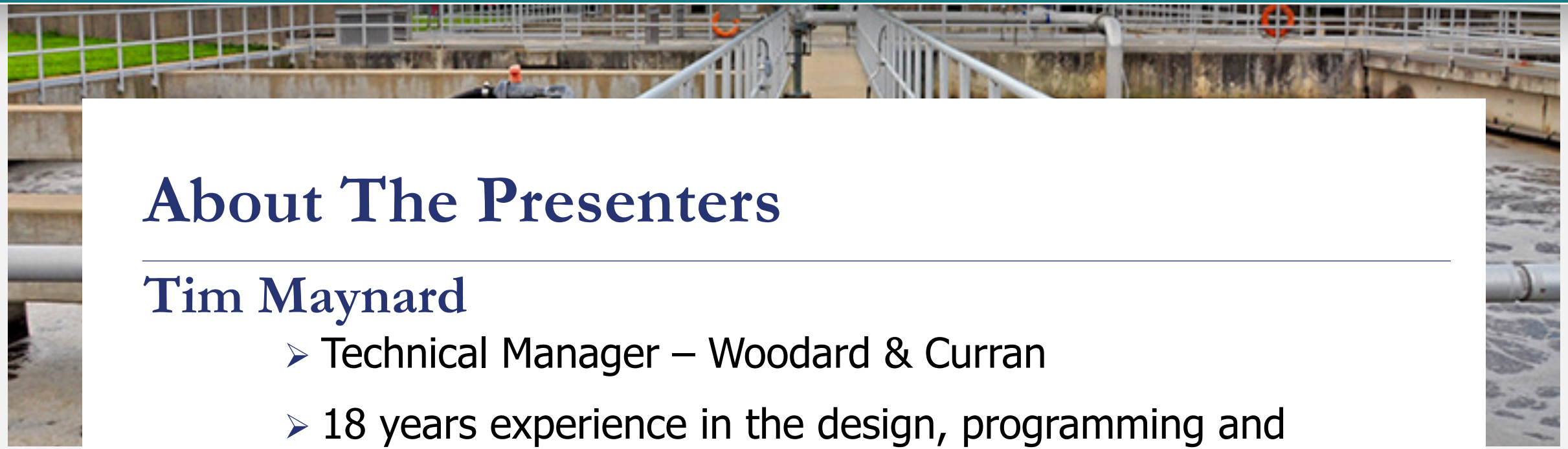
Woodard & Curran

LOWELL WATER
Community-Health-Environment

Lowell Water Utilities –

SCADA Upgrades



About The Presenters

Tim Maynard

- Technical Manager – Woodard & Curran
- 18 years experience in the design, programming and implementation of control systems in the industrial, manufacturing, food and beverage, municipal and industrial water/wastewater markets.

Evan Walsh

- Engineering Supervisor – Lowell Water
- Grade 7-C Operator, 10 years assisting in Operational Support at the facility.

LOWELL WATER
Community-Health-Environment

Lowell Water Utilities –
SCADA Upgrades Agenda

- Project Overview Goals
- Existing SCADA System Architecture
- Proposed SCADA System Architecture
- Remote Access Approach
- Summary and Conclusions

LOWELL WATER
Community-Health-Environment

Lowell Water Utilities –
Project Motivation

- 3 Main Goals for the project:
  - Operational Efficiencies
  - Risk Management
  - Long Term Cost Savings

LOWELL WATER
Community-Health-Environment

SCADA Remote Access - Efficiency

- Real Time Access/Feedback
  - Diagnose issues before sending personnel onsite
  - Ease of maintenance tasks at remote facilities
- Enable troubleshooting when access is challenging (e.g. weather)
- Emergency situations can be evaluated instantaneously
- Ordinance employees can be the first line of response to reduce call-ins and overtime costs
- Integration with other software to maximize use (HACH WIMS, CMMS, etc.)

LOWELL WATER
Community-Health-Environment

SCADA Remote Access - Risk Management

- Acceptable Risk
  - False sense of security
    - Air-gapped systems still vulnerable
  - Security Maintenance Team (Lowell Water, MIS, & W&C)
    - Three-layered support team
    - Strength at all three levels
- Risk Ownership
  - Responsibility for accepting risk associated with Lowell's water infrastructure belongs to the Water Utility Executive Director
- Centralized User Management
  - Managing SCADA access privileges

LOWELL WATER
Community-Health-Environment

SCADA Remote Access - Risk Management

- Managing and operating two utilities that are physically separated
  - SCADA Manager, Maintenance Superintendent, and Operation Superintendents
- Improved operational awareness minimizes consequence of failures
  - Public health and safety
  - Environmental damage
  - Equipment cost

LOWELL WATER
Community-Health-Environment

SCADA Remote Access - Cost Savings

- Staffing
  - Operations staff can be deployed more effectively
  - Reduce overtime costs and off hour call-ins
  - Connect systems together eliminates redundant SCADA manager positions
- Contracted Services
  - Support from contractors can be drastically reduced
- Hardware
  - Less expensive hardware at each node; easier to replace
  - Longer lifecycle and lower cost

