

Refining Wireless

A Case Study of Wireless Technology
for Improved Metals Refining

Authored by Matthew Lee
Senior Engineer
iVolve Pty Ltd

Revision 1
30 October 2007

© 2007 iVolve Pty Ltd (Australia)

Introduction

The processes used to perform the electrolytic refining of metals such as copper, gold, lead and zinc are highly complex and require the constant monitoring of potentially thousands of electrical and chemical parameters to ensure they remain within desirable limits.

As a result, electrolytic refineries have always been very difficult and expensive to operate.

Brisbane-based process control group MIPAC recognised the value of utilising wireless communications to monitor each individual component in the refinery, and approached iVolve to assist them with the design and implementation of a solution.

By combining the capabilities of one of iVolve's wireless communications products (Nexis™) with their expertise in product development, industrial solutions and wireless communication systems, iVolve were able to ensure the resulting product fully met all the requirements and was ready for real-world installations.

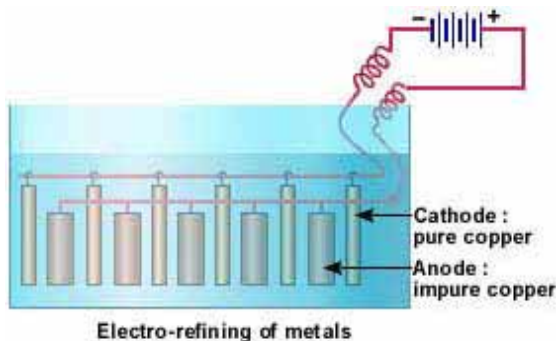
The final key component in the overall solution, an ultra-low-power, wireless sensor, was developed by Syndetic, another Brisbane-based company with expertise in electronics design.

This paper provides an overview of iVolve's role in the development of this exciting new product, called CellView, and the communications technologies it utilises to deliver state-of-the-art monitoring capabilities, and improvements in process efficiency and safety, to the electrolytic refining industry.

The Problem

Electro-refining plants typically consist of hundreds or thousands of electrolytic “cells” (often referred to as “baths”) arranged into groups known as “lines”.

Each cell contains a number of alternating anodes and cathodes (typically 20-40) suspended in an electrolytic solution. When a large current is applied to the cell, the base metal is transferred from the anode to the cathode, leaving almost all of the impurities in the electrolyte.



The operating parameters of each cell must be constantly monitored to ensure that the electrorefining process is occurring under optimal conditions.

If these conditions are maintained throughout the duration of the process, which can take up to several weeks, the result is a cathode of highly pure metal.

During this time, however, a number of problems can occur that can have an impact upon both the efficiency of the process and also the safety of the

personnel involved. These problems are often very difficult to detect in a timely manner.

Short circuits are one of the most significant problems that can occur. A short circuit between any of the anodes and cathodes in a cell results in several problems

1. The electrolytic process between all the plates in the cell stops since the current flows directly through the short
2. The temperature of the cell increases, producing high levels of dangerous gases

