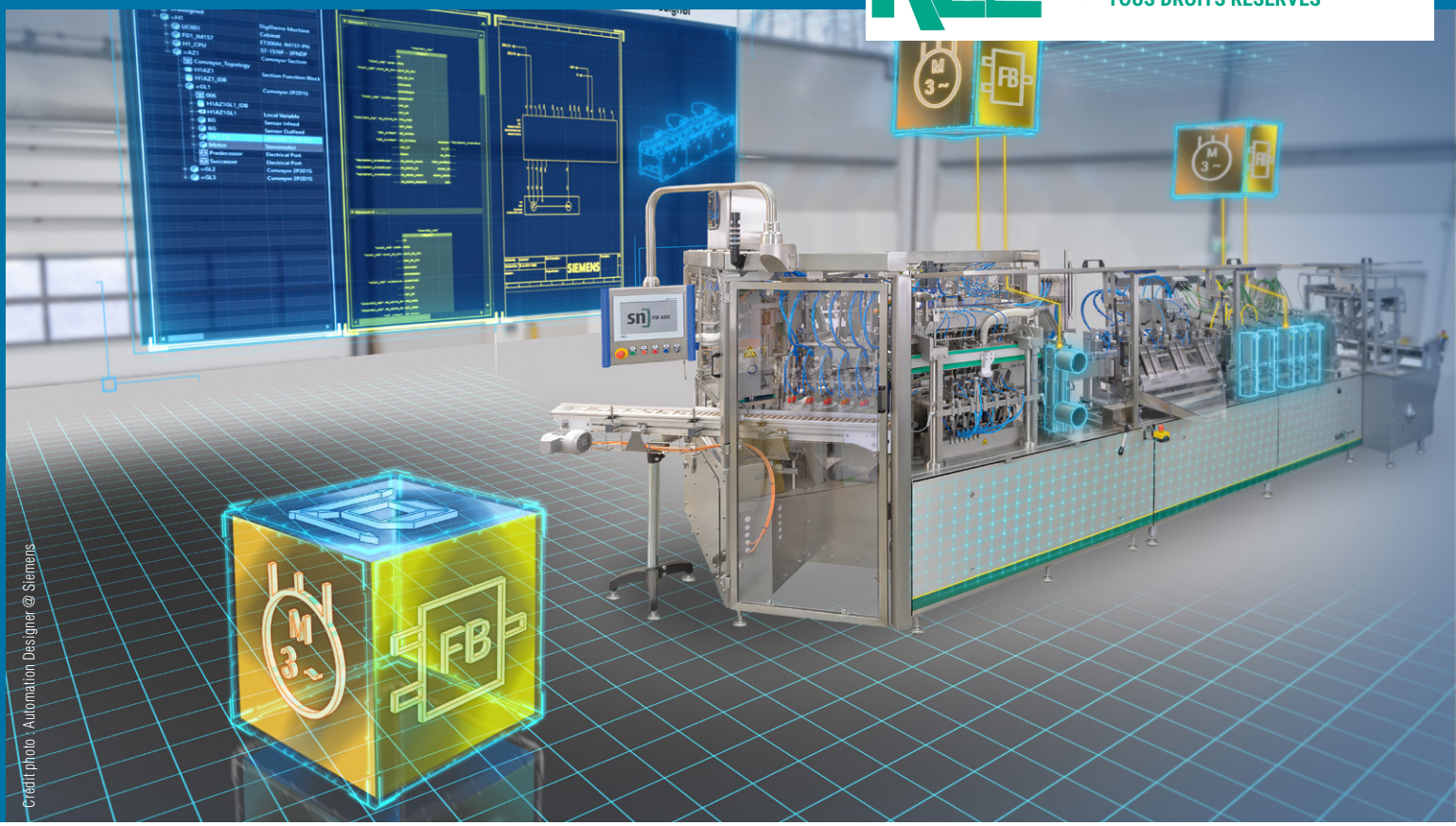
REE REVUE DE L'ÉLECTRICITÉ ET DE L'ÉLECTRONIQUE



Crédit photo : Automation Designer @ Siemens

Tour d'horizon sur Industrie 4.0

Introduction

Industrie 4.0 est une initiative née en Allemagne en 2011 visant à redynamiser l'industrie européenne face à la concurrence asiatique en utilisant les technologies du numérique. Le concept met en œuvre diverses technologies dont la REE a rendu compte à plusieurs reprises. Une approche plus globale est proposée dans ce dossier mais, avant de laisser le lecteur l'aborder, nous proposons un tour d'horizon du concept Industrie 4.0 qui aidera à mieux en comprendre les fondements.

Jean-Pierre Hauet
Président de l'ISA-France

La démarche Industrie 4.0

Le concept Industrie 4.0 a été présenté en 2011 à la Foire de Hanovre en Allemagne. La préoccupation essentielle était de redonner à l'industrie allemande un nouvel élan lui permettant de faire face à la concurrence croissance des industries asiatiques, japonaises et chinoises. Ce concept a fait des émules et a été repris dans de nombreux pays et notamment en France dans le cadre du projet « Industrie du futur » lancé par le président de la République en avril 2015, projet s'appuyant lui-même sur les travaux de l'initiative « 34 plans Nouvelle France industrielle » lancée dès 2013.

