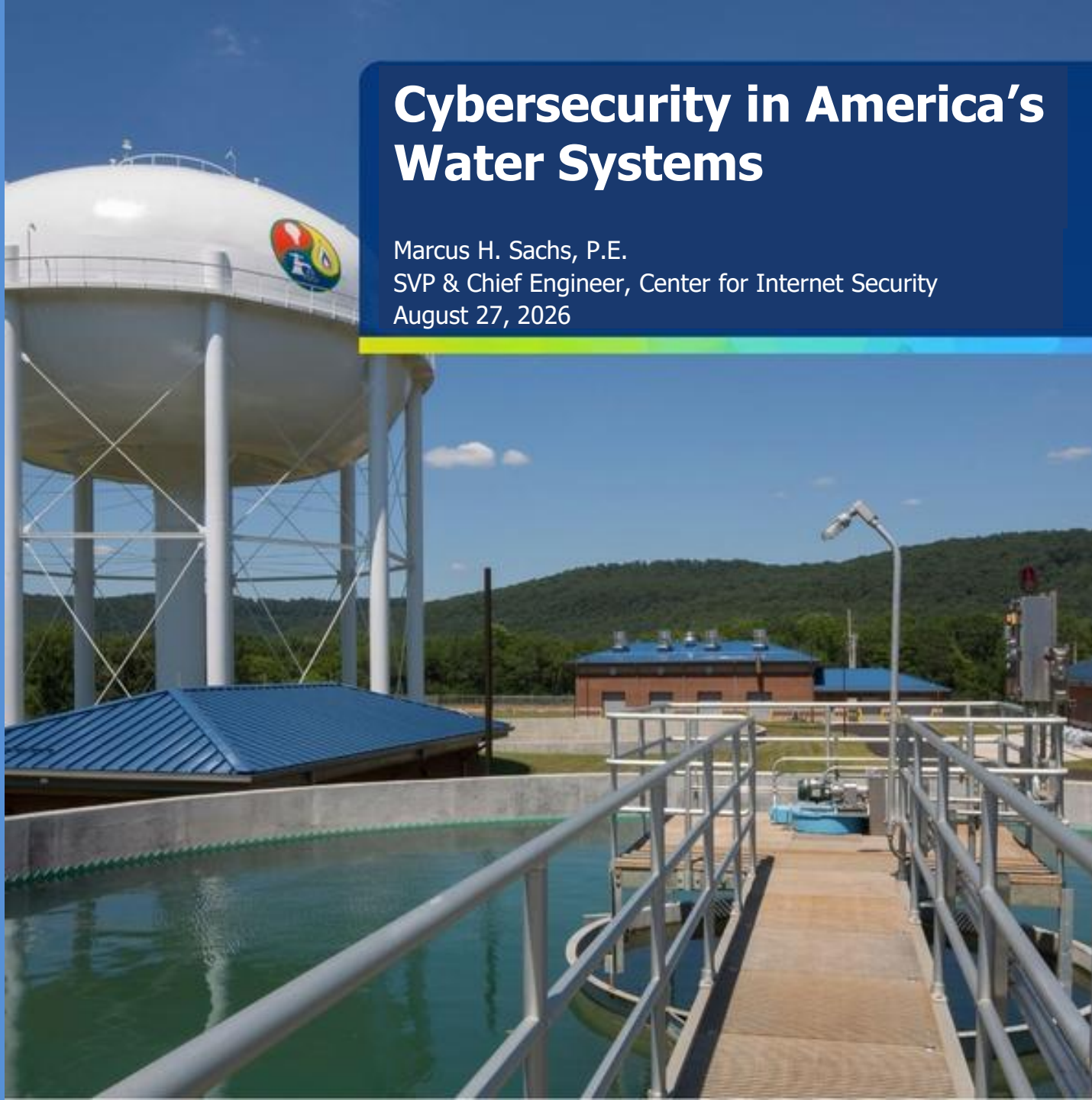




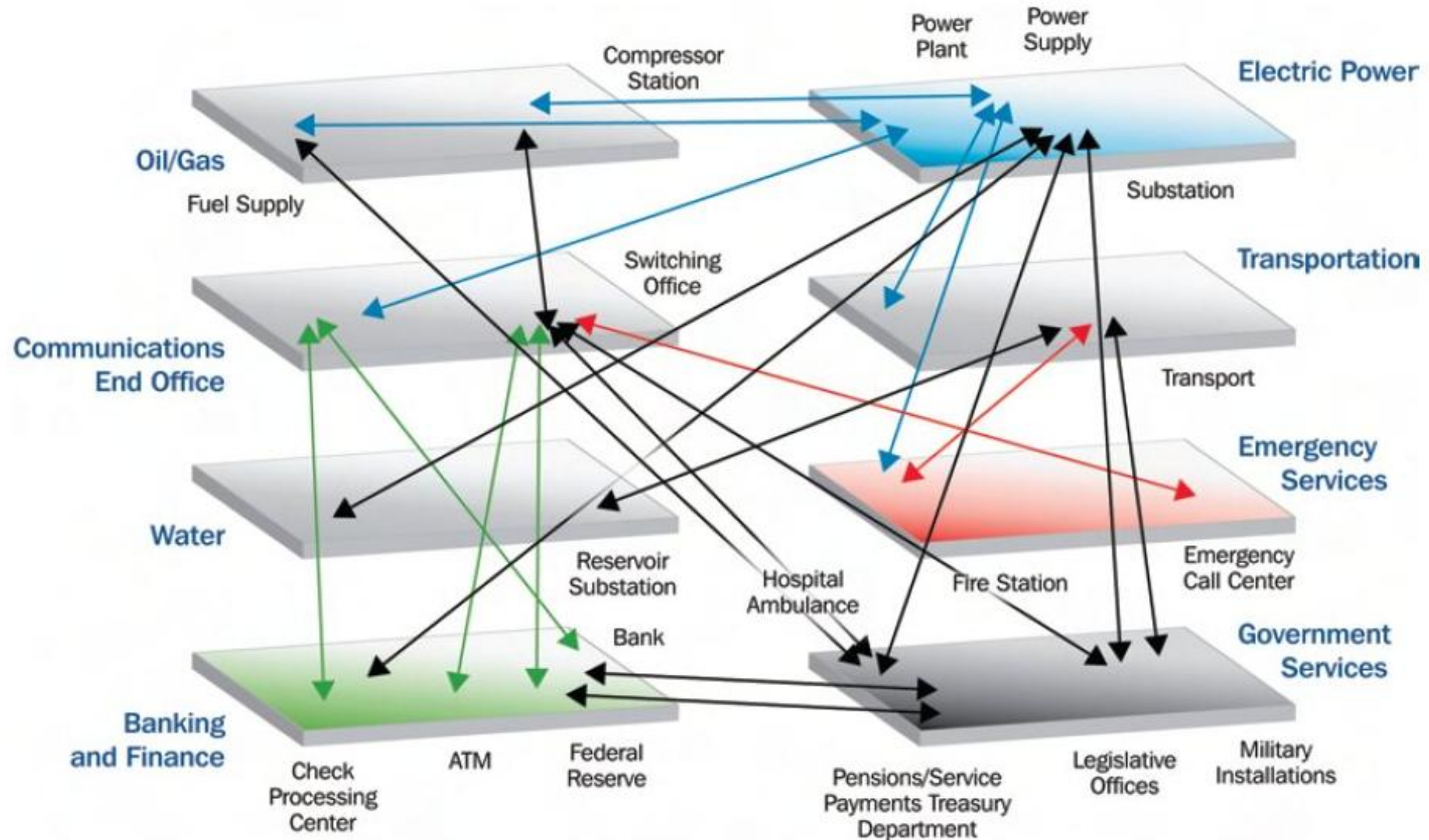
Cybersecurity in America's Water Systems

Marcus H. Sachs, P.E.
SVP & Chief Engineer, Center for Internet Security
August 27, 2026





Critical Infrastructure Dependencies





Critical Infrastructure's Common Denominator

- Most critical infrastructure sectors depend on cyber networks for data exchange
- Likewise, the cyber infrastructures depend on the physical world for the movement of the data
 - Fiber optic cables
 - Copper wires
 - Microwave and satellite systems
- All sectors depend on electricity
- *Some (most) sectors depend on water*

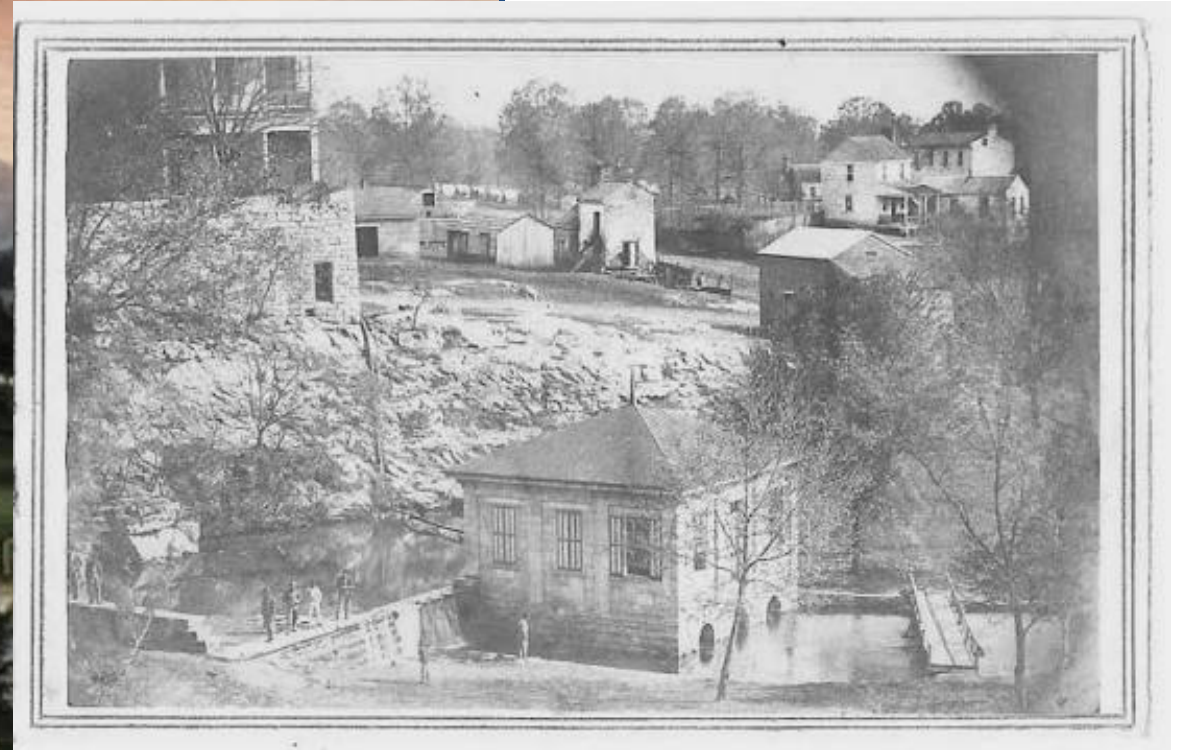
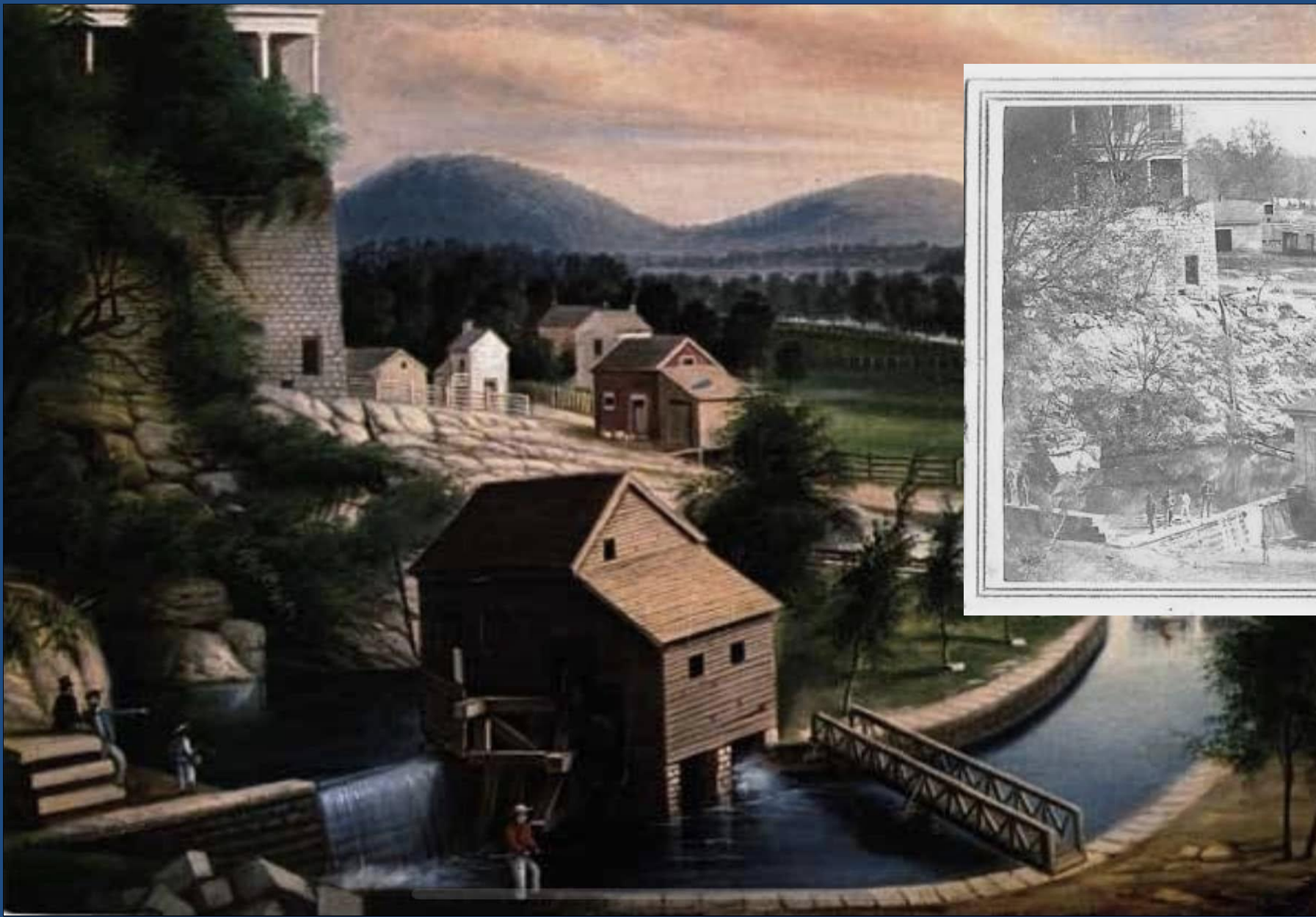




Water Sector Dependencies

Sector	Dependence on Water	Examples
Energy	Very high	Thermoelectric cooling, steam production, hydroelectric generation, refining, fuel processing
Chemical	Very high	Process water, cooling, steam, washing, dilution, fire suppression
Food and Agriculture	Very high	Irrigation, livestock, food processing, sanitation, cleaning
Healthcare and Public Health	Very high	Dialysis, sterilization, laboratories, cooling, sanitation, patient care
Nuclear Reactors, Materials and Waste	Very high	Reactor cooling, spent-fuel cooling, heat removal and safety systems
Commercial Facilities	High	Fire suppression, HVAC, sanitation, hotels, restaurants, large buildings
Emergency Services	High	Firefighting, hospitals/EMS facilities, emergency shelters, decontamination
Defense Industrial Base	High	Manufacturing, cooling, testing, fire protection and installation operations
Information Technology	Increasingly high	Data-center cooling, particularly evaporative and chilled-water systems
Government Facilities	Moderate to high	Building operations, cooling, sanitation, laboratories and continuity facilities
Communications	Moderate	Data-center/network-facility cooling, fire protection and personnel support

The Big Spring





Huntsville Water Established 1823

Oldest System West of the Appalachians

- 1823 – Huntsville Waterworks with cedar pipes
- 1836 – First cast iron pipe laid
- 1843 – Big Spring deeded to COH (~ 111 customers)
- 1858 – COH purchased water works for \$10,000
- 1914 – First chlorinator installed
- 1954 – Huntsville Utilities Waterworks Board formed
- 1955 – Lincoln & Dallas Wells replaced Big Spring as water supply
- 1964 – South Parkway Plant constructed (12 MGD – Million Gallons per Day)
- 1966 – South Parkway expanded to 24 MGD
- 1971 – Williams Well drilled to 4.5 MGD
- 1978 – South Parkway expanded to 36 MGD
- 1988 – Southwest Plant constructed to 12 MGD
- 1989 – Southwest Plant high rated to 18 MGD
- 1992 – Southwest Plant high rated to 24 MGD
- 1992 – Lincoln Dallas Plant constructed to 9 MGD
- 1996 – Hampton Cove Plant constructed to 2 MGD
- 2001 – Southwest Plant expanded to 48 MGD
- 2008 – South Parkway Plant expanded to 48 MGD
- 2017 – Southeast Plant constructed 12 MGD

Old Pump House



A Sunday Outing



Huntsville's First Water Pipes Were Cedar Logs





Cedar Pipe Discovered in 2020





Water Systems

- Water was originally obtained and consumed within the same local area
 - Wells and springs
 - Rivers and lakes
 - Cisterns and other local storage
- As communities grew, water service evolved into centralized treatment and distribution systems
 - Treatment plants
 - Pumping stations
 - Storage tanks and reservoirs
- Distribution networks
 - Centralized systems provide major public health and operational efficiencies
 - Reliable treatment and disinfection
 - Consistent pressure and availability
 - Economies of scale in treatment and distribution





