

TECH & AI CASE STUDY - WATER UTILITY - 2026

OT Security That Segmented a Water Utility's Treatment Network

Based on a delivery engagement with Tallgrass Water Authority

60% to 100%

OT ASSET INVENTORY ACCURACY

-90%

CROSS-ZONE NETWORK PATHS

100%

VENDOR SESSIONS RECORDED

0 to 2 per year

MANUAL-FALLBACK DRILLS

A fillable practice edition: the full story, 8 actions,
6 reflections and a 90-day plan - work it with your team.

Free - no email required
emersontechnology.com

MAKE THIS PRACTICE BOOK YOURS

Work it, do not just read it

This practice book turns the Tallgrass Water Authority case study into a working session for your team. Read the full story first - what happened, what was built and what it changed. Then tick the 8 actions you can commit to, write short answers to the 6 reflections, and finish with a 90-day plan. Every field in this PDF is fillable: open it in Adobe Acrobat Reader, Chrome, Edge or macOS Preview, type directly into the boxes and save.

YOUR NAME	ROLE
COMPANY	TEAM / DEPARTMENT
DATE	EMAIL (OPTIONAL)

MY GOAL FOR THIS PRACTICE SESSION

- 01 The story** - What happened at Tallgrass Water Authority - before, during and after the project.
- 02 The results** - The numbers that changed, plus industry benchmarks from public research.
- 03 The 8-action checklist** - Tick boxes as your organization completes each step. Owner and date fields included.
- 04 The 6 reflections** - Fillable questions that pressure-test your own roadmap.
- 05 My 90-day plan** - Three fillable phase cards that turn this case study into your roadmap.

RUN IT AS A 90-MINUTE TEAM SESSION

25 min READ Read the story together. Ask everyone to note the one number that surprised them most.	40 min PRACTICE Work the 8-action checklist and the 6 reflections. Assign an owner and a date to every action you commit to.	25 min COMMIT Fill in the 90-day plan. One goal per phase, one number that tells you it worked. Book a review date before you leave the room.
--	--	---

THE STORY

What happened, and why it worked

01 The Company

Tallgrass Water Authority is a regional water utility operating three treatment plants and 41 remote pump and lift stations, serving a dispersed population across several counties. Its mandate is unglamorous and absolute: keep water moving and keep it safe. The authority's operational technology — SCADA supervisory systems, programmable logic controllers, remote terminal units, chlorination dosing equipment and the radio links that reach 41 remote sites — is maintained by plant staff and a two-person IT team for whom operational technology was always a side duty stacked on top of corporate systems.

The authority is small in headcount and large in consequence. A disruption to chlorination or pumping is not a data problem or a downtime metric; it is a public-health event, with boil-water notices, regulatory consequences and community trust at stake. That asymmetry shaped every decision in the security program that followed: the bar for "safe to change" was extremely high, and the utility's leadership was unwilling to accept any improvement plan that introduced operational risk of its own. Federal warnings about intrusions at US water utilities had already made the board uneasy — the question was never whether to act, but how to act without becoming the story.

02 Where Things Stood

The network that connected corporate offices to plant floors was a product of decades of incremental fixes. Corporate IT and plant-floor SCADA shared switches, spare ports and a handful of always-on vendor modems installed by equipment suppliers years earlier. No one could say which engineer laptops could reach programmable logic controllers, because the answer changed whenever a contractor visited a site. The asset inventory was roughly 40% wrong: a 1990s-era RTU still performing a real function and an undocumented cellular gateway both surfaced during early discovery, neither of which appeared in any record the authority maintained. Remote access was the most acute exposure. Vendors who serviced dosing systems, pumps and telemetry equipment expected always-on connectivity, and the always-on modems delivered it — unmonitored, unrecorded and reachable from wherever the vendor happened to be. CISA advisories on intrusions at US water utilities cite exposed remote-access software and default credentials as recurring entry points, and Tallgrass's environment contained textbook versions of both patterns. Meanwhile, the industrial ransomware trend was impossible to ignore: Dragos's year-in-review logged a record 1,013 ransomware incidents against industrial organizations in 2023, an 87% year-over-year increase, and water utilities featured in the sector breakdown.

The organizational gap compounded the technical one. Accountability for plant technology risk sat implicitly between the two-person IT team and plant operations, each assuming the other was watching, and no single leader owned the converged environment. The board wanted assurance; the state's drinking-water security review was approaching; and the utility's own staff knew that a network audit conducted clumsily could interrupt treatment as effectively as an attacker could.

