

Tuning into wireless

Process industries, including refineries and oil and chemical storage companies, are on the cusp of a new application of existing technology. For the daring storage company there is money to be saved and for equipment manufacturers producing this future-proof technology, there is money to be made

by Brian Warshaw

Since the inauguration of the crystal wireless set at the turn of the 20th century, with its inherent crackle and drift away from the wavelength frequency, wireless technology has come a long way.

Those pioneers, with headphones glued to their ears, could not have imagined the technology being used for process monitoring and alarm generation at a bulk liquid storage terminal. Even the terminology would have been unknown to them, as perhaps it is to many who work in the industry at present. With few exceptions today's experience of wireless instrumentation is limited to the point of negligibility; but there are facilities in the US and Europe that have installed, or are piloting, wireless monitoring systems.

Among the first to take the plunge into wireless technology was Standic, an independent liquid storage and distribution company at Dordrecht, the Netherlands.



Honeywell Enraf SmartRadar wireless level gauge installed at Standic terminal, Dordrecht

Koos Donkers, operations manager is quoted as saying: '...wireless solutions have helped us save approximately €30,000 and we are completely wireless. We no longer have to depend on hardwires and arduous manual tasks to get readings. The solution works entirely trouble free and we are confident we will continue to see increased cost savings.'

The project started during the final quarter of 2006 with two tanks, and now more than 10 tanks have been converted, with the target being all 60 tanks on the site. The terminal, which is not manned at night, has added CCTV to the wireless network, which has enhanced security and safety monitoring.

Point-to-point wireless communications

One of the first companies to develop industrial wireless products and systems for process and manufacturing applications is Australian-based Elpro Technologies, which is now owned by the UK's MTL Instrument Group. One of its earliest installations was around four years ago, as part of an instrumentation upgrade at an old chemical storage site in the Houston area of the US.

The tank farm was separated from the main processing plant by a major roadway, with the feedstock being pumped through several pipelines. Data was transmitted by a telephone telemetry system, which, in addition to being unreliable was incapable of being expanded to add flow data and valve status, and also had to be connected to the plant's ethernet LAN system.

A reluctance to cable under the road due to insufficient details of buried pipes and services, led the company to select the Elpro's wireless instrumentation backbone.

Each storage tank had a radar level gauge, and high and low level contact switches, all of which connected to a 105U-G Modbus unit. Wireless transmissions from the tank communicate directly with the Elpro Ethernet unit at the main plant, and hence into the distributed control system (DCS).

The principle of the Elpro telemetry is that it transmits



Wireless Rosemount 3051S liquid level differential pressure transmitter

digital, analogue and pulse signals on an ultra high frequency wave band, which in most countries is licence-free. Modules are programmed to transmit when there is a change in parameter, update time, or poll response. The company considers this to be good radio communications,

with the fewer the better, believing that high levels of communication traffic could cause congestion, necessitating re-transmissions, and the inevitable missed messages.

