Gestion des données dans l'industrie 4.0 :

Atteindre une visibilité totale à l'ère de l'IoT

cisco

Gestion des données dans l'industrie 4.0 :

Atteindre une visibilité totale à l'ère de l'IoT

Les industriels font visiblement preuve d'innovation. Ils ont considérablement amélioré leurs processus au cours des dernières décennies (par exemple, Six Sigma et la simplification des techniques de production).

Aujourd'hui, la transformation numérique révolutionne le secteur industriel. Toutefois, dans les usines, il reste un volume considérable de silos de données et d'appareils non connectés.

En tant qu'industriel, vous pouvez exploiter ce potentiel pour gagner en efficacité et en productivité. Mais dans l'état actuel, ces silos et appareils non connectés engendrent vite des congestions opérationnelles.

L'émergence de l'Ethernet industriel dans l'usine vient toutefois changer la donne.

Associé à d'autres technologies de l'industrie numérique, l'Ethernet industriel :

- Élimine les silos de réseaux
- Fait converger les réseaux industriels et d'entreprise
- Rapproche les technologies opérationnelles (OT) et les technologies de l'information (IT)

Avec leurs nombreux bénéfices, ces avancées présentent également des défis potentiels pour l'usine :

- Des risques pour la sécurité
- Des défis en matière de gestion des bases de données
- Des problèmes de gestion du réseau

Pour s'adapter à ce nouveau monde, où les flux de données ne s'arrêtent jamais, il faut savoir saisir les opportunités. L'objectif est de collecter et d'exploiter toutes les données pertinentes sans faire courir de nouveaux risques à votre entreprise.

Cisco Digital Network Architecture (DNA) pour l'industrie

Aujourd'hui, **près de 4 industriels sur 5 s'attendent à ce que la révolution numérique ait un impact modéré ou majeur[1].** Cette pression continue sur les industriels les incite à trouver de nouveaux modes d'innovation et à renforcer la productivité de leurs usines.

Cisco DNA révolutionne la façon dont les industriels conçoivent, mettent en place et gèrent leurs bureaux et leurs usines. Avec Cisco DNA, les déploiements sont plus rapides et la gestion du réseau est centralisée et simplifiée. Vous pouvez mettre en service plusieurs sites réseau en quelques jours plutôt qu'en plusieurs mois. Cisco DNA offre également des informations réseau exploitables pour optimiser les opérations sur la chaîne de production. **Grâce aux solutions Cisco DNA pour les industriels, vous pouvez déployer des capacités numériques clés s'appuyant sur une infrastructure numérique – en toute sécurité, simplement et judicieusement.**

En savoir plus sur Cisco DNA pour les industriels.

1. http://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/digital-network-architecture/at-a-glance-c45-739029.pdf

Section I. Saisir les opportunités offertes par une usine connectée

La connexion d'appareils auparavant non connectés offre deux opportunités principales : une meilleure visibilité sur l'usine et des capacités analytiques avancées.

Une meilleure visibilité sur l'usine

Selon une étude menée par le ministère de l'Industrie et le Symop, l'âge moyen de l'ensemble des équipements industriels s'élevait à 17,5 ans en 2015.[2] Par conséquent, la plupart de ces machines industrielles ne sont pas connectées au réseau.

Mais les temps changent. De nos jours, l'utilisation de l'Ethernet industriel est devenue la norme dans les réseaux d'usine. Et le domaine des réseaux industriels continue à connaître des avancées. Les normes telles que Time Sensitive Networking (TSN, IEEE 802.1) permettent même d'exécuter sur l'Ethernet industriel les applications déterministes dont les boucles de contrôle sont les plus exigeantes. Et cela contribue à renforcer l'interopérabilité dans l'usine.

Grâce à toutes ces innovations, les industriels rassemblent désormais leurs « îlots de données ». Le secteur **industriel génère en effet plus de données que tout autre secteur de l'économie française**[3].

