Modern Applied Science; Vol. 11, No. 6; 2017
ISSN 1913-1844 E-ISSN 1913-1852
Published by Canadian Center of Science and Education

Wastewater Automation – The Development of a Low Cost, Distributed Automation System

Tom Davies[1] & Stanislaw Paul Maj[2]

[1] Shire of Moora, Western Australia

[2] Engineering Institute of Technology, Western Australia

Correspondence: Stanislaw Paul Maj, Associate Dean (Research), Engineering Institute of Technology, 1031 Wellington St., West Perth, Western Australia, 6005. Tel: 1300-138-522. E-mail: davieslanguage@yahoo.com, Sewerage@moora.wa.gov.au, paulm@eit.edu.au

Received: March 25, 2017 Accepted: April 8, 2017 Online Published: April 23, 2017

doi:10.5539/mas.v11n6p41 URL: https://doi.org/10.5539/mas.v11n6p41

The research is supported by Shire of Moora.

Abstract

In developed countries wastewater management is considered a vital aspect of community health and wellbeing. Failures in wastewater management may result in the release of pathogens into natural water bodies and in extreme circumstances into drinking water. Illnesses caused by contamination range from gastroenteritis and viral infections to death. As such in Australia it is a highly regulated industry accountable to a range of state authorized bodies such as Department of Environment Regulations (DER) and Department of Health (DoH) . The Shire of Moora was made responsible for their wastewater system in 2013. An analysis of this system found that the SCADA system conveyed fault location but no alarm status information. It should be noted that alarm status is needed in order to determine required responses. In order to address this problem a range of different potential solutions were evaluated according to a wide range of ranked factors such as cost, security, features etc. This resulted in the design and implementation of a low cost, distributed wireless solution based on the IEEE 802.15.4 standard. The authors believe this is the first implementation of this system in a rural/regional environment.

Keywords: wastewater management, automation, distributed automation

1. Introduction

1.1 Waste Water Treatment

The Australian rural Shire of Moora wastewater system serves a population of circa 1,500 people and over 100 commercial/industrial organizations. It consists of 17km of piping, 5 lagoons and 7 catchment areas each with a pump station. Wastewater in each catchment area is collected by gravity feed. Seven catchment areas pump the wastewater to a single collection point in the 1st catchment area from which it is pumped to the Wastewater Treatment Plant (WWTP). The WWTP consists of four treatment lagoons and a single reuse lagoon with a gas chlorine disinfection system. Treated waste water is then used to irrigate parks and sports fields. Wastewater, prior to treatment, represents a significant potential risk to the public (DoH, 2017). Dangers include pathogens that cause skin and eye infections, gastroenteritis and hepatitis (DoH, 2017). Hence chlorination levels must be strictly adhered to and treated water sampled on a regular basis for the presence of pathogens such as E.coli. Given the potential dangers to the public, within Australia wastewater treatment is a highly regulated industry and must report to four government bodies: Economic Regulatory Authority (ERA) (ERA, 2017), Department of Water (DoW) (DoW, 2017), Department of Health (DoH) (DoH, 2017) and the Department of Environment Regulations (DER) (DER, 2017). In order to operate, a WWTP must have appropriate licenses from each of these authorities. These regulatory bodies can and do prosecute compliance failures (DER, 2017; DoH, 2017; DoW, 2017). The Australian Water Corporation handed responsibility of the wastewater scheme to the Shire of Moora in 2013. The inherited control system consisted of a pre-2000 Supervisory Control and Data Acquisition (SCADA) system based on a switchboard and Programmable Logic Control (PLC) based pump control with dial alarms utilizing landline connectivity. Each pump station has three alarm conditions namely: high level, power

out and pump fail. Analysis of the inherited system found scope for significant improvements. Problems identified included:

- Alarm system provided alarm but with no identification of reason for alarm
- System trending not available
- Limited ability to configure current system

2. Method

2.1 Design Method

There were three aspects to the design method. Firstly system requirements; secondly potential technical solutions and thirdly vendor packaged solutions. The priorities for this project were high reliability with low cost. The proposed system, whilst it must be reliable, does not need a high bit rate, neither are the applications time critical. It was also a requirement that any installation could be completed by non-specialized staff thereby minimizing costs. It is recognized that technologies are constantly evolving and hence an analysis was conducted of communication systems and standards such as IEEE 802.15.4 Internet of Things (TI, 2017), Modbus etc. to determine what, if any, new technologies would be relevant. Industrial automation has a range of vendors offering a wide range of different technical solutions each with their associate costs, advantages and disadvantages.

