Chasing the White Rabbit…

Why Time Synchronization for OT and SCADA systems is a lot harder than it seems

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

Members Meeting (virtual lunch & learn) – ISA New Jersey Section
April 26, 2022 – International Society of Automation – New Jersey, USA – www.isanj.com

About the Speaker

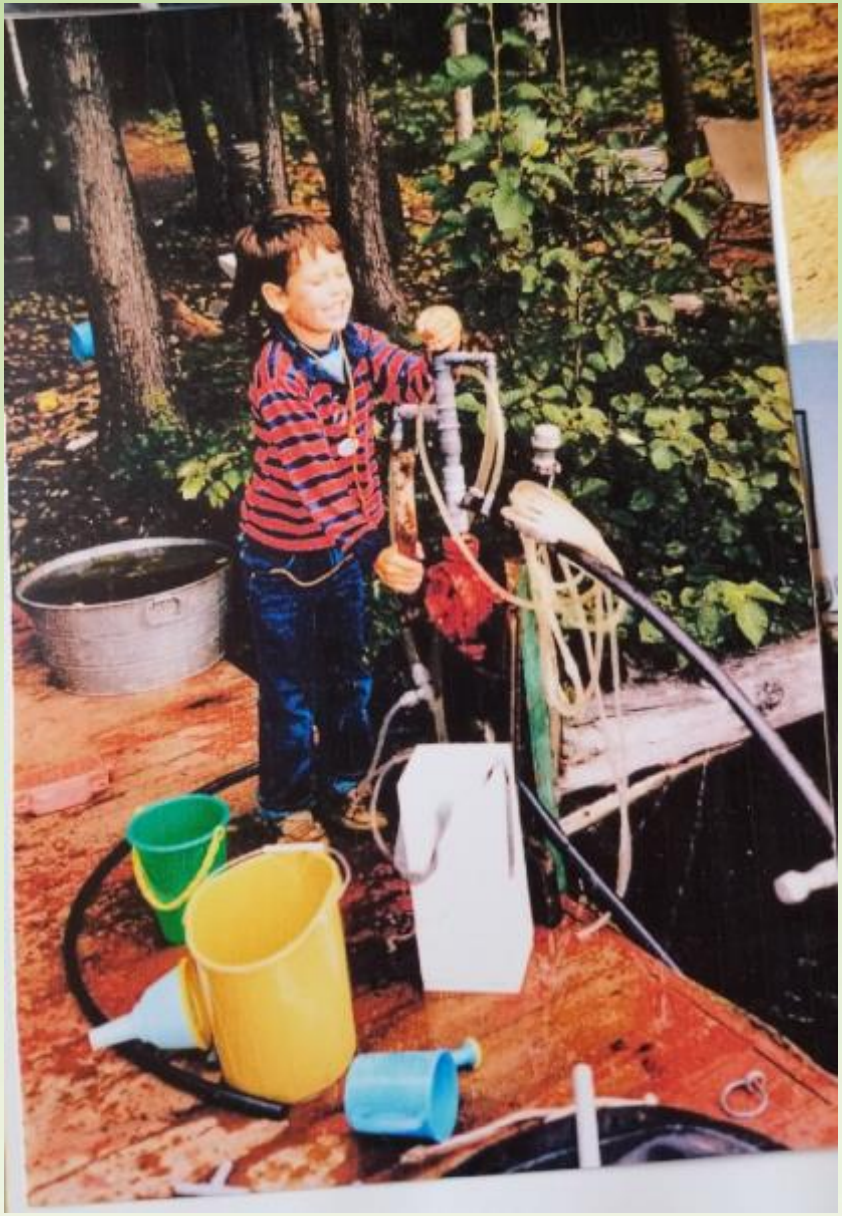
Graham Nasby, P.Eng., PMP, CAP
Water SCADA & Security Specialist
City of Guelph Environmental Services

- 20 years experience in operations, construction and automation sector
- Joined Guelph Water Services in 2015

- Co-chair of ISA112 SCADA Systems standards committee
- Voting member of ISA101 HMI Design and ISA18 Alarm Management committees
- Past Section President, Division Director, Technical VP within ISA at the society-level
- Member of IEC/SCC TC65A "Industrial process measurement, control and automation"
- Member of CSA P125 "Operational Technology: Functional Safety and Security"
- Active volunteer with American Waterworks Association and Water Environment Federation

- Sessional instructor at McMaster University (Hamilton, ON) and Conestoga College (Cambridge, ON)
- Has published over 50 papers and articles on automation topics
- Received ISA's technical division leader of the year award in 2013
- Received "Mid-Career Achievement Award" from his *alma mater* University of Guelph in 2014
- Recipient of the ISA's society-level Standards Excellence award in 2021

- Contact: graham.nasby@grahamnasby.com .



I wanna be a Water Guy when I grow up!

Presentation Outline

- How we use Time in OT & SCADA systems
- Compliance data needs correct time/date-stamps
- What Needs Synchronizing

- Technical Introduction to Time (& Some History)
- Local Time Zones, Daylights Savings Time
- Time Sources

- Time Synchronization Protocols
- Sample “Time Distribution” architecture
- Using Time Synchronization in SCADA Systems
- How Guelph Water Synchronizes time in its SCADA system
- Best Practices & Take-Aways