En exploitant de façon stratégique ces données, vous pouvez :

- Acquérir une visibilité totale sur les performances et l'état de fonctionnement des machines et des ressources, ce qui :
  - Améliore l'efficacité globale des équipements
  - Diminue les temps d'arrêt
  - Accélère le lancement de nouveaux produits
  - Améliore la rotation des stocks
- Mieux coordonner l'entretien des systèmes pour éviter les interruptions non prévues de l'activité et optimiser les unités de production de l'usine grâce à la maintenance prédictive.
- Mieux connaître votre consommation d'énergie pour optimiser les workflows et les opérations afin de réduire les coûts.

Cisco Kinetic

Cisco Kinetic relie vos environnements IT et OT et de plus larges réseaux d'objets connectés (IoT) pour les regrouper dans une seule vue opérationnelle. Le résultat est une plate-forme centrale qui offre des informations qu'aucune autre technologie ne peut offrir.

Avec Cisco Kinetic, vous pouvez :

- **Bénéficier d'une visibilité complète sur vos appareils IT et OT**
- **Renforcer l'efficacité de vos usines**
- **Simplifier la gestion des sites à distance**

En savoir plus sur Cisco Kinetic

« Le secteur industriel génère plus de données que tout autre secteur de l'économie française. »

Tweetez cette citation

2. http://www.symop.com/wp-content/uploads/2015/03/20150217_Symop_reaction_etude-VDEF.pdf
3. http://www.mckinsey.com/business-functions/operations/our-insights/digital-manufacturing-the-revolution-will-be-virtualized

Section I. Saisir les opportunités offertes par une usine connectée

La connectivité n'est toutefois qu'un avantage parmi d'autres. Dès que vos appareils sont connectés, vous avez besoin d'analyses exploitables pour intégrer les données dans les processus de l'entreprise. Cet afflux de nouvelles données émanant de l'usine engendre de nouvelles opportunités :

1. **Renforcer la rentabilité.** L'analyse des données émanant des machines vous aide à identifier les améliorations à apporter au niveau de la production et des politiques. Par exemple, la gestion de la maintenance, des réparations et des opérations peut nécessiter beaucoup de temps et de ressources. Mettre en œuvre un système de surveillance conditionnelle reposant sur l'analyse prédictive peut vous aider à :
   - Éviter les interruptions
   - Réduire les interventions humaines
   - Mieux planifier les périodes de maintenance
   - Diagnostiquer au mieux les problèmes
2. **Identifier les gains potentiels d'efficacité.** L'analyse des données en temps réel peut vous aider à améliorer la qualité, le rendement et l'efficacité des équipements. De nombreux industriels intègrent les données de leurs progiciels de gestion intégrée (ERP) et de systèmes de gestion de la fabrication (MES). Cela permet de comparer les entrées en temps réel et les données historiques pour :
   - Améliorer les taux d'utilisation
   - Renforcer la visibilité
   - Identifier les sources de perturbation majeures en amont
   - Assurer un contrôle qualité plus tôt dans le processus de production
3. **Optimiser l'activité de l'entreprise.** Grâce à l'analytique, vous pouvez voir, comprendre et suivre les déplacements du matériel dans l'usine. Cela vous permet d'être plus efficace et d'éviter les interruptions de production. Ces informations améliorent également la gestion de la chaîne logistique, de la planification et des stocks, optimisant ainsi vos marges et l'expérience des clients.

Analytique IoT à la périphérie du réseau : Cisco et SAS

Dans le monde connecté de l'Internet des objets (IoT), plusieurs pétaoctets de données sont générés en temps réel. La capacité à collecter, à surveiller et à traiter rapidement les informations est essentielle pour une entreprise moderne.

Cisco et SAS se sont associés pour créer la plate-forme d'analytique IoT Edge-to-Enterprise IoT Analytics Platform. Elle permet aux entreprises de collecter, de traiter et d'analyser rapidement de grands volumes de données en temps réel, à la fois à la périphérie de leur réseau et dans leur data center. L'objectif de l'IoT est d'obtenir des résultats exploitables. Pour cela, il n'y a qu'une solution : il faut pouvoir analyser rapidement les données.