Water System Basics

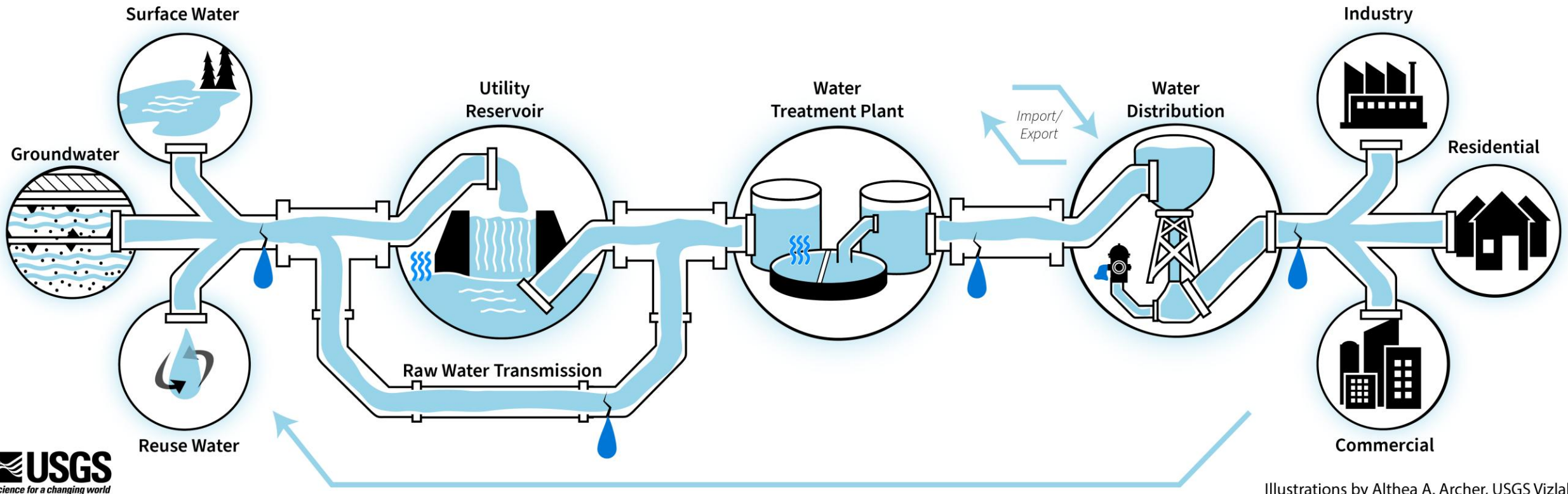
- Most municipal systems combine treatment, storage, and distribution
 - Source water
 - Treatment plant
 - Clearwell or finished-water storage
 - High-service pumps
- Water moves through pressure zones, pipes, valves, and tanks
 - Elevated tanks help maintain pressure
 - Pumps move water uphill or across distance
 - Valves isolate areas and control flow

The system must operate continuously:

- *Demand changes throughout the day*
- *Pressure must be maintained*
- *Water quality must be preserved from plant to customer*

- *Pumps create pressure, tanks create time.*
- *The physical process continues when the network fails.*
- *A sensor measures a process; it does not make the process true.*
- *Water moves slowly; control commands move fast.*

Water Supply Diagram



Illustrations by Althea A. Archer, USGS Vizlab



Where Does Our Water Come From?

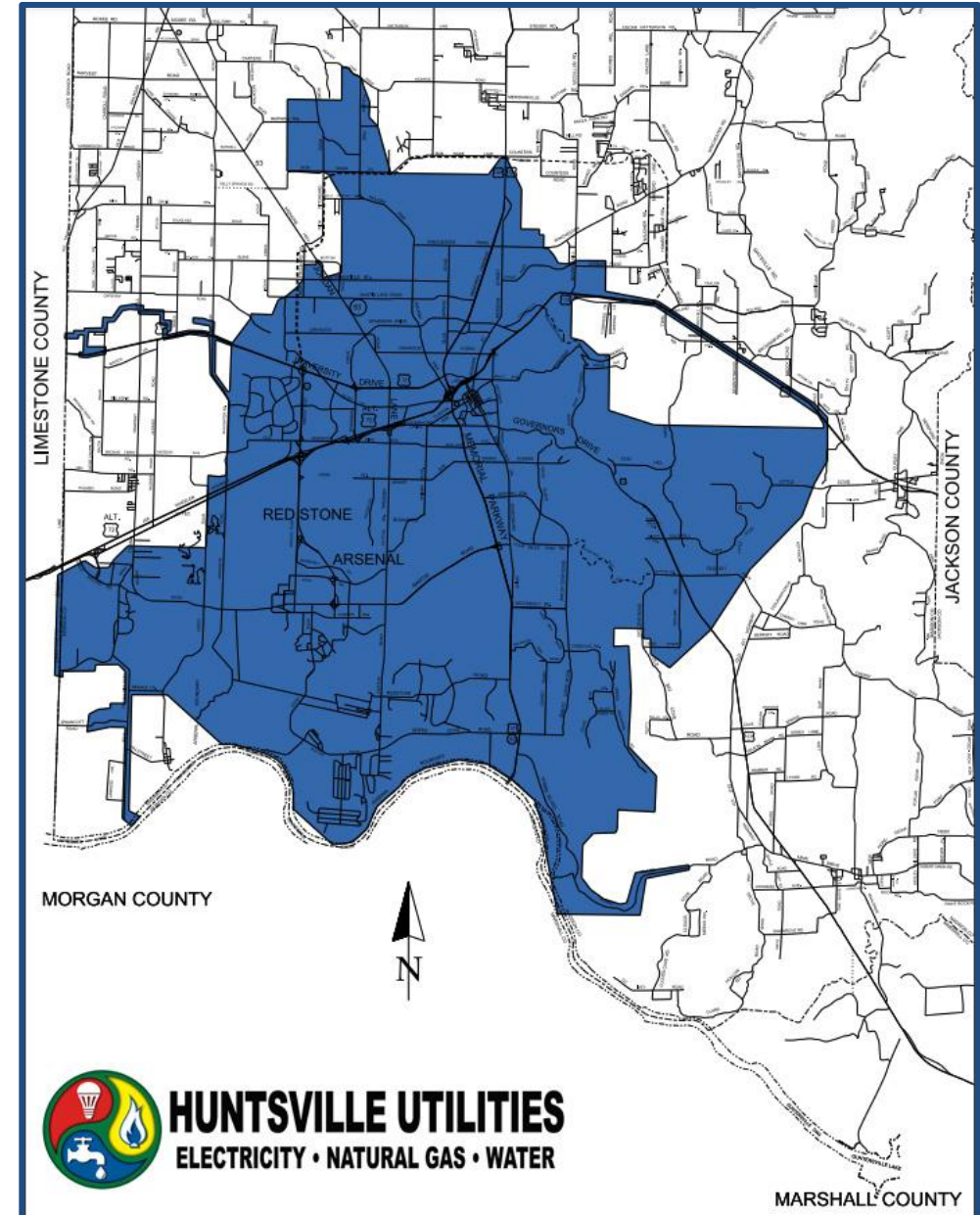
- **Surface Water**

- Pumped from the Tennessee River
- Processed through the South Parkway, Southwest and Southeast Treatment Plants

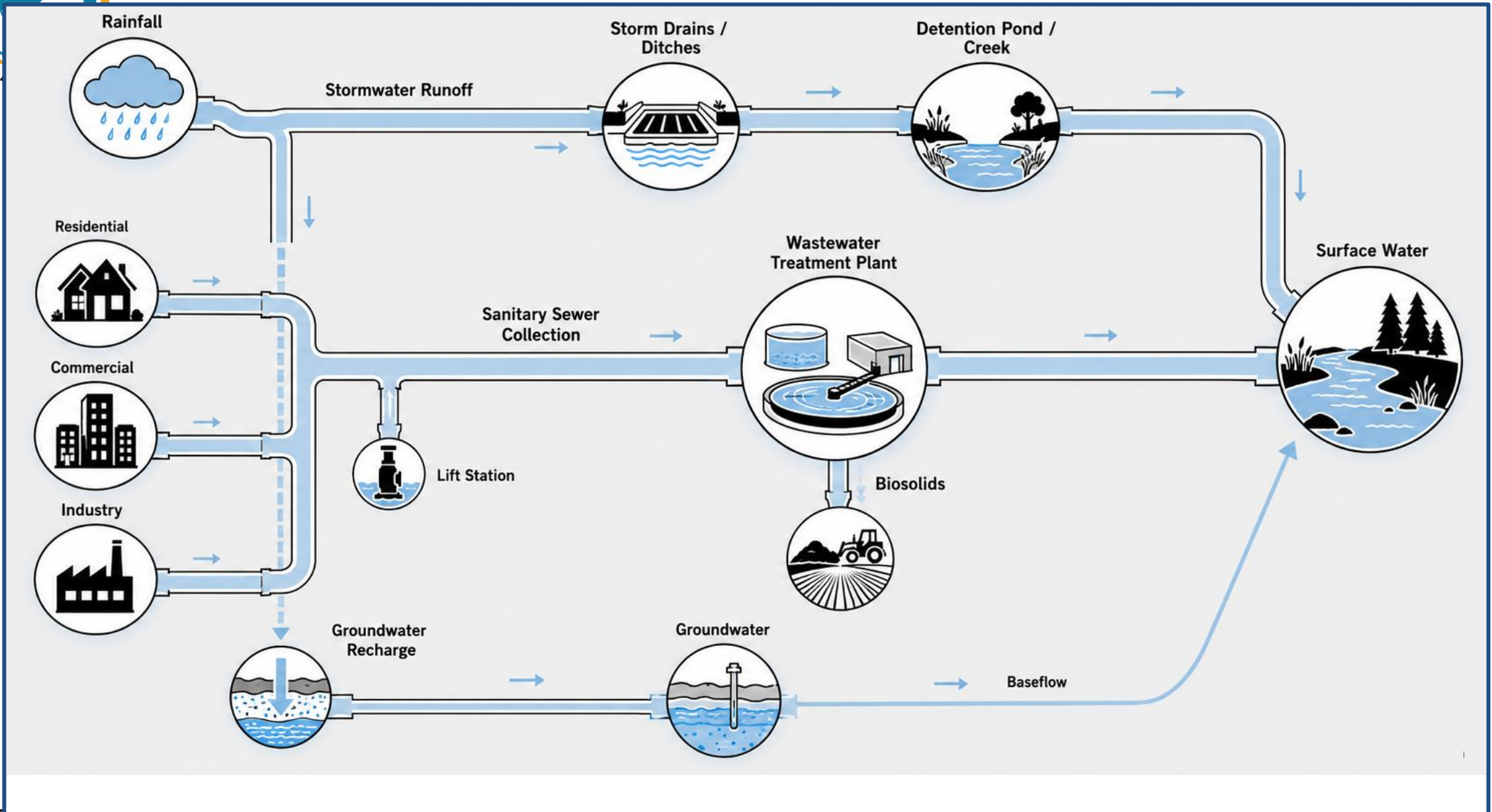
- **Groundwater**

- Supplied from the Lincoln and Dallas Well Treatment Plant and Williams Well
- All groundwater wells produce water from limestone aquifers

https://www.hsvutil.org/community_resources/educational_resources/water.php



Wastewater and Stormwater Return Flow





After We Use It, Where Does Our Water Go?

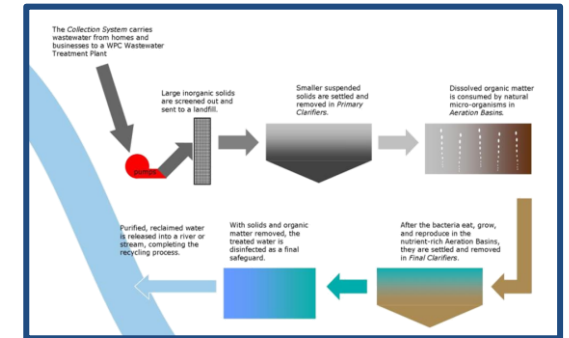
- Water Pollution Control (WPC) uses a large collection system to get wastewater from Huntsville's homes, businesses, and other facilities to one of its six treatment facilities.
- Collection Systems
 - The collection system is a large network:
 - 1,400 miles of underground sewer pipes (ranging from 8 inches to 78 inches in diameter)
 - 35,000 manholes (to access the system for maintenance)
 - 63 pumping stations





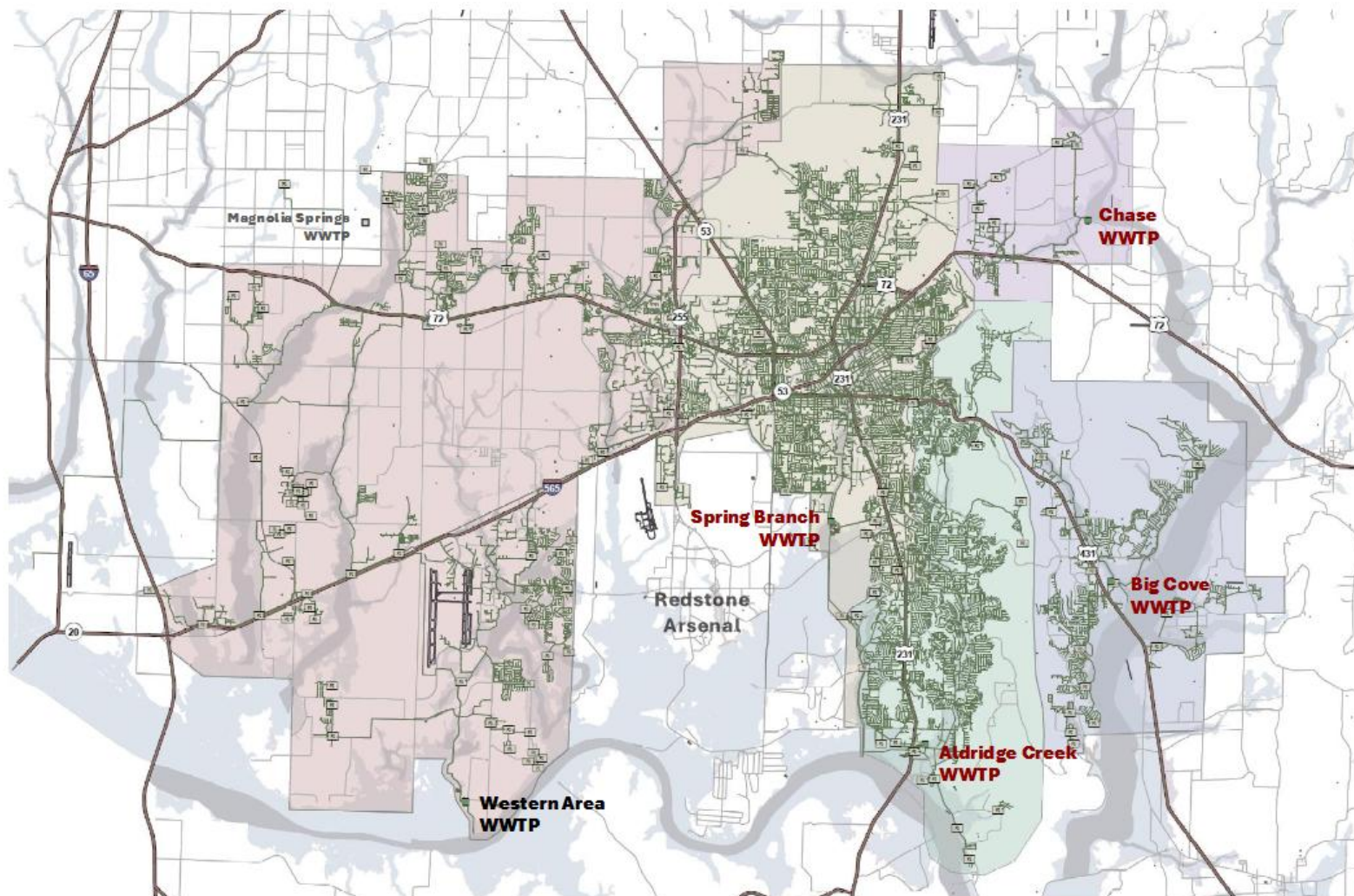
Wastewater Treatment

- WPC operates six wastewater treatment plants (WWTPs)
- WWTPs remove pollutants through several basic steps:
 - The sewer system delivers wastewater to a WWTP at the Headworks
 - Large, inorganic solids are removed with Bar Screens
 - Smaller inorganic solids are settled out and removed in Primary Clarifiers
 - Suspended organic solids are consumed by natural micro-organisms in oxygen-rich Aeration Basins
 - Dead and excess micro-organisms are settled out and removed in Final Clarifiers
 - Remaining micro-organisms are eliminated through disinfection
- The clean, clear reclaimed water is released back into a local waterway



<https://www.huntsvilleal.gov/residents/water-sewer/sanitary-sewer/wastewater-collection-treatment/>

Wastewater Treatment Facility Upgrades



* Western Area WWTP is currently undergoing capital improvements.

“RED” – Denotes needed Capital Improvements

Water Pollution Control currently operates and maintains six (6) wastewater treatment facilities.

These facilities have a permitted treatment capacity of 110 million gallons per day.

