more devices at once and has been optimized for low power consumption. This low power consumption is achieved by the ***Direct Sequence Spread Spectrum*** *(****DSSS****) which allows devices to sleep without the requirement for close synchronization. Another spread spectrum technique under development,* ***Ultra-Wide Band*** *(****UWB****), broadcasts simultaneously on a very large frequency range at low power. The idea is that the signal is spread so thinly that interference will be negligible in any given frequency. UWB is expected to be able to deliver high throughput, particularly in areas with physical obstacles.*

Some examples of industrial applications where cable replacement has been successfully deployed are given below:

- ***Phoenix Contact*** *(Germany): use Bluetooth to replace parallel wiring. A wireless multiplexer can replace wires for up to 32 digital inputs, 32 digital outputs, 2 analogue*

inputs and 2 analogue outputs. The product mirrors the inputs to the outputs and vice versa. The latency from input to output is 10 ms or less.

- ***Expert Monitoring*** *(UK): have developed WiSNet which allows sensors or instruments to be installed wirelessly. A typical WiSNet system consists of an Ethernet / USB network controller and sensor transmitter modules that enable sensors to be positioned anywhere inside or outside manufacturing plants. The transmitters use Bluetooth to send sensor data to a wireless network controller unit connected to a PC.*
- ***EnVision*** *(USA): have developed a wireless sensor that enables bioprocessors to monitor fermentation and cell culture processes directly in reactors. The sensor can be configured by either a Bluetooth wireless browser-based user interface or configured for Foundation Fieldbus communications.*
- ***Bromma Conquip*** *(Sweden): use Bluetooth to replace the cables connecting the control systems of harbor conveyor cranes with configuration and maintenance tools.*
- ***Schneider Toshiba Inverter Europe*** (***STIE***) *(France): use Bluetooth to replace the cables that connect a configuration tool (running on a PC or PDA) to their family of inverter products.*

Hybrid Wired/Wireless Fieldbus Networks

The need to retrofit any support for wireless to existing installations instead of creating new systems from scratch, increases the requirement for hybrid wired/wireless fieldbus networks. The standard ***Profibus Decentralised Periphery*** *(****DP****) network is based on a standard RS485 interface but often using unusual baud rates (93.75 and 187Kbps). The protocol has timing requirements; however, these requirements are adjustable because they were originally introduced to support modems. In order to be able to replace a fieldbus such as Profibus DP with a wireless link, it is very important to keep messages unbroken to support the timing requirements of the fieldbus protocol.*

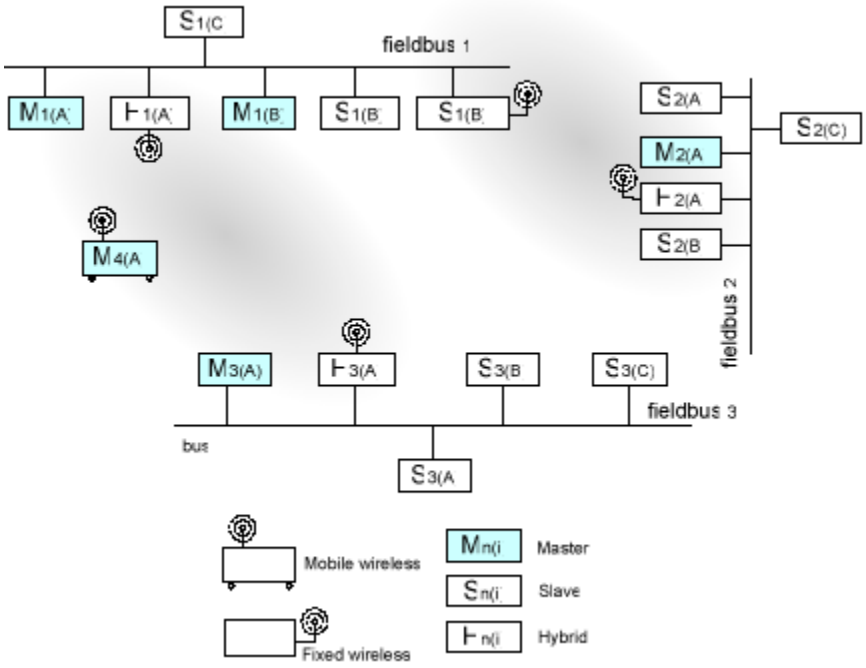

Figure 1 Example of a hybrid wired/wireless profibus topology.