En savoir plus sur l'approche de Cisco et de SAS en matière d'analytique IoT.

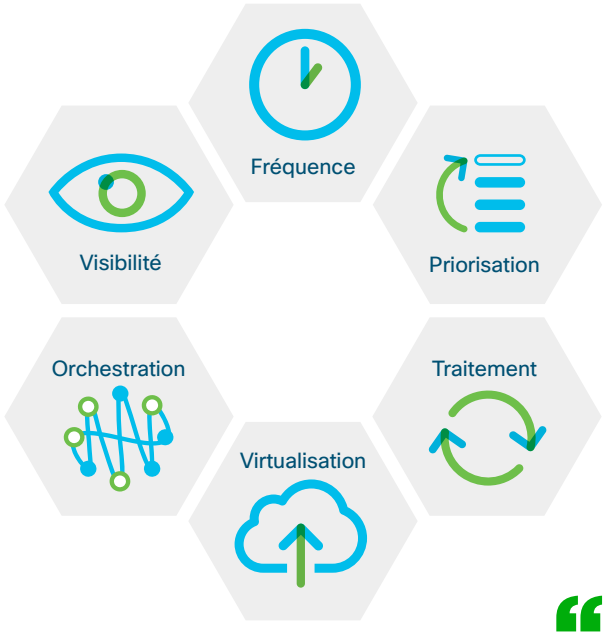
Section II. Éviter les problèmes classiques

D'ici 2020, IDC (International Data Corporation) estime que l'Internet des objets (IoT) comprendra environ 30 milliards de terminaux. Ce chiffre pourrait dépasser les 80 milliards en 2025[4]. Et d'ici 2019, 43 % des données de l'IoT seront traitées à la périphérie des réseaux[5].

Outre les nombreux bénéfices que présentent ces appareils connectés, ils ne sont pas exempts de risques potentiels. Les industriels se heurtent souvent à deux difficultés : la surcharge de données et les menaces pour la sécurité.

Éviter la surcharge de données

Tous ces nouveaux objets connectés génèrent un raz-de-marée de données. Et votre entreprise doit déterminer où placer ces données, à quelle fréquence et comment les utiliser. Vous devez évaluer vos flux de données et prendre en compte six facteurs clés.



1. **Fréquence :** les opérations industrielles génèrent souvent des flux de données de taille réduite à une fréquence élevée. **Mais ce n'est pas parce que vous pouvez extraire des données toutes les 10 millisecondes que c'est une bonne idée.** Il est important de comprendre à quelle fréquence les données sont utiles à l'entreprise pour les extraire en fonction des besoins. Cela évite les extractions de données inutiles qui sont source de surcharge, de latence ou même de pannes du réseau.

   L'analytique réseau permet également de repérer les anomalies : les problèmes ou les modifications inconnues qui ne correspondent pas à un trafic normal. Les analystes avertis font varier la densité des données dans le temps. En d'autres termes, ils conservent les données de haute densité pendant une courte période, puis ensuite les données de densité moindre. Vous pouvez ainsi conserver les données collectées toutes les 100 ms pendant deux semaines, puis en éliminer certaines et stocker les données collectées chaque seconde pendant deux mois, puis celles collectées chaque seconde pendant un an, etc.

2. **Hiérarchisation :** avec le nombre de plus en plus élevé d'appareils connectés à Internet, vous devez désigner les services prioritaires sur le réseau. Certains appareils sont plus sensibles aux retards, à la gigue et aux pertes de paquets. Il est donc important que le trafic non essentiel n'affecte pas la fiabilité du réseau. Grâce au protocole standard TSN et à l'automatisation de la qualité de service (QoS), votre entreprise peut donner priorité au trafic critique pour garantir l'intégrité du réseau. Même en cas de fort encombrement, les fonctionnalités QoS permettent de s'assurer que le trafic important parvient à destination.

