



# The contrasting requirements of today's SCADA applications

Considerations and case studies

John Yaldwyn, CTO



# SCADA and an introduction to 4RF Communications



Today's topic: SCADA (supervisory control and data acquisition) VHF/UHF radios for smart monitoring and control applications in oil and gas, utility, and transport sectors.

4RF designs and manufactures high performance microwave point to point and VHF/UHF point to multipoint radio equipment for critical infrastructure applications:



- Extending the reach of communications infrastructure - more distance, more data, more dependability
- World class research and development team in New Zealand exporting to customers in more than 120 countries across six continents
- Customers include emergency and military organizations, public safety and homeland security, government, utilities, telecommunications operators, oil, gas and mining and transport operators



# Transitioning from legacy serial to IP

In the past SCADA system relied on analog FM radios and 1,200 bps AFSK modems – this legacy equipment is still widely used.

Meanwhile the world is migrating from the use of legacy serial protocols to IP-based systems. The benefits of IP and IP SCADA networks are becoming clearer.

Equally clear is the fact that this migration will not happen immediately. Vendors need to support users with equipment that is both backwards-compatible and future-proof. However, IP also brings additional security concerns that need to be addressed.



How far along the road are you?

“The speed of technology change in the telecommunications market is high compared with utility technology. Utilities expect asset life of up to 40 years. This exposes utilities to risk of obsolescence and associated cost of maintaining obsolete technologies.”  
[EON, EUTC 2009]

# What are the benefits of an IP SCADA network?

For utilities and SCADA, using IP has a number of benefits:

- Network interoperability between devices
- Over-the-air control of remote devices, e.g. SNMP
- Reduced requirement to visit remote sites
- Ease of interface to modern PC and server systems
- Common cabling systems



The migration to IP is not solely related to the benefits of IP: regulatory pressure or government cyber security concerns may mandate a security upgrade of existing serial network.

Past infrastructure roll-outs have considered communications last. Critical equipment is selected first then a supporting network designed. Moving to IP allows installation of network connectivity first, with the knowledge that all IP equipment choices can be supported.

# SCADA equipment is evolving to support IP

The benefits of IP mean that the latest generation of SCADA remote devices\* are IP based, with many advantages:

- Low cost, reliable, and scalable
- Widely accepted, a proven standard
- Multiple applications share network resources (however, this does present possible security issues)
- Ubiquity, use over virtually any physical medium

However, there is a huge deployed base of older generation SCADA systems using serial RS-232/V.24.

Network infrastructure, including radio devices, therefore needs to work with a wide range of SCADA equipment.



\* SCADA devices: remote terminal unit (RTU) or intelligent electronic device (IED)

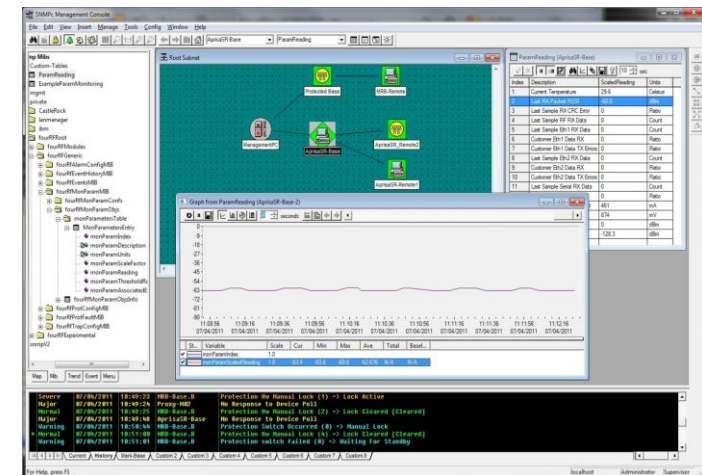
# So what should a 21<sup>st</sup> century SCADA radio look like?

Today's VHF/UHF SCADA radio needs to be flexible, spectrally efficient, and secure.

It should provide a means to mix legacy serial and modern IP SCADA elements in one unified network, ideally with the ability to connect serial devices via IP using a form of terminal server capability.

Security needs to be considered from all 360 degrees and older RTU devices should be able to be secured by 'wrapping' unsecured serial traffic into a securely protected radio infrastructure.