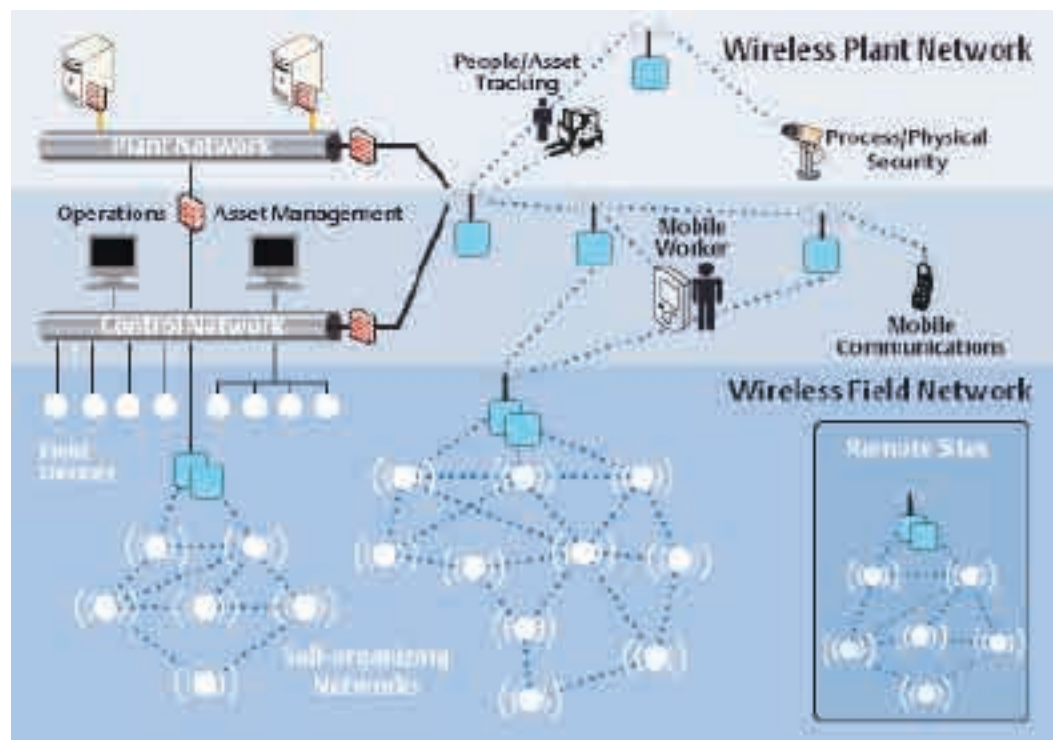
Working on peer-to-peer addressing basis, Elpro considers its system to be more effective than the

master/slave configuration, wherein a failure of the slave causes the whole system to fail. The operating range of the 105U unit is subject to obstructions in the radio path, the type and height of aerial used, transmission power. Communication distances of between 2 and 10 kilometres can be achieved, boosted, if necessary, by the use of up to five repeater units.

In addition to Modbus and Ethernet compatibility, Gateway units will communicate with Profibus, DF1, DeviceNet, and Modbus Plus data highways, all units offering RS232, and RS485 serial ports. The units operate on low power, typically 24 volts DC in the main plant, and in remote locations, solar power batteries can be used.

Wireless implants

In Europe the Rosemount division of Emerson Process Management has been marketing its range of Smart Wireless pressure, temperature, level and flow measurement instruments since April 2007. The range already includes the Rosemount wireless 3051S liquid level differential pressure transmitter and the portfolio will be extended with the introduction of radar level gauges in the early part of 2009.



Emerson's Smart wireless architecture combines field and plant networks

Protection systems

In an internal memorandum issued at the end of 2007, Honeywell Enraf outlined the protection and security measures taken to prevent corrupted or invalid data in its OneWireless communications network.

Although there are many technologies available to counteract wireless network intrusion, none prove absolutely secure. The best strategy, according to the memorandum, is to combine a number of security measures, making it as hard as possible for hackers to access the network.

Seven known threats are listed. Some are intentional and malicious, while others are unintentional. Several will be known from personal experience by anybody using a PC or laptop to surf the internet and use emails.

The threat from hackers is existent and remains so for the foreseeable future. This type of intrusion can be made with the intention of corrupting data or of spying, and can only be challenged by IT personnel and systems engineers keeping one step ahead of the hackers.

Access to the wireless network can also be unintentional, and occurs when a user turns on a computer that is configured to connect to all available wireless access points in the area. The potential danger is that, like the work of the hacker, it would put the network at risk from unidentified and possibly malicious persons. By designing a combination of antenna characteristics and radio output power to provide a wireless service area just large enough to include all the network devices, a barrier is created to the inadvertent intruder.

Man-in-the-middle

The man-in-the-middle attack profile impersonates a real access point in the wireless system thereby creating a gateway to a real access point, allowing data to be transferred for later evaluation by the hacker. This is countered in OneWireless by its ability to detect unauthorised access points and to notify the system administrator.

Most wireless access points contain some type of media access control (MAC) identification filters. However, given sufficient time and a combination of software programmes, hackers are able to impersonate a network resource and gain entry to the computer.

Honeywell says that several methods can be used in combination to limit the scope of the hacker. It can switch off the network naming facility, which makes the network invisible to the honest laptop or PDA user. Disabling the network's dynamic host configuration protocol (DHCP) server, and using static IP addresses for the various network devices also makes it more difficult for a casual or unsophisticated intruder to log on to the network.