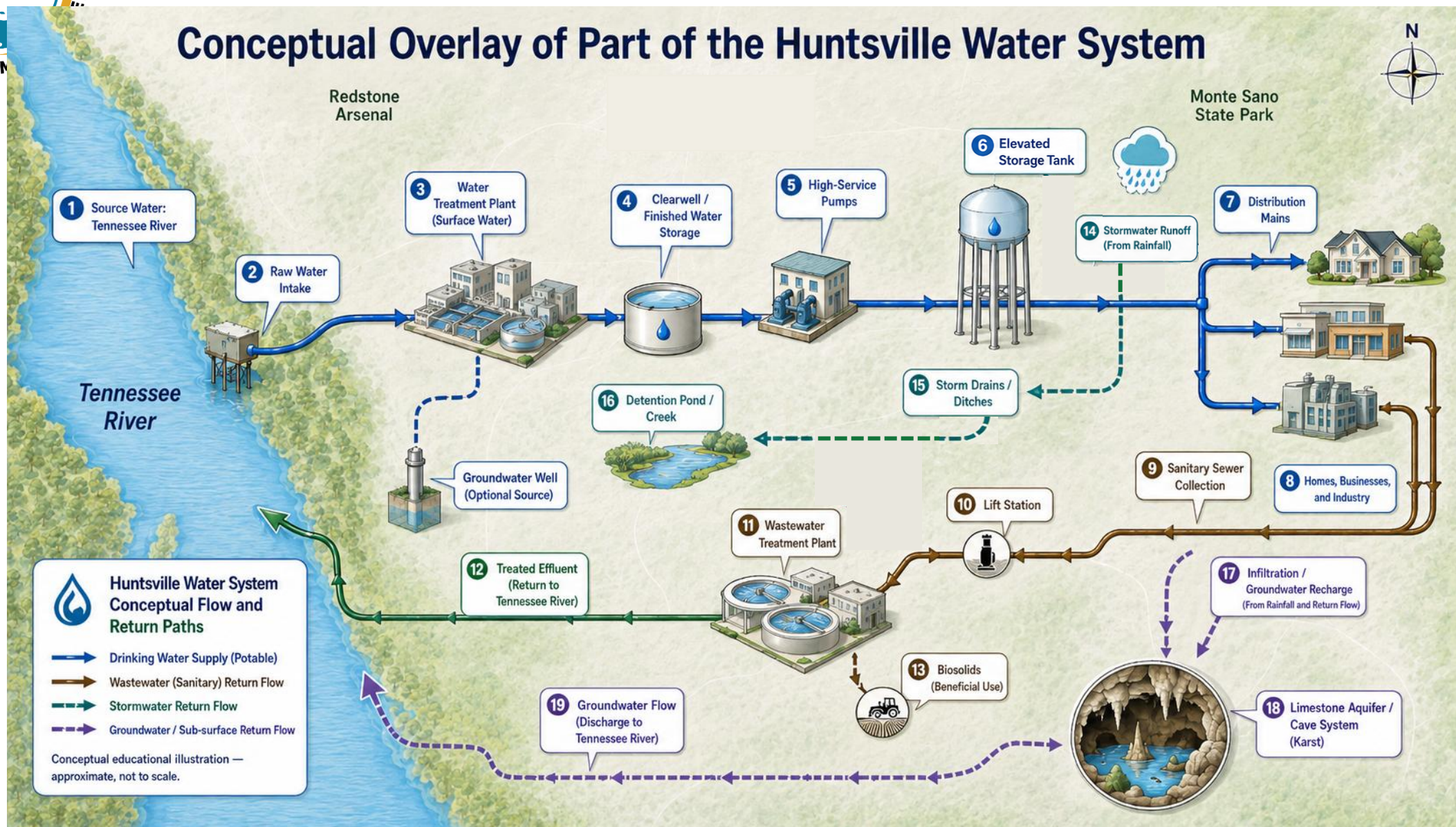
These wastewater treatment facilities have a combined average age of 48 years in service.

Four (4) of the Six (6) treatment facilities are in need of capital improvements to ensure reliable operation and permitting requirements.

Wastewater Treatment Facilities

Spring Branch WWTP 1960 and 1969	(65 years)
Aldridge Creek WWTP 1966 and 1988	(59 years)
Big Cove WWTP 1988	(37 years)
Chase WWTP 1987	(38 years)
Western Area WWTP 1983, 2000, and 2024	(42 years)

Concept Illustration - Huntsville

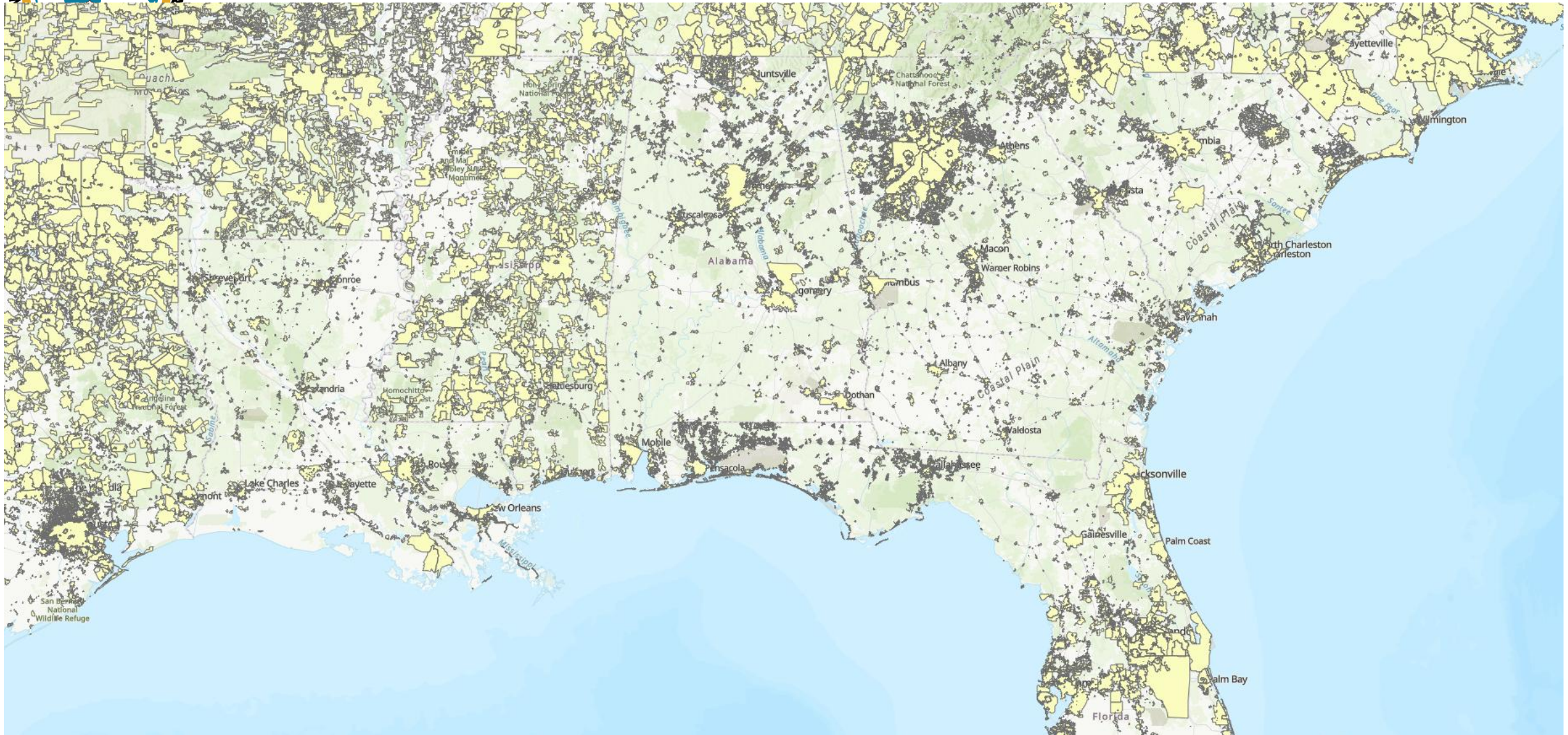




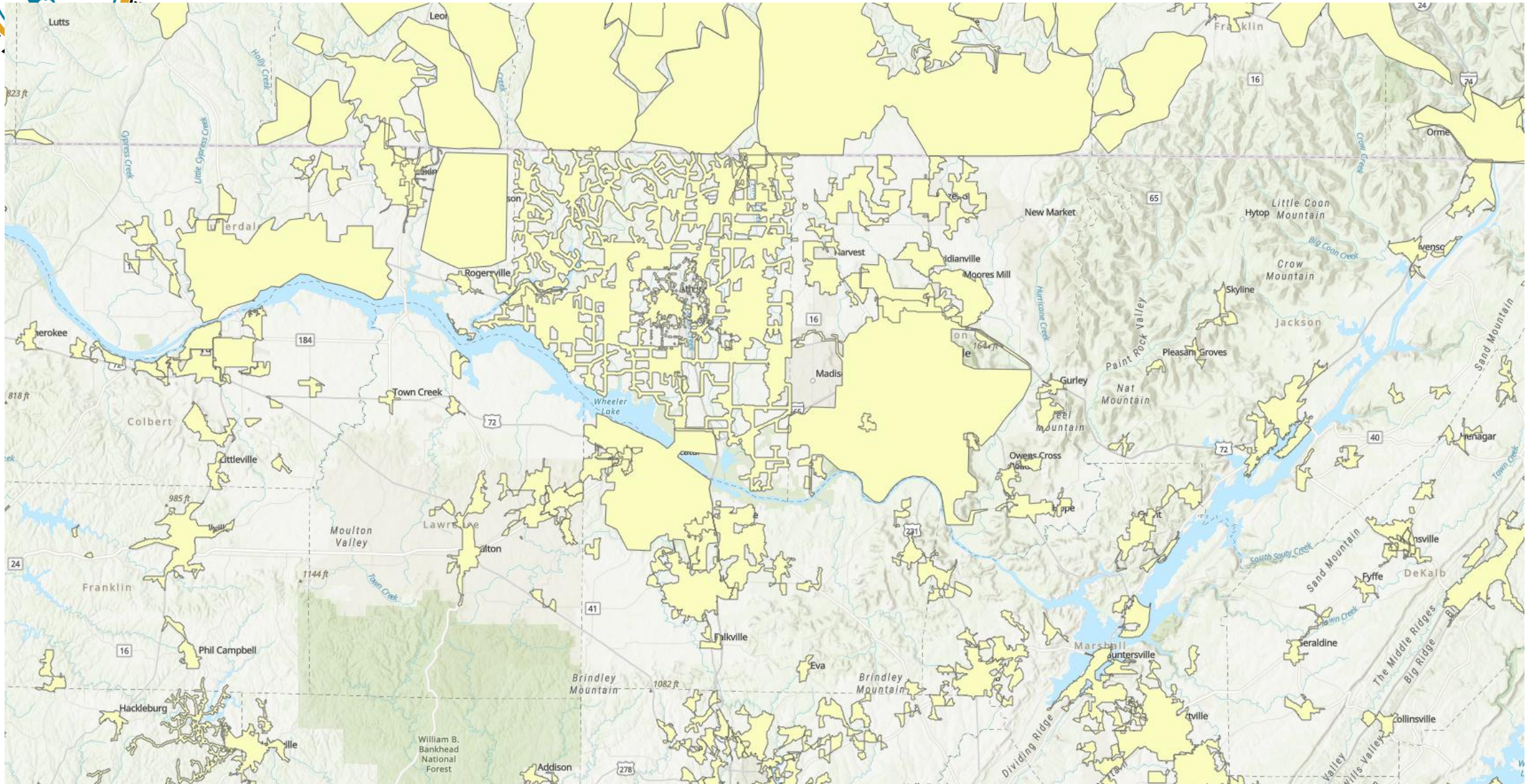
America's Water Systems Are Primarily Local

- **Unlike electricity, there is no national interconnected water grid**
 - Approximately 150,000 public drinking-water systems
 - Range from very small rural utilities to major metropolitan systems
 - Treatment, pumping, storage and distribution are normally controlled locally
 - Neighboring systems may have interconnections, but there is no continental operational network
- ***No equivalent to a NERC Reliability Coordinator or Balancing Authority for the Electric Sector***

Southeast USA Community Water Systems



Tennessee Valley Community Water Systems





Even Though Water Is Local, Regulation Is Not

- **Federal**

- EPA
- Safe Drinking Water Act
- Clean Water Act / NPDES

- **State**

- Drinking-water primacy agency
- Environmental/wastewater regulator
- Water-resource agencies

- **Local**

- Water utility
- Wastewater utility
- Municipal stormwater system



Federal and state agencies establish and enforce health and environmental requirements; local utilities operate the physical systems



National Pollutant Discharge Elimination System (NPDES)



What is NPDES?

The NPDES permit program addresses water pollution by regulating point sources that discharge pollutants to waters of the United States

Created in 1972 by the Clean Water Act, the NPDES permit program is authorized to state governments by EPA to perform many permitting, administrative, and enforcement aspects of the program



“Clean” Storm Water?

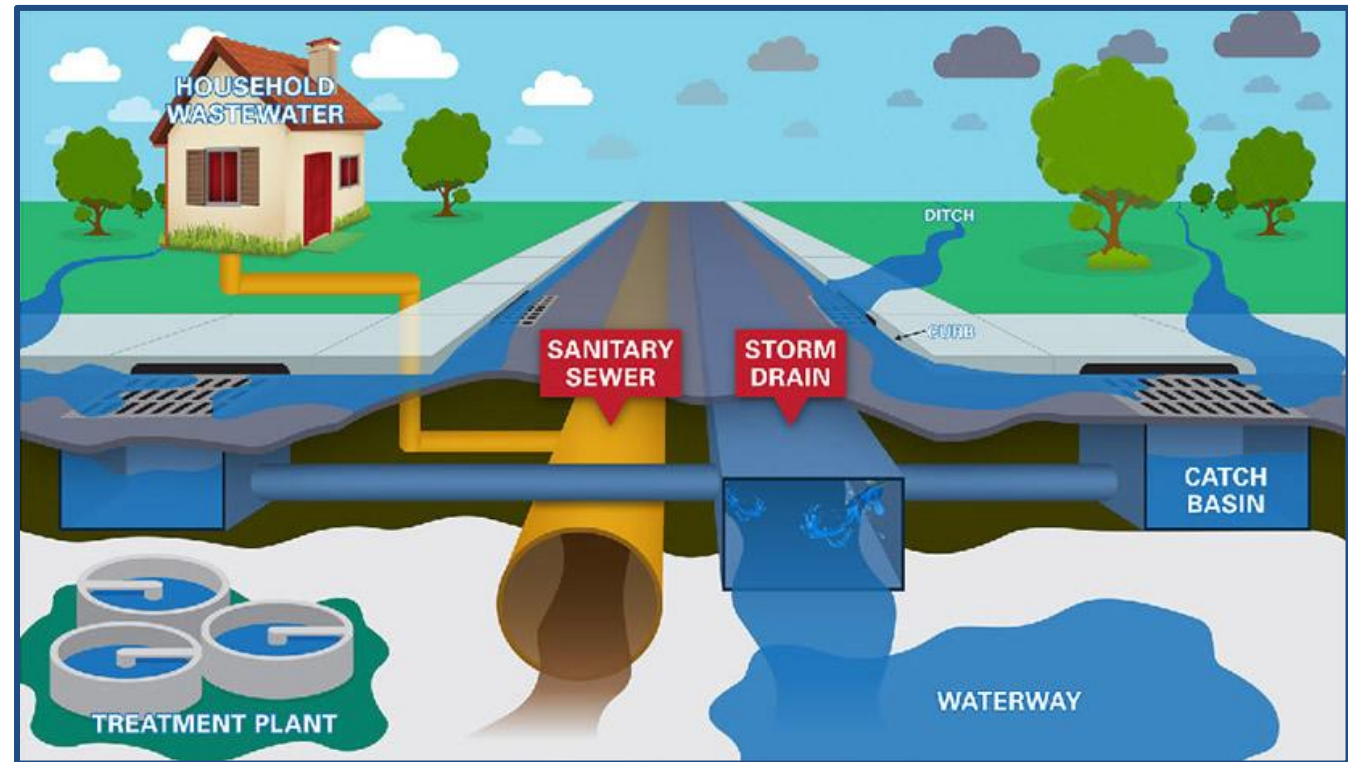
- A major contributor to contamination of our waterways is polluted stormwater
 - Stormwater is pure rainwater plus anything the rain carries along with it
 - In urban areas, rain that falls on the roof of your house, or collects on paved areas like driveways, and roads is carried away through a system of pipes or ditches
 - The stormwater flows directly from streets and gutters into our rivers
- Sediment and other debris clog drains and waterways causing flooding
- Stormwater pollution can harm aquatic life and make fish inedible
- Polluted storm water can pose a health risk to people





Preventing Stormwater Pollution

- Where possible, direct downspouts and gutters to drain into plant beds or lawn areas
- Decrease soil erosion by planting ground-cover where lawn grass won't grow
- Use brick pavers, gravel, or other porous materials for driveways, walkways and patios
- Sweep grass clippings, fertilizer and soil from driveways and streets back onto the lawn
- Avoid placing yard debris near storm drains where it can wash during heavy rains





