SECURITY CONSIDERATIONS FOR WATER SUPERVISORY, CONTROL, AND DATA ACQUISITION RADIO

John Yaldwyn (4RF Limited, Wellington)

ABSTRACT

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 media, such as the wireless radio-based systems used for utility communications.

Private narrowband supervisory, control and data acquisition (SCADA) radio is an effective and economic industrial machine to machine (M2M) communications tool with a proven heritage. Water utility owned private radio networks provide an alternative to more complex third-party public cellular systems and usually offer better availability in the rural and remote terrain in which water catchment areas are usually located. The bandwidth required for monitoring and control technologies have escalated, particularly through the adoption of new IP based SCADA protocols such as Worldwide Industrial Telemetry Standards (WITS-DNP3 and WITS-IOT), the demand for better security, and the penetration of information technology (IT) network oversight into all levels of operational technology (OT) telemetry and control networks. These drivers have led to the development of IP capable long range field area network radio systems.

While security of supply is a top priority for water utilities, communication security often does not receive the attention it deserves. Deploying a radio-based network requires close attention to security, both the encryption used to protect over the air transmission itself and the authentication used to control network access by devices and users.

In the UK, Northern Ireland Water has deployed WITS-DNP3 for telemetry monitoring and control of approximately 4,500 clean and wastewater assets.

The company serves 1.8 million people, each day providing 570 million litres of potable water and treating 340 million litres of wastewater. It is responsible for 26,800 km of watermains and 15,800 km of sewerage pipes, as well as 23 water treatment plants and 1,030 wastewater treatment works. Telemetry device are connected via RS-232 serial, a combination of Proteus protocol outstations at 2400 bps and Talus T4e WITS-DNP3 outstations at 9600 bps.

Here in New Zealand, Wellington Water serves the 400,000 residents of the Wellington region with 49 million litres of drinking water each year. The company is also responsible for waster and storm water management with 6,900 km of pipelines and 138,000 connections.

The chaotic topography of Wellington's terrain makes setting up a radio network challenging due to line of sight issues. Telemetry equipment consist of Abbey System Swampfox RTU connected with Ethernet.

In these two systems a field area network (FAN) implements an IP backbone network to link pumps, valves, level sensors and flow meters to a central Regional Telemetry System using UHF radios designed in New Zealand by 4RF. As with most water systems, telemetry not only supports alarm annunciation, operational monitoring and control, as well as capturing data for historical operational and regulatory purposes. This paper will review security options for threats that exist from disgruntled ex-employees, those who hack for fun, terrorist, and state sponsored actors who make deliberate attacks against information systems controlling real world infrastructure such as water.

KEYWORDS

Water, IP, cyber security, FAN, radio, SCADA, WITS protocol

PRESENTER PROFILE

John Yaldwyn is CTO and founder of 4RF, with a focus on RF system level design and cybersecurity. He is a member of the Victoria University Engineering Faculty Advisory Board.

1 INTRODUCTION

Private SCADA radio systems, sometimes called multiple address systems (MAS) and more recently field area network (FAN), operate in the VHF and UHF licensed radio spectrum. Access to this spectrum is controlled in New Zealand by the Radio Spectrum Management (RSM) business unit of Ministry of Business, Innovation and Employment (MBIE). These systems are a popular and effective means for data collection and remote control over distances ranging up to 100 km, with distances of 10 to 50 km being typical. In response to pressure for 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 the usually available RSM 12.5 kHz bandwidth channels, with even higher rates possible certain bands where high bandwidths are available. In addition to speed, users contemplating migration to these new radio devices benefit from a range of new operational enhancements including IP support and SNMP management.

