SCADA Data Redundancy for Compliance

Guelph Water's Approach

Graham Nasby, P.Eng, PMP, CAP
Water SCADA & Security Specialist
City of Guelph Water Services

2019 OWWA Ontario Water Conference
May 6-8, 2019 – Shaw Centre Ottawa – Ottawa, Ontario, Canada

About the Speaker

Graham Nasby, P.Eng., PMP, CAP
Water SCADA & Security Specialist
City of Guelph Water Services

- 10 years in the consulting sector
- Joined Guelph Water Services in 2015

- OWWA and WEAO Member, Member of OWWA Automation Committee
- Co-chair of ISA112 SCADA Systems standards committee
- Voting member of ISA101 HMI Design standards committee
- Voting member of ISA18 Alarm Management standards committee
- Named Canadian Expert on IEC/SCC-TC65 with Standards Council of Canada

- Guest instructor at McMaster University and Fleming College
- Has published over 40 papers and articles on automation topics
- Received University of Guelph “Mid Career Achievement Award” in 2014
- Named ISA’s technical division leader of the year award in 2013.

- Contact: graham.nasby@guelph.ca

So I got to live the dream!

Presentation Outline

- About Guelph Water
- SCADA Systems Review
- Data-Logging Requirements: O.Reg. 170
- Impact of SCADA Network & Data-Logging Outages

- SCADA Data-Logging design goals
- Guelph Water Solution: 3 layers of data-logging
- Time Synchronization
- PLC/RTU Redundancy
- Network Redundancy
- Server Redundancy

- Lessons Learned
- Best Practices Moving Forward

City of Guelph Water Services

- Guelph, Ontario, Canada
- 140,000 residents
- 21 groundwater wells
- 3 water towers

- 549 km of water mains
- 49,000 service connections
- 2,750 fire hydrants
- 35 unmanned facilities
- 46,000 m^3/day [12 MGD]
- 60,000 m^3/day peak [15 MGD]

Guelph Water Supply Operations

- Main Operations Centre: Woods
- 35 unstaffed facilities

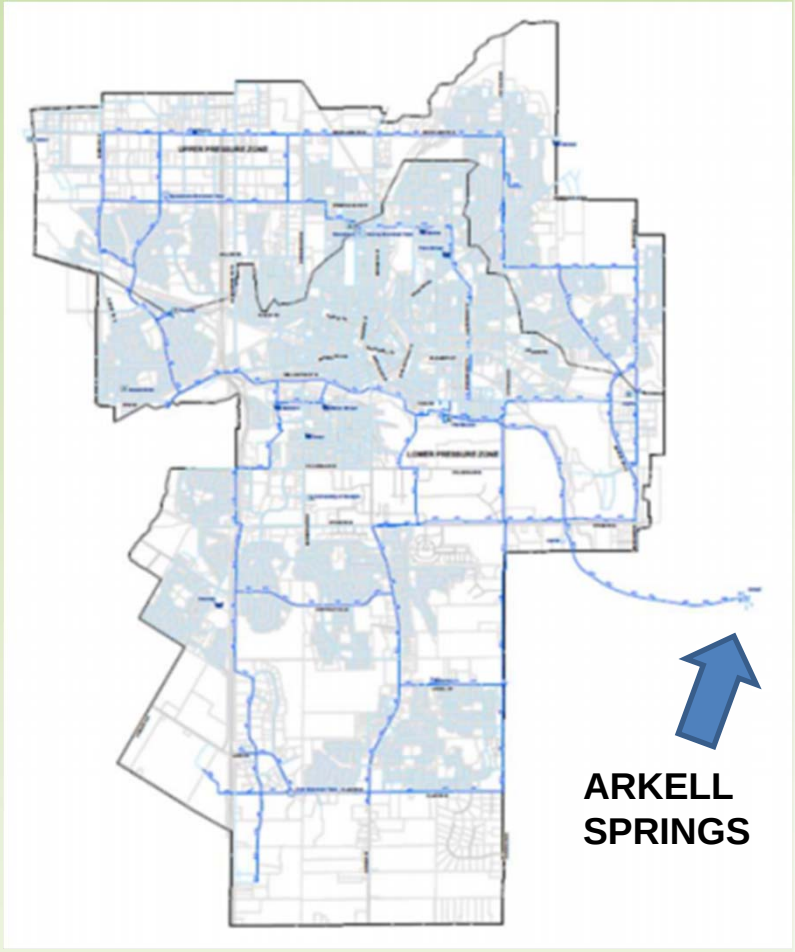
- Supply Operations
  - Staffed 8am-4pm Mon-Fri
  - On-Call Supply Operator evenings/weekends

- SCADA Interfaces
  - Central Control Room (always available)
  - Remote View Nodes at various facilities
  - Call-out alarms from SCADA system

- 30-40 minutes to drive across the city

Guelph Water Connected with SCADA

- Approx. 15km x 15km area
- 35 Facilities
  - 4 booster stations
  - 21 wells
  - 2 valve chambers
  - 3 water towers
  - 5 monitoring sites
- 40 PLCs plus 2 data centers
- Redundant Data-Logging
  - Traditional SCADA data-logging
  - QuickPanels with store/forward
  - DNP3 Data-loggers with store/forward
- High availability SCADA network
  - Primary: private fibre optic
  - Secondary: private wireless, with 45 second auto-failover

