Keeping utilities running

Protecting electric power, water, natural gas and renewable energy infrastructure.

The stakes

Utilities do not just keep the lights on. They keep hospitals running on backup power, water safe to drink, gas flowing to homes in winter and emergency services able to respond. When a utility fails, it does not fail alone. It takes other sectors with it.

State-linked groups have demonstrated that the objective is disruption, not data theft. Volt Typhoon spent 300 days undetected inside a U.S. electric and water utility, mapping OT operating procedures and grid topology.[1] The FBI and CISA have confirmed the pattern is not isolated: utilities have become a primary target for state-linked actors, ransomware groups and destructive attacks alike.

That disruption is most likely to land at a remote substation, a water pumping station or a rural generation site, where there is no IT professional on-site and the nearest specialist may be hours away. The window to restore power, water pressure or gas flow to a community is measured in minutes, not business days.

The American water works lesson

In 2024, the largest U.S. water utility suffered a cyberattack that did not touch operational systems but forced billing suspension and portal shutdown. IT systems that OT depends on, including Active Directory, historians, GIS, OMS and billing, are equally in scope.[2]

[1] https://www.securityweek.com/chinas-volt-typhoon-hackers-dwelled-in-us-electric-grid-for-300-days

[2] https://www.amwater.com/press-room/press-releases/corporate/american-water-reactivating-systems-after-cyber-event-10102024

The threat landscape

One in five ICS / OT organizations experienced a confirmed cyber incident in the past year. Not alerts. Confirmed incidents affected operational systems, with 40% causing direct operational disruption and nearly one in five taking more than a month to remediate. For utilities, that remediation gap is not a statistic. It means days without reliable power, water or gas supplied to the communities that depend on them.

One in five

ICS / OT organizations experienced a cyber incident in the past year.

SANS State of ICS/OT Security 2025

40%

of those incidents caused operational disruption, affecting production, service delivery or public operations. 37.9% originated from ransomware.

SANS State of ICS/OT Security 2025

19%

of OT incidents took more than a month to recover in 2025. Detection has improved. Restoration remains the critical gap.

SANS State of ICS/OT Security 2025

Small and medium utilities are described as target rich but cyber poor: high-value targets with no dedicated cybersecurity teams and limited resources to recover.

The solution: Recovery that works where your team cannot

Acronis Cyber Protect for OT delivers IT-grade cyber resilience to utility OT environments without disrupting live operations. It is designed around a core operational reality: when an incident happens at a remote substation, pumping station or energy site, the person closest to the system may be an automation engineer or shift supervisor, not a cybersecurity specialist. Recovery workflows are built to work in their hands locally, with minimal dependence on external connectivity or specialist intervention.

Zero-disruption backup

Full-image and file-level backup with no reboots and no downtime. Sector-by-sector mode activates automatically for proprietary OT file systems. VSS-consistent snapshots across multivolume SCADA and historian configurations.

Bare-metal and Universal Restore

Recover to dissimilar or replacement hardware automatically. Universal Restore injects the correct drivers without manual reconfiguration, which is critical when the original industrial PC is obsolete or unavailable.

Air-gapped and offline operation

All components deploy on premises. The management server runs fully offline. Anti-malware definitions update without internet access, and agents continue protection for 30 days if the management server is unreachable.

One-Click Recovery for operators

Authorized local personnel, including substation engineers, water operations managers and shift supervisors can follow a guided recovery workflow to restore a failed system to its last known-good state, helping reduce recovery time from hours or days to minutes, depending on site conditions.

Safe and verified recovery

Backup images are scanned for malware and validated before restoration, helping reduce the risk of reinfecting a recovered SCADA or HMI system. Detected threats are flagged and can be removed as part of the recovery workflow.

Immutable backup storage

Backup archives cannot be deleted, modified or encrypted by ransomware, even if credentials are compromised. Governance and Compliance modes with retention periods of up to 10 years for regulatory mandates.

Legacy systems: Protecting what others have abandoned

Utility OT assets operate for 30 years or more. The computerized systems managing them, including HMIs, SCADA servers and engineering workstations, often run operating systems that mainstream vendors stopped supporting years ago.

Windows 10 in OT: managing lifecycle risk[3]

Many utility OT workstations still run Windows 10 editions with different support timelines. Some are already out of support, while others face lifecycle milestones in 2027, 2029 or later. Upgrading or patching these systems is often not a routine refresh; it can trigger costly revalidation, break licensed SCADA / HMI software or void OEM support contracts. Acronis acts as a compensating control, combining image-based backup with application allowlisting to help operate legacy systems more safely when immediate OS migration is not feasible.

Acronis provides broad support with full backup and recovery support from Windows XP SP1 / SP2 / SP3 through Windows Server 2025, Linux kernel 2.6.9 to 5.19 and all major hypervisors, covering every OT generation.

