SENIOR DESIGN PROJECT REPORT

Campbell Consulting, LLC: Wireless ICS Training Platform

Submitted to

Faulty Advisor: Professor William Lin
Electrical Engineering Technology Program
Engineering Technology Department
by
Cassandra Boman and Nick Pohlman

April 29th, 2019

Campbell Solutions: Wireless ICS Training Platform

ABSTRACT

Essential public services, such as Electric, Water and Gas Utilities, are becoming increasingly reliant on network connected devices to control their processes. Wireless control systems are becoming more common in distributed systems, since they offer many advantages over hard wired alternatives. While cyber physical systems such as PLCs offer many advantages, they are also vulnerable to cyber-attacks. Military force readiness for defense of critical infrastructure against cyber-attacks requires state of the industry industrial control systems for cyber security training. A remote terminal unit using broad spectrum radio was integrated into an existing Water Treatment Plant SCADA system and provided to the US Army for training.

Keywords: Cyber Security, Industrial Controls Systems, Operational Technology, Information Technology, PLCs, SCADA, Utilities, Distributed Systems, Systems Integration, Water Treatment.

Campbell Solutions: Wireless ICS Training Platform

TABLE OF CONTENTS

Campbell Solutions: Wireless ICS Training Platform

REVISION HISTORY

Version	Date	Revised by	Description
1.0	9 December 2018	Cassandra Boman and Nick Pohlman	Initial Version
2.0	13 December 2018	Cassandra Boman and Nick Pohlman	Second Version
3.0	29 April 2019	Cassandra Boman and Nick Pohlman	Final Version

Campbell Solutions: Wireless ICS Training Platform

1. INTRODUCTION

Industrial control systems have traditionally been comprised of operational technology using analog systems that are isolated from the internet. Modern industrial control systems use Programmable Logic Controllers (PLCs) and Supervisory Control and Data Acquisition (SCADA) software that are connected by some form of network. This has prompted a change in industry to cyber physical systems that use information technology to control operational technology. Cyber physical systems are popular because they allow system owners to improve system quality by acquiring data and increasing control capabilities. While these systems mostly communicate through hard wired means, such as fiber optic and ethernet cable, wireless communications are becoming more common. The increase in wireless connected systems is for three reasons. First, it allows companies to reduce cost, since they do not need to route cables. Second, it reduces physical system complexity by reducing number of cables needed. Finally, it allows equipment to be added to areas that was originally impractical. This last reason is particularly popular with public services with complex distribution networks, such as electric, gas, and water utilities.

The increased reliance on IT connected controls, especially wireless systems, comes with increased security risk. The potential damage to critical infrastructure, such as water treatment and electric power, has prompted interest in defending these assets from cyber-attack. In particular, the U.S. Military has sought out ways to defend essential public services. Force readiness requires cyber security training on modern industrial control systems. Training platforms, that are close as possible to state of the industry, are required to train the next generation of cyber warriors. Muscatatuck Urban Training Center (MUTC) is a U.S. Army National Guard base with fully integrated cyber physical systems that make it ideal for this type of training. Existing on post facilities, including a coal fired steam plant and water treatment plant, can allow for cyber security training with minimal additions to infrastructure. While the infrastructure is mostly intact, the control systems are outdated and require retrofitting to meet current industrial standards. Modifying the current control scheme of the Bush Creek Water Treatment Plant to include a remote terminal unit with wireless communications would satisfy the need for a training platform.

Campbell Solutions: Wireless ICS Training Platform

Problem Statement

Project Need

A wireless industrial control system is needed at MUTC for cyber security training.

Key Objectives

The key objectives for this project are:

I. The system must use a wireless protocol as its primary means of communication.
II. The system must integrate into an existing industrial facility on post.
III. Data transmitted by the remote terminal unit (RTU) to the main system must be used to control a process. At a minimum, the remote unit must pass an analog value to the main system.
IV. The system must be located at a remote location from the main system.
V. The system must meet industrial standards.

System Overview

Project Proposal

To meet the above requirements the IUPUI Design Team, on behalf of “Campbell Consulting, LLC, proposed the following means to meet the project key objectives:

A Wireless ICS Training Platform that:

I. Uses Broad Spectrum Radio
II. Integrates with Bush Creek Water Treatment Plant
III. Controls Water Treatment Plant Backwash Flow
IV. Measures Intake Pressure at on base Steam Plant
V. RTU will include Hardware Protection (Fusing, Circuit Breakers, Surge Protection) and Message Verification in Software

General Topology

The system will consist of an RTU housed in a standard industrial panel located at the Steam Plant. Using Cambium Broad Spectrum Radio, the RTU will measure intake pressure at the Steam Plant and transmit the data wirelessly to Bush Creek Water Treatment Plant. Intake Pressure will be added into the Water treatment Backwash Flow control algorithm. Doing so will increase local water distribution quality by limited pressure loss, improve Steam Plant reliability by preventing boiler tripping, utilize wireless communication and provide a realistic process under control for training.

2. SYSTEM-WIDE DESIGN DECISIONS

General Project Design Decision

In general, the project stakeholders' primary interest is a wireless control system that is part of a larger process for existing facilities on post. Cost and safety the driving factors for the stakeholder's decision for choosing a process. The choice was ultimately between the Water Treatment Plant Intake Structure and Backwash Flow Control. In the end, plant owners chose to abandon the Intake Structure, making the first option impossible. This decision was made for the following reasons.