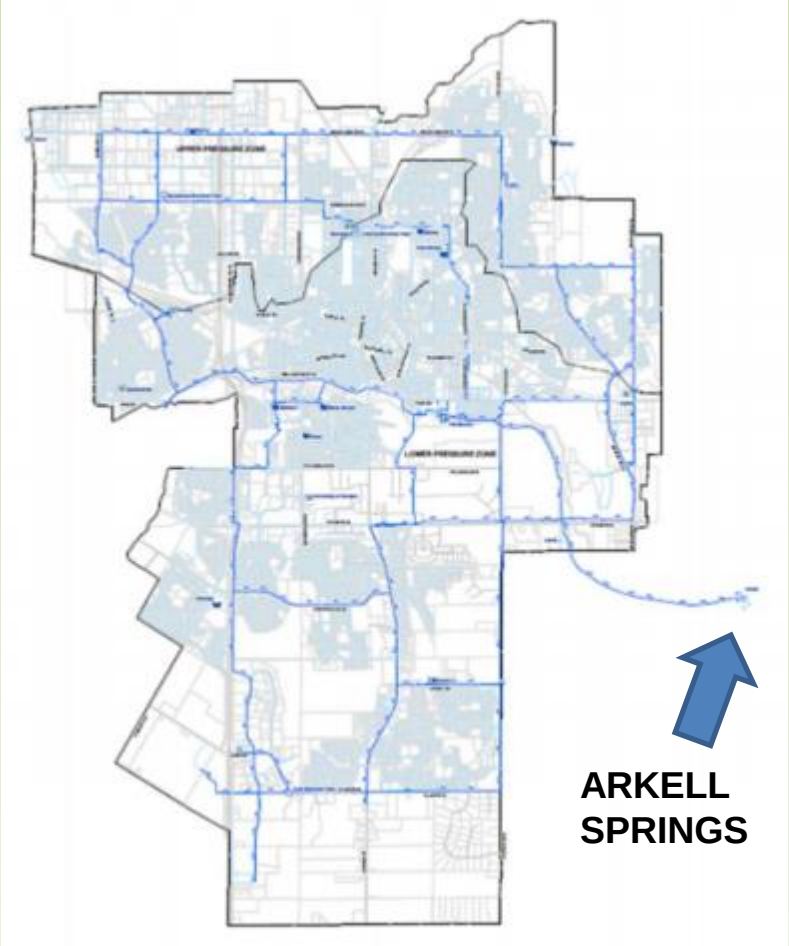
City of Guelph Water Services

- 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 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

