Acronis Cyber Protect for oil and gas, power and energy

Purpose-built cyber resilience for critical industrial operations

Executive summary

Oil and gas and power and energy operations depend on PC-based operational technology (OT) systems to safely generate, transmit, store and distribute energy. These environments face unique constraints: long lifecycle legacy systems, connectivity-restricted sites and low tolerance for downtime. At the same time, ransomware increasingly targets OT.

Acronis Cyber Protect for OT is engineered to deliver secure backup, fast recovery and operational resilience for OT systems without disrupting production. It helps organizations restore validated system states, reduce recovery time and support recovery and audit requirements common in industrial cybersecurity standards.

Trusted by automation vendors

YOKOGAWA · Honeywell · GE VERNOVA · ABB · EMERSON

Why Acronis for power and energy and oil and gas?

- Low agent footprint
- Offline / air-gapped operation
- Bare-metal restore speed
- Backup validation / anti-malware scanning
- One-click recovery
- Legacy OS support
- Universal Restore
- Immutable storage + replication + encryption

Acronis Cyber Protect for OT is purpose built around OT priorities: availability, convenience, recovery, prevention, legacy reality and mixed environments, and operator-led recovery workflows for remote and constrained environments.

Business value

Operational value:

- Minimize mean time to recovery (MTTR) for critical OT systems.
- Maintain production continuity.
- Reduce risk by restoring validated system states.

Risk and brand protection:

- Reduce the likelihood of unsafe or compromised restores.
- Demonstrate cyber resilience and recovery readiness to internal governance, partners and regulators.

Total cost of ownership (TCO) impact:

- Reduce OpEx by minimizing downtime and simplifying recovery of critical OT systems.
- Optimize CapEx by extending the lifecycle of legacy assets and enabling recovery to replacement hardware.

OEM and partner value:

- Embed resilience into delivered systems.
- Reduce post-deployment support burden.
- Enable recurring revenue through resilience services and lifecycle support.

Industries covered

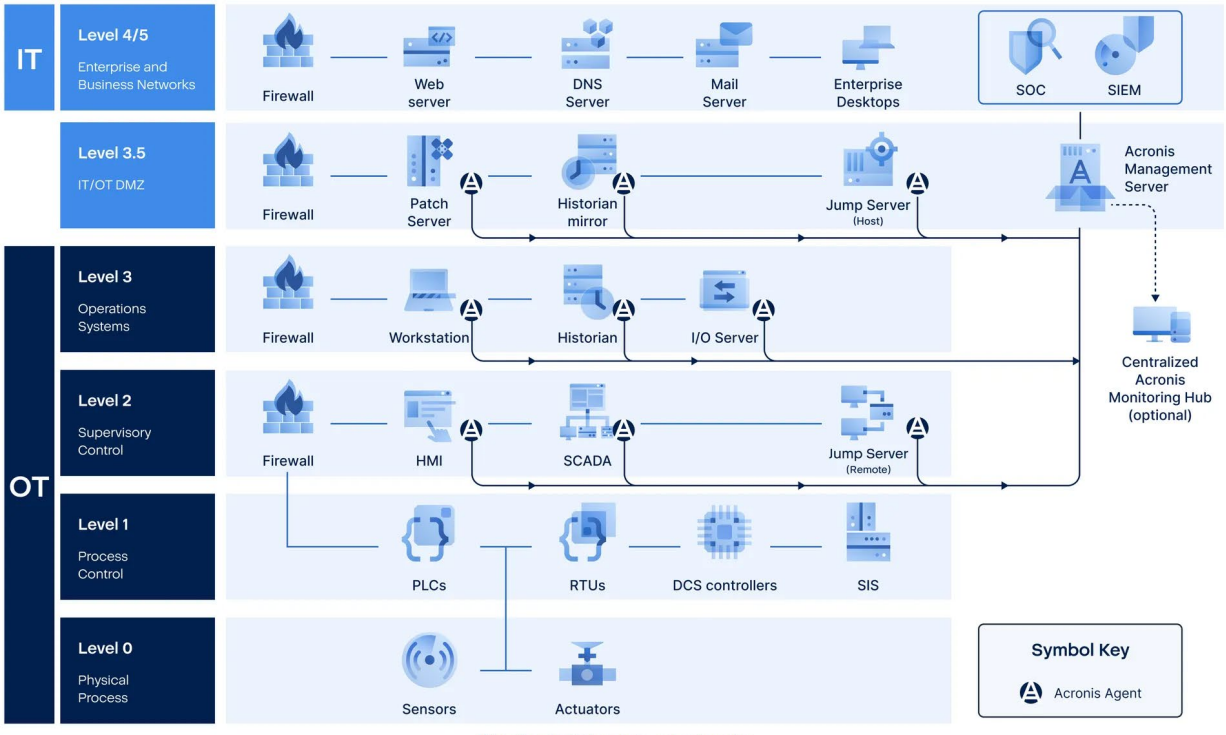
Power and energy:		
Power generation (thermal, nuclear, hydro, wind, solar, biomass and waste to energy).	Transmission and distribution (transmission networks, including HVDC systems, substations, distribution networks).	Grid edge and distributed energy (distributed energy resources (DER), microgrids, BESS).
Oil and gas:		
Upstream (exploration, drilling, offshore / onshore production, natural gas production and field processing).	Midstream (gas compression and transmission, pipeline transportation, storage terminals, LNG liquefaction and shipping).	Downstream (refining, petrochemical and chemical production, gas-to-liquids (GTL), LNG regasification).

