

ÉVOLUTIONS TECHNOLOGIQUES

FICHE VARIABLE

INTERNET DES OBJETS

COLLÈGE DE PROSPECTIVE
CHANTIER INDUSTRIE



SYSTÈME DE VARIABLES

Cette fiche s'inscrit dans un système global de variables.

Les variables faisant l'objet d'une fiche sont celles identifiées lors des premières tables rondes du chantier prospectif comme porteuses d'évolutions majeures ayant un impact direct ou indirect sur l'industrie.

Chaque fiche rassemble, sauf exception, la documentation permettant de comprendre l'évolution passée, présente et future d'une variable.

Elle expose les dynamiques d'évolution (tendances, ruptures...), et propose quelques évolutions possibles (micro-scénarios travaillés en atelier).

1. CONTEXTE ÉCONOMIQUE GLOBAL

Croissance économique mondiale
Monnaie
Europe, Brexit
Production française
Export
Coûts de production
Intervention de l'Etat
Internationalisation
Ressources (énergie, matières...)

2. ÉVOLUTIONS ÉCONOMIQUES DE L'INDUSTRIE

Servicialisation de l'industrie
Modèles d'affaires
Logistique et Supply Chain

3. ÉVOLUTIONS RÉGLEMENTAIRES

Sécurité industrielle
Règlementations
Changements climatiques

4. ATTRACTIVITÉ RÉGIONALE

Capital humain
Attractivité régionale
Infrastructures
Environnement institutionnel,
économique, gouvernance
locale
Recherche et développement

5. ÉVOLUTIONS TECHNOLOGIQUES

Big Data
Intelligence Artificielle
Réalité augmentée
Cobotique
Fabrication additive
Internet des objets
Gestion de cycle de vie du
produit

6. ÉVOLUTIONS SOCIÉTALES

Imaginaire de l'industrie

Tendances de consommation

TRAJECTOIRE DE LA VARIABLE

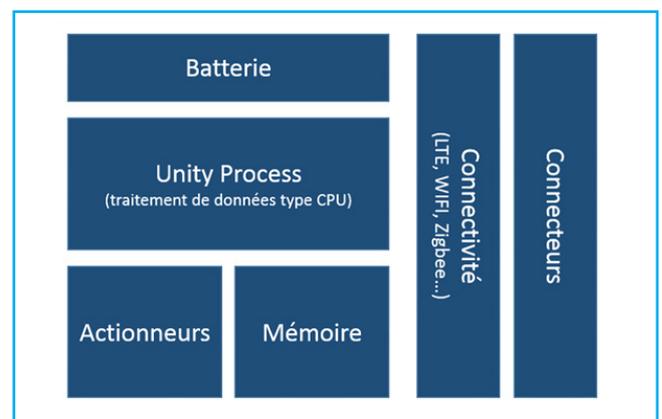
Les trois premières révolutions industrielles ont donné lieu à trois étapes cruciales dans le développement de l'industrie : la mécanisation, l'électricité et l'informatique. L'introduction de l'Internet des objets (dit IoT) et des services dans l'environnement manufacturier inaugure une quatrième révolution industrielle qui permet une ingénierie de bout en bout dans l'ensemble de la chaîne de valeur, **répondant aux exigences de massification des produits singuliers et personnalisés, mais surtout, des marges de création de valeur ajoutée indépendamment des coûts salariaux.** Les possibilités offertes par l'Iot atteignent également le vieillissement de la population active (en améliorant les conditions de travail) et peut proposer une réponse à la pénurie de compétences hautement qualifiées (ce à quoi peut répondre en partie la cobotique ou l'intelligence artificielle). Mais la création de valeur se situe surtout dans les possibilités d'optimiser les moyens et les ressources : polyvalence des équipements de production en cas de panne, flexibilité du processus de production, anticipation des approvisionnements par une meilleure gestion des ressources, gestion de l'énergie des bâtiments et des processus de fabrication...

L'Union Internationale des Télécommunications (UIT) définit en 2012 l'Internet des objets (ou Internet of things -IoT-) comme une « **infrastructure mondiale pour la société de l'information, qui permet de disposer de services évolués en interconnectant des objets (physiques ou virtuels) grâce aux technologies de l'information et de la communication interopérables existantes ou en évolution** ». Cette dualité entre objets physiques et virtuels est importante : les objets physiques ont une représentation virtuelle connectée à Internet ; ces objets ont une certaine intelligence leur permettant de communiquer avec le réseau, ou avec les autres objets, d'où l'enjeu de leur interopérabilité au cœur de l'Iot. Les objets, dans le monde de l'IoT, sont caractérisés par leur capacité à se connecter (inter connectivité), pouvant utiliser différents réseaux ou protocoles (hétérogénéité), et évoluent avec leur environnement complexe (dynamique).