03 The Challenge

The challenge was to secure a live water treatment network — segmented, monitored, with vendor access controlled — without interrupting treatment operations even once. Every conventional security project step carries operational risk in an industrial environment: running scans can crash legacy controllers, reconfiguring switches can drop telemetry, and cutting vendor access can strand maintenance during a failure. NIST's guide to industrial control system security, SP 800-82, recommends segmenting OT networks and designing for safe degradation — operations first, prevention second — and that principle had to govern not just the design but the sequence in which every change was made.

The second challenge was knowledge itself. You cannot segment a network you do not understand, and the authority's documentation was 40% wrong in ways that mattered: the undocumented cellular gateway and the legacy RTU were exactly the kinds of assets that make zone boundaries fictitious. Any program that began by changing configurations would have baked those errors into the new architecture. The inventory had to be rebuilt from observed reality before the first firewall rule was written, and it had to be done passively — watching traffic rather than probing devices — because probing is how industrial assessment projects become operational incidents.

Finally, the program had to fit the authority's real capacity. A two-person IT team could not operate a security operations center, and plant operators could not be asked to become network engineers. Every control selected had to be operable by the people Tallgrass actually employs, and every procedure had to survive being executed at 2 a.m. by someone paged out of bed.

04 Discovery and Diagnosis

Emerson Technology began with 60 days of passive monitoring of OT traffic across all three plants, building a ground-truth asset inventory from observed communication patterns without touching a single control system. The passive window paid for itself immediately: it corrected the 40% inventory error, mapped every conversation between controllers, supervisors, historian servers and engineering workstations, and catalogued every remote-access path — including the always-on vendor modems and the undocumented cellular gateway — with the evidence of what each one actually connected to.

The traffic baseline doubled as a behavioral reference. Modbus and DNP3 command patterns were profiled plant by plant, establishing what normal looks like for dosing setpoints, pump starts and telemetry polls, which is the foundation any protocol-aware alerting needs before it can distinguish an anomaly from a Tuesday. Interviews with plant operators and the two-person IT team mapped maintenance rhythms, vendor visit patterns and the informal knowledge that keeps remote stations running. The diagnosis ended with a jointly agreed target architecture: Purdue-model zones separating enterprise, DMZ, supervisory and control levels, a brokered pattern for vendor access, protocol-aware monitoring, and — because no technical control is sufficient on its own — documented manual fallback procedures that operators could run if systems ever degraded. Operations signed off on the plan only after every change was annotated with its rollback path.

05 The Solution

The implementation followed the passive-to-active arc the diagnosis established, changing the network only after the network was understood.

A ground-truth inventory, built passively

The 60-day passive window produced an OT asset inventory that was 100% accurate by construction, because it was built from what the network actually did rather than what records claimed. Every asset received an owner, a criticality rating and a place in the target zone model, and the two surprises — the legacy RTU and the cellular

gateway — were brought under management before segmentation began. The inventory was not a one-time artifact: the monitoring platform keeps it current as traffic patterns shift, so the accuracy persists instead of decaying the way spreadsheet inventories do.

Purdue-model segmentation without downtime

The network was re-layered into enterprise, DMZ, supervisory and control zones with enforced firewall boundaries, collapsing 90% of east-west network paths. Cutover was sequenced plant by plant during scheduled maintenance windows agreed with operations, with each firewall policy staged in monitor-only mode before enforcement so operators could review exactly what would change. A unidirectional flow replicates historian data to the IT side for reporting, giving corporate users the visibility they need without creating a path back into the control network. Zone boundaries now contain a corporate-side compromise before it can ever reach field controllers — which is the entire point of the exercise.

Brokered vendor access and protocol-aware eyes

Every vendor remote session now enters through a brokered jump host with per-session credentials, MFA and full session recording, and every always-on modem was retired. Vendors keep their access; the authority keeps the evidence. Protocol-aware monitoring baselines Modbus and DNP3 traffic and alerts on anomalous commands — an unexpected write to a controller being the alert that matters — with playbooks written jointly with operations so that a 2 a.m. page has an owner, a decision tree and a phone number. Finally, the program documented manual fallback procedures with operators rather than for them: how dosing runs by hand, how pump dispatch works by phone, what each plant can do for a full shift without network connectivity. A fallback no operator has rehearsed is a wish, not a plan, so the drills are part of the design.

06

The First 90 Days

The first month belonged entirely to passive monitoring and inventory, with weekly working sessions between Emerson Technology analysts, the IT team and plant leads to review observed assets and traffic. The second month built the zone model in staging: firewall policies for the supervisory and control boundaries were drafted, simulated against the recorded traffic baseline, and walked through with operations until every allow rule had a stated business reason. The brokered jump host was deployed and piloted with two friendly vendors, whose feedback shaped the session workflow so compliance would not become a reason maintenance slipped.

