SCADA Basics

Maine Water Utilities Association
February 5, 2020

JT Trinward, P.E.
Woodard & Curran
About the Presenter

- 18 years experience in the design, programming, and service of instrumentation and control systems, with 15 years involving municipal and industrial water and wastewater projects.

- Discipline Leader with Woodard & Curran for the Instrumentation and Controls (I&C) team, acting as technical and resource manager for staff engineers and CAD designers.
SCADA Basics: Agenda

- What is SCADA and why is it needed?
- SCADA Components (PLC & HMI)
- Data and what to do with it
- Industrial networking
- Cybersecurity
- Technology: Information vs Operation
- Questions
Quick Poll

- How many folks in attendance are:
  - Operations staff?
  - Lead operations/superintendents?
  - Directors/management?

- At your plant/utility/DPW, how many of you:
  - Have a SCADA system?
  - Have remote access to a SCADA system?
What is SCADA?

- Supervisory Control and Data Acquisition
- A system that provides control and supervisory overview of a process. It allows an operator to monitor the process and make changes to the process controls. It also collects data on the process for historical trending and process analysis.
- While we only associate SCADA with water and wastewater, it is a general term that can be used in any process.
Why is SCADA Needed?

- Onsite operational control
- Remote site monitoring and operation
- Operational efficiency
- Alarming, and alarm call outs
- All information in one place, data analysis
- Automated reporting
Acronyms and Definitions

- **SCADA** – Supervisory Control And Data Acquisition
- **PLC** – Programmable Logic Controller
- **HMI** – Human Machine Interface
- **OIT** – Operator Interface Terminal
- **VPN** – Virtual Private Network
- **I/O** – Inputs/Outputs

And dozens more….. I provided a cheat sheet hand-out
What Makes Up a SCADA System?

- Many separate components combined in a meaningful way constitute a complete SCADA system.
- First, are the devices being monitored and controlled:
  - Equipment and Processes (i.e. Pumps, Filters, Blowers, Mixers, Tanks)
- Then, there are the monitoring and controlling devices:
  - PLCs
  - HMIs
  - OITs
  - Control Panels
  - Instruments
Programmable Logic Controllers (PLC)

- The brain of the control system
- A microprocessor-based device used to control industrial systems
- Takes in information, sends out instructions (I/O)
- Meant to last for years
PLC Existing Hardware Platforms

PLC-5

SLC 5/05
PLC - Computing Power

A little bit about bits…

- PLC 5
  - 8 Bit
  - Nintendo Entertainment System

- SCL 5/05
  - 16 Bit
  - Super Nintendo
Computing Power

Control Logix 1756-L81E

- 1 gigabit Ethernet Port
- Can Connect to 60 Ethernet / IP Devices
- USB 2.0
- 3 MB Memory
- 128,000 IO Points
PLC Inputs & Outputs (I/O)

- Digital Inputs & Outputs
  - On or Off; 0 or 1; Bits
- Analog Inputs & Outputs
  - Continuous Values; Bytes
PLC Inputs & Outputs (Discrete I/O)

- **Digital Input (DI)**
  - Binary (on/off, in alarm/not in alarm, open/closed, etc.)
  - Typically 24VDC

- **Digital Output (DO)**
  - Similar to DI, but triggers an action
  - Typically 24VDC, but can be 120VAC
  - Typically uses relays to isolate power
PLC Inputs & Outputs (Discrete Types)

- What are some examples of Digital Inputs?
  - Level Switches, On/Off Switches, Start/Stop Pushbuttons, etc.

- What are some examples of Digital Outputs?
  - Pump start commands, Alarm horns and lights, etc.
PLC Inputs & Outputs (Analog I/O)

- **Analog Input (AI)**
  - Continuous real number signal; range defined by device and program
  - Typically 4-20mA signal

- **Analog Output (AO)**
  - Control variable for any non-digital continuous processes
  - Typically 4-20mA signal
PLC Inputs & Outputs (Analog Types)

- Why do we use 4-20mA?
  - Voltage signals attenuate over long distances. Current does not.
  - Easy to detect errors such as a damaged cable if current stops.

- What are some examples of Analog Inputs?
  - Chlorine Residual (mg/L), Flow Rate (GPM, MGD), Tank Level (ft), etc.