Finally, a comprehensive standards based SNMP network management system should enable visibility of all remote sites.



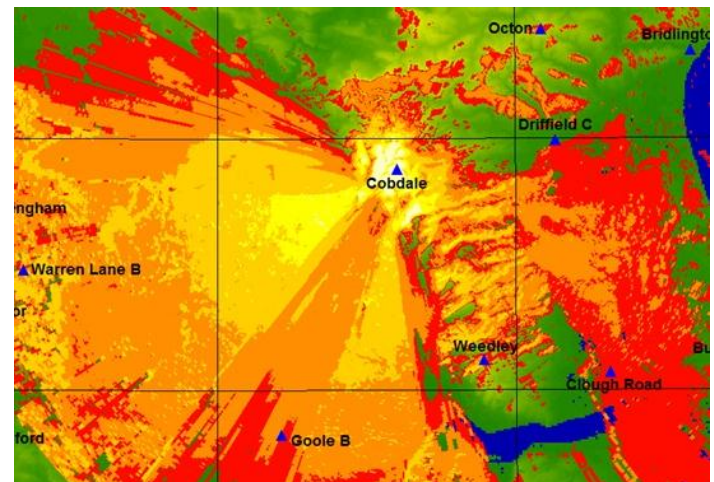
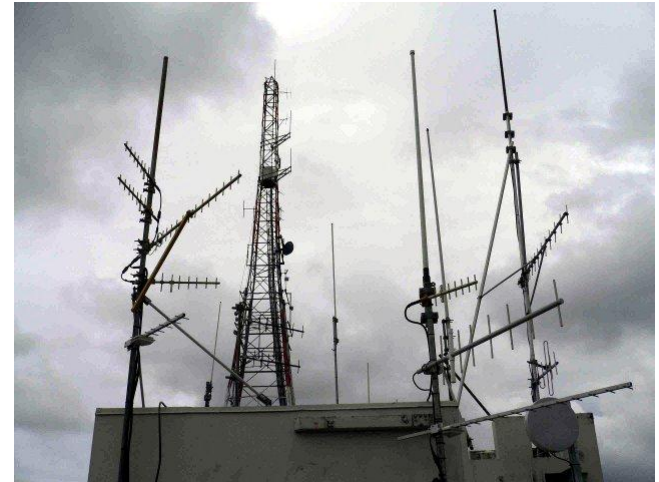
# The RF environment

Modern SCADA radios use digital modulation for point to multipoint applications and operate in sometimes crowded bands shared with land mobile radio and other applications.

They need to handle multiple strong signals while receiving co-channel signals with highly varying signal strengths.

SCADA base stations communicate with remote units, often more than 50 for a single base station with links greater than 60 km, depending upon the terrain. Topographic features such as hills, mountains, trees, foliage, and other path obstructions (buildings) all limit radio coverage.

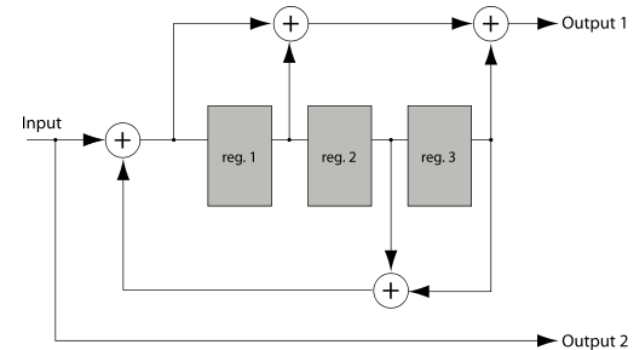
Real world performance will be determined by many factors including location, number of remote stations, and the traffic profile across the network.