Figure 1 depicts three fieldbusses that incorporate fixed wireless devices. At the low baud rate of 9.6Kbps the full number of 7 wireless nodes in a Bluetooth network can be supported, however at 93.75Kbps only 2-3 nodes can be supported. The maximum bandwidth in a point-to-point configuration is 187Kbps.

Modbus Remote Terminal Unit (RTU) fieldbus also uses RS485 as a transport media and has been successfully replaced by a Bluetooth wireless link both in single-point and multi-point configurations. Examples include the Phoenix Contact and STIE products mentioned above which use Modbus RTU on top of wireless links.

Mesh Networks

The traditional wireless systems have mostly used base station style radio links, with point-to-point or point-to-multipoint transmission. These wireless approaches have liabilities in industrial applications such as rigid structure, meticulous planning requirements and dropped signals. Rather than relying on a central communication coordinator and its associated reliability and efficiency issues, it is possible to use a collection of wireless devices maintaining connectivity to create a path for data packets to travel. This approach is known as a mesh network (Figure 2) and in many ways it resembles an idealized version of a top-level Internet backbone in which physical location is less important than capacity and network topology. In mesh networks each node has a low-power transmitter and communicates directly only with neighbouring nodes and these latter nodes relay data to more distant nodes. Should a link become congested or a node fail, the mesh automatically redirects data packets via an alternative path. This characteristic makes mesh networks virtually immune to localized interference such as that caused by motors turning on or arc welders.

Mesh networks allow applications to grow based on demand (the addition of new nodes is relatively simple), limiting fixed costs and providing great flexibility and capacity. They also minimize the need for elaborate site surveys or physical modifications to plants. Moreover, because of the short range of each transmission, the approach provides better utilization of available bandwidth than systems using high-power transmitters. Unlike other approaches, in mesh networks the major design requirement is the lowest possible node cost.

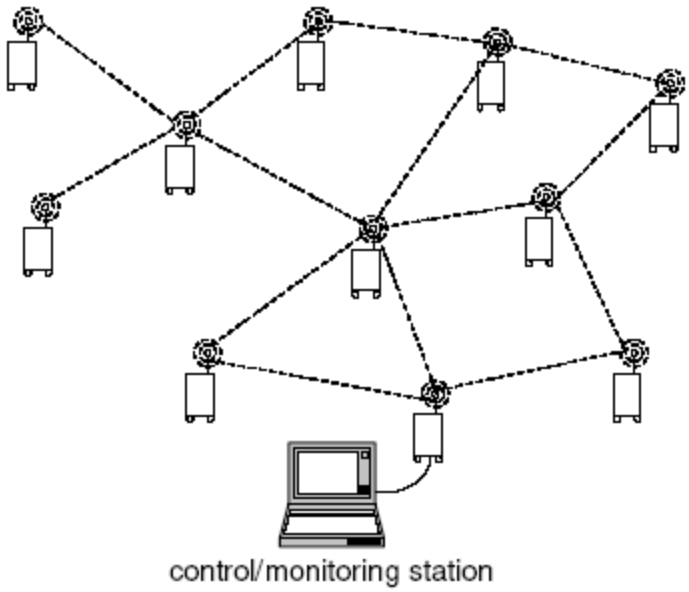

Figure 2 Wireless mesh network topology.

Many important questions remain though with respect to power management, routing strategies and algorithms in mesh networks. Even if good answers were to be given, mesh networks would not displace all existing industrial networks since deterministic operating modes (low latency and jitter) cannot be guaranteed.