1. **Low Water Treatment Plant Capacity Factor.**
   Bush Creek Water Treatment Plant is for training purposes only. While the plant can supply potable water to the local water distribution network, the plant is not continuously manned. Consequently, the total annual volume of water supplied by the plant is low and the base does not rely on the plant for potable water.
2. **High Cost of Chemical Storage**
   In order to comply with local water board regulations, a plant that purifies raw water and supplies it to a distribution network must meet water quality standards. To meet these standards, plants must use chemicals and store them at the plant. The high cost of storage, coupled with the plant's low capacity factor, made this option cost prohibitive.
3. **Intake Structure Instability and Environmental Issues**
   The Intake Structure was found to be unsound and was deemed unsafe. Lead present in the structure's paint was also deemed hazardous.

Due to the above reasons, it was found to be more cost effective to abandon the Intake Structure and deem the plant "Training Only". Since the plant no longer drew raw water or supplied water to the distribution system, the plant only needed to recirculate water for operations training. The only source of water to keep the plant supplied was the local water distribution network which was accessed by a backwash valve. While this reduced the operating cost of the plant, issues were caused the flow rate of water into the backwash valve. Solving these issues is central to the chosen process under control.

Water Distribution Issues

A high flowrate must be used to fill the Treatment Plant in a reasonable period of time. Bush Creek Water Treatment Plant shares a water distribution network with all the facilities on post. While the effect of a high-water flow rate into the Backwash Valve on other facilities on post, the notable exception is the Steam Plant. The coal fired Steam Plant is the only source of heating for all buildings on post and supplies heat with hot steam. To accomplish this, the Steam Plant needs a stable water pressure and flow from the water distribution network. Enough drop-in pressure at the intake of the Steam Plant will cause the plant's safety system to trip and shut down its boilers.

A plant shutdown results in an undesirable and lengthy interruption of the posts heating system. Due to winters experienced on the base, this event must be avoided.

Theory of Operation and Control Methodology

To safely control the Backwash Flow Rate to fill the Treatment Plant in a reasonable period while avoiding trips at the Steam Plant due to pressure drops, a control methodology must be developed from the system's theory of operation. From Bernoulli's Principle, the relationship between volumetric flow rate and pressure differential can be derived.

<u>Volume Flow Rate and Pressure Control:</u>

$$Q_{volume} = Av$$

$$\Delta P = QR_{pipe}$$

$$P_{STP} = P_{Distro} - QR$$

$$P_{STP} \propto \frac{1}{Q_{WTP}}$$

Pressure at the Steam Plant is shown to be inversely proportional to the Backwash Volumetric Flow Rate. Understanding this relationship, pressure at the intake of the steam plant can be maintained while allowing a reasonable flow rate into the Treatment Plant. This can be achieved by measuring the pressure at the Steam Plant and using it to linearly regulate the max flow rate set point of the Backwash Valve.

The backwash flowrate for the Treatment Plant can be set by controlling the position of up to five separate filter valves. These valves are pressure compensated and allow the user to control flow by setting a valve position, without worrying about differential pressure between the input and output of the valve. Closed loop control of valve position is achieved using a Proportional Integral (PI) Controller. It should be noted that the PI form used is the discrete realization of the PI velocity form. This form takes the derivative of the traditional PI equation. Instead of reporting a position, the controller calculates a change in position for the valve. The equation removes the integral term, avoiding issues with integral wind up. Since the PI coefficients remain the same, the controller operates transparently from the traditional form and can be tuned using the same methods as a traditional PI. Other than the change in equation, the controller can be approached as if it were the normal PI form.

Modifying the max setpoint linearly allows the additional variable to function as a outside "slow" loop for the PI controller. The pressure is sampled every 5 minutes and reduced 5 PSI if the recorded pressure is below an allowable point.

Campbell Solutions: Wireless ICS Training Platform

This is shown in the following equation:

Velocity Form PI with Variable SP

$$E_{[n]} = SPV_{[n]} - PV_{[n]}$$
$$SPV_{[0]} = 300\ gpm$$
$$if:\ P_{STP} < 70psi$$
$$SPV_{[n]} = SPV_{[n-1]} - 5gpm$$
$$else:\ SPV_{[n]} = SPV_{[n-1]}$$
$$CV_{[n]} = CV_{[n-1]} + KC[\Delta E + \frac{1}{60T_i} E\Delta t]$$

Where :

P_{STP} = Steam Plant Intake (STP) Pressure in psi
P_{Distro} = Butlerville Water Distribution Network Pressure in psi
Q_{WTP} = Water Treatment Plant (WTP) Backwash Volume Flow Rate in gpm
E = Error
SPV = WTP Backwash Volume Flow Rate Variable Set Point in gpm
PV = WTP Backwash measured Volume Flow Rate in gpm
CV = Backwash Valve Position (% of Full Scale)
KC = Controller Gain (Dependent)
Ti = Integral Time Constant in minutes per repeat
Δt = time update in seconds

It should be noted that additional safety interlocks are included in the control methodology to prevent trips at the Steam Plant. These will be covered in the software section.