3. **Traitement :** les modèles classiques envoient les données au data center principal pour qu'elles soient analysées. Cela n'est toutefois pas pratique dans de nombreux cas.

> *« Ce n'est pas parce que vous pouvez extraire des données toutes les 10 millisecondes que c'est une bonne idée. »*

Tweetez cette citation

4. http://www.cisco.com/c/en/us/solutions/industries/manufacturing/connected-factory/time-sensitive-networks.html
5. Source : IDC Dawn of the DX Economy and the New Tech Industry, nº DR2017_GS1_FG, février 2017

Section II. Éviter les problèmes classiques

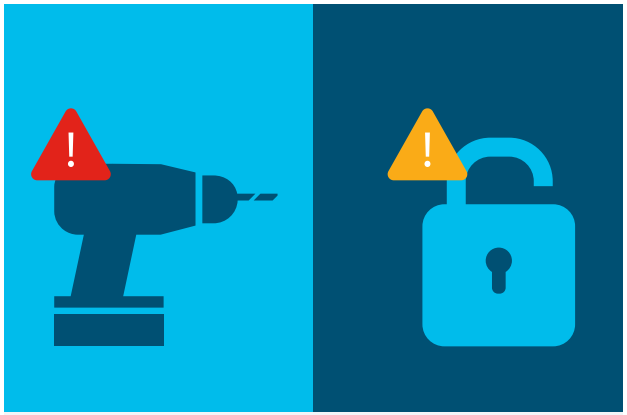
Les données de production nécessitent souvent une analyse en temps réel et des temps de réponse de l'ordre de la milliseconde. Il est notamment important de traiter les données stratégiques en temps réel. En traitant les données à la périphérie du réseau, vous réduisez la latence et garantissez que les données sont correctement envoyées à l'utilisateur. Les architectes réseau doivent envisager une solution hybride de traitement des données à la périphérie et de traitement centralisé dans le data center.

4. **Virtualisation :** de nombreux industriels dissocient le matériel des systèmes d'exploitation pour faciliter la normalisation, la gestion centralisée, la mutualisation des ressources pour les serveurs et les applications, et la reprise après sinistre. La virtualisation permet non seulement de renforcer la flexibilité de l'activité, mais elle peut également affecter la conception du data center, le stockage des données, la sécurité et les performances du réseau. La prévisibilité de la disponibilité et des performances applicatives est essentielle pour ces services.
5. **Orchestration :** avec l'afflux des données IoT, il est important de prévoir qui les reçoit et comment elles sont utilisées. Les équipes techniques peuvent retirer de nouvelles informations de la connectivité des machines, mais cela n'est utile que si ces données peuvent s'appliquer à leurs tâches quotidiennes. Elles ne doivent pas être submergées de trop nombreuses données. Vous pouvez par exemple partager certaines données avec un constructeur de machines en vue d'optimiser le fonctionnement de ses machines, sans vouloir lui indiquer combien de pièces vous produisez.

   En outre, sans une orchestration appropriée, des informations sensibles risquent d'être involontairement divulguées. Il est important de sensibiliser vos équipes et de contrôler qui reçoit les données, quand, comment et pourquoi. L'automatisation est essentielle dans la gestion et la simplification des processus d'orchestration.
6. **Visibilité :** les infrastructures réseau modernes ne sont plus des îlots d'informations isolés au niveau de l'appareil. Les outils de reporting sur tableau de bord peuvent désormais recueillir des données du réseau en temps réel, ce qui permet aux équipes OT et IT de mieux comprendre le fonctionnement du réseau pour mieux l'adapter et l'automatiser.

Réduire les risques

Les industriels souhaitent que leur activité bénéficie de la connexion de nouveaux appareils, mais sans compromettre la sécurité.



Les failles au niveau du réseau de l'usine peuvent engendrer des risques pour la sécurité physique et des interruptions majeures de l'activité, par exemple suite à un vol de propriété intellectuelle (méthodologie, code de programme).