Recovery and restoration: Not the same thing

In utility environments, confusing these two terms costs service continuity, and in the worst cases, public safety.

Recovery means getting frequency control restored or water pressure resumed from whatever validated state is available, fast. Partial operations keeping a hospital on power are not a failure state. They are the first mission.

Restoration means returning the full certified system stack to a known-good baseline safely, without reintroducing malware or corruption.

Acronis supports both. One-Click Recovery helps deliver rapid operational continuity, enabling authorized personnel to initiate restoration locally without specialist intervention. Validated, forensic-grade backup supports complete, verified restoration, including scanning backup images for malware before use and providing blockchain-notarized, chain-of-custody evidence for post-incident investigation and audit.

According to the SANS State of ICS/OT Security 2025 report, while nearly half of OT incidents are detected within 24 hours, 19% take more than a month to fully restore. Detection has improved. Restoration remains the critical gap.

[3] https://learn.microsoft.com/en-us/windows/release-health/release-information

What Acronis protects across the utility estate

Utility environment	Systems and data Acronis protects
Electric power: generation, transmission and distribution, grid edge	SCADA / EMS servers, substation control PCs, HMI workstations, DER / microgrid controllers, BESS site controllers, historian servers. Data protected includes OS images, SCADA / HMI configs, alarm logic, historian databases and engineering project files.
Water and wastewater	Water treatment SCADA, HMI workstations, pump and lift station control PCs, reservoir monitoring systems. Data protected includes OS images, treatment process configs, pump control logic and regulatory reporting data.
Natural gas distribution	Pipeline monitoring servers, compressor station PCs, regulator station PCs, SCADA servers, custody-transfer systems. Data protected includes process configs, monitoring data, calibration files and pipeline operational records.
Renewable energy: wind, solar, hydro, biomass and green hydrogen	Turbine / inverter controller PCs, plant management servers, BESS management systems, environmental monitoring. Data protected includes control software, site configs and operational datasets.
IT systems OT depends on	Active Directory / DNS, jump hosts, historians (IT side), GIS, OMS, AMI / MDMS, billing and customer portals. Data protected includes system images, configuration data, customer and operational records.

SIEM integration: Acronis on-premises SIEM integration forwards backup, security and RMM alerts to third-party SIEMs via syslog, helping OT and security teams centralize incident awareness across all protected environments.

Compliance and assurance

Acronis helps utilities generate recovery-plan evidence and backup validation records, restore testing outputs and retention controls, and secure supplier assurance documentation that can support audit readiness across key frameworks. Acronis is IEC 62443-4-1 certified.

NERC CIP (North America)

Can help provide evidence for CIP-009 recovery plan documentation through backup validation records and forensic backup data. Designed to operate in fully isolated networks without cloud dependency.

NIS 2 Directive (Europe)

Can contribute to Article 21 business continuity and backup management expectations. Immutable backups and configurable retention periods align with NIS 2 data-protection and recovery-readiness intent.

IEC 62443 (global)

IEC 62443-4-1 SSDLC certified. Live, nondisruptive backups and integrity verification align with resource availability and continuity expectations within the IEC 62443 framework.

EU Cyber Resilience Act

Secure development lifecycle certification can support OEM supplier assurance assessments increasingly required in utility procurement under the EU CRA.

Note: Acronis supports recovery-plan evidence and audit readiness. Compliance with any regulatory framework remains the responsibility of the operator.

OEM partners and integrators

Acronis Cyber Protect for OT is available as a white-label, co-branded or reference-sold solution, enabling OEM partners and control system integrators to embed OT cyber resilience directly into their utility system portfolios.

Acronis works with OEMs and industrial technology partners across OT environments globally, including ABB, Emerson, GE Vernova, Honeywell, Rockwell Automation, Schneider Electric and Yokogawa.

For OEM partners

- Embed One-Click Recovery natively. Become a resilience partner, not just a hardware supplier.
- Help reduce reactive support call volume and engineer travel costs for common recovery scenarios.
- Enable recurring managed resilience services and expanded contract revenue.
- IEC 62443-4-1 certified, which is increasingly decisive in utility procurement and EU CRA compliance.

For control system integrators

- Package recovery as part of SCADA / HMI / OT server delivery.
- Standardize restore procedures across all delivered utility systems.
- Reduce post-deployment support burden and SLA liability.
- Add recurring resilience services to project and managed service portfolios.
- Reference sell or co-brand alongside your integration practice.

Ready to protect the infrastructure communities depend on?

Talk to an Acronis OT specialist or your OEM partner to arrange a live demonstration.

TALK TO AN OT EXPERT

Acronis

Learn more at
acronis.com