Wunderlich-Malec

www.wmeng.com/solutions/
it-ot-convergence

The Importance of Defensible Architecture in Water / Wastewater Cybersecurity

December 4, 2025

Mark Riehm
Wunderlich-Malec

Industrial Foundation Networks

Wunderlich-Malec

www.wmeng.com/solutions/
it-ot-convergence/

Wunderlich-Malic is one of the largest and well-established Engineering, System Integration, and Process Automation providers in North America.

- **35+ Facilities Nationwide**
- **40+ Years of Experience**
- **450% Growth in 5 Years**
- **600+ Employees**
- **10K+ Completed Projects**

Industrial Foundation Networks

Wunderlich-Malec

www.wmeng.com/solutions/
it-ot-convergence

WM's IFN team is dedicated to Industrial Foundation Networks.

We design, build, and operate defensible infrastructure for water/wastewater customers that is **fully functional**, **highly available**, and **cyber-secure**.

Industrial Foundation Networks

Wunderlich-Malec

www.wmeng.com/solutions/
it-ot-convergence

Water Under Attack!

- **Water and Wastewater utilities are under increasing attack** from criminal, nation-state and hacktivist threat actors seeking to disrupt operations, compromise health and safety, and extort money.
- **Many water systems rely on outdated Operational Technology (OT)** that was never designed to withstand modern cyber threats.
- **Defensible architecture is especially critical in water and wastewater cybersecurity** to secure infrastructure that directly affect public health, environmental safety, and community trust.

Wunderlich-Malec

www.wmeng.com/solutions/
it-ot-convergence

This Presentation Is:

- **A Technical Introduction** to Defensible Architecture for Water/Wastewater cybersecurity.
- **A Roadmap** to help you establish a cybersecurity baseline and meet EPA compliance.
- **A Link to Critical Resources** to help you secure your OT infrastructure.

Wunderlich-Malec

www.wmeng.com/solutions/
it-ot-convergence

Key Resources

- **#1: EPA "Water Cybersecurity Assessment Tool" (WCAT) – Water/Wastewater Cybersecurity Guidance**

  Primary water sector cybersecurity guidance aligned to CISA and NIST CSF, organized by "Identify, Protect, Detect, Respond, Recover".

  - WCAT Assessment Workbook

  https://www.epa.gov/system/files/documents/2024-12/epa-water-cybersecurity-assessment-tool-3.1_links.xlsx

  - WCAT Fact Sheets with drilldown guidance

  https://www.epa.gov/waterresilience/wcat-fact-sheets

- **#2 NIST Cybersecurity Framework 2.0 and SP 800-82r3 "Guide to Operational Technology (OT) Security" – OT Foundational Cybersecurity Guidance**

  Provides guidance on improving Operational Technology (OT) systems security while meeting unique OT performance, reliability, and safety requirements.

  https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf

- **Cybersecurity Funding**

  Learn about funding options available to support increasing cyber resilience.