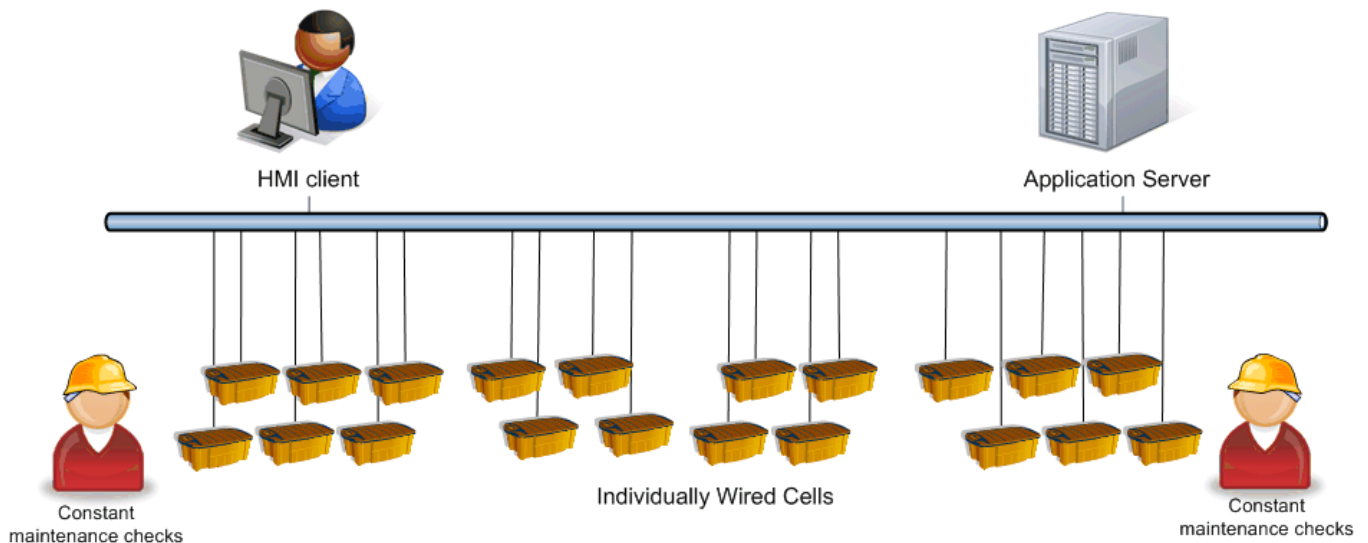
As such, any faults must be detected quickly and appropriate maintenance personnel informed.

Traditional monitoring systems have typically consisted of a SCADA/PLC system or DCS, with each cell being wired back to a central control room. Inside the control room, the Operator Interface (or HMI - Human-Machine Interface) provides a graphical view of the plant, including any active alarms or alerts.

Some refinery floors cover an area the size of several football fields. With this in mind, it is easy to imagine the amount of wiring that must be installed to provide monitoring for each and every cell back to the central control room.

With several thousand cells requiring monitoring, this adds up to an extremely costly exercise, not just for the cabling but also the labour required for installation and commissioning.

Add to that the ongoing maintenance costs, and it is easy to see that monitoring systems consume a significant proportion of the setup and operational costs of a refinery.



The Solution

The obvious solution to the high cost of materials and labour for a wired monitoring system is.... “get rid of the wires”.

By installing a wireless system, the site operator can realise significant savings in both cost and time. Installation costs (in the order of several million dollars) are estimated to be reduced by 50% or more. Installation times of several months are expected to be slashed by 75% or more.

Without kilometres of wires running through conduit in and around vats of scalding hot acid, maintenance costs will also be reduced to a shadow of their former self. In a wireless-based system, virtually all components will be out in the open (one side-effect of using wireless) and thus easily accessible.

Additionally, an intelligently planned wireless installation will allow for simple future expansion and also permit additional uses for the wireless infrastructure (such as roaming operator tablets with real-time access to the SCADA system, VoIP, remote email access, etc).

Wireless Options

There are a multitude of options available for components in the overall solution. It would be possible to utilise a local “collection” node, with small

groups of sensors hard-wired back to each node. Each node could then link wirelessly back to the control room.

However, to maximise the benefits of implementing a wireless system, as outlined above, each cell’s sensor should have its own wireless connection into the SCADA system. This solution also has the advantage of greatly simplifying maintenance.

The next question, then, is how to best architect a wireless network with thousands of sensor nodes. One significant point of consideration for the system is the power supply of the wireless sensors. A battery that will run for at least two years before replacement requires the sensor to have a very low power consumption with minimal “on” time duty cycles.

And last but not least, which of the available wireless technologies on the market would be most appropriate for this solution. The selection of this component had to address the power requirements outlined above, as well as issues such as security, spectrum availability in all target markets and scalability.

It was decided early on that the use of the 2.4GHz spectrum would be the most appropriate to ensure the solution could be used globally with little or no regulatory obstacles.