It might seem that alternative wireless technologies such as cellular could 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 with utilities. This is more than institutional engineering bias; it is the result of simple economics. Cellular companies are not in the business of considering the priorities of a few tens of thousands of critical infrastructure points ahead of millions of consumers and cellular mobile networks are not designed to operate under extended power outages. The attempt by the U.S. Federal Communications Commission (2007) to mandate a minimum of 24 hours of cellular resilience as a result of reviewing the impact of the Hurricane Katrina in 2005 on communications infrastructure failed after cellular industry objections and was cut to 8 hours. In New Zealand, resilience is entirely up to the operators. While the New Zealand Government National Infrastructure Unit (2014) noted that mobile services were operating within 24 hours of the Christchurch 2011 earthquake, a more detailed engineering review of resilience (Giovinazzi et al., 2017) highlighted a number of infrastructure shortcomings affecting mobile services following the 2016 Kaikōura earthquake.

Systems based on land mobile infrastructure have also been used for private SCADA communications. Modern digital LMR systems such as DMR and Tetra (TCCA 2013) 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 major 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 interrupted voice communications both serious issues in emergency situations.

In contrast to repurposed cellular or mobile radio infrastructure, dedicated SCADA radio systems may be dimensioned for capacity needs and resourced with appropriate emergency electrical power according to the requirements and priorities of the end user.

Abbey (2015) discussed many of these issues in the context of mission-critical processes such as water supply and sewage disposal. Included were some specific observations on cellular and Christchurch 2011 earthquake. However, one of the most critical resilience issue not discussed was that related to cyber security, perhaps indicative of the reduced threat climate at that time.

2 PRACTICAL DEPLOYMENT CONTEXT

Before discussing cyber security in detail, it is important to further understand the context. In the design of new systems considerable emphasis is usually placed on IP traffic and management, given the confluence of industrial control system (ICS) and IT interests. In the past, infrastructure roll-outs have considered communications only after selection of critical control equipment and then a supporting ICS network designed. Moving to IP allows the design of FAN connectivity to proceed early, with the knowledge that later equipment choices can be supported on the FAN IP platform within the capacity limits. The need for serial device connectivity cannot always be escaped so a radio-based FAN system should also 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.

Initially IP networks have been charged simply with the task of carrying traditional serial protocols in a suitable form of IP encapsulation ranging from simple character strings carried in UDP packets to more complex protocols that include handshake line encoding as described by Clark (1997). More recently water industry specific IP protocol standardization efforts have occurred, as described by Bartingdale (2007) with real world deployments in major water utilities such as at Northern Ireland Water, see Bradley (2015).

Advances in management technology allows the network connectivity components switches, routers, and radios to be monitored along with the industrial control end devices. The involvement of IT often drives the need to provide for this new management functionality but care is needed to maintain the recommended OT/IT management system isolation and to respect the differing responsibility domains.

3 SECURITY CONSIDERATIONS FOR REMOTELY CONNECTED ASSETS

Having introduced resilience concerns and the migration to IP in the ICS space it is necessary to address cyber concerns not traditionally considered with legacy serial SCADA technology. Threats exist from disgruntled ex-employees, those who hack for fun, radical protest groups, and state sponsored actors who make deliberate attacks against information systems affecting real world infrastructure, property, and ultimately society. The water industry should be under no illusion that the critical infrastructure under its control is not attracting unwanted attention. In a particularly interesting article (Mahairas & Beshar 2018) the FBI discussed recent attacks and vulnerabilities specific to the water industry.

As we know from history dating back to World War II, radio based networks by their nature offer a convenient vector for interception but this need not be a major concern if proper security protection mechanisms are implemented. With suitable care in design water industry owned SCADA radio networks can be made secure and operate with higher availability than systems that rely on public carrier infrastructure, including cellular based systems.

A comprehensive security evaluation is the first step in working towards SCADA ICS network protection. This evaluation should include the security fundamentals of integrity, availability, confidentiality, and non-repudiation, as well as threat analysis, management protocols, and best practice recommendations.

4 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 or control room. A water pump start message that is changed in transmission to a stop message may have catastrophic consequences. The network availability is also critical, lost pump messages also have consequences.