Selon la Société de l'électricité, de l'électronique et des technologies de l'information et de la communication (SEE) l'IoT est définie comme « un réseau de réseaux qui permet, grâce à des dispositifs d'identification électronique d'entités physiques ou virtuelles dites « objets connectés » et via des systèmes de communication appropriés, sans fil notamment, de communiquer directement et sans ambiguïté, y compris au travers de l'Internet, avec ces objets connectés et ainsi de pouvoir récupérer, stocker, transférer et traiter sans discontinuité les données s'y rattachant ».

Un objet connecté à Internet est composé de **transducteurs** (capteurs des informations d'environnement et les transformant en information numérique et les actionneurs), de **données**, d'un système de transmission, d'une infrastructure d'interconnexion, d'une application et une interface utilisateur ou Homme-Machine (IHM).

Figure 1 : Les composantes physiques d'un objet connecté



L'objet est connecté à Internet, mais peut l'être également à un réseau local, à un nuage d'équipement type cloud (ou Fog, au plus près des sources de données, qui est en passe de prendre le relais), voire à un autre objet (M2M). **Les objets connectés se situent en périphérie des réseaux** (avec des problématiques d'accès à des infrastructures ou autres équipements).

L'hétérogénéité des objets physiques (mode d'alimentation, d'information, de connectivité...) nécessite une **architecture réseau** ou un cadre logique pour construire des solutions intégrées, fiables, rentables et donc interopérables. L'IoT s'appuie sur l'architecture théorique OIS sur laquelle se base l'ensemble des architectures utilisées qui ne parviennent pas, à ce jour, à faire consensus. Le modèle TCP/IP qui sert de référence pour le web n'est pas adapté aux IoT, dans la mesure où il demande des échanges de messages volumineux et une capacité réseau trop importante (cf. contraintes d'énergie dans les IoT). Les architectures se construisent au regard des spécificités des constructeurs (Cisco, IBM, Amazon, Google...), du modèle d'affaire (modalités de création de valeur ajoutée de l'IoT) et du domaine d'application (santé, smart transport ...). Les protocoles vont permettre de passer de l'objet à l'applicatif.

L'IoT pose plusieurs défis technologiques : une qualité de services et d'usages, l'adressage des messages dans une prolifération d'objets connectés, et des problématiques d'interconnexion avec les infrastructures. La sécurisation

des données est un défi de taille, tout comme la gestion des énergies des IoT qui est un paramètre de choix en matière d'infrastructure pour les industriels.

Les équipements déployés sont hétérogènes, ce qui complexifie leur opération et coordination en temps réel. A cela

s'ajoutent d'autres contraintes, notamment celle de faire coexister plusieurs générations de machines, issues de différents fabricants, avec des systèmes propriétaires et sans passerelles vers les mondes de l'IoT et de l'IIoT.

Figure 2: Les concepts clefs de l'IoT



Source : A partir de CSI force



PASSÉ > PRÉSENT > FUTURS POSSIBLES

QUELLE A ÉTÉ L'ÉVOLUTION PASSÉE DE LA VARIABLE ?

L'Internet des objets repose sur la combinaison de nombreuses technologies matures aux niveaux électronique, informatique et réseaux. Il ne s'agit pas d'une technologie nouvelle, et les principes de l'IoT sont déjà présents depuis de nombreuses années dans certains secteurs. Toutefois, la création de valeur par l'IoT est en soi une révolution (notamment sur le segment d'analyse de données).

Historiquement, l'IoT trouve ses origines dans le développement des communications Machine to Machines (M2M) et de la RFID. Le terme IoT apparaît en 1999 avec Kevin Ashton (Procter & Gamble) reliant la RFID à l'Internet comme réponse aux problèmes d'approvisionnement et de disponibilité des produits. Mais c'est en 2003 que la première lampe LED intelligente est mise sur le marché par la société VIOLET.

La généralisation des smartphones a été un levier de l'IoT jusqu'à la création des adresses IPSO, adresses IP dédiées de l'IoT (les adresses IPv4 ne sont pas adaptées).

Dans l'industrie, l'IoT apparaît dans la gestion de l'énergie du processus de production et des objets connectés eux-mêmes (mise en veille). Il participe à une maintenance prédictive en limitant les temps morts et en s'appuyant sur la Big Data.

L'Internet des objets se développe à un rythme rapide, en partie grâce à l'explosion de la disponibilité de matériel informatique de petite taille et peu coûteux. Les kits de prototypage et les cartes de développement de l'IoT combinent des microcontrôleurs et des processeurs avec des puces sans fil et d'autres composants dans un ensemble prêt à être programmé.