This decision then led to the following technologies being available for consideration for the wireless communications with the sensors:

- Wi-Fi (802.11b or 802.11g)
- ZigBee (802.15.4)
- Proprietary Systems

Each of these options was initially considered and subsequently rejected as unsuitable for this particular project for various functional reasons, as outlined below.

Wi-Fi

Wi-Fi provides large amounts of bandwidth, but at a relatively high cost and with large power requirements. Additionally, several thousand Wi-Fi clients on a single network segment would make for unacceptable transmission collisions, eating up valuable battery life.

ZigBee

ZigBee has become a very popular technology for wireless sensor networks. However there are disadvantages:

- Only reduced-function end nodes can operate on batteries (i.e. routers cannot)
- At the commencement of this project, there were very few stable implementations available
- ZigBee Alliance costs are significant

Proprietary Systems

Today there are also a number of proprietary Wireless Sensor Network (WSN) implementations available.

These include offerings from the likes of Dust, Crossbow and Ant. The proprietary WSN components considered were either overly expensive and/or did not meet the battery requirements dictated by the project specifications.

Network Architecture

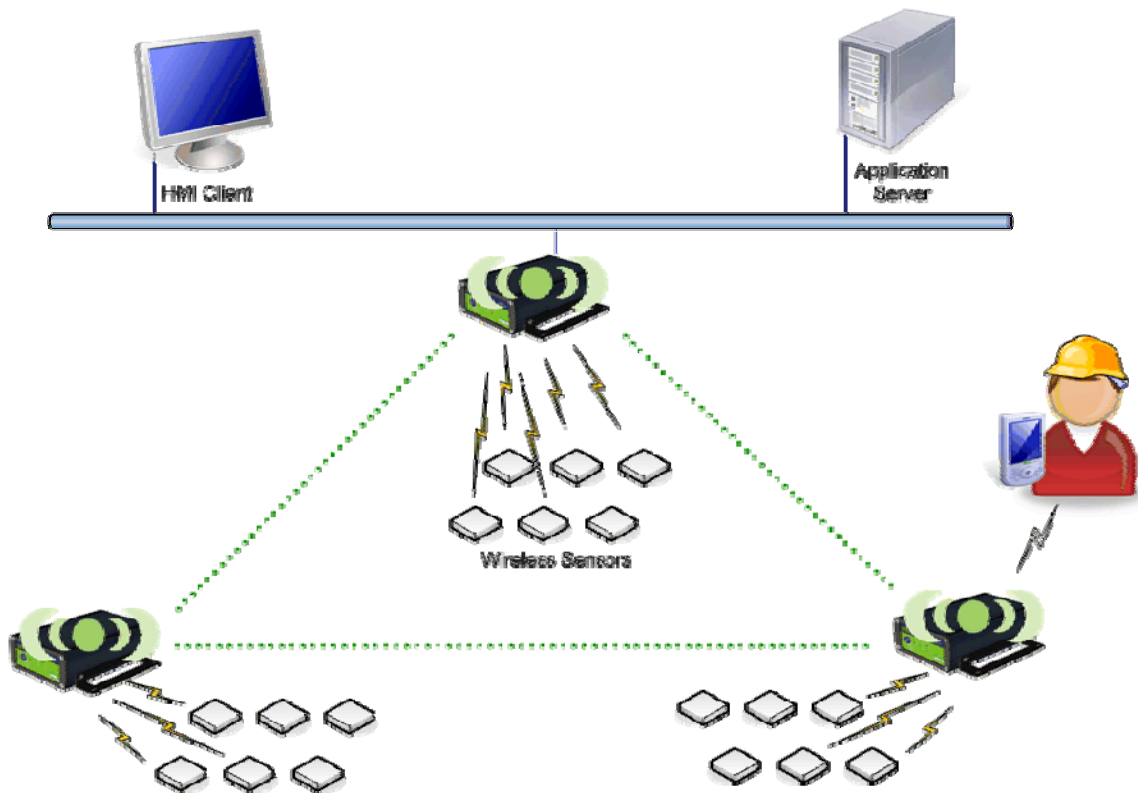
It was obvious at this point that the ideal solution would require a combination of wireless technologies to ensure all the requirements could be met.

