Acronis

Preserving operational technology (OT) uptime in highly-automated factory-floor environments

For manufacturers, maintaining the uptime of operational technology (OT) on the factory floor is critical. Even brief periods of downtime have cascading effects: loss of valuable production time, reduced output, supply chain disruptions, lost revenues, frustrated customers and opportunity costs.

This need for high OT availability presents a variety of IT challenges, some of which are unique to the manufacturing industry. Specifically, the computers running the applications that control OT systems are a potential weak link. These systems can fail for a variety of reasons, including worn-out hardware (especially non-solid-state disk drives), power surges, software bugs like memory leaks, and operator errors.

When these computers fail, as every computer eventually does, production operations grind to a halt. Thus, the ability to restore critical systems very quickly — and across a variety of failure scenarios — becomes essential to maintaining high factory floor uptime.

Maintaining the uptime of these computers presents some additional challenges. The OT control software they run requires a very stable environment, which often includes a version of Windows or Linux that is no longer supported. The original computer hardware models are likely no longer manufactured. Backup software often does not support outdated OS and hardware models. And most production environments have plenty of OT expertise on hand, but very limited IT skills.

This white paper examines the high costs of downtime in highly automated OT environments, the challenges faced in ensuring continuous OT uptime, the special concerns of maintaining the computers that run OT control software, and some proven solutions for restoring those computers reliably and quickly.

Downtime is expensive

For manufacturers, maintaining continuous uptime of factory floor operations is critical. Each minute of downtime is extremely costly.

Yet unplanned downtime — whether due to hardware failure, human error or even malicious activity — remains commonplace in the manufacturing industry. A study by Aberdeen Research found that 82% of companies had recently experienced unplanned downtime, at costs that reached as high as $260,000 per hour.

Factory downtime adversely affects manufacturers in several ways:

- **Lost production** and the missed opportunities for profit that result.
- **Increased direct labor costs** proportional to the quantity of goods produced, as these costs remain the same whether production is ongoing or not.
- **Reputational harm** as slowed or unmet deliveries damage customer relationships and diminish your brand's value.
- **Contractual liabilities**, should the downtime affect your ability to meet agreed-upon obligations.

Yet another Aberdeen study indicates that the manufacturing sector as a whole loses upwards of $50 billion each year to unplanned downtime. Yet, while efforts to improve reliability face several challenges, there are solutions that make doing so not only possible, but also easy and efficient.

Data protection challenges in the manufacturing sector

Factory-floor environments are characterized by a wide array of interconnected devices and equipment, some of which run on legacy software that is not widely supported by modern vendors. Data protection solutions must be compatible with such environments, without requiring a highly specialized team to configure and maintain them.

Maintaining support for aging systems

OT manufacturers commonly use a legacy version of Windows Server or Linux on the computers that run their OT control software. This is often whatever version of the OS was current at the time the OT and its associated software was first purchased and installed.

There is little incentive to update such software, and good reason not to do so. An OS update might yield unexpected incompatibilities that could reduce the OT application's functionality or break it entirely. Stability is everything.

An obvious way to protect and restore these computers in the event of failure is with backup software: make a copy of the OS and its software, keep it in a safe place and use it to restore the system, perhaps to new computer hardware if necessary. However, many vendors of backup and disaster recovery solutions no longer support the older OSs still in common use in highly automated OT environments.

A lack of skilled IT support staff on-site

The typical factory floor environment is staffed with OT engineers to manage, support and maintain the OT

environment. However, the IT technicians that know how to manage, support and maintain traditional Windows and Linux computing platforms — which run the applications that control the OT infrastructure — are far less likely to be physically located on-site.

Best practices for maintaining OT uptime in automated factory-floor environments

To preserve the uptime of computers running OT control software, OT leaders should seek solutions that:

- **Can restore the computer from backup quickly and reliably**. This requires a backup platform that still supports older versions of operating systems, including those which may no longer be supported by their original vendor.
- **Can seamlessly restore the OT control computer software and OS to different hardware if necessary**. In the event of hardware failure, a replacement system is unlikely to be identical in configuration to the original. Rebuilding the environment with the correct drivers and other variable configuration elements can be a lengthy, tedious and error-prone process. The optimum solution is a "bare-metal" restoral that rebuilds the entire image (OS, applications, settings and data) reliably, in a single, error-free step.
- **Can be executed by OT engineers without extensive IT operations experience or skills**. Every step of the restoral operation — whether a simple reboot, reimaging of existing hardware or bare-metal restoral to new hardware — should be simple and intuitive enough to be executed by on-site OT engineers or other personnel with only basic IT skills.

Leading makers of OT in the manufacturing sector — including ABB, Siemens, Honeywell and Emerson Electric — have selected Acronis as their backup vendor of choice. For plants with mixed OT environments that include any of these vendors, there are powerful benefits to be had from standardizing the use of Acronis Cyber Protect as the backup solution for your other computers, applications and data.

Conclusion / summary

The ability to simply, quickly and reliably restore the computers that control OT is essential to maintain uptime in highly-automated factory-floor environments.

Acronis Cyber Protect has a number of powerful advantages here, including:

- Broad backup support for a range of common server OSes, including legacy versions like Microsoft Windows XP
- Rapid, unattended recovery capabilities, reducing incident-related downtime to a matter of minutes
- The ability to create a live replacement server (on physical hardware or as a virtual machine) from your latest backup
- Advanced cybersecurity and support for access controls, integrated natively into the solution

The solution is simple to use and enables quick restoration of factory-floor operations when disaster strikes. Should an OT server fail, Acronis reimages a new one — to the same hardware, a different model of server, or even as a virtual machine — that can be automatically substituted for the failed one without the need for highly-skilled, local IT support.

Ultimately, the success of any manufacturing enterprise depends on its ability to protect its data assets and maintain seamless operations. By understanding the associated backup and restoral challenges, and adopting a proactive approach to minimizing downtime, manufacturers can ensure their resilience against a variety of potential disruptions. This, in turn, will position them to thrive in an increasingly competitive and interconnected global market, while inspiring trust among their customers, partners and stakeholders alike.

About Acronis

Acronis unifies data protection and cybersecurity to deliver integrated, automated cyber protection that solves the safety, accessibility, privacy, authenticity, and security (SAPAS) challenges of the modern digital world. With flexible deployment models that fit the demands of service providers and IT professionals, Acronis provides superior cyber protection for data, applications, and systems with innovative next-generation antivirus, backup, disaster recovery, and endpoint protection management solutions powered by AI. With advanced anti-malware powered by cutting-edge machine intelligence and blockchain based data authentication technologies, Acronis protects any environment – from cloud to hybrid to on premises – at a low and predictable cost.

Founded in Singapore and headquartered in Switzerland, Acronis now has more than 2,000 employees and offices in 34 locations worldwide. Its solutions are trusted by more than 5.5 million home users and 500,000 companies, and top-tier professional sports teams. Acronis products are available through over 50,000 partners and service providers in over 150 countries and 26 languages.

Acronis

Learn more at
www.acronis.com