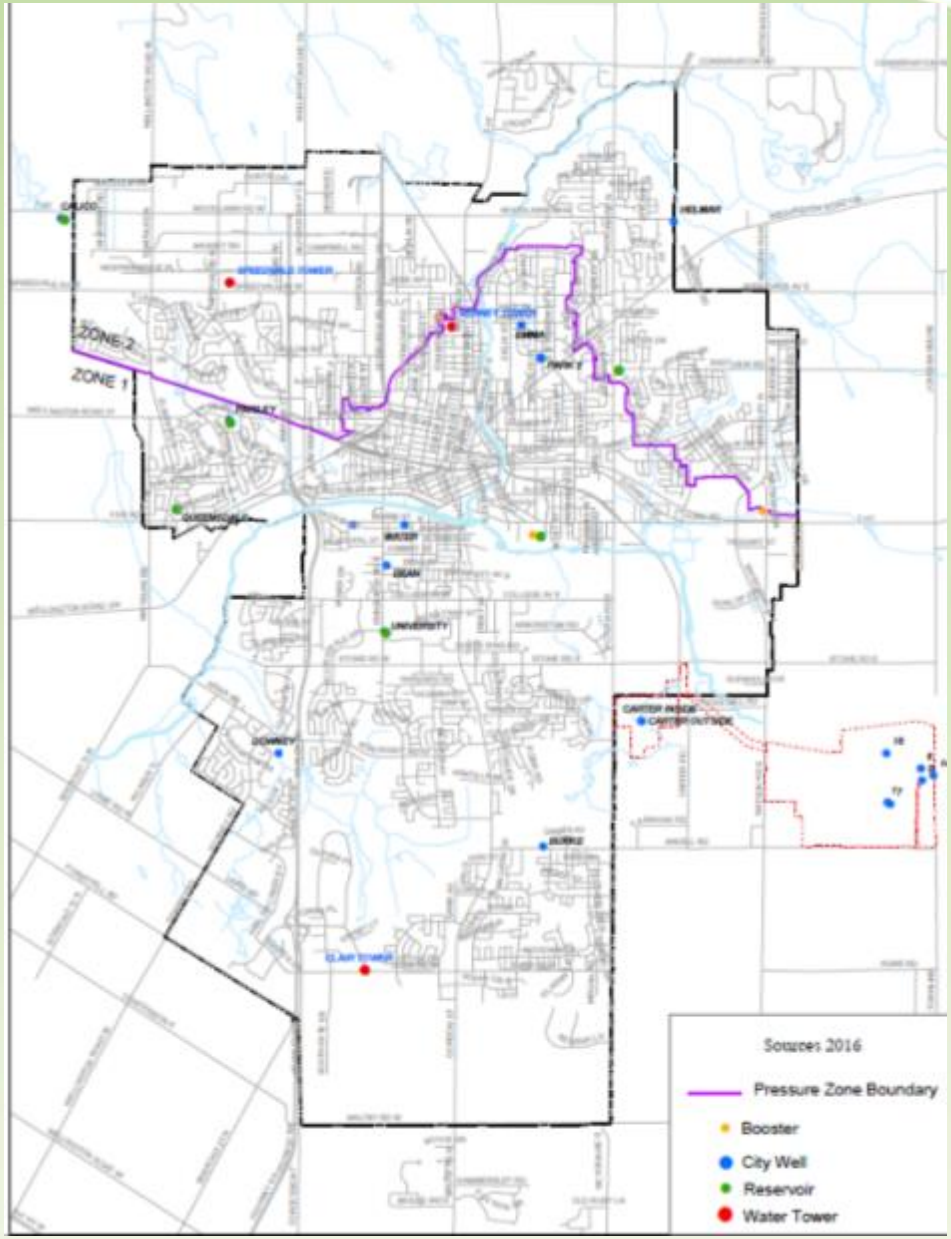


Water Supply Facilities

- 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

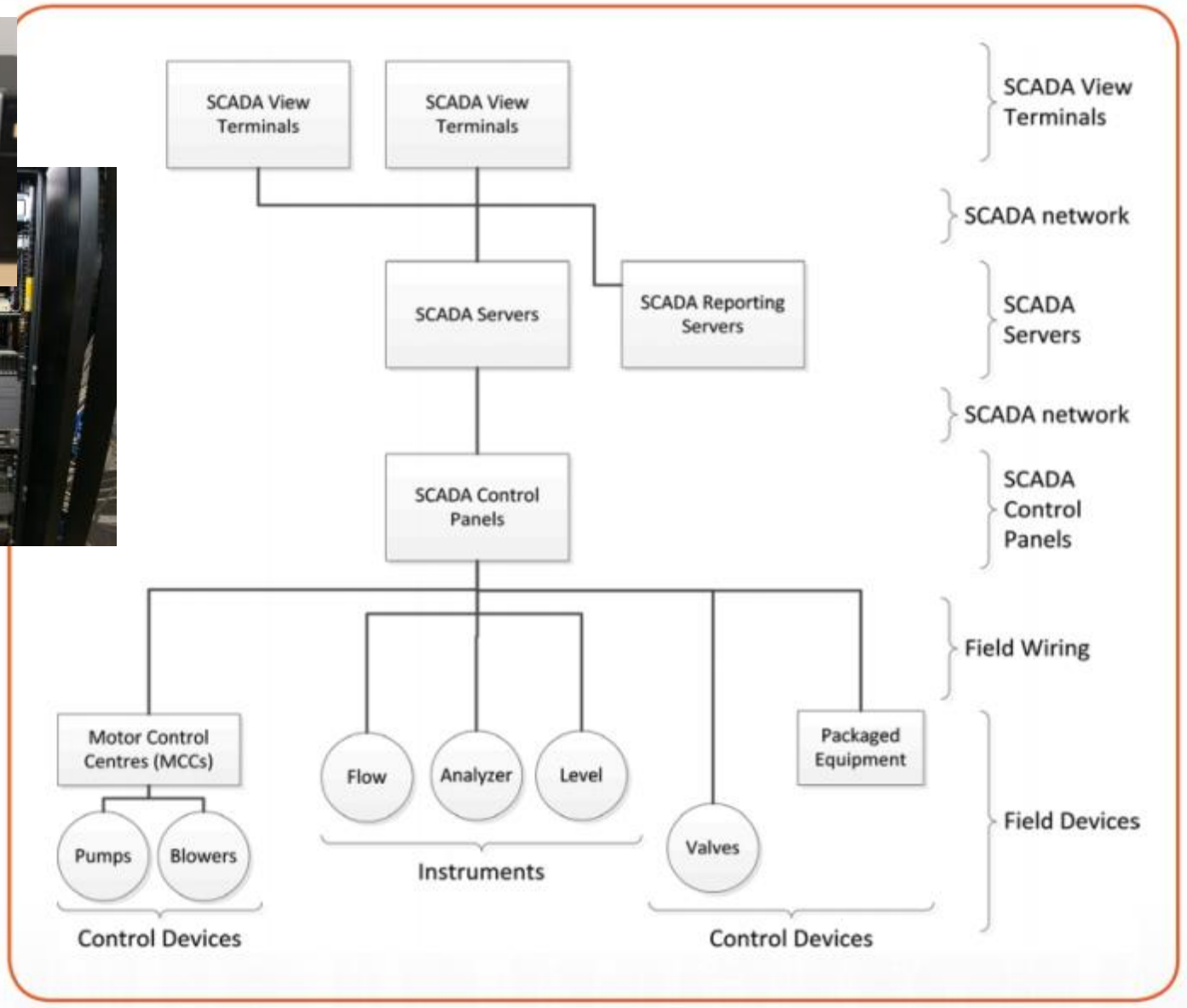
All sites are linked together with SCADA Network for remote control, automatic control, monitoring and logging.



What is SCADA?

SCADA = Supervisory Control and Data Acquisition

Typical SCADA Architecture



How Time is used in SCADA Systems

- **Time/Date-stamp logged data**
  - In Historian, In PLCs, In Dataloggers
- **Backup Data Logging**
  - If clocks are not perfectly time synchronized, backup logging does not work
- **Daily Flow Totalization**
  - Start/End of Each day, Daily Flow Totals
- **Time-based Control**
  - Alarm Call Out Systems: Who it Calls First
  - Reservoir and Tower Filling
  - Filter Backwashes
  - Time of Day Peaking Wells
  - Automated Backups
- **Report Generation**
  - Select date/time ranges
  - On-Demand & Auto-Generated Reports

SCADA Datalogging – Water Sector Example

- **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

- Process Values needed to prove primary disinfection
  - E.g., Levels, Flow Rates, Chlorine Concentration, UV Dose, etc.

Meaning: Timestamps on logged data must be correct.

