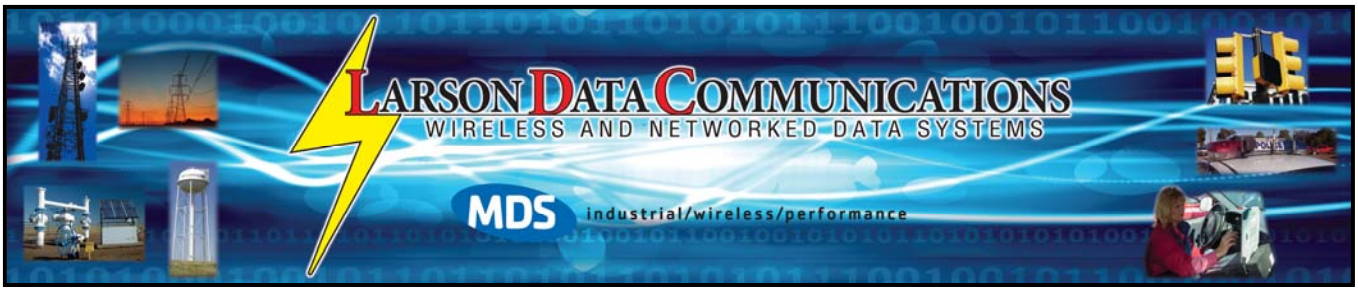

Wireless Data Communications Systems Analysis

City of Blaine Public Works – Water Department

Performed For:

City of Blaine
10801 Town Square Drive NE
Blaine, MN 55449

Analysis By:

Larson Data Communications
GE MDS Full Service Partner
for IA, MN, MT, ND, NE, SD & WY

6 July 2017

Report Summary

I. Introduction & Purpose

Larson Data Communications, Inc. was commissioned by the City of Blaine to conduct a wireless system analysis for City's Water Department and to present our findings with regard to the current condition of this system's existing SCADA radio system components; and further, our recommendations toward improving and/or upgrading this system such that it will be capable of performing as a highly reliable, easily maintainable, cost efficient wireless network capable of supporting the currently defined and future operational and functionality requirements of the City of Blaine Water Department SCADA/Controls System. The purpose of this report is to present the results of this system analysis.

II. Analysis Methodology

The analysis of the City of Blaine Water Department SCADA communications network was conducted in multiple phases:

Phase I consisted of gathering existing SCADA communications network system data such as control site location; radio configuration, antenna system, & FCC License (if/as applicable) information; as well as other available communications system information and using this data to perform a computer software based Electromagnetic Propagation Study/Path Analysis of each existing or required radio link of the City's wireless communications network(s) and the communications system as a whole.

This type of highly informative and useful computer modeling study is used to analyze the geospatial terrain profile and link characteristics of each radio signal path to evaluate the effectiveness and efficiency of an existing radio system and/or to determine the optimal antenna system selection, mounting height, polarization, and directional orientation of a new or upgraded system in addition to considering other potentially useful available communications assets and options. The results of this initial analysis is used as a system baseline against which all subsequent testing is performed, and from which all system upgrade & refinement recommendations are made. The results of the wireless portion of this preliminary "Path Study" are contained in Appendix A of this report.

The tested existing wireless system & network topology map is contained in this report and can be viewed in Section III.

Phase II of a system analysis typically involves actual on-site testing of each existing or proposed control site radio link and any other communications assets as may be available for requested consideration. In some cases, other radio links suggested by the Phase I computer model analysis are also tested as may identified as potentially desirable or preferable over existing or proposed network topologies.

With all Phase I data collection and preliminary analysis done prior to that date, Phase II on-site system evaluation & testing work was conducted during the week of July 17th- 21st, 2017.

For existing systems, work during this phase consists of establishing the current condition, degree of functionality, and level of actual performance of all SCADA radio system components at each radio equipped system control site. This process involves the conduct of an on-site visual inspection, and also Test, Measurement, and Diagnostic Equipment (TMDE) evaluation of several critical wireless system electromagnetic environment and radio product specific performance parameters.

> [Note: Typical items of TMDE used to evaluate the above parameters include Digital Multimeters, Radio Frequency Site Analyzers, Communications Service Monitors, and Frequency Spectrum & Time Domain Reflectometry Analysis devices.]