En matière de réseau de communication, les réseaux industriels sont composés, historiquement, des réseaux câblés (Ethernet) dont le remplacement n'est pas à l'ordre du jour mais qui, au-delà d'une meilleure performance que les réseaux sans fil en matière de débit et de fiabilité, imposent des restrictions concernant la typologie des réseaux.

PASSÉ > PRÉSENT > FUTURS POSSIBLES

QUELLES SONT LES DYNAMIQUES À L'ŒUVRE ?

Les estimations du nombre d'objets connectés et de nœuds dans le monde sont variables d'une étude à une autre mais confirme l'explosion de l'IoT sur le court et moyen terme. Il s'ensuit que les architectures IT actuelles ne sont pas adaptées à la complexité et le foisonnement des données. **Aussi, la tendance est la recherche de nouveaux systèmes** combinant des technologies telles que l'apprentissage automatique, le raisonnement machine et l'automatisation afin de simplifier les opérations et de soutenir la prise de décision humaine, ce à quoi aspire, au final, l'IoT.

Dans l'IoT, les applications migrent du physique au virtuel, aux *conteneurs* et au sans-serveur. Le réseau doit

être envisagé davantage comme un ensemble croissant de « *clusters nerveux* » interconnectés et situés à proximité des données. Selon Ravi Chandrasekaran, VP senior de l'ingénierie des réseaux d'entreprise chez Cisco, « *les réseaux vont fonctionner comme un système doté d'une autonomie croissante, qui prendra en compte son propre état, l'état dynamique de tous les utilisateurs et applicatifs, et la grande variété des options envisageables* ». L'IA a un rôle crucial à jouer, notamment en aidant le domaine des IT à modifier automatiquement le routage du trafic, demander plus de bande passante, exiger une modification de politique par exemple.

La majorité des entreprises maintiennent leurs données dans des installations leur appartenant. Selon l'étude d'Uptime Institut sur les Datacenters en 2020, la majorité des répondants à leur étude (58 % aujourd'hui, 54 % dans deux ans) ont déclaré que la plupart de leurs charges de travail

sont traitées et/ou stockées dans des centres de données d'entreprise. Par contre, la moitié de toutes les charges applicatives seront exécutées en dehors du data center de l'entreprise d'ici 2021, soit dans des infrastructures cloud et data center externes, soit à la périphérie du réseau.

La désagrégation des serveurs

Intel et l'architecture x86 puis x64 ont dominé l'espace des processeurs informatiques pendant la majeure partie des quarante dernières années. Aujourd'hui identifié comme un concurrent direct sur le marché historique d'Intel – les ordinateurs – les puces ARM viennent faire concurrence. Toute son histoire a consisté à mobiliser ses efforts sur des marchés que la technologie x86 n'avait pas pleinement exploités ou sur lesquels elle présentait des faiblesses.

Les réseaux et équipements : un modèle économique porté par la propriété intellectuelle

Une partie de l'architecture de l'IoT, promettant le développement de l'économie de la fonctionnalité, se structure autour de la propriété intellectuelle. Cette approche a deux conséquences directes.

D'une part, le marché se structure autour de normalisation des techniques et innovations industrielles par le biais des consortiums. Les produits sous licence permettent de « contrôler » le marché. Ainsi, emboîtant le pas à plusieurs tentatives de Microsoft, Apple a décidé de reconcevoir sa gamme d'ordinateurs autour de puces maison d'ARM¹, en remplacement d'Intel, et se lance dans la production de son propre SoC² (système sur puce qui peut alimenter un dispositif d'edge computing par exemple), comme elle le fait pour l'iPhone et l'iPad, ce qui pourrait permettre à l'entreprise d'économiser jusqu'à 60 % sur les coûts de production, selon ses propres estimations. A ce propos, et pour ce qui est de l'IoT grand public, la Commission européenne a lancé une enquête sectorielle sur l'IoT des consommateurs, des « éléments point[ant] vers la restriction de l'accès aux données et de l'interopérabilité de ces données, ainsi que vers certaines formes d'autofavoritisme et de pratiques liées à l'utilisation de normes propriétaires³. »

De son côté, Intel a annoncé en 2020 le lancement de deux nouveaux processeurs industriels pour l'internet des objets visant à créer un écosystème pour l'IoT industriel qui sera activé par la 5G. Les processeurs Intel Atom x6000E Series sont conçus pour prendre en charge le traitement des graphiques et des médias dans un format compact (avec un gain de performance doublé au regard des anciennes générations. Siemens a inclus la série Intel Atom x6000E dans ses systèmes).