« Industrie 4.0 » comme « Industrie du futur » sont présentés comme une révolution : la 4e révolution industrielle qui fait suite à celles de la mécanisation, de l'électrification et de l'automatisation (figure 1).

L'idée de base d'Industrie 4.0 est de faire bénéficier l'industrie des progrès considérables réalisés dans le domaine des technologies de l'information et de la communication. Il faut dire que, jusqu'au début des années 2000, le monde industriel (les OT : *Operational Technologies*) vivait relativement à l'écart des IT (*Information Technologies*) qui avaient par contre conquis les mondes de la gestion, des services et du commerce. Les processus industriels étaient alors fonctionnelle-

ment et physiquement structurés selon le modèle hiérarchique dit de Purdue en niveaux successifs allant du procédé à la gestion de l'entreprise (figure 2).

La 3e révolution industrielle, amorcée à partir de 1969 – date d'apparition du premier automate industriel développé par l'équipe de Richard E. Morley (Modicon) – couvrait typiquement les niveaux 0 à 3. La structure physique des systèmes de contrôle industriel était alors calquée sur leur structure fonctionnelle et ces systèmes étaient construits autour de réseaux de communication correspondant à chacun des niveaux et ayant chacun leurs spécificités propres (figure 3) :

- réseaux de terrain ;
- réseaux de contrôle ;
- réseaux de supervision ;
- réseaux d'entreprise.

Industrie 4.0 a apporté à cette structure plusieurs évolutions majeures :

- une intégration beaucoup plus profonde du monde OT avec le monde IT ;

- la prise en compte des percées technologiques réalisées au niveau des capteurs, permettant de faire remonter vers les niveaux supérieurs des informations plus nombreuses et plus variées ;

- l'introduction dans le cœur même des processus de nouvelles technologies numériques : intelligence artificielle, réalité augmentée, jumeaux numériques, fabrication additive, robotique autonome et collaborative, etc. ;

- plus récemment, l'introduction de l'informatique (*cloud computing*) permettant d'accéder à des capacités de traitement et de stockage mutualisées à partir de n'importe quel poste client au travers de l'Internet.

Il est apparu alors possible de reconcevoir l'usine du futur comme un ensemble d'îlots fonctionnels autonomes, dotés de capacités de traitement de l'information

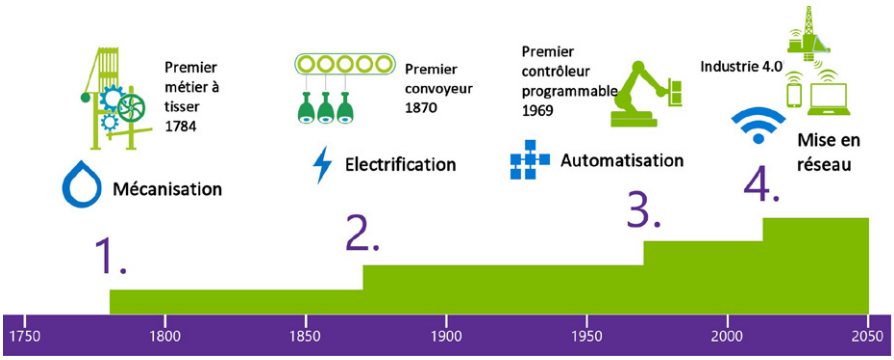


Figure 1 : Les quatre grandes révolutions industrielles.

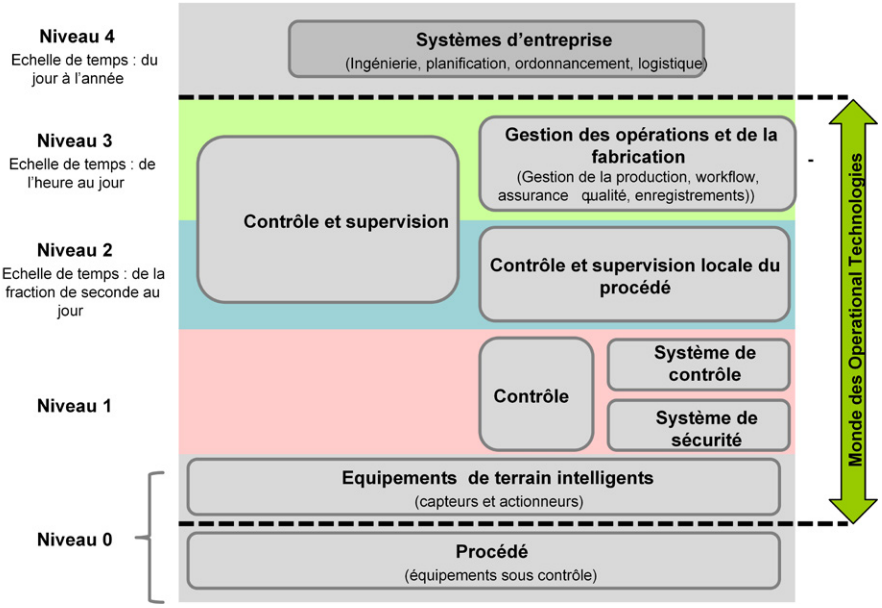


Figure 2 : La segmentation de l'entreprise en niveaux fonctionnels selon le modèle de Purdue.