The third month executed the first production cutovers during scheduled maintenance windows, sequenced from the least critical plant to the most, with monitor-only operation for a week before each enforcement.

Protocol-aware monitoring went live in alert-tuning mode, and within six weeks of deployment it produced its first actionable alert — an anomalous command pattern during a vendor session — which was triaged using the playbook operations had already rehearsed. The manual-fallback documentation was completed with operators and the first drill was scheduled. By day 90, cross-zone paths had fallen 90%, vendor sessions were fully brokered and recorded, and the authority's board received a report written in operational language rather than security jargon. Treatment operations ran normally through every week of the program, which was the metric plant managers cared about most.

07 The Results

The authority now operates from a 100%-accurate OT asset inventory, every vendor session is brokered and recorded, and cross-zone network paths fell 90%. Protocol-aware monitoring has moved from tuning to trusted — its first actionable alert arrived within six weeks of deployment and was handled exactly as the joint playbook prescribed. The state drinking-water security review passed with the segmentation design cited as a model, and manual-fallback drills are on the standing calendar twice a year. Treatment operations ran normally throughout the entire program.

METRIC	BEFORE	AFTER
OT asset inventory accuracy	60%	100%
Cross-zone network paths	-	-90%
Vendor sessions recorded	-	100%
Manual-fallback drills	0	2 per year

The organizational result may outlast the technical one. A single leader is now accountable for both corporate and plant technology risk, ending the arrangement in which two teams each assumed the other was watching. Vendor relationships improved rather than soured, because brokers with per-session credentials are easier for contractors to use than hunting for a modem that may or may not be powered. The board reviews a quarterly risk summary grounded in observed network behavior, and the utility's operators — the people who would actually run a plant through a degradation event — have rehearsed the procedures that would carry them through one.

08 What Your Business Should Do

The Tallgrass pattern applies to any organization where operational technology meets corporate IT, and its first lesson is about sequence, not tools. Start with passive OT monitoring — watch network traffic for at least 60 days before changing anything, because a ground-truth inventory built from observed traffic beats any spreadsheet you inherited. Layer the network to Purdue zones, separating enterprise, DMZ, supervisory and control levels with enforced firewall boundaries, since zone boundaries contain a corporate-side compromise before it can ever reach field controllers. Broker every vendor remote session through a jump host with per-session credentials, MFA and full recording: vendors keep their access, you keep the evidence, and the always-on modem — CISA's most-cited water sector entry point — disappears from your attack surface.

Deploy monitoring that understands your plant's protocols, whether Modbus, DNP3 or something older, and alert on unexpected commands — an anomalous write to a controller is the alert that matters. Write fallback procedures with operators, not about them: document how plants run on manual control, from hand dosing to phone dispatch, and remember that a fallback no operator has rehearsed is a wish, not a plan. Drill degradation twice a year, practicing manual operations alongside technical restore tests, so each drill validates the procedures, the communications tree and the muscle memory of the people who will need all three. Give IT and OT one accountable owner, because converged environments fail quietly where two teams each assume the other is watching. And plan maintenance around water quality — schedule segmentation cutover, patching and monitoring changes with operations so compliance obligations never compete with security work, because in this sector operations constraints shape the design, not the other way around. Apply these eight steps at your own pace with the action checklist in this practice book, and let the reflection questions guide each review cycle: how accurate is your asset inventory, which vendor modems could you not explain on a diagram, and what would a two-hour disruption to dosing or pumping actually cost in public-health and trust terms?

REAL-WORLD PROOF & BENCHMARKS

Dragos's industrial cybersecurity year-in-review reportedly logged a record 1,013 ransomware incidents against industrial organizations in 2023, an 87% year-over-year increase. - Dragos Year in Review

CISA advisories on intrusions at US water utilities reportedly cite exposed remote-access software and default credentials as recurring entry points. - CISA advisories, 2024

NIST's guide to industrial control system security, SP 800-82, recommends segmenting OT networks and designing for safe degradation — operations first, prevention second. - NIST SP 800-82

THE PRACTICE PAGES

The 8-action checklist

Work through the list with your team. Tick each box as your organization completes the step, and fill in an owner and a target date so every action has a name and a deadline.

☐**1. Start with passive OT monitoring**

Watch OT network traffic passively for at least 60 days before changing anything. A ground-truth asset inventory built from observed traffic beats any spreadsheet you inherited.