Technology Roadmap

Embedded systems are now ubiquitous. They can be found in a diverse range of appliances, from mobile phones to smoke alarms, from refrigerators to trucks. Enabling these systems to communicate opens up new areas of applications: smart buildings, industrial automation, healthcare, power distribution and host of others. Some of the applications will result in a more efficient, accurate or cost effective solution than previous ones. Others will be new, previously unimagined or impossible. We are in the middle of a major technological revolution that will affect many aspects of our lives.

Moving to this exciting new technique in system development necessitates a common language for all systems. Without this, we risk repeatedly 're-inventing the wheel' at a high cost in money and effort, and we compromise the inter-operability of sensors between applications.

*The **RUNES** (**Reconfigurable Ubiquitous Networked Embedded Systems**) project has a vision to enable the creation of large-scale, widely distributed, heterogeneous networked embedded systems that interoperate and adapt to their environments. The inherent complexity of such systems must be simplified for programmers if the full potential for networked embedded systems is to be realized. The widespread use of network embedded systems requires a standardized architecture which allows self-organization to suit a changeable environment.*

RUNES aims to provide an adaptive middleware platform, a common language that will simplify the application creation process. This will allow for a dramatic cut in the cost of new application development and a much faster time to market, transforming applications which are already technically possible into forms that are easy and straightforward for designers to use;

and enabling applications which were previously unattainable. The project will also examine the potential uses and implications of the technology, develop demonstrator systems and design training courses to aid in dissemination of RUNES technology.

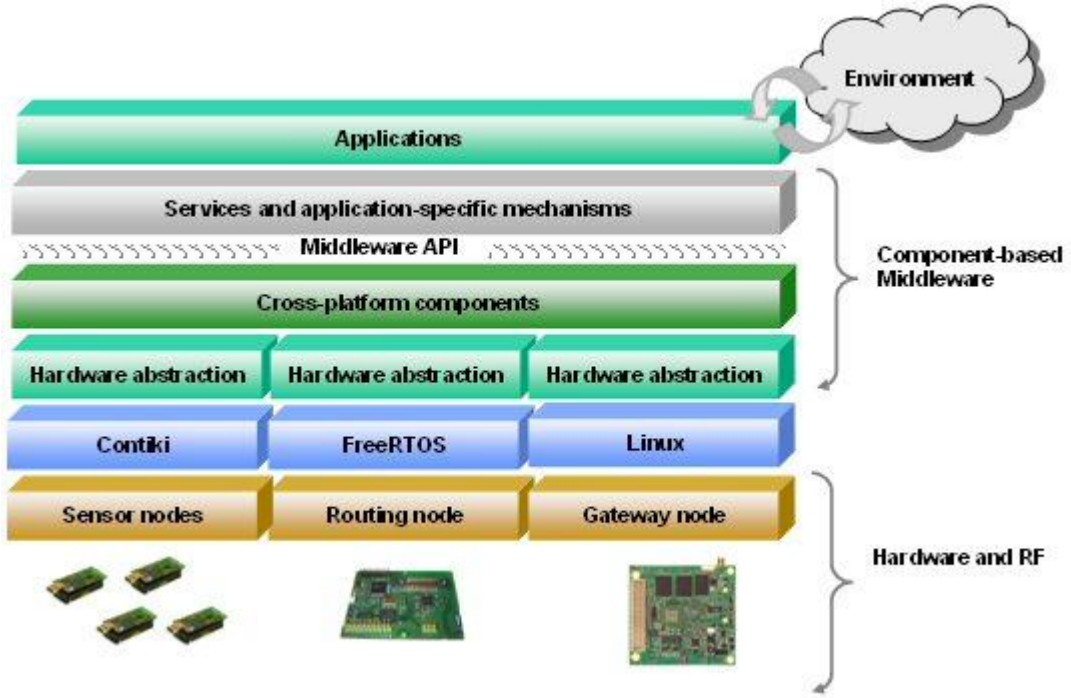

Figure 3 An overview of the RUNES technology which enables the creation of large scale, widely distributed, heterogeneous networked embedded systems that interoperate and adapt to their environments.