2.1 <u>Hardware</u>

This section elaborates on the hardware engineering requirements and the justifications used for this project. This primarily discusses the customers parts list and the required physical devices needed for this overall project in the main water treatment plant and the steam plant. These parts include both PLC components to allow expandability for more devices to be added into the design. This also includes the power requirements for each device to be allowed to operate in working condition and allow to be continuously operating for future training events with the military or other utility companies.

Campbell Solutions: Wireless ICS Training Platform

Designator	Marketing Requirement	Engineering Requirement	Justification
HW-1	1, 2, 3, 4, 5	PLC components must come off the approved common parts list	The customer has a list of common parts that a readily available, easy to obtain or replace, and adhere to industry standards. These parts are proven to be compatible with the existing system and allow for expansion of the system. Documentation for these components is readily available.
HW-2	4, 5	System will be backed up by a UPS sized to allow 15 minutes of operation in the event of power failure	System is a utility that must be able to operate continuously. In the event of power loss, the system must be able to shut down safely.
HW-3	2, 4, 5	System power supplies will be fed from 120VAC, single phase power	120VAC is the standard voltage supplied for electrical service
HW-4	1, 2, 3, 4, 5	PLC power supplies will output 24VDC	DC systems are common with PLCs. The system must be easily expanded and compatible with multiple proprietary systems. All components having a common voltage will reduce types of power supplies needed, allowing the system to be easily modified and reducing cost. DC power supplies are more reliable than AC systems, since they are less susceptible to line impedance issues. AC systems have two zero crossings per period, which may cause issues with relays or sensors.
HW-5	1, 2, 3, 4, 5	The type of IO available to the system will be: Digital Inputs: 24VDC Digital Outputs: 24VDC Sourcing Analog Inputs: 4-20mA Analog Outputs: 4-20mA	24VDC and 4-20mA are common IO for PLCs. Items from the common parts list are all compatible with these IO.
HW-6	4, 5	System will include 20% spare IO	This allows room for potential additions in the system for future components.
HW-7	1, 3, 4	System will use 2.4 GHz spectrum radio antenna for wireless network and maintain above -90 dbm	The location of the input structure makes it difficult and impractical to route conduit for sense lines. A wireless network reduces the hard wiring required. This will allow easy installation and modification of system. The existing wireless network is radio.
HW-8	5	All components have an operating temperature of -31.1 degrees C to 40.6 degrees C or Better	The record low temperature for North Vernon Indiana is -31.1 degrees C and the record high temperature is 40.6 degrees [5]. System components may be outdoors or in non-heated buildings.

Campbell Solutions: Wireless ICS Training Platform

2.2 Software

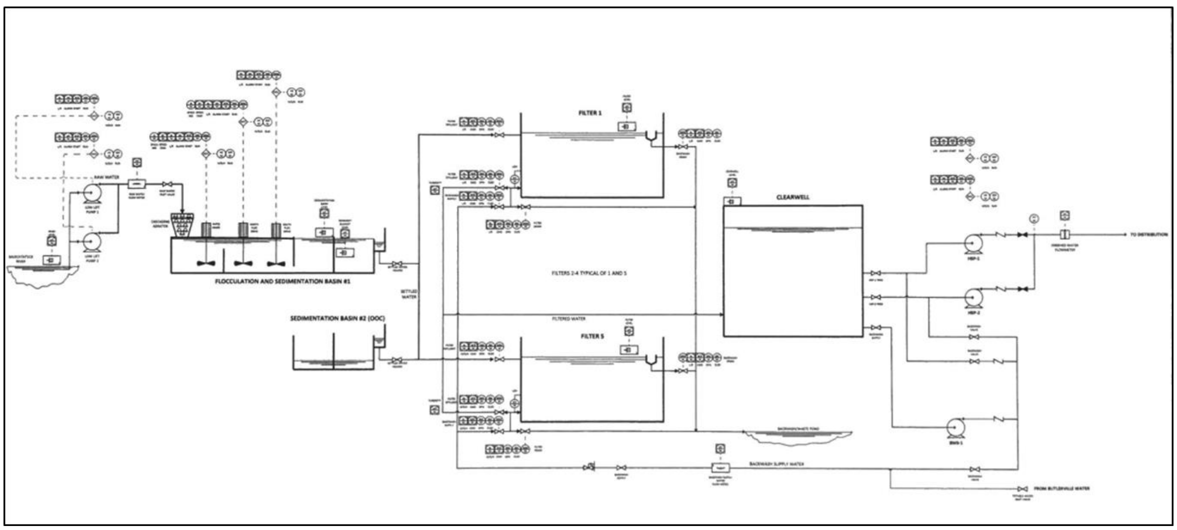
This section elaborates on the software engineering requirements and the justifications used for this project. This primarily depicts the programming for all the signals in the plant, the RS Logix code, the HMI screen that will be displayed in the main water treatment plant, the sampling time with steam plant loop rate, and will report to the operators of the current PSI level from the steam plant while using a dead band.