D'autre part, cette approche par la propriété intellectuelle modifie les règles d'appariement entre l'offre et la demande d'emploi sur le marché du travail. En effet, les certifications sont des signaux plus importants de « qualité sur le marché de l'emploi » que le diplôme en lui-même. Ainsi, le *Certified Information Systems Security Professional* (CISSP) est une certification professionnelle, internationale et commercialement indépendante, en sécurité des systèmes d'information. Le programme de certification est géré par le « *International Information Systems Security Certification Consortium* » et est historiquement une des premières certifications de cybersécurité « puisqu'elle a vu le jour aux États-Unis au début des années 1990 » et l'une des plus difficiles au monde à obtenir. Au 31 mai 2019, 136 480 personnes étaient certifiées CISSP dans 175 pays, majoritairement aux États-Unis. La France arrive 13^{ème} du classement avec 1 077 personnes certifiées. Le Cisco Certified Internetwork Expert (CCIE) est souvent considéré par l'industrie des télécommunications comme étant le « doctorat des réseaux ».

La concurrence des moyens de communication

Il existe un consortium traitant de la standardisation des connexions, 3GPP. Derrière ce consortium se trouvent des organismes de standardisation en télécommunication comme ETSI en Europe, CCSA en Chine, ATIS aux États-Unis qui s'occupent du développement et de la maintenance des standards GSM, UMTS, LTE, et LTE Advanced. La partie LTE fait référence aux réseaux Long Term Evolution, une norme qui évolue sous l'impulsion du consortium 3GPP tous les 12 à 18 mois. Le nom commercial « 4G » recouvre la norme LTE, mais également sa prolongation, la norme « LTE Advanced », qui permet *un débit descendant de 1Gbit/sec*. Certains opérateurs ont utilisé un nom commercial « 4.5G », « 4.9G » pour représenter la norme LTE Advanced. La 5G est une autre prolongation de cette norme LTE. Au sein de l'ATIS, la branche américaine du consortium 3GPP se trouvent les grands noms de l'industrie comme Alcatel-Lucent, Intel, Google, Nokia, Verizon, Cisco, Oracle, etc. Des concurrents tels que Sigfox ou le consortium LoRa risquent de se trouver fragilisés. Les premiers aboutissements du consortium 3GPP ont permis d'aboutir aux normes « LTE Cat M1 » (plus couramment appelée « LTE-M ») et NB-IoT, technologies permettant de réduire la consommation énergétique des appareils connectés. Il s'agit là aussi d'évolutions de la norme LTE.

L'enjeu de la sécurité

La sécurité des données, des systèmes de production et des informations des usagers est un enjeu de taille dans

¹ Arm Holdings, Ltd. est propriétaire de la conception de ses puces et de l'architecture de leurs jeux d'instructions, comme le Arm64 64 bits. Elle accorde des licences à d'autres sociétés, qu'elle appelle "partenaires". Elles utilisent l'architecture d'Arm comme une sorte de modèle, construisant des systèmes qui utilisent les noyaux d'Arm comme processeurs centraux. Chaque appareil incorporant un processeur Arm tend à être son propre système unique, comme le processeur mobile Qualcomm Snapdragon 845

² Une grande partie des fonctionnalités de l'appareil peut être fabriquée sur la puce elle-même, cohabitant avec les noyaux exclusifs d'Arm, plutôt que construite autour de la puce dans des processeurs, accélérateurs ou extensions séparés. Son but est d'exploiter la simplicité, de rendre toutes les fonctionnalités du processeur sur une seule puce. Garder un jeu d'instructions réduit signifie que le processeur peut être codé en utilisant un nombre de bits moins important, ce qui réduit la consommation de mémoire ainsi que le temps de cycle d'exécution. A contrario, la puissance du x86 vient de sa capacité à accomplir de nombreuses choses avec une seule instruction

³ Commission européenne, « Pratiques anticoncurrentielles : la Commission ouvre une enquête sectorielle sur l'internet des objets pour les consommateurs », 16 juillet 2020

le domaine des IoT, et encore plus pour l'IIoT industriel (Industrial IoT, IIoT). De nombreuses menaces planent sur ces appareils et le nombre de cyberattaques vers ces dispositifs ne cesse d'augmenter. La Finlande, premier pays à avoir mis en place un label cybersécurité est au cœur de l'actualité avec un piratage informatique sans précédent via les systèmes informatiques de la société Vastaamo, qui gère pour le compte du service public de santé une vingtaine de centres de psychothérapie. L'Organisation internationale de normalisation (ISO), en collaboration avec la Commission électrotechnique internationale (IEC), a publié à cet effet, en 2018, la nouvelle norme *ISO/IEC 30141:2018 Internet of Things* établit une architecture de référence normalisée pour l'IIoT afin de garantir la sécurité des systèmes et des données

QUELLES SONT LES DYNAMIQUES EN RÉGION HAUTS-DE-FRANCE ?