The wireless network can be disrupted if an access point is bombarded by bogus requests, in which the level of demand denies the service to legitimate users; and by an injection attack whereby the hacker makes use of access points to introduce false networking re-configuration commands that affects routers, switches, and intelligent hubs. These types of attack can cause the system to crash, and in the case of the latter, require rebooting or even the reprogramming of the intelligent networking devices.

Counter attack

To counter these, and other attacks, OneWireless deploys an active management of network security keys, giving each device a specific key to use before enabling it to communicate through the network, thus preventing unauthorised devices from joining the secure sensor network. This defence is supported by remote authentication dial in user service (Radius), a protocol used for remote network access to verifying identities through a username and password that is already predetermined by the user. Data privacy is maintained through the use of several different forms of encryption.

Honeywell advocates that wireless network users need to be educated in maintaining its security, and in actively monitoring it for weaknesses and breaches.

Mike Ferris, European marketing manager for Smart Wireless solutions, is an enthusiast for wireless technology: 'There are significant cost savings in using wireless technology in respect to installation. There is no requirement for cabling containment, conduit, trunking or junction boxes. There are also savings in labour, in materials, and in space. The requirement for site drawings is also reduced, commissioning is simpler, and the up time is faster.'

'We are seeing immediate interest from existing plants that require additional measuring points, and for new processes that require measurement installed for the first time. Wireless is opening up a whole new paradigm shift in the market place, because it offers customers the opportunity to deploy this technology very quickly; and also in a very cost-effective manner.'

'The wireless instrument looks no different from a wired device,' Ferris explains, 'except that the wireless versions have a black antenna sticking out of the top. In terms of process connections, orientation, installation procedures and practices, they are identical, and that is one of the key selling points.'

Emerson uses time-synchronised mesh protocol (TSMP) communication technology developed by Dust Networks, a leader in standards-based intelligent wireless sensor networking (WSN), in its Smart Wireless devices.

Emerson has developed a few rules of thumb to guide customers. 'In a dense area of pipework, with a lot of structural steel, we suggest the communication distances between nodes (transceiver devices) are designed to around 75m,' explains Ferris. 'In an open area, such as a tank farm, we would suggest that this could be more than doubled to 200m. 'A good rule of thumb, depending on site layout,' he says, 'would be to design each gateway installation to accept around 100 measurement nodes. In reality we find that most customers segment their plant into a number of tank farms,

and typically only want to have 40 or 50 instruments on each gateway.'

The Smart Wireless architecture combines both field installed process instrumentation, and plant networks. Emerson is collaborating with Cisco to deliver an open wireless plant network that offers a number of applications including voice, mobile communication, asset and location tracking, mobile worker, and video applications.

Instrument transmissions on current networks are running at 15-second up-date rates. 'By the end of this year,' Ferris says, 'this will be down to eight seconds, and early into next year we will be at a four-second update rate.'

This is currently a monitoring technology and these updates rates are more than adequate for most monitoring applications. It is not yet a control technology, and that is true of the technologies across all companies.

'I am not aware,' he concludes, 'of any process automation vendor that is today supplying wireless technology for real-time closed loop control purposes. However, as advancements in power technology continue, the day in which wireless communication is deployed on closed loop control systems is probably not too far in the future.'

Honeywell's technology

Honeywell has had great success with its wireless equipment. Its OneWireless universal mesh network solution, which, since June has been compliant with the ISA100.11a standard, is based on three important components. First is the need for data providers; second is a network of infrastructure devices, and finally, data clients.

A data provider is typically a wireless transmitter that provides measured or control data. Commonly these provide temperature, pressure, or other analogue data; but can also include PDA or handheld computers, Notebooks, wireless CCTV cameras, and hazardous gas analysers.

The Honeywell Instant Location System (HILS) for personnel and mobile

Equipment suppliers using wireless technology

In addition to Emerson and Honeywell Enraf, the following companies manufacture or will manufacture wireless instruments during 2008:

ABB has confirmed to its clients that it will be introducing WirelessHART compliant instruments during 2008: www.abb.com

Accutech (division of Adaptive Instruments) currently supplies instruments for pressure, temperature, level, switch inputs, and a multi-input field unit. This can add wireless capabilities to existing or new wired measurement sensors such as radar tank gauges, flow meters, chemical analysers, or any other device that has voltage or current outputs.