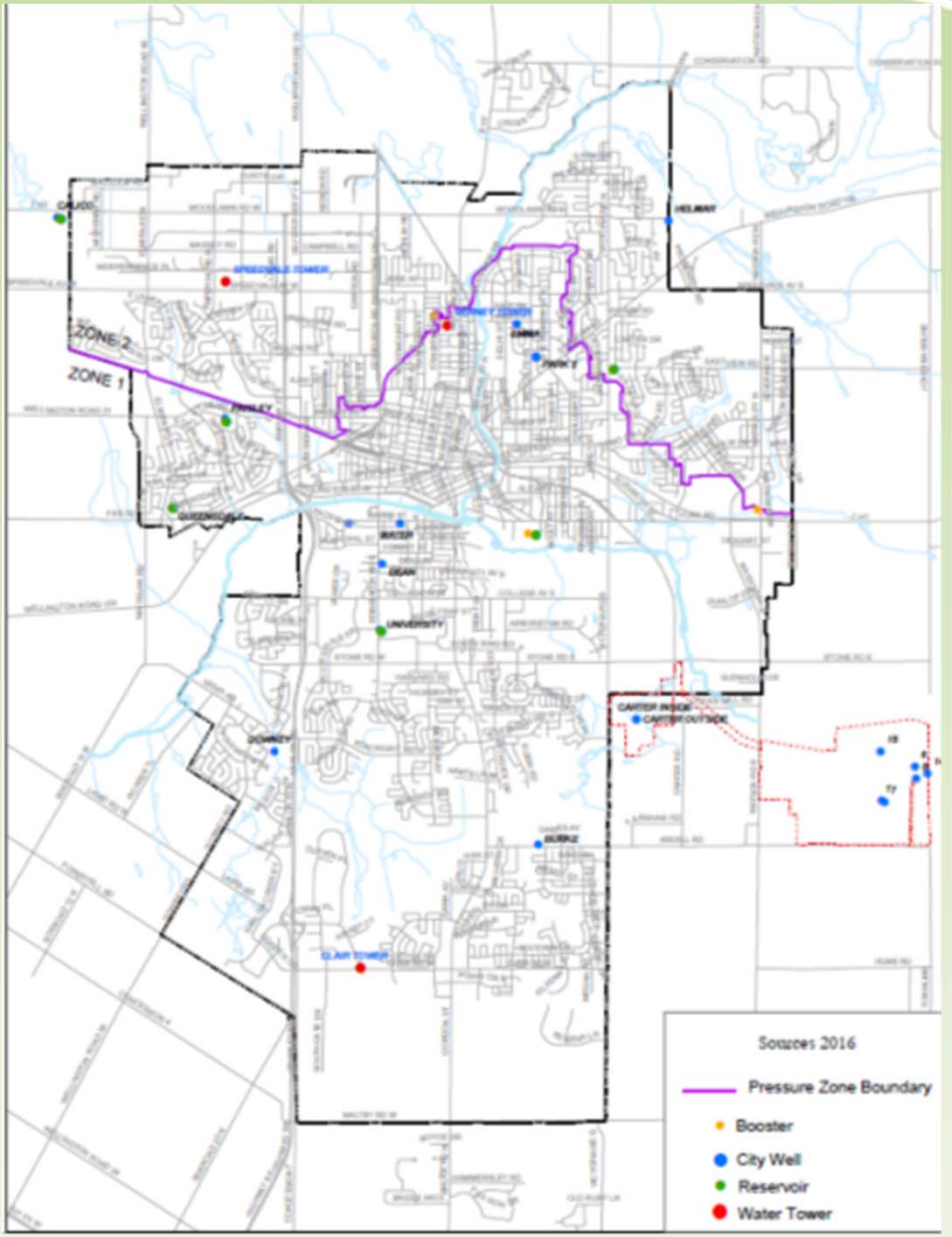


Water Supply Facilities

- Woods Station
  (Chlorine Bldg., UV Bldg., Reservoirs, Booster Station)

- Arkell Wells 1 & 7
- Arkell Well 6
- Arkell Well 8
- Arkell Well 14
- Arkell Well 15
- Carter Wells
- Diversion Chamber
- Dodds Valve Chamber
- Edinburgh Well
- Smallfield Well
- Water Street Well
- Emma Well
- Park Wells
- Clythe Station
- Paisley Station
- Membro Well
- Downey Well
- Verney Tower
- Burkes Well
- Arkell Well
- Clair Tower
- Clair Booster
- Robertson Booster
- Helmar Well
- University Well
- Dean Well
- Calico Well
- Speedvale Tower
- Scout Camp
- Queensdale Well
- Gazer Mooney Analyzer

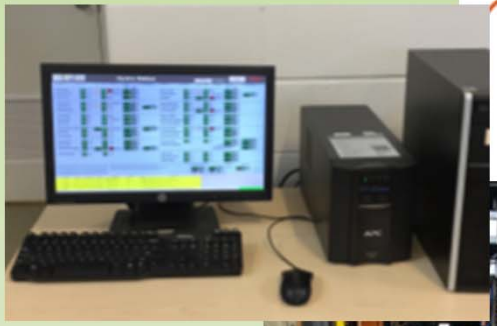
All sites are linked together with SCADA Network for remote control, automatic control, monitoring and logging.

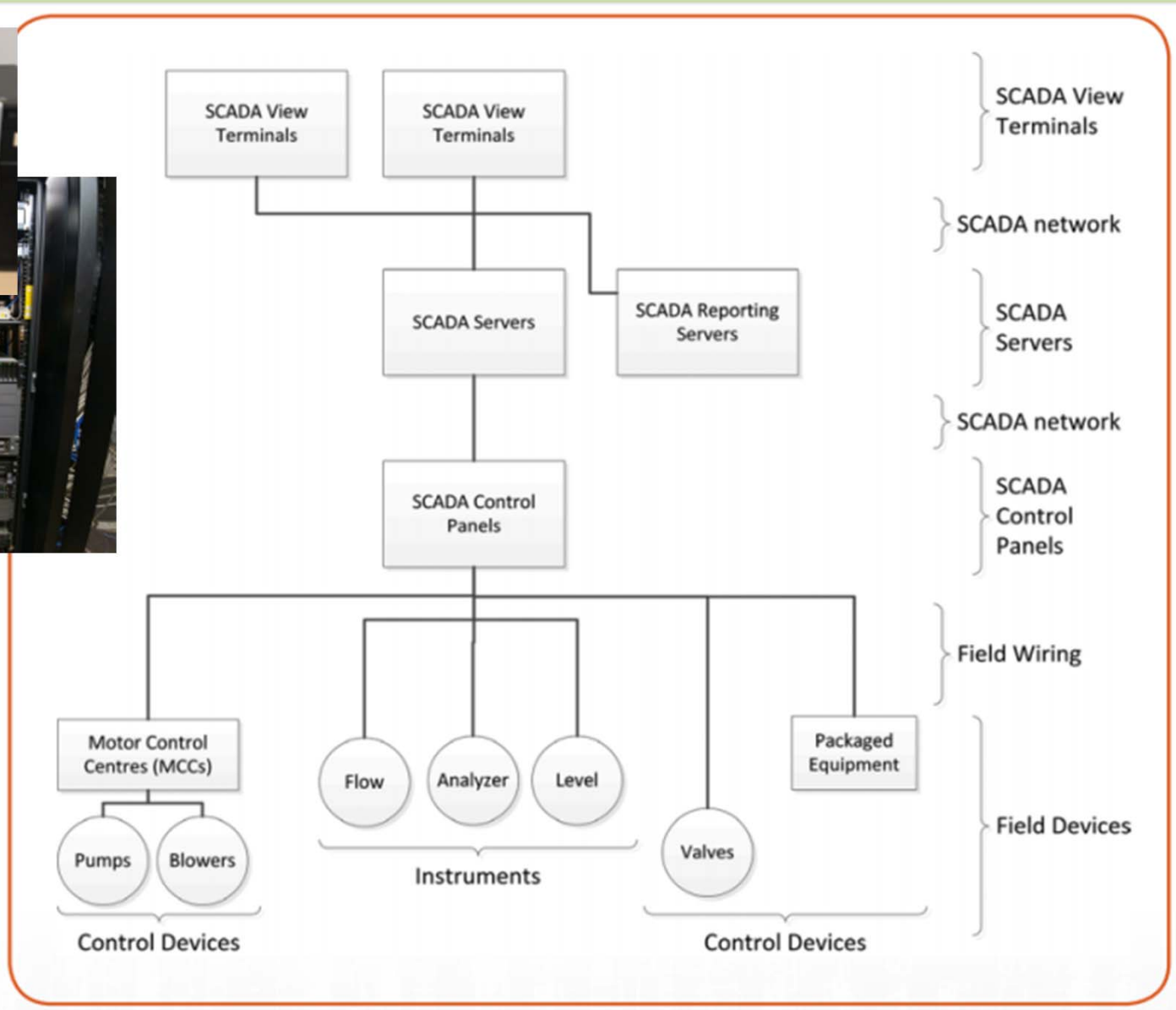


What is SCADA?