Les failles au niveau de l'entreprise peuvent engendrer des risques en matière de confidentialité, et endommager la réputation de l'entreprise et la confiance des clients.

Protéger l'intégrité de la production est primordial, mais connecter des appareils qui ne l'étaient pas auparavant présente le risque d'introduire de nouvelles failles de sécurité.

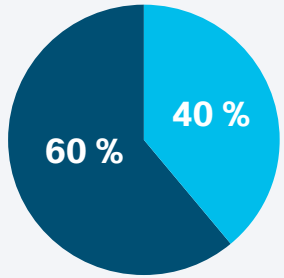
La compatibilité des solutions de sécurité doit être intégralement testée afin de garantir l'efficacité des systèmes et de leur protection.

En général, les anciens appareils de l'usine n'ont pas été conçus dans un esprit de sécurité et ne sont pas en mesure de se protéger. Quant aux nouveaux appareils, ils présentent également un certain nombre de risques. En effet, même si de nombreux fournisseurs ont considérablement progressé en matière de sécurité, beaucoup ont encore du retard. Ils doivent souvent mettre à niveau leurs appareils qui sont déjà déployés. Les vulnérabilités qui en résultent sont autant d'opportunités pour les cybercriminels d'exploiter ces appareils pour accéder au réseau.

Le manque de visibilité peut également entraîner des risques pour la sécurité. Dans de nombreux cas, des appareils sont ajoutés au réseau sans vision globale : sans coordination entre les départements OT/IT, ou sans que les départements informatiques en soient même informés. Ce n'est plus acceptable. Aujourd'hui plus que jamais il est important que la visibilité soit totale. Vous devez être en mesure de détecter, d'intégrer et de segmenter automatiquement le trafic des appareils pour assurer la sécurité de votre environnement.

Les réseaux modernes doivent se comporter comme des systèmes de sécurité. Ils doivent apporter les informations contextuelles nécessaires, et identifier les modèles de trafic et les flux de données. Grâce à la collecte et à l'analyse des données, vous pouvez établir le trafic de référence d'un réseau. Vous pouvez ensuite configurer des alertes pour vous avertir en cas d'anomalies.

Selon le rapport semestriel 2017 de Cisco sur la cybersécurité, 40 % des professionnels de la sécurité industrielle ne disposent pas d'une stratégie de sécurité formelle[6].