SCADA Data Logging – Water Sector Example (cont'd)

From O.Reg. 170, Section 6.5 – a drinking water regulation from Ontario, Canada

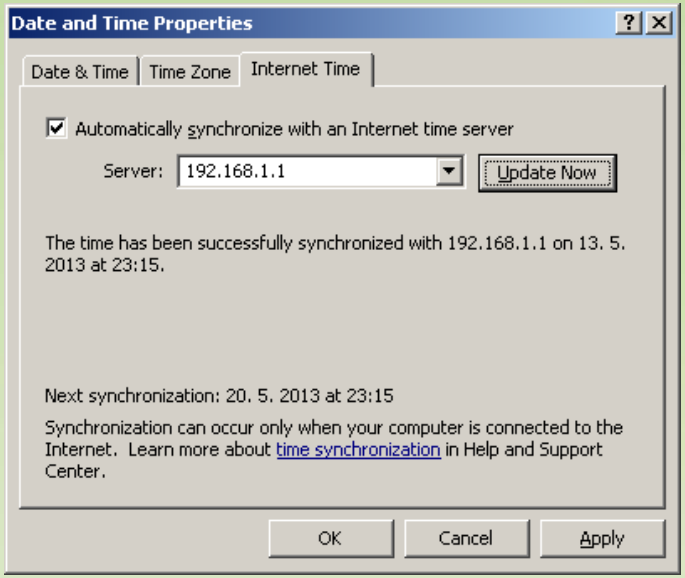
Continuous Monitoring

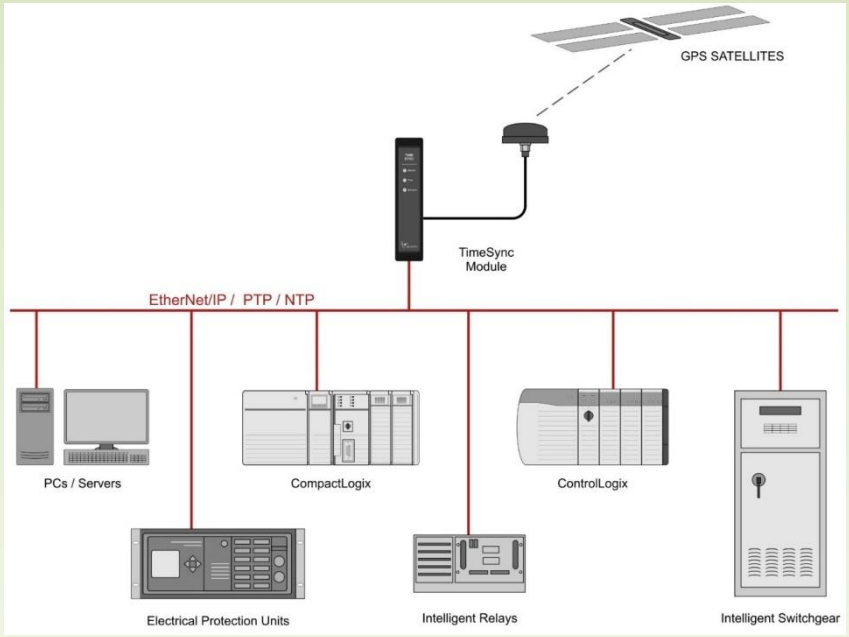
TABLE

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

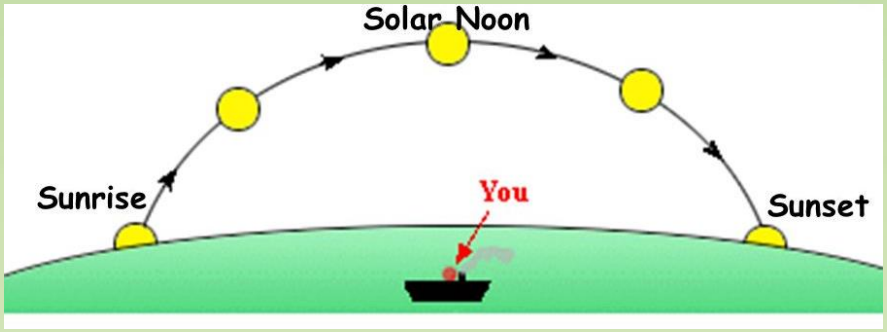
What Needs Time Sync?

- SCADA Servers
  - Data Gathering Machines
  - Historians
  - View Nodes
  - Reporting Systems
  - Backup Systems
- SCADA View Nodes
- Network Routers/Switches
- PLC/PAC/RTU
- Dataloggers
- Instrumentation with Logging



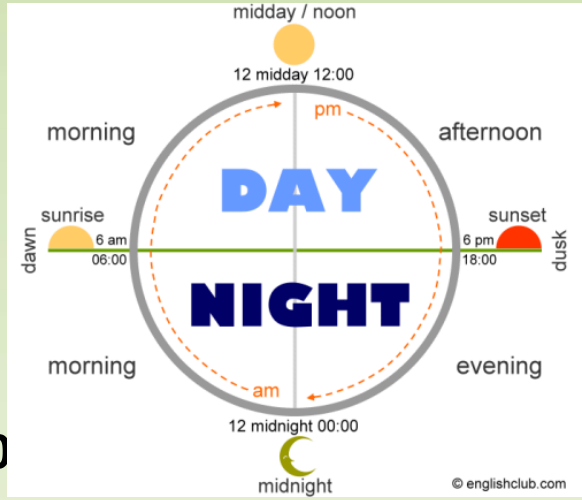


What is Time?



Local Solar Time

- 24 hours in a day
- With 12noon being the sun at its highest

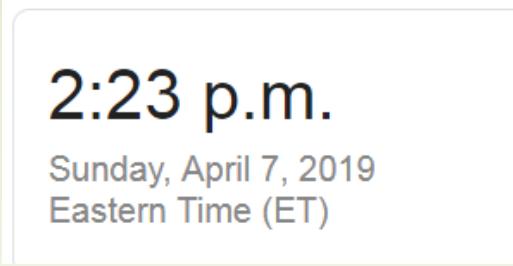


Local Time

- A “local solar time” that is picked for each area
- Will be part of a “Time Zone”
- Expressed as an offset from “UTC Time”
- Canadian Daylight Savings Eastern Time is UTC-04:00

UTC Time

- The local time at Greenwich
  (an observatory near London UK)



Note: The actual technical definitions for time are more complex -- this us just an introduction.

