Wie Sie die Verfügbarkeit von OT-Umgebungen sicherstellen

OT-Ausfälle verursachen hohe Kosten

OT-Systeme sind eine kritische Komponente für die Aufrechterhaltung der Produktion und der Rentabilität von Unternehmen. Wenn sie ausfallen, kann es zu Störungen in Produktionslinien, Pipelines, Stromnetzen und Lieferketten kommen. Die daraus resultierenden Ausfallkosten können sich auf Zehn- bis Hunderttausende von Dollar pro Stunde belaufen. Laut einer Umfrage von ABB erlebten 69 % der Unternehmen in letzter Zeit einen Ausfall pro Monat – und diese Ausfälle kosteten die Unternehmen 150.000 USD pro Stunde[1]. Weitere Folgen von OT-Ausfallzeiten sind:

- Entgangene Umsätze aufgrund nicht ausgeführter Aufträge und längerer Lieferzeiten.
- Höhere direkte Arbeitskosten pro produzierter Warenmenge.
- Verlust von Kundenvertrauen und Imageschäden durch verspätete oder nicht eingehaltene Lieferungen.
- Schrumpfende Marktkapitalisierung, da Kapitalgebende das Vertrauen in die Fähigkeit des Unternehmens verlieren, die Produktion aufrecht erhalten zu können.
- Vertragsstrafen für die Nichteinhaltung von Service Level Agreements und anderen vertraglichen Verpflichtungen.
- Bußgelder und strafrechtliche Sanktionen für die Nichteinhaltung regulatorischer Anforderungen an die Cyber-Resilienz.

Es steht also viel auf dem Spiel, wenn es darum geht, OT-Systeme vor Cyberangriffen, Naturkatastrophen, Hardware- und Softwarefehlern sowie menschlichem Versagen zu schützen – und sie bei einem Ausfall schnell wieder verfügbar zu machen.

Viele Wirtschaftszweige wie die Automobilindustrie, die Energiewirtschaft, die Pharmaindustrie und die Logistikbranche sind in hohem Maße von der Automatisierung ihrer Echtzeit-Produktionsprozesse abhängig. Ein großer Teil dieser Automatisierungstechnik wird von Windows- oder Linux-PCs gesteuert, konfiguriert und überwacht. Diese gehören zu den Bereichen Operational Technology (OT), Industrial Control Systems (ICS) und Cyber-Physical Infrastructure (CPI). Typische OT-Anwendungen sind SCADA-Systeme (Supervisory Control and Data Acquisition), Prozessleitsysteme (PLS), Human Machine Interfaces (HMIs) und Operational Historian-Software, die Prozessdaten in Echtzeit erfassen.