Designator	Marketing Requirement	Engineering Requirement	Justification
SW-1	1, 2, 3, 4, 5	Programming will capture all signals in plant	The entire system will need to be able to receive and log every signal inside the plant without running excessive wiring to each device. System must use all sensors effectively for controls.
SW-2	2, 3, 4, 5	Programming will use RS Logix for controls	RS Logix is IEC –61131 compliant, commonly available and compatible with PLC components off the common parts list.
SW-3	2, 3, 4	HMI screen in main plant will display Steam Plant Pressure	Operators must always be aware of Steam Plant Pressure value for safety and ensuring the boilers do not shut down from an insufficient flowrate.
SW-4	1, 3, 4, 5	RS Logix code will consist of requesting the steam plant's current pressure within 5 minutes	The RS Logix code will be designed to store and move values of the pressure from the steam plant. This loop rate will occur every 5 minutes to ensure communication is continuing from the water treatment plant and steam plant.
SW-5	1, 4, 5	Alarms report with exception of the difference in Steam Plant Pressure	Operators must be aware of the changes of pressure in the Steam Plant. A dead band is used to ensure the Operators are informed from a pressure difference of 2 PSI.

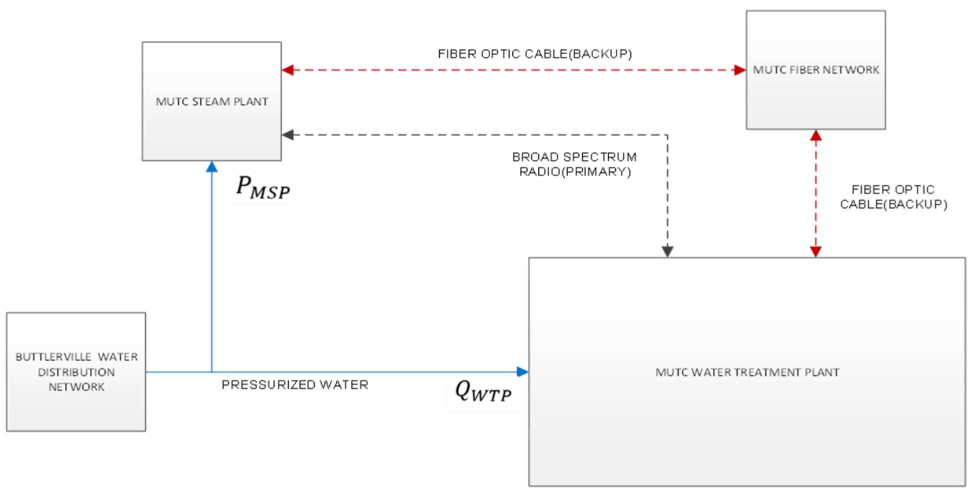
Campbell Solutions: Wireless ICS Training Platform

2.3 Interface

These three diagrams consist of the Initial P&ID, High-level block diagram, and the network diagram. The existing P&ID was used as a starting block for the entire project that focuses primarily on the main water treatment plant of the MUTC. The High-level block diagram displays the water distribution system from the water treatment plant and the steam plant. This includes the wireless communication and the fiber optic back up system. The last diagram consists of the network diagram displaying the means of wireless communication for the RTU in the steam plant to the main PLCs in the water treatment plant.



Campbell Solutions: Wireless ICS Training Platform



3. SYSTEM ARCHITECTURAL DESIGN

The system architectural design for the project is a description of each state and modes of the devices being implemented into the waste water treatment plant. This includes components depicted in the system and hardware engineering requirements of section 2.1 and 2.2. These parts consist of the required power, PLCs components, wireless communication devices such as the radios, the switches, and interfaces for the HMI.

3.1 System components

The two locations for components are the main water treatment plant and the steam plant. The main water treatment plant consists of the existing PLC units and will include the addition of an HMI, Cambium Radio, and Antenna. The main water treatment plant PLC will be the control system for the entire plant and control the backwash flow valve that distributes water to the water treatment plant and the steam plant. An HMI is required to monitor the steam plant's pressure value, receiving reports every five minutes, and control the backwash flow valve. The Cambium Radio is required to communicate wirelessly with the steam plant's RTU PLC.

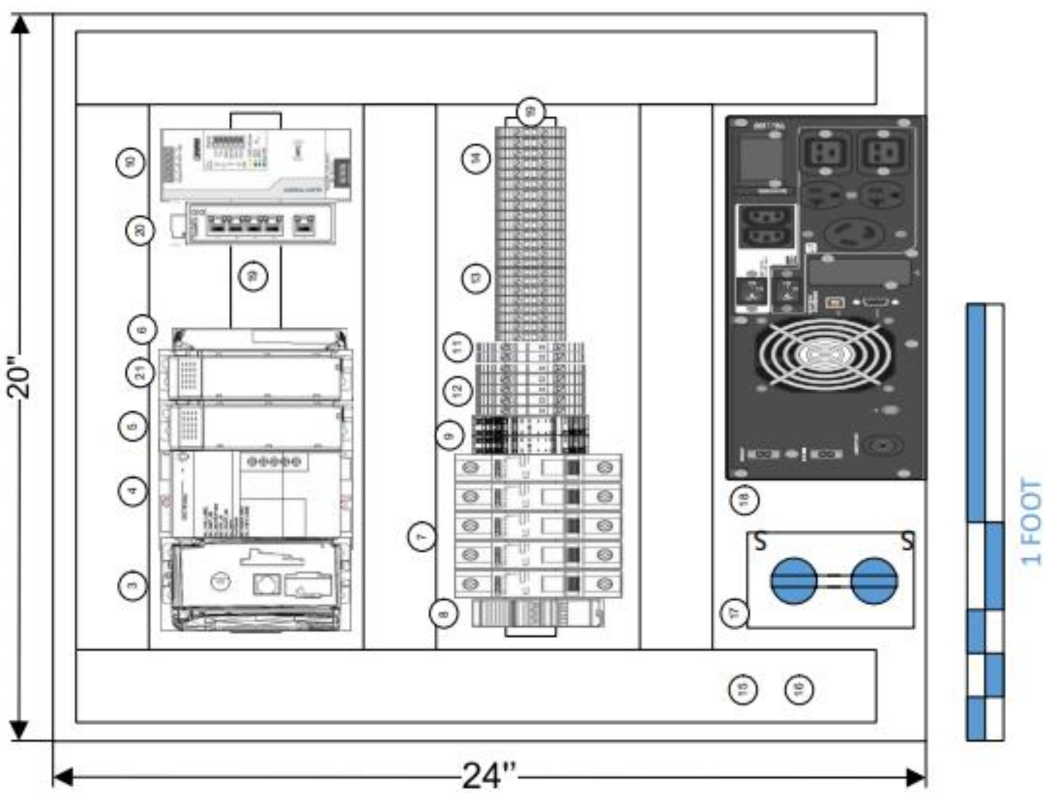
The steam plant RTU will consist of a PLC, a Stratix 8000 switch, 24VDC Power Supply, UPS, and its hardware protection. The facility will also have the Cambium Radio and the antenna for wireless communication. The PLC, Switch, and power supply; will be housed in a cabinet and include the Compact Logix equipment listed below. A Stratix 8000 switch connects the RTU