LOWELL WATER
Community-Health-Environment

SCADA Definitions - Alphabet Soup

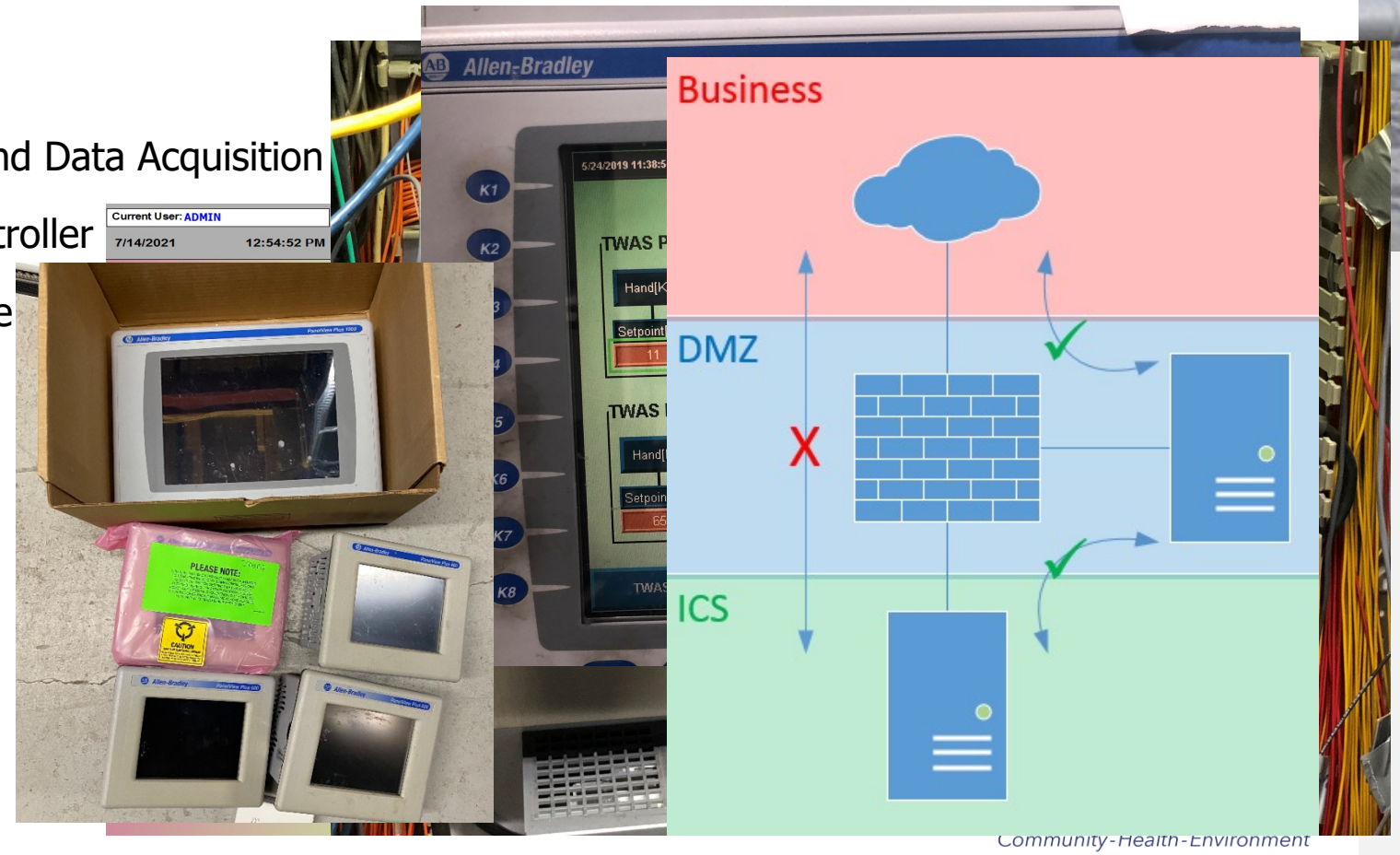
Acronyms

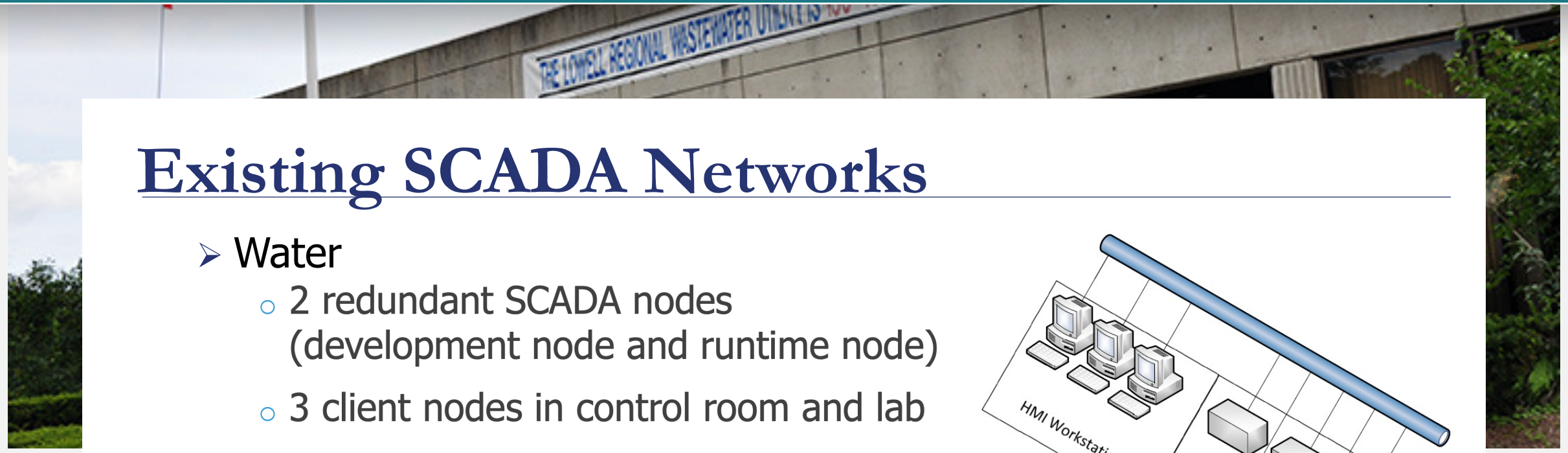
SCADA – Supervisory Control And Data Acquisition