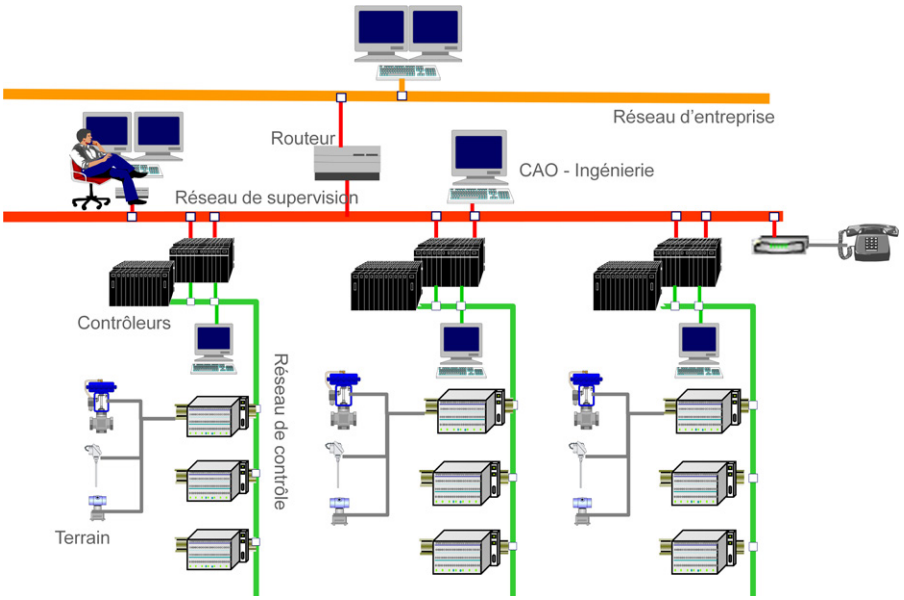


Figure 3 : Schématique d'un système de contrôle commande conventionnel.

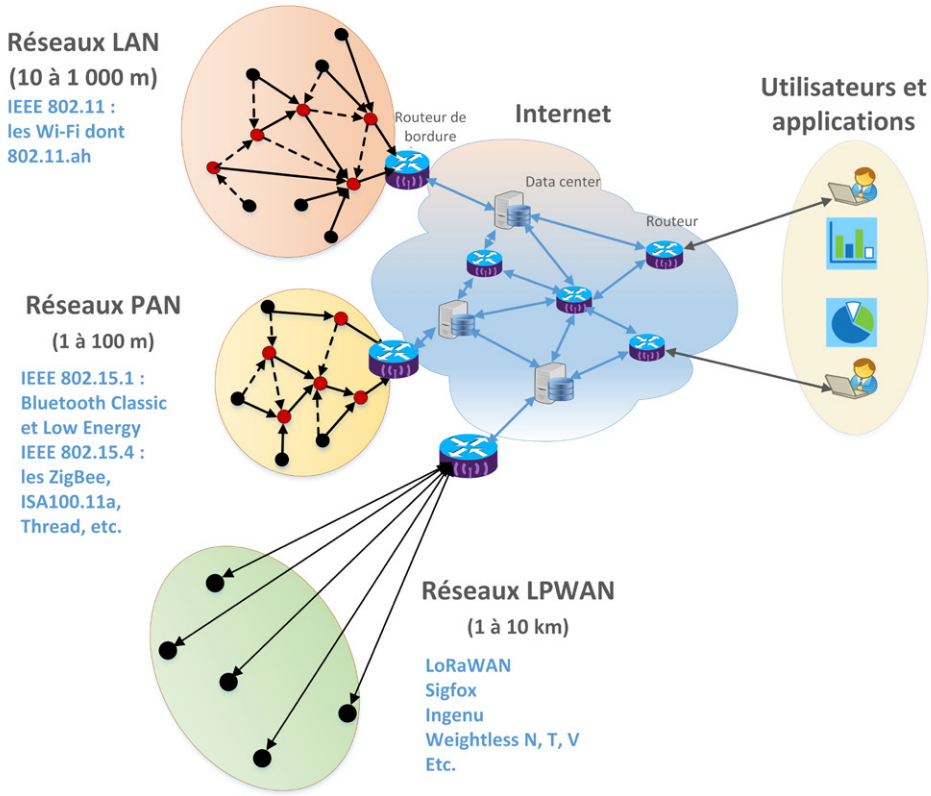


Figure 4 : Schématique d'une connectivité entre réseaux locaux construite autour d'Internet.

propres à leur vocation (qui peut être la conception, la fabrication ou la maintenance), capables d'échanger de l'information entre eux et avec les fonctions de supervision, de planification et d'optimisation, aptes à être surveillés en permanence afin de détecter de façon précoce des déviations ou des alarmes éventuelles.

