Security considerations for narrowband supervisory, control, and data acquisition (SCADA) radio systems

John Yaldwyn
CTO, 4RF Limited
Wellington, New Zealand

Abstract

Private narrowband supervisory, control and data acquisition (SCADA) radio is an effective and economic grid communications tool with a proven heritage. Utility owned narrowband private radio networks provide an alternative to more complex third-party networks. The bandwidth requirements for today's grid monitoring and control technologies have escalated, particularly through the adoption of new IP-based SCADA protocols, the demand for better security, and the penetration of network management into all levels of grid communication networks. However, owning and controlling your own network requires close attention to security, both the symmetrical encryption used to protect over the air transmissions and the authentication used to control device and user network access. Deployment of a radio based solution and its integration with information technology systems requires critical security design decisions.

Narrowband SCADA radio overview

Private SCADA radio systems, sometimes called Multiple Address Systems (MAS) operate in the FCC Part 90 220 MHz, VHF, UHF, 900 MHz, and Part 101 bands. These are popular and effective means of data collection and remote control over long distances ranging from ten up to 100 miles, with distances of 35 to 50 miles being typical. In response to pressure for both higher data rates and more efficient use of the radio spectrum, SCADA radios are now available from a number of manufacturers that operate at rates from 9,600 to 60,000 bps in FCC part 90 channels, with even higher rates possible in FCC part 101 bands. In addition to speed, users contemplating migration to these devices will benefit from a range of new operational enhancements including IP support and SNMP management. However, one of the most critical features that must be considered is security.

It might seem that alternative wireless technologies, particularly cellular, would be appropriate for SCADA networks. While these public systems might superficially seem suitable, issues of reliability, quality of service, and lack of service priority alignment make them unpopular within most utilities. This is more than institutional bias; it is the result of simple economics for cellular companies. They are not in the business of considering the priorities of a few tens of thousands of critical infrastructure points ahead of tens of millions of consumers. Mobile networks are not designed to operate under extended power outages. The attempt by the FCC post Katrina [1] to mandate a minimum of 24 hours of cellular resilience failed after industry objections and was cut to 8 hours.

Systems based on land mobile infrastructure have also been used for private SCADA communications. Modern digital LMR systems such as DMR and Tetra [2] are low speed systems designed specifically to support mobility. The modulation and coding systems used are suitable for low speed digital voice but not high speed data. DMR systems for example offer just 1,200 to 2,400 bps a fraction of the rates offered by modern SCADA radios in the same RF channel bandwidth. There is no question of the usefulness of dedicated digital land mobile radio networks for voice mobility requirements but when network incidents occur heavy voice traffic is inevitable, unfortunately occurring at the same time as high demand for telemetry data. The combined result is overloading with lost data or voice communications. This is a serious issue in emergency situations.

In contrast dedicated SCADA radio systems may be dimensioned for the capacity needs and resourced with appropriate emergency power according to the requirements and priorities of the end user.

Practical deployment design decisions

In the design of new ‘greenfield’ systems considerable emphasis should be given to IP-based traffic [3] and management given the confluence of industrial control system (ICS) and information technology (IT) interests. The migration to IP in the ICS space is not solely related to the benefits of IP as regulatory pressure and government cyber security concerns now mandate security not possible with the use of serial technologies. In the past infrastructure roll-outs have considered communications only after selection of critical control equipment and then a supporting ICS network was designed.

Moving to IP allows installation of network connectivity first, with the knowledge that later equipment choices can be supported on the IP ICS platform. However, the need for serial device connectivity cannot always be avoided so the radio system should provide a means to mix legacy serial and modern IP SCADA elements in one unified network. The ability to connect serial devices via IP is now common; using a form of terminal server capability to enable transport over IP infrastructure and connection via IP to ICS network servers or workstations with virtual serial port driver software.

The IP ICS enhancements also allow advanced IP capabilities such as routing, VLANs, and device traffic management to be implemented. In complex or busy networks partitioning offers many advantages. Features such as QoS and VLAN [4], combined with the option of isolating Ethernet ports by function, delivers capacity and security benefits [5] through the separation of ICS data from system management.

Coverage of radio systems is constrained by technical radio parameters such as output power and receiver sensitivity as well as topographic features such as hills, mountains, trees, foliage, and other path obstructions including buildings. Real world performance will be determined by many factors including location, number of remote stations, and the traffic profile across the network. Correctly engineering coverage and capacity is a specialist task and a capable radio engineering oriented system integrator is required. Modern path planning tools allow clear modelling and demonstration of coverage designs. End users should participate in the review of coverage predictions and discussion of any necessary design trade-offs.