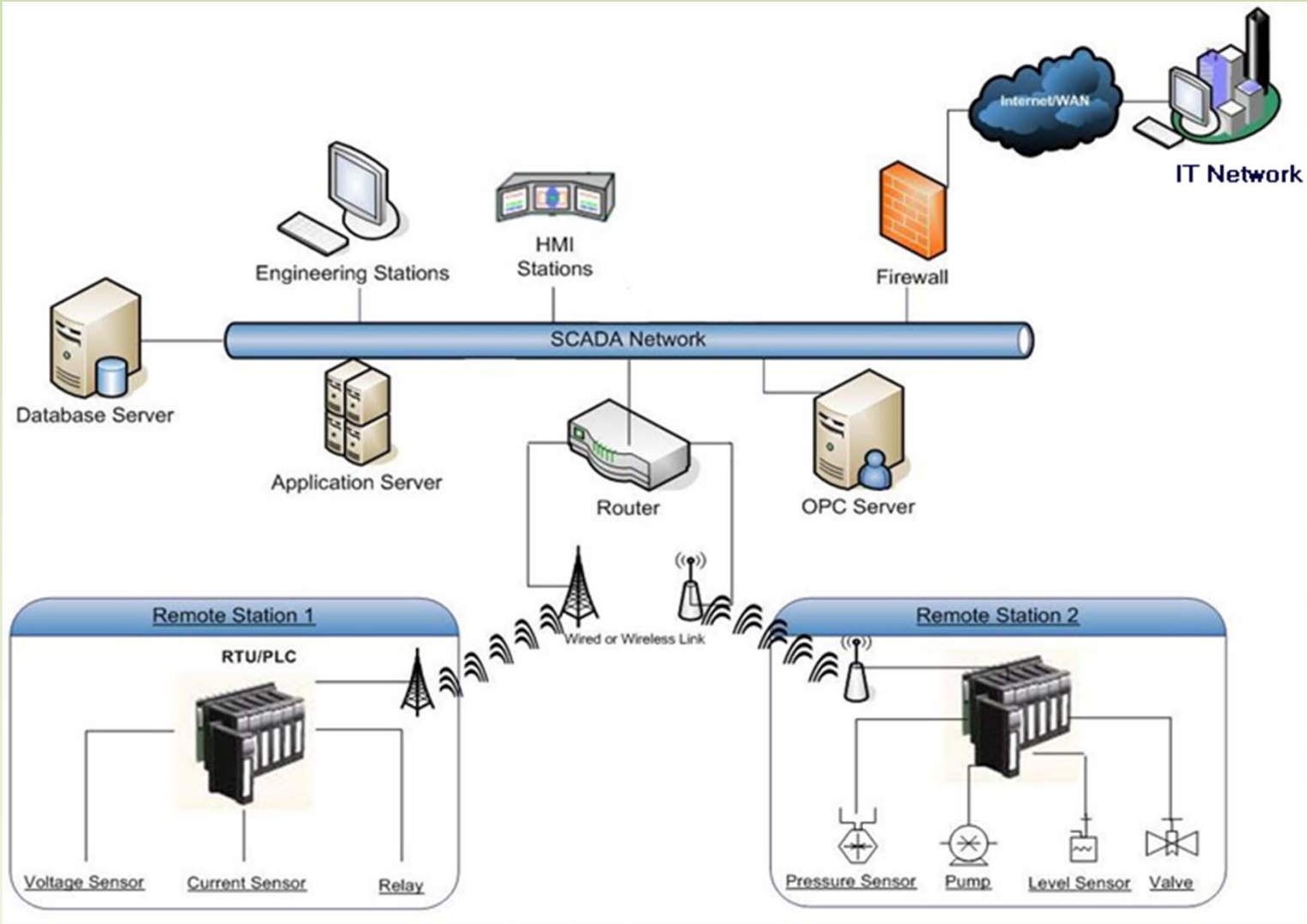
SCADA = Supervisory Control and Data Acquisition

Typical SCADA Architecture





Typical SCADA Network



Regulatory Requirements

- **O.Reg. 170 – Drinking Water Systems**
- Free Chlorine Residuals Must be Logged Minimum Every 5 minutes
- Filter Plants: Turbidity must be logged every 15 minutes
- Low chlorine/turbidity alarms must be communicated promptly

- Most IT Systems only reach 90 - 95% uptime (outages at night ok)
- SCADA system must be online 24/7, 365 days/year (outages not ok)
- **Very challenging to meet uptime requirements SCADA network**
- Less than 5 min downtime/year = 99.9995% uptime
- SCADA system has to be **10,000 X more reliable** than an IT system

From O.Reg. 170, Section 6.5

Continuous Monitoring

TABLE

Item	Parameter	Minimum Testing and Recording Frequency	Maximum Alarm Standard	Minimum Alarm Standard
1.	Free chlorine residual required to achieve primary disinfection	5 minutes	Not applicable	0.1 milligrams per litre less than the concentration of free chlorine residual that is required to achieve primary disinfection
2.	Free chlorine residual and total chlorine residual measured for the purpose of determining combined chlorine residual required to achieve primary disinfection	5 minutes	Not applicable	0.1 milligrams per litre less than the concentration of combined chlorine residual that is required to achieve primary disinfection
3.	Free chlorine residual in a distribution sample	1 hour	Not applicable	0.05 milligrams per litre
4.	Free chlorine residual and total chlorine residual measured for the purpose of determining combined chlorine residual in a distribution sample	1 hour	Not applicable	0.25 milligrams per litre
5.	Turbidity	15 minutes	1.0 Nephelometric Turbidity Units (NTU)	Not applicable

“Nines” Availability

I.T.

SCADA

Availability %	Downtime per year	Downtime per month	Downtime per week	Downtime per day
90% ("one nine")	**36.5 days**	**72 hours**	**16.8 hours**	**2.4 hours**
95% ("one and a half nines")	18.25 days	36 hours	8.4 hours	1.2 hours
97%	10.96 days	21.6 hours	5.04 hours	43.2 minutes
98%	7.30 days	14.4 hours	3.36 hours	28.8 minutes
99% ("two nines")	**3.65 days**	**7.20 hours**	**1.68 hours**	**14.4 minutes**
99.5% ("two and a half nines")	1.83 days	3.60 hours	50.4 minutes	7.2 minutes
99.8%	17.52 hours	86.23 minutes	20.16 minutes	2.88 minutes
99.9% ("three nines")	**8.76 hours**	**43.8 minutes**	**10.1 minutes**	**1.44 minutes**
99.95% ("three and a half nines")	4.38 hours	21.56 minutes	5.04 minutes	43.2 seconds
99.99% ("four nines")	**52.56 minutes**	**4.38 minutes**	**1.01 minutes**	**8.64 seconds**
99.995% ("four and a half nines")	26.28 minutes	2.16 minutes	30.24 seconds	4.32 seconds
99.999% ("five nines")	**5.26 minutes**	**25.9 seconds**	**6.05 seconds**	**864.3 milliseconds**
99.9999% ("six nines")	**31.5 seconds**	**2.59 seconds**	**604.8 milliseconds**	**86.4 milliseconds**
99.99999% ("seven nines")	**3.15 seconds**	**262.97 milliseconds**	**60.48 milliseconds**	**8.64 milliseconds**
99.999999% ("eight nines")	**315.569 milliseconds**	**26.297 milliseconds**	**6.048 milliseconds**	**0.864 milliseconds**
99.9999999% ("nine nines")	**31.5569 milliseconds**	**2.6297 milliseconds**	**0.6048 milliseconds**	**0.0864 milliseconds**