# System gain via FEC, throughput gain via LZ and proxy

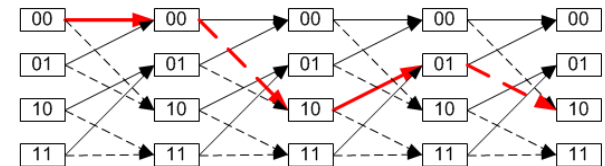
System gain through modulation and FEC:

- Continuous phase 4FSK, robust and energy efficient
- Forward error correction (FEC) rate 3/4 trellis code, this efficient convolutional code works well with arbitrary length SCADA data
- FEC significantly improves the radio performance in terms of distance and immunity to interference



Payload compression helps throughput:

- Dynamic table based lossless Lempel-Ziv (LZ)
- Compresses both serial and Ethernet up to 50%



Proxy addressing option:

- Typical 100 byte SNMP messages can be reduced to 10 bytes saving bandwidth and reducing overhead

More usable bandwidth delivered.



# Real world performance

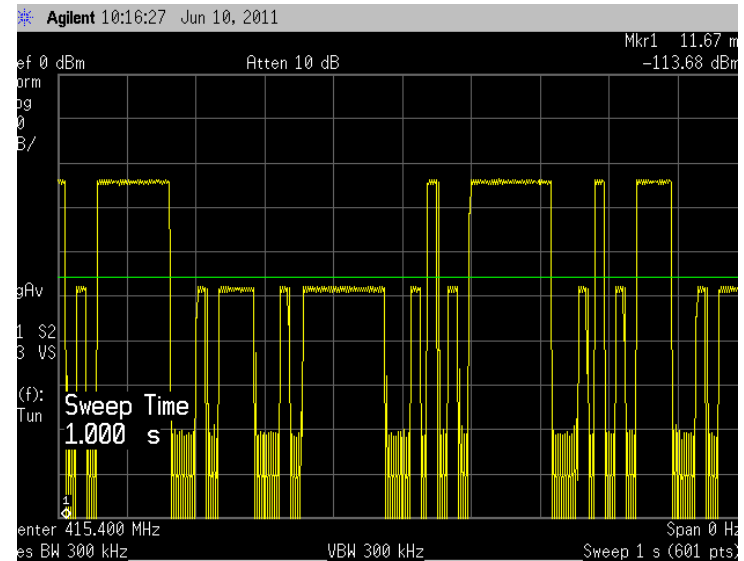
The real world performance of a SCADA network relies on robust and efficient modulation, powerful error correction, RF considerations, and an effective MAC.

- Industry receiver sensitivity (for  $10^{-6}$  BER) at 9,600 bps ranges from -106 dBm to -110 dBm (12.5 kHz channel)
- Sensitivity (for  $10^{-6}$  BER) at 19,200 bps is typically -96 dBm (12.5 kHz channel)

Operation at 19,200 bps needs 10 to 14 dB more power for same performance

- Transmitter would need to be increased by 50 to 125 W for same performance

Rather than raw speed, real world performance depends on less obvious features such as RF performance, intelligent design of the media access control (MAC) data communication protocol sub-layer, high speed transmit-receive switching, and compression features.



# Security in the headlines

ITU secretary general Dr Hamadoun Touré has called for an international cyberwar peace treaty - Jan 2010.



“I do not rule out the prospect of an **aggressive** act of such a scale which deliberately **targets** the networks that are the nervous system of the country's **critical infrastructure** - that is, the energy grid, our water supplies”

March 11 2010, Rt Hon Baroness Pauline Neville-Jones, ex UK Minister of State for Security and Counter-Terrorism.



# Cyber terrorism

The cyber threat to “the **massive grids** that power our nation ... is one of the **most serious** economic and national **security challenges** we face as a nation”.  
President Obama - May 29 2009.



In this context, cyber terrorism is the use of the Internet to make deliberate terrorist attacks against information systems affecting real world infrastructure, property, or lives. Real threats exist from disgruntled ex-employees, those who ‘hack for fun’, radical environmentalists, terrorists, and state sponsored entities.



# SCADA network security

Cyber security is a key issue today, and rarely out of the headlines. SCADA radio needs to be secure.

Security has become a key differentiator in the marketplace and in the real world.