  https://www.epa.gov/waterresilience/cybersecurity-funding

Wunderlich-Malec

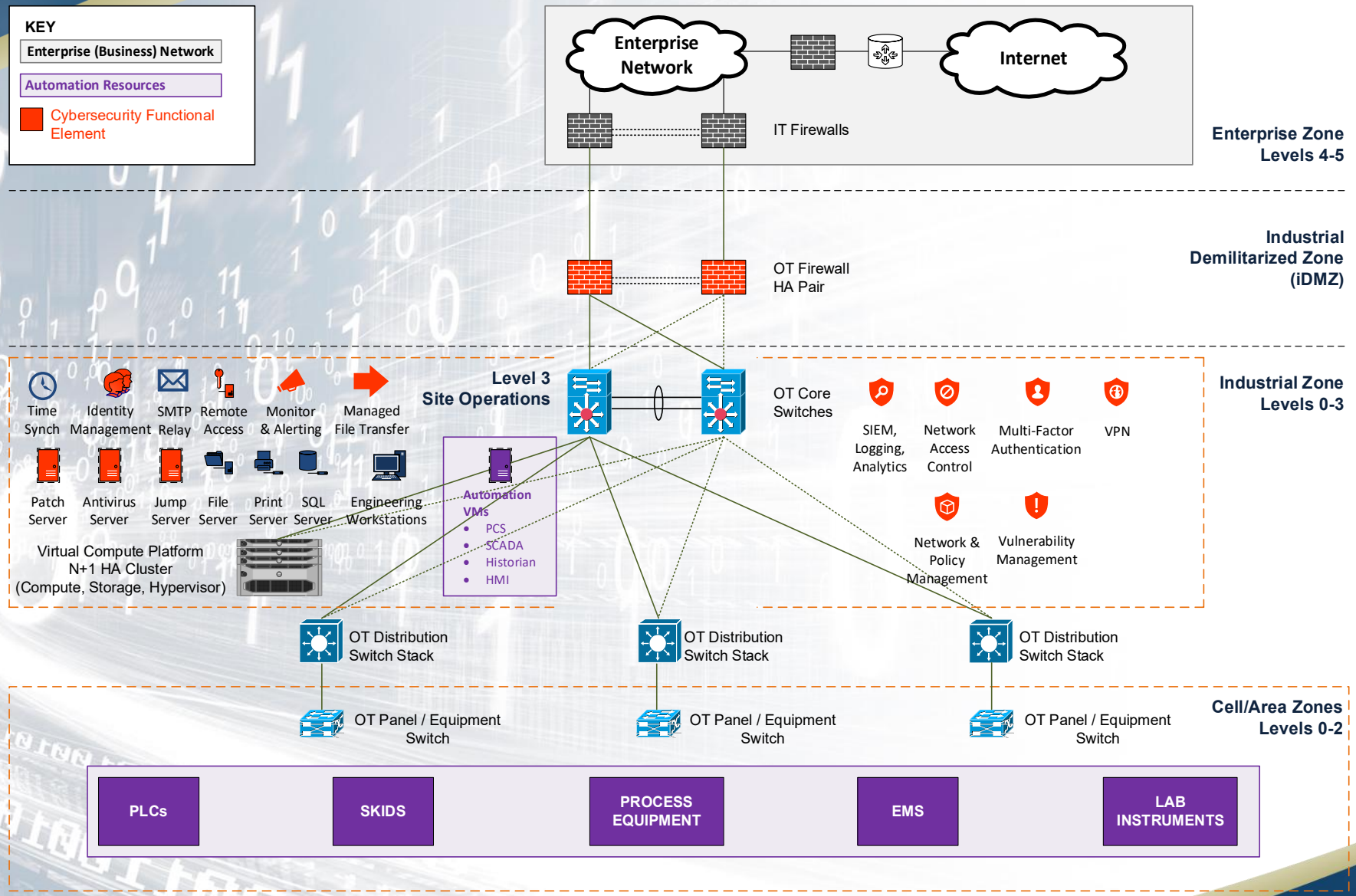
www.wmeng.com/solutions/
it-ot-convergence

Defensible Architecture Requires Multiple Elements

- Asset Management
- Network Segmentation & Management
- Identity and Access Management
- Backup
- Vulnerability Management
- Malware Protection
- Monitoring & Alerting
- Secure Remote Access
- Server Protection
- Computer Protection

Wunderlich-Malec

Defensible Architecture Elements



Industrial Foundation Networks

Wunderlich-Malec

www.wmeng.com/solutions/
it-ot-convergence

Asset Management

- **Maintain an updated inventory** of all IT assets, and OT assets (PLCs, HMIs, SCADA, etc.).

