OT Cyber-Resilience for the AI-Attack Era

An affordable assessment and procedure fixes for water and industrial operators

ROI, LLC · vendor-neutral OT reliability & cyber-resilience advisory · roi.llc

In August 2026, more than 100 companies, including OpenAI, Anthropic, Microsoft and Google, warned that AI will make cyberattacks far more widespread and named water and critical infrastructure as targets. AI does not invent new doors. It makes the open ones, exposed PLCs, weak passwords, flat networks, cheaper and faster to exploit at scale. The same basic gaps let attackers take over 30-plus Minnesota water systems this summer. You do not need frontier AI to be exposed, or to fix it.

What the assessment checks

1. Exposure & remote access

Find internet-facing PLCs and SCADA and any insecure remote access, the exact attack vector.

2. Credentials & access control

Default, weak, or shared passwords, and exactly who can reach your controllers.

3. IT / OT segmentation

Whether your control network is truly separated from the office network and the internet.

4. Backups & recovery

Config and program backups, tested restore steps, and manual-operation runbooks.

5. Operator detection & alarms

Whether operators will notice a loss of control and can run the plant by hand.

6. Obsolescence & patch status

Aging PLCs, firmware levels, and open vendor advisories that need attention.

What you walk away with

- **A prioritized findings report** red / amber / green, so you know what is exposed and what to fix first.
- **A fix-it-this-week quick-wins list** mostly free configuration and procedure changes your staff can make now.
- **Ready-to-use procedures & policy templates** remote access, credentials, backup, incident response, manual operation.
- **Alignment to CISA, EPA / AWIA, AWWA and IEC 62443** so the work is audit-, grant- and board-ready.
- **A funding-ready action plan** one page you can take straight to your board or into a grant application.

It is fixes, not a fortune.

Most of what stops the next attack costs little: take PLCs off the public internet, put remote access behind a VPN, change default passwords, segment the network, and back up your configs. We find the gaps and hand you the plan. You do not need a million-dollar platform to close the doors the attackers used.

Why ROI: an independent, vendor-neutral controls engineer with more than 25 years in DCS, PLC and SCADA who fixes the fundamentals affordably and complements, not replaces, your security specialists. You will not be oversold.

OT cyber-resilience assessment

Free OT-exposure snapshot · water utilities and industrial plants · grant eligible

Scan for a free audit