The company says its communication spectrum is spread over different frequencies wherein both the transmitter

and receiver are synchronised to hop to different frequencies as the communications continue. It is a technique that has been a key element of the US military's communication security techniques, because it adds security and ensures that noise interference at any one frequency does not block the communications: www.accutechinstruments.com

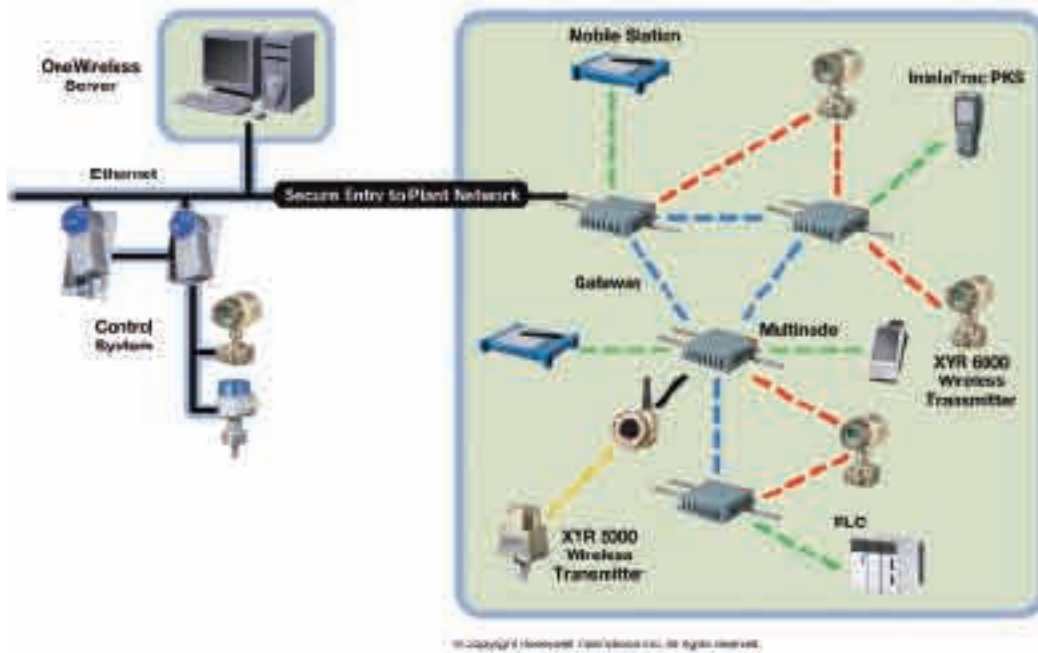
Endress+Hauser played an active part in development of the WirelessHART technology and has confirmed its intention to manufacture wireless instruments during this year: www.endress.com

Siemens Energy and Automation is currently supplying a one-way point to point wireless system for

monitoring and data acquisition. Field devices such as level and pressure transmitters, alarm/status switches, and valve positioners are connected to the transmitter inputs. The transmitter wirelessly sends this analogue and digital process data to a receiver connected to a controller, recorder, PLC or personal computer.

The company also has a two-way multi-point to point system in which a master transceiver can send and receive analogue and discrete signals to and from up to 8 remote transceivers. A serial data system is available that can handle, based on a single master transceiver, 254 remote store-and-forward transceivers. During 2008 Siemens' instruments will be modified to meet the WirelessHART standard: www2.sea.siemens.com

Communication principle of the Honeywell wireless system



Key

- The multinode has three independent transceivers, and therefore uses three types of wireless connections:
- Between multinodes and PDA's, Notebooks, PLC's, CCTV, legacy Enraf gauges etc. (in general COTS equipment)
- Between mutual multinodes, to create the wireless network through meshing.
- Between multinode and sensor device i.e. XYR6000 series sensors and IO, wireless Enraf gauges

equipment is also capable of being integrated into the plant wireless network. These devices communicate through the ISA100.11a compliant sensor network interface, or through the WiFi 802.11a/b/g compliant interface of the multinode network infrastructure device. Existing instruments installed on the site can either be hard-wired, or use an extra custom made wireless

interface to connect to one of the multinode routers. The multinodes maintain a wireless network by creating a mesh with neighbour devices. In the OneWireless solution the multinode also provides an interface for the data providers and data clients. The multinode also connects the existing wired instruments to the wireless network. There are three separate radio transceivers within the

multinode to perform these tasks; the sensor, WiFi, and meshing, and the system uses the highest level of technology to protect these wireless links from unauthorised access. The multinode transceivers can accept at least 40 wireless devices operating on network, using 2.4 GHz band, they can also use 5.6 and 5.8 GHz frequencies, depending on local conditions. Transmissions are on the