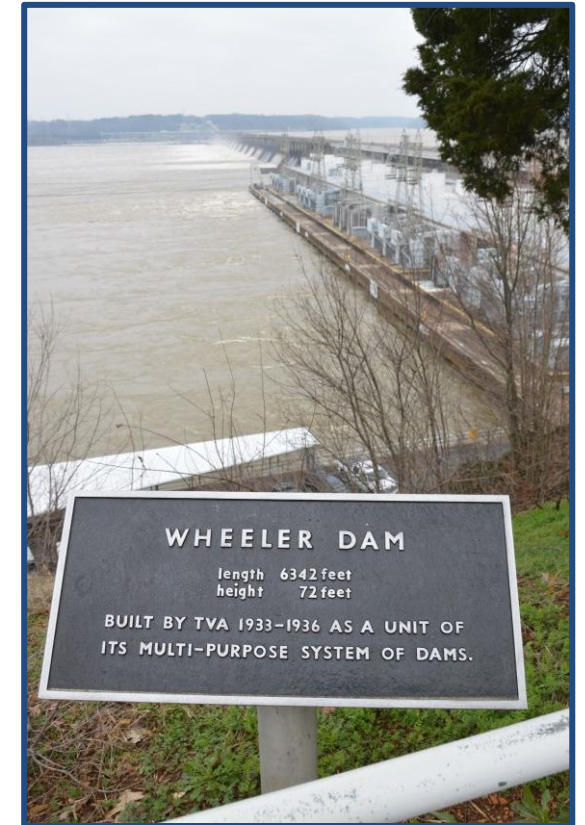
Huntsville Stormwater Management



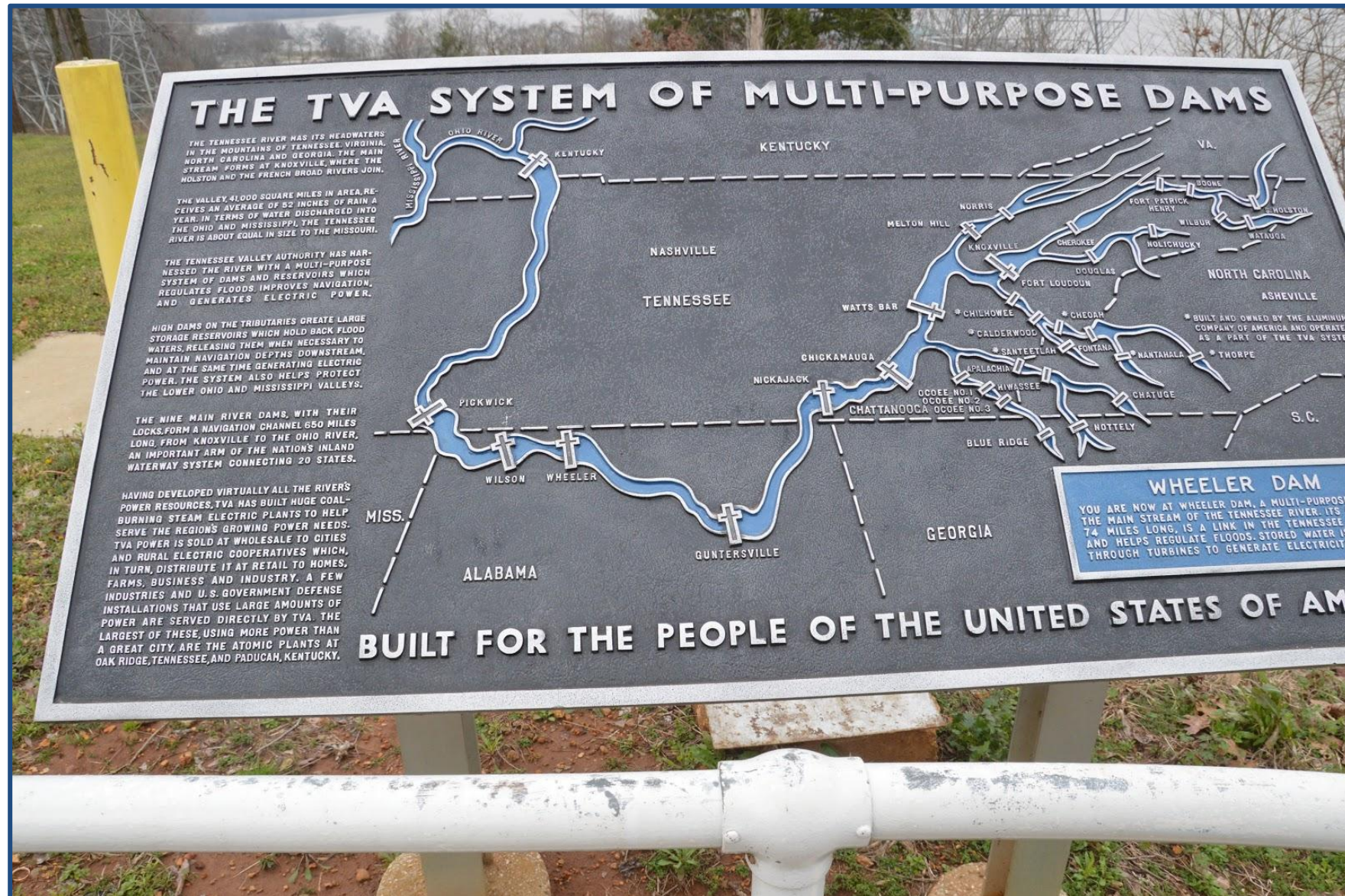


Water Resource Management

- Individual water utilities may be local, but the water itself is not
- Rivers, aquifers and watersheds cross political boundaries
- Consequently, there are organizations such as:
 - Interstate river-basin commissions and compacts
 - State water-resource agencies
 - U.S. Army Corps of Engineers
 - Bureau of Reclamation in much of the West
 - Watershed authorities
 - The Tennessee Valley Authority
- Huntsville Utilities draws surface water from the Tennessee River
 - The river is part of a much larger managed river system
 - But TVA does not operate Huntsville's drinking-water system



Tennessee Valley Authority



Coordination Without Central Control

Water sector coordination is extensive, but day-to-day operations remain local.

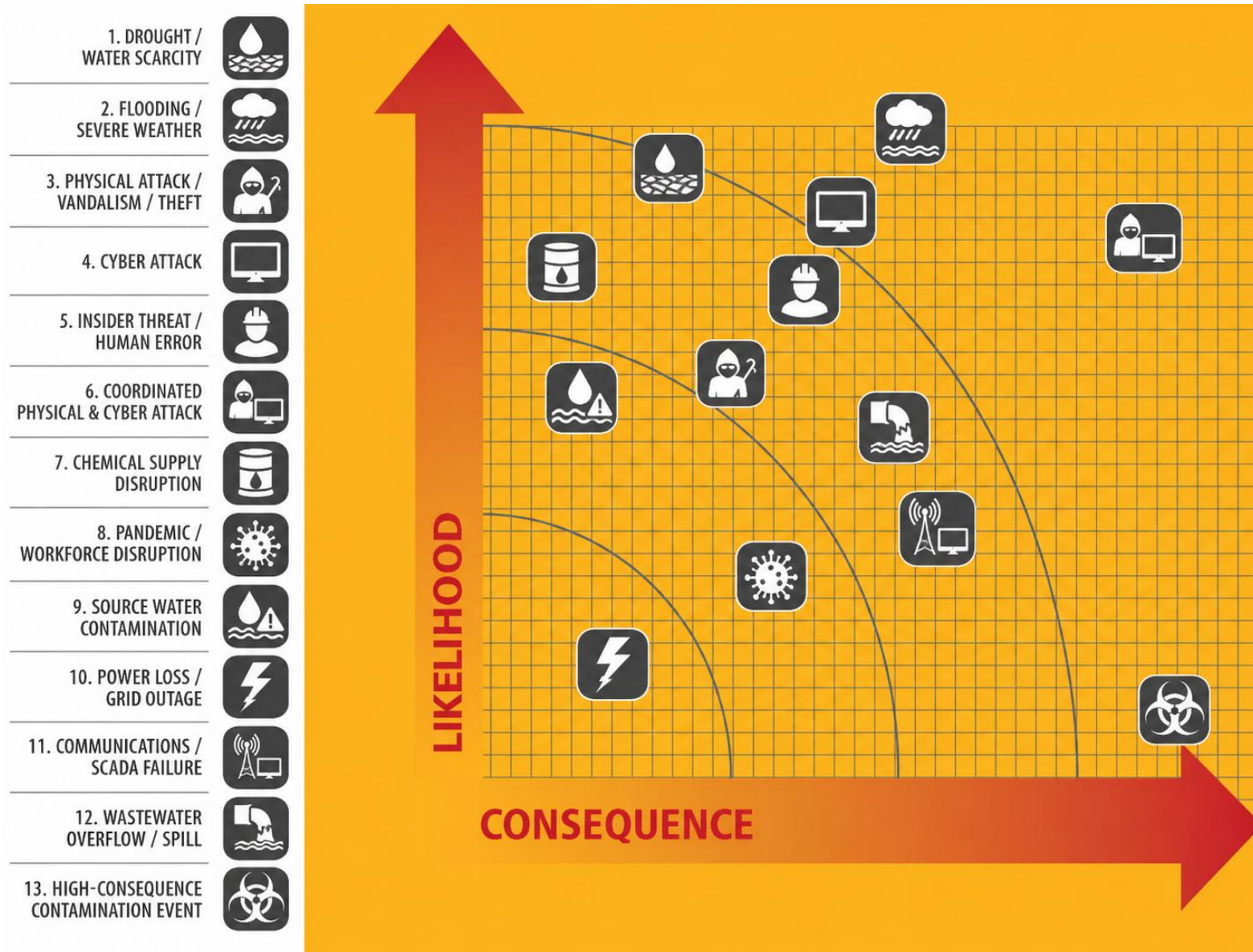




Water System Security



Water Sector Threat Landscape





Most Common Threat Agents



Agent	Success
Squirrel	1252
Bird	639
Snake	117
Raccoon	115
Rat	53
Cat	28
Marten	25
Jellyfish	13
Monkey	12
Human	3*

<http://cybersquirrel1.com/>



Natural Threats – Flooding

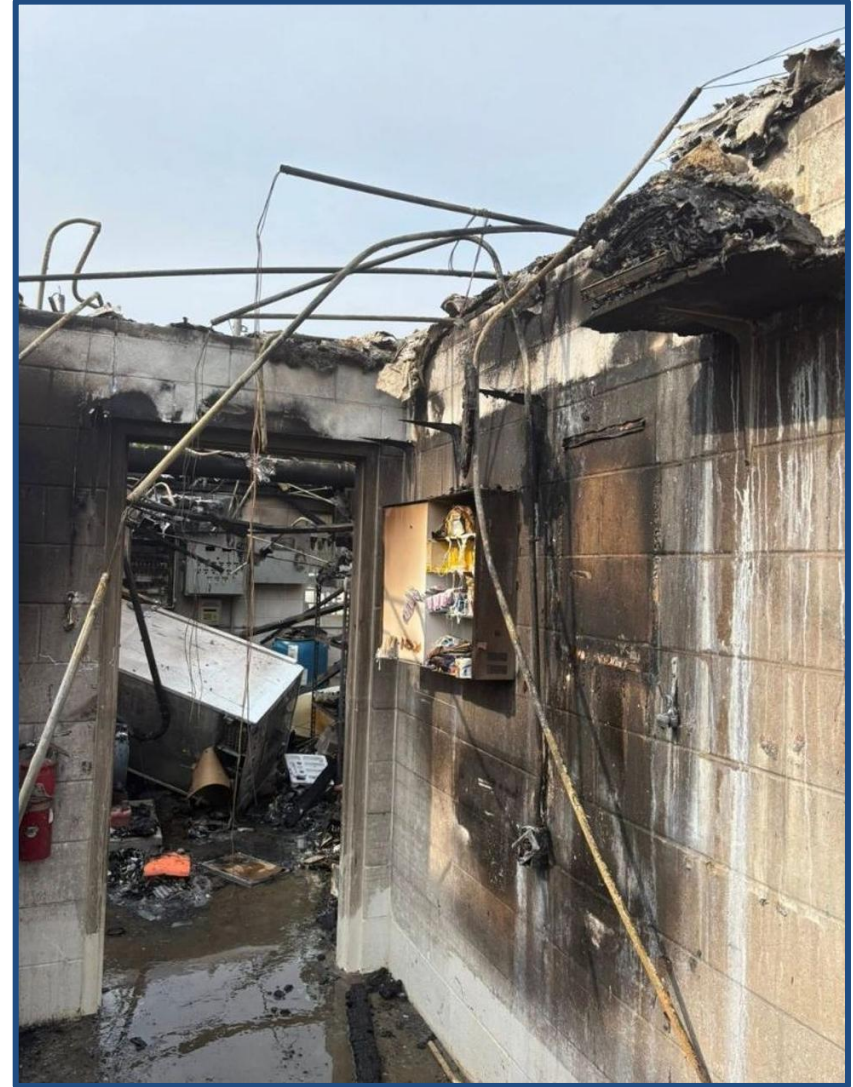




Natural Threats – Tornadoes



Natural Threats – Lightning



Operational Threats – Fire





Physics Threats – Broken Pipes





Human Threats – Vehicles





Human Threats - Vandalism





Targeted Threats – Pipe Bombs





Criminal Threats – Copper Theft

COPPER WIRE THEFT

DECATUR TWP., CLEARFIELD COUNTY



- REPORTED MAY 16TH, 10 A.M.
- 550 FEET CUT AND STOLEN
- WATER TREATMENT PLANT ON DRANE HIGHWAY



Bear Sighting

Notice to Lax Kw'alaams Members



Public Works is advising community members to use caution following a bear sighting near the Water Treatment Plant

The bear was observed walking alongside the road leading to the Water Treatment Plant. Since this area is frequently used by community members for walking, ATV use, and accessing the back roads, the public is asked to use caution.

Sighting details

Location: Water Treatment Plant (Back Road Area)

Date: Friday, July 10, 2026

Time: Approximately 8:00 AM

Please use caution

- Please avoid the area if possible until the bear has moved on.
- Do not approach, feed, or attempt to photograph the bear.
- Keep children and pets away from the area.
- If you must travel through the area, remain alert, make noise, and leave immediately if the bear is seen.
- Report any additional bear sightings to Public Works or the appropriate authorities if the bear remains in the area.



Photo taken near Water Treatment Plant road at approximately 8:00 AM, July 10, 2026

This notice is intended to help keep community members informed and encourage everyone to use caution while travelling in the area.



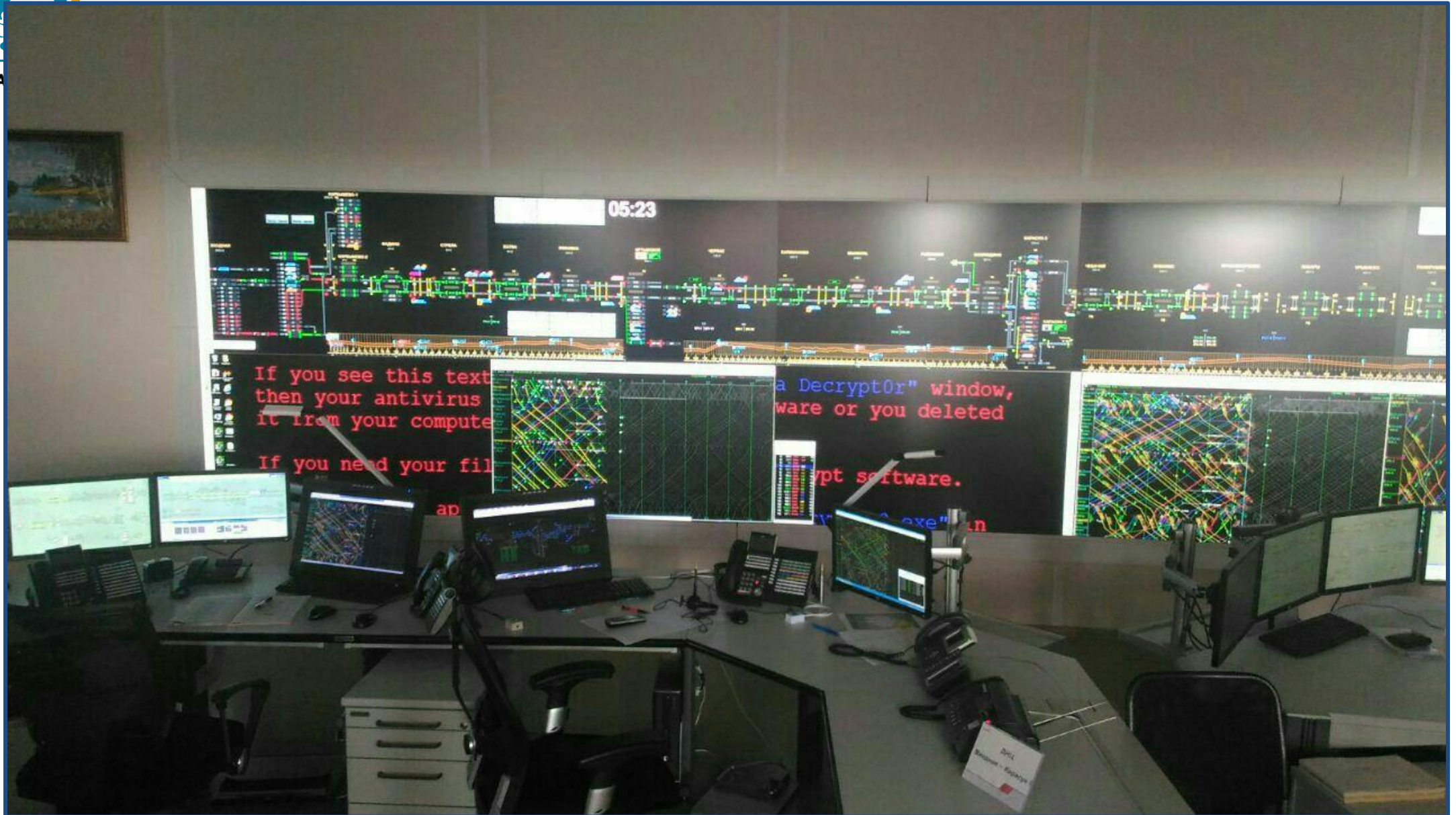
Lax Kw'alaams Band
208 Sheshuak Street
Lax Kw'alaams, BC V0V 1H0
Phone: (250) 625-3293 Fax: (250) 625-3246