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

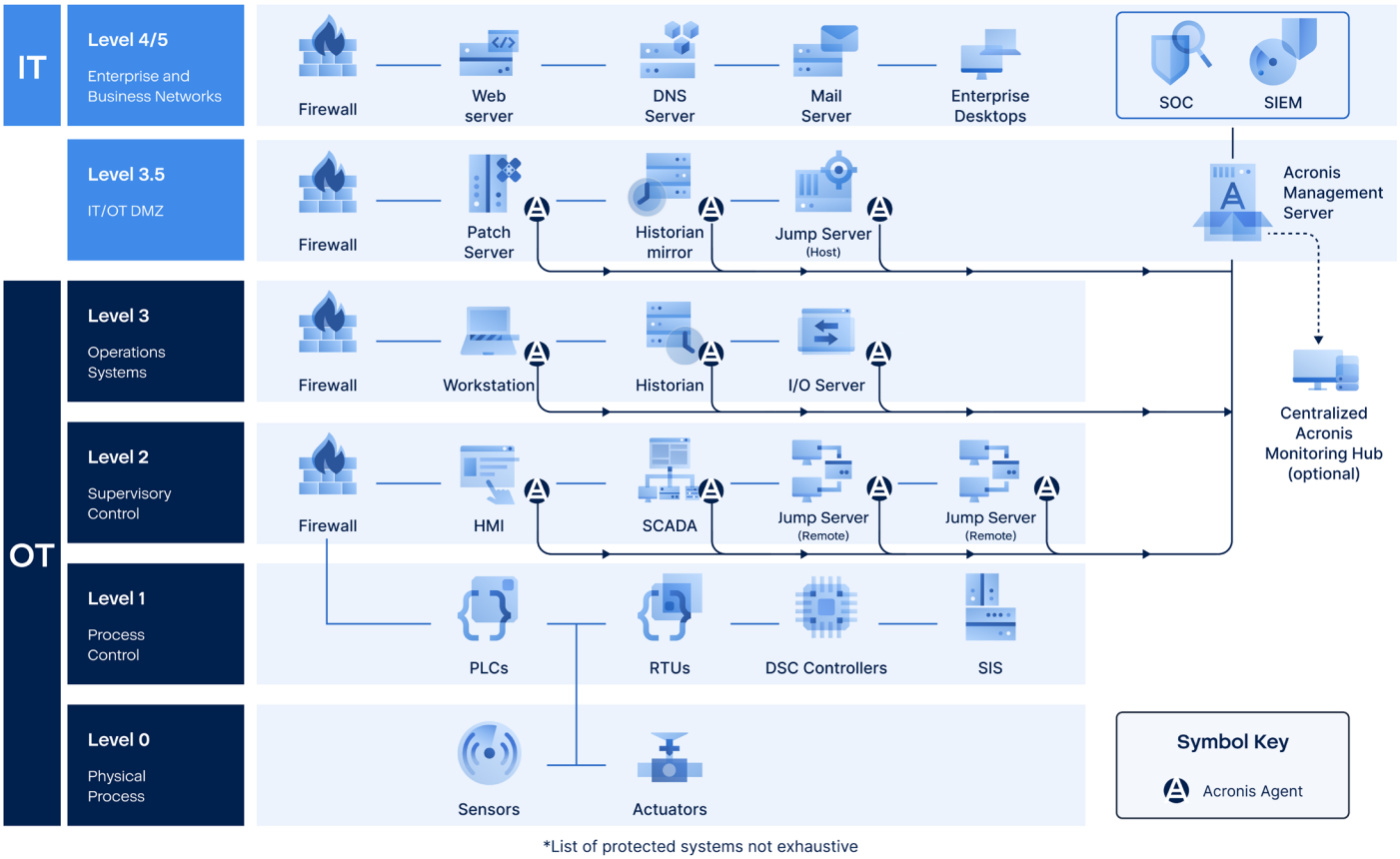
Herausforderungen bei der Aufrechterhaltung der Verfügbarkeit von OT-Systemen

Der Druck, die Ausfallzeiten von OT-Systemen so gering wie möglich zu halten, wird noch dadurch verstärkt, dass OT-Umgebungen besondere Eigenschaften aufweisen, die es (im Vergleich zu herkömmlichen Back-Office- und Front-Office-IT-Systemen) schwieriger machen, sie stets betriebsbereit zu halten:

- Viele OT-Systeme laufen auf Hardware und Betriebssystemen, die viele Jahre alt sind, einige sogar noch aus der Windows XP-Ära. Upgrades auf neue Hardware- und Betriebssystemversionen sind riskant und können dazu führen, dass OT-Systeme nur noch eingeschränkt nutzbar sind oder ganz ausfallen.
- Das Alter dieser Systeme macht es zudem schwierig oder unmöglich, sie mit aktuellen Cybersicherheitsmaßnahmen wie Endpoint Detection and Response (EDR) auszustatten.
- Wenn ein Betriebssystemhersteller das Ende des Supports für eine bestimmte Produktversion ankündigt – wie Microsoft im April 2014 für Windows XP – beenden die großen Backup-Anbieter den Support für diese Produktversion in der Regel innerhalb von fünf Jahren, oft sogar früher. Ohne die Unterstützung eines großen Backup-Anbieters sind OT-Techniker:innen gezwungen, sich auf langsame, manuelle und fehleranfällige Backup-Prozesse zu verlassen. Diese erfordern geplante Ausfallzeiten, die kostspielig sind.
- Die Einrichtungen, in denen sich OT-Systeme befinden, verfügen selten über einen lokalen IT-Support und sind oft weit von zentralen IT-Teams entfernt. Darüber hinaus sind OT-Umgebungen häufig vom Internet isoliiert, um Cyberrisiken zu reduzieren. Dies wiederum verhindert den Einsatz von RMM-Tools (Remote Monitoring and Management) durch die IT-Abteilung. Es kann zeit- und kostenaufwendig sein, IT-Personal an die Produktionsstandorte zu bringen, was die Kosten eines Ausfalls weiter in die Höhe treibt.