OWNER

TARGET DATE

STATUS

--	--	--

☐**2. Layer the network to Purdue zones**

Separate enterprise, DMZ, supervisory and control levels with enforced firewall boundaries between each. Zone boundaries contain a corporate-side compromise before it can ever reach field controllers.

OWNER

TARGET DATE

STATUS

--	--	--

☐**3. Broker every vendor remote session**

Replace always-on modems and shared vendor accounts with a brokered jump host offering per-session credentials, MFA and full recording. Vendors keep their access; you keep the evidence.

OWNER

TARGET DATE

STATUS

--	--	--

☐**4. Baseline OT protocols for anomalies**

Deploy monitoring that understands Modbus, DNP3 or your plant's protocols and alerts on unexpected commands. Anomalous writes to a controller are the alert that matters.

OWNER

TARGET DATE

STATUS

--	--	--

☐**5. Write fallback procedures with operators**

Document how plants run on manual control — hand dosing, phone dispatch — with operators, not consultants. A fallback no operator has rehearsed is a wish, not a plan.

OWNER

TARGET DATE

STATUS

--	--	--

☐

6. Drill degradation twice a year

Practice running treatment on manual procedures alongside technical restore tests twice a year. Each drill validates the procedures, the communications tree and the muscle memory of operators.

OWNER

TARGET DATE

STATUS

--	--	--

☐

7. Give IT and OT one accountable owner

Name a single leader accountable for both corporate and plant technology risk. Converged environments fail quietly where two teams each assume the other one is watching.

OWNER

TARGET DATE

STATUS

--	--	--

☐

8. Plan maintenance around water quality

Schedule segmentation cutover, patching and monitoring changes with operations so compliance obligations never compete with security work. In water utilities, operations constraints shape the design, not vice versa.

OWNER

TARGET DATE

STATUS

--	--	--

AFTER THE CHECKLIST: OUR TOP 3 PRIORITIES

From the eight actions above, write down the three you will start first - and the single number you expect each one to move. Three priorities with owners beat eight without any.

PRIORITY 1 NUMBER IT SHOULD MOVE	PRIORITY 2 NUMBER IT SHOULD MOVE	PRIORITY 3 NUMBER IT SHOULD MOVE
--	--	--

THE PRACTICE PAGES

Reflections for your team

Use these questions in your next planning session and type short answers into the boxes. The gaps you find are usually the fastest wins.

Q1. How accurate is your OT asset inventory today, and when did anyone verify it against real traffic?

Q2. Which vendor modems or remote-access paths into your control network could you not explain on a diagram?

Q3. If a controller received an unexpected write command at 2 a.m., who would see the alert — and what would they do?

Q4. Could your plants run on manual procedures for a full shift, and when did operators last practice it?

Q5. Where does accountability for plant technology risk sit in your organization — one named leader, or between two teams?

Q6. What would a two-hour disruption to dosing or pumping actually cost in public-health and trust terms?

THE PRACTICE PAGES

My 90-day plan

Finish the session by committing to a plan. Three phases, one goal each, one number that tells you it worked. Bring this page to your next leadership review - or to a free consultation with Emerson Technology, and we will pressure-test it with you.

Days 1-30 Focus: audit and alignment

PRIMARY GOAL**KEY ACTIONS****HOW WE MEASURE SUCCESS****OWNER**

Days 31-60 Focus: build and prove

PRIMARY GOAL**KEY ACTIONS****HOW WE MEASURE SUCCESS****OWNER**

Days 61-90 Focus: scale and measure

PRIMARY GOAL

KEY ACTIONS

HOW WE MEASURE SUCCESS

OWNER

Tip: save a copy per team so each group keeps its own answers. Revisit the reflections every quarter - the questions stay the same even as the numbers move.

BOOK THE REVIEW BEFORE YOU CLOSE THE BOOK

Plans without a review date drift. Before you close this practice book, agree on when you will come back to these pages, who will run that session, and when you will check the numbers again. If you want an outside pair of eyes, bring this page to a free consultation with Emerson Technology and we will pressure-test the plan with you.

REVIEW DATE	REVIEWED BY	NEXT CHECK-IN
------------------------------------	------------------------------------	--------------------------------------

Ready for a transformation like Tallgrass Water Authority's?

Emerson Technology designs and builds the data, AI, cloud and automation systems behind results like these. On a free consultation call we will map this exact playbook to your business - your data, your constraints, your numbers.

Book a free consultation

support@emersontechnology.com

or start online: emersontechnology.com/contact