Operational challenges in energy and oil and gas OT environments

Challenge	Why it matters
High downtime cost	Outages can cause safety risks, production loss, service disruption and regulatory exposure. Fast recovery is critical.
Cybersecurity challenges	Ransomware and targeted cyberattacks increasingly threaten SCADA, HMI, historian, engineering workstations and other critical OT systems.
Air-gapped and restricted connectivity sites	Remote and distributed sites may have limited connectivity. Continuous production, segmented networks and legacy systems complicate patching, so backup and recovery must work locally.
Legacy OS and hardware	Many OT systems run long-lived Windows / Linux builds or vendor-locked images where upgrades are risky or prohibited.
Fragile and deterministic systems	Operationally sensitive: OT environments require strict control over reboots, software updates, agent deployment and configuration changes. Protection must be low impact, predictable and operationally safe.
Limited on-site IT support	Distributed sites often depend on operators or OT engineers. Recovery must be simple and fast, even without on-site IT support.
Compliance and assurance pressure	Operators face growing expectations for recovery readiness, audit evidence and supplier assurance aligned with industrial cybersecurity frameworks.
Vendor lock in	Proprietary OEM software, licensed images and hardware-specific configurations can limit flexibility, increase costs and complicate migration, recovery and rebuilds.

What systems and data Acronis Cyber Protect secures

OT environment area	Systems protected	Data protected
Core OT and ICS	SCADA servers / clients, HMI workstations, DCS operator stations, engineering workstations, historians, OT application servers.	OS images, application stacks, SCADA / HMI configurations, historian databases, alarm logic, operating parameters.
Energy infrastructure	Substation control PCs, HVDC / FACTS servers, DER / microgrid controllers, BESS site controllers, EV charging management servers.	Site control software, configuration files, operational datasets, device drivers, recovery images.
Oil and gas operations	Pipeline monitoring servers, leak detection systems, refinery DCS / SCADA systems, turbomachinery control PCs, custody-transfer systems.	Process configurations, monitoring data, calibration / tuning files, operational records.
Engineering and digitalization	Engineering PCs, CAD / CAM workstations, simulation systems, asset management servers, digital twin platforms.	Engineering project files, drawings, models, documentation, configuration repositories, IP-sensitive project data.
OT DMZ and support systems	Jump hosts, data acquisition servers, authentication / security servers, intermediate OT / IT systems.	Access gateway configurations, logs, system images, policy / configuration data.



*List of protected systems not exhaustive

SIEM and SOC visibility: Acronis on-premises SIEM integration forwards alerts and events covering backup, security and RMM to third-party SIEMs via syslog or file export, helping OT and security teams centralize monitoring and incident awareness across protected environments.