Control Rooms at Control Centers

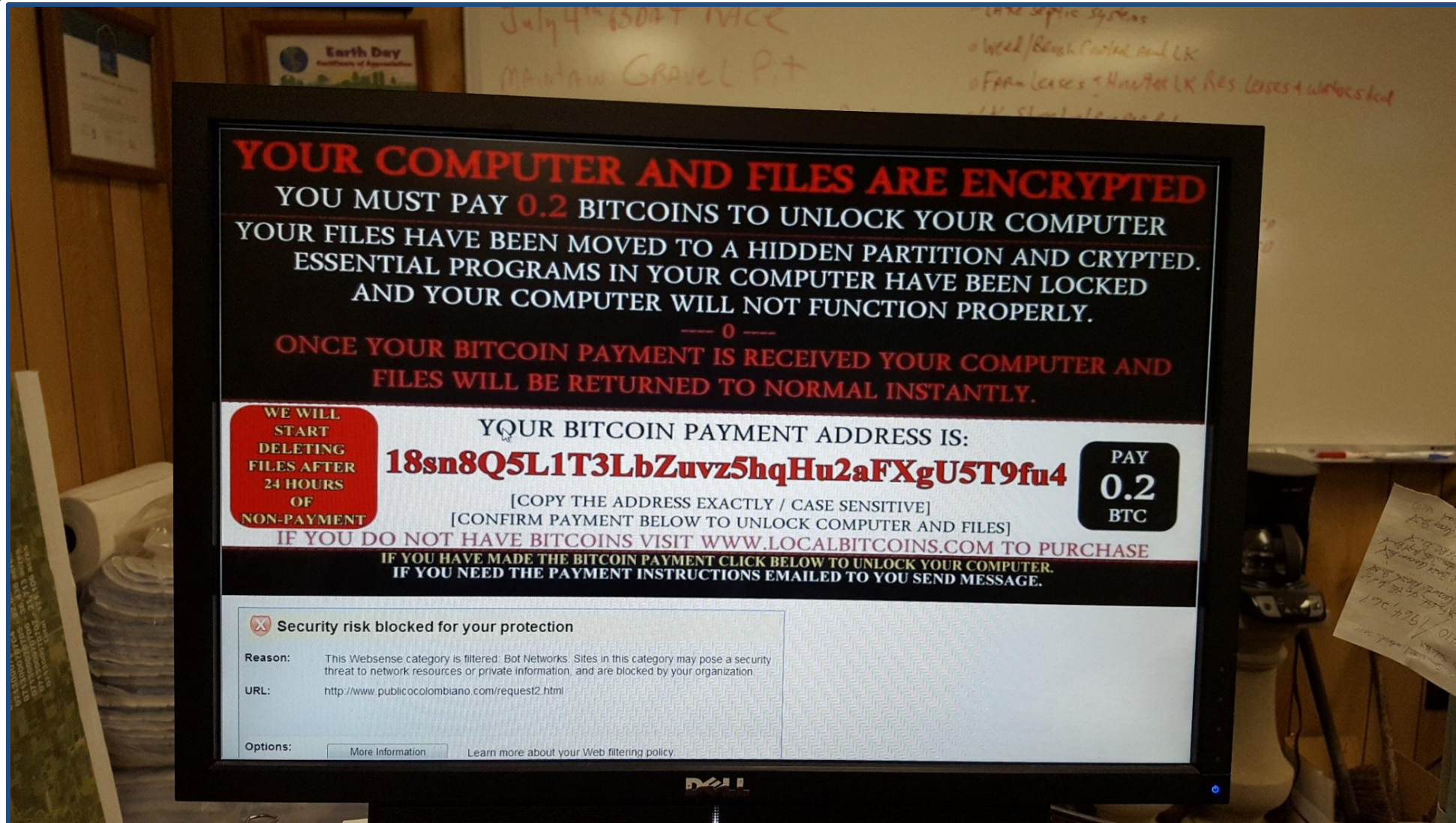


You Don't Want This in a Control Room





Most Likely Cyber Threat to Water Utilities

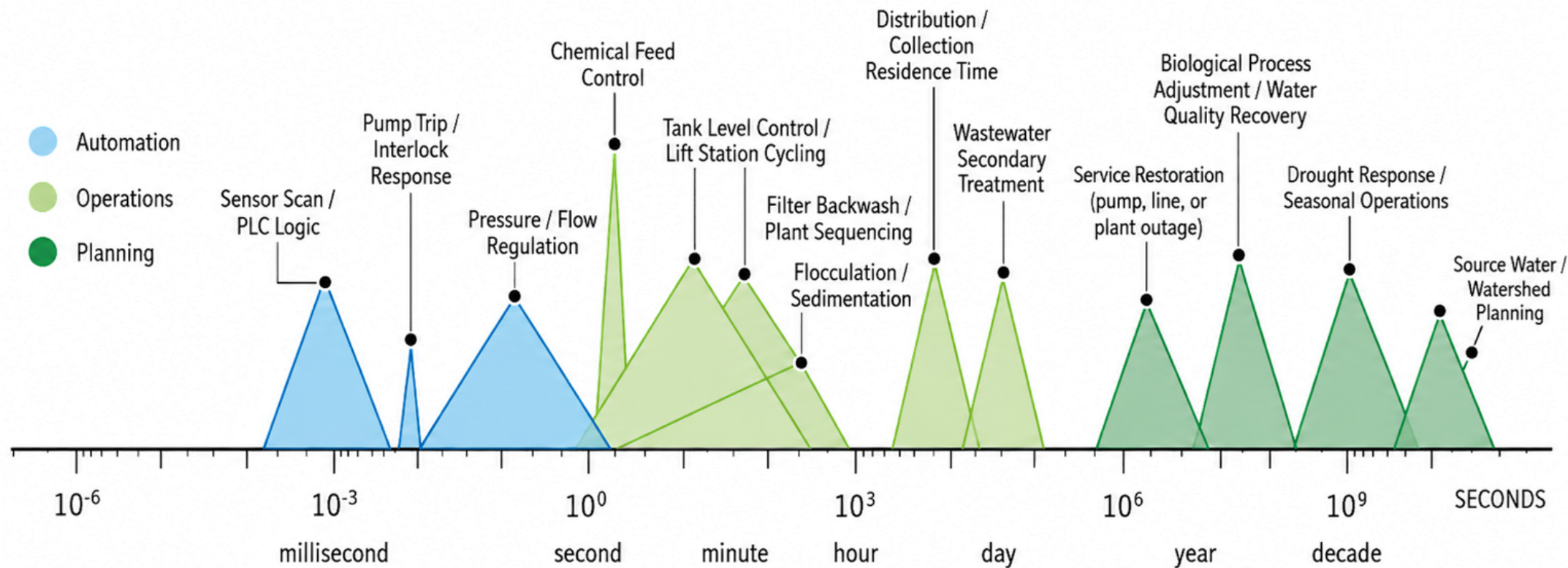


Least Likely Cyber Threat





Managing Multiple Event Speeds – Traditional Water Operations



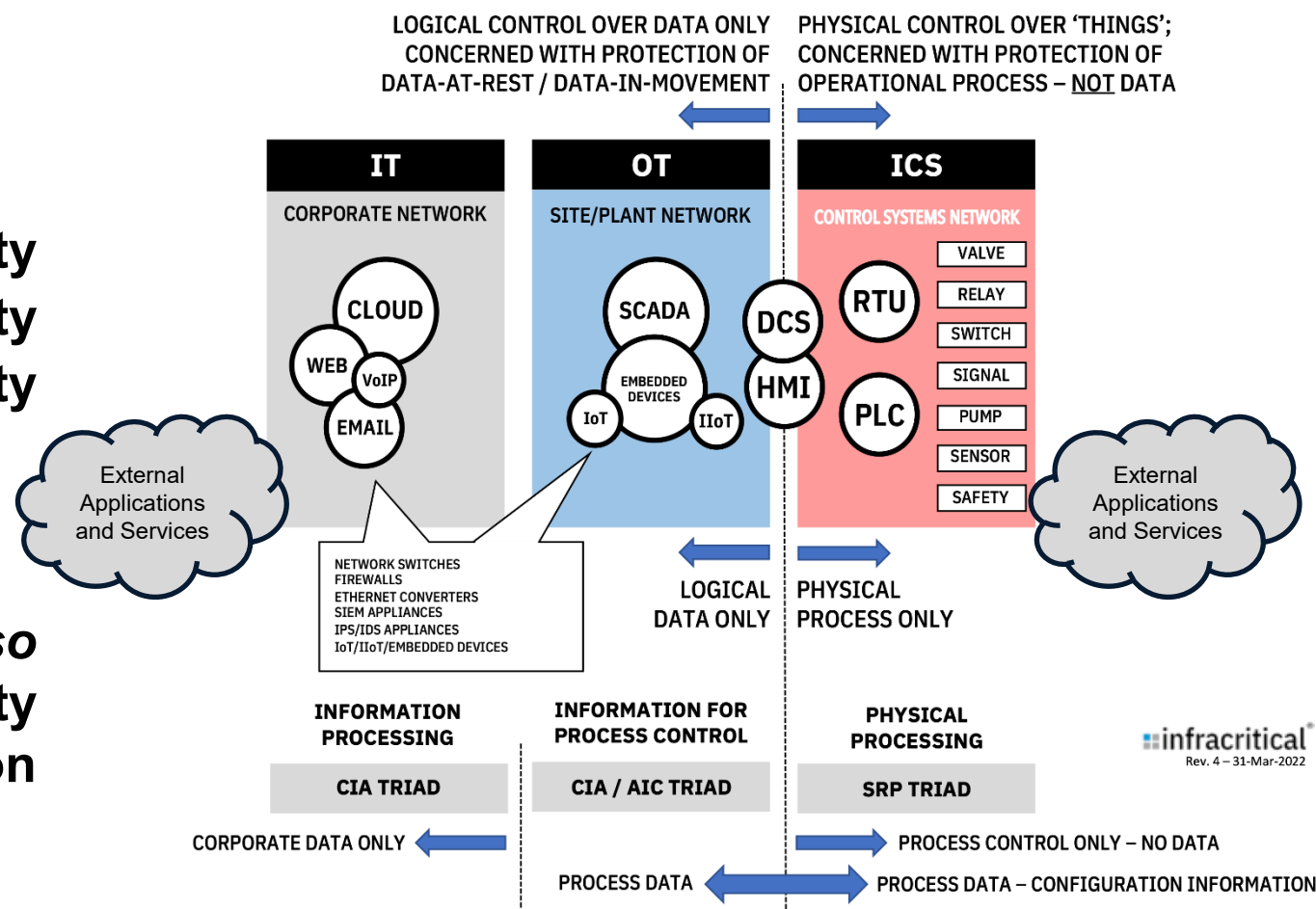
Water is a “slow” infrastructure, when compared to electric power, telecommunications, or financial



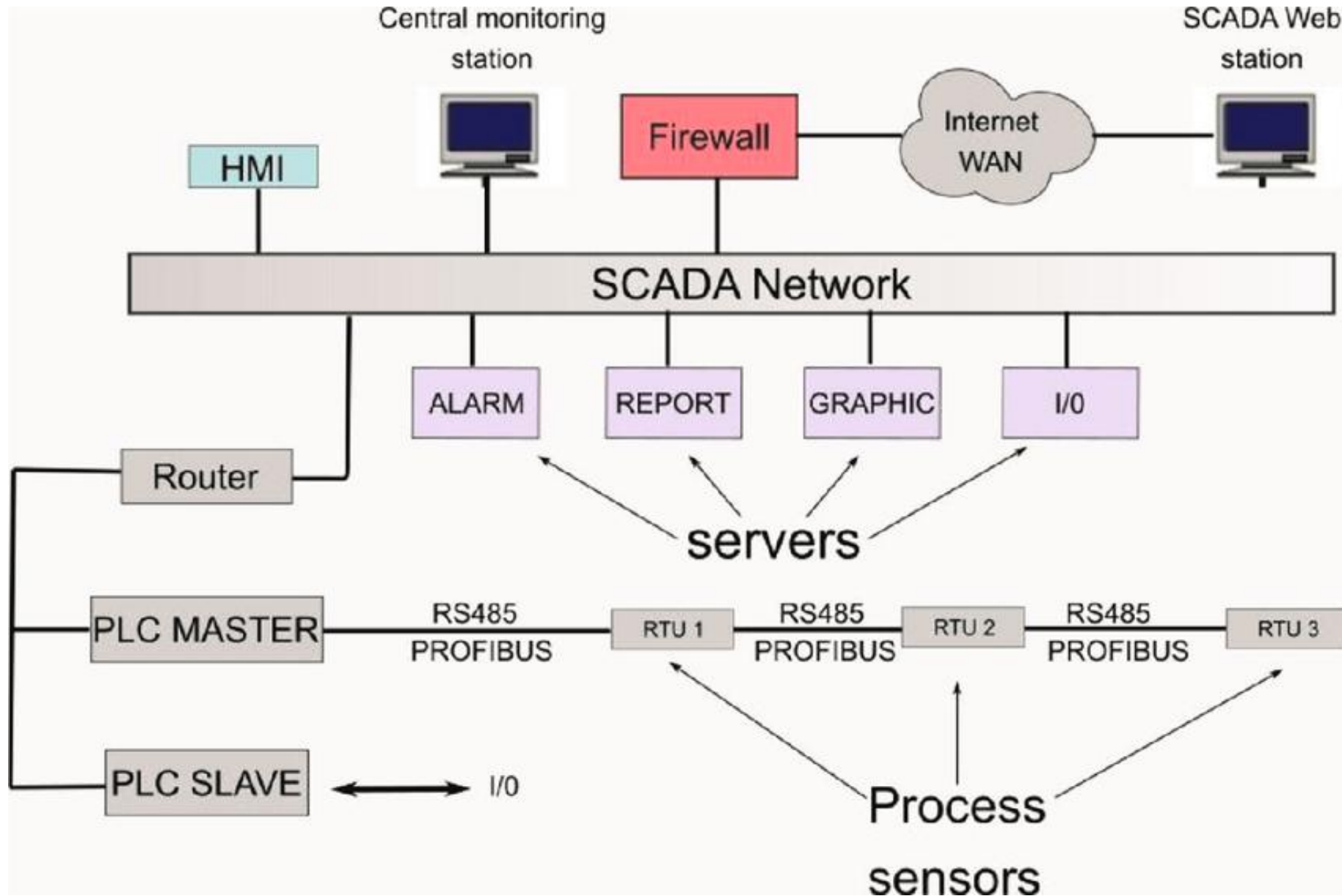
Information Technology (IT) vs Operational Technology (OT) vs Industrial Control Systems (ICS)

**Confidentiality
Integrity
Availability**

**....also
Authenticity
Non-Repudiation**



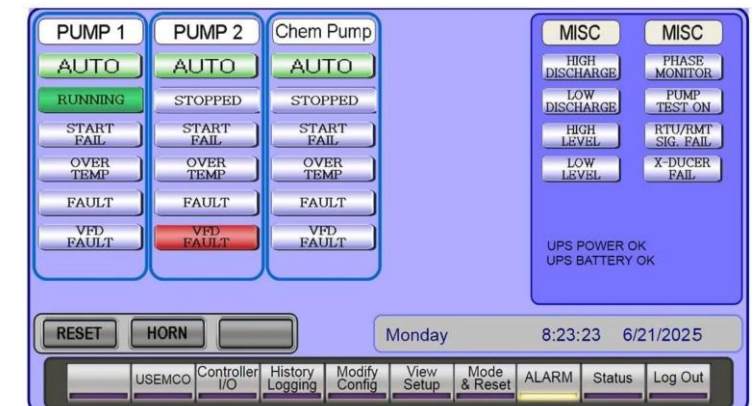
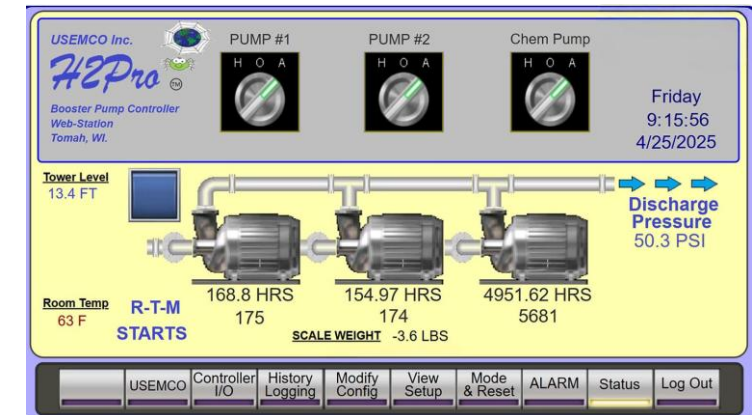
Water/Wastewater Automation Control System