Impact of SCADA Datalogging / Network Outages

- Data Logging
  - Meeting the 5 minute chlorine data-logging requirement
- Process Visibility
  - Ability of Operators to “see” the status/trend of remote sites
- Speed of Response
  - Ability to make adjustments remotely vs. Driving a truck to site
- Automatic Control of Pumps based on Water Tower Levels
  - Requires PLC-to-PLC communications to work

- **SCADA Outages can be <u>very disruptive</u> to Operations**
  - Operator have to be on site to physically write-down residuals every 5 min
  - Operator stationed at a Water Tower to call in pump starts/stops via radio

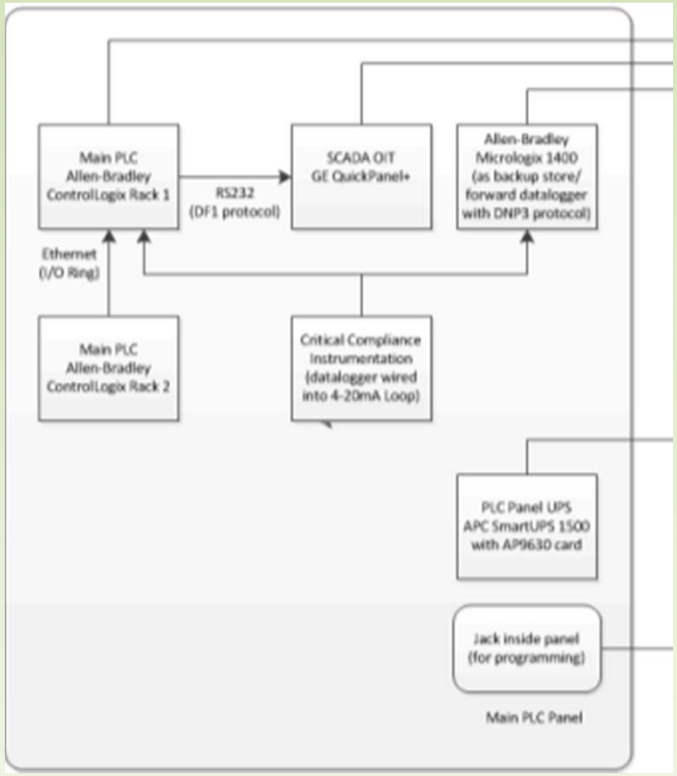
Guelph Water Data Redundancy Goals

- Ensure compliance with O.Reg. 170 data-logging requirements
- Avoid SCADA data gaps
- Be able to continue operating a site with confidence:
  - (a) if there is a SCADA network outage
  - (b) if there is a loss of any one data-logger
  - (c) always have at least two levels of data-logging active at all times

- Loss of any one facility or a server outage = no loss of data
- Ensure that logged data is always available with a self-serve tool
- Eliminate the need for manual data extraction from data-loggers

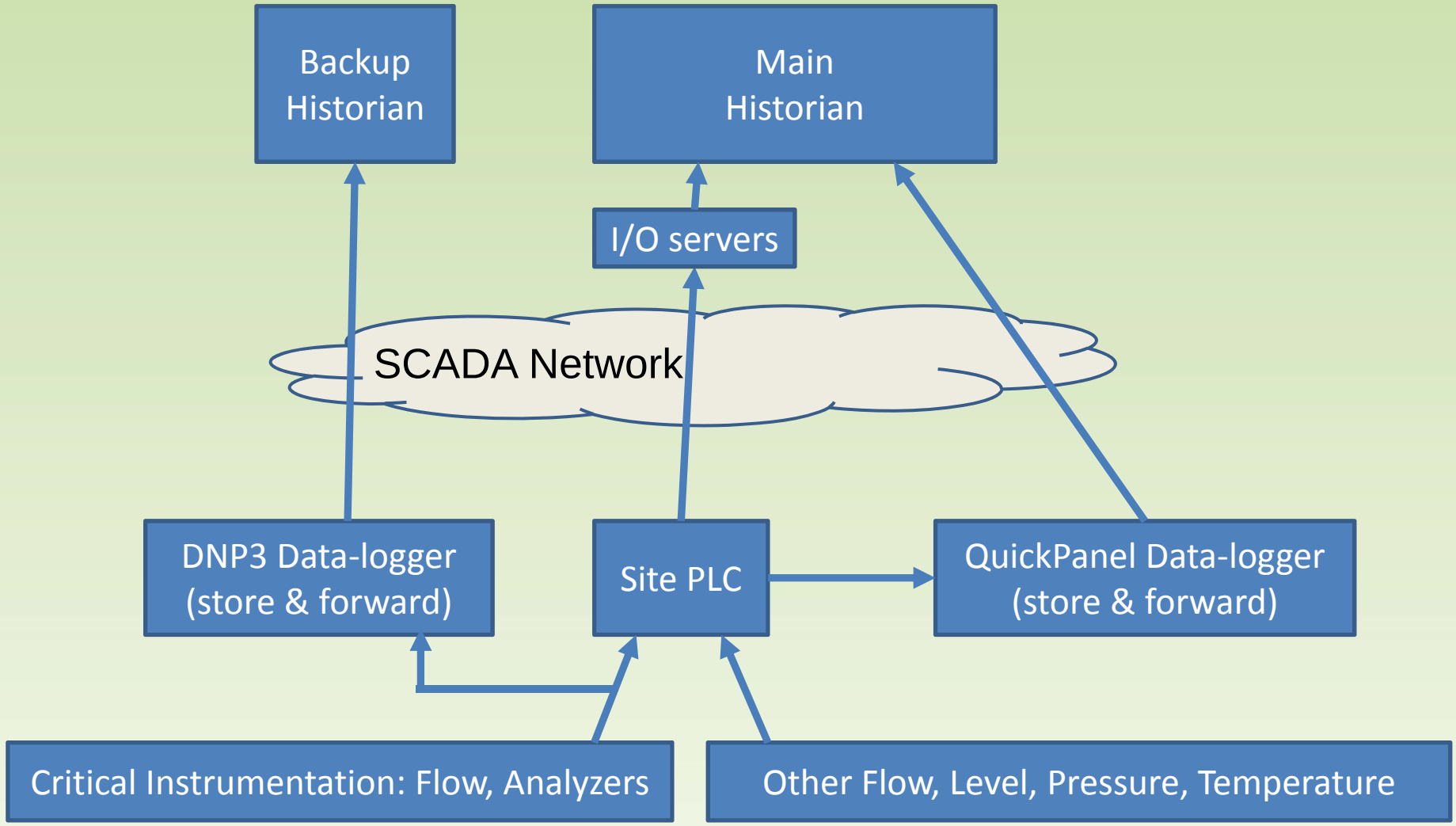
Back up Data-Logging

- No technology or person is perfect…
- So we have backup data-logging to guard against failures/mistakes