Phase II inspection & testing includes evaluation of methods of installation and condition of all GE MDS or other radio equipment and other communications networking equipment as might be required; power supplies; lightning protection devices; grounding systems & methodology; transmission line components; antennas; antenna mounting location, bracketing & orientation; and the RF electromagnetic spectrum in the frequency bands in use or being considered for use. Further, each transmission line and antenna system is tested for resonance at the system's current or proposed operating frequency. For existing systems, each site's current Receive Signal Strength Indication (RSSI) level as well as Signal-to-Noise Ratio (SNR) or Link Quality Indicator (LQI) as appropriate to the radio system is also observed & recorded.

During this phase, all on-site inspection, test and evaluation findings and results for each site are documented on "Radio System Site Evaluation Worksheets." This documentation also includes the identification of any failed or failing system components.

Following the Phase I and Phase II portions of each system analysis, actions occurring during Phase III combine and evaluate all system data collected to that point: the entire communications system as a whole, identified/defined operational requirements & future goals, computer modeled "ideal" radio link data, "actual" over-the-air radio link performance data collected in the field, and all site specific data & installation information. In this phase of the analysis, all observed and/or tested parameters are measured against and compared to the system modeling work completed for this system in Phase I. This analysis phase looks specifically at the entire radio system and link topology as a whole - toward evaluating the soundness and reliability of the existing or proposed overall data connectivity scheme as well as its throughput capacity and data transfer/network efficiency.

In the case of a proposed system, or proposed changes to an existing system, this aggregated data is used to further develop and refine the radio network topology and antenna system design prior to final network decisions and the beginning of data communications system construction. In the case of existing system or equipment analysis, this data is used to identify to the owner any failed/failing components requiring attention, toward providing a basis from which to evaluate the soundness and efficiency of the existing radio network topology and antenna system installation, and also to provide the analysis team with highly reliable radio link & site data which can be used to develop specific suggestions and recommendations as to how a particular system's performance, reliability, and supportability might be enhanced or improved.

Findings & Test Results

1. The City of Blaine Water Department SCADA system is currently hosted at Water Treatment Plant #1 and is communicating to water distribution and wastewater collection control system sites via (1) link of fiber optic cable and (2) independent wireless networks.

Water Treatment Plant #1 is connected to Tower #1 via a City owned fiber optic cable. With the SCADA Master data communications connectivity thus extended to Tower #1, both antenna systems of the (2) independent wireless networks supporting the Water Department's control system are hosted by this structure. The topologies of the City's (2) wireless networks are shown graphically on "Network Overview Maps" included in Section IV of this report.

2. One of the (2) independent wireless networks, over which some Water Department control system communications are being carried, is a City IT Department managed Motorola "Canopy" unlicensed 5.8 GHz license free radio system. As the City Utilities staff expressed their particular desire to discontinue use of this system, the condition and current performance parameters of this system were not tested or otherwise evaluated.

The City also notes that "Connect Anoka County" fiber optic cable terminations exist at (8) key City facilities. These "Connect Anoka County" fiber optic network connections are owned by Zayo Broadband, a Boulder, CO based company that installed the cable infrastructure in partnership with Anoka County in approximately 2011. Per the installation agreement, Anoka County controls 25% of the fibers of this 287 mile ARRA funded broadband network. These connections are reported to exist at 145 government locations within the county.

> Note: "Connect Anoka County" fiber optic network information included here is based on a rural broadband update report posted January2nd, 2015 by the Blandin Foundation ™ on their website: (https://blandinonbroadband.org/2015/01/02/anoka-county-broadband-2014-update-nearly-complete-coverage-with-help-from-arra-funding/)

There appeared to exist no current working knowledge on the part of the City staff as to what the procedure would be for the City to work with either Zaya Broadband or the County to activate and provision some number of these connections or what the financial costs would be incurred in actually building out and configuring a usable "Connect Anoka County" fiber optic data network linking the City Water Department facilities.

Further, while these "Connect Anoka County" fiber optic network cable drop points are known to exist at these (8) locations within the City, these potentially useful network connection routes would necessarily involve connection points and networking equipment belonging to, and maintained by, 3rd parties outside the City staff. For this reason alone it seemed, the prevailing sentiment among City staff was a justifiably high degree of reluctance to employ this potentially available "existing" method of communication for a critical infrastructure application - provided a reasonably viable and cost effective alternative was available.

So, though 5.8 GHz Canopy wireless radio system and "Connect Anoka County" fiber optic assets are available, the condition and current performance parameters of these systems were not tested or otherwise evaluated. However, for report clarity with regard to the availability of existing

communications systems, and also for communications system information consolidation purposes, general information concerning both of these system has been included in this analysis report.

Accordingly, available information concerning the City's existing 5.8 GHz Motorola Canopy radio equipment specification & that network's topology map and a location & fiber status list of the City's "Connect Anoka County" fiber optic network cable drop sites can be found in Section IV of this report.