Security must be designed into products and networks from the start:

- Taking account of the key considerations of integrity, availability, confidentiality, and non-repudiation
- Building on industry best practice and standards
- With security features throughout the interfaces, operating system, and management



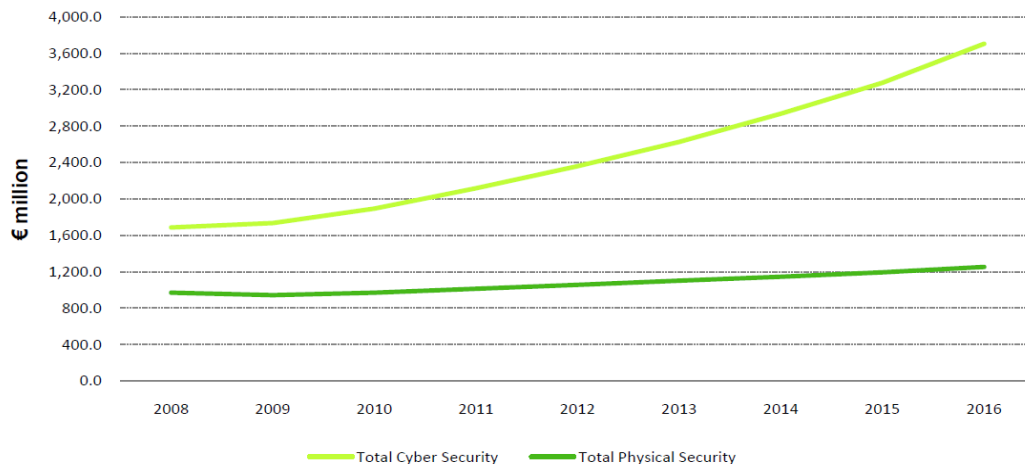
# SCADA radio needs to be secure

Additional security and resiliency is provided by the fact that private SCADA networks are not subject to public network overloads caused by sporting fixtures or major public events. ACMA take note.

Incorporating security within the SCADA network saves money and reduces the risk of early obsolescence as government infrastructure security recommendations turn to regulation.



Critical Infrastructure Security Investment, Europe by Type, 2008-2016,



Source: Solomon Barnes Consultancy

# What is meant by the 360 degree approach to security?

Examples:

- Over the air protection
- Protected management interfaces
- Secure USB software upgrades
- Micro-firewalling Ethernet interface
- Using government standards and best practice

This approach means securing the perimeter around the SCADA radio and the design environment of the product – all external ports must be considered:

- Antenna
- Ethernet
- Serial
- USB

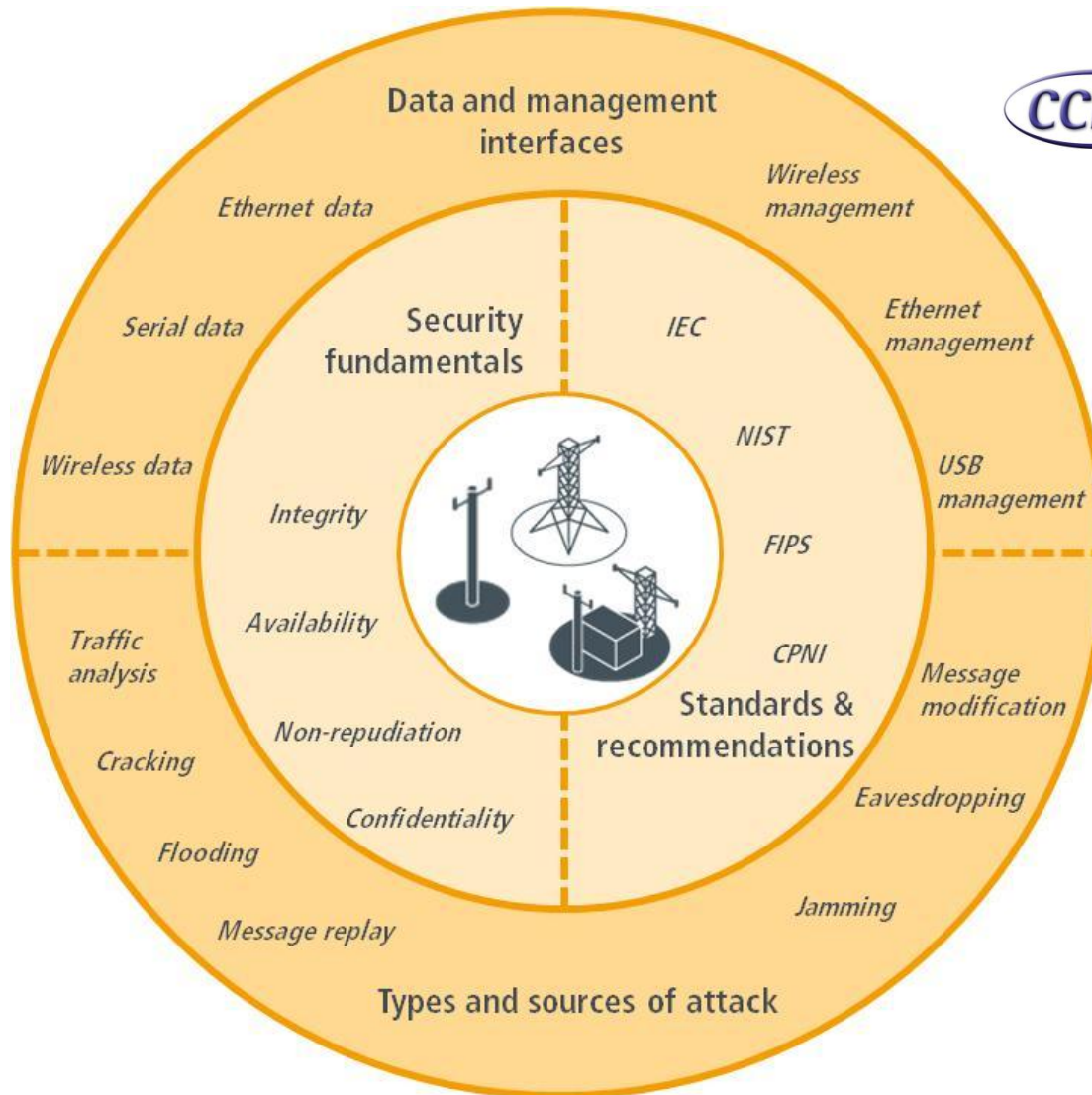


Management

Data

“The price of peace is eternal vigilance”, Leonard Courtney, 1st Baron Courtney

# Security considerations and recommendations



Specific references include IEC/TR 62443 (TC65) 'Industrial Communications Networks – Network and System Security', IEC/TS 62351 (TC57) 'Power System Control and Associated Communications – Data and Communication Security', and IEEE P1711/P1689/P1685.

# SCADA security must be designed in from the start

A comprehensive and in-depth approach to cyber security from the very start is the best way to protect a network. Takes into account four key factors:

- Security fundamentals: integrity, availability, confidentiality, and non-repudiation
- Sources and types of attack: communications and control systems are subjected to attack from many sources, internal and external, malicious and accidental
- Types of traffic and interfaces, both management and data, that could be compromised
- Security standards and recommendations: industry best practice



# Key considerations – integrity and availability

A reliable network must be designed around maintaining integrity and availability.

What is integrity and why is it important?

- Integrity is preventing the unauthorised modification of information
- The communications network must ensure that a control message received by a remote asset is the same message that was originally sent to that asset
- A 'halt' message that has been changed to a 'run' message may have catastrophic consequences

What is availability and why is it important?

- Availability is preventing the denial of a service
- If a control message is sent to a remote asset there must be an assurance that the message actually arrives at the remote asset
- A 'halt' message that never arrives may also have catastrophic consequences

CBC MAC authentication combined with powerful FEC and CRC mechanisms is a robust means to address these goals.

# Key considerations – confidentiality and non-repudiation

A secure network must be designed around maintaining confidentiality and non-repudiation.

What is confidentiality and how it is achieved?

- Confidentiality is preventing the unauthorised access to information
- Encryption is used to reduce information leakage as far as possible to potential attackers: the key can be securely changed by over the air rekeying (OTAR)

What is non-repudiation and how is it achieved?