Par cette approche décentralisée mais intégrée, on peut atteindre une meilleure productivité grâce à une automatisation plus poussée, à un meilleur enchaînement des tâches et à des stratégies de maintenance améliorant la disponibilité. On y voit également la possibilité de surveiller de plus près les émissions pouvant porter atteinte à l'environnement et d'assurer un niveau de sécurité plus élevé pour le personnel.

L'approche modulaire et le recours accru aux technologies numériques permet de donner davantage de flexibilité et de polyvalence aux chaînes de production ainsi que plus de souplesse pour accompagner la croissance souhaitée de l'activité.

La connectivité au cœur du débat

La communication entre les entités constitutives de l'usine du futur est à l'évidence essentielle. L'une des hypothèses sous-jacente à Industrie 4.0 est que les communications sans fil continueront à se développer en offrant des performances et des niveaux de coût permettant d'assurer la plupart des communications entre équipements et, au travers de routeurs ou de passerelles, vers l'Internet.

L'usine deviendra alors un ensemble d'ateliers desservis par des réseaux locaux et fédérés par l'Internet (figure 4).

Il est vrai que l'offre en réseaux locaux s'est considérablement enrichie au cours des dernières années. On a vu arriver les réseaux à très courtes distances (Bluetooth, Zigbee, WirelessHart, ISA100…), les réseaux à courte et moyenne portées (la grande famille des Wi-Fi) et plus récemment les réseaux locaux à longues distances (LoRaWAN et Sigfox notamment). Le lecteur se reportera sur ces questions au numéro spécial de la REE consacré en 2018 à l'Internet des objets.

Ces solutions n'ont cependant pas pénétré autant qu'on l'espérait le monde industriel, peut-être par excès de prudence et de conservatisme de la part de l'industrie mais aussi parce qu'il est difficile de trouver une solution répondant aux exigences que l'on peut avoir aux différents niveaux des procédés : exigences de compétitivité, de disponibilité, de débit, de distance, de latence, de déterminisme, de cybersécurité, de résistance au brouillage, de consommation d'énergie, d'extensibilité… Aujourd'hui deux solutions semblent prendre le dessus : Bluetooth Low Energy (BLE) pour les petits réseaux maître-esclaves très courtes distances et le Wi-Fi 802.11ax (alias Wi-Fi 6) qui est susceptible de répondre à beaucoup des exigences listées précédemment en s'installant dans la bande des 6 GHz, nouvelle bande libre créée au niveau international et qui sera très prochainement ouverte en France dans la bande 5 945 à 6 425 MHz.

Cependant, ces solutions locales entrent maintenant en compétition avec la 5G et plus spécifiquement avec l'édition 16 du 3GPP (juillet 2020) conçue pour répondre aux besoins industriels. L'article de **Suzanne Debaille et Denis Manteau** sur les nouvelles technologies pour réseaux industriels apporte au lecteur beaucoup d'informations sur les progrès que va apporter la 5G à différents niveaux. Par rapport aux solutions fondées sur les réseaux locaux, un avantage essentiel est son universalité. Elle intègre en effet les profils de communication IoT déjà présents dans la 4G : eMTC (ou LTE-M) pour les communications *machine to machine* jusqu'à 1 Mbit/s et NB-IoT pour les communications locales à faible débit (quelques dizaines de kbit/s) mais longues distances. La 5G offre également la possibilité de construire des réseaux privés, en Allemagne par allocation de fréquences dédiées, en France par un service de *network slicing* par

lequel les opérateurs émulent par voie logicielle un réseau privé. On annonce également pour la 5G des temps de latence de l'ordre de la milliseconde, correspondant aux exigences requises par les procédés industriels temps critique et par le véhicule autonome et connecté. Et bien sûr, elle permettra d'associer le local au global, sans solution de continuité.

Il est encore trop tôt pour juger de l'accueil qui sera réservé à cette technologie que l'on présente volontiers comme une technologie de rupture. Toutes les fonctionnalités ne sont pas encore disponibles, notamment celles dépendant de la mise en service de la nouvelle radio 5G dans la bande des ondes millimétriques à 26 GHz. Mais un indice intéressant est de voir qu'en 2021, les solutions 4G/5G de l'IoT commencent à prendre le pas sur les solutions LPWAN de l'IoT (LoRaWAN et Sigfox) (figure 5). Quant à la compétition entre la 5G et le Wi-Fi, on peut penser que des solutions vont s'imposer permettant, sur le plan local, de tirer parti des complémentarités entre la 5G et le Wi-Fi 6. D'ores et déjà plusieurs solutions sont proposées en ce sens.