The resulting network design comprises three tiers:

1. Wireless sensor nodes
2. Wireless data concentrators
3. Control LAN

Sensors

The wireless sensor nodes (first tier) are installed on each cell. These devices were custom-designed by Syndetic. They utilise low bandwidth RF transceivers operating in the 2.4 GHz ISM band and operate with extremely low power requirements. Each sensor is responsible for monitoring an individual cell, and reporting the results at a configurable rate back to a data concentrator (tier 2). The sensors use a special channel hopping and selection algorithm to



minimise interference with neighbouring sensors and to ensure they are always communicating with the best data concentrator. This approach also ensures that should a data concentrator fail or be disabled, the sensor will automatically switch channels and begin communicating via the new best option. This fault tolerant approach ensures the system will provide maximum availability.

Data Concentrators

The data concentrators perform the task of coordinating communications with a collection of sensors.

Each data concentrator contains a 2.4GHz transceiver similar to that used in the sensors. Unlike the sensors,

however, each concentrator is configured to use a single channel. This allows the channels to be optimally distributed across the entire refinery.

The data concentrator also provides the sensor with key configuration parameters such as how often to perform measurements.

The information the concentrator receives from the sensors is then forwarded on to the Control Network for analysis, reporting and archiving. This communication occurs over a high bandwidth backhaul link utilising open-standard 802.11bg (Wi-Fi) radios.

The final role allocated to the data concentrators was that of a standard Wi-Fi-compliant Access Point. By

requiring each data concentrator to operate as an Access Point, each concentrator can then also be used to provide Wi-Fi access to personnel in the refinery using devices such as PDAs and laptops. These devices then become an important tool for mobile monitoring of the system as well as an aid during commissioning and maintenance.

To provide sufficient levels of redundancy and scalability across the backhaul network, a mesh routing solution was required.

Using a mesh network (as opposed to standard access point / repeater network) for this “tier” was essential for a number of reasons:

- There is no need to provide traditional Wi-Fi access points and clients. The mesh router acts as both an access point and client to other routers, all in the one device. This keeps the hardware cost, count and complexity as low as possible.
- Additional nodes can be added to the network (or existing nodes moved) as required, with minimal, and in most cases no network reconfiguration.
- Data security can be maintained between mesh devices. Wi-Fi / 802.11 does not specify a standard for data encryption *between* repeater nodes, only between the client (eg. laptop) and the Access Point.

Fortunately, iVolve’s Nexis product already provided much of the functionality required by the data concentrator devices, requiring only the addition of the 2.4GHz radio transceiver required to communicate with the sensors, and some enhancements to the device’s firmware to implement the sensor management logic.

Control Network

The final tier in the CellView network is the Control Network. The control network consists of a central server (or multiple servers for a redundant configuration) providing data storage, configuration management and reporting facilities for the CellView solution. One or more of the data concentrators are then connected to a local Ethernet network. These devices operate as gateways between the server(s) connected to the Ethernet network, and the remaining data concentrators via the wireless mesh network. This architecture ensures all components in the system are redundant and in most cases self-healing and fault-tolerant.

The CellView server also provides an embedded OPC Server to ensure standards-based interoperability with other systems such as SCADA, DCS and other HMI systems. This allows the information retrieved from the cells to be viewed, graphed and alarmed in real-time, providing immediate

notification to operators whenever a problem is detected with a cell.