How Acronis protects OT systems

OT-optimized backup: Full-image and file-level backups with a low footprint suitable for live OT systems, and no planned downtime required for many deployments.

Designed for segmented and air-gapped sites: Supports offline operation and local storage (SAN / NAS / dedicated storage zones) and can be deployed to align with OT network segmentation and restricted connectivity.

Safe and verified recovery: Backup validation and integrity checks and optional malware scanning of restore points to reduce the risk of restoring compromised systems.

Fast, operator-led recovery: Guided, simplified recovery workflows for sites with limited IT presence, enabling local teams to restore systems when remote access is not available.

Hardware-independent restore: Restore to new or different hardware (including P2P, P2V and V2P)* to keep operations running when original industrial PCs are obsolete or unavailable.

Safety-critical OT systems and SIS support:
In oil and gas and power operations, the priority is clear: safety first. Safety instrumented systems (SIS), including platforms such as Triconex, DeltaV SIS and Honeywell Safety Manager, depend on PC-based engineering workstations, configuration repositories, maintenance systems, documentation systems, historian interfaces and supporting servers to support safe operations.

Acronis Cyber Protect for OT focuses on protecting and recovering these supporting PC-based systems. By helping restore them to a validated, known-good state after hardware failure, corruption, ransomware or operational disruption, Acronis supports cyber resilience around safety-critical OT environments while maintaining a clear distinction between cyber resilience and functional safety.

Protect any PC-based OT system from the XP era to the present with Acronis

Acronis supports legacy PC operating systems that other vendors have abandoned:

Windows

- Windows Server 2003 SP1, R2 and later, 2008/2008 R2, 2012/2012 R2, 2016, 2019, 2022 except Nano
- Windows Small Business Server 2003/2003 R2, 2008, 2011
- Windows Home Server 2011
- Windows MultiPoint Server 2010, 2011, 2012
- Windows Storage Server 2003, 2008/2008 R2, 2012/2012 R2, 2016
- Windows XP Professional SP1, SP2, SP3
- Windows 7, 8/8.1, 10 (except RT), 11 (all editions)

Linux

- Kernel 2.6.9 to 5.19
- RHEL 4.x, 5.x, 6.x, 7.x, 8.x*, 9.0*, 9.1*, 9.2*, 9.3*
- Ubuntu 9.10 - 23.04
- Fedora 11 - 31
- SUSE Linux Enterprise Server 10, 11, 12, 15
- Debian 4.x, 5.x, 6.x, 7.0, 7.2, 7.4-7.7, 8.0-8.8, 8.11, 9.0- 9.8, 10.x, 11.x
- CentOS 5.x, 6.x, 7.x, 8.x*
- Stream 8*, 9*
- Oracle Linux 5.x, 6.x, 7.x, 8.x*, 9.0*, 9.1*, 9.2*, 9.3*
- CloudLinux 5.x, 6.x, 7.x, 8.x*
- ClearOS 5.x, 6.x, 7.x
- AlmaLinux 8.x*, 9.0*, 9.1*, 9.2*, 9.3*
- Rocky Linux 8.x*, 9.0*, 9.1*, 9.2*, 9.3*
- ALT Linux 7.0

* P2P, P2V and V2P, meaning the system can be restored from physical-to-physical, physical-to-virtual or virtual-to-physical environments, ensuring recovery remains possible even when the original industrial PC or its exact hardware is no longer available.

Key operational scenarios covered

OT system failure	Ransomware or malware incident	Failed patch or vendor update	Loss of engineering stations	Remote or offshore site outage
Industrial PC disk or motherboard failure. Restore the full system quickly to resume operations without rebuilding from scratch.	Isolate affected systems and restore clean, validated backups to return to a known-good operating state while reducing reinfection risk.	Roll back to the last known-good operational state after a change causes instability or unsafe behavior.	Restore engineering PCs and project repositories to avoid weeks of reconfiguration and to support safe change control.	Enable local recovery without internet or VPN dependency for substations, compressor stations, rigs and remote production sites.

Restore paths by failure mode

Acronis Cyber Protect for OT provides multiple recovery options so teams can select the safest and fastest restore path based on the failure mode, site constraints and operational priorities.