In good radio system 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, ideally the AES (NIST 2001) method. Encryption on its own is not a security panacea as even encrypted messages can be replayed by an attacker once the consequences of the control message, established by some means of observation, are known.

Water supply and wastewater infrastructure is characterized by large pumps and easily observable physical assets such as storage facilities and weir gates so correlation with data transmission is readily achievable.

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 such as that proposed by Schaad and Housley (2002) based on previous work by the NSA and NIST.

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 (2007) and described by Whiting et al. (2003).

5 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 risk surfaces or interfaces of an individual SCADA product or ICS system. Each interface such as serial, Ethernet, USB, and over-the-air RF path 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 devices, 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-firewalls, a concept proposed by Gangadharan and Hwang (2001), at each IP interface. The UK Centre for the Protection of National Infrastructure (CPNI) was an early advocate of this approach. Such micro-firewalls control the use of unwanted traffic such as daemons, telnet, and similar protocols. Wherever possible the use of government standards should be an important part of establishing SCADA industry best practice.

6 PHYSICAL CYBER ASSET SECURITY

With SCADA assets often mounted outdoors, the 360 degree review needs to be extended to consider a perimeter defence around the SCADA radio and the other telemetry components. With the typical industry use of control enclosures at remote sites, reliable detection of surreptitious entry is as important as keeping intruders out. Such enclosures should have dual means of intrusion detection, interfaced to the radio system alarm inputs. Tamper evident seals should be affixed to remotely located cyber assets.

An attack once known can be dealt with by good cyber incident response procedures NERC (2014). It can often be the unrecognized cyber intrusions that are often most damaging as these allow the long term observation and of the victim ICS and attack calibration.

7 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 (Case et al. 2002) and web-style browsing. These require access controls such as password-based authorisation to restrict access to parameters to reduce the potential of inadvertent or malicious tampering.

User authentication is best managed centrally, where local logon credentials are referred to a central authorization server. There are few reason not to embrace full authorization, authentication, and accounting (AAA) best practices managed in part by the IT specialists. Where browser-based methods are supported, session cookies must be expired when the browser is closed and 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. Browser security is critical but unfortunately embedded web servers in SCADA equipment are often quite primitive, vulnerable, and outside the of routine IT security audits. Good browser security (HTTPS TLS 1.2 with AES) and modern cryptography key exchange mechanisms (such as elliptic curves) should be enforced for reasons of security and performance.

The IP FAN enhancements now available allow advanced IP capabilities such as routing, VLANs, and device traffic management to be implemented with the advantage of partitioning in complex or busy networks to isolate different types of traffic. Using features such as QoS and VLAN as recommended by ABB (2011) combined with the option of isolating Ethernet ports by function enables capacity and security benefits through the separation of OT ICS data from other IT and management systems as recommended by the UK and US governments communication security agencies, CPNI (2005) and NSA (undated).

8 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 government recommendations and advice.

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 U.S. 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, publish the well-established NERC CIP V5 Implementation Information cyber security standards for critical infrastructure protection, these provide a very useful and accessible security framework reference.

Other useful tutorial 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'

9 CONCLUSIONS

Just a decade ago SCADA devices were slow, serial based, without remote management, and there was little interest in SCADA security. In the 21st century the world has changed as IP displaces serial, capacity requirements are growing to accommodate new protocols and management, and the necessity for effective security measures is now critical. While some SCADA radio systems have reached the speeds necessary to support widespread deployment of IP and offer encryption, like many other SCADA remote ICS assets, few have the necessary security features, management safeguards, and the other components discussed here that are needed to fully address cyber security issues. The careful selection of SCADA network and other ICS components incorporating the range of security measures described here is needed along with a considered security design to provide protection from cyber threats.

ACKNOWLEDGEMENTS

The author wishes to note the passing of Lester Abbey in 2016, a sad loss to the New Zealand SCADA industry.