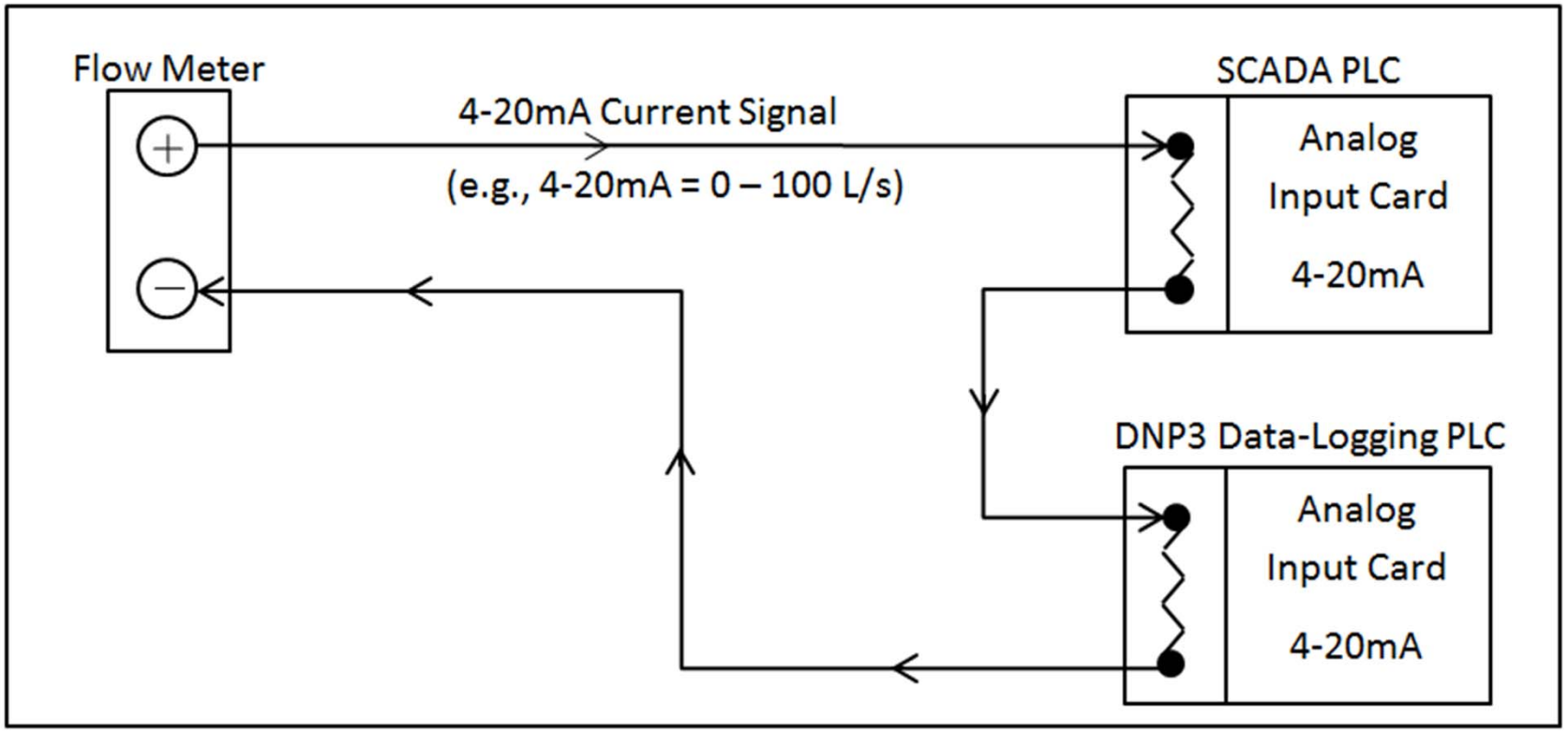


- **Primary Logging**
  - Facility PLC
  - SCADA server reads data in “real-time”
- **Backup Data-logging**
  - “QuickPanel” store/forward data-logger
  - Continuously logs into a buffer
  - Pushes data up to SCADA server
  - If no connectivity, stores timestamped data
  - When network connectivity restored, forwards logged data up to server
- **DNP3-based Data-loggers** New Technology

Guelph Water Data Logging Infrastructure



Wiring a DNP3 Data-Logger into the Loop



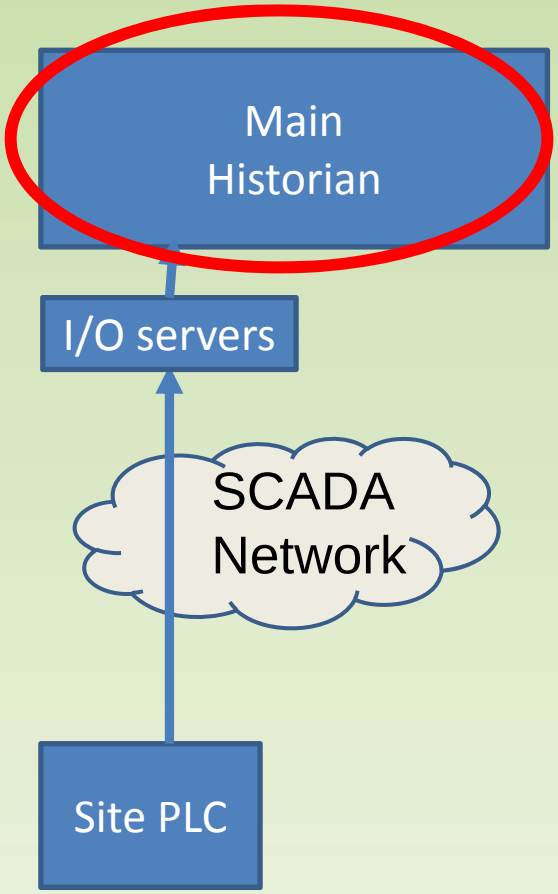
Wiring the DNP3 data-logger using the "wiring-into-the-loop" feature of 4-20mA analog signals.

Notice how if one PLC fails, its resistor allows the signal to continue flowing through the other PLC.

SCADA Systems require Time Synchronization

- **Backup Datalogging only works if date/timestamps are correct**
- **In SCADA Systems, all devices with clocks must be synchronized**
  - **PLC/RTUs, Dataloggers, Servers, Routers, OITs, VMs, Laptops, Nodes, Workstations**
- **Most common approach is to have a Time Server**
  - **Must Receive "time" from known-good time source**
    - **Several Options: Internet Time, GPS, Cellular Networks, Radio Sources**
  - **Time must be "distributed" to other servers/computers using NTP protocol**
  - **Operator Displays, Dataloggers, PLC/RTUs may use NTP or SNTP protocol**
  - **Some PLCs require a special time-sync protocol (e.g., CIP protocol)**