Table 1. Ranked design factors

Factors	Rank	Scale 1-10	Meaning
Reliable & reputable	1	10	great track record and reputation.
		5	Average track record and reputation
		1	no known information.
Cost -	2	10	within budget for the complete product e.g. $25,000
		5	Over budget 50%
		1	completely inappropriate price range e.g. $100,000
Staff setup difficulty	3	10	external engineer / specialized contractor required
		5	Complex installation
		1	simple setup by untrained staff
Local supplier	4	10	WA based company / agent
		5	Australian / NZ company / agent
		1	Overseas company / agent
GUI suitability	5	10	Clear GUI displaying desired trends with history and logging
		5	Basic symbols
		1	Just numbers / raw data
Features	6	10	Many features to select from
		5	Some features
		1	No extra features
Support	7	10	Easy, free information and help
		5	Cumbersome, paid support
		1	No support
Security	8	10	Many high quality security features
		5	Option of some security features
		1	Limited or no security
Operating & servicing costs	9	10	Cost free connectivity and minimal servicing
		5	Some paid components
		1	Paid connection at every site and expensive servicing

A literature search was conducted of solutions employed by WWTPs having the most similar environment to the Shire of Moora. A literature search and research led to the selection of nine possible solutions. The possible solutions were analyzed by means of measuring nine key qualities each on a scale of one to ten. These qualities

were deemed the most important by the organization so the comparison could be made quantitatively. In order to arrive at an objective, quantifiably decision factors were identified and ranked. For each factor a scale was defined (table 1). Using table 1 (ranked design factors) a quantitative analysis of nine different potential solutions was evaluated (table 2). The highest ranking solution was the ZigBee Mesh network. Significantly security was identified as a factor that was not identified in the initial analysis (Melgares, 2011).

Table 2. Ranked system evaluations

Score out of 90	Company A (KAPP, 2017)	Rockwell solution Company B Internet of Things (TI, 2017)	Company C ZigBee (NHP, 2011)	Company D Schneider (Schneider, 2007)	Company E Oleumtech (Munday, 2015)	Company E ZigBee + 3G (Munday, 2015)	Company E ZigBee RTU (Munday, 2015)	Company F Burket (Burkert, 2017)	Company G Flexy (Ewon, 2017)
Reliable & reputable	10	4	8	10	8	8	5	8	6
Cost	3	10	10	2	7	8	9	8	7
Staff setup difficulty	5	7	9	6	6	6	6	8	7
Local supplier	10	10	10	10	9	9	5	8	8
GUI suitability	10	6	9	10	7	6	6	6	6
Features	10	6	8	10	8	7	5	6	6
Support	10	8	10	10	7	6	4	6	5
Security	9	4	6	10	8	6	4	6	6
Operating & servicing costs	3	7	8	4	7	5	8	8	6
Total	70	62	78	72	67	61	52	64	57
Rank	3	6	1	2	4	7	9	5	8

2.2 Security Analysis

The IEEE 802.15.4 standard does have encryption inbuilt. According to the 802.15.4 standard, “A device may optionally implement security” (IEEE Standard 802.15.4., 2011). This is done by setting the attribute macSecurityEnabled.. The proposed solution is based on a low bandwidth, read-only protocol which represents an intrinsically low security risk. However given the system is concerned with public health and the associated need for regulatory compliance a detailed security risk analysis (OWASP, 2017) was conducted in which potential threats were identified and their likelihood and impact defined as either low medium or high – both of these factors defining the severity (table 3). From table 3 three potential threats were identified to have medium severity, namely: selective jamming; alarm masking and false alarms. One of the the most likely attack is a selective jamming attack which requires motive and only some technical knowledge. The consequence is a block of information which could potentially mask an alarm. The jamming action would be observable by the monitoring system – once the jamming characteristics are measured, an alarm can be configured to be triggered when jamming occurs. In this way, the impact will be minimised.

