Preserving uptime in operational technology (OT) environments

The high costs of OT system downtime

Operational technology (OT) systems are a critical link in maintaining production uptime and company profitability. When they fail, they can bring down assembly lines, pipelines, utility grids and supply chains with them. The costs of the resulting outages can run from tens to hundreds of thousands of dollars per hour. A survey by ABB found that 69% of companies had recently experienced downtime once per month, and outages cost businesses $150,000 per hour[1]. Other consequences of OT downtime include:

- Sales opportunity costs due to unfulfilled orders and longer lead times.
- Increased direct labor costs per quantity of goods produced.
- Customer relationship and brand reputation damage caused by slow or unmet deliveries.
- Shrinking market capitalization as investors lose confidence in the business's ability to maintain consistent production.
- Financial penalties for unmet service level agreements and other contractual obligations.
- Compliance fines and criminal penalties for failure to meet regulatory requirements for cyber resilience.

As a result, the stakes are high in defending OT systems against cyberattacks, natural disasters, hardware failures, software glitches and human errors — and getting them back online quickly when they fail.

Many industries rely heavily on automation for real-time production processes, including the automotive, energy, power, pharmaceutical and logistics sectors. Much of that automation technology is controlled, configured and monitored by PCs running Windows or Linux that fall under the rubric of operational technology (OT), industrial control systems (ICS) and cyber-physical infrastructure. Common OT applications include supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), human-machine interfaces (HMI), and operational historian systems that capture real-time process data.

[1] ABB. "Value of Reliability: ABB Survey Report 2023."

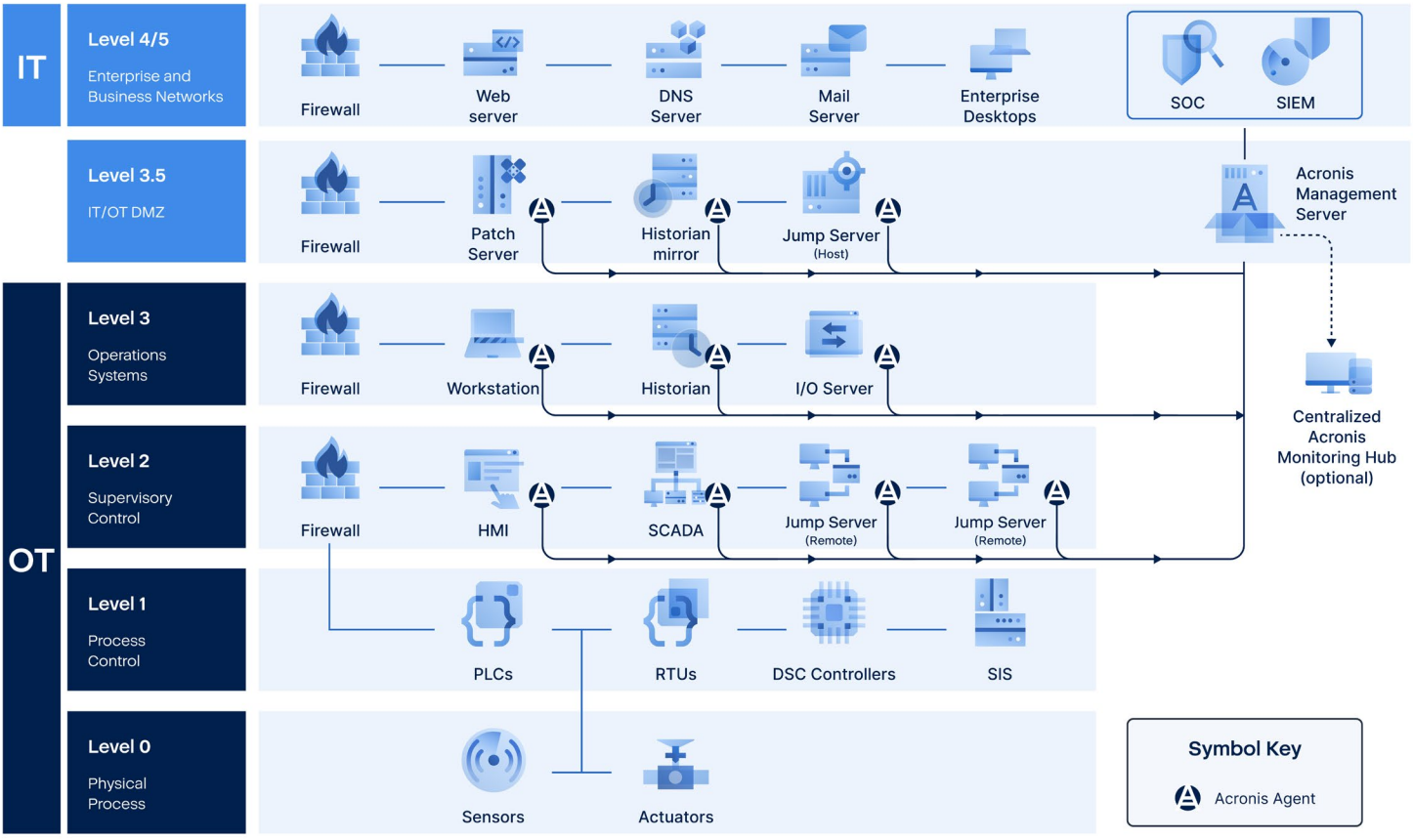
The challenges of maintaining OT system uptime

The pressure to minimize OT system downtime is amplified by the fact that OT environments have unique attributes that make them harder to keep up and running than traditional back-office and front-office IT systems:

- Many OT systems run on hardware and operating systems (OSs) that are many years old, some dating as far back as the Windows XP era. Upgrading them to new hardware and OS revisions is risky, with the potential to break or limit OT application functionality.
- The age of these systems also makes it difficult or impossible to equip them with up-to-date cybersecurity measures like endpoint detection and response (EDR).
- When an OS vendor announces its end-of-support date for a particular version of the product — for example, as Microsoft did with Windows XP in April 2014 — major backup vendors generally stop supporting it within five years, and often sooner. Without the support of a major backup vendor, OT engineers are forced to rely on slow, manual, error-prone backup processes that require costly scheduled downtime to execute.
- The facilities where OT systems are located rarely have local IT support and are often remote from centralized IT teams. Furthermore, OT environments are often air gapped to reduce cybersecurity risks, which prevents IT from using remote monitoring and management tools. Physically dispatching IT personnel to production facilities can be slow and expensive, extending costly outages.