Water Control Systems

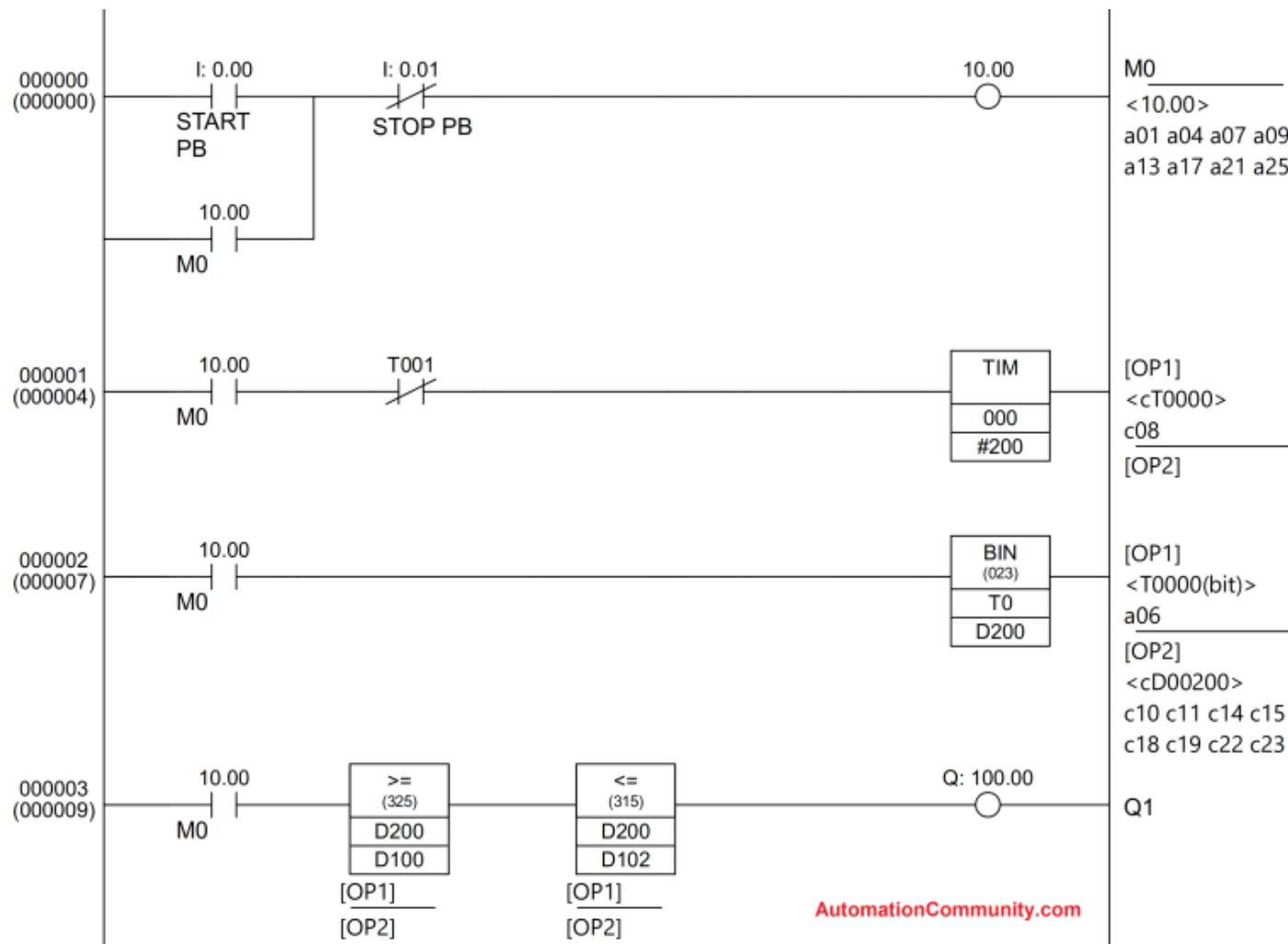
- SCADA – Supervisory Control And Data Acquisition
- PLC – Programmable Logic Controller
- RTU – Remote Terminal Unit
- Flow and Pressure Devices
 - Magnetic flow meters
 - Pressure transducers
 - Flow switches
 - Variable frequency drive pumps
- Level Control Devices
 - Ultrasonic level transmitters
 - Submersible pressure transducers
 - Float switches
- Water Quality Sensors
 - pH sensors
 - Turbidity sensors
 - Dissolved oxygen sensors





Programmable Logic Controllers

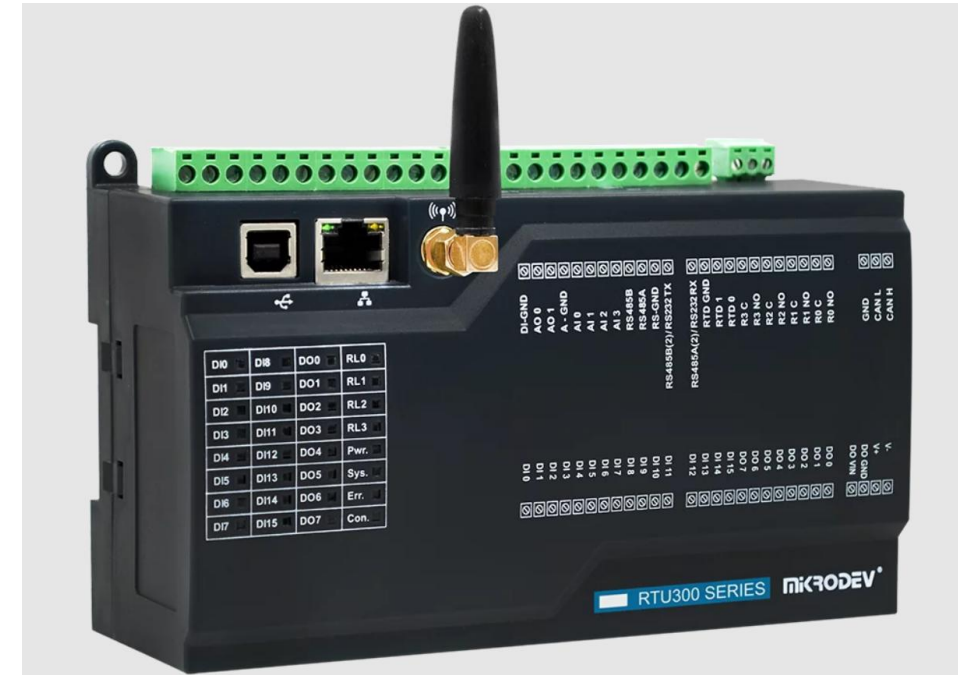
- **Industrial Computers:** Purpose-built microprocessors that automate machinery and manufacturing processes
- **Rugged Design:** Built to withstand harsh factory environments, extreme temperatures, and electrical noise
- **Real-Time Monitoring:** Continuously reads inputs (sensors, switches) and executes logic to control outputs (motors, valves)
- **Modular Scalability:** Easily expanded with specialized I/O modules to adapt to changing factory needs
- **Standardized Programming:** Utilizes intuitive languages like Ladder Logic, mimicking traditional electrical relay diagrams.
- **High Reliability:** Replaces hundreds of physical relays with code to minimize downtime and simplify troubleshooting



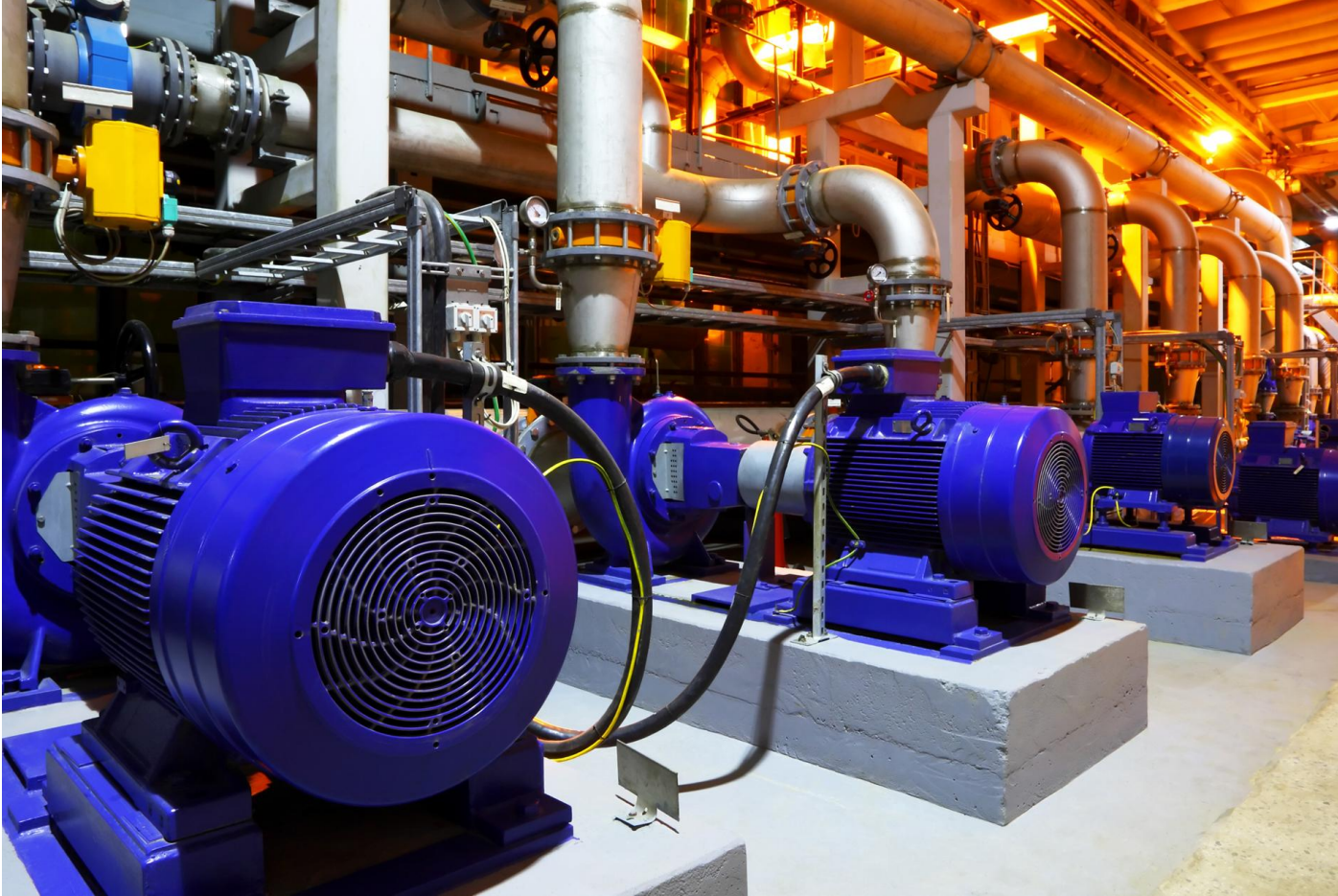


Remote Terminal Units

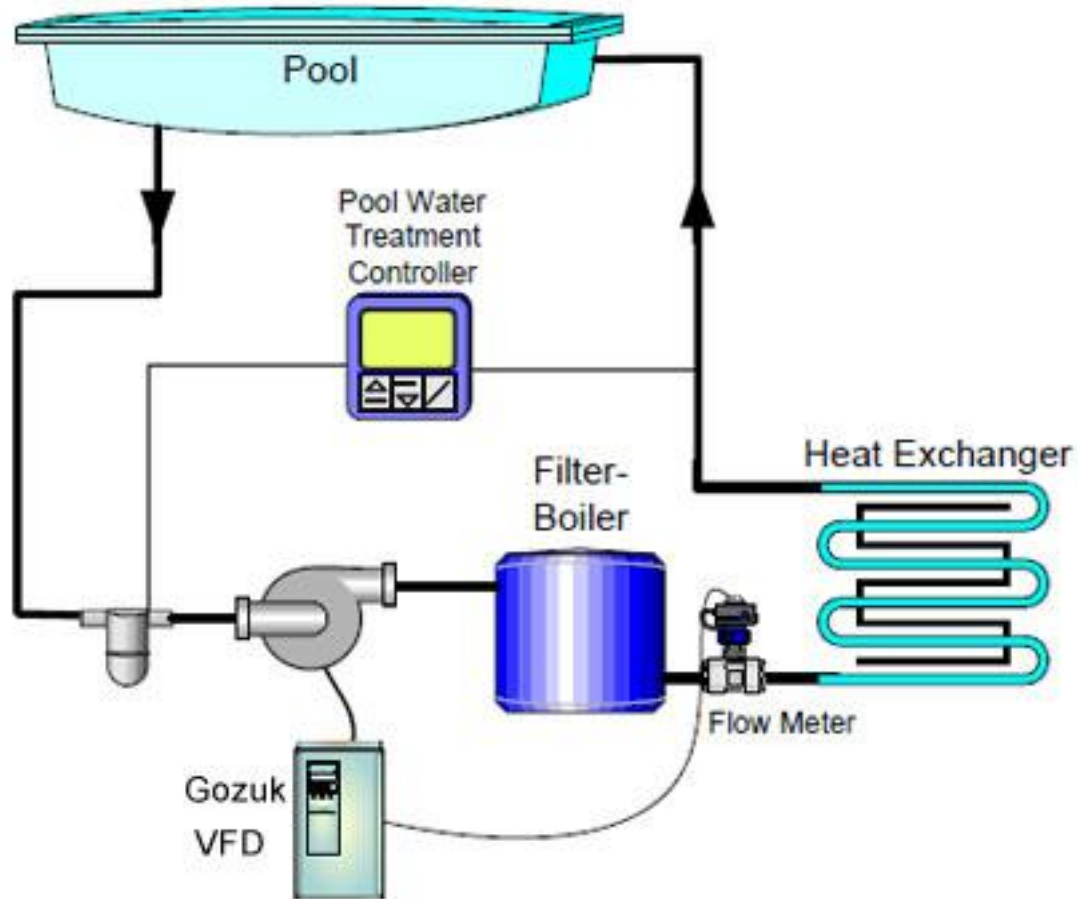
- **Field Telemetry Nodes:** Microprocessor-based devices that connect physical sensors and actuators in remote locations to a central control system
- **Long-Distance Communications:** Transmits real-time operational data across long distances using wireless, cellular, radio, or satellite networks
- **Environmental Hardening:** Designed to operate reliably in unconditioned, geographically isolated environments under extreme weather and temperature conditions
- **Autonomous Intelligence:** Capable of executing local control loops and logging critical data independently if communication with the main network drops
- **Low Power Efficiency:** Optimally engineered to run on minimal power, frequently relying on solar panels and batteries in off-grid field sites
- **SCADA Integration:** Acts as the primary eyes and ears for centralized SCADA (Supervisory Control and Data Acquisition) architectures