Local Time Means using Time Zones

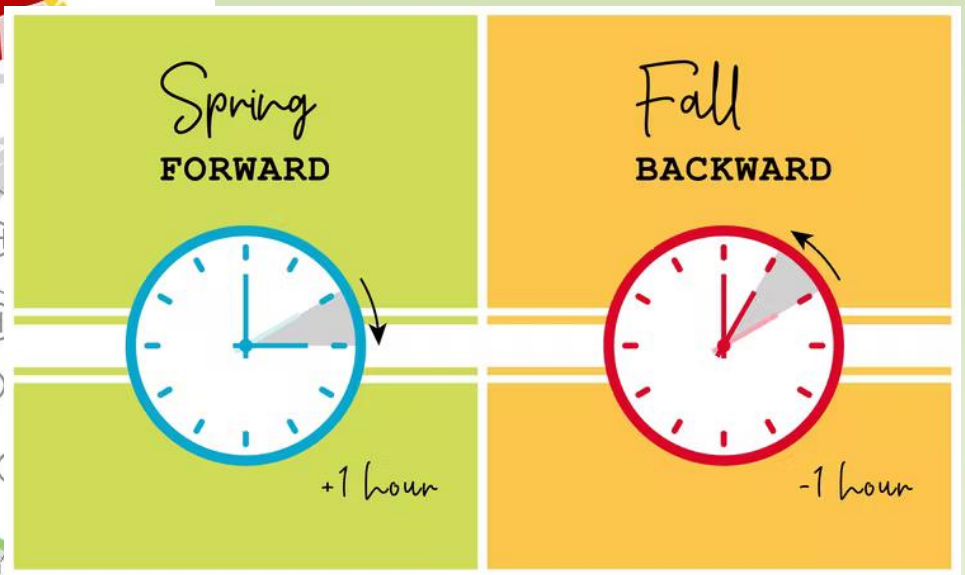


Image courtesy of whatsanswer.com

Remember Greenwich?

- Observatory built near London in 1675, by order of King Charles II
- Built to precisely measure “local solar noon”
- “Greenwich Mean Time”
- (now called UTC = universal coordinated time)

- Red ball drops at 1:00 PM every day
- Use by ships to synchronize their clocks
- Ship navigation depends on precise time

- Red Ball was an early method for “time synchronization”

Note: The actual technical definitions for time are more complex -- this is just an introduction

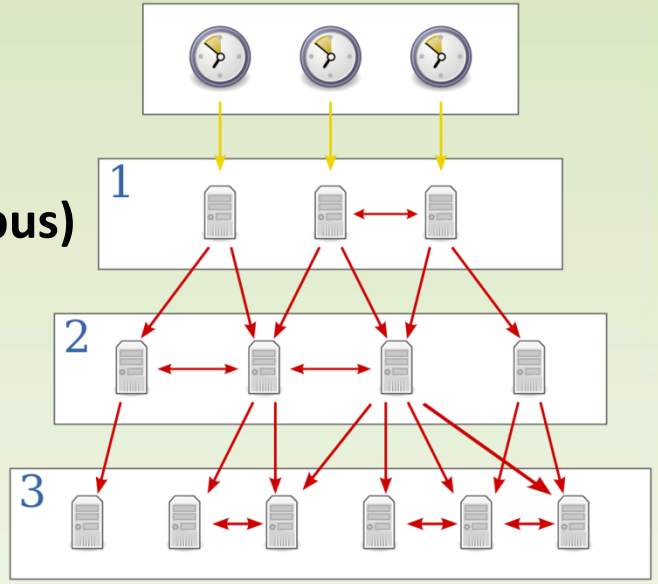
Modern Time Sync Protocols

General Ethernet Networks

- **NTP = network time protocol (approx. 1ms accuracy)**
- SNTP = simple network time protocol
- PTP = precision time protocol (<1ms accuracy)
- w32time = propriety protocol used by Window XP, Server2003

Control System Networks

- **Proprietary network protocols (e.g., CIP, GE, etc.)**
- **DNP3 = has time synchronization built in**
- **Some fieldbus protocols have time sync (e.g., profibus)**