3. The primary wireless network connecting to the majority of the City Water Department's control system sites is a legacy UHF (400 MHz Band) licensed radio system. The "Master Station" radio and antenna system for this network is located at Tower #1, from which it communicates to all other "Remote" Water Department control system sites on this network. This radio system operates under FCC license Call Sign WPYP217. This license was originally issued on 9/18/2003 (renewed 8/23/2003) and operates on a frequency assignment of 451.28750 MHz. A copy of FCC License WPYP217 is included in Section VII of this report.

This legacy UHF licensed radio network as it currently exits is made up of a combination of (3) radio hardware equipment platforms:

- Maxon SD-125
- GE MDS 4310
- GE MDS 4710

The Maxon radio is a very old, often highly problematic crystal controlled oscillator type of unit. This radio is capable of operating only in a mode known as "Bell 202 Modem" and as configured, only at a very low data throughput speed. This is a type of switched audio tone communications methodology originally developed for wireless signaling between telegraph machines. It was later adapted for signaling between other types of electric & electronic devices and found use in many (very simple/basic) early generation wireless SCADA systems. This radio has long been out of production and is no longer factory supported.

The GE MDS 4310 radio is an early generation analog only radio that went out of production many years ago and is no longer factory supportable. These radios appear to have been added to the system later and would have been a logical choice as this platform was capable of operating in the older, very simple over-the-air signaling mode employed by what is assumed to be the original radios in this network, the Maxon SD-125.

Similarly, the GE MDS 4710 radio is a later but still relatively early generation digital radio that was capable of operating in a reverse compatible analog mode compatible with all operating modes of the 4310 radio, which also included the very early Bell 202 configuration employed by the Maxon SD-125. Several 4710 radios were added to the system over the years. But the 4710 - workhorse though this radio platform was for many years – has now also been out of production for many years and, like the GE MDS 4310, is no longer factory supportable.

The (3) different radio platforms making up this UHF licensed radio network are currently very inefficiently configured to operate in the most sophisticated mode and at the fastest signaling rate *of*

its least sophisticated and slowest radio, the Maxon SD-125. The Maxon SD-125 radio is capable of only a very low speed signaling rate of 300 "Baud" (a telegraph related measure of signaling speed, in this case equating to 300 bits per second).

This aged system remains in operation between Water Treatment Plant & Tower #1 and some Water Department control system sites. However, as will be detailed later in this report, it currently regularly experiences communications outages and has, over these many years, become increasingly unreliable.

The already problematic level of communications system unreliability was recently made significantly worse when Tower #1 was taken out of service for refurbishment in the fall if 2016. Toward facilitating the tower's complete removal from service – including service as host to multiple tower-top mounted antenna systems – the City Water Department's UHF radio system "Master Station" antenna was removed from it mounting position atop Tower #1 and temporarily mounted to a much shorter wood pole very near the large diameter base of the water tower structure.

UHF radio frequency signals can be significantly adversely affected by the presence of various man-made and/or naturally occurring obstacles lying in the direct path between antenna systems of electromagnetic radiation based communication systems. Man-made obstacles such as large electromagnetically reactive/reflective structures - metal sided buildings, bridges, grain elevators, elevated water towers, and other similar steel structures can cause an extreme distortion of intended electromagnetically radiated antenna patterns, as can large naturally occurring obstacles such as trees and other forms of tall vegetation.

The temporary mounting position (~south of the lower structure and under the tank portion of Tower #1) selected for this critical antenna system, relative to both the very large electromagnetically reactive/reflective steel structure of Tower #1 itself and the locations of the majority of Remote radio equipped Water Department control system sites (~north of Tower #1) resulted in a severely distorted and degraded electromagnetic radiation pattern between the control system's "Master Station" radio antenna and antenna systems of the outlying "Remote" radio sites. This further and critically weakened the already marginally usable signal levels at these Water Department control system sites.

As the "Master Station" antenna was moved at about the same time the leaves were going off of the City's deciduous tree population last fall, the decreases in radio signal strengths resulting from the newly introduced Tower #1 obstruction radiation pattern distortion were somewhat offset by the increases in radio signal strengths gained as a result of the seasonal decrease in vegetation obstruction & absorption losses. The offsetting effects of these approximately simultaneous events was masked until the spring of this year when the seasonal vegetation losses again weakened this system's weak and distorted radio communications system signals. The resulting critically low signal levels manifested themselves in the numerous and recurring control system communications network outages and "comm fails" experienced earlier this year by the City Water Department's SCADA system, which very unfortunately led to multiple highly disruptive water shortage events.