PLC – Programmable Logic Controller

HMI – Human Machine Interface

DMZ – Demilitarized Zone





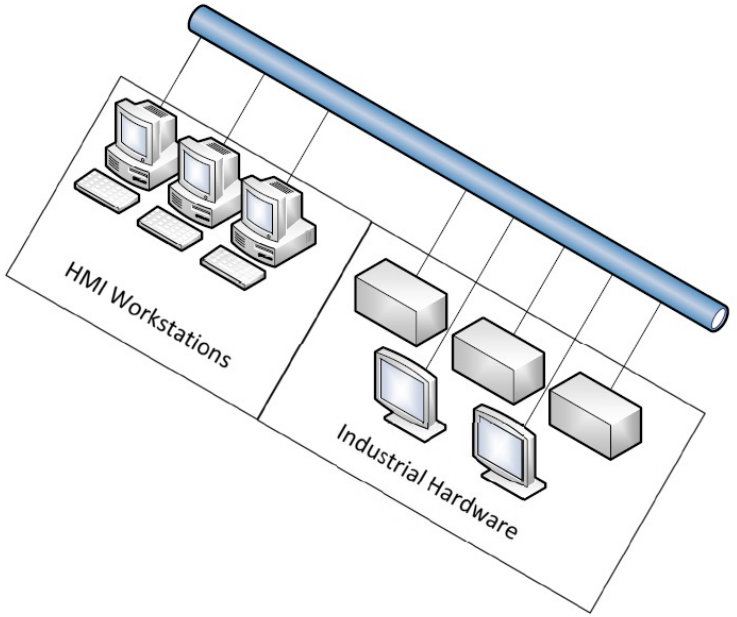
Existing SCADA Networks

- Water
  - 2 redundant SCADA nodes (development node and runtime node)
  - 3 client nodes in control room and lab
- Wastewater
  - 2 redundant SCADA nodes (development node and runtime node)
  - 12 client nodes, at strategic locations throughout the facility

LOWELL WATER
Community-Health-Environment

Existing SCADA Networks

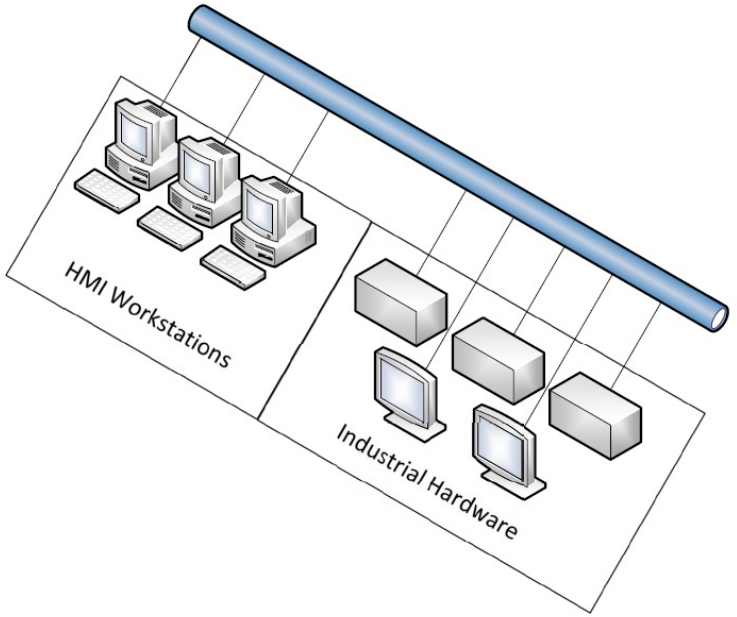
- Large Flat Networks
- Each SCADA node is a full Windows PC
  - Often an additional PC on an employee's desk
  - Update requirements
  - Hardware Cost/labor to replace
- Software licensing is costly
- Manual Access To Data



LOWELL WATER
Community-Health-Environment

Existing SCADA Networks

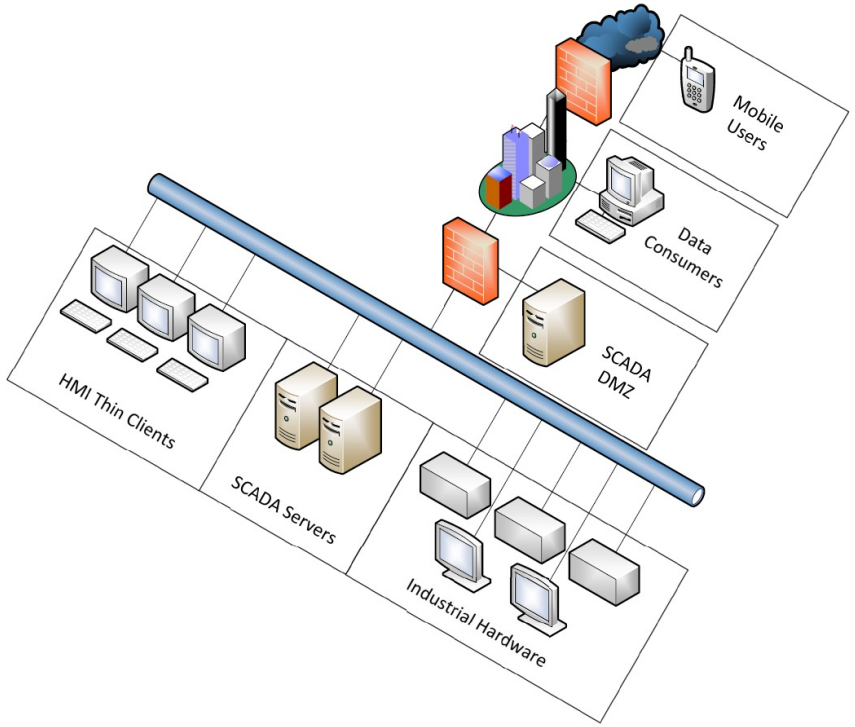
- Updates can only be done from the Development Node
  - Updates need to be manually copied to the clients
- False Sense of Security