Acronis meistert die besonderen Anforderungen von OT-Umgebungen an die Cyber-Resilienz

Die Acronis Cyber Protect-Plattform wird in der Fertigungsindustrie und anderen Branchen eingesetzt, um eine Vielzahl von OT-Systemen zu schützen, einschließlich (aber nicht beschränkt auf) die im Purdue-Modell in Abbildung 1 gezeigten Beispiele.



*List of protected systems not exhaustive

Abbildung 1: Purdue-Modell mit Beispielen für OT-Systeme, die von Acronis geschützt werden

Acronis Cyber Protect bietet Backup & Recovery-Funktionalitäten für OT-Systeme mit Funktionen, die in Produktionsumgebungen mit extrem hohen Verfügbarkeitsanforderungen unverzichtbar sind:

- Möglichkeit, den Acronis Cyber Protect-Agenten zu installieren und Backups durchzuführen, ohne dass das OT-System jemals offline geschaltet oder neu gestartet werden muss.
- Schnelle, zuverlässige und vollautomatische Backup-Ausführung, die das OT-System von der Backup-Verarbeitung und -Speicherung entlastet.
- Möglichkeit zur Standardisierung (oder individuellen Anpassung) von Backups über Systeme und Standorte hinweg mithilfe von Data Protection-Plänen.
- Optionale Cybersicherheitsfunktionen, die über denselben Acronis Agenten bereitgestellt werden, einschließlich EDR-Funktionalität, Malware- und Ransomware-Schutz.

Acronis schützt auch veraltete OT-Systeme

Acronis erhöht die Stabilität von OT-Umgebungen durch den Schutz aller Betriebssysteme von der XP-Ära bis heute (einschließlich Betriebssystemen, die von anderen Anbietern längst nicht mehr unterstützt werden). Dies gewährleistet eine schnelle und zuverlässige Wiederherstellung selbst veralteter Systeme mit der Option, ein System bei Bedarf über Bare Metal Recovery auf fabrikneue PC-Hardware zu replizieren. Diese Funktion installiert automatisch alle notwendigen neuen Treiber, um sicherzustellen, dass das Betriebssystem und die OT-Anwendungen erfolgreich auf der neuen Hardware laufen. Abbildung 2 zeigt die Bandbreite der von Acronis unterstützten Betriebssysteme und Hypervisoren von der XP-Ära bis heute und hebt die in OT-Umgebungen am häufigsten verwendeten Versionen von Windows und Linux hervor:

Branchenweit umfassendste Abdeckung von Betriebssystemen und Hypervisoren

Windows
- Windows Server 2003 SP1, R2 und neuer, 2008, 2008 R2, 2012/2012 R2, 2016, 2019, 2022 außer 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 (alle Editionen), 10 – alle Editionen, außer Windows RT

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

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

Hypervisor

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 bis 4.1.5

Linux KVM
8 bis 7.6

Scale Computing Hypercore
8.8, 8.9, 9.0

Red Hat Enterprise Virtualization (RHEV)
3.6 bis 2.2

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

Virtuozzo
7.0.14 bis 6.0.10

Virtuozzo Infrastructure Platform
3.5

Nutanix Acropolis Hypervisor (AHV)
20160925.x bis 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 bis 5.19
- RHEL 4.x, 5.x, 6.x, 7.x, 8.x*, 9.0*, 9.1*, 9.2*, 9.3*
- Ubuntu 9.10 bis 23.04
- Fedora 11 bis 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

Abbildung 2: Von Acronis unterstützte Betriebssysteme

Acronis ermöglicht die Wiederherstellung von OT-Systemen, ohne dass die IT-Abteilung involviert werden muss

