Municipal Water OT Cyber-Resilience

An independent assessment and procedure fixes, not a six-figure security overhaul

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

In July 2026, a coordinated attack reached internet-exposed PLCs at 30-plus water systems across Minnesota and seven states, changing passwords, locking out operators, and forcing manual operation. The gaps they walked through were basic OT hygiene, not exotic hacks. You do not need an expensive cybersecurity program. You need to close those doors, and most of the fixes are configuration and procedure changes at little or no cost.

What the $25,000 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 AA26-097A, EPA / AWIA and AWWA guidance** so the work is audit- and grant-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.

$25,000 fixed-fee assessment

scott@roi.llc · roi.llc

Start with a free OT-exposure snapshot · grant-funding eligible · approvable at the utility-manager level