A technology roadmap for industrial control and automation was developed in the context of the RUNES project. The goal of technology roadmapping is to plot the future development of a technical field and help set more competitive and realistic targets. The objective of RUNES is to derive architectures and provide middleware and specialized simulation and verification tools that enable the creation of large-scale, widely distributed, heterogeneous networked embedded systems which interoperate and adapt to their environments. The roadmap is composed of the knowledge and views of over 25 organizations (large and small companies and research institutes) collected across Europe between Oct 2004 and Apr 2005. The focus of the roadmap is approximately 10 years although timescales for technological progress are notoriously difficult to predict. Below we summarize the technical, organizational and social issues identified.

Action plans for strategic positioning and resource allocation are also defined. Apart from the textual description of the roadmaps, we have summarized some of the findings in graphical form in Figure 4. The span of different technologies does not necessarily coincide with the first specification releases but mainly with the time adoption started. Regarding the decline of particular technologies, some assumptions, based on the information currently available, are made.

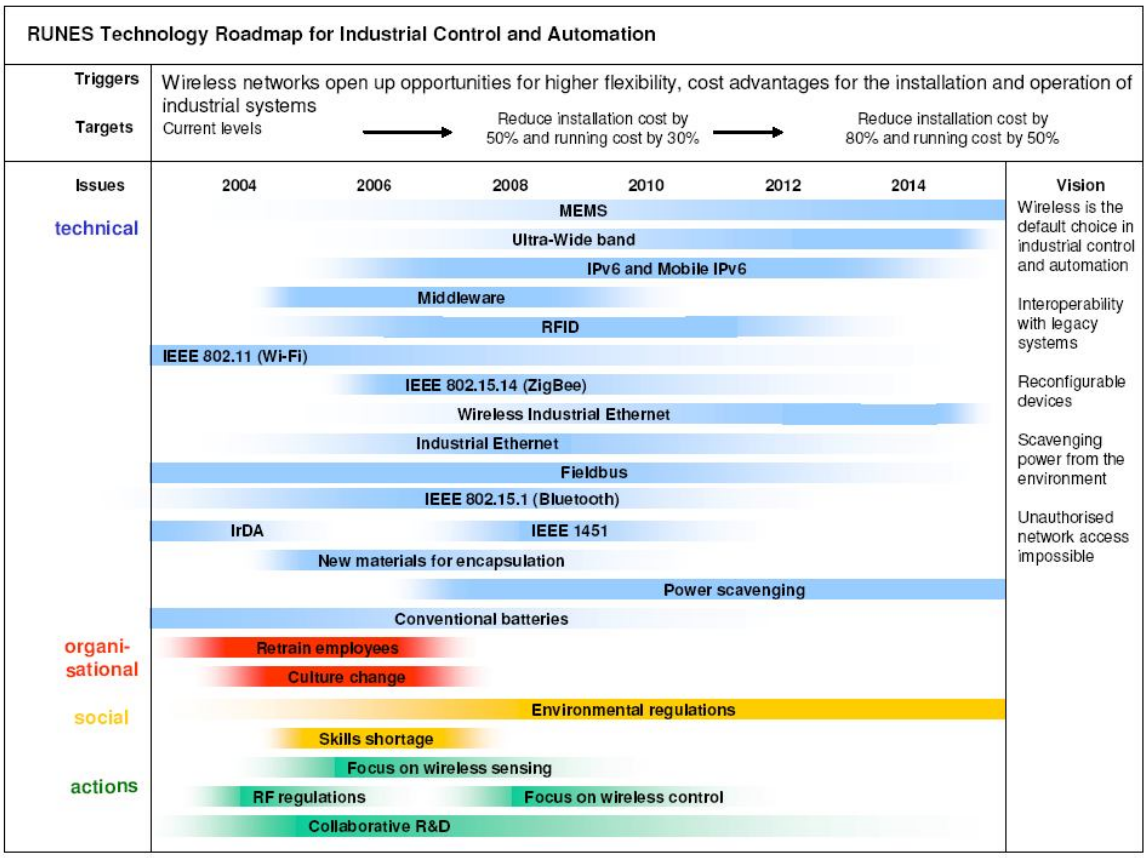

Figure 4 The RUNES technology roadmap for industrial control and automation in graphical form.