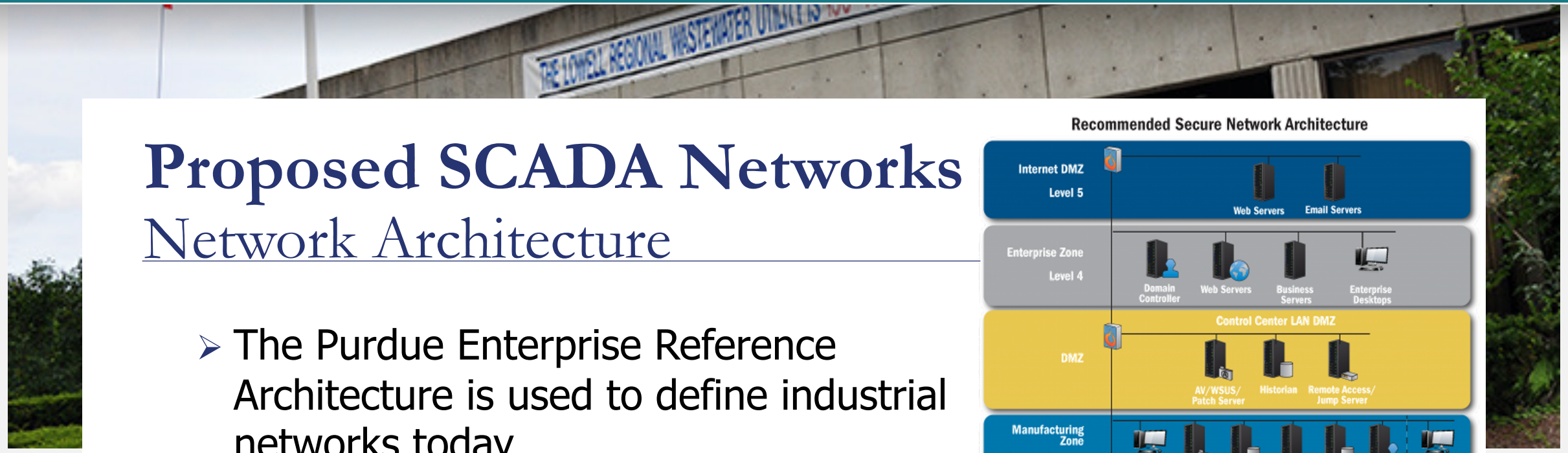
LOWELL WATER
Community-Health-Environment

Proposed SCADA Networks

- Server/client architecture for HMIs to promote expandability and versatility
- Securely provide data to external systems (ex: CMMS)
- Facilitate access to all facilities from common resources (e.g. SCADA Manager)
- Secure remote access to facilities



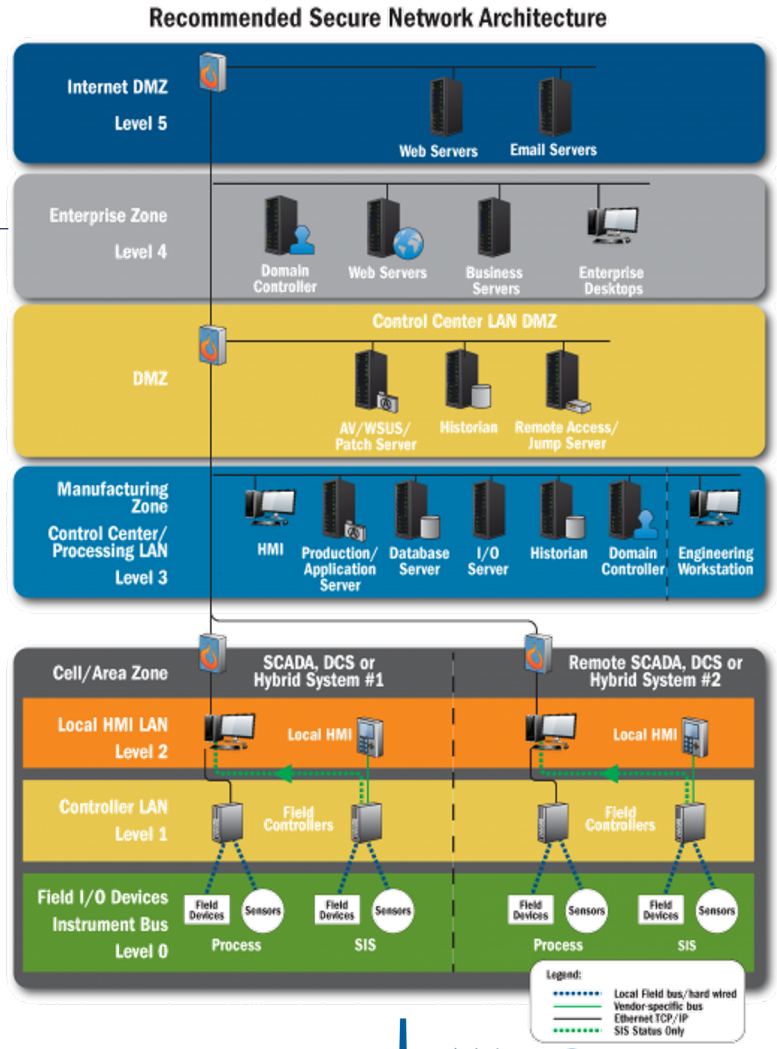
LOWELL WATER
Community-Health-Environment



