Verfügbarkeit operativer Technologie in hochautomatisierten Werken schützen

In der Fertigung ist die laufende Verfügbarkeit operativer Technologie (OT) im Werk von entscheidender Bedeutung. Selbst kurze Ausfälle können einen Dominoeffekt auslösen, in dessen Folge es zum Verlust wertvoller Produktionszeit, geringerer Produktivität, gestörten Lieferketten, Umsatzeinbrüchen, frustrierten Kunden und verpassten Chancen kommt.

Die Notwendigkeit der hohen OT-Verfügbarkeit stellt die IT vor verschiedene Herausforderungen, die teils nur in der Fertigungsbranche zu finden sind. Insbesondere die Computer, auf denen Anwendungen zur Steuerung von OT-Systemen laufen, sind potenzielle Schwachstellen. Die Gründe für den Ausfall dieser Systeme sind vielfältig und reichen von Hardware-Verschleiß (besonders bei herkömmlichen Festplatten) und Stromspitzen über Softwarefehler wie Speicherlecks bis hin zu Anwenderfehlern.

Wie jeder andere Computer sind diese Systeme dazu verurteilt, früher oder später auszufallen – und dadurch die Produktion zum Erliegen zu bringen. Deshalb ist eine schnelle Wiederherstellung kritischer Systeme (in vielfältigsten Szenarien) ausschlaggebend für hohe Verfügbarkeit im Werk.

Diese Verfügbarkeit zu gewähren, birgt jedoch noch weitere Herausforderungen. Die verwendete OT-Steuersoftware erfordert eine äußerst stabile Umgebung, was oft bedeutet, dass nicht mehr unterstützte Windows- oder Linux-Versionen im Einsatz sind. Auch kann es sein, dass die ursprüngliche Hardware nicht mehr hergestellt wird. Veraltete Betriebssysteme und Hardware werden von Backup-Software oft nicht unterstützt. Und in den meisten Produktionsumgebungen finden sich zwar zahlreiche OT-Expert:innen, denen es jedoch an umfassenden IT-Kenntnissen mangelt.

In diesem Whitepaper geht es um die hohen Kosten von Ausfallzeit in hochautomatisierten OT-Umgebungen, Herausforderungen bei der Gewährleistung durchgängiger OT-Verfügbarkeit, Besonderheiten beim Betrieb der Computer, auf denen OT-Steuersoftware ausgeführt wird und bewährte Lösungen zur zuverlässigen und schnellen Wiederherstellung dieser Computer.

Der hohe Preis von Ausfällen

Für Hersteller ist ein unterbrechungsfreier Werksbetrieb von entscheidender Bedeutung. Jede Minute an Ausfallzeit verursacht hohe Kosten.

Dennoch sind ungeplante Ausfälle in der Fertigungsindustrie keine Seltenheit, sei es aufgrund von Hardware-Fehlern, menschlichem Versagen oder Sabotage. Laut einer Studie von Aberdeen Research ist es in der jüngeren Vergangenheit in 82 % aller Unternehmen zu ungeplanten Ausfällen gekommen. Die Kosten dafür erreichten bis zu 260.000 USD pro Stunde.

Hersteller sind auf verschiedene Arten von Ausfällen ihrer Anlagen betroffen:

Produktionsverluste und dadurch verpasste Gewinnchancen.

- **Höhere direkte Arbeitskosten** proportional zur Menge der gefertigten Produkte, da diese Kosten bei laufender und stillstehender Produktion gleich bleiben.
- **Rufschädigung**, da verzögerte und nicht erfüllte Aufträge Kundenbeziehungen schädigen und den Wert Ihrer Marke schmälern.
- **Vertragliche Verbindlichkeiten**, falls Sie Vereinbarungen aufgrund eines Ausfalls nicht erfüllen können.