Datalogging Layer #1 – Traditional SCADA logging



- **Traditional SCADA System Logging**
- **Centralized SCADA servers**

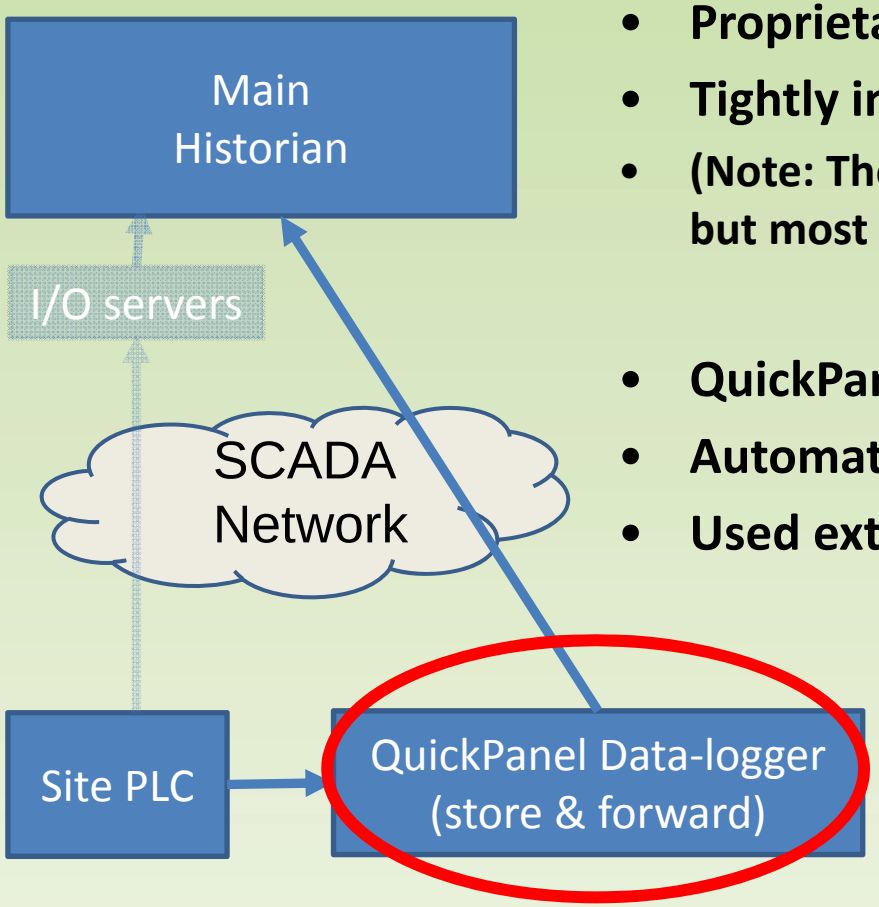
- **"Data Tags" which are used to send data to/from Operator Screens are also logged on set intervals**

- **Communications with PLCs are instantaneous**
- **"Data Tags" are configured to fetch updated values on set intervals (e.g., every 5 seconds)**
- **"Data Tags" are then configured to be logged into the Historian on set intervals (e.g., every 5 minutes)**

- **If a network connection is lost to a site PLC, no data can be displayed or logged from that site**

Data timestamping at server

Datalogging Layer #2 – GE QuickPanels



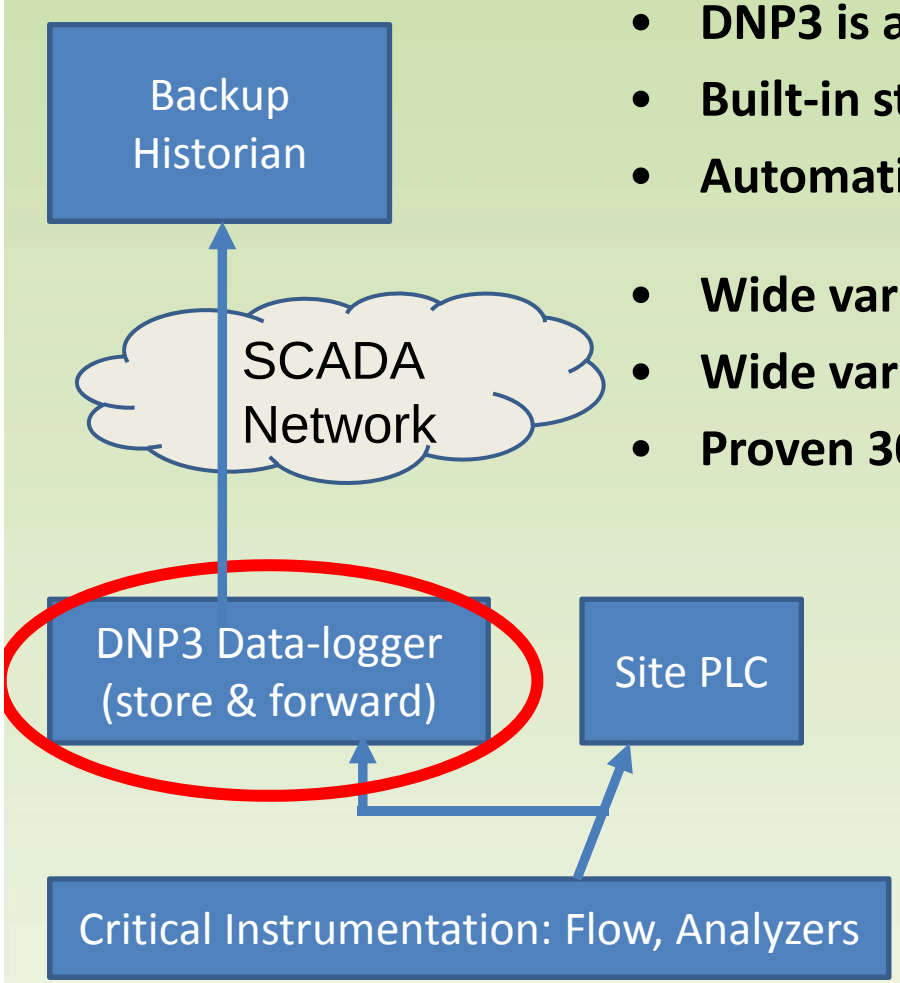
- **Proprietary Product**
- **Tightly integrated with the GE Historian**
- **(Note: There are alternative products from other vendors, but most require a computer or industrial PC at each site.)**

- **QuickPanels act as store/forward datalogger**
- **Automatic time synchronization with Historian**
- **Used extensively throughout Ontario**

- **During a network outage, the QuickPanel will continue logging its "data tags" on a configured interval**
- **When connectivity is restored, the QuickPanel automatically uploads data records to the Historian**