Security considerations for remotely connected assets

Cyber security is a key issue today and rarely out of the headlines. While most public focus relates to the Internet, SCADA engineers and security experts know that cyber terrorism concerns go beyond the wired Internet to other mediums, such as wireless. Real threats exist from disgruntled ex-employees, those who 'hack for fun', radical protest groups, and state sponsored entities who make deliberate attacks against information systems affecting real world infrastructure, property, and ultimately lives.

As we know from history, radio based networks by their nature offer a convenient vector for hacking but this need not be a concern if proper security protection mechanisms are implemented. Enterprise owned SCADA radio networks can be made more secure and operate with higher availability than systems that rely on telco infrastructure, including cellular based systems.

With increasing concerns worldwide and high profile incidents, such Stuxnet and Aurora, utilities and energy companies must consider and plan for the emerging security regulatory environment increasingly being mandated by governments. Cyber Security Executive Order 13636 demands a common approach to reducing the risk critical infrastructure and the components of the various national strategies to fulfil this order are relevant to this industry.

SCADA radio security considerations

A comprehensive security evaluation is the first step in working towards SCADA ICS network protection. This evaluation should include fundamentals, threat analysis, management, and best practice:

- Fundamentals: integrity, availability, confidentiality, and non-repudiation
- Threat analysis and attack vectors
- Management interfaces and protocols
- Industry security standards and government best practice recommendations

Fundamentals

A reliable network must be designed around maintaining integrity and availability. Integrity aims to prevent the accidental or malicious modification of SCADA information transiting the network. The SCADA communications network must ensure that control messages received by remote assets are the same messages that were originally sent by the SCADA master. A sectionalizer 'open' message that changes to a 'close' message may have catastrophic consequences. The network availability is also critical, a lost sectionalizer message also has consequences.

In good RF hardware design the use of forward error correction (FEC) and redundancy check (CRC) mechanisms help address these goals. When used in combination with proper coverage planning they eliminate the effect of interference and other potentially negative propagation effects.

A secure network must be designed around maintaining confidentiality and non-repudiation. Confidentiality prevents unauthorised access to data, implemented using encryption to reduce the leakage of information to potential attackers. Robust and recognised cryptographic algorithms should be used such as triple DES or ideally the newer AES [6]. Encryption on its own is not a security panacea as even encrypted messages can be replayed by the attacker once the consequences of the control message, established by some means of observation, are known.

Of course using a strong cryptographic algorithm is of little use if the keys are not managed correctly. It is prudent to implement periodic key changes initiated by a suitably vetted company security officer responsible not only for the keying material but for the frequency and timing of key changes. In advanced systems, keying material for sessions is distributed electronically by means of a recognised Over the Air Rekeying (OTAR) mechanism [7].

Non-repudiation goes the necessary step further by establishing the authenticity of data so that valid commands are not refuted and invalid commands are ignored, preventing replay and man-in-the-middle attacks. Authentication is a degree of sophistication still not common in SCADA equipment designs. An effective means of user data authentication is the cipher block chaining message authentication code (CBC-MAC) technique specified by NIST [8] and described in RFC3610 [9].

Attack vectors

The military phrase '360 degree perimeter' is used to describe the establishment of an outwards facing defence around a secured objective. This terminology can be used to describe the consideration and protection of the risks surfaces or interfaces of an individual SCADA radio product. Each interface such as serial, Ethernet, USB, and over-the-air RF must be considered for weakness, from both user data and management perspectives. For example it is now common for USB interfaces to be used in conjunction with portable solid state memory devices to upload new firmware into products. To prevent maliciously altered software from being introduced into radios, the hardware should be programmed to recognize and load only firmware files present on a USB memory stick that have been signed or encrypted with the system key.

The 360 degree concept can be extended to consider management interfaces (further addressed below) and advanced new concepts, such as the incorporation of distributed micro-firewall [10] at each Ethernet interface, the UK Centre for the Protection of National Infrastructure (CPNI) was an early advocate of this approach [11]. Such micro-firewalls at least control the use of ICMP (and other daemons), telnet, and FTP protocols. The use of government standards wherever possible should be an important part of establishing SCADA industry best practice.

Physical cyber asset security

With SCADA assets often mounted outside otherwise protected buildings, the 360 degree review needs to be extended to consider a perimeter defence around the SCADA radio and the other telemetry components. With the industry standard use of NEMA enclosures at remote sites, reliable detection of surreptitious entry is arguably more important than keeping intruders out. Such enclosures should have dual means of intrusion detection, perhaps magnetic reed and micro switch types, interfaced to the radio alarm inputs. Tamper evident seals should be affixed to cyber assets. An attack once known can be dealt with by good cyber incident response procedures [12]. It is the unrecognised attacks that are often most damaging [13].