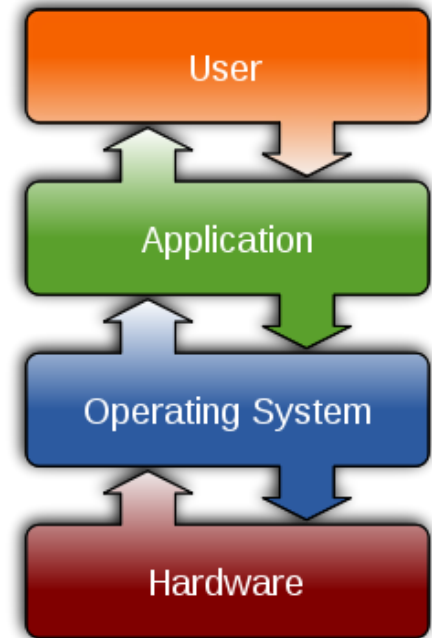
- Non-repudiation is preventing the denial of an action
- Data authentication ensures that data and commands cannot be refuted, preventing replay and man-in-the-middle attacks

These functions can be implemented through the use of robust and recognised cryptographic algorithms and techniques based on the AES standard, using block ciphers and 256 bit keys and the NIST specified CBC MAC method of authentication.

# Internal operating system security measures

SCADA radio operating system measures should comprise:

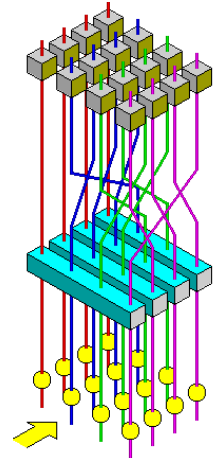
- No output is displayed during boot sequence – together with closing ports during system start-up, this prevents interruption of the start-up sequence and the ability compromise operation
- No user access to radio's internal file system – the core operating system should not be accessible to, or programmable by, the end-user thus ensuring the core functionality of the radio cannot be compromised
- Telnet port block – restricting Telnet access prevents unauthorised access to the management functions of the radio
- ICMP block – blocking ICMP data protects the network should it become subject to a denial of service attack
- FTP block – limiting access to file transfer functionality prevents unauthorised users transferring and uploading malicious files over the communications network



# Security technical summary

Good SCADA security incorporates a number of key technical factors:

- Advanced Encryption Algorithm (AES), based on the Rijndael proposal as specified in FIPS PUB 197, configurable as 128, 192, or 256 bit encryption, with OTAR, optionally applied to all management and user data
- Cipher Block Chaining Message Authentication Code (CBC-MAC) specified in NIST SP 800-38C ensures data is from an authorised source
- Use of licensed frequency bands offers regulatory protection against interference from other users or unauthorised interference – while this does not stop jamming from occurring, enforcement measures are provided by the government licensing agency unlike unlicensed systems where there is no protection
- Encrypted software upgrades (i.e. from USB memory sticks) prevents a hacked version of device software being injected
- Data / management IP port segregation avoids management masquerade
- Operating system considerations





## Case Studies



# Marlborough Lines

Marlborough Lines is an electricity distribution company, covering more than 11,000 square kilometres of rural NZ.

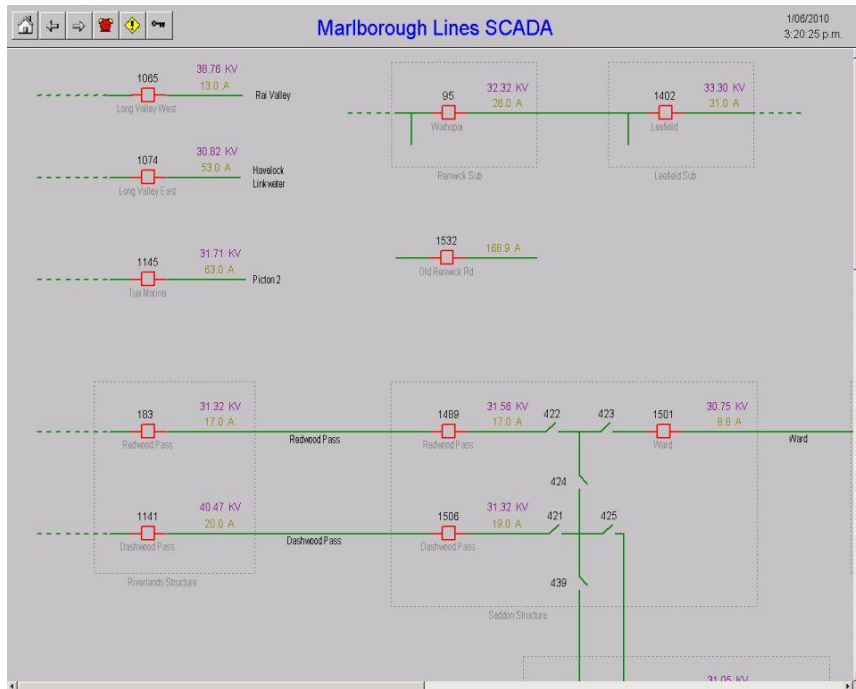
The company receives 33kV supply from national grid operator Transpower and distributes to 23,900 consumers.