Data timestamping at QuickPanel

Datalogging Layer #3 – DNP3 Dataloggers



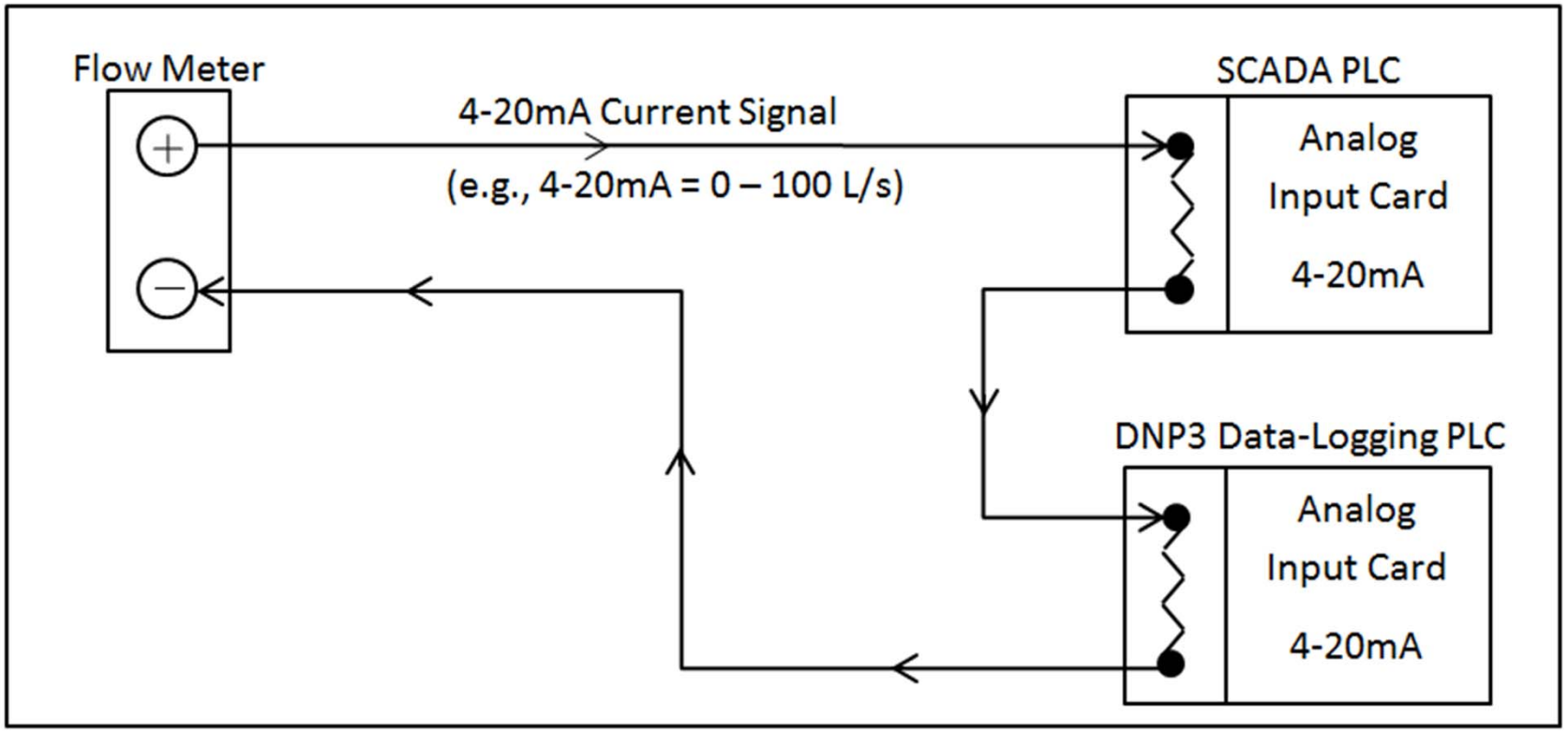
- DNP3 is a publicly available protocol
- Built-in store/forward datalogging
- Automatic time synchronization

- Wide variety of PLC/RTU options (act as dataloggers)
- Wide variety of historians that support DNP3
- Proven 30-year track record in Electric Power Industry

- During a network outage, the DNP3 Data-logger will continue logging its "data tags" on a configured interval
- When connectivity is restored, the DNP3 Data-logger automatically uploads data records to the Historian
- We "wire logger into the loop" to avoid single point of failure with site PLC

Data timestamping at DNP3 Data-logger

Wiring a DNP3 Data-Logger into the Loop



Wiring the DNP3 data-logger using the "wiring-into-the-loop" feature of 4-20mA analog signals.

Notice how if one PLC fails, its resistor allows the signal to continue flowing through the other PLC.

Why use DNP3 protocol for Data-logging?

- **Automatic store/forward data logging is built into the protocol**
- **Timestamping data at the device/instrument**
- **Automatic Time synchronization with Server**
- Both “log on time interval” and “log on change” logging supported
- Data Quality Flags

- Supports both Encryption and Authentication
- Automatic Error checking of data packets
- Prioritized Communications (Tags can be grouped in classes 0-4)
- Variety of networks supported: Ethernet, Serial, ATM, Cellular, etc.
- Supports wide range of analog, digital, and structured datatypes

SCADA Network Redundancy

- **Having Robust SCADA network makes data-logging more robust!**
- Adding redundancy to SCADA networks is now much easier

- Guelph Water SCADA Network
  - Dual connections at all sites
  - Primary: Private MPLS Fibre-optic connection
  - Secondary: Private Cellular Network, also running MPLS
  - BGP (Border Gateway Protocol)
  - If Primary connection goes down, the Secondary takes over in 45 secs

- The technology and affordability of building redundant networks has improved greatly
- There are other utilities in Ontario using Cellular+Cellular and DSL+Cellular options
- Special attention has to be paid to how the routers are set up. Must be automatic.

SCADA Network Redundancy Options

- **There are numerous SCADA network technologies out there**
  - **Fibre optic (public)***
  - **Fibre optic (MPLS)**
  - **Fibre optic (utility owned)**
  - **Cellular / Wireless***
  - **DSL (private or public)***
  - **Ethernet over Cable***
  - **Radios – licensed***
  - **Radios – unlicensed***
  - **Bell Lines**
  - **Private Cables**
  - **?**

*these approaches usually require extra VPN routers/firewalls be used

Server Redundancy

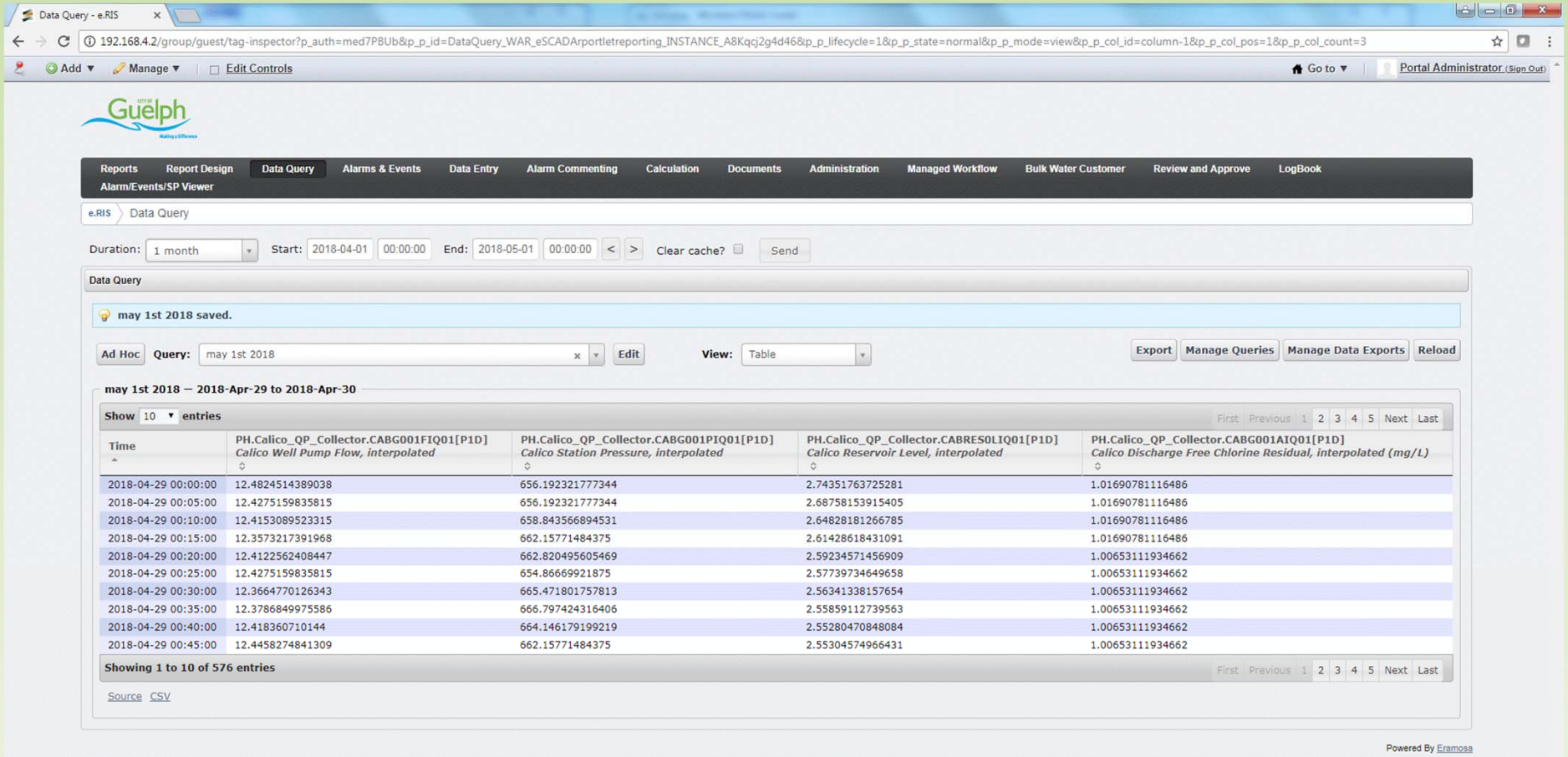
- Don’t put all your eggs in one basket!
- Frequent and automated backups are recommended