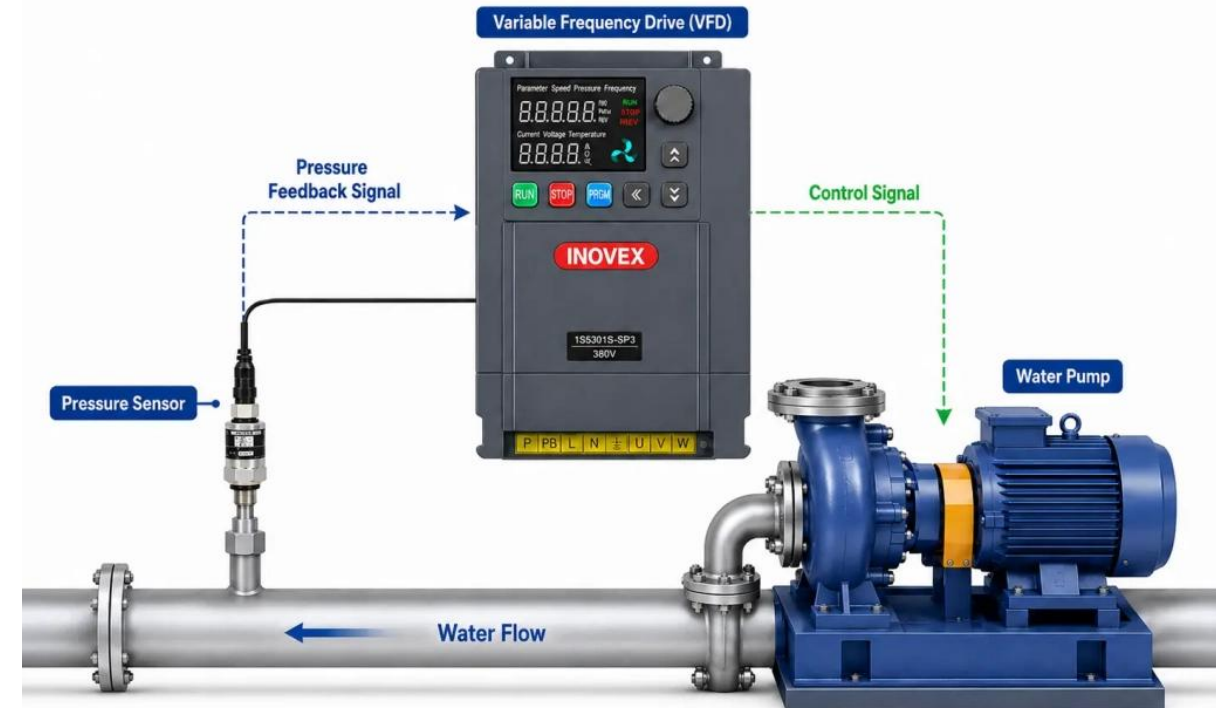
Variable Frequency Drive Pumps



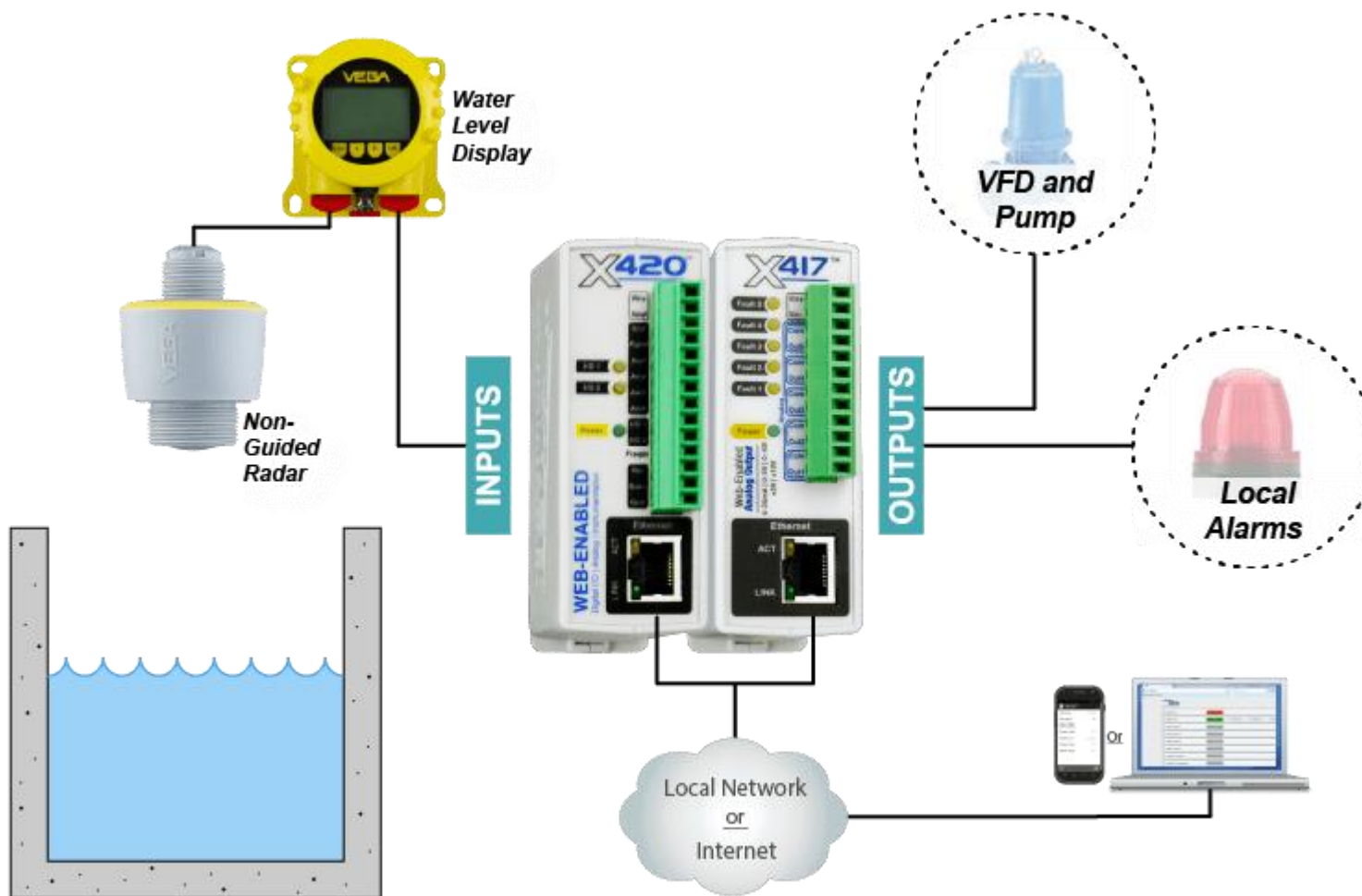
Variable frequency drive device changes the speed of the motor by adjusting the frequency and voltage of the electricity in response to water pressure changes



— Constant-Pressure Water Supply System —

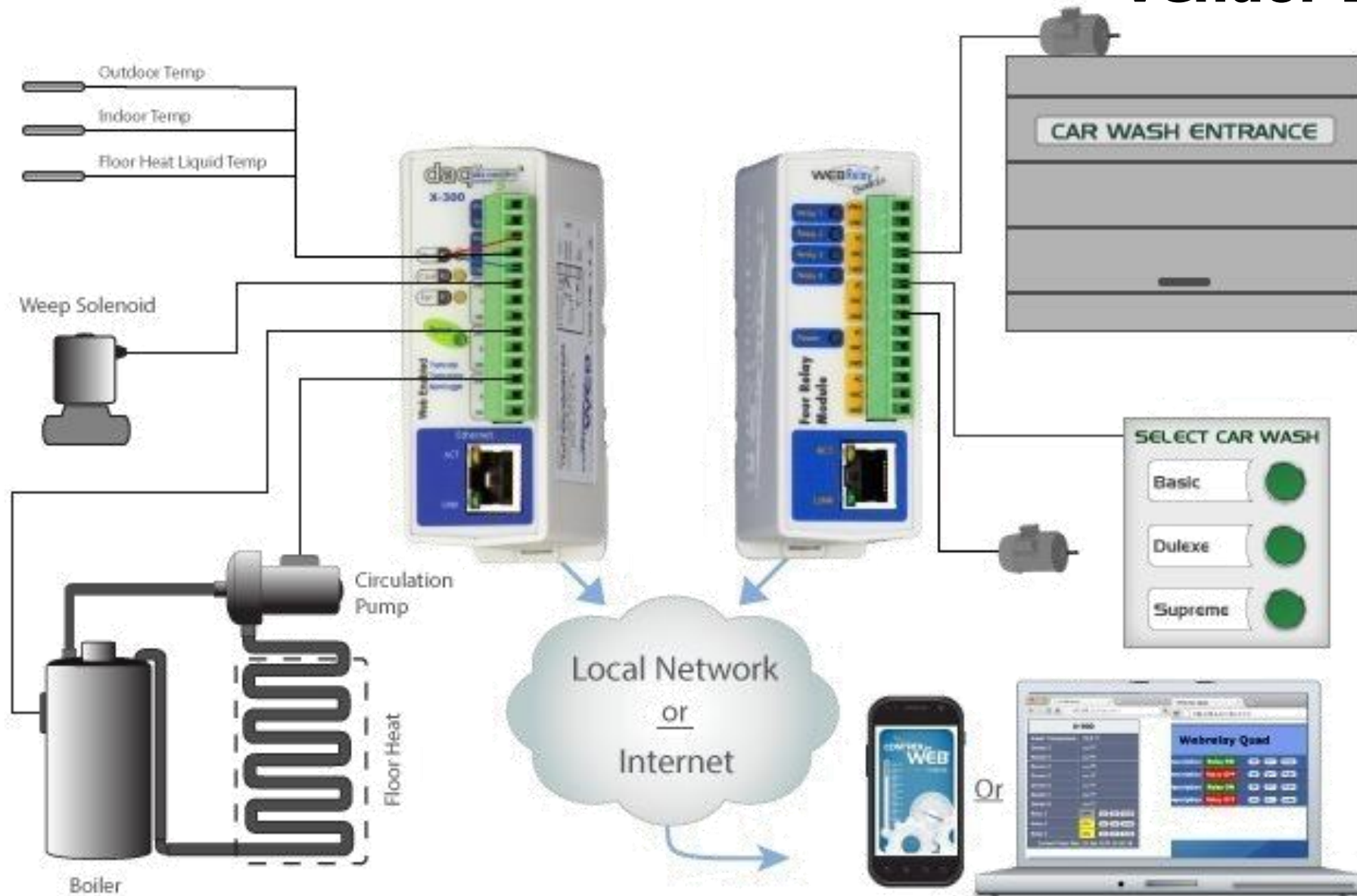


PLC Vendor Diagram



<https://controlbyweb.com/blog/water-treatment-control-system/>

Vendor Diagram



<https://controlbyweb.com/blog/car-wash-controller/>



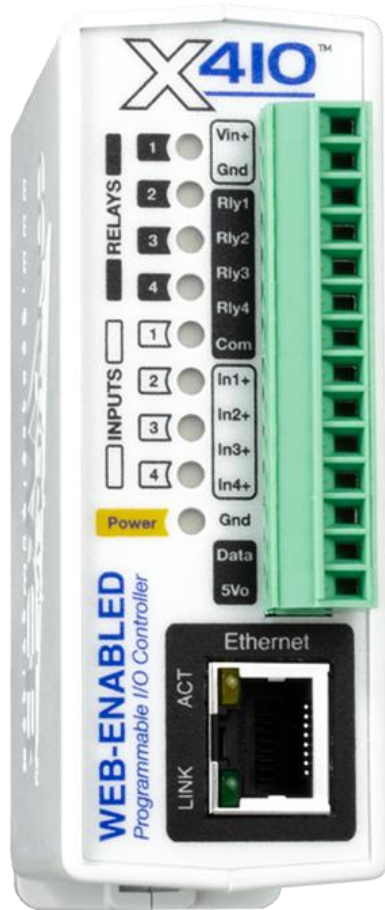
X-410™ | Edge Programmable Controller

- **The X-410™ is a versatile industrial I/O controller** with four relays, four digital inputs, and one temperature input, designed for reliable edge control. Its built-in web server allows for efficient deployment and its embedded GUI logic builder enable event-driven or scheduled automation without external software or licensing fees.
- **Through peer-to-peer communication**, the X-410™ can seamlessly expand with other ControlByWeb® devices, making it an efficient choice for system integrators and OEMs who need scalable, protocol-ready control in demanding environments.
 - 4 Relays & 4 Digital Inputs
 - Up to 16 Temperature Sensors
 - Ethernet, Cellular, or WiFi
 - 9-28VDC and/or POE
- **Cellular and WiFi are Now Available.** Note that X-410CW and X-410W models include cellular and WiFi capability respectively, which allows for more flexibility for your application.
- **Global Cellular Coverage.** Discuss international cellular options with a sales engineer.

<https://controlbyweb.com/x410/>



Cellular-enabled Programmable Logic Controller



Cell/WiFi Model (X-410CW-I) ▼

\$429.99

Select a Cellular Data Plan

- ☐ No Cellular Data Plan
- ☐ Cellular Failover – 5MB/month | \$4.99/month (Billed Annually)
- ☐ Standard – 10MB/month | \$7.99/month (Billed Annually)
- ☐ Enhanced – 30MB/month | \$14.99/month (Billed Annually)
- ☐ Advanced – 50MB/month | \$20.83/month (Billed Annually)

Cell plan prices are annual. Plans auto-renew on the anniversary of activation.



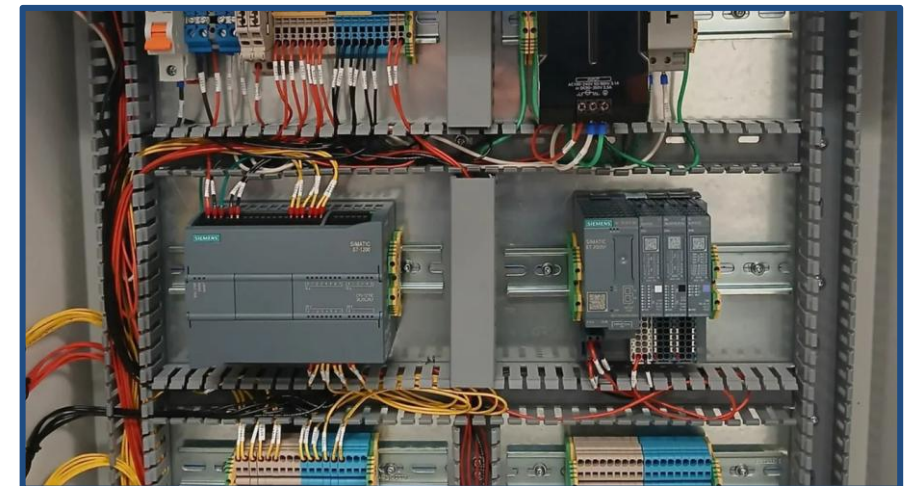
Rockwell Automation PLCs

- **The News:** An aggressive, ongoing campaign directly breached water facilities in multiple states, forcing several towns into manual operations and boil-water notices
- **The Impact:** The primary hardware targeted in these active breaches are the **MicroLogix 1100 and 1400 series** controllers
 - Hackers are exploiting an authentication bypass flaw in the Studio 5000 Logix Designer software to manipulate the controllers, alter IP addresses, and change administrative passwords to lock out legitimate operators
 - PLCs were accessible via cellular modems



Siemens PLCs

- **The News:** U.S. authorities issued a high-alert advisory warning that hackers are actively utilizing **AI-generated exploit scripts** written in Python to scan, identify, and fingerprint internet-exposed **Siemens S7 Series PLCs**
- **The Impact:** The attacks target manufacturing, energy, and water facilities
 - While the current activity is primarily highly automated reconnaissance and capability building, agencies warn it is direct preparation for potential future disruptions
 - Particular vulnerabilities include the legacy **S7-1200 series** devices





Schneider Electric PLCs

- **The News:** Federal agencies updated their multi-agency safety alerts to formally expand the scope of active threat tracking to **Schneider Electric** hardware
- **The Impact:** Specifically, attackers have been caught trying to interact with and exploit **Schneider Electric BMX P34** and **Modicon M340** PLCs

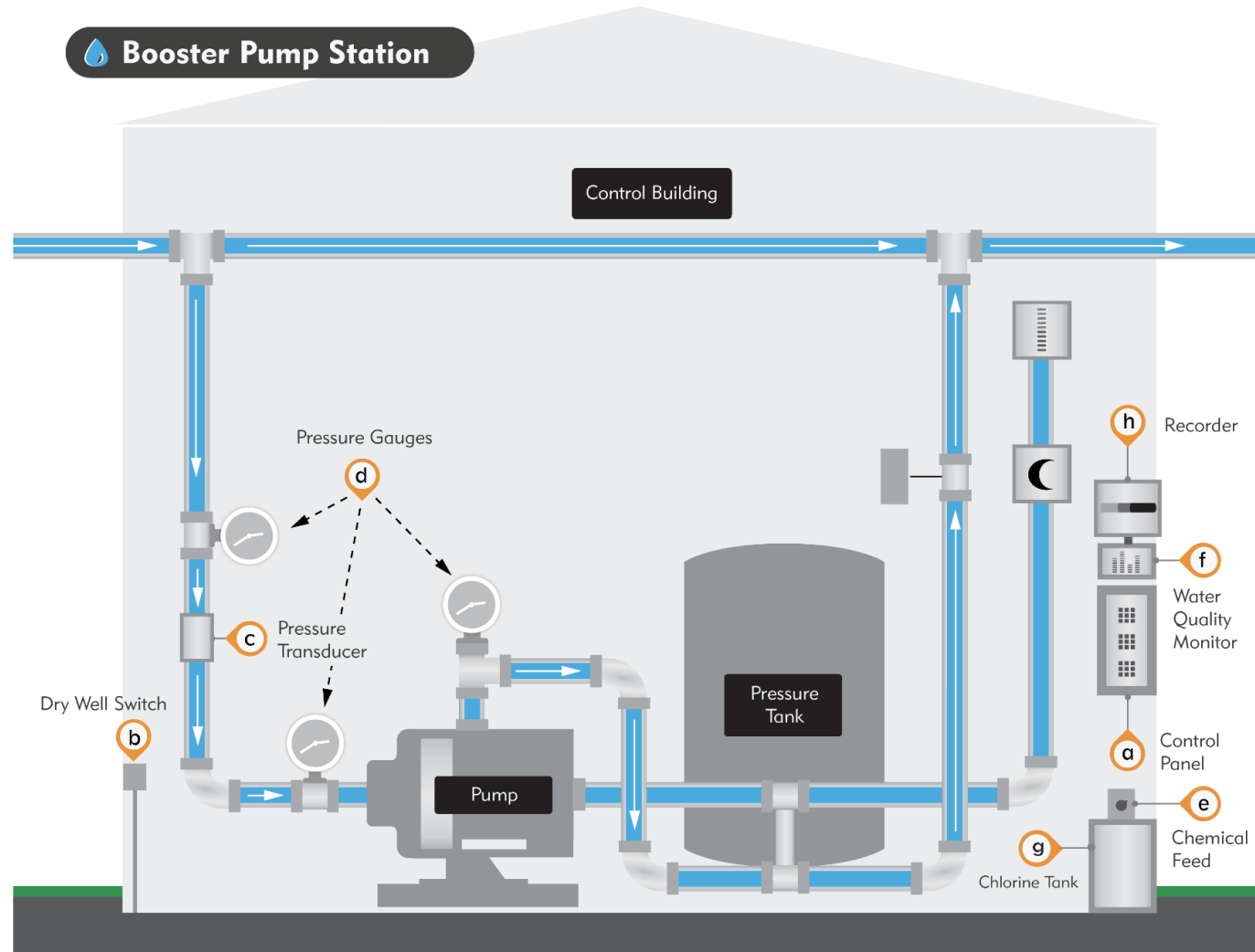
<https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-097a>