Acronis bietet eine einzigartige Funktion namens One-Click Recovery. Diese Funktion ist von entscheidender Bedeutung in OT-Umgebungen, in denen keine IT-Mitarbeiter:innen vor Ort sind und/oder die über keine Internetverbindung verfügen (der Einsatz von RMM-Tools durch die IT-Zentrale ist dort nicht möglich). Mit Acronis One-Click Recovery können alle Mitarbeiter:innen vor Ort, unabhängig von ihren IT-Kenntnissen, in wenigen einfachen Schritten ein ausgefallenes OT-System aus einem lokalen Backup wiederherstellen. Auf diese Weise können kostspielige Produktionsunterbrechungen aufgrund ausgefallener OT-Systeme, deren Behebung Stunden oder sogar Tage dauern kann (einschließlich der Zeit für die Anreise des IT-Personals), auf wenige Minuten reduziert werden. Die Funktion unterstützt die Wiederherstellung von OT-Systemen aus einem lokalen Laufwerk-Backup oder aus der Acronis Cloud. Die Backups sind durch Bitlocker-Verschlüsselung und Kennwörter, die zur Wiederherstellung notwendig sind, geschützt.

Führende Anbieter von Automatisierungslösungen schützen ihre OT-Systeme mit Acronis

Führende OT- und ICS-Anbieter (u. a. ABB, Siemens, Honeywell) verwenden Acronis Cyber Protect als Backup-Lösung für ihre Kund:innen (mit White-Labeling- oder Co-Branding-Möglichkeit). Kein anderer Data Protection-Anbieter verfügt über eine vergleichbare Anzahl von Partnerschaften und Empfehlungen aus der Automatisierungsbranche.

Acronis ist anerkannter Marktführer für Cyber-Resilienz im OT-Bereich

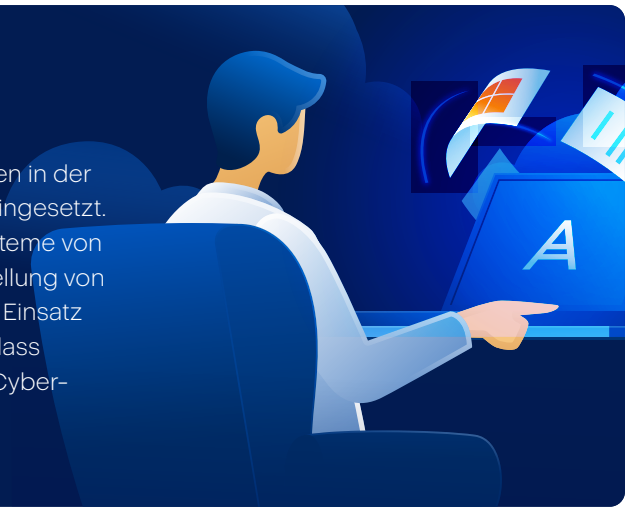
Führende Technologie-Analysehäuser wie Forrester Research, TAG Infosphere und Omdia stufen Acronis als führenden Anbieter für den Schutz von OT-Systemen ein.

Bericht von TAG Infosphere LESEN

Bericht von Omdia LESEN

Fazit

Acronis Cyber Protect wird weltweit zum Schutz von OT-Systemen in der Fertigung und anderen industriellen Produktionsumgebungen eingesetzt. Die einzigartige Kombination aus Data Protection für Betriebssysteme von Windows XP bis heute, One-Click Recovery für die Wiederherstellung von OT-Systemen durch Personal ohne IT-Kenntnisse und der breite Einsatz bei führenden Automatisierungsanbietern haben dazu geführt, dass Acronis Cyber Protect von Analyst:innen als führend im Bereich Cyber-Resilienz für OT-Systeme eingestuft wird.



WEITERFÜHRENDE LITERATUR

Weitere Informationen zu Acronis Cyber Protect für OT

- Acronis Lösungen für die Fertigungsindustrie
- Infografik: Betriebstechnologie mit One-Click Recovery jederzeit verfügbar halten
- Anwenderbericht: Tata Steel Downstream Products Limited
- Anwenderbericht: ABB
- Anwenderbericht: Johnson Electric
- Anwenderbericht: BDR Pharma
- Testen Sie Acronis Cyber Protect kostenlos
- Vereinbaren Sie eine professionelle Beratung zu Cyber-Resilienz in OT-Umgebungen

Acronis

Weitere Informationen finden Sie auf www.acronis.com