Selon Nord France Invest, la région Hauts-de-France compte près de 2 700 ESN (entreprises de services numériques) telles qu'OVH, IBM ou CGI. Ce secteur regroupe plus de 40 000 emplois. La région dispose également d'un écosystème important avec Euratechnologies regroupant 300 entreprises, et d'un cluster IIoT.

L'une des forces de la région est la présence d'un Cluster IIoT et de pôles comme EuraTechnologies, qui réunit de grands groupes, un réseau important de startups, des laboratoires de recherche comme l'INRIA et des établissements d'enseignement supérieur. Ce pôle est aujourd'hui le premier incubateur de startups en France.

PASSÉ > PRÉSENT > FUTURS POSSIBLES

QUELLES SONT LES INFLEXIONS ET RUPTURES QUI POURRAIENT MODIFIER LES DYNAMIQUES EN COURS ?

Il faut savoir qu'un **réseau** convergent doit relever plusieurs défis présents dans l'architecture réseau hétérogène actuel : **plus de transparence** (toutes les données de toutes les hiérarchies peuvent être accessibles à tous les éléments de l'usine sans traduction intermédiaire), **moins de planification réseau** (à savoir que les topologies plus flexibles facilitent les évolutions et amélioration du réseau et des logiciels), **moins de dépenses en capital** (réduire les coûts de câblage, réduire les passerelles entre les réseaux avec différents protocoles), **moins de dépenses de fonctionnement** (réduire l'effort d'administration réseau), **plus de bandes passantes** (pour éviter toute limitation à une seule vitesse de réseau) et **optimisé** pour M2M.

Dans le domaine des réseaux (et donc de l'inter-connectivité), Cisco annonce 5 technologies majeures, qui impacteront la numérisation de l'économie. Dénommées sous le vocable « assurance réseau », ces technologies permettent de vérifier continuellement la cohérence de l'état et du comportement du réseau avec l'intention choisie.

L'automatisation des réseaux et leur autonomie

L'une des technologies clefs est l'**automatisation des réseaux**, de la configuration, de la gestion, du test, du déploiement et de l'exploitation des périphériques virtuels et

physiques d'un réseau. Cette automatisation des réseaux se concrétise **grâce aux innovations tel que le réseau défini par logiciel ou SDN** (le Software-Defined Network permet une abstraction de l'infrastructure et les périphériques associés des applications et des services réseau pour que les administrateurs réseau puissent contrôler, modifier et gérer le réseau).

L'automatisation des réseaux s'appuie également sur l'émergence **du réseau intuitif ou IBN**. Cette automatisation est capable de s'auto surveiller pour s'assurer que le réseau respecte l'intention des politiques définies au moment de la configuration. Il augmente les capacités d'automatisation du SDN avec la possibilité de « *convertir l'intention en politique, de collecter des données, d'apporter de la visibilité et des perspectives pertinentes, puis de vérifier que le réseau accomplit véritablement ce qui a été prévu* ».

L'intelligence artificielle en support pour faire face aux environnements réseaux complexes et dynamiques

L'**IA** (intelligence artificielle dédiée aux opérations informatiques ou AIOps) est un autre vecteur de transformation des IIoT et l'une des technologies clefs identifiées par Cisco car elle permet d'envisager une meilleure utilisation des données (qui doivent être de qualité) afin de garantir un fonctionnement efficace des réseaux et une prise en compte permanente des besoins des industriels. Elle peut, par exemple, permettre de prédire les problèmes et favoriser le dépannage des systèmes complexes. Au milieu d'un volume colossal de données, l'IA cerne la complexité des communications et des réseaux et propose des ajustements **dynamiques**.

Des solutions de stockage et de traitements de données hybrides

La croissance exponentielle des données n'amènera pas nécessairement les entreprises à « exporter » toutes leurs charges applicatives ou données en dehors de leurs sites et doivent penser aux réseaux **multi-cloud**. Pour que le **cloud** puisse répondre aux défis de développement des applications (agilité, évolutivité...), plusieurs éléments d'architecture émergent : le SD-WAN⁴, l'**accès cloud direct** (avec la possibilité de sécuriser la connexion directe des utilisateurs du site distant jusqu'aux services cloud), les **installations de colocation et les Cloud Exchanges**, ainsi que les services 5G et haut débit à large bande passante proposés à moindre coût.