REFERENCES

ABB Switzerland Ltd (2011) *SCADA over IP-based LAN-WAN connections.* https://library.e.abb.com/public/4d9098ca528fd57fc1257b0c005525c3/802.pdf

Abbey, L. (2015) *'Resilience in Water and Wastewater Telemetry and Control Systems'* Water New Zealand Annual Conference, September 2015. https://www.waternz.org.nz/Attachment?Action=Download&Attachment_id=359

Bartingdale, B. (2007) *'WITS The Revolution Begins…'* IET Water Event, April 2007.

Bradley, P. (2015) *'Northern Ireland Water Telemetry Outstation Project'* IET Water: Process Control and Automation. Engineering for the Water Industry, May 2015.

Case, J., Mundy, R., Partain, D., and Stewart, B. (2002) '*Introduction and Applicability Statements for Internet Standard Management Framework',* IETF RFC 3410, December 2002.

Centre for the Protection of National Infrastructure (CPNI) (2005) *Firewall Deployment for SCADA and Process Control Networks: Good Practice Guide*, February 2005. http://energy.gov/sites/prod/files/Good%20Practices%20Guide%20for%20Firewall%20Deployment.pdf

Clark, G. (1997) *'Telnet Com Port Control Option'*, IETF RFC 2217, October 1997.

Gangadharan M. and Hwang K. (2001) *'Intranet Security with Micro-Firewalls and Mobile Agents for Proactive Intrusion Response'*, Proceedings of the 2001 International Conference on Computer Networks and Mobile Computing, October 2001.

Giovinazzi, S., Austin, A., Ruiter, R., Foster, C., Nayyerloo, M., Nirmal-Kumar, N., and Liam Wotherspoon, L. (2017) *'Resilience and Fragility of the Telecommunications Network to Seismic Event: Evidence after the Kaikōura (New Zealand) Earthquake'* Bulletin of the New Zealand Society for Earthquake Engineering, Vol. 50, No. 2, June 2017.

Mahairas, A. and Beshar, P. J. (2018) *'A Perfect Target for Cybercriminals America's water supply is increasingly digitized, and increasingly vulnerable'* The New York Times, November 19, 2018.

New Zealand Government National Infrastructure Unit (2014) *Infrastructure Evidence Base Telecommunications Sector*.
https://treasury.govt.nz/sites/default/files/2017-12/nip-evidence-telecommunications.pdf

Schaad, J. and Housley, R. (2002) 'Advanced Encryption Standard (AES) Key Wrap Algorithm', IETF RFC 3394, September 2002.

TETRA + Critical Communications Association (TCCA) (2013) *TETRA versus DMR*, December 2013.

https://www.pc5e.nl/downloads/pd785/dmr/TETRAversusDMRsmeDec2013v1.pdf

U.S. Federal Communications Commission (2007) 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.
https://docs.fcc.gov/public/attachments/FCC-07-177A1.pdf

U.S. National Institute of Standards and Technology (NIST) (2001) *Federal Information Processing Standards Publication 197* Announcing the ADVANCED ENCRYPTION STANDARD (AES), November 26, 2001.

U.S. National Institute of Standards and Technology (NIST) (2007) *Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality*, NIST publication SP 800-38C, Updated July 2007 superseding May 2004.

U.S. North American Electric Reliability Corporation (NERC) *CIP V5 Implementation Information*
https://www.nerc.com/pa/CI/Pages/Transition-Program.aspx

U.S. North American Electric Reliability Corporation (NERC) (2014) *Cyber Security — Incident Reporting and Response Planning Incident Reporting and Response Planning* NERC CIP-008, revised July 2014.

U.S. National Security Agency Systems & Network Analysis Centre () *Securing Supervisory Control and Data Acquisition (SCADA) and Control Systems (CS)*.
https://www.nsa.gov/ia/_files/factsheets/scada_factsheet.pdf

Whiting, D., Housley, R., and Ferguson, N. (2003) *Counter with CBC-MAC (CCM),* IETF RFC 3610, September 2003.