Application is recloser monitoring - these devices automatically attempt transient fault clearing, 70% success rate w/o callouts.

In this deployment UHF SCADA remote stations were installed inside pole mounted Nu-Lec recloser control cabinets linking to the SCADA master via DNP3 protocol.



# Marlborough Lines



This GUI shows a part of the recloser monitoring network.

Reclosers can operate autonomously but without SCADA operators must rely on customer telemetry.

To create the connection to the recloser a device was added to the SCADA master software and then a DNP3 Class 0 integrity poll was configured to be requested every 3 seconds.

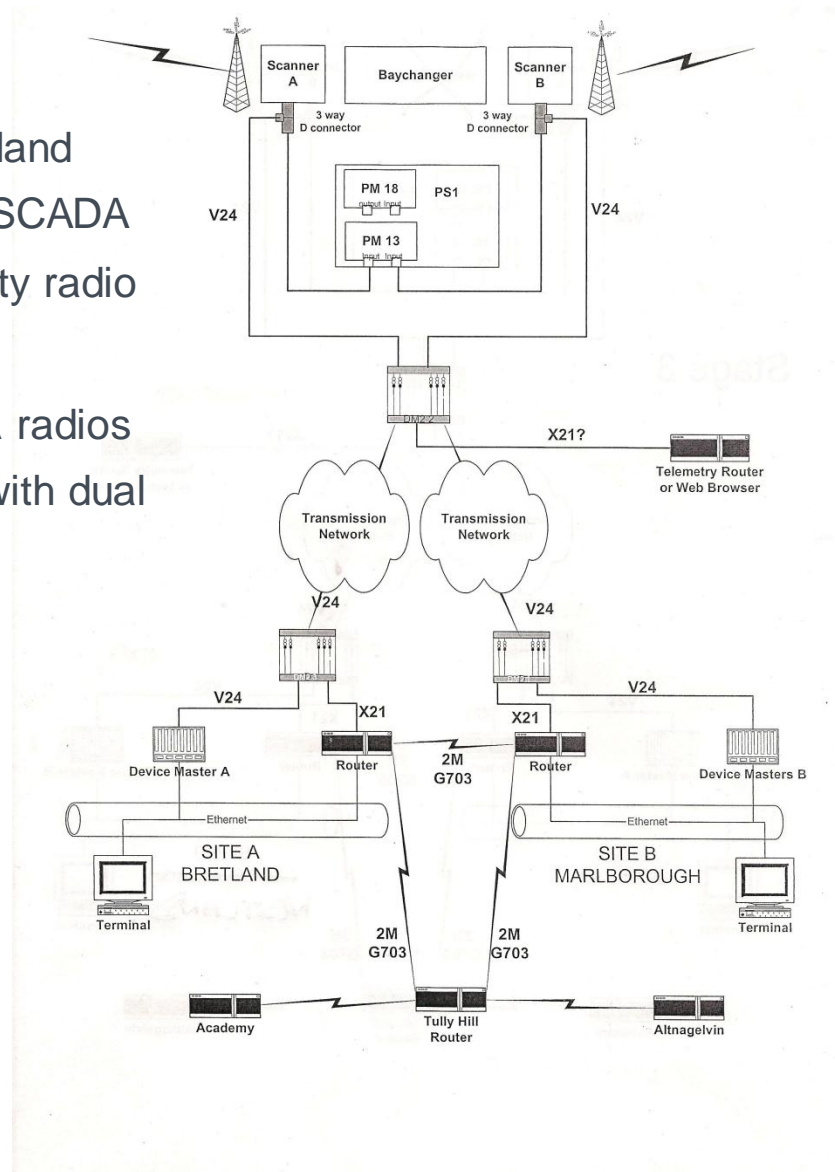
The poll requests all data points from the recloser (around 200 bytes at the data link layer) across the UHF SCADA link.