Wunderlich-Malec

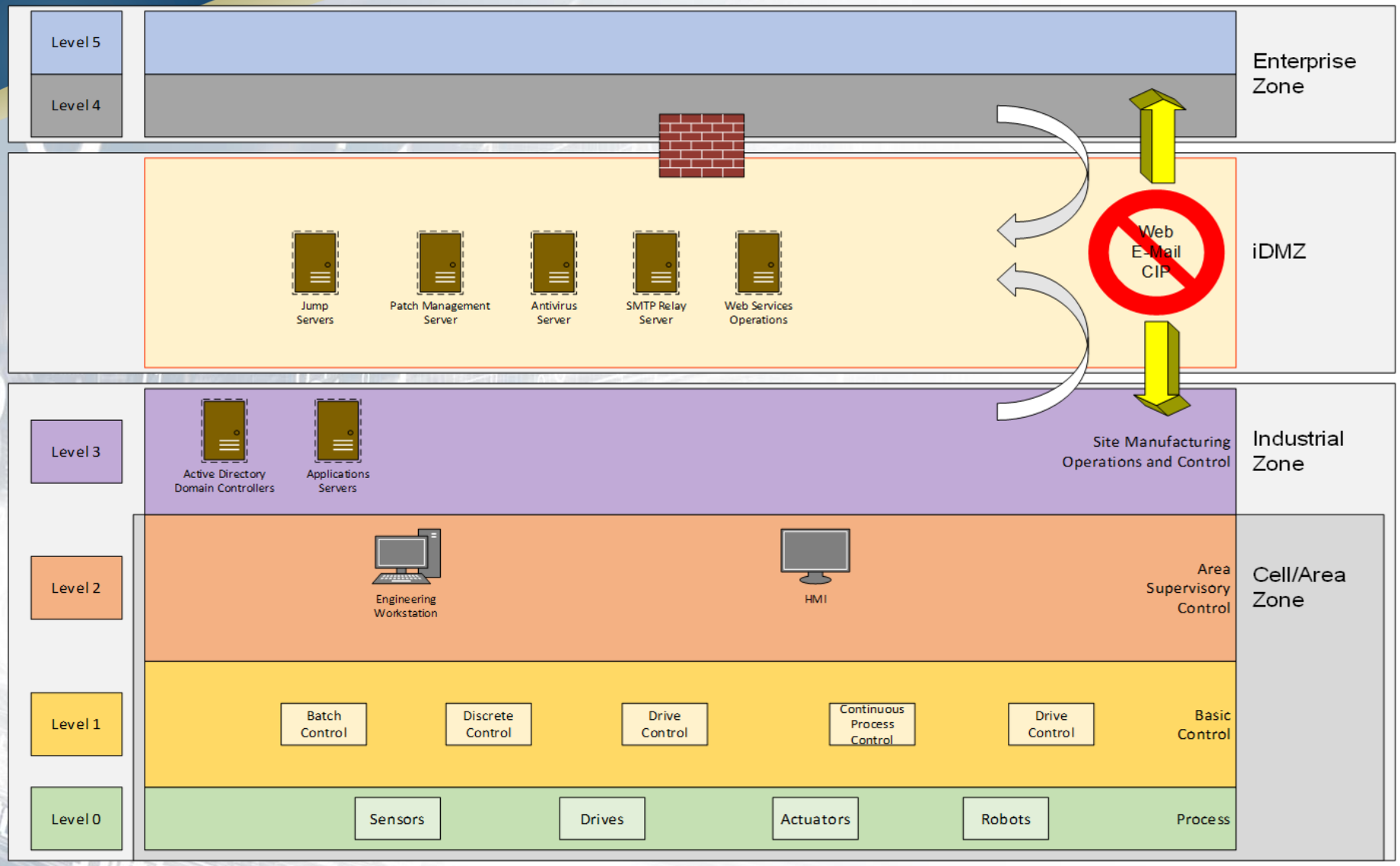
www.wmeng.com/solutions/
it-ot-convergence

Network

- **Implement an OT HA firewall pair** for network resilience and enable security updates without production downtime.
- **Implement Next Generation Firewalls (NGFWs)** to allow deep packet inspection of ICS protocols, allow micro-segmentation of networks to isolate critical systems, provide real-time monitoring and logging, and integrate threat intelligence.
- **Segment the WWS network** to separate OT from IT and the Internet per the Purdue Model by creating an Industrial Zone for all OT assets, separated from the IT network by an Industrial DMZ (iDMZ).
- Move all **endpoints requiring Internet access** to the **iDMZ.**
- **Implement VLANs and firewall rules** to deny all connections to the OT network from the IT network by default, unless explicitly allowed (by IP address and port) for specific system functionality.
- **Isolate vulnerable unsecured legacy components** by VLAN as a compensating control.

Wunderlich-Malec

OT's Purdue Model (PERA)



Industrial Foundation Networks

Wunderlich-Malec

www.wmeng.com/solutions/
it-ot-convergence

Identity and Access Management

- **Use AD-integrated accounts** wherever possible.
- **Maintain separate IT and OT AD domains** where feasible.
- Require users to have **separate usernames and passwords for IT and OT network access**, to reduce the risk of attackers moving between both networks using a single login.
- Separate logins for each user – **no shared account use**.
- **Implement Least Privilege**. Restrict each user, system or task to the minimal level of access required to perform its tasks.
- **Implement Role-based Access Controls (RBAC).** Restrict system access based on the roles assigned to users.
- **Separate user and privileged** (e.g., System Administrator) **accounts**.
- **Change passwords** for all hardware built-in accounts.
- **Require a minimum length** for passwords.
- **Immediately disable access** to an account or network when access is no longer required due to retirement, change of role, termination, or other factors.
- **Detect and block** repeated unsuccessful login attempts.