"Toutes les fonctionnalités ne sont pas encore disponibles, notamment celles dépendant de la mise en service de la nouvelle radio 5G dans la bande des ondes millimétriques à 26 GHz."

Il est probable que les industriels vont réaliser progressivement l'intérêt de la 5G qui permet de faire circuler l'information depuis le robot ou la machine jusqu'au plus haut niveau de la pyramide de gestion de l'entreprise et de la rendre accessible partout dans le monde et à tout moment. N'oublions pas non plus l'intérêt que le déploiement des ondes millimétriques va présenter pour la localisation précise des véhicules, de chariots ou des robots.

Toutefois, les équipements sans fil conservent un handicap qui est leur alimentation en énergie, souvent par piles ou par batteries qui, malgré le soin apporté à limiter les consommations, notamment en limitant le débit de données et en recourant à des protocoles très frugaux tels que LoRaWAN ou Sigfox, finissent par se décharger. Les batteries continuent à progresser et diverses solutions de piégeage de l'énergie dans le milieu ambiant (*energy harvesting*) sont disponibles. Mais les solutions filaires conservent un certain avantage et deux initiatives sont à suivre attentivement :

- les normes SPE (*Single-pair Ethernet*) qui intéressent l'automobile mais aussi l'industrie : la norme IEEE 802.3bp offre par exemple un débit de 1 Gbit/s sur 40 mètres avec une paire de cuivre assurant la communication et l'alimentation en énergie des transmetteurs ;

- les normes TSN (*Time Sensitive Networking*), développées par le comité IEEE 802.1 et non plus IEEE 802.3, qui permettent de distribuer des trames Ethernet en respectant une synchronisation temporelle et faire, par ●●●

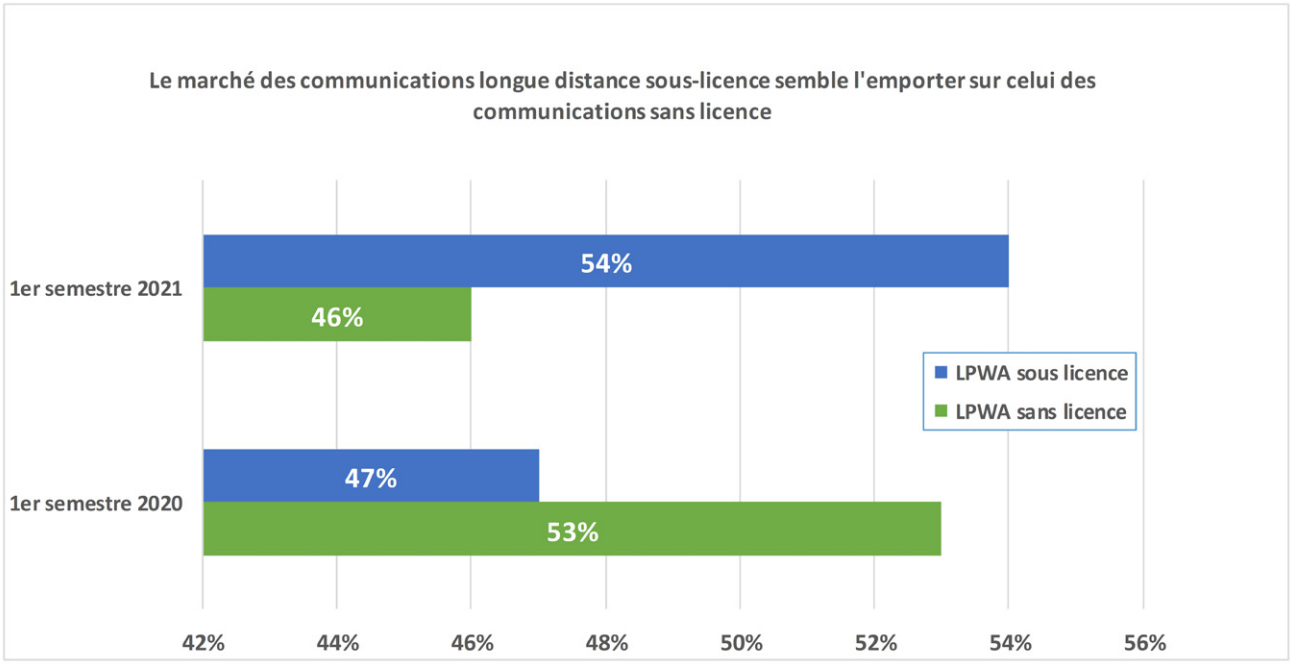


Figure 5 : Répartition du marché des communications longues distances (LPWAN) aux premiers semestres des années 2020 et 2021 – Source : IoT Analytics.