Mesh Networks Primer

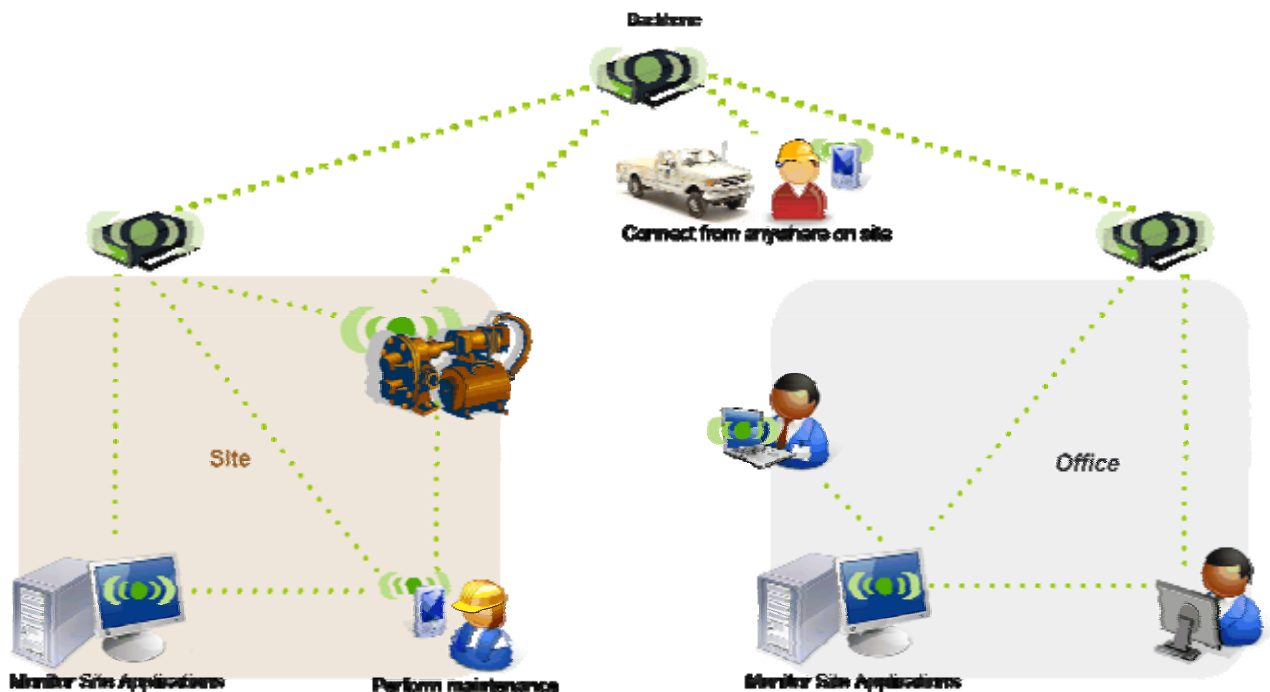
One of the key features of the CellView system is the use of a mesh network to provide the backhaul links for the cell monitoring data as well as local WiFi access.

Mesh network provide a very powerful and flexible way to extend the coverage of a traditional access point-based wireless network. The network nodes, typically routers, utilise special routing algorithms to dynamically adapt to topology changes in the network. Using the intelligence of each node, meshing helps the components join together in a self-organising structure.

Communications paths are dynamically established between neighbouring nodes on demand. If one node becomes unavailable for any reason, the other nodes will “heal” the network by creating an alternate path. This is what is meant when a mesh network is described as “self healing”. This behaviour provides inherent redundancy into a mesh network.

When evaluating a mesh network, one must give the following features consideration:

Autonomy: Mesh nodes should be able to operate *stand-alone*, forming mesh networks without the need for a centralised management server. This is essential for remote, mobile applications where a path back to “head office” is not guaranteed.



Redundancy: The nodes should be able to be utilised such that there is no single point of failure that can severely interfere with the operation of the network.

Capacity: The network should provide a high-capacity backbone to ensure there are no bottlenecks. The network should also cater for future applications and expansion.

Scalability: The network should use a modular design that enables it to be extended to new areas in the future with minimal loss of performance.

Security: The network should provide data security as required by its administrators.

Mobility: The network should support mobile nodes / access points, and dynamically adjust as these devices move around the site.

Maintainability: The network should maximise the use of common components to minimise spare parts requirements.

Open Standards: The network should utilise open-standards based equipment (where possible) to maximise interoperability with other vendors and suppliers of equipment and services.

Client Access: The network should provide open-standard Wi-Fi compliant access for clients.