Radio

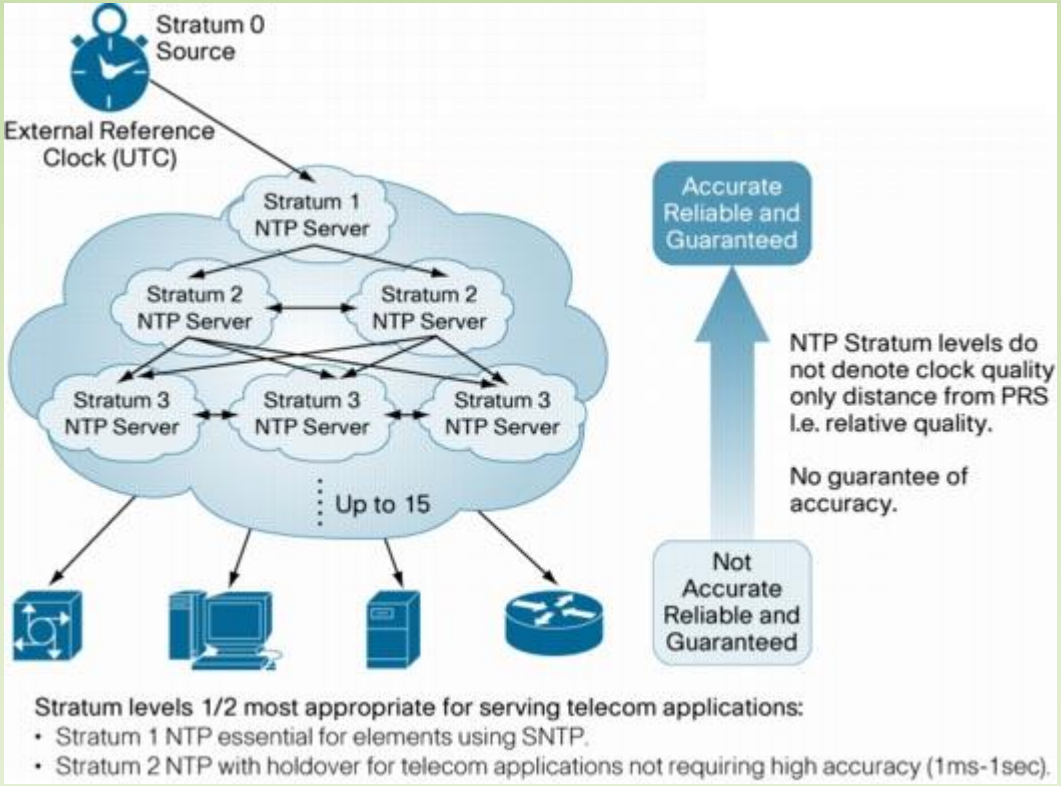
- **Atomic Clock Broadcasts** (e.g., WWV from Colorado)

Hardwired Signals

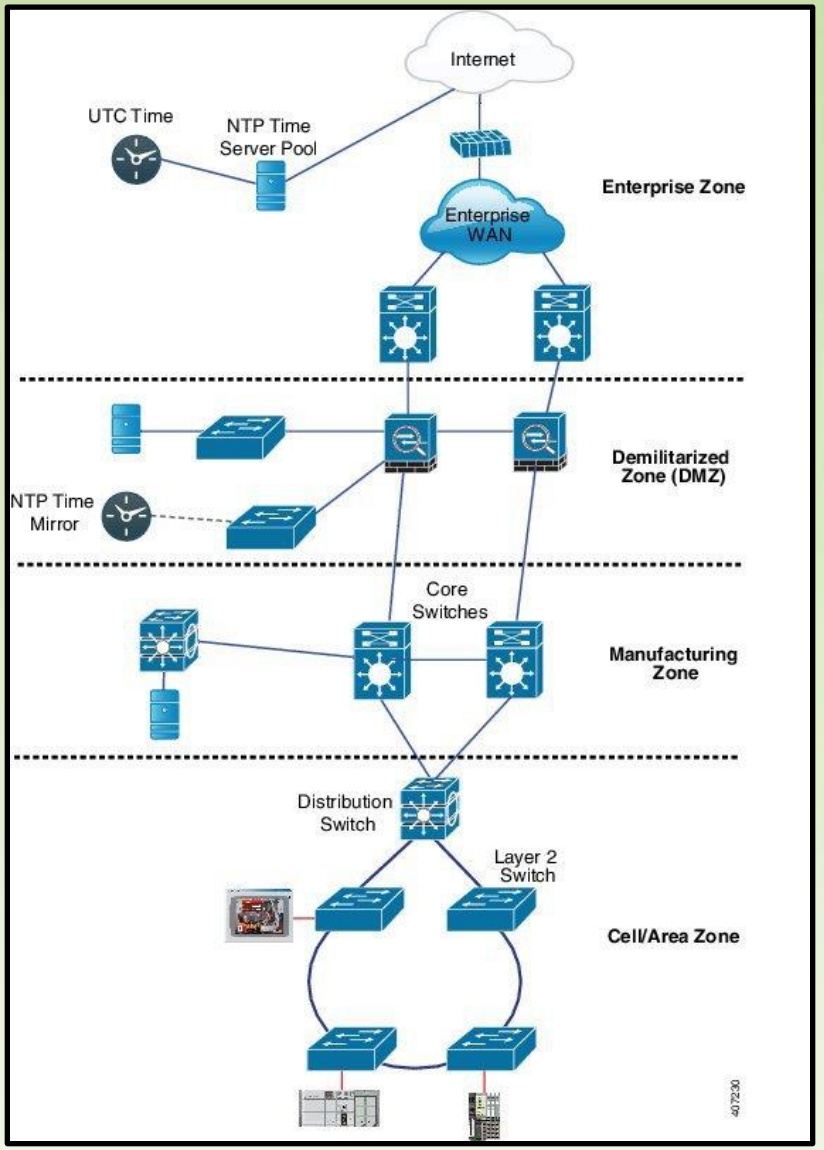
- **IRIG B, Pulse, Sine Wave, etc.**

Note: The actual technical definitions for time are more complex -- this is just an introduction