Proposed SCADA Networks

Network Architecture

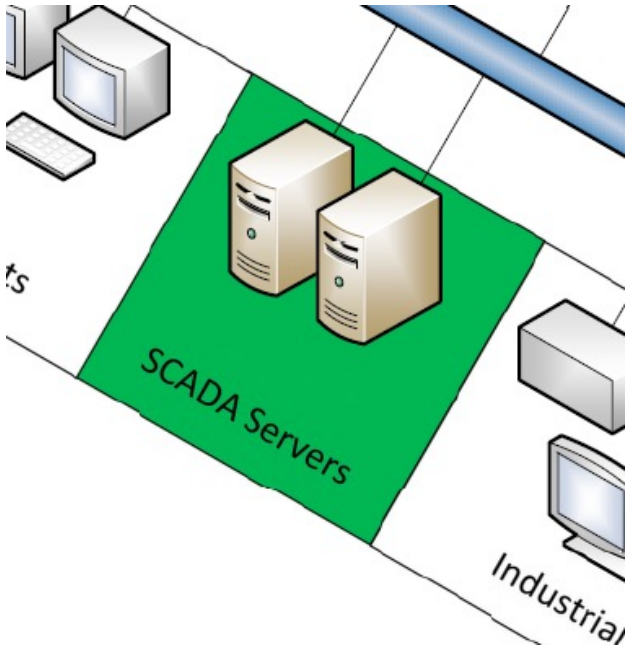
- The Purdue Enterprise Reference Architecture is used to define industrial networks today
- Segment network into levels and zones
- Access policies for data to traverse levels



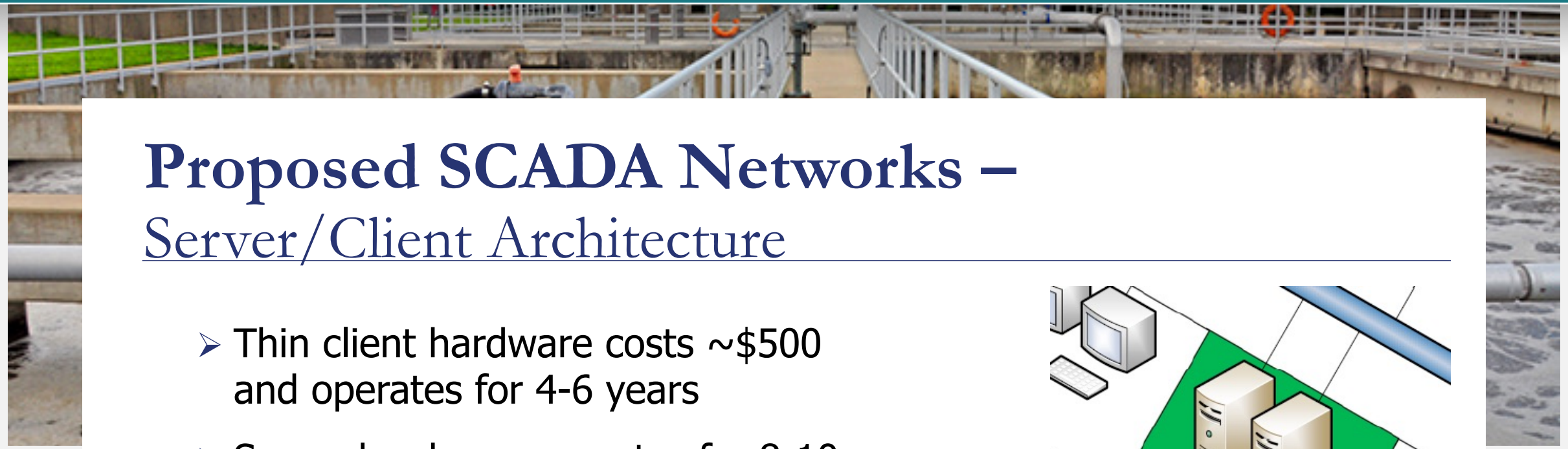
LOWELL WATER
Community-Health-Environment

Proposed SCADA Networks –
Server/Client Architecture

- Two redundant servers, located in secure locations
- Engineering workstation (not pictured) for server administration and programming
- Thin client hardware at all other current locations, including main SCADA nodes in control rooms