Eine weitere Studie von Aberdeen Research zeigt, dass die Fertigungsbranche insgesamt durch ungeplante Ausfallzeiten jährlich mehr als 50 Milliarden USD verliert. Zwar gilt es beim Verbessern der Zuverlässigkeit, zahlreiche Hürden zu überwinden, aber es gibt Lösungen, mit denen dies nicht nur möglich wird, sondern auch einfach und effizient gelingt.

Data Protection – Herausforderungen in der Fertigung

In Fertigungsanlagen findet sich eine breite Vielfalt an vernetzten Geräten. Auf einigen läuft veraltete Software, die von aktuellen Anbietern nicht unbedingt unterstützt wird. Data-Protection-Lösungen müssen mit derartigen Umgebungen kompatibel sein, wobei für ihre Konfiguration und Wartung kein hochspezialisiertes Personal erforderlich sein darf.

Unterstützung veralteter Systeme

OT-Steuersoftware läuft häufig unter veralteten Versionen von Windows Server oder Linux. Dabei handelt es sich oft um die Version dieser Betriebssysteme, die bei Kauf und Installation der OT und ihrer Software gerade aktuell war.

Es gibt kaum Anreize zur Aktualisierung dieser Software und sogar gute Gründe dagegen, denn dabei kann es zu unerwarteten Inkompatibilitäten mit Anwendungen kommen, die so in ihrer Funktion eingeschränkt oder gänzlich unbrauchbar werden. Stabilität hat Vorrang.

Ein einfacher Weg zum Schützen und Wiederherstellen dieser Computer bei Ausfällen ist Backup-Software: Es wird eine Kopie des Betriebssystem und der zugehörigen Software erstellt, sicher verwahrt und zum Wiederherstellen des Systems verwendet, ggf. auch auf neuer Hardware. Allerdings unterstützen viele Anbieter von Lösungen für Backups und Disaster Recovery die älteren Betriebssysteme nicht mehr, die in hochautomatisierten OT-Umgebungen noch vielerorts im Einsatz sind.

Mangel an erfahrenem IT-Supportpersonal vor Ort

In Werken arbeiten üblicherweise Techniker:innen, die auf die Verwaltung, Unterstützung und Wartung von OT-Umgebungen spezialisiert sind. IT-Mitarbeiter:innen, die herkömmliche Windows- und Linux-Plattformen verwalten, unterstützen und pflegen können – auf denen Anwendungen zur Steuerung der OT-Infrastrukturen laufen – sind dort weitaus weniger häufig anzutreffen.

Best Practices für OT-Verfügbarkeit in hochautomatisierten Werken

Um die Verfügbarkeit von Computern zu sichern, auf denen OT-Steuersoftware läuft, müssen führende Lösungen:

- **Computer per Backup schnell und zuverlässig wiederherstellen**. Dazu ist eine Backup-Plattform nötig, die auch ältere Betriebssystemversionen unterstützt, einschließlich jener, die von ihrem ursprünglichen Anbieter keinen Support mehr erhalten.
- **Software und Betriebssysteme von OT-Steuercomputern bei Bedarf nahtlos auf neuer Hardware wiederherstellen**. Bei einem Hardware-Fehler ist es unwahrscheinlich, dass die Konfigurationen von Original- und Ersatzsystem identisch sind. Der Wiederaufbau der Umgebung mit den korrekten Laufwerken und anderen variablen Konfigurationselementen kann langwierig, mühevoll und fehleranfällig sein. Die Ideallösung ist eine „Bare-Metal"-Wiederherstellung, bei der das gesamte Image (Betriebssystem, Anwendungen und Daten) zuverlässig in nur einem fehlerfreien Schritt wiederhergestellt wird.
- **Von OT-Techniker:innen ohne umfassende operative IT-Kompetenzen umsetzbar sein**. Jeder Schritt der Wiederherstellung – egal, ob einfacher Neustart, Neukonfiguration vorhandener Hardware oder Bare-Metal-Wiederherstellung auf neuer Hardware – sollte einfach und intuitiv genug sein, um vor Ort von OT-Techniker:innen oder anderem Personal mit IT-Grundkenntnissen umgesetzt werden zu können.