Table 3. Security analysis

Attack	**Likelihood**	**Impact**	**Severity**
Creating false alarms	Low	High	MEDIUM
Corrupting data	Low	Medium	LOW
Giving false readings	Low	Medium	LOW
Masking real alarms	Low	High	MEDIUM
Creating a profile for future attacks	Low	Medium	LOW
Attempting exploitation by use of gathered data	Low	Low	LOW
Jamming the airwaves by transmitting on the same frequency	Medium	Low	LOW
Selective jamming of the airwaves by transmitting on the same frequency at specific times	Medium	Medium	MEDIUM

A change of frequency (which may prove difficult) or an effort to apprehend the offender by use of frequency monitors and loggers may be a possible treatment. The other two attacks (false alarm and masking) require motive and technical expertise – and considerable research / inside information. Hence the most likely source of this type of attack may be a disgruntled employee. The consequence could be false alarms requiring staff callouts or an attempt of completely masking an alarm which could, in the worst case scenario, result in a sewage overflow. This hazard could be mitigated by having staff physically do inspections at least twice per week. As it would take about 4-5 days for the system to go from alarm state (extra high level) to an overflow, it would require a combination of staff negligence and effective hacking for this to occur. Even in this scenario, stopped sewerage services prior to an overflow would undoubtedly result in customers phoning in and complaining that their drains aren't flowing. To mitigate these potential scenarios encryption can be enabled in the ZigBee protocol by checking a security flag (IEEE Standard 802.15.4., 2011). Once hacking is suspected, security measures can be put into place such as encryption and changing of node IDs and resetting register address locations. This means that the hacker would have to start their research all over again. The regime of changing addresses may be a good security practise to adopt akin to changing passwords.

2.3Wireless Network

The wireless mesh network encompassing the Shire of Moora and wastewater scheme equipment was designed based on the 802.15.4 phase-shift-key. This has the ability to be restored even in low signal to interference environments (IEEE STD 802.15.4., 2006). The ZigBee standard employs several frequencies and they have been designed for minimal interference with other well-known networks such as WIFI (table 4) (IEEE Standard 802.15.4., 2011). The 900MHz frequency has the range and bandwidth to meet system requirements and hence selected and tested.

Table 4. IEEE 802.15.4 frequency characteristics (Conlab, 2017)

Frequency	Range urban	Range outdoors	Tx power	Data rate	Rx Sensitivity
2.4GHz	100m	2km	63mW	256Kbps	– 102dBm
900MHz	600m	14km	250mW	10K / 200Kbps	– 101dBm / – 110dBm
868MHz	600m	14km	250mW	10K / 200Kbps	– 101dBm / – 110dBm

A signal strength survey was carried out using a Zigsense Range Tester (ZigSense, 2010). The device was designed to help conduct an RF site survey in order to optimise wireless communications paths of identify problem locations. The test was carried out using 900MHz frequency and at 250mW transmission power. Two units communicate with each other across a site a give a signal strength output. The outputs were interpreted by the manufacturer as shown in table 5. To address the problem of weak signals a higher powered dome antenna (50w) was selected.

Table 5. Range Tester output tests for Site

Between Central Station and:	Reading	Interpretation
Pump Station 1	-82 dBm	Slightly weak
Pump Station 2	-82 dBm	Slightly weak
Pump Station 3	-62 dBm	Good
Pump Station 4	-73 dBm	OK
Pump Station 5	-85 dBm	Weak
Pump Station 6	-85 dBm	Weak
Pump Station 7	-95 dBm	Too Low

3. Results

3.1 Initial Trials

A prototype was installed arbitrarily at pump station 3 consisting of: Two Remote End Units; one antenna; one current transformer and one Level transducer. The remote prototype was wirelessly connected to a Central station with a network controller; gateway and antenna. The trial was for 3 months with the following results:

Communications: no down time. A power loss was experienced triggering the ZigBee module to operate using its backup battery. The system was therefore configured to send an alarm during power loss.

Alarm Monitoring: the alarm system was based on configurable SMS messaging with specific alarm parameters. On receiving an alarm, a staff member could remotely log on and read system parameters. The alarm system activated for all alarms.

Trending: historical data could be accessed and hence trending was possible.