Typical Time Distribution Architecture



Source: Symmetricom / Microsemi



How to apply this to a
SCADA control system network

Source: Cisco

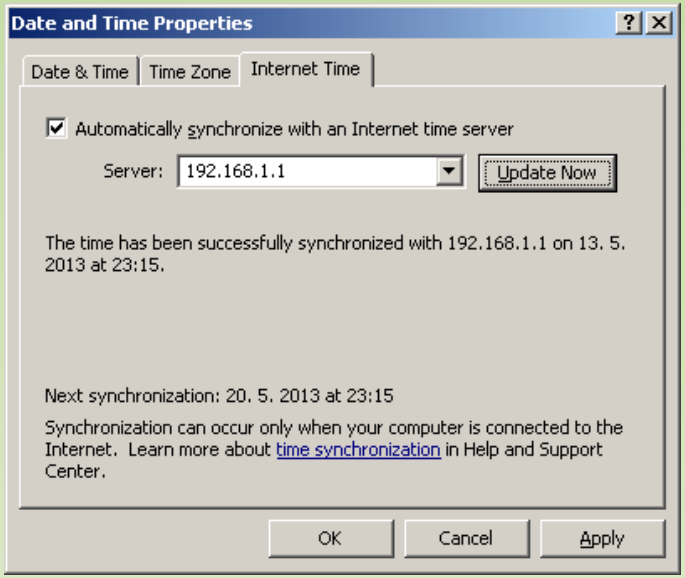
Picking a Time Source

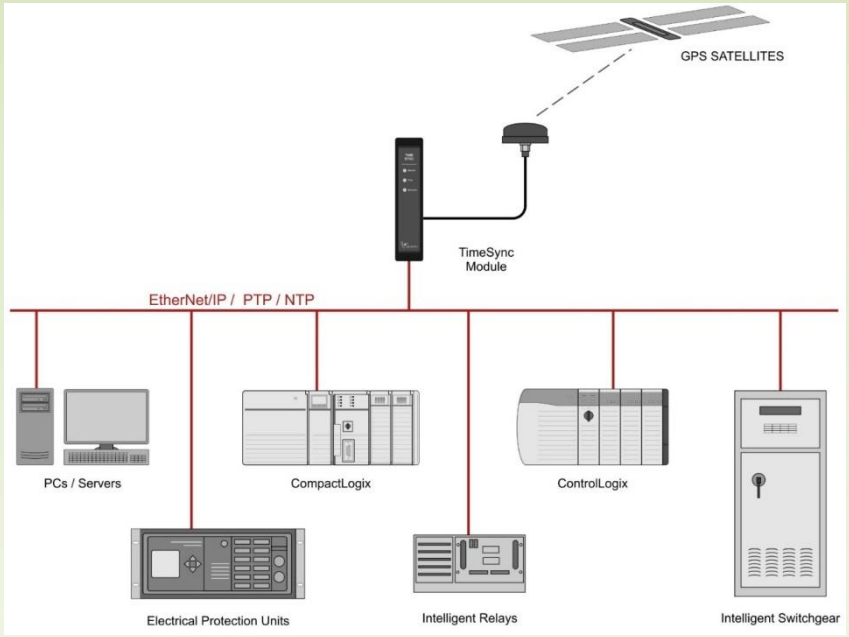
- **GPS Receiver** – gets time from GPS Satellites (which have atomic clocks)
- **AM Radio Broadcasts** – there are signals with time codes (from atomic clocks)
- **GSM/CDMA Cellular Signals** – contain time codes (from Cell Towers)
- **Raw Internet connection** – from Internet time servers (firewalls must be used!)
- **Your IT Department** – via Internet time servers (firewalls must be used!)
- Periodically setting a master clock manually – not recommended
- None – not recommended

- **Most common approach is to have a Time Server**
  - **Must Receive "Time" from known-good time source**
  - **Will often have a "holdover clock" to keep time, when external source not available**
  - **Time is then "distributed" to other servers/computers using NTP protocol**
  - SCADA Network routers often used to further distribute time across network
  - Some PLCs may require a helper server to run a special time protocol (e.g., CIP, GE)

Reminder: Devices that need time synchronization

- SCADA Servers
  - Data Gathering Machines
  - Historians
  - View Nodes
  - Reporting Systems
  - Backup Systems
- SCADA View Nodes
- Network Routers/Switches
- PLC/PAC/RTU
- Dataloggers





Guelph Water SCADA Time Sync Scheme

Primary Time Server (with holdover clock)

NTP-Peering

SCADA Network

Secondary Remote Time Server (with holdover clock)

NTP-Primary

Main SCADA Router (Hub Site)

NTP-Secondary

W32 Time Server (for winXP/2003)

NTP Protocol

Backup Historian (DNP3 Protocol)

Logix Time Sync Server (for Allen-Bradley PLCs)

DNP3 Protocol

w32time Protocol

SCADA Historians

PROCESS SITES

CIP

Control PLC

Backup Logger PLC

SCADA Servers (old Windows)

SCADA Hosts, Servers & SAN (newer Windows)

DMA Flowmeters Server

Site Router

DNP3 Protocol

View Node (if present)