Les enjeux de la mixité des réseaux sans-fil et filaires pour les industriels

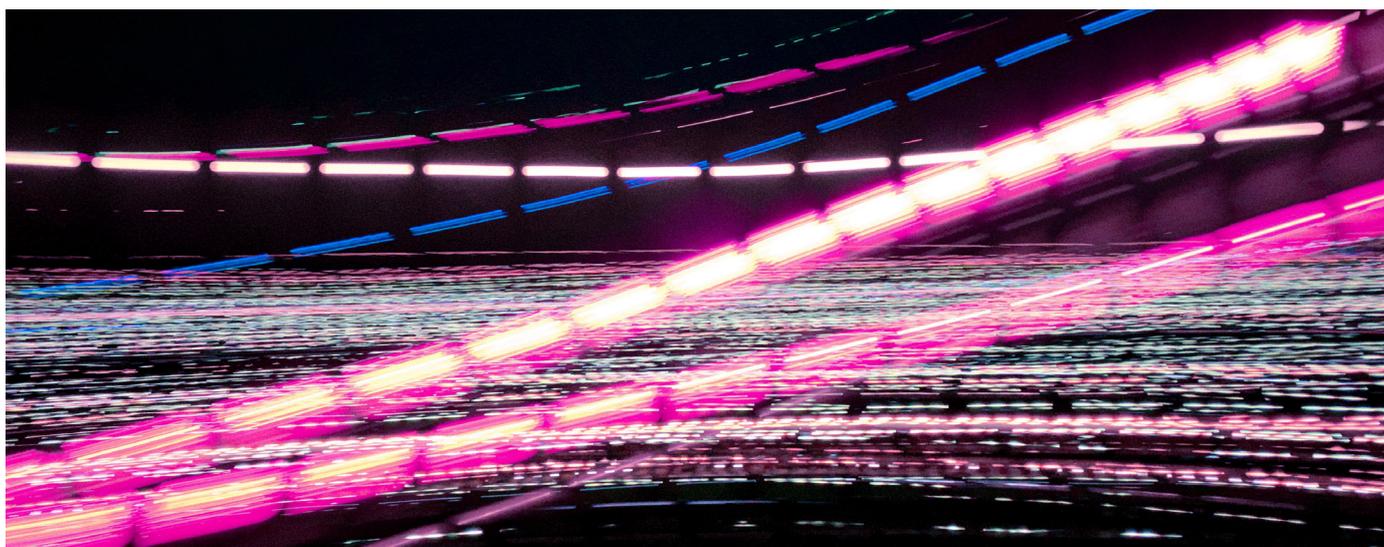
Selon les estimations de Cisco, 29,3 milliards de dispositifs seront en réseau d'ici 2023, contre 18,4 milliards en 2018. Parmi ceux-là, 16,2 milliards d'appareils seront connectés par fil/Wi-Fi d'ici 2023, contre 9,6 milliards en 2018. Bien que les périphériques sans fil représenteront 43 % de tous les équipements connectés en 2022, le réseau filaire présente des innovations importantes pour les parcs industriels (réseau Ethernet 400 Gbit/s commuté⁵). Les modules M2M représenteront 50 % (14,7 milliards) de tous les dispositifs en réseau d'ici 2023 contre 33 % (6,1 milliards) en 2018 au niveau mondial. A cela s'ajoute la **norme TSN qui offre une solution de communication en temps réel, nécessaire à la gestion des parcs industriels, de la maintenance prédictive ou de la mobilisation de l'IA**.

Pour ce qui est du réseau sans fil, ce dernier a bénéficié des innovations dans le domaine du silicium et de l'optique. Les nouveaux réseaux Wi-Fi 6 complémen-

taires à la 5G (pour le mobile public) devraient assurer des gains de performance augmentés. Le Wi-Fi 6 apporte des débits de données plus élevés⁶, une latence plus faible, une densité d'équipements accrue et des performances globales améliorées. Afin d'assurer le passage d'un réseau à un autre avec une faible latence, il existe l'**OpenRoaming** qui s'appuie sur la technologie **Passpoint de la Wi-Fi Alliance**. Cette technologie offre aux utilisateurs une itinérance facile et sécurisée entre différents réseaux Wi-Fi 6 et 5G publics via une fédération basée dans le cloud de réseaux d'accès et de fournisseurs d'identité, dont des opérateurs mobiles. **La sécurité du réseau des entreprises devra alors être renforcée**. L'enjeu sera ainsi que les industriels puissent assurer une unification de leur architecture mixte.