Configuration: Significantly it was possible to customise alarm parameters for different pumps at different pump stations.

3.2 Trending Analysis

Once the characteristic behaviour of the pumps and water levels were determined then significant deviations could be identified. During the trials, for one pump, the current deviated outside of the acceptable range. Hence the pump was lifted and serviced to avoid potential failure. During the trial various incidents were recorded, hence it was possible to obtain an accurate understanding of all aspects of the system.

4. Discussion

The problems to be addressed were: alarm identification; provide trending and configuration. The system met all design requirements. ZigSense cloud based applications were easy to configure making effective graphical trending possible (Conlab, 2017). Scripting is an option that will be pursued to further customize the cloud app and to calculate and log further diagnostic data such as total pump operating hours and set pump current alarms according to defined algorithms. Currently, logs are downloaded (up to two months' worth) and calculations are made on the excel file. It is noted that this operation can be automated at the cloud level (Conlab, 2017). All non-technical staff were given an introduction to the new system – none experienced any problems. The current high gain omnidirectional antennas may not be the optimal solution as they were found to be slightly delicate for outdoor use – vandalism is the main concern. A sturdier dome antenna will be trialled next (Rojone, 2009). There was no significant loss of signal throughout a three month trial. One unexpected outcome is that the staff determined that after getting to know the system, only one remote end unit is required. The removal of one unit greatly simplifies installation and reduces cost. This modification also means that less parameters are required to be monitored – giving rise to a simpler and easier to monitor system.

Acknowledgments

The research is supported by Shire of Moora.

References

Conlab (2017). ZigSense - Wireless Sensing Technology. Retrieved from http://www.zigsense.com.au

Rojone (2009). A-490-18F 838 MHz Next G Antenna. R. P. Ltd, Rojone Pty Ltd. A-490-18F 838 MHz Antenna.doc 2.

ZigSense (2010). ZigBee Range Tester model ZS24-RGR-001: 2.

DER (2017). About the Department of Environment Regulation. Retrieved from http://www.der.wa.gov.au

DoH (2017). Department of Health, Government of Western Australia. Retrieved from http://ww2.health.wa.gov.au

ERA (2017). Economic Regulation Authority. Retrieved from https://www.erawa.com.au

DoW (2017). Department of Water, Government of Western Australia. Retrieved from http://www.water.wa.gov.au

DER (2017). Summary of Prosecutions. Retrieved from https://www.der.wa.gov.au/our-work/enforcement/summary-of-prosecutions.

DoH (2017). Publication of names of offenders list. Retrieved from http://ww2.health.wa.gov.au/Articles/F_I/Food-offenders/Publication-of-names-of-offenders-list

DoW (2017). Compliance and Enforcement. Retrieved from http://www.water.wa.gov.au/licensing/water-licensing/compliance-and-enforcement

TI (2017). Internet of Things. http://www.ti.com/ww/en/internet_of_things/iot-products.html

Burkert (2017). Burkert Fluid Control Systems. Retrieved from http://www.burkert.com.au

DoH (2017). Sewage Spills. Retrieved from http://healthywa.wa.gov.au/Articles/S_T/Sewage-spills

Ewon (2017). Discover Ewon. Retrieved from http://www.ewon.biz

KAPP (2017). The automation and control system specialists. Retrieved from http://www.kapp.com.au/.

Munday, P. (2015). Automation IT awarded contract to upgrade SCADA system for Unitywater Sewage Pump Stations. A. I. P. Ltd, Automation IT Pty Ltd.

NHP (2011). Solutions for the Water & Wastewater Industry. N. E. E. P. P. Ltd: 16.

Schneider (2007). Your solution for water and wastewater pumping stations. S. Electric, Schneider Electric.

OWASP (2017). OWASP Risk Rating Methodology. Retrieved 2017, from https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

IEEE Standard 802.15.4 for local and metropolitan area networks— Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) LAN/MAN Standards Committee of the IEEE Computer Society IEEE-SA Standards Board, 2011.

Adams, J. T. An Introduction to IEEE STD 802.15.4. (2006) Freescale Semiconductor. Inc.

Melgares, R. A. (2011). 802.15.4 / ZigBee Analysis and Security: Tools for Practical Exploration of the Attack Surface.