Campbell Solutions: Wireless ICS Training Platform

PLC with the Cambium Radio. The Cambium radio antenna will attach to the roof of the facility and will include lightning protection.

The purchased equipment, with Panel Drawing, is shown below:

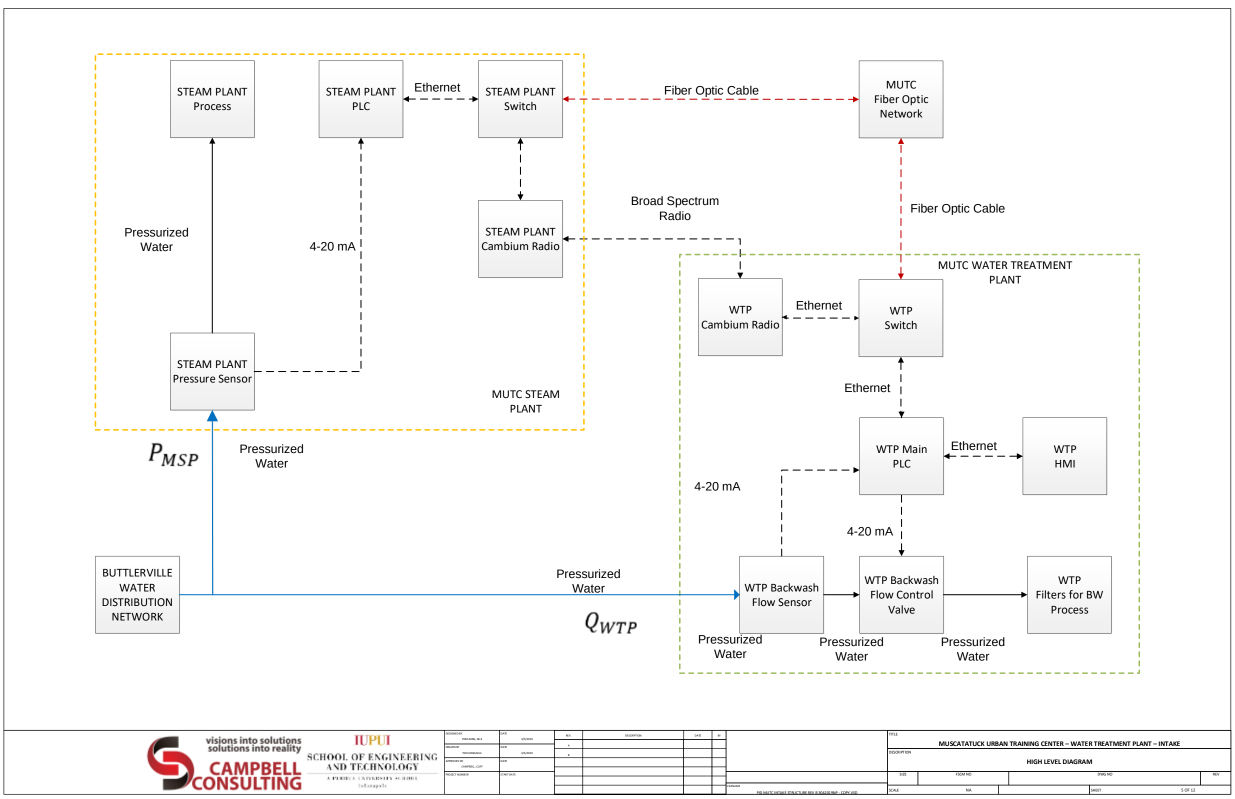
- 1769-ECRRIGHT END CAP TERMINATOR
- 1769-L32ECOMPACTLOGIX ETHERNET PROCESSOR
- 1769-IF4INPUT CARD
- 1769-0F4COMPACTLOGIX 4 POINT A/0 MODULE
- 1769-PA2COMPACTLOGIX POWER SUPPLY
- 1769-IQ1624VDC SINK/SOURCE INPUT CARD
- 1769-0B1616 POINT 24VDC SOURCING OUTPUT
- STRATIX 8000 SWITCH
- CAMBIUM NETWORK RADIOS   2.4 GHz, 13 MILES RANGED, AES SECURITY