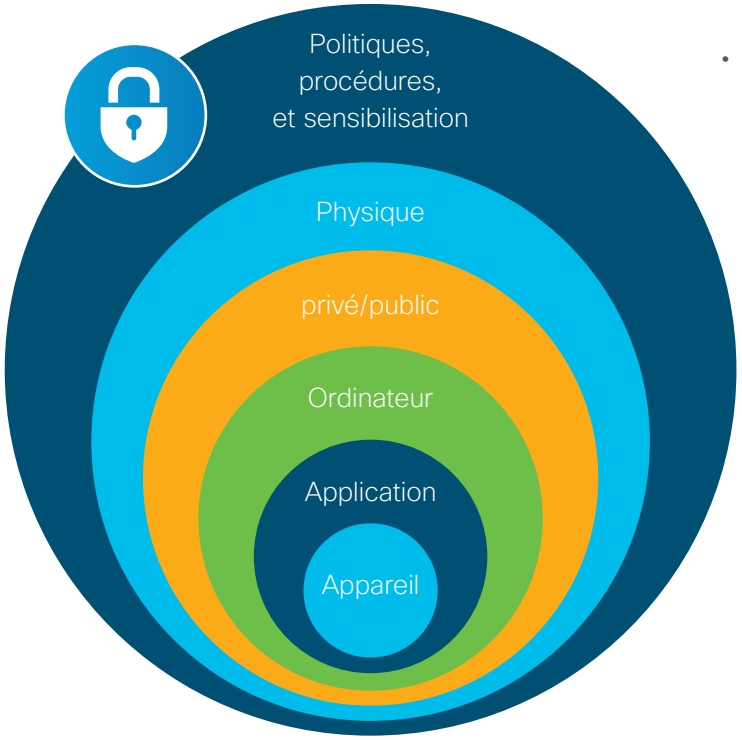


6. http://www.cisco.com/c/dam/m/digital/elq-cmcglobal/witb/1456403/Cisco_2017_Midyear_Cybersecurity_Report.pdf?elqTrackId=f6ccd8439e9945639096a9846044695a&elqaid=5897&elqat=2

3 façons de protéger vos données

Comment réduire les risques en matière de sécurité ? Mettez en place des bonnes pratiques, des nouvelles technologies et des stratégies fiables.

1. **Protection en profondeur :** se protéger contre les menaces avancées d'aujourd'hui demande une stratégie de sécurité holistique. C'est pourquoi les industriels se tournent vers une approche en profondeur. Les stratégies de défense qui agissent « en profondeur » comprennent des couches de contrôle de sécurité indépendantes (physique, procédurale et électronique).



2. **Bonnes pratiques fiables :** dans le contexte moderne de l'IoT, certaines bonnes pratiques classiques sont toujours valables. Par exemple :
   - La segmentation des appareils demeure une première étape importante
   - Il reste important d'établir des politiques spécifiques pour définir l'accès des appareils
   - L'utilisation de pare-feu performants est essentielle

3. **Nouvelles technologies :** parallèlement, de nouvelles technologies jouent également un rôle important :
   - Analytique et visibilité réseau : de nouvelles solutions permettent d'établir une surveillance et des rapports constants.
   - Contrôle d'accès : vous pouvez aujourd'hui définir des autorisations au niveau des appareils et des utilisateurs, avec un profil qui enregistre leurs entrées et sorties dans l'entreprise ainsi que leurs droits d'accès.
   - Threat Intelligence : les cybercriminels développent de nouvelles techniques d'attaque à un rythme croissant et la production industrielle devient une de leurs cibles privilégiées. Les flux d'informations tiers facilitent la mise en corrélation et la détection des incidents avant la propagation des problèmes.

Quelle est l'efficacité de votre stratégie de défense « en profondeur » ?

Une stratégie de défense en profondeur efficace couvre la sécurité procédurale, physique et électronique.

Vous voulez en savoir plus ? Pour commencer, vous devez évaluer votre situation actuelle.

Lancez-vous.

Et ensuite ?

Le secteur industriel se modernise à un rythme plus soutenu que jamais. Les entreprises éliminent les silos et connectent des objets précédemment non connectés.

Vous aurez donc bientôt accès à des volumes de données plus importants que jamais, qui vous aideront à renforcer la productivité, à réduire les interruptions et à optimiser l'efficacité de vos équipements.

Pour gagner en efficacité et développer votre activité, vous devez vous appuyer sur une architecture réseau robuste. Cela passe par une approche radicalement moderne de l'architecture réseau, de la connectivité, de la visibilité et de la sécurité, tout en rapprochant les technologies de l'information (IT) et les technologies opérationnelles (OT).

Cisco est à vos côtés pour vous aider à exploiter pleinement la connectivité tout en évitant les problèmes associés.

Prêt pour la prochaine étape ? Découvrez :

- Cisco Kinetic
- Cisco DNA pour les industriels
- L'usine intelligente avec Cisco
- Cisco IoT Threat Defense

Siège social aux États-Unis
Cisco Systems, Inc.
San José. CA

Siège social en Asie-Pacifique
Cisco Systems (États-Unis) Pte. Ltd.
Singapour

Siège social en Europe
Cisco Systems International BV Amsterdam.
Pays-Bas

Cisco compte plus de 200 agences à travers le monde. Les adresses, numéros de téléphone et de fax sont répertoriés sur le site web de Cisco, à l'adresse : **www.cisco.com/go/offices**.