Failure mode	Recommended restore path	What Acronis enables	Typical personnel
Accidental deletion or corruption of a limited set of files.	Granular restore (file / folder restore).	Restore only the required files (e.g., project artifacts, configuration files, reports) without rebuilding the entire system. Minimizes operational impact and avoids unnecessary changes to the OT workstation or server.	Controls / automation engineer or OT / ICS engineer.
Partial application failure or misconfiguration (system still boots).	Roll back to last known-good state (restore point).	Revert the system to a validated restore point after a failed patch, vendor update or configuration error. Helps return the OT application stack to a predictable operational state.	Controls / automation engineer or OT / ICS engineer.
System will not boot (disk failure, corrupted OS, ransomware impact).	Bare-metal restore (bootable rescue media: Linux or WinRE).	Boot the device using Acronis rescue media and restore the full image (OS, applications, drivers and data) to return the system to a known-good operational state without manual reinstallation.	OT / ICS engineer or trained site technician.
Hardware failure with no identical spare available.	Dissimilar hardware restore (Universal Restore).	Restore the system image to replacement hardware and inject required boot-critical drivers (e.g., storage controllers / chipsets) to bring legacy and vendor-specific OT stacks back online when original industrial PCs are obsolete or unavailable.	OT / ICS engineer or site technician (IT optional).
Remote site outage (limited / no IT access).	Operator-led recovery (one-click recovery).	Guided, simplified recovery workflows enable non-IT personnel to restore OT systems locally and safely, reducing downtime where travel time or remote access constraints delay recovery.	Operator / shift supervisor or field / substation technician.
Ransomware or malware incident (risk of reinfection during restore).	Safer recovery (scan / validate restore points before recovery).	Validate backups and scan restore points for malware prior to restoration to reduce the risk of restoring compromised images. Supports a safer recovery workflow when returning OT operations to a known-good state.	OT / ICS engineer with OT security lead.

Failure mode	Recommended restore path	What Acronis enables	Typical personnel
Virtualized OT workloads need the fastest service return (where virtualization is permitted).	Rapid recovery using standby virtual machines.	Where virtualization is permitted, recover OT workloads as virtual machines to shorten service restoration and allow full validation steps to be completed without delaying operational uptime.	OT platform / virtualization engineer (OT / IT shared).
Audit, maintenance and resilience assurance requires proof of recoverability.	Verified recoverability (backup validation and bootability checks).	Validate that backups are recoverable by performing integrity checks and bootability verification. Provides operational assurance that critical OT systems can be restored within required recovery objectives.	OT / ICS engineer with OT security / compliance.

By selecting the restore path that matches the failure mode, OT teams can reduce downtime, avoid unnecessary system changes and return operations to a validated state aligned with site procedures and change-control policies.

Compliance and assurance alignment

Acronis Cyber Protect for OT supports recovery readiness, audit evidence and supplier assurance expectations commonly used in energy and industrial cybersecurity programs, including alignment with IEC 62443 recovery readiness principles and regional regulations, such as NIS 2, OT resilience requirements found in critical infrastructure regulations and sector-focused recovery planning and testing, as well as supplier assurance and secure development expectations increasingly relevant to OEMs under the EU Cyber Resilience Act (CRA).

GDPR NIS2 NIST IEC NERC CIP CRA

Acronis Cyber Protect platform compliance enablers

- Verified recovery evidence.
- Encrypted backups with retention controls.
- Controlled recovery processes.
- SSDLC practices to support supplier assurance assessments.

Acronis IEC 62443-4-1 Certified

IEC 62443-4-1 certification confirms that Acronis applies secure development lifecycle (SSDLC) practices aligned with industrial expectations. For oil and gas and power and energy organizations, this strengthens supplier assurance, reduces supply chain risk and supports confidence in OT resilience solutions.

Summary

Acronis Cyber Protect enables oil and gas and power and energy organizations to recover critical OT systems safely, predictably and quickly without disrupting operations, while supporting the growing demands of industrial cybersecurity and recovery readiness.

Acronis

Learn more at acronis.com