S'il reste à définir si la **sécurité réseau** est une technologie, il n'en demeure pas moins qu'elle est l'un des enjeux majeurs à venir pour l'IoT et les innovations technologiques sur lesquelles elle s'appuiera dans son développement. Les réseaux intuitifs sont une solution technologique pertinente pour la sécurité, dans la mesure où ils peuvent détecter des anomalies et, de fait, des attaques potentielles au sein d'un réseau distribué.

En matière de sécurité et de traitement de l'information, il est possible de déplacer le stockage des données sur une interface gérée par la DPU (Data Processor Unit), de sorte que l'unité centrale accède aux données stockées en utilisant le réseau plutôt que le bus système (dispositif de transmission de données partagé entre plusieurs composants d'un système numérique), permettant ainsi des contrôles de politique et de sécurité pour la connexion. En découplant les parties initialement interdépendantes les unes des autres, et en plaçant chacune d'entre elles derrière des adresses dans un réseau neutre, la position dominante de l'architecture x86 (Intel) ne serait plus assurée au moyen d'un bus inévitable et non substituable, un avantage pour ARM.



⁴Technologie de connectivité Internet professionnelle permettant de construire un réseau virtuel prenant appui sur un réseau physique et de le piloter depuis un point central. Autrement dit, elle permet d'accéder aussi bien aux applications internes qu'à celles externalisées, en utilisant le meilleur chemin suivant le trafic

⁵ Les 400 Gbit/s du 400 GBASE-SR16 seraient transmis sur deux rubans de seize fibres optiques multimodales chacun : un pour la transmission de 16 fois 25 Gbit/s, l'autre pour la réception de 16 fois 25 Gbit/s. Les dernières innovations permettent d'envisager l'Ethernet Terabit

⁶ Sachant que selon l'indice Cisco VNI 2018, l'échelle mondiale, le trafic IP d'entreprise atteindra 63,3 exaoctets par mois en 2022, soit le triple du trafic enregistré en 2017

MICRO-SCÉNARIOS

Elaborés en atelier, ces scénarios proposent un contenu de l'évolution possible de la variable étudiée, articulés à partir de trois hypothèses :

- **une hypothèse basse** (quelle évolution de la variable défavoriserait l'industrie régionale),
- **une hypothèse haute** (quelle évolution de la variable favoriserait l'industrie régionale),
- ainsi qu'un scénario s'inscrivant davantage dans une forme de continuité (**hypothèse tendancielle**).

A noter : les micro-scénarios du bloc « évolutions technologiques » ont été développés en agrégeant l'ensemble des connaissances produites sur l'ensemble des variables étudiées (Big Data, cobotique, intelligence artificielle etc.). En conséquence, ils sont identiques sur l'ensemble des fiches produites, mais proposent un contenu séquencé selon une entrée économique, environnementale, et sociale.

UNE INTÉGRATION INSUFFISANTE DES ENJEUX DES TECHNOLOGIES NUMÉRIQUES QUI MET LES INDUSTRIELS À LA TRAÎNE DE L'ÉCHIQUIER INTERNATIONAL

Peu informées, mal préparées, les industries régionales travaillent à leur transformation numérique au cas par cas, au gré des demandes de leurs clients. Il en résulte des pertes de parts de marchés pour celles qui anticipent le moins l'évolution des attentes.

Au niveau local, en dépit de l'implication des représentants économiques (branches professionnelles, institutionnels...), seules les entreprises de taille conséquente et les entreprises appartenant à un groupe parviennent à tirer leur épingle du jeu et à développer des stratégies numériques efficaces et globales.

En conséquence, l'outil de production est vieillissant pour les établissements les moins intégrateurs de technologies numériques, et la production en recule car de moins en moins adaptée aux besoins des clients (de plus en plus exigeants). L'industrie n'attire plus, peine à recruter, et ne renouvelle pas ses compétences.

Une partie des industries régionales est peu ou mal connectée. Le niveau de digitalisation des petites structures se limite à rendre visible l'activité de l'entreprise ou à l'usage de logiciels de gestion administrative ou de comptabilité. Elles sont vulnérables aux nouvelles formes de cyberattaques (rançons).

Par ailleurs, les outils financiers publics visant à digitaliser plus largement l'industrie ont davantage profité à des entreprises qui souhaitaient se relocaliser en France, mais qui n'ont pas nécessairement été créateurs d'emplois.

Sur un plan environnemental, les aides publiques se concentrent davantage sur les ruptures technologiques vers une industrie décarbonée (hydrogène...).