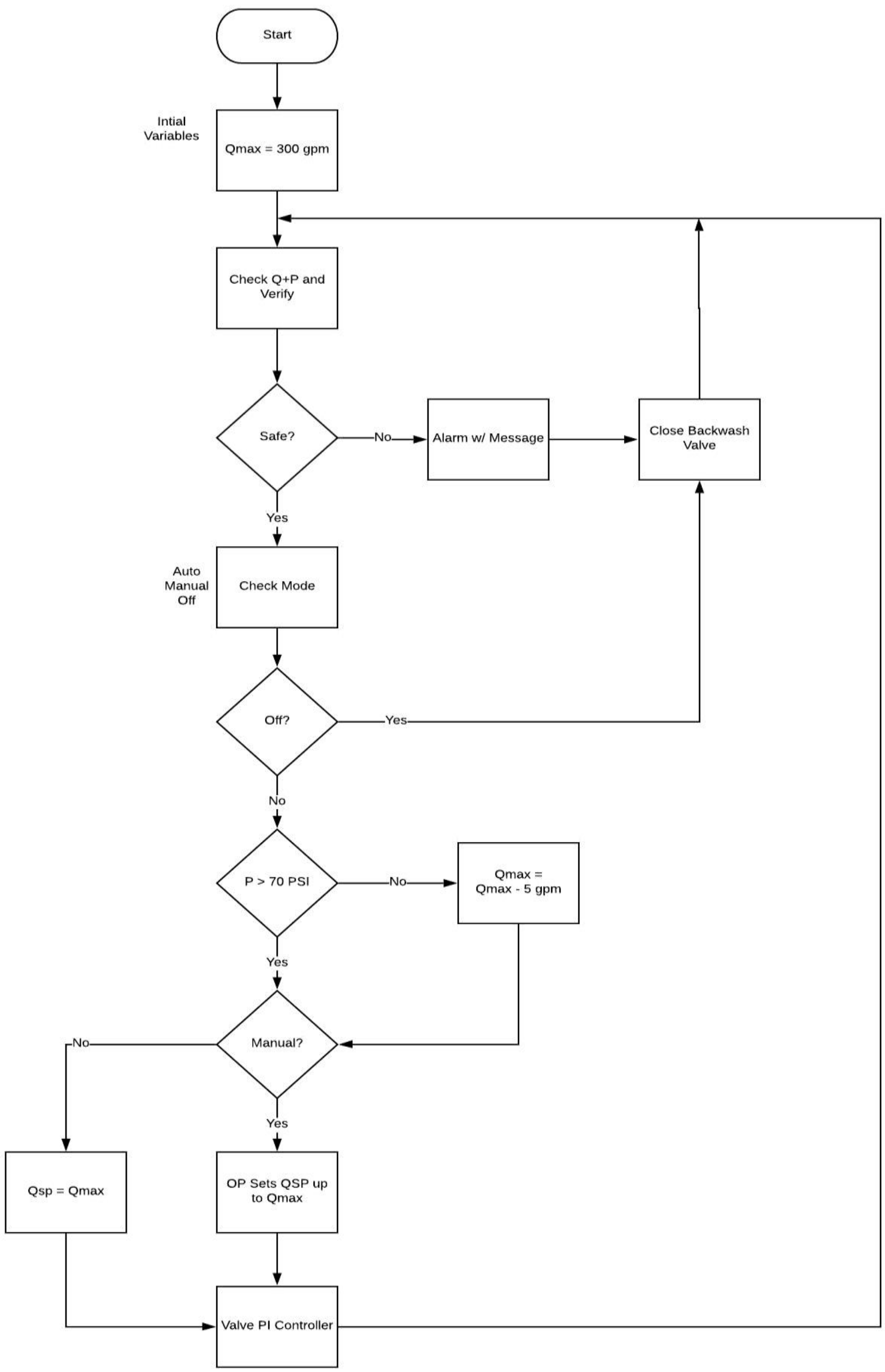
Campbell Solutions: Wireless ICS Training Platform

3.2 <u>Concept of execution</u>

The two below diagrams show a Low-level block diagram and a flowchart for the messaging system. The low-level block diagram displays how the Steam plant will measure the pressure throughout the plant to provide information wireless from the RTU to the HMI in the main water treatment plant. The main water treatment plant will be receiving the information and to use a PI control loop to turn the backwash valve on or off based on the level of the steam plants pressure. The flowchart demonstrates the RS Logix code to determine when to turn the backwash flow valve on or off if the pressure is below 70 PSI.



Campbell Solutions: Wireless ICS Training Platform



3.3 Interface design

This section discusses the layout of each components of the steam plant, main water treatment plant, and wireless network diagram incorporated into both locations. These parts and requirements are listed in Sections 2.1, 2.2, and 2.3. The sub sections will consist how each part interfaces with the other and elaborates the outcome from each system.