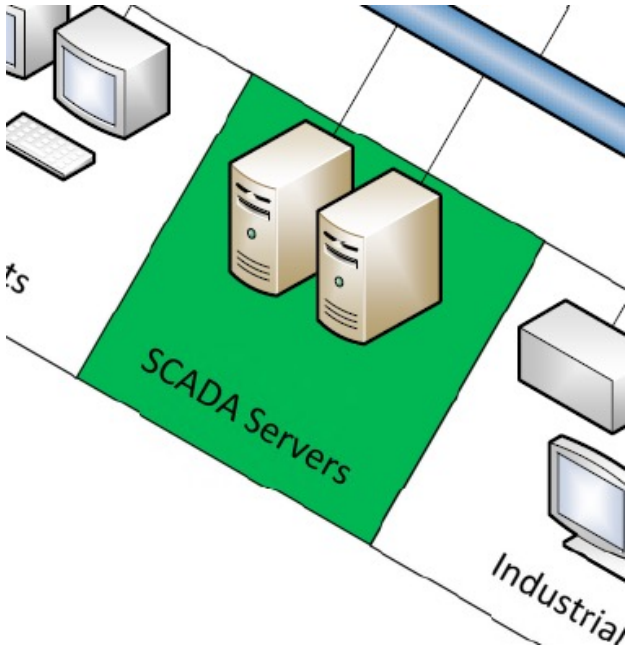


LOWELL WATER
Community-Health-Environment



Proposed SCADA Networks –
Server/Client Architecture

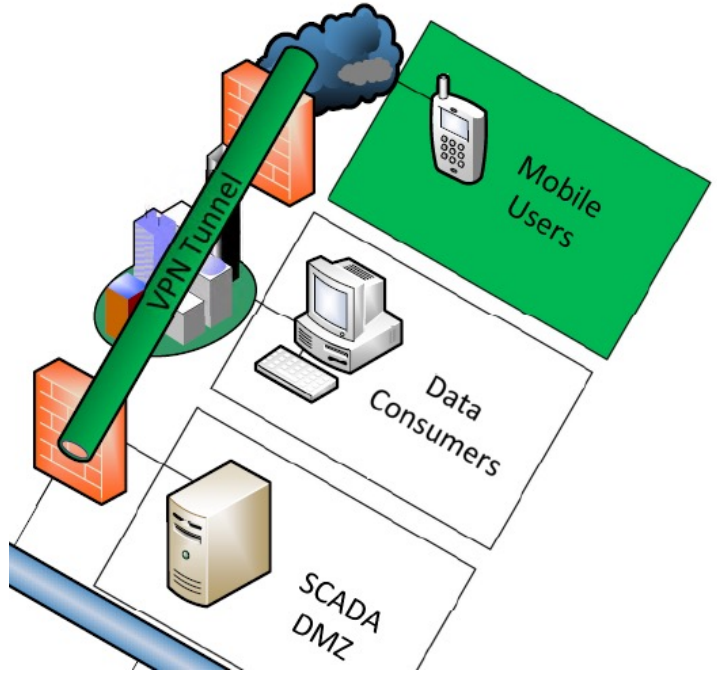
- Thin client hardware costs ~$500 and operates for 4-6 years
- Server hardware operates for 8-10 years
- Does not run a native OS, so does not become obsolete
- Hardware replacement in 10 minutes, as opposed to 4-8 hours
- Lower long-term maintenance costs



LOWELL WATER
Community-Health-Environment

Proposed SCADA Networks - Remote Access

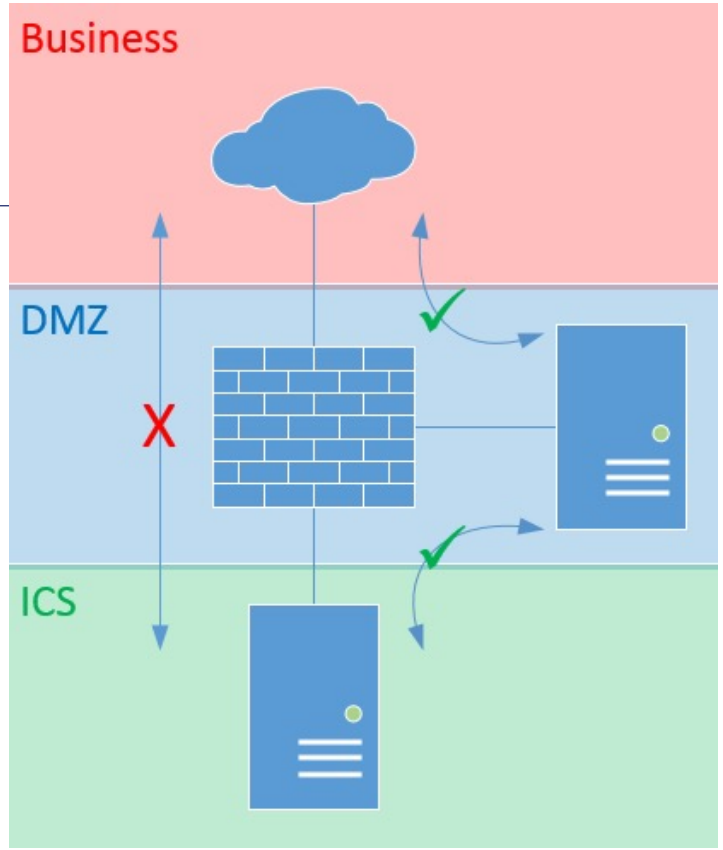
- DMZ & firewall facilitates secure remote access to SCADA networks
- Multifactor authentication used for added security
- Remote access privileges restricted by user requirements
- Ability to monitor and audit system activity (accountability)
- May disconnect facility firewall and inhibit remote access without affecting SCADA operations