Benefits of using Nexis

The Nexis product, in addition to its mesh router / Wi-Fi access point functionality, contains an industrial computer with a variety of I/O interfaces. This enables customised applications to be developed for customers' unique requirements.

Furthermore, the Nexis platform was designed from the ground up to operate in the harshest environments and will happily operate in environments with very high magnetic fields (where many other devices fail), as experienced in metals refining plants.

In the case of the CellView solution, the Nexis enclosure was redesigned to cater for the wireless transceiver which operates as the "Access Point" to the sensor nodes on each cell. It has a serial (RS-232) interface through which it communicates with its host Nexis. The low-level protocol is handled between the wireless nodes and the access point node, with higher-level processing handed off to the host Nexis.

The ability of Nexis to handle some of the communications processing on-board means that less data is required to be sent across the Wi-Fi network to the control room. It also means that it can operate as an intelligent "parent" to the sensor nodes, should the backhaul communication link to the control room / application server be lost.

This last feature is extremely important to this particular application. The largest single consumer of power in the sensor nodes is operating the RF receiver. For the wireless sensor to locate a "parent", it must scan through the available RF spectrum looking for beacons. If the parent (in our case, the Nexis router) stops communicating with the sensor node, the node will continue scanning for another parent. Because Nexis is able to maintain association tables and perform low-level protocol communications with the sensors, a communications outage back to the control network does not cause the sensors to continuously search for a new parent that does have the communications link in place.

system has already been sold to an Asian copper refinery.

In addition to operating as a mesh node, Nexis also provides the services of a standard Wi-Fi access point. This means that clients can access the control LAN while out on the refinery floor. Via a PDA application, they are able to monitor and control the refinery process, as well as perform tasks such as sensor commissioning and maintenance, or even make VoIP phone calls.

Status of Project

The system described in this document is currently undergoing trial at a potential customer site. To date, it has been largely successful as a trial. The network architecture used has worked well, with very little effort required integrating the various tiers.

Interest in the product has been very good and the first MIPAC CellView

About the author

Matthew Lee

Matthew Lee is the Senior Engineer at iVolve Pty Ltd.

As Senior Engineer, Matthew oversees key service projects and is the chief consultant and software engineer for the development of iVolve's products.

Matthew has over 15 years professional experience working as a Software and Communications Engineer specialising in networking and wireless communications systems for both large and small engineering and consulting organisations, and as a Software Engineer for iVolve.

Some of the projects he has been involved in include a real-time production monitoring system for mines, implementing a wireless network for monitoring refrigerated shipping containers, a DSL line card and POTS line testing system.

Matthew has a Bachelor degree in Electrical Engineering from The University of Queensland.



About iVolve

Founded in 1995, iVolve is an innovative and dynamic Australian company specialising in developing world class solutions for the mining, manufacturing and minerals industries. Our networking and industrial expertise allows us to develop unique products specifically for the demands of the rugged industrial environment which are currently used by a number of the world's largest mining companies.

iVolve has a unique combination of vendor-independent skills and experience in wired and wireless networking for industrial and high security or integrity sites. Our engineering team can assist with firewalls, Virtual Private Networks, data protection, remote access, and wireless networks.

iVolve's dedicated team of software engineers have a thorough understanding of all emerging technologies as well as an in-depth knowledge of a wide array of SCADA and DCS systems, Logic Controllers and other industrial systems.



About MIPAC

MIPAC is a specialist Australian company dedicated to the pursuit of cost effective and appropriate process control solutions. MIPAC's core business is process control and it is this specialisation that has allowed the group to develop a full suite of services and products to facilitate a successful control solution for any application.



About Nexis

Nexis is an embedded industrial computer engineered to withstand the tough electrical and magnetic environments found in refineries, smelters and other industrial situations. In addition to providing an integrated platform for custom applications, Nexis includes wireless mesh routing and standard Wi-Fi access point and client capabilities. 802.11a, 802.11b and 802.11g are all supported by a modular architecture allowing for future technology upgrades.