Führende OT-Hersteller in der Fertigungsbranche – darunter ABB, Siemens, Honeywell und Emerson Electric – setzen für Backups auf Acronis. Werke mit OT-Anlagen von diesen und anderen Herstellern profitieren umfassend von Acronis Cyber Protect als standardisierte Backup-Lösung für alle weiteren Computer, Anwendungen und Daten.

Zusammenfassung

Die einfache, schnelle und zuverlässige Wiederherstellung von OT-Steuercomputern ist ausschlaggebend für die zuverlässige Verfügbarkeit von hochautomatisierten Fertigungsanlagen.

Dafür bietet Acronis Cyber Protect zahlreiche wichtige Vorteile, darunter:

- umfassende Backup-Unterstützung diverser gängiger Serverbetriebssysteme, einschließlich veralteter Versionen wie Microsoft Windows XP
- Funktionen für schnelle, automatische Wiederherstellungen, die vorfallsbezogene Ausfälle auf wenige Minuten verkürzen
- Möglichkeit zum Erstellen eines Live-Ersatz-Servers (auf physischer Hardware oder als virtuelle Maschine) aus Ihrem aktuellen Backup
- erweiterte Cyber Security und Unterstützung von Zugriffskontrollen, die nativ in die Lösung integriert sind

Die benutzerfreundliche Lösung ermöglicht eine schnelle Wiederherstellung des Werksbetriebs im Ernstfall. Fällt ein OT-Server aus, erstellt Acronis einen neuen – auf derselben Hardware, auf einem anderen Servermodell oder auch als virtuelle Maschine. Der neue Server ersetzt den ausgefallenen nahtlos, ohne dass erfahrene IT-Expert:innen vor Ort sein müssen. Letztendlich hängt der Erfolg eines Fertigungsunternehmens von seiner Fähigkeit ab, seine Daten zu schützen und einen nahtlosen Betrieb aufrecht zu erhalten. Wenn Hersteller die Herausforderungen im Zusammenhang mit Backups und Wiederherstellungen verstehen und Ausfallzeit proaktiv minimieren, können sie sich vor den verschiedensten Störungen schützen. Dadurch bleiben sie auf dem immer härter umkämpften und enger vernetzten Weltmarkt konkurrenzfähig und sichern sich das Vertrauen von Kunden, Partnern und Stakeholdern.

Über Acronis

Acronis vereint Data Protection und Cyber Security in einer integrierten, automatisierten Cyber Protection-Lösung, die mit Verlässlichkeit, Verfügbarkeit, Vertraulichkeit, Authentizität und Sicherheit (engl. safety, accessibility, privacy, authenticity, security, kurz: SAPAS) die Herausforderungen der modernen digitalen Welt zu bewältigt. Dank flexibler Deployment-Modelle, die die Anforderungen von Service Providern und IT-Verantwortlichen erfüllen, bietet Acronis hervorragende Cyber Protection für Daten, Applikationen und Systeme mit innovativen Lösungen, die Virenschutz der nächsten Generation, Backup, Disaster Recovery und Verwaltung für den Endpunktschutz mit KI umfassen. Unterstützt durch erweiterten Malware-Schutz mit modernster Maschinenintelligenz und Blockchain-basierter Authentifizierung schützt Acronis Ihre Daten in allen lokalen, Cloud-basierten und hybriden Umgebungen – zu geringen und vorhersagbaren Kosten.

Acronis wurde in Singapur gegründet und hat den Hauptsitz in der Schweiz. Heute beschäftigt das Unternehmen mehr als 2.000 Mitarbeiter:innen an 34 Standorten auf der ganzen Welt. Den Acronis Lösungen vertrauen bereits mehr als 5,5 Millionen Privatanwender:innen und 500.000 Unternehmen und erstklassige Profisport-Teams. Acronis Produkte können über mehr als 50.000 Partner und Service Provider in über 150 Ländern und in 26 Sprachen erworben werden.

Acronis

Weitere Informationen unter www.acronis.com