" Pour beaucoup d'utilisateurs potentiels, le problème de la connectivité et de l'interopérabilité des équipements se résume à des questions de réseaux de communication. "

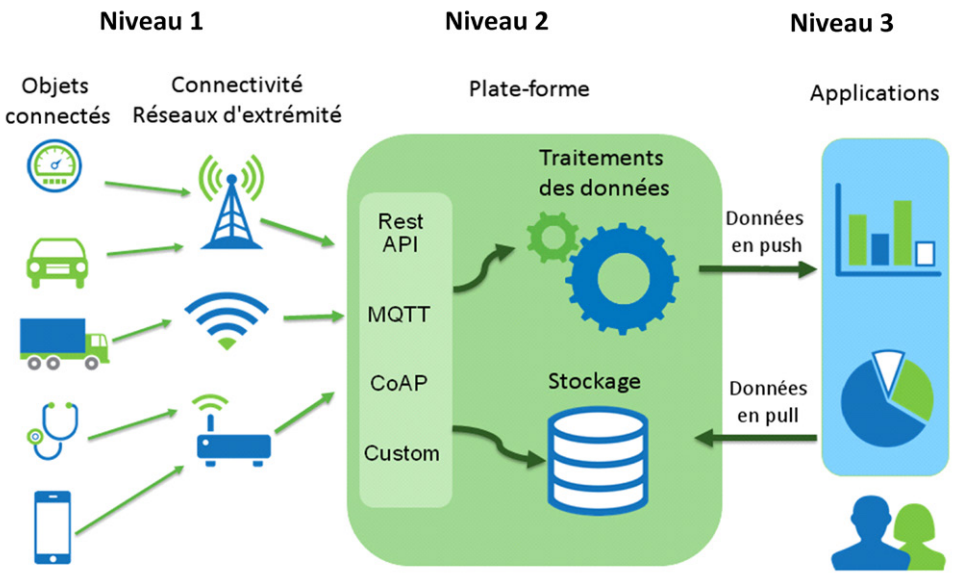
exemple, coexister des données à temps critique avec des applications vidéo sur un même câble Ethernet. Ces normes TSN peuvent être intégrées à des protocoles de niveau supérieur tels que Profinet ou OPC-UA.

Les nouveaux protocoles

Pour beaucoup d'utilisateurs potentiels, le problème de la connectivité et de l'interopérabilité des équipements se résume à des questions de réseaux de communication. Mais ces réseaux sont destinés à supporter des protocoles et ces protocoles doivent être sûrs, fiables et efficaces et adaptés au monde industriel.

Les Allemands ont opté dans le cadre d'Industrie 4.0 pour le protocole OPC-UA conçu pour permettre l'interopérabilité entre équipements d'origines diverses. OPC-UA fonctionne sur le modèle client-serveur tout en assurant l'identification des agents connectés, l'intégrité et la confidentialité des échanges. Ce protocole est de plus en plus reconnu, dans l'industrie pharmaceutique, dans l'*oil and gas*, dans la robotique et dans le *building automation*. Toutefois le protocole, ou plutôt la suite de protocoles OPC-UA, est complexe et peut poser des problèmes de compatibilité avec la dynamique des procédés.

Dans le même temps, émerge le protocole MQTT (*Message Queuing Telemetry Transport*) qui assure de façon efficace la remontée des données vers un équipement servant de courtier d'informations (un *broker*) qui les met à la disposition des utilisateurs s'abonnant aux services qui les intéressent. Utilisé par les grands acteurs du *cloud*, fondé sur le modèle *publish/subscribe*, il permet d'éviter l'interrogation inutile des données à évolution lente et réduit ainsi considérablement les débits à faire transiter.



I Figure 6 : Architecture infonuagique à trois niveaux.

Cloud computing et *Edge computing*

Les industriels ont également mis du temps à découvrir les apports de l'infonuagique (*cloud computing*), du partage de ressources qu'elle permet et des fonctionnalités qu'elle rend accessible à moindre coût. La virtualisation et le renvoi dans le *cloud* de fonctionnalités jusqu'à présent supportées par des équipements propriétaires et dédiés, attire de plus en plus d'utilisateurs et sera à coup sûr une autre grande conquête d'Industrie 4.0.

De nombreuses grandes sociétés proposent des plates-formes dans le *cloud* qui trient, stockent et traitent les données par des applications (appelées *analytics*) qu'elles mettent à la disposition de leurs clients : Azure de Microsoft, AWS d'Amazon, Google Cloud de Google, Watson d'IBM, Mindsphere de Siemens, Predix de GE, etc.

Toutes ces plates-formes ont grosso modo la même architecture et conduisent à regrouper la collecte et le traitement des données en trois tiers (figure 6).

Il demeure que le *cloud* n'a pas vocation à accueillir toutes les données que l'industrie manipule quotidiennement et qui n'ont, en règle générale, qu'un intérêt épisodique. En outre, la dynamique d'accès, de transfert et de traitement dans le *cloud* peut être incompatible avec les exigences de la dynamique du procédé. Enfin, certains opérateurs peuvent rechigner à envoyer dans le *cloud* des données qu'ils considèrent comme sensibles.