4. City Water Department FCC License WPYP217 limits radios operating under this license to a maximum Transmitter (Tx) Power Output of 2 Watts and a maximum "Effective Radiated Power* (ERP)" of 2 Watts.

[* (ERP) A composite calculation of radio Transmitter Power Output, minus cabling attenuation & other signal "losses," plus antenna system directivity & pattern shaping signal "gains."]

This system analysis revealed that virtually the City's entire radio system is being operated at Tx Power and ERP levels well beyond those authorized under FCC License WPYP217.

5. The City's existing licensed UHF radio network topology map as well as a by-site list of radio equipment models, antenna types and installation heights, and measured performance data have been incorporated into a table formatted summary sheet that also illustrates overall network connectivity, all individual radio network segments, and all individual site-to-site radio link connections. This consolidated summary table/matrix can be found in Section IV of this report.

6. This analysis identified numerous City Water Department SCADA radio system components that have either already failed completely or are currently operating in a severely deteriorated condition and require urgent replacement. Among these severely deteriorated components are antenna systems that are no longer resonant or functioning correctly within their intended operating frequency band, numerous corroded/oxidized or otherwise deteriorated connectors, and deteriorated/damaged coaxial transmission lines. A full listing of these failed and failing components is included on the Site Worksheets located in Section VI of this report.

7. This analysis identified all directional antennas as being the "open element" Yagi type antennas. This type of antenna is highly susceptible to the adverse effects of antenna icing.

Note: At 400 MHz UHF and higher frequencies, as little as $1/10^{th}$ of an inch of ice/frost/wet snow accumulation on the exposed elements of this type of antenna can completely reverse the directivity gain and radiation pattern of the antenna – such that the signal is actually transmitted in a direction opposite that intended. This reversal in directivity gain in almost all cases severely degrades the performance of the radio link such an antenna is supposed to be supporting. And, in many cases, causes the link to fail completely for as long as the ice/frost/snow remains on the antenna elements.

Adverse antenna installation issues exist at multiple sites within this radio system. These issues vary from site to site but all detract from optimal system performance. These antenna type, gain, and physical mounting location or position issues are detailed on the individual Site Worksheets Section VI of this report.

8. In order to more thoroughly evaluate the City's existing 450 MHz radio system and evaluate other possible wireless communications system frequency band options, a review was conducted of all existing Water Tower Antenna Space Lease Holder radio system frequencies. This review indicated that ALL current antenna space lease holder radio systems are operating at frequencies far removed from the City Water Department's 450 MHz frequency. The City's UHF Licensed radio system is at virtually no risk of nearby electromagnetic radiator interference from any Antenna Space Lease Holder equipment. The City's current list of Water Tower Antenna Space Lease Holders and the transmitting frequencies of their respective radio equipment suites is included in this report in Section VII.

As a further step in evaluating possible frequency band options, Frequency Spectrum Analysis testing was performed at each of the City's water tower sites in both the 450 MHz licensed, and 900 MHz "Industrial, Scientific, & Medical (ISM)" unlicensed frequency bands.

These tests showed that both the UHF licensed and 900 MHz unlicensed frequency bands were only moderately and lightly occupied respectively. And, that all measureable transmitters appeared to be operating normally and within their assigned channel spaces. The results of these frequency spectrum Analysis test are included in this report in Section VII.

Given this highly favorable initial spectrum availability finding, actual radio path testing of both frequency bands was undertaken. To conduct this type of testing, radio and antenna system equipment designed for use in each of these (2) frequency bands was sequentially temporarily installed on City Water Towers #1, #3, & #4 (Tower #2 was not considered a viable radio network segment host site due to a large quantity of existing radio system antenna systems installed at this site). With these systems installed, signal strength and quality measurements were then taken between these temporary "Master Station" radios & their fixed antenna systems, and portable "Remote" radio & antenna systems dispatched to all City identified existing and potential Water Department control system sights.