QuickPanel OIT

SCADA View Nodes

DMA Flowmeters

Building Power Meter

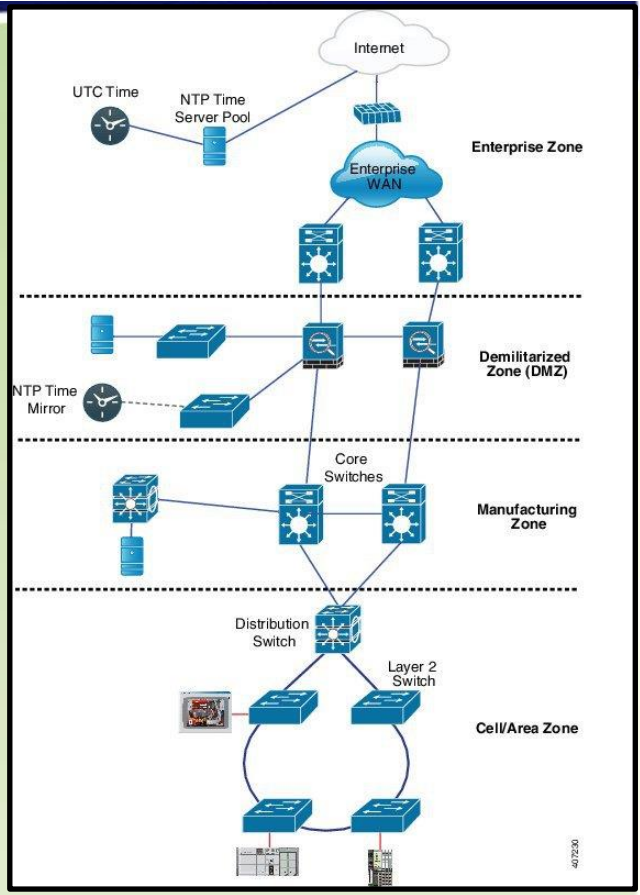
PLC Panel UPS

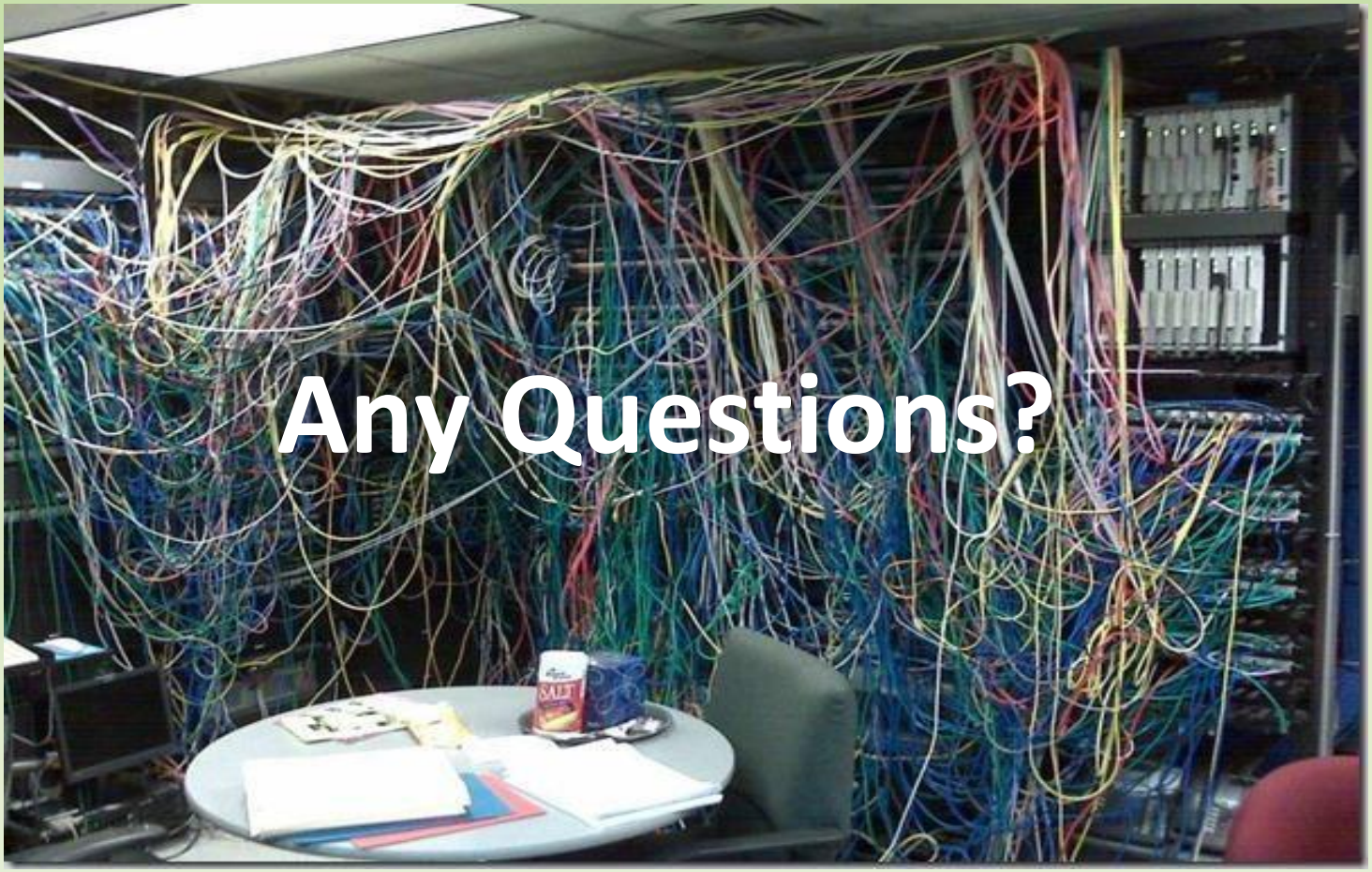
View Node UPS

Note: This is a summary. Firewalls/network zones not shown.

Time Sync Best Practices

- **Yes, you do need to do this!**
  - **Timestamps need to be correct on logged data**
  - **Backup dataloggers are only useful if time is correct**
  - **Calculating Daily Flow Totals, Viewing/Reporting Data**
  - **Time-based control: Peaking Wells, Filling Reservoirs at Night**
- **Select a Time Source for your SCADA System**
  - Not Good: No Time Source
  - Poor: Pick one server as “Master”
  - Good: NTP from IT Department
  - Better: GPS Time Server, with secondary NTP backup
  - Best: Two GPS Time Servers, NTP peering each other
- **Distribute Time in the SCADA System**
  - Not Good: No Time Sync Distribution
  - Poor: Historian, View Nodes, and Reporting Servers synced
  - Good: Historian, View nodes, PLCs, and Reporting Servers synced
  - Better: Historian, View Nodes, OITs, PLCs, Switches, Reporting synced
  - Best: Every device, which has a clock in it, is receiving time synchronization





* Not a High Performance SCADA System

Graham Nasby, Water SCADA & Security Specialist
graham.nasby@grahamnasby.com