# Northern Ireland Water

The state-owned water provider in Northern Ireland serves 1.7 million people and is updating their SCADA management system with the largest water utility radio project in Europe this year.

4RF is supplying more than 1,900 UHF SCADA radios for a network typical of the UK water industry, with dual connections to dual protected bases stations.

## Northern Ireland's water crisis



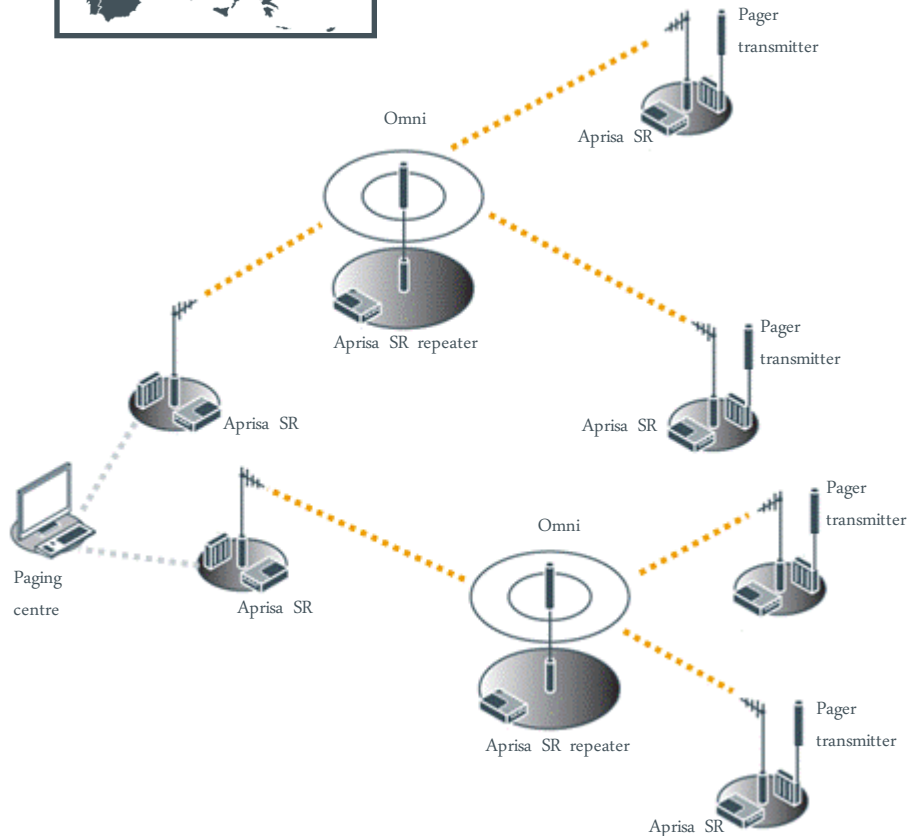
## Northern Ireland Water

The UK requirement is for a data driven Protected Station that provides dual radios, dual serial ports, and interface protection for two SCADA radios when configured as a single base station operating through independent antennas. In other words complete duplication rather than the more traditional redundant switch over solution.

Each radio in this configuration has own unique IP and MAC address but knows the address of the partner radio. On power-up, the primary radio will assume the active role and the secondary radio will assume the standby role. Radio selection is made by the SCADA master software.



# Ministry of Defense, Slovenia



Unusual SCADA system for critical public safety applications replacing analog mountain backhaul system for Slovenia's Ministry of Defense pager network.

The challenge:

- Easy installation needed: many remote sites and mountainous terrain
- Challenging environmental conditions, with below freezing temperatures
- Increased speed and security were essential

The result:

- Used the same channels as the analogue system being replaced
- 78 radios deployed, 14 base stations, 16 repeaters, and 48 remote stations
- Longest link was 56.7 km