Technical Issues

Security

Major concerns about the integrity of signal transmission and reception have been expressed by industrial end-users who are worried about leaving their control and business systems vulnerable to hacking or denial of service attacks. Several solutions are based on proprietary protocols designed specifically with security concerns in mind, although this can be a barrier for future upgrades with standard equipment. Spread spectrum schemes provide inherent security against jamming or interference. Systems can employ 128-bit encryption with dynamically generated keys in order to prevent eavesdropping and unauthorized access. However, this is computationally too expensive for deterministic communication. Continuous monitoring of network activity and attempted access should also be supported. Spread spectrum technology provides inherent security against jamming or interference.

Robustness

The consequences of unreliable control and monitoring are not trivial. Industrial applications entail the risk of substantial losses through equipment damage, personnel injuries, loss of raw materials and environmental pollution. From the perspective of the integrator or end user, communications expertise and comprehensive technical support are key considerations that distinguish ordinary wireless products from the robust wireless communication solutions

required by industrial users. Many of today's wireless solutions offer mean time between failures which are unacceptable to deliver sustained performance in harsh environments. Any early failures could slow adoption of wireless. Encapsulation of sensitive electronic components is particularly important to achieve improved product reliability and extended lifecycles in harsh environments. Positioning of antennas is also critical in order to ensure reliable operation, as it can affect the bandwidth and data transfer rates.

Fail-safe/fail-soft operation

Designers of wireless industrial systems need to provide redundancy and allow degradation. Systems must be designed to go into a safe mode if and when a failure happens (fail-safe). Systems must also be capable of operating at a reduced level of efficiency after the failure of a component or power source (failsoft). Placing devices on different networks provides substantial fail-soft operation in that the failure of a single network only affects the devices that it supported. Devices connected to other, unrelated and perhaps geographically distributed, networks would be unaffected by the events that caused the failure of the first network.

Interference immunity

Multi-path fading is caused when multiple copies of a source signal arrive at a receiver through different
reflected paths and affects wireless communications indoors. The phase variance in the signal copies can result in interference that reduces signal strength, effective range, and data transfer rates. A wireless node has to handle multi-path signals, but interference can be caused by signals from other nearby systems particularly for unlicensed frequency bands. Extremely critical wireless equipment can operate inside a Faraday cage.

Power availability

As the speed of embedded processors increases and more peripherals are integrated into a single chip, the applications that run on these devices become more computationally intensive. However, technological advances of the batteries which power the embedded systems lags significantly behind, and as a result, power consumption is one of the most important issues for mobile wireless embedded systems. The major sources of energy waste include packet collisions, overhearing unwanted packets, control packet overheads and idle listening. For monitoring applications unnecessary high sampling rates also waste energy. One answer to the power problem is to scavenge power from the industrial environment. For instance, this could include development of photoelectric cells that draw energy from lighting. Power scavenging technology is something that industrial sector are thinking about already as supplying power to remote areas is costly.

Interoperability

At present, there are a number of different protocols for fieldbusses and industrial Ethernet, and end-users are concerned about the long-term cost implications of installing closed wireless systems. Until standards have been established and the market has become one for volume suppliers, fears of being left with an obsolete system may hold back widespread adoption. An important component towards interoperability is middleware, which defines appropriate abstractions and mechanisms for dealing with the heterogeneity of devices. Because ideally devices must operate unattended, the middleware has to provide new levels of support for automatic configuration and error handling. Development of middleware is a key activity

within the RUNES project. The IEEE Smart Transducer Interface for Mixed-Mode Communication Protocol (1451.4) was also revived last year in recognition of a need for a standardized approach to device interfaces.