- **The News:** While older news relative to this summer's sudden spikes, **Unitronics** hardware remains a heavy fixture in federal tracking and incident response reporting
- **The Impact:** Attacks initially targeted **Unitronics Vision Series** PLCs with integrated Human-Machine Interfaces (HMIs) by *exploiting default factory passwords*, which continues to serve as the baseline case study for the current defensive push to disconnect PLCs from the public internet entirely



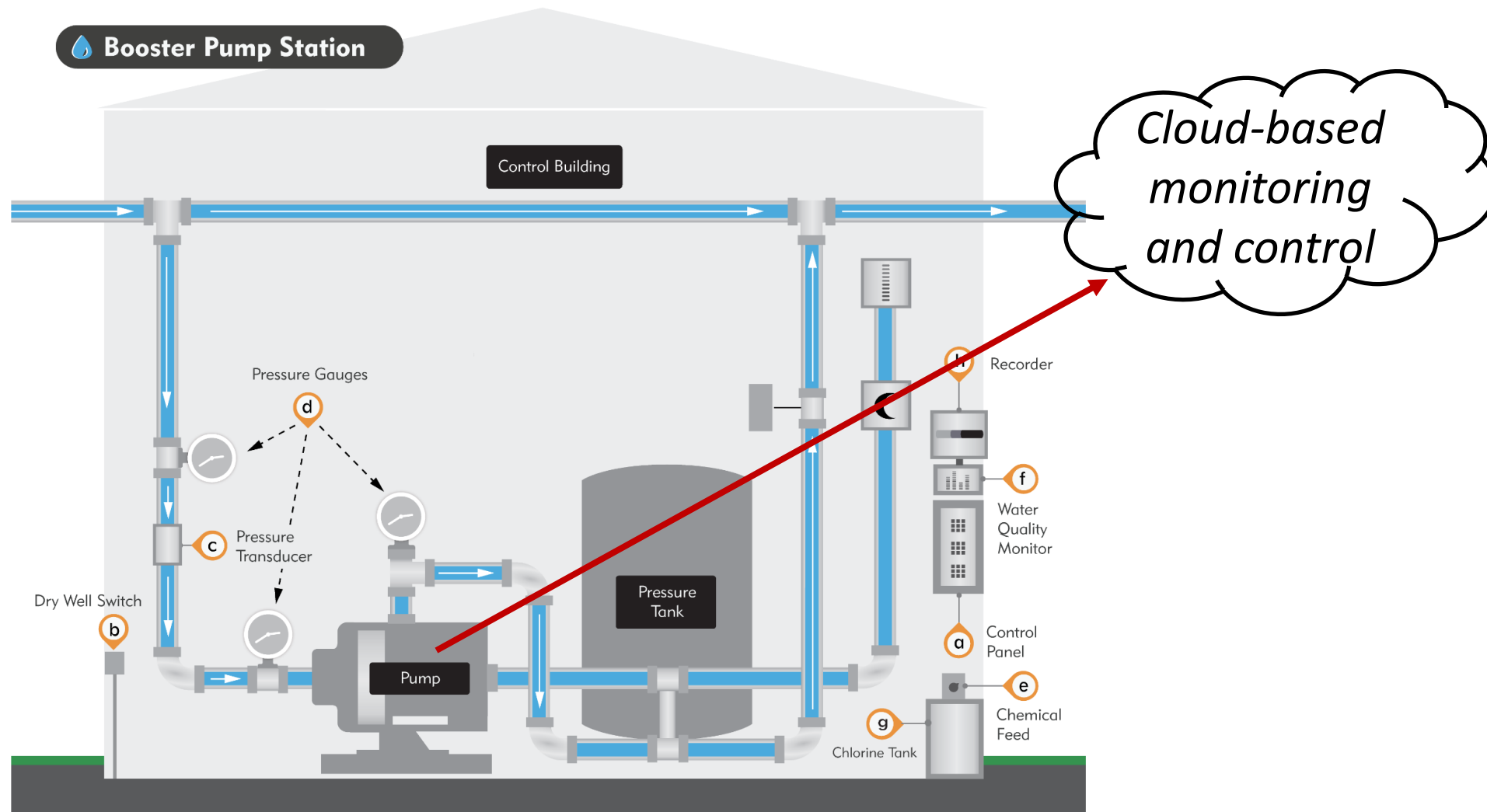
Water Booster Pump Station



Water Booster Pump Station Archives App4Water

https://bm Lovesk.xyz/product_details/13200675.html

Water Booster Pump Station



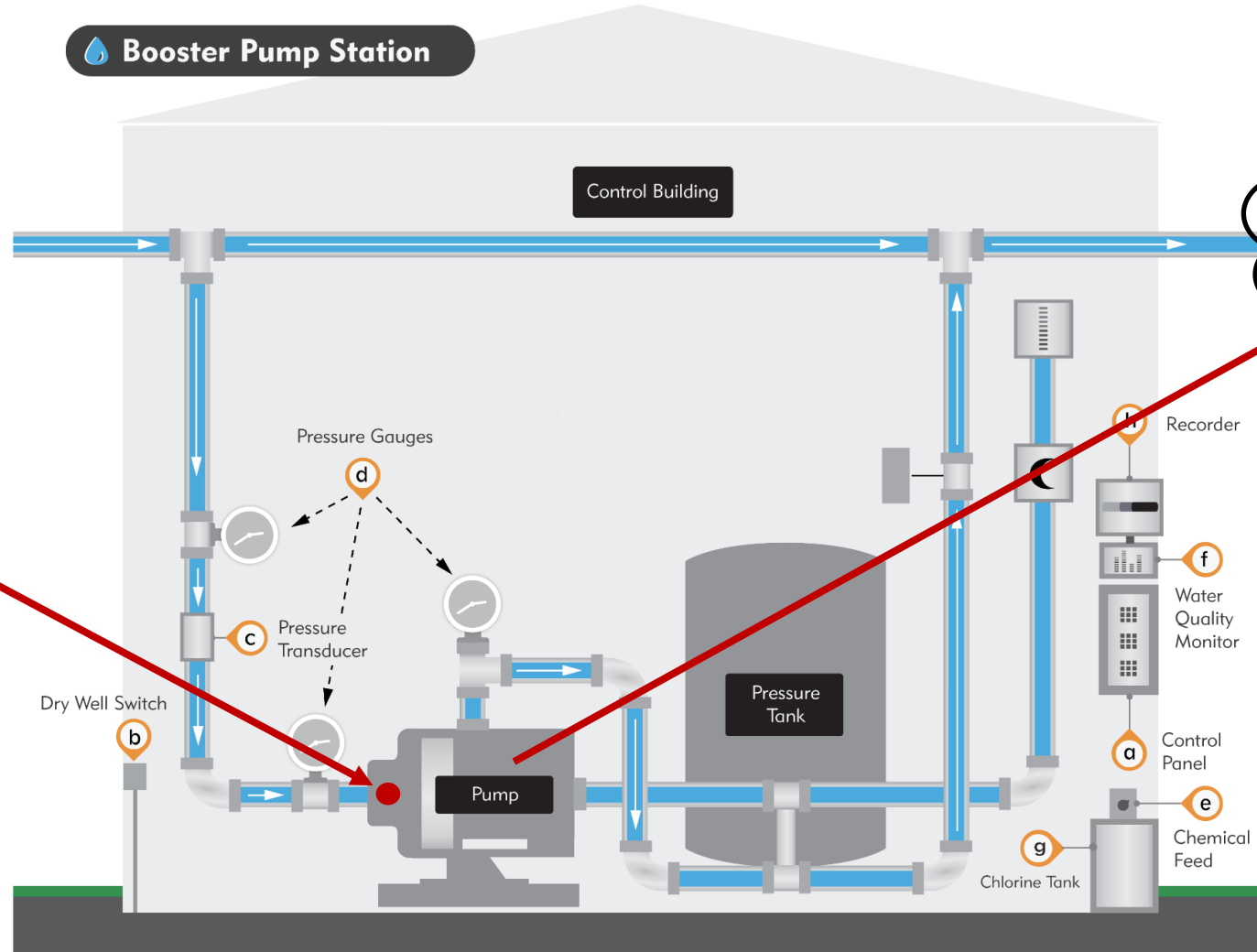
Water Booster Pump Station Archives App4Water

https://bmxmlvesk.xyz/product_details/13200675.html

Water Booster Pump Station

Booster Pump Station

*Mechanical
Time Delay
Relay*



*Cloud-based
monitoring
and control*



A Growing Concern: IoT Devices

Shodan

Developers Book View All... Show API Key

SHODAN

Explore Downloads Reports Enterprise Access Contact Us My Account Upgrade

The search engine for Water Systems

Shodan is the world's first search engine for Internet-connected devices.

Create a Free Account Getting Started

Explore the Internet of Things
Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

See the Big Picture
Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

Monitor Network Security
Keep track of all the computers on your network

Get a Competitive Advantage
Who is using your product? Where are they



Search for "Allen-Bradley"

Shodan

Maps

Images

Monitor

Developer

More...

SHODAN

Explore

Downloads

Pricing

Allen-Bradley country:"US"

Account

TOTAL RESULTS

2,505

TOP CITIES

Chicago

277

Dallas

256

San Jose

136

Reston

80

New York City

78

More...

TOP PORTS

44818

2,442

161

61

80

1

502

1

TOP ORGANIZATIONS

Verizon Business

1,756

AT&T Enterprises, LLC

108

T-Mobile USA, Inc.

58

Comcast Cable

40

Communications, LLC

35

Charter Communications Inc

35

View Report

View on Map

Advanced Search

Access Granted: Want to get more out of your existing Shodan account? Check out [everything you have access to.](#)

166.249.200.191

2026-08-26T19:06:16

Verizon Business

United States, Frederick

Product name: 1769-L33ER/A LOGIX5333ER

Vendor ID: Rockwell Automation/**Allen-Bradley**

Serial number: 0x60eb9569

Device type: Programmable Logic Controller

Device IP: 192.168.0.2

166.153.66.251

2026-08-26T23:17:55

Verizon Business

United States, Fannett

Product name: 2080-L50E-24AWB

Vendor ID: Rockwell Automation/**Allen-Bradley**

Serial number: 0x70c3be7c

Device type: Programmable Logic Controller

Device IP: 192.168.1.50

107.190.155.225

2026-08-26T23:04:34

225.107-190-155-net.sccoast.net

Horry Telephone Cooperative, Inc.

United States, Prospect

Product name: 1766-L32BXBA C/21.02

Vendor ID: Rockwell Automation/**Allen-Bradley**

Serial number: 0x60cae016

Device type: Programmable Logic Controller

Device IP: 192.168.2.2

166.143.97.218

2026-08-26T22:45:42

Verizon Business

United States, Lynchburg

Product name: 1766-L32BWA B/11.00

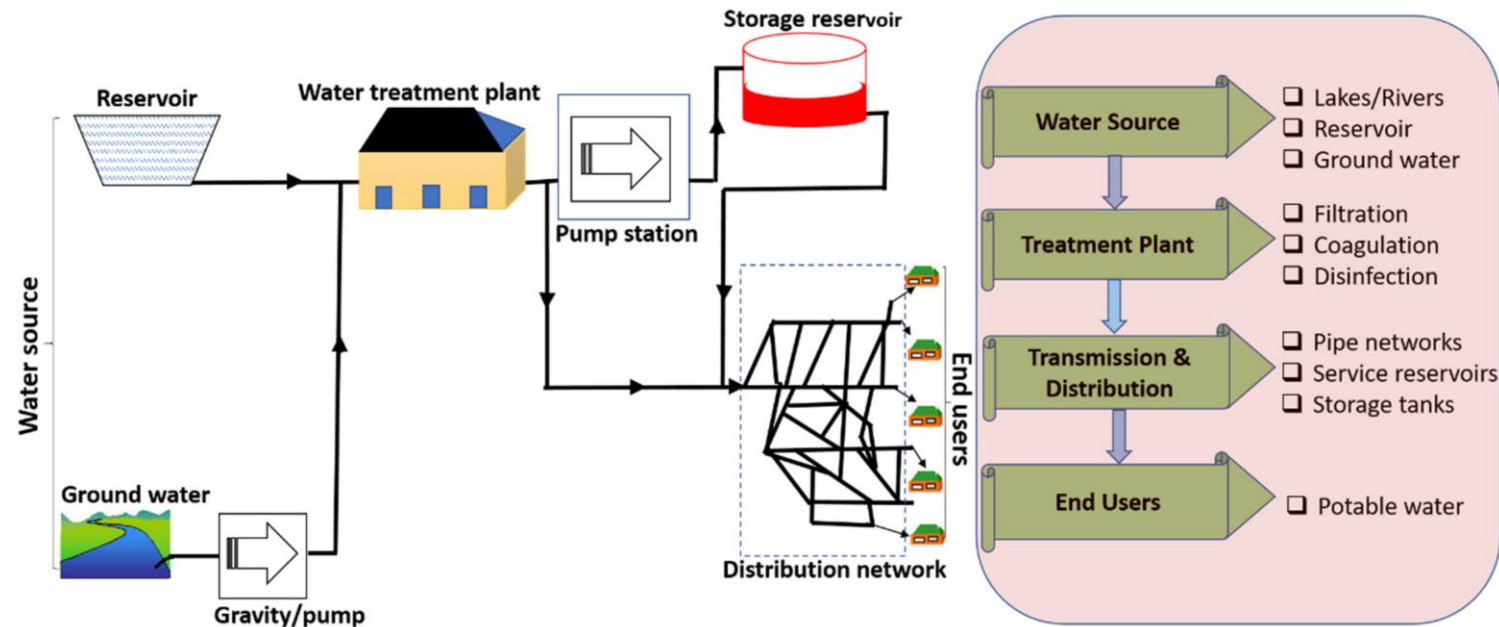
Vendor ID: Rockwell Automation/**Allen-Bradley**

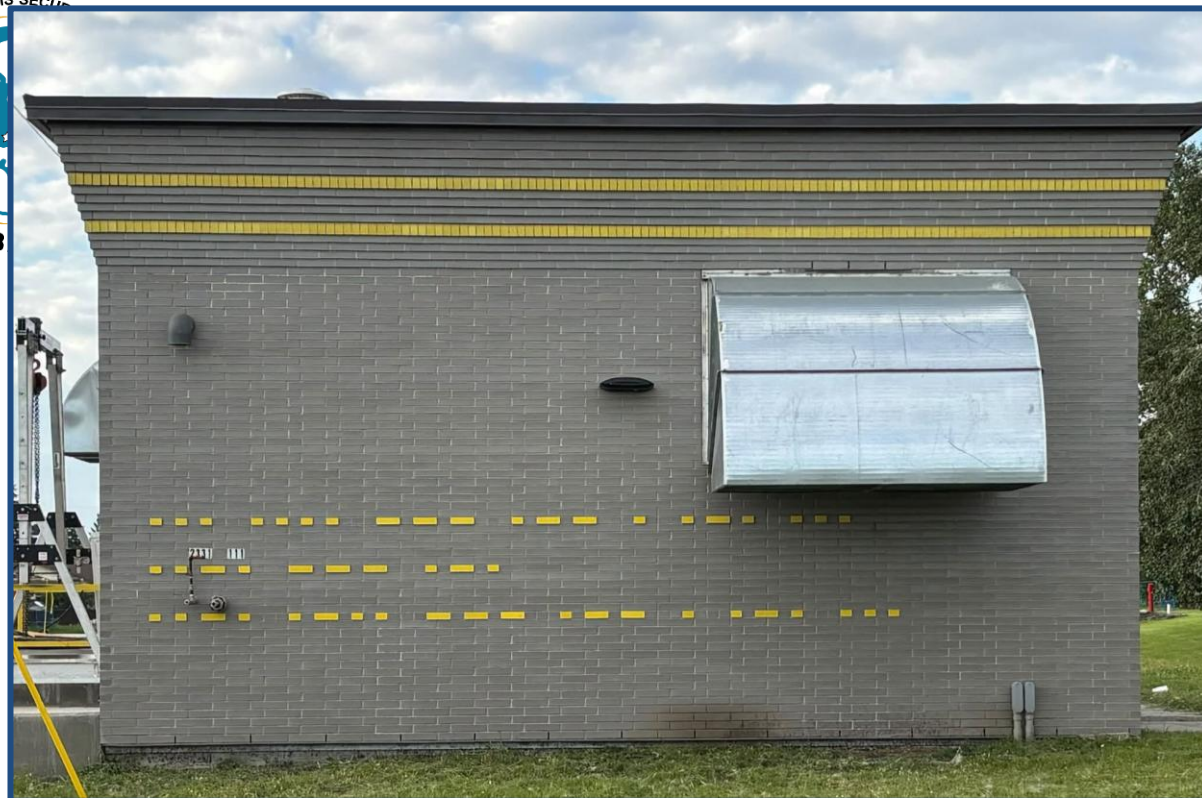
Serial number: 0x406187c1

Device type: Programmable Logic Controller

Device IP: 192.168.10.10

- Water systems are physical systems increasingly controlled by digital systems
- Water usually moves slowly; control commands do not
- Cyber compromise matters when it changes the ability to observe, control, or safely operate the process
- The objective is safe water and contained wastewater, even when part of the digital system fails
- Cyber systems can command the process, but physics determines what happens next





Edmonton, Alberta





Cybersecurity in America's Water Systems

Marcus H. Sachs, P.E.

SVP & Chief Engineer, Center for Internet Security

August 27, 2026

Questions?