Management security

One advantage of modern IP based systems is ease of management through industry standard means, such as the secure version of the simple network management protocol SNMPv3 [14] and web-style browsing. These require access control list with multiple authorisation levels to restrict access to parameters to reduce the potential of inadvertent or malicious tampering, such as disabling encryption or authentication. User authentication should be incorporated with session cookies that expire when the browser is closed. Automatic logout should be mandated so that if a user fails to end their management session it will be terminated after a pre-determined time. Support for improved radio-to-browser security (HTTPS TLS 1.2 with AES) with faster and more modern Elliptic Curve cryptography (ECC ECDHE_ECDSA key exchange mechanisms [15]) should now be included for reasons of security and performance [16].

Other security precautions such as data / management IP port segregation (only possible on devices with multiple Ethernet physical interfaces) should be considered.

Standards and recommendations

For a full appreciation of the range of security threats and solutions, SCADA radio system implementers should review security recommendations for industrial control systems published by multiple standards bodies in addition to industry-specific and state or federal regulations.

The unique security implications of communications with cyber assets located outside the traditionally defined electronic security perimeter (ESP) can be addressed by reference to existing and developing critical infrastructure protection (CIP) standards which provide both guidelines and challenges for the secure connection of remote assets by radio.

The North American Electric Reliability Corporation (NERC), responsible for the reliability of US power grids, has established the 'Cyber Security Standards' for critical infrastructure protection (CIP-002 through CIP-009) currently being updated to CIP Version 5 standard that provides an essential security framework reference [17].

The UK government CPNI, formally the National Infrastructure Security Coordination Centre (NISCC), also publish a wide range of references including the excellent previously referenced good practice firewall guide.

Other useful standards include:

- IEC/TS 62351 (TC57) 'Power System Control and Associated Communications – Data and Communication Security'
- IEC/TR 62443 (TC65) 'Industrial Communications Networks – Network and System Security'
- IEEE P1711/P1689/P1685 for consideration of serial communications cryptographic retrofits
- NIST IR-762823 DRAFT 'Smart Grid Cyber Security Strategy and Requirements'

Summary

Just a decade ago SCADA devices were slow, serial based, and without remote management. There was little interest in SCADA security. In the 21st century the world has changed as IP displaces serial, the need for speed growing to accommodate new protocols and management, and through the necessity for effective security measures. While some SCADA radios have reached the speeds necessary for widespread private narrowband IP SCADA and offer encryption, few have the necessary features such as authentication, firmware encryption, management safeguards, and the other components needed to fully address cyber security issues. The selection of future-proof designs for SCADA network components incorporating security measures is needed to provide protection from threats and reduce compliance costs as government infrastructure security recommendations turn into regulations.

References

1 Recommendations of the Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks, Order, EB Docket No. 06-119, WC Docket No. 06-63
2 TETRA+ Critical Communications Association 'TETRA versus DMR', October 2012
3 Kwok-Hong Mak, 'Migrating electrical power network SCADA systems to TCP/IP and Ethernet networking', Power Engineering Journal Volume 16, Issue 6, December 2002
4 ABB Switzerland Ltd 'SCADA over IP-based LAN-WAN connections', March 2011
5 NSA Systems & Network Analysis Centre 'Securing Supervisory Control and Data Acquisition (SCADA) and Control Systems (CS)'
6 NIST FIPS PUB 197 Advanced Encryption Standard (AES)
7 RFC 3394 Advanced Encryption Standard (AES) Key Wrap Algorithm
8 NIST publication SP 800-38C 'Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality'
9 RFC3610 Counter with CBC-MAC (CCM)
10 Muralidaran Gangadharan, Kai Hwang, 'Intranet Security with Micro-Firewalls and Mobile Agents for Proactive Intrusion Response', Proceedings of the 2001 International Conference on Computer Networks and Mobile Computing, p.325, October 16-19 2001
11 CPNI Firewall Deployment for SCADA and Process Control Networks Good Practice Guide'
12 NERC CIP-008 Incident Reporting and Response Planning
13 FIPS 140-2: Security Requirements for Cryptographic Modules
14 RFC 3410 'Introduction and Applicability Statements for Internet Standard Management Framework'
15 NSA Suite B and NIST SP 800-56A
16 NSA 'The Case for Elliptic Curve Cryptography'
17 NERC CIP Version 5 Reliability Standards 'Project 2014-02 Critical Infrastructure Protection Standards Version 5 Revisions'