Dans une région présentant un profil industriel énergétique particulièrement consommateur (d'énergie, comme de matières), le caractère émergent des technologies développées et leurs coûts d'entrée (R&D) et d'acquisition (investissements) découragent massivement les PME/TPE et artisans de production.

D'un point de vue social, les salariés peu formés, peu préparés, voient dans la technologie un concurrent et pas un facilitateur accentuant ainsi la baisse de l'acceptabilité technologique nécessaire à une industrie connectée.

MICRO-SCÉNARIOS SUITE

LA DIFFICILE MISE EN RÉSEAU DU TISSU INDUSTRIEL

Le tissu industriel est mal identifié par les plans de soutien nationaux à la digitalisation de l'industrie. Les artisans de production, par exemple, ne sont pas intégrés dans les politiques d'investissement et d'accompagnement à la transformation numérique. Ces derniers se cantonnent à développer des marchés locaux avec l'appui de technologies abordables (objets connectés, système d'*edge computing*, fabrication additive...). Leur modèle économique est fragilisé par la faiblesse du nombre de leurs clients.

La propriété intellectuelle continue d'être dominante dans la régulation de l'innovation.

Les investissements publics en faveur d'une transition environnementale profitent assez peu à certains secteurs *a contrario*, par exemple, de l'agriculture, secteur précurseur dans les nouvelles technologies liées à la gestion de l'environnement.

L'innovation sociale est mal intégrée dans le soutien aux vecteurs de transition qui se cantonnent à des expérimentations locales.

Depuis la stratégie de Lisbonne, les taux d'emploi se sont améliorés en France même si les salariés accusent un retard dans la maîtrise des savoirs de base.

L'industrie connectée modifie le contenu de ces savoirs de base qui s'élargissent aux habilités numériques (capacité à supporter la charge cognitive d'une relation Hommes-Machines, capacité à protéger sa vie privée avec l'usage des réseaux sociaux...) mais sans réelle capacité à construire une offre d'accompagnement de ces mutations de compétences. De nouveaux risques liés à la santé au travail émergent, dans un contexte de fragilisation du modèle social suite à la destruction d'emplois liés au numérique. Ce recul du nombre d'emplois induit à terme une baisse de recette pour les collectivités.

LA MAÎTRISE DE LA CHAÎNE DE VALEUR NUMÉRIQUE POUR DE NOUVELLES CRÉATIONS DE VALEUR

Grâce à un cadre sécurisant (choix logiciels, aides publiques...), les industries investissent massivement dans les technologies numériques.

Les industries augmentent leur productivité grâce à ces solutions et sont plus innovantes (ex : fabrication additive qui permet des prototypes rapides), leurs capacités d'adaptation aux besoins des consommateurs s'améliorent.

À la recherche de toujours plus de gains de productivité, de plus en plus d'entreprises se tournent vers la digitalisation de leur appareil productif.

Parallèlement les plans de relance gouvernementaux se succèdent, les encourageant dans cette voie. Cela permet aux établissements à la fois de limiter leurs coûts (gestion des stocks), d'améliorer leur performance environnementale (optimisation de la consommation d'énergie et de matières) et d'améliorer les conditions de travail des opérateurs.

Des plans de formation et de sensibilisation sont également déployés, permettant aux jeunes générations de mieux connaître les nouveaux métiers que l'industrie connectée leur propose.

RÉFÉRENCES DOCUMENTAIRES

- Jean-Pierre Hauet. L'Internet des objets - Deux technologies clés : les réseaux de communication et les protocoles (Partie 1), 2016
- Rhonda Ascierio, Andy Lawrence. Global data center survey 2020. Uptime Institute. 2020
- Cisco. Rapport sur les tendances mondiales des réseaux en 2020. 2019
- SEE. Synthèse de l'étude Internet des objets 2018. Novembre 2017
- Autorité de régulation des communications électroniques et des postes (ARCEP). Livre blanc : « Préparer la révolution de l'internet des objets ». Document n°1 : « Une cartographie des enjeux ». 7 novembre 2016
- Iot Business Club. IoT France 2020 : Les leviers de l'accélération
- Alliance Industrie du Futur. Le guide des technologies de l'Industrie du Futur. Mars 2018
- EBG/WAVESTONE. L'IoT industriel. DU POC à l'industrialisation
- PIPAME. Prospective. Marchés des objets connectés à destination du grand public. 2018



Date de publication : février 2021

Rédaction : Karen Maloingne - Ahlam Benlemselmi
Christophe Meulemans - Sylvie Delbart
Contact : collegedeprospective@hautsdefrance.fr

Retrouvez l'actualité et les publications du collège sur le site
de l'Agence Hauts-de-France 2020-2040
<https://2040.hautsdefrance.fr>