LOWELL WATER
Community-Health-Environment

DMZ Architecture –
Industry Standard

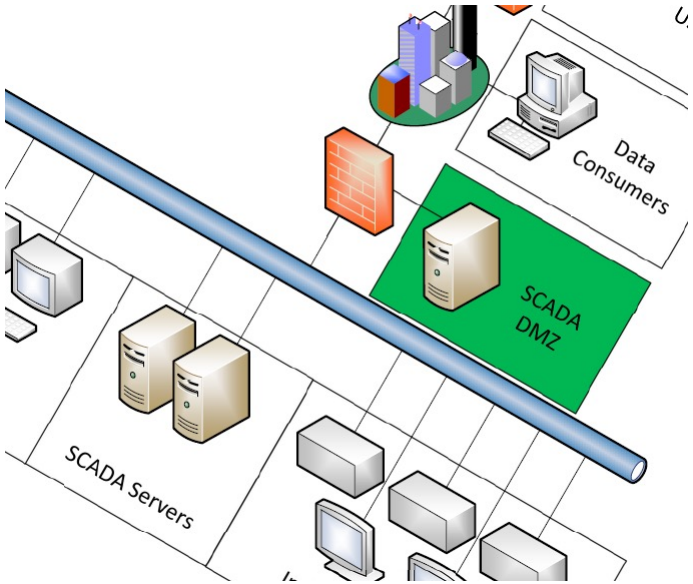
- Used to move data into and out of a secure zone of a network
- Traffic not allowed to pass directly between business and ICS networks
- Traffic must terminate in DMZ
- Hardware/software in DMZ facilitates required communication as needed



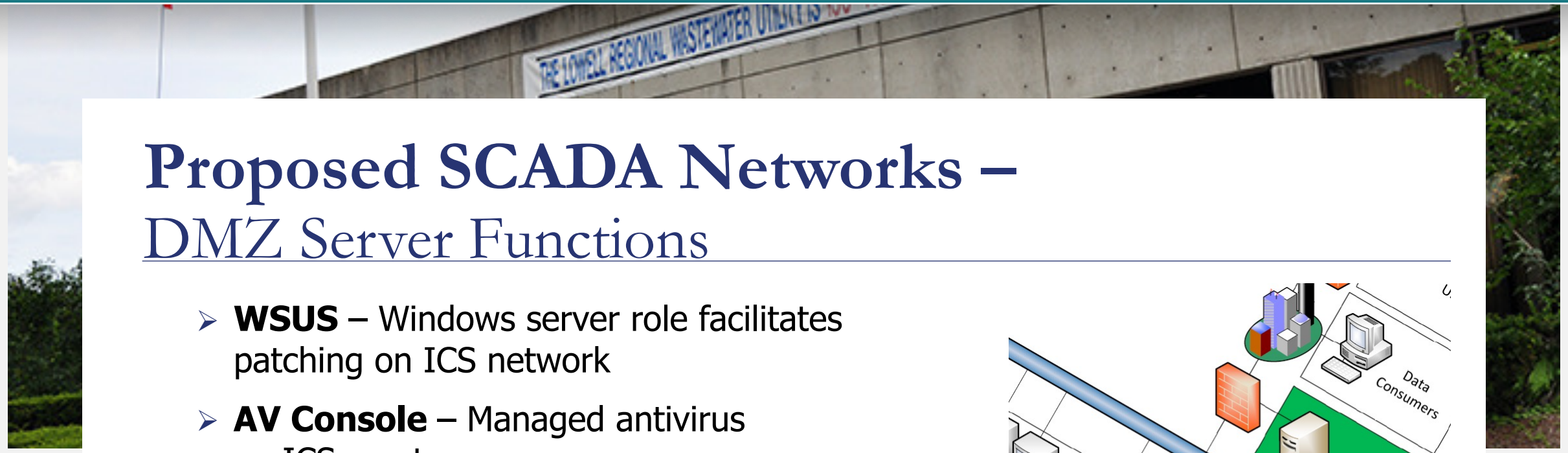
LOWELL WATER
Community-Health-Environment

Proposed SCADA Networks - DMZ

- Robust firewall (Cisco ASA) protects SCADA network, including intrusion prevention and anti-malware capabilities
- Server(s) in DMZ can make SCADA data available elsewhere
  - Provide data to CMMS or other systems
  - External systems do not communicate directly with PLCs
  - Aggregate logs
- Server(s) in DMZ can bring in external data without exposing control to untrusted networks
  - Facilitate patching
  - Bring files into network