3.3.1 Interface identification for the Steam Plant

The first part contains the steam plant and how each device will interact with the other for the success of this project. The steam plant will consist of all PLC components that will be in a cabinet for the Compact Logix equipment. This will connect to every device. The devices consist of the PLC components, Stratix 8000 switch, UPS, and the Cambium Radio and Antenna. Diagram can be referenced from Section 2.3.

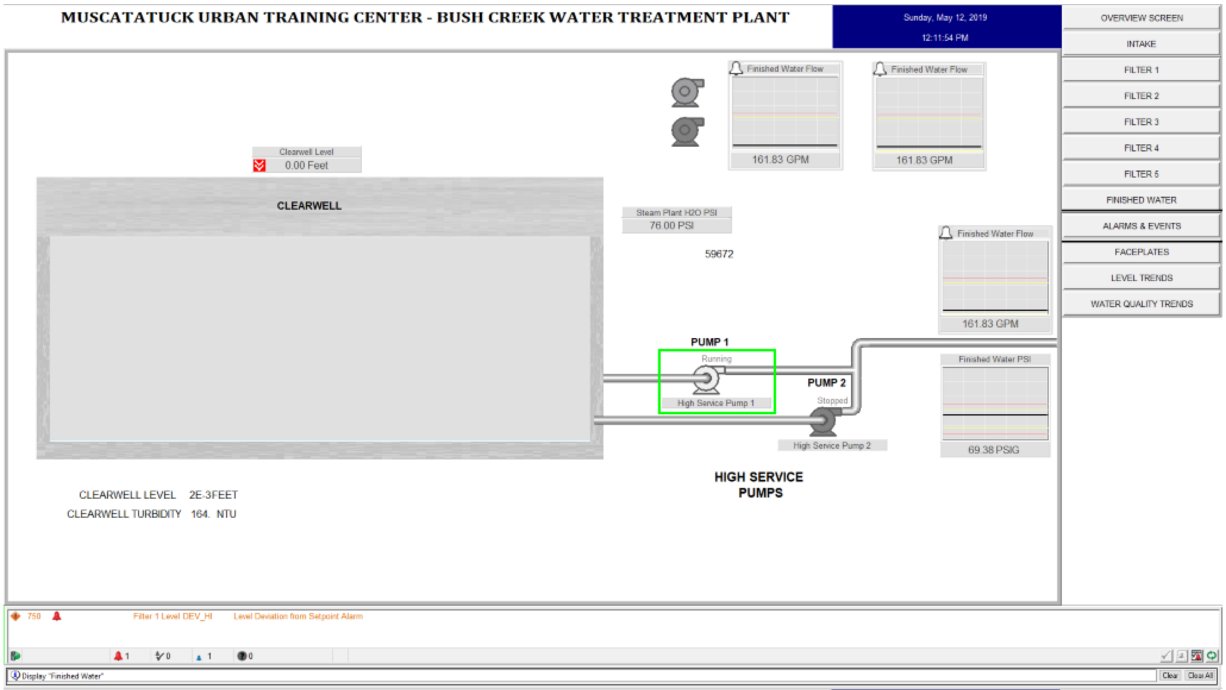
3.3.2 Interface identification for Main Water Treatment Plant

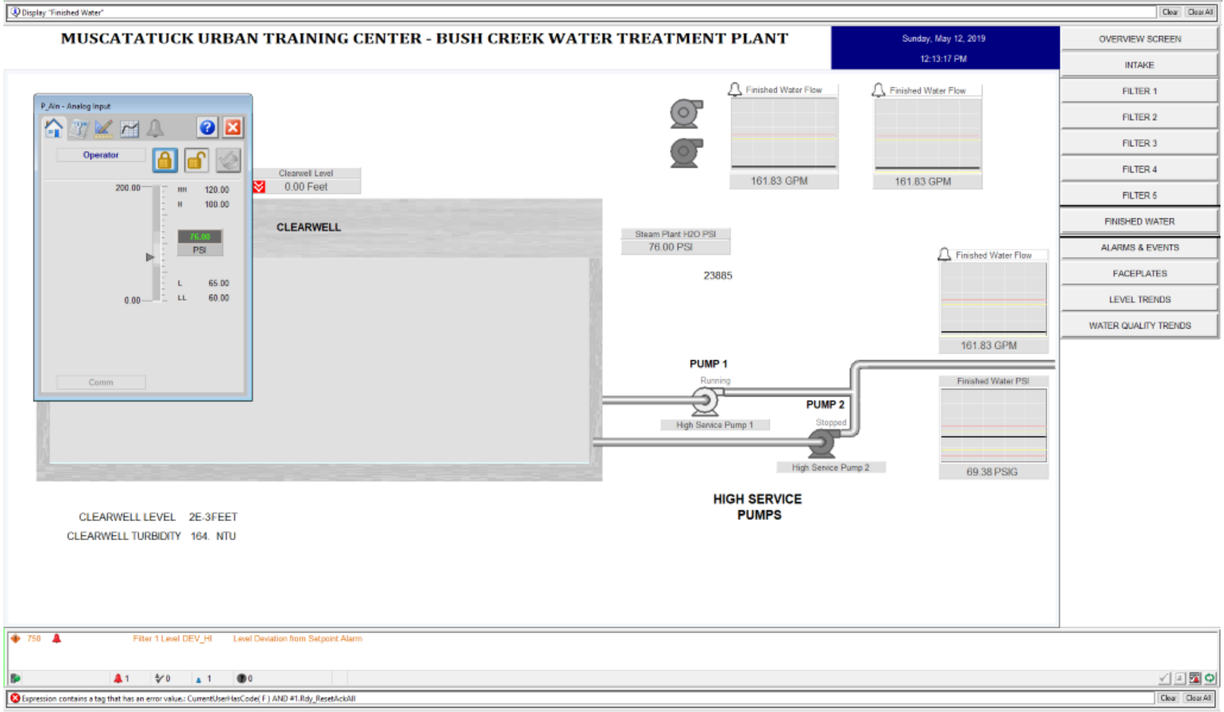
The main water treatment plant consists of all main PLC components that will be in a cabinet for the Compact Logix equipment. The devices that will be connected to this PLC would be the HMI display, and the Cambium Radio and Antenna. The Cambium radio antenna will attach to the roof of the facility and will include lightning protection. Diagram can be referenced from Section 2.3.