- What are some examples of Analog Outputs?
  - Pump Speed Commands, Valve Position Control, etc.
I/O Wiring Example
Instruments

- Level
- Pressure
- Flow
- Temperature
- Analytical
  - pH
  - Turbidity
  - Chlorine
SCADA Control Panel

- Houses PLC, telemetry equipment, Ethernet switch, uninterruptible power supply, terminals, fuses and other components
- Designed for the area where it is installed (panel NEMA rating)
- NEVER open a panel unless you are a Qualified Electrical Worker
SCADA Control Panel Examples
Control Panel Design Example
Operator Interface Terminal (OIT)

- Small displays intended for monitoring and control of local instruments and equipment
- Often mounted in the door of a control panel
- Screens specifically designed for use in small form factor (6-12”)
- Touchscreen or keypad (keypad technology becoming obsolete)
**Human Machine Interface (HMI)**

- Software application that provides a graphical representation of the process and displays real-time status, variables and alarms
- Customized for each process and client
- Application has security built in to restrict access to only screens and functions necessary to execute job function
Additional SCADA Software

- **Reporting**
  - Software automatically populates reports

- **Alarm Dialing**
  - Software and Hardware Dialers
  - Can call or text operators
  - For emergencies, can call down a list until someone responds
HMI – The Human Machine Interface
HMI Screen Example Wastewater - (Old Style)
HMI Screen Example Water - (Old Style)
HMI Screen Example (High Performance)
HMI Screen Example (HP-HMI Dashboard)
Virtual Machine – What is it?

- A virtual machine (VM) is a software program or operating system that not only exhibits the behavior of a separate computer, but is also capable of performing tasks such as running applications and programs like a separate computer.
- Virtual Machine needs a manager, also called a Hypervisor.
- A Hypervisor is a type of software that allows us to run an operating system within another operating system. (VMWare is an example)
- Why run a Virtual Machine?
  - Running different versions of Windows for different applications? XP, Windows7, Windows10
  - Applications that do not work well on the same OS
HMI - Historical Trending (Lots of Data)

- Historical Data saved on HMI or dedicated Historical computer or Virtual Machine
- Stored as Native Database (Software specific)
- Utilizing SQL Database – conforms to IT and able to migrate easily to CMMS and other platforms
HMI Data Integration: Technology is Transforming Aquariums to Lakes
Information Data Management: Roadmap and Guides are Essential
Information Data Management: How it all might work

Field Device
Utility Cloud APP
doforms

GIS

Firewall

Internet Cloud Storage Service

ArcGIS

HACH WIMS

SEMS

Cloud Storage Service

Lab Data, SCADA Data & Manual Data Entry

CMMS

Work order/Maintenance

CMMS

Manager/ Director

HACH WIMS & CMMS

SCADA
Information Data Management: Dashboard availability
Data Visualization: Now We Can Magnify its Communication Potential
SCADA System Networking

- Very simplistic in the past
  - Large, flat networks
  - Maximizing availability, minimizing security

- As components and data requirements become greater, networks becoming more complex and sophisticated

- Embracing common IT networking practices
  - Network segmentation
  - Virtual networks
SCADA System Telemetry - Radio

- Water/wastewater systems inherently have remote locations
- Reliable communication needed for optimal operations
- Unlicensed Radio Frequency
  - Lower broadcast power (shorter distances)
  - Prone to interference (sharing other populated bandwidths)
- Licensed Radio Frequency
  - Higher broadcast power
  - Line of sight still critical, but higher power can ‘punch’ through foliage
  - Less interference (reserved bandwidth through FCC)
SCADA System Telemetry - Cellular

- Cellular
  - Higher bandwidth than radio
  - Security cameras
  - Lower upfront capital cost than radio
  - Recurring fees
  - Dependent on 3rd party infrastructure
SCADA System Networking

- **LAN** – *Local Area Network*
  - Within a plant or building

- **WAN** – *Wide Area Network*
  - Connecting multiple facilities or City/Town network

- **VLAN** – *Virtual Local Area Network*
  - Logical separation for local networks
  - Segregates data of differing priority or use

- **VPN** – *Virtual Private Network*
  - Secure way to connect remote sites over untrusted networks
Remote Access

- Most municipalities and utilities are embracing remote access to better monitor, control and maintain their SCADA systems.
- Requires specific hardware and configuration to be completed safely and securely.
- User Administration – require credentials to access system remotely.
- Firewall – monitoring incoming and outgoing traffic.
System Architecture Drawing Example
SCADA Cybersecurity

- As with many concepts in our industry, defined by risk management and mitigation
- The ‘good guys’ are always a step behind the ‘bad guys’
- Not IF but WHEN
- Much of cybersecurity is minimizing impact and hastening recovery
Cybersecurity – Defense in Depth

- Multiple Layers of Security
- Establish a network protection strategy based on the principle of defense-in-depth
- Simply defending the perimeter is not enough.
  - If the perimeter defense is breached, the ‘gooey center’ is easily compromised.
- Including countermeasures at each level increases the chances to thwart an attack.
Cybersecurity – Areas of Concern

- **Intentional Attacks**
  - Foreign powers
  - Hacker Groups
  - **Disgruntled Employees / Ex-employees**
  - Goal is to damage equipment, inhibit production

- **Unintentional Attacks**
  - Amateur hackers
  - Malware/virus introduced through infected USB
  - Operator error at HMI causes system crash
Aspects of Cybersecurity

- Physical component
  - Doors, fences, cameras, locks, guards, mean-looking dogs

- Technological component
  - Network switches, firewalls, routers, software

- Administrative component
  - Policy, procedures, training, audits

- Internet of Things (IoT) Security
  - Staff mobile devices, Vendor equipment
Cybersecurity – Physical Security