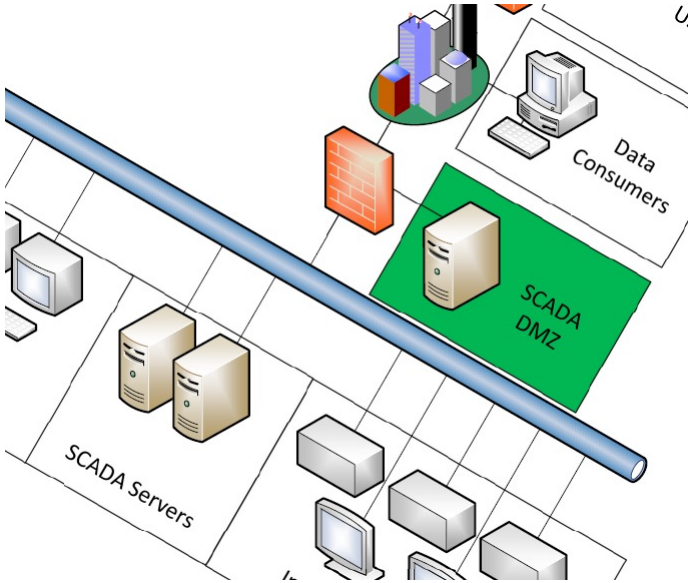


LOWELL WATER
Community-Health-Environment



Proposed SCADA Networks –
DMZ Server Functions

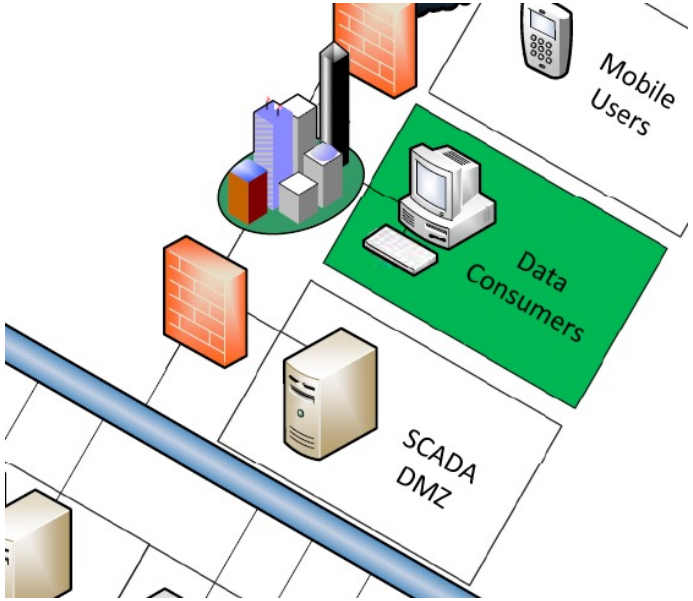
- **WSUS** – Windows server role facilitates patching on ICS network
- **AV Console** – Managed antivirus on ICS assets
- **SIEM** (Security Information & Events Manager) – Log aggregation and analysis
- **Jump Host** – Choke point for remote connections to ICS network
- **File Transfer** – Manage files in/out of ICS network
- **Data Connector** – Connection for future CMMS or other systems



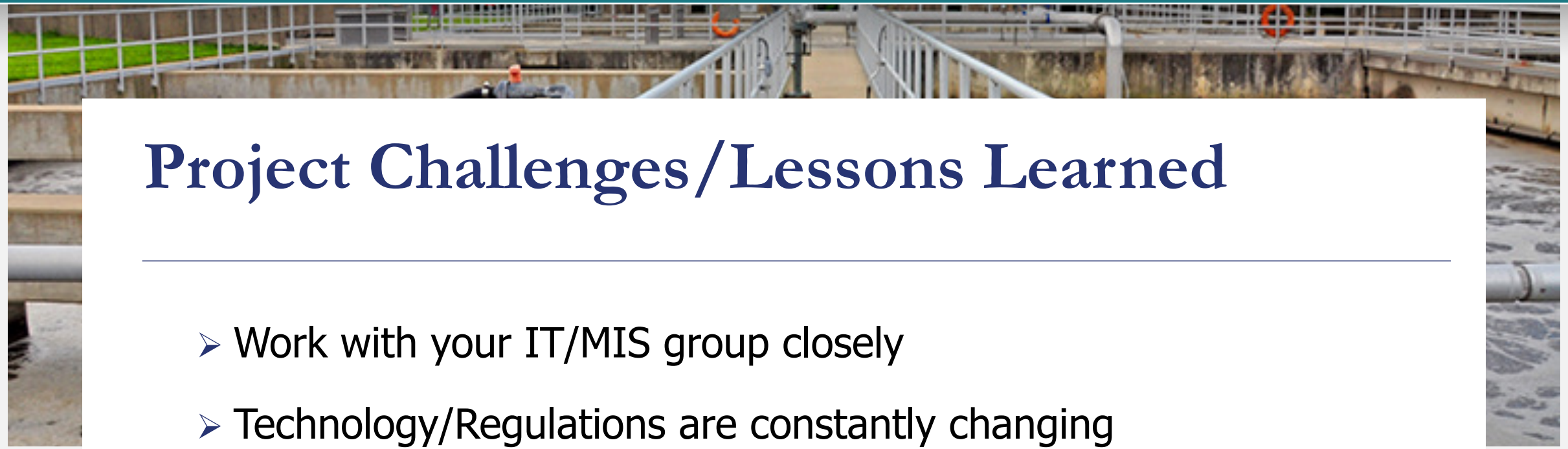
LOWELL WATER
Community-Health-Environment

Proposed SCADA Networks –
City Network Access

- Users/devices/software in the City's network can access data from the SCADA system
- SCADA assets are not directly exposed to external networks
- Users in common location may access data from multiple facilities



LOWELL WATER
Community-Health-Environment



Project Challenges/Lessons Learned

- Work with your IT/MIS group closely
- Technology/Regulations are constantly changing
- Buy in from Staff changing their day to day workflow
- Technology is not cheap…find the solution that meets your goals without breaking the bank
- Identify other needs that can be done in parallel

LOWELL WATER
Community-Health-Environment

Summary and Conclusions

- Upgrade SCADA computer networks at both utilities
- Develop architecture to support an integrated water utility
- Utilize industry standard equipment and protocols to provide secure remote access to SCADA assets
- Provide means to better integrate current City software and applications with real-time SCADA data
- Capitalize on strong in-house technical capabilities and trusted SCADA/cyber security consultant
- Realize quantifiable cost savings and operational efficiencies

LOWELL WATER
Community-Health-Environment

Questions / Discussion

LOWELL WATER
Community-Health-Environment