Maintenir la disponibilité des systèmes dans les environnements OT

Les coûts élevés des interruptions d'activité des systèmes OT

Les systèmes de technologie opérationnelle (OT) jouent un rôle essentiel dans le maintien de la continuité de production et de la rentabilité des entreprises. En cas de défaillance, ils peuvent entraîner l'arrêt de la chaîne de montage, de l'exécution du pipeline, des réseaux électriques ou encore des chaînes logistiques. Le coût de ces interruptions peut atteindre plusieurs dizaines, voire centaines de milliers de dollars par heure. Une enquête menée par ABB a révélé que 69 % des entreprises subissaient des interruptions au moins une fois par mois, pour un coût moyen de 150 000 dollars par heure[1]. Parmi les autres conséquences des interruptions d'activité des environnements OT, on peut citer :

- La perte d'opportunités commerciales liée aux commandes non honorées et à l'allongement des délais de livraison.
- L'augmentation des coûts de main-d'œuvre directe par unité produite.
- La détérioration des relations clients et de la réputation de la marque à cause de livraisons lentes ou incomplètes.
- La baisse de la capitalisation boursière, les investisseurs perdant confiance dans la capacité de l'entreprise à assurer une production stable.
- Les pénalités financières en cas de non-respect des contrats ou des accords de niveau de service.
- Les amendes et sanctions pénales pour non-conformité aux exigences en matière de cybersécurité.

C'est pourquoi il est crucial de protéger les systèmes OT contre les cyberattaques, les catastrophes naturelles, les défaillances matérielles, les bugs logiciels et les erreurs humaines, et de pouvoir les remettre en service rapidement en cas d'incident.

De nombreuses industries dépendent fortement de l'automatisation pour leurs processus de production en temps réel, notamment les secteurs de l'automobile, de l'énergie, de l'électricité, de la pharmacie et de la logistique. Une grande partie de cette technologie d'automatisation est contrôlée, configurée et surveillée par des PC sous Windows ou Linux, qui relèvent des technologies opérationnelles (OT), des systèmes de contrôle industriel (ICS) et de l'infrastructure cyber-physique. Parmi les applications OT courantes, on trouve les systèmes de contrôle et d'acquisition de données (SCADA), les systèmes de contrôle distribués (DCS), les interfaces homme-machine et les systèmes historiques opérationnels qui capturent les données de processus en temps réel.

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

Les défis du maintien de la disponibilité des systèmes OT

La pression pour limiter les interruptions dans les systèmes OT est d'autant plus forte que ces environnements ont des spécificités qui compliquent leur maintien en fonctionnement par rapport aux systèmes informatiques classiques de front- et back-office :

- De nombreux systèmes OT sont exploités sur du matériel et des systèmes d'exploitation vieux de plusieurs années, parfois datant de l'époque de Windows XP. Les mettre à niveau vers un nouveau matériel ou un système d'exploitation plus récent risque de faire échouer ou de limiter les fonctionnalités des applications OT.
- L'ancienneté de ces systèmes rend également difficile, voire impossible, l'implémentation de mesures de cybersécurité modernes comme les solutions EDR de détection et de réponse des terminaux.
- Lorsqu'un éditeur de système d'exploitation annonce la fin de la prise en charge d'une version, comme ce fut le cas pour Windows XP en avril 2014, les principaux éditeurs de solutions de sauvegarde cessent généralement leur support dans un délai de cinq ans, parfois même plus tôt. Sans solution de sauvegarde fiable, les ingénieurs OT doivent recourir à de longues procédures manuelles, sources d'erreurs, qui nécessitent une interruption d'activité planifiée et coûteuse.
- Les sites hébergeant des systèmes OT disposent rarement d'un support informatique local et sont souvent éloignés des équipes IT centrales. De plus, ces environnements sont fréquemment isolés pour des raisons de sécurité, ce qui empêche l'utilisation d'outils de gestion et de surveillance à distance. Faire intervenir l'équipe IT sur place est à la fois long et onéreux, prolongeant ainsi les interruptions coûteuses.

Acronis répond aux exigences spécifiques de cyberrésilience des environnements OT

La plate-forme Acronis Cyber Protect est largement utilisée dans le secteur industriel et de la fabrication pour protéger divers systèmes OT, y compris (mais sans s'y limiter) ceux illustrés dans le modèle Purdue présenté en figure 1.