Interfaces

Most industrial processes now modelled and controlled in IT systems, but they require the user to be physically at a terminal. Given the increasing need for workers to access systems remotely more research on machine to human interfaces needs to be undertaken. Human to human interfaces via devices that allow voice, image and video communication is another potentially important field given that they provide natural and real-time exchange of information, e.g. when someone on a factory floor needs to report a fault to an expert. Very few projects have addressed multimodal interaction such as gesture based programming of robotic arms.

Organizational Issues

Culture

The industrial automation sector, in general, is very conservative. Companies do not want to take chances with large investments in new installations and require demonstration of practicality (preferably by someone else). People involved in risk management are not receptive to new technologies. However, cheaper, faster, safer and more reliable options are always there for successful innovators. Often, employees who misunderstand new technology and lack confidence in its ability to improve over previous practice use many new systems in a suboptimal way. Collaboration between control people and radio people is not close enough. Major cultural differences exist between Europe and the less cellular-oriented US.

Work force

Industrial companies are expected to face a strategic human resource issue. The shift from a wired to a wireless plant, particularly one that can operate autonomously, will require adjustments in the work force. Engineers should understand radio technologies and be able to handle false alarms; hence revised technical training will be required. A shortage in embedded software development skills has also been identified.

Social Issues

Workforce

In general new levels of automation devalue unskilled labour through its replacement with less expensive systems. This is expected to increase job security concerns for people who only posses skills in declining technologies.

Environmental

Industrial control and automation have an enormous direct and indirect impact on the environment. New stricter regulations have been introduced and this trend is expected to continue. The deployment of large numbers of wireless sensors can be used for instance in warning systems to reduce the risk of environmental pollution.

Actions

The use of wireless systems for industrial applications is in its infancy. The adoption period is expected to be longer than other sectors (building automation and control, medical care, disaster response and automatic meter reading) reviewed in the RUNES technology roadmaps as end-users migrate incrementally from wire to wireless. Companies dealing with automotive, food processing, petrochemical and asset tracking applications were identified as the early adopters.

A clear difference in the adoption time scales between wireless in control and monitoring was revealed. While technologies are maturing, wireless will not be used for critical control applications. Monitoring in hazardous and inaccessible areas will be given priority in the short/medium term and in moving towards this some lessons can be learnt from successful automatic meter reading deployments. Many wireless systems on the market today do not meet local/national regulations, because they transmit too much power or operate in frequencies that are not approved for unlicensed use. Therefore, it is important to determine whether or not the radio subsystems can be programmed to meet these regulations. Since 2003 the ATEX directive has become mandatory for all electrical and mechanical equipment used in potentially explosive atmospheres and any new networked embedded components will need to comply with it.

The required R&D will involve expertise and engineering skills in communications, sensors and industrial computer systems which are very difficult to find under one corporate roof. Partnerships will therefore be essential. Sources for funding and mechanisms for facilitating collaborative R&D must be identified. Industrial companies collaborating with academia should persuade the latter to reconnect software and hardware education in their curricula.

Concluding Remarks

The traditional approach to the design of industrial control and monitoring systems – designing an architecture that integrates actuators and sensors within a single physical platform under centralized control – is changing. The emerging view, as motivated by new large-scale applications in the factory floor is one in which actuators, sensors, computing, and human interfaces may be distributed across multiple physical platforms. Adopting this new view of industrial systems design requires researchers to address a range of issues, architectures and applications related to wireless connectivity. In industrial control and monitoring there are certainly many future alternatives, however, the process of technology roadmapping helps narrow down the field of possible solutions to those more likely to be pursued. Most of the issues and technical requirements are not orthogonal and as such trade-offs depend on applications.