- Guelph Water approach
  - Main Process Historian (Primary Datalogging, QuickPanels)
  - Backup Process Historian, different server technology (DNP3 data-loggers)
  - Backup system that takes “snapshots” of the historians 4 times a day
  - Use of a Virtualized Server environment that makes server updates easier
  - Use of RAID for server storage, and off-site backup locations
  - Alternate data centre with standby servers, always ready in case of issue at main site

Traditional approach of just one centralized historian to rule them all is not recommended.

Some utilities now use layered historians, where higher level historians keep replicate copies of data.

Accessing your Logged Data

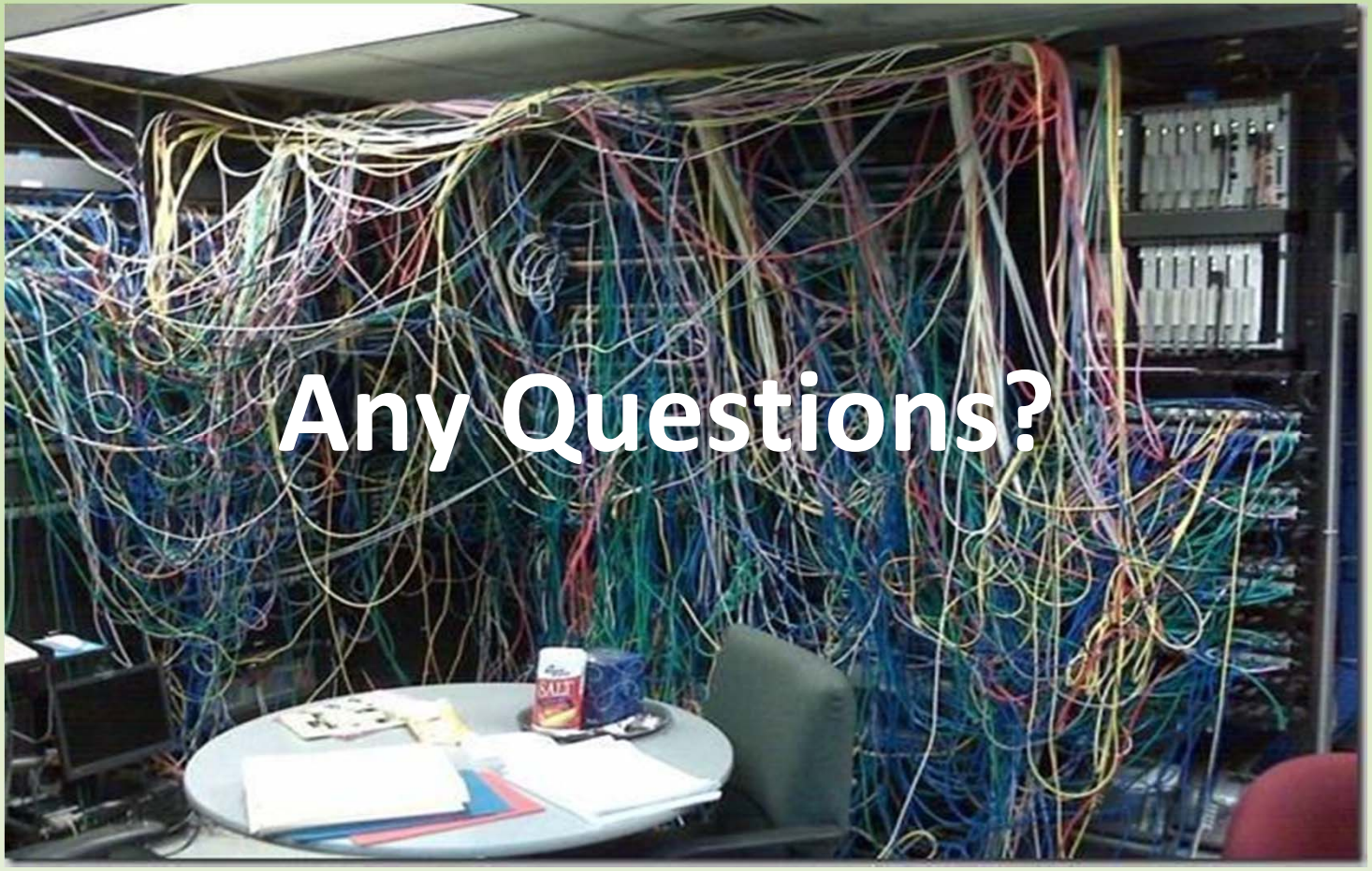


A web-based tool is used to make all data <u>always</u> accessible to water utility staff.

Take Aways

- A functioning SCADA system is critical for operations
  - Data-logging is needed to meet requirements of O.Reg. 170
  - Having redundant store/forward datalogging is recommended
  - Design SCADA systems with redundancy: PLC/RTUs, Network, Servers, Backups
  - SCADA outages can be very disruptive to operations and have compliance risks
- The Uptime requirements for SCADA systems are very high
  - A typical SCADA system has to be 10,000X more reliable than an IT system
  - O.Reg. 170 requires chlorine residual logging every 5 minutes (no exceptions!)

1. **Use redundant data-logging to guard against equipment/network failures**
2. **Consider using a redundant wide-area SCADA network with automatic failover**
3. **Look at DNP3 protocol to add redundancy for store & forward data logging**
4. **Think about how your operations/compliance team will get access to the data**



* Not a High Performance SCADA System

Graham Nasby, Water SCADA & Security Specialist
graham.nasby@guelph.ca