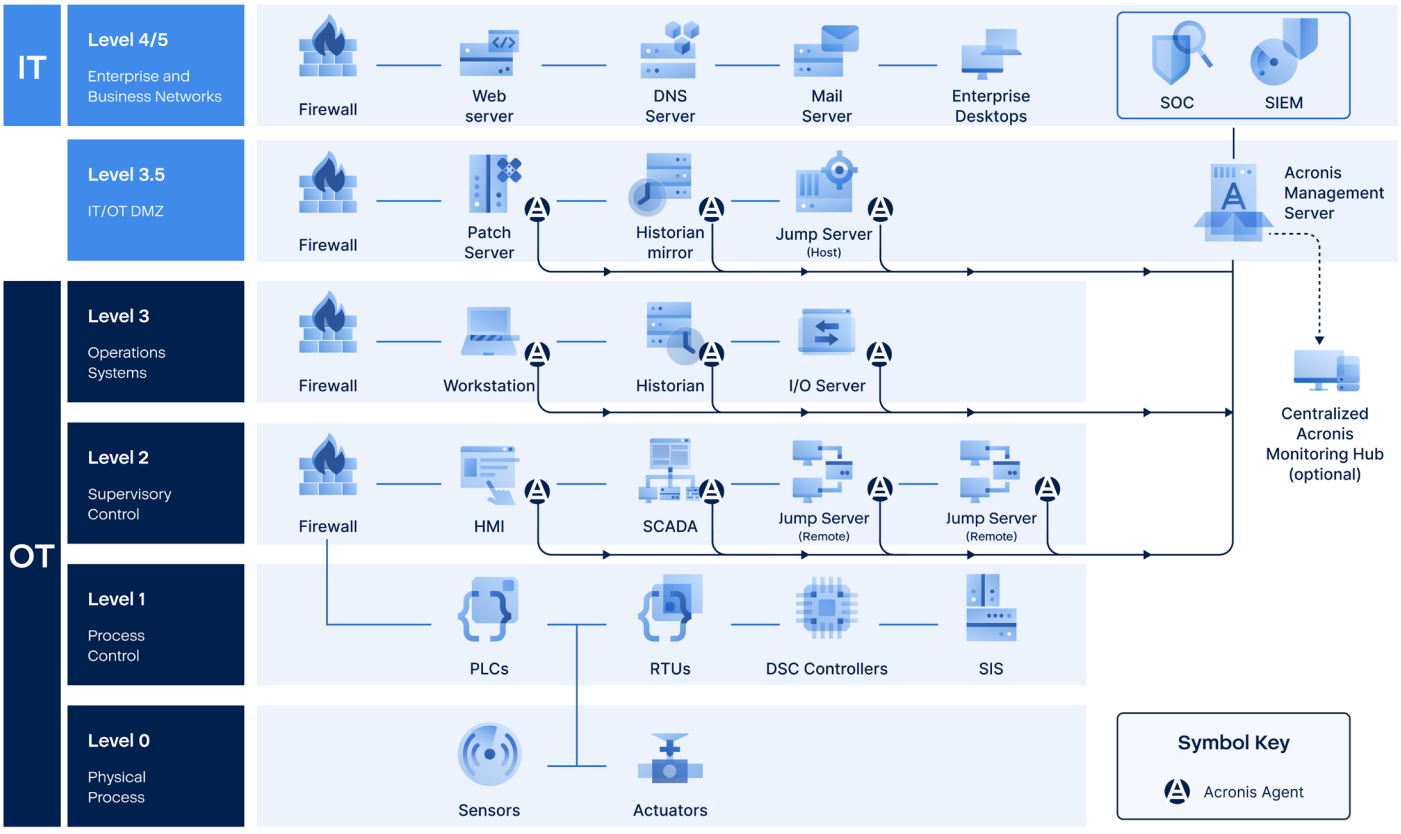

Figure 1 : Exemples de systèmes OT protégés par Acronis dans le modèle Purdue

Acronis Cyber Protect assure la sauvegarde et la restauration des systèmes OT grâce à des fonctionnalités essentielles pour les environnements de production nécessitant un haut niveau de disponibilité, notamment :

- La possibilité d'installer l'agent Acronis Cyber Protect et d'effectuer des sauvegardes sans jamais mettre le système OT hors ligne ou le redémarrer.
- Une exécution rapide, fiable et entièrement automatisée des sauvegardes, qui décharge la sauvegarde et le stockage hors du système OT.
- La possibilité d'uniformiser (ou de personnaliser) les sauvegardes sur l'ensemble des systèmes et sites grâce à des plans de protection des données.
- Des fonctions de cybersécurité optionnelles via le même agent Acronis, comme l'EDR, l'anti-malware et l'anti-ransomware.