C'est pourquoi sont proposées des architectures hybrides dans lesquelles une partie des services que peut héberger le *cloud* est supportée par des équipements qui restent au plus près du procédé. C'est ce qu'on appelle l'*edge computing* ou informatique de bordure ou de périphérie. Dans cette approche, on peut, par exemple, faire supporter par

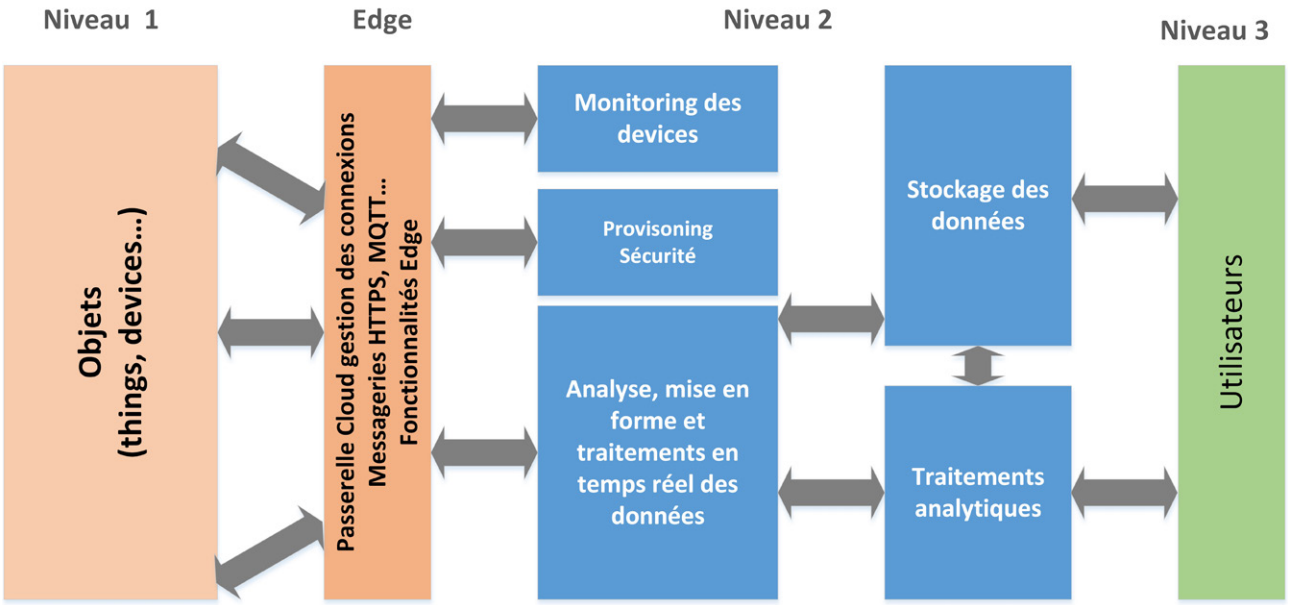


Figure 7 : Insertion des fonctionnalités Edge dans l'architecture *Cloud*.

les routeurs de bordure qui apparaissent dans la figure 4 des traitements qui pourraient être transférés dans le *cloud* mais que l'on préfère conserver en local.

L'*edge computing* s'apparente à un *cloud* privé et cette répartition des traitements, répondant à un principe de subsidiarité, a conduit Cisco à proposer l'appellation de *fog computing*.

La figure 7 montre comment cet échelon intermédiaire vient fonctionnellement s'imbriquer entre le niveau 1 et le niveau 2 des architectures *cloud* telles que décrites en figure 6.

La cybersécurité

Aucune industrie n'est aujourd'hui à l'abri de cyber-attaques. Mais l'usine Industrie 4.0 du fait de l'importance qu'y revêt le numérique constitue une cible privilégiée. La surface d'attaque se trouve renforcée par le nombre d'équipements connectés, leur dispersion géographique, leurs origines diverses, le fait qu'ils peuvent être laissés sans surveillance. La diversité technologique est nécessairement génératrice d'un nombre de vulnérabilités accru et la multiplicité des réseaux, généralement sur protocole IP, facilite la propagation des logiciels malveillants qui pourraient être introduits dans le système. Il convient donc d'être particulièrement vigilant, dès la conception du système, notamment en segmentant le système en zones de sécurité qui assurent une défense en profondeur.

L'ensemble de normes ISA/IEC 62443 définit un cadre précis à respecter pour construire un programme de sécurité et le mettre en œuvre. L'article de **Vincent Nicaise** (Stormshield) expose très clairement la démarche à suivre dans le cadre de ce référentiel.

Une attention particulière est à porter aux équipements d'extrémité souvent laissés sans surveillance : quelle est leur origine ? Comment s'est-on assuré que l'on pouvait les admettre sans risque dans le système ? Comment sont-ils protégés ? Sont-ils *secure by design* ? C'est-à-dire possèdent-t-ils par construction les attributs qui permettent de les connecter sans risque dans un réseau de confiance ? A quelles données ont-ils accès ?