3.4 User Setup and Operation

The setup operation for this project will be using the HMI display in the main water treatment plant and the PLC cabinet installed at the steam plant. This system heavily relies on wireless control and operation for the user to use in the waste water treatment plant. The display screen will be utilized in the main plant that will display the steam plant's pressure value, controlling the backwash flow valve, and any active alarms that have been sent to the display. The operation of the system for the user will allow the individual to determine the outcomes of the alarms and the action to take. If the steam plant pressure is too low, the RS Logix code will shut the valve and refuse any changes from the operator until the system as returned above 70 PSI. If the steam plant's pressure is operating at a reasonable value, the operators can modify the steam plant's set point.

Campbell Solutions: Wireless ICS Training Platform





Campbell Solutions: Wireless ICS Training Platform

4. CONCLUSIONS AND RECOMMENDATIONS

Results:

Cambium Radio Field Test:

The Cambium Radios were field tested on site at MUTC, with one unit connected to the Treatment Plant SCP and a second unit located at the Steam Plant. Radios were mounted approximately 20 feet above ground level at the Treatment Plant and 15 feet above ground level at the Steam Plant, with both radios oriented to each other. Ground distance between radios was approximately 1500 ft, with buildings and trees in line of sight. Signal degradation between the radios was no worse than -75dBm. Communications were rated as acceptable quality and exceeded the -90dBm signal loss requirement. Radios were essentially “transparent” to the network.

Panel Factory Acceptance Test:

Panel hardware was tested with a power supply and multimeter. Wire routing and connections were double checked for quality and correct landings. The result was double checked by the Industrial Sponsor. Both digital and analog signals were tested by using a 24VDC and 4-20mA supply, respectively. Panel was verified as operational.

Panel Software was tested in a step by step process. First, code was simulated internal to the RTU to ensure algorithms were functional. The code was trouble shot by forcing unexpected values to proof against disturbances. Code was then separated into RTU and SCP routines and were tested over an ethernet network connection. Finally, code was tested using 4-20mA signals into analog input. The HMI was also checked during this time. Proper operation was checked by the Industrial Sponsor and was verified as operational. The system was approved and passed factory acceptance testing.

Final Field Test and Commissioning.

The final field test was not conducted do to an ongoing military operation. The panel was passed on to the Industrial Sponsor.

Recommendations

The panel is has passed factory acceptance testing and the radios have passed field testing. The system should be double checked during installation and commissioning. Final coefficients for the control algorithm may require trial and error. All industrial equipment should be operated within specifications and with due caution. The design team takes no liability for damage to equipment during the operation, proper or otherwise, of this system.

Conclusions:

Campbell Solutions: Wireless ICS Training Platform

The risk of cyber-attacks damaging industrial operational equipment is increasing. As network connected devices are integrated into distributed systems, care must be taken to protect critical infrastructure. Wireless systems present an increased risk and are not as secure as point to point wiring. By using the Wireless ICS Training Platform, U.S. Military cyber security professionals will be better able to protect essential public services such as water, electric, or gas utilities. The increase in Force Readiness will result in a more secure cyber physical environment and allow systems integrators to further develop information technology with operational technology.

Campbell Solutions: Wireless ICS Training Platform

REFERENCES

1. “Muscatatuck History,” *atterburymuscatatuck.com*. [Online]. Available: https://www.atterburymuscatatuck.in.ng.mil/Portals/18/PageContents/Home/About Us below/History/AM MUTC history.pdf. [Accessed: 06-Oct-2018].

2. *History | Atterbury-Muscatatuck*. [Online]. Available: https://www.atterburymuscatatuck.in.ng.mil/Home/AboutUs/History.aspx. [Accessed: 06-Oct-2018].

3. Mohedas, S. R. Daly, and K. H. Sienko, “Requirements Development: Approaches and Behaviors of Novice Designers,” *Journal of Mechanical Design*, vol. 137, no. 7, p. 071407, 2015.

4. S. Zenios, *Biodesign: the process of innovating medical technologies*. Cambridge: Cambridge Univ. Press, 2010.

5. “Intellicast - North Vernon Historic Weather Averages in Indiana (47265),” *Intellicast - Baltimore Historic Weather Averages in Maryland (21202)*. [Online]. Available: http://www.intellicast.com/Local/History.aspx?location=USIN0490. [Accessed: 06-Oct-2018].