Wunderlich-Malec

www.wmeng.com/solutions/
it-ot-convergence

Backup

- **Regularly backup OT/IT systems** so you can recover to a known and safe state in the event of a compromise. Test backup procedures and isolate backups from network connections.
- **Implement the NIST 3-2-1 rule**:
  3) Keep three copies: one primary and two backups;
  2) Keep the backups on two different media types; and
  1) Store one copy offsite.

Wunderlich-Malec

www.wmeng.com/solutions/
it-ot-convergence

Vulnerability Management

- **Keep a list of threats** and attacker tactics, techniques, and procedures (TTPs) for cyberattacks relevant to the WWS.
- **Patch or otherwise mitigate known vulnerabilities** within the recommended timeframe, including firmware, OS and applications.
- **Implement compensating controls** to mitigate risks until patching can be performed.

Wunderlich-Malec

www.wmeng.com/solutions/
it-ot-convergence

Malware Protection

- **Deploy antivirus/Endpoint Detection and Response (EDR)** solutions that are certified for industrial systems.
- **Ensure the solution supports** offline updates and low system resource usage.
- **Avoid solutions that may interfere** with real-time operations or deterministic behavior.

Wunderlich-Malec

www.wmeng.com/solutions/
it-ot-convergence

Monitoring and Alerting

- **Maintain an up-to-date list of all OT assets** (PLCs, HMIs, SCADA, etc.).
- **Know how devices communicate** and what protocols are used (e.g., Modbus, OPC, etc.).
- **Deploy passive network monitoring tools** that do not interfere with real-time operations. Tools like Dragos, Claroty, or Nozomi Networks are designed for OT environments.
- **Avoid active scanning** unless explicitly tested and approved.

Wunderlich-Malec

www.wmeng.com/solutions/
it-ot-convergence

Secure Remote Access

- **Implement a bastion host / jump server** located in the iDMZ that acts as a gateway to the Industrial Zone.
- **Secure access to the gateway** with MFA, RBAC & least privilege.
- **Implement secure credential management** that obscures privileged accounts and passwords without exposing them to end users.
- **Implement monitoring, logging and auditing** of sessions and access.

Wunderlich-Malec

www.wmeng.com/solutions/
it-ot-convergence

Server Protection

- **Restrict physical access** to OT server locations to authorized personnel.
- **Remove unnecessary services and software** and disable unused ports and protocols to reduce attack surface.
- **Enforce RBAC** to assign access based on job function and least privilege.
- **Disable default accounts** or change default credentials.
- **Disable Microsoft Office macros**, or similar embedded code, by default on all assets.

Wunderlich-Malec

www.wmeng.com/solutions/
it-ot-convergence

Client Computer Protection

- **Remove unnecessary software** and services
- **Disable unused ports** and interfaces.
- **Disable Microsoft Office macros**, or similar embedded code.
- **Enforce least privilege**. Only allow access to what's necessary for the role.
- **Auto-lock screens** after inactivity.
- **Disable local accounts** or rename default ones (e.g., Administrator).
- **Restrict local admin rights**—users should not have elevated privileges.
- **Install OT-compatible antivirus/EDR solutions** that won't interfere with real-time operations.
- **Restrict Internet access** unless absolutely necessary. Place client computers needing Internet access in the iDMZ.

Wunderlich-Malec

www.wmeng.com/solutions/
it-ot-convergence

Recommendations

- **Establish Governance.**
  - Appoint internal cybersecurity responsibility and create a security program including policies, procedures, and compliance per WCAT guidance.
- **Assess and Remediate Infrastructure.**
  - **Complete WCAT assessment workbook.**
  - **Do an infrastructure gap assessment** using WCAT and industry best practices.
  - **Create a remediation plan** and **3-year budget.**
  - **Learn** about **financial aid** options and **apply for assistance.**
  - **Identify skillsets** required for success.

Wunderlich-Malec

www.wmeng.com/solutions/
it-ot-convergence

Recommendations

- **Consider OT Managed Services.**
  - **Engage an OT Managed Services Provider (MSP)** to jumpstart your water cybersecurity program through **education**, **assessment**, **infrastructure remediation**, and **OT operations**. Plan on a one-year initial engagement, then determine if it makes sense to bring the functions in-house or continue outsourcing.
- **Participate in Dragos Community Defense Program (CDP).**
  - The CDP provides US and Canada-based water, electric, and natural gas providers with less than $100M US in annual revenue **free access to Dragos Platform** software. These tools can help improve security postures and reduce OT risk.

https://www.dragos.com/community/community-defense-program

Get This Presentation!

- www.wmeng.com/solutions/it-ot-convergence
- IFN@wmeng.com