Les équipements de bordure, les *edge devices*, qui assurent la liaison avec le *cloud* et peuvent supporter des fonctionnalités *edge*, sont bien évidemment des équipements clés qui devront faire l'objet d'une protection renforcée.

Le *cloud* et les communications avec le système devront faire l'objet d'une analyse particulière avant de décider quelles données peuvent être hébergées dans le *cloud*.

Enfin, il est clair que la prévention et la détection précoce des intrusions va devenir le maître-mot : mieux vaut prévenir que guérir et on voit se de développer divers systèmes de détection d'intrusions fondés sur des sondes analysant le trafic à des endroits judicieusement choisis et le comparant à un modèle standard construit au démarrage de l'usine et éventuellement enrichi par apprentissage. D'autres systèmes, plus simples de mise en œuvre, arrivent sur le marché sous forme de clés USB permettant de scanner les équipements et de détecter les logiciels malveillants sans impacter les performances du système.

Technologies et exemples applicatifs

Les technologies applicatives qu'Industrie 4.0 est susceptible de supporter sont très variées et s'enrichissent régulièrement. ●●●

Da façon non exhaustive, on peut citer :

- l'intelligence artificielle, pour l'interprétation des données, la reconnaissance de formes, la détection de signaux, etc.
- le traitement des données massives (*big data*) pour l'analyse statistique de séries volumineuses de données collectées dans le *cloud*, la détection des signaux faibles et leur interprétation ;
- la localisation et le *geofencing* pour la gestion de flottes, la logistique, les magasins automatisés, la robotique mobile, etc.
- la robotique intelligente ;
- la modélisation, la simulation, les maquettes et les jumeaux numériques ;
- la réalité augmentée ;
- la fabrication additive ;
- les outils intelligents ;
- etc.

Chacune de ces technologies nécessiterait un article. Dans le présent dossier, nous avons préféré nous concentrer sur quelques cas d'applications qui sont particulièrement illustratifs de l'intérêt que présente l'approche Industrie 4.0, aussi bien pour les grandes entreprises que pour les petites.

Hacene Lahreche, Cedric Gallais et **Franck Doute** nous exposent le programme Usine du futur de la SNCF, ses principes, ses outils et ses applications au matériel roulant, aux entrepôts et à la gestion des actifs. Il montre l'intérêt de l'approche par jumeau numérique et réalité augmentée dans les processus de conception, de production et de maintenance en ouvrant la voie au traitement des problèmes de connectivité par la 5G et le Wi-Fi 6.

Thierry de Vanssay, consultant indépendant, montre comment les technologies 4.0 ont permis à une PME française du domaine de la chaussure (Chamatex) de relocaliser la fabrication de chaussures de sport en France en créant une nouvelle usine ASF 4.0, dans une approche qui pourrait être étendue à l'ensemble du secteur.

Florence Verzelen expose la démarche de Dassault Systèmes dans le domaine des jumeaux numériques et montre comment les outils développés par Dassault Systèmes permettent d'accélérer les processus d'innovation et de conception de nouveaux produits dans divers domaines : automobile, aviation, construction, santé, équipements industriels…

Vincent Nicaise détaille la démarche à suivre dans le cadre du référentiel ISA/IEC 62443 pour construire un programme de sécurité et le mettre en œuvre. Il expose les spécificités techniques et organisationnelles de la cybersécurité appliquée aux systèmes industriels. Il définit une approche de défense en profondeur où chaque fonction de sécurité est un rempart nécessaire au blocage ou au ralentissement d'une cyber-attaque.

Matthieu Peterschmitt (Eco-Adapt) aborde la question de la maintenance prédictive et des performances énergétiques des machines tournantes et montre à quelles conditions les méthodes d'analyse à haute fréquence des signaux électriques envoyés par les machines permettent de faire un diagnostic pertinent.

Suzanne Debaille et **Denis Manteau** exposent les progrès que va apporter la 5G à différents niveaux pour réseaux industriels. Les évolutions informatiques du *cloud* et les nouvelles fonctionnalités de la 5G permettent de disposer en milieu industriel de solutions de traitement économique pour de gros volumes de données et des applications adaptées à la mobilité. Ces solutions imposent une réflexion sur l'évolution de la connectivité des usines. ■

L'auteur

Jean-Pierre Hauet est président de l'association ISA-France, section française de l'ISA, International Society of Automation. L'ISA compte plus de 30 000 membres dans le monde. Sa mission est de promouvoir les techniques et de faire progresser les compétences de ses membres dans les secteurs de l'instrumentation, des systèmes et de l'automation.

Au cours de sa carrière, Jean-Pierre Hauet a été notamment président directeur général des Laboratoires de Marcoussis du groupe Alcatel Alstom. Il a été directeur de la branche Produits et Techniques de Cégélec et Chief Technology Officer du groupe Alstom.

Les articles