- Port Restriction & USB / Ethernet
  - Group Policy (GPO)
  - Physical keys
  - Software disabling
Cybersecurity – Device Hardening & Logging

- PLC – Key in Run Mode
- PLC Firmware Updates (Planned)
- Password on all devices
- Turning off unused features/services
- Event auditing & data logging
Cybersecurity – Updates, Patching, Protection

▪ OS / Anti-virus (Windows 7 not supported!)
  ➢ Require updates in security plan
  ➢ Set patch reminders/schedule

▪ Application Whitelisting

▪ Firewalls

▪ Authentication

▪ VPN

▪ Intrusion Detection

- Cisco IDS4215-K9
- WatchGuard XTM 330
Account Management

- Encompasses both OS accounts (i.e. Windows) and HMI accounts (login information required to make process changes)
- ‘Everyone uses the same one’
- Shared account information
- Old accounts never disabled/removed
- Improper access levels
Password Management

- Default passwords on equipment not changed; available in easy to find manufacturer documentation
- Too weak, easy to guess
- No periodic change requirements
- Shared between multiple parties
- Not updated or changed during personnel turnover
Cybersecurity – Network Segmentation

- VLANs
- Switches
- DMZ
Firewalls

- Device or application that scans incoming traffic to detect and block malicious code
- Both network and host-based
- Often installed but configured improperly (or not at all)
- No periodic audit or update
- Logs not kept or reviewed to detect anomalies or issues
Information Technology (IT) vs. Operational Technology (OT)

- Often, support and maintenance of some or all aspects of a SCADA system are handled by the IT department.
- While IT and OT principles are very similar (80-90%), there are some significant differences that need to be understood.
- The mindset of IT professionals may not be completely applicable in the OT environment.
## IT versus OT

<table>
<thead>
<tr>
<th>Category</th>
<th>Information Systems</th>
<th>Control Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Impact</td>
<td>Loss of data</td>
<td>Loss of operation, production, life</td>
</tr>
<tr>
<td>Risk Management</td>
<td>• Recover by reboot</td>
<td>• Fault tolerance essential</td>
</tr>
<tr>
<td></td>
<td>• Safety a nonissue</td>
<td>• Explicit hazard analysis expected</td>
</tr>
<tr>
<td>Reliability</td>
<td>• Occasional failures tolerated</td>
<td>• Outages unacceptable</td>
</tr>
<tr>
<td></td>
<td>• Beta test in field accepted</td>
<td>• Quality assurance testing expected</td>
</tr>
<tr>
<td>Performance</td>
<td>• High throughput demanded</td>
<td>• Modest throughput acceptable</td>
</tr>
<tr>
<td></td>
<td>• High delay and jitter accepted</td>
<td>• High delay a serious concern</td>
</tr>
<tr>
<td>Security</td>
<td>• Most sites being insecure</td>
<td>• Priority to functionality and reliability</td>
</tr>
<tr>
<td></td>
<td>• Little separation among intranets on same site</td>
<td>• Tight physical security</td>
</tr>
<tr>
<td></td>
<td>• Focus on central server security</td>
<td>• IS network integrated with plant network</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Focus on central server as well as edge control device stability</td>
</tr>
<tr>
<td>Category</td>
<td>Information Systems</td>
<td>Control Systems</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>--------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>System Operation and Change</td>
<td>• Generic, typical operating systems</td>
<td>• Proprietary operating systems</td>
</tr>
<tr>
<td>Management</td>
<td>• Straightforward upgrades</td>
<td>• Software changes in consultation with vendors only</td>
</tr>
<tr>
<td></td>
<td>• Changes using automated deployment tools</td>
<td></td>
</tr>
<tr>
<td>Communications</td>
<td>• Standard communications protocols</td>
<td>• Mix of proprietary and standard communications protocols</td>
</tr>
<tr>
<td></td>
<td>• IT networking practices</td>
<td>• Networks requiring the expertise of controls engineers</td>
</tr>
<tr>
<td>Component Lifetime</td>
<td>Lifetime on the order of three to five years</td>
<td>Lifetime on the order of 15-20 years</td>
</tr>
</tbody>
</table>

"SCADA Cybersecurity Framework", Samir Malaviya, ISACA Journal Volume 1, 2014
Cybersecurity at odds with Information flow

- Access and flow of information always at odds with protection
Why Do SCADA Systems Need Cybersecurity Now?

- In today’s infrastructure environment, connectivity is king
- The ‘Internet of Things’ (IoT) is here to stay
  - More and more SCADA components will have the ability to connect over the Internet, either wired or wireless
- Remote access becoming more common and important
  - When you let the ‘good guys’ in, you need to make sure to keep the ‘bad guys’ out
THANK YOU!

QUESTIONS?

JT Trinward, P.E.
Woodard & Curran
jtrinward@woodardcurran.com
(207)558-4246