Acronis protège même les systèmes OT les plus anciens

Acronis renforce la stabilité des environnements OT en assurant la protection de tous les systèmes d'exploitation, de l'ère Windows XP à aujourd'hui (y compris ceux abandonnés depuis longtemps par d'autres éditeurs). Cela garantit une restauration rapide et fiable, même pour les systèmes hérités les plus anciens, avec la possibilité de répliquer un système sur un nouveau matériel via un processus appelé restauration sur système nu, si nécessaire. Cette fonctionnalité installe automatiquement les pilotes requis pour garantir le bon fonctionnement du système d'exploitation et des applications OT sur le nouveau matériel. La figure 2 présente la gamme de systèmes d'exploitation et d'hyperviseurs pris en charge par Acronis depuis l'ère Windows XP, en mettant en évidence les versions de Windows et Linux les plus utilisées dans les environnements OT :

La meilleure couverture de l'industrie de différents systèmes d'exploitation et hyperviseurs

Windows
- Windows Server 2003 SP1/2003 R2 et versions ultérieures, 2008, 2008 R2, 2012/2012 R2, 2016, 2019, 2022, à l'exception de Nano Server
- Windows Small Business Server 2003/2003 R2, 2008, 2011
- Windows Home Server 2011
- Server MultiPoint Windows 2010/2011/2012
- Windows Storage Server 2003, 2008, 2008 R2, 2012, 2012 R2, 2016
- Windows XP Professionnel SP1, SP2, SP3
- Windows 7, 8/8.1, 11 (toutes les éditions), 10, toutes les éditions, à l'exception de Windows RT

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

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

Hyperviseurs

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 à 4.1.5

Linux KVM
8 à 7.6

Scale Computing Hypercore
8.8, 8.9, 9.0

Red Hat Enterprise Virtualization (RHEV)
3.6 à 2.2

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

Virtuozzo
7.0.14 à 6.0.10

Virtuozzo Infrastructure Platform
3.5

Nutanix Acropolis Hypervisor (AHV)
20160925.x à 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 : Kerrnel 2.6.9 à 5.19
- RHEL 4.x, 5.x, 6.x, 7.x, 8.x*, 9.0*, 9.1*, 9.2*, 9.3*
- Ubuntu 9.10 à 23.04
- Fedora 11 à 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 : Prise en charge par Acronis des systèmes d'exploitation et des hyperviseurs

Acronis permet la restauration des systèmes OT sans intervention de l'équipe IT

Acronis inclut One-Click Recovery, une fonction de restauration en un clic, essentielle dans les environnements OT qui manquent de personnel IT sur site ou qui sont isolés, empêchant ainsi l'utilisation des outils de gestion à distance par le personnel IT centralisé. Cette fonction permet à tout collaborateur, quel que soit son niveau de compétence en informatique, de restaurer un système OT défaillant en quelques instants à partir d'une sauvegarde locale. Les interruptions de production coûteuses causées par des pannes de systèmes OT, qui pourraient durer des heures, voire des jours, en attendant l'intervention du personnel IT sur site, peuvent ainsi être réduites à quelques minutes. Cette fonctionnalité permet de restaurer les systèmes OT à partir d'une sauvegarde de disque locale ou depuis Acronis Cloud, et de sécuriser les sauvegardes avec le chiffrement Bitlocker et des mots de passe de restauration.

De grands fournisseurs de systèmes d'automatisation font confiance à Acronis pour protéger leurs systèmes OT

Les principaux fournisseurs de systèmes OT et ICS, tels qu'ABB, Siemens, Schneider Electric, Rockwell Automation et bien d'autres, utilisent Acronis Cyber Protect comme solution de sauvegarde pour leurs clients, soit en marque blanche, soit en co-branding. Aucun autre fournisseur de solutions de protection des données ne bénéficie d'un réseau de partenariats et de soutiens aussi large au sein de l'industrie de l'automatisation.

Acronis est reconnu comme le leader de la cyberrésilience des systèmes OT

Des cabinets d'études technologiques de renom, tels que Forrester Research, TAG Infosphere et Omdia, classent Acronis parmi les leaders de la protection des systèmes OT.

Rapport TAG Infosphere LIRE

Rapport Omdia LIRE

Conclusion

Acronis Cyber Protect est utilisé pour protéger les systèmes OT dans les environnements de production industrielle et de fabrication à travers le monde. Sa combinaison unique de protection des systèmes d'exploitation depuis l'ère Windows XP à aujourd'hui, et de la fonctionnalité One-Click Recovery permettant aux collaborateurs sans connaissance informatique de restaurer les systèmes OT en un clic, ainsi que son adoption par les principaux fournisseurs de systèmes d'automatisation, ont fait d'Acronis un leader en cyberrésilience des systèmes OT, selon la communauté des analystes.

POUR ALLER PLUS LOIN

En savoir plus sur Acronis Cyber Protect pour les systèmes OT

- Solutions Acronis pour le secteur de la fabrication
- Infographie : Acronis One-Click Recovery : des technologies opérationnelles toujours disponibles
- Étude de cas : Tata Steel
- Étude de cas : ABB
- Étude de cas : Johnson Electric
- Étude de cas : BDR Pharma
- Bénéficiez d'un essai gratuit d'Acronis Cyber Protect
- Contactez un spécialiste de la cyberrésilience des systèmes OT

Acronis

Pour en savoir plus, rendez-vous sur www.acronis.com