> *Note: The 450 MHz radio platform used for actual radio path testing was the GE MDS Orbit LN4, a 406.1 MHz – 470 MHz licensed band radio operating on channels assigned to FCC Itinerant License File No. 0006179849. For purposes of this system test, the radio was operated at its standard power output level and highest (QAM 64) modulation rate, and at a payload data throughput rate of 60 kbps.*
>
> *The 900 MHz radio platform used for actual radio path testing was the GE MDS Orbit NX915, a 902-928 MHz unlicensed band radio operating in accordance with FCC rules pertaining to this band. For purposes of this system test, the radio was operated at both its highest modulation rate at a payload data throughput rate of 1250 kbps and at a lesser modulation rate at a payload data throughput rate of 500 kbps.*
>
> *[The Manufacturer's Specification & Product Information Brochure for both of these products are contained in this report and can be found in Appendix F]*

The comparative 450 MHz and 900 MHZ test results obtained in this manner from each of these Water Tower sites to Water Department sites throughout the entire area of the City of Blaine indicated a clear performance advantage in favor of the 450 MHz system over the 900 MHz system. The 450 MHz system test results indicated a very desirable level of performance within the boundaries of the City; so desirable in fact that highly advantageous alternative network connectivity and topology options were identified as testing progressed and were developed for inclusion within this report. These alternative network connectivity & topology options are discussed in detail in the Section III of this report and are in shown in a graphical format in Section IV of this report.

The totality of the 900 MHz system test results on the other hand indicated that a system reliability in this band would require prohibitively expensive and aesthetically intrusive antenna support structures at most of the City's system control sites. These test results effectively eliminated a 900 MHz license

free radio system from serious consideration as a viable City connectivity option. Accordingly such an option was not included for consideration within this report.

The field test results for both the 450 MHz and 900 MHz series of radio path tests are included in this report and can be found in Section VI.

9. All over-the-air Receive Signal Strength Indicator (RSSI) values recorded for each of the City Water Department radio links tested during the on-site evaluation phase were found to be generally in line with the Phase I Path Analysis predicted values. This significantly positive finding confirms that there are no unknown obstructions or otherwise unaccounted for variables adversely affecting either the physical or electromagnetic radiation space between system sites. This is an excellent finding.

Conclusions & Recommendations

1. The enclosed on-site test results, as expected, indicate that the existing Water Department SCADA radio system requires urgent attention and corrective action in multiple areas.

2. Referring back to Finding and Test Result #4 earlier in this report, urgent action is required to either bring this system into lawful compliance with FCC License WPYP217 or, alternatively, cease communications on this assigned channel altogether.

3. Considering in total all of the issues described in Section III of this report, even if this existing older generation radio system was restored to its optimal performance levels, this communications system still be completely inadequate relative to the City's current needs.

And, as it currently exists, the City Water Department's radio system is not capable of reliably supporting even the existing PLC based control system if it were to be operated in a manner capable of supporting current system operational needs. And, it certainly does not have the capacity to also transport the additional data communications throughput required to support planned upgrades and expansions of this system. Urgent action MUST be taken to provide the Water Department a communications system with adequate levels of operational and functional reliability and network data throughput speed.

4. Beyond the present and looking forward, the period of time low data speed RS-232 only types of radio systems will be able to support evolving PLC communications standards & requirements is very limited. Major PLC manufacturers, including Allen Bradley and Modicon for example, have already begun the discontinuation of their manufacture and support of legacy RS-232 serial PLCs.

5. Current generation and known future generation control system technologies require some Ethernet data capability as do support methodologies like remote access control system maintenance & programming services. The capability to support these types of data communications, over-the-air to each control system site on the network, could drastically improve system integrator response times while also drastically decreasing systems integrator support service mobilization costs by greatly decreasing the number of issues requiring actual on-site services.

6. Given that multiple urgent issues exist, the correction of which will involve the purchase of some number of radio system components and will also very likely involve vendor mobilization expenses, it is recommended that the City and City Utility Department staffs consider implementing (within any existing fiscal constraints) system reconfiguration, equipment upgrade, and network data throughput enhancing options that could be cost-effectively accomplished if done in conjunction with the correction of the existing urgent issues identified in this report.

7. There are multiple options and possible courses of action for restoring and improving the reliability and future supportability of the City Water Department's wireless communications network. Some corrective actions and upgrade options are interrelated and/or interdependent. And, as the radio network repair, reconfiguration, upgrade options, and considerations associated with correcting the above described issues are beyond the intent of this report summary, they are discussed in detail separately in Section III of this Report.

III. Administrative Notes

Every effort has been made to ensure the accuracy and completeness of this report. However, should any technical or administrative error be identified within this report, please bring the discrepancy to our attention – we would very much appreciate the opportunity to correct it.

Larson Data Communications very much appreciates the opportunity to work with the City of Blaine, the staff within City's Water Department, and with those whom the City entrusts as formal and subject matter experts and consultants. We greatly value your trust in our company & our staff and we appreciate & thank you for your business. Please let us know how we can be of further service or assistance.

Mike Larson
Senior Wireless Systems Engineer

Aaron Gerfen
Wireless Systems Application Engineer