Acronis meets the unique cyber reslience requirements of OT environments

The Acronis Cyber Protect platform is widely used in manufacturing and industry to protect a variety of OT systems. including (but not limited to) the examples in the Purdue Model shown in Figure 1



*List of protected systems not exhaustive

Figure 1: Purdue Model examples of OT systems protected by Acronis

Acronis Cyber Protect provides backup and recovery for OT systems with features that are essential in production environments that require extremely high uptime, including:

- The ability to install the Acronis Cyber Protect agent and conduct backups without ever taking the OT system offline or rebooting it.
- Fast, reliable, fully automated backup execution that offloads backup processing and storage overhead from the OT system.
- The ability to standardize (or customize) backups across systems and sites with data protection plans.
- Optional cybersecurity functions using the same Acronis agent, including EDR, anti-malware and anti-ransomware.

Acronis protects even the oldest OT systems

Acronis reinforces the stability of OT environments by protecting every operating system from the XP era to the present (including OSs long abandoned by other vendors). This ensures fast, reliable recovery of even the oldest legacy systems, with the option to replicate a system onto new PC hardware via a process called bare-metal recovery, if necessary. This feature automatically installs any necessary new drivers to ensure that the OS and OT applications run successfully on the new hardware. Figure 2 shows the range of Acronis support for OSs and hypervisors dating from the XP era to the present, highlighting the Windows and Linux versions most commonly used in OT environments:

Industry-best coverage of various OSs and hypervisors

Windows

- Windows Server 2003 SP1, R2 and later, 2008, 2008 R2, 2012/2012 R2, 2016, 2019, 2022 except Nano Server
- 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, 11 (all editions), 10, – all editions, except Windows RT

Microsoft SQL Server
2022, 2019, 2017, 2016, 2014, 2012, 2008 R2, 2008, 2005

Microsoft Exchange Server
2019, 2016, 2013, 2010, 2007

Hypervisors

VMware vSphere
4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7.0, 8.0

Microsoft Hyper-V Server
2022, 2019, 2016, 2012/2012 R2, 2008/2008 R2

Citrix XenServer / Citrix Hypervisor
8.2 - 4.1.5

Linux KVM
8 - 7.6

Scale Computing Hypercore
8.8, 8.9, 9.0

Red Hat Enterprise Virtualization (RHEV)
3.6-2.2

Red Hat Virtualization
4.0, 4.1, 4.2, 4.3, 4.4

Virtuozzo
7.0.14 - 6.0.10

Virtuozzo Infrastructure Platform
3.5

Nutanix Acropolis Hypervisor (AHV)
20160925.x through 20180425.x

MacOS

- **OS X** Mavericks 10.9, Yosemite 10.10, El Capitan 10.11
- **macOS** Sierra 10.12, High Sierra 10.13, Mojave 10.14, Catalina 10.15, Big Sur 11, Monterey 12, Ventura 13, Sonoma 14

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

Figure 2: Acronis support for operating systems and hypervisors

Acronis enables OT system restoral without IT intervention

Acronis offers a unique feature called One-Click Recovery that is critical in OT environments that lack on-site IT staff and / or are air gapped, thus preventing the use of remote management tools by centralized IT staff. Acronis One-Click Recovery enables any local worker regardless of their IT skill level to recover a failed OT system from local backup with just a few keystrokes. Costly production outages due to OT system failures that might take hours or days to resolve, including the time necessary for IT staff to be dispatched to the site, can be reduced to a matter of minutes. The feature supports the ability to recover OT systems from a local disk backup or the Acronis Cloud, and to secure backups with Bitlocker encryption and recovery passwords.

Acronis OT system protection is used by leading automation vendors

Leading OT and ICS vendors — including ABB, Siemens, Honeywell and more — use Acronis Cyber Protect as the backup solution for their customers as part of a white-labeled or co-branded solution. No other data protection vendor enjoys a similar range of partnerships with and endorsements by the automation industry.

Acronis is recognized as the OT cyber resilience leader

Leading technology research firms like Forrester Research, TAG Infosphere and Omdia rate Acronis a leader in OT system protection.

TAG Infosphere report READ

Omdia report READ

Conclusion

Acronis Cyber Protect is used to protect OT systems in manufacturing and industrial production environments around the world. Its unique combination of data protection for operating systems from the XP era to the present, One-Click Recovery for OT system restoral by non-IT workers, and adoption by leading automation vendors have all contributed to its recognition by the analyst community as a leader in OT cyber resilience.

FURTHER READING

Learn more about Acronis Cyber Protect for OT

- Acronis manufacturing solutions
- Infographic: Maintaining OT uptime with One-Click Recovery
- Case study: Tata Steel downstream products
- Case study: ABB
- Case study: Johnson Electric
- Case study: BDR Pharma
- Get a complimentary trial of Acronis Cyber Protect
- Talk to an OT cyber resilience specialist

Acronis

Learn more at acronis.com