Industrial, Scientific, and Medical (ISM) band that does not usually require a licence, or the payment of a fee. Honeywell Enraf's manager of commercial operations, Rokan Salihi, explains that once the wireless infrastructure of multinode routers had been installed, the price premium for wireless tank gauging instruments above the standard wired units is no more than 10%. Within the XYR series of wireless instruments that are suitable for installation at a tank farm, Salihi says that Honeywell can already monitor pressure, and temperature. By installing a separate wireless transmitter to work in association with any digital or analogue output device, it could be made to communicate with the network. The integral wireless version of the SmartRadar tank level gauge is currently on target to be launched early in 2009.

Wireless without strings

At least until acquisitions alter the market composition, terminal owners have the luxury of installing a wireless network that is independent of the major instrument suppliers. US companies such as FreeWave Technologies of Boulder, WorldTelemetry, Tulsa, and Australia's Elpro Technologies supply technologies that can be

used to create a wireless network throughout the plant for process monitoring.

California's Dust Networks recently updated its embedded wireless sensor network solution to the SmartMesh IA-510 model, which includes the new WirelessHART communications protocol.

Dust's pioneering role with its TSMP provided the foundational building block to the new HART Communications Foundation standard for wireless field devices, a part of the HART 7 release. The key features of this new, ultra low-power wireless sensor network standard includes: time-synchronised communication, channel hopping, automatic node joining and network formation, fully redundant mesh routing, and secure message transfer.

Time-synchronised communication between nodes requires a common understanding of time; to know precisely when to talk, to listen, and to sleep. Channel hopping is a technique for crossing multiple frequencies, and a proven way to avoid and overcome interference

to the radio waves. Using this technique, Dust has demonstrated that thousands of nodes can operate together in the same radio space, without affecting end-to-end reliability. Every node is capable of discovering its neighbouring nodes, can ascertain their physical features, establish links, and form a network.

A fully redundant mesh routing requires an ability to try different paths, and repeat the previous transmission. Both are features of the WirelessHART protocol, and thus the network can be



Dust Networks' 2.4 GHz M2510 wireless module measures 24.4mm x 39.9mm x 8.58mm

expanded quickly, and by somebody without extensive wireless expertise. Finally, there is the need for secure message transference, and WirelessHART incorporates encryption to prevent unauthorised reading, authentication to confirm the identity of the sender, and integrity to ensure that the message delivered has remained unaltered during transmission.

Choosing the right system

Availability of proven wireless sensor network products will enable the commercial market to respond quickly to the needs of terminal operators when they finally make the decision to adopt the technology.

For at least two decades there has been little to differentiate the field instruments provided by the major manufacturers, including Emerson, ABB, Endress & Hauser, Siemens and Honeywell Enraf. All meet the high standards of reliability and accuracy demanded by users and

regulatory authorities.

Therefore, price, availability, and prejudice has determined the choice of supplier; but wireless technology could change this, and in so doing, change the current market share of these manufacturers.

The future could see more consideration being given to the selection of the wireless network supplier rather than to the marque of the instrument manufacturer. Small independent companies could provide add-on wireless communication units suitable for existing process monitoring devices as well as new instruments. Whole terminals could be transformed into wireless sites, with the technology being introduced quickly and inexpensively. ●

Useful contact details:

- **Standic**
www.standic.com
- **Elpro Technologies**
www.elprotech.com
- **Emerson Process Management**
www.emersonprocess.com
- **FreeWave Technologies**
www.freewave.com
- **WorldTelemetry**
www.lpgcentral.com
- **Dust Networks**
www.dustnetworks.com
- **Honeywell International**
www.honeywell.com/ps/wireless