Sujet élaboré par une cellule pédagogique nationale

EXAMEN PROFESSIONNEL DE PROMOTION INTERNE D'INGÉNIEUR TERRITORIAL

SESSION 2026

ÉPREUVE DE PROJET OU D'ÉTUDE

ÉPREUVE D'ADMISSIBILITÉ :

L'établissement d'un projet ou étude portant sur l'une des options, choisie par le candidat lors de son inscription.

Durée : 4 heures
Coefficient : 5

SPÉCIALITÉ : INFORMATIQUE ET SYSTÈMES D'INFORMATION
OPTION : RÉSEAUX ET TÉLÉCOMMUNICATIONS

À LIRE ATTENTIVEMENT AVANT DE TRAITER LE SUJET :

- Vous ne devez faire apparaître aucun signe distinctif dans votre copie, ni votre nom ou un nom fictif, ni initiales, ni votre numéro de convocation, ni le nom de votre collectivité employeur, de la commune où vous résidez ou du lieu de la salle d'examen où vous composez, ni nom de collectivité fictif non indiqué dans le sujet, ni signature ou paraphe.
- Sauf consignes particulières figurant dans le sujet, vous devez impérativement utiliser une seule et même couleur non effaçable pour écrire et/ou souligner. Seule l'encre noire ou l'encre bleue est autorisée. L'utilisation de plus d'une couleur, d'une couleur non autorisée, d'un surligneur pourra être considérée comme un signe distinctif.
- Le non-respect des règles ci-dessus peut entraîner l'annulation de la copie par le jury.
- Les feuilles de brouillon ne seront en aucun cas prises en compte.

Ce sujet comprend 53 pages.

Il appartient au candidat de vérifier que le document comprend le nombre de pages indiqué.

S'il est incomplet, en avertir le surveillant.

- Vous répondrez aux questions suivantes dans l'ordre qui vous convient, en indiquant impérativement leur numéro.
- Vous répondrez aux questions à l'aide des documents et de vos connaissances.
- Des réponses rédigées sont attendues et peuvent être accompagnées si besoin de tableaux, graphiques, schémas...
- Pour les dessins, schémas, cartes et plans, l'utilisation d'une autre couleur que le bleu ou le noir ainsi que l'utilisation de crayons de couleur, feutres, crayon de papier sont autorisées.

Vous êtes ingénieur territorial au sein de la direction du numérique et des systèmes d'information d'Ingéagglo, une communauté d'agglomération de 180 000 habitants.

Depuis quelques années, plusieurs directions métiers (déchets, voirie, éclairage public) ont été approchées par des prestataires privés proposant des solutions « internet des objets » (IoT) spécifiques aux domaines adressés. Des expérimentations ont même déjà été menées : sondes de qualité de l'air dans la ville-centre et sur les principaux axes urbains, éclairage intelligent sur certains quartiers du territoire, taux de remplissage des bennes sur les centres de collecte et conteneurs enterrés.

Ces initiatives posent des questions de cohérence, d'interopérabilité, de sécurité et de pilotage global. L'exécutif communautaire souhaite disposer d'une vision d'ensemble du sujet et d'une stratégie de convergence autour de l'IoT en lien avec le futur schéma directeur d'aménagement numérique du territoire, les évolutions récentes de la 5G, du numérique responsable et des enjeux de cybersécurité.

Question 1 (4 points)

Le directeur général des services (DGS) vous confie la rédaction d'une note détaillant les enjeux d'une stratégie IoT territoriale au service d'une smart city et prenant en compte les expérimentations déjà menées.

Question 2 (6 points)

Ingéagglo envisage de structurer et généraliser ses initiatives IoT.

a) Vous détaillerez l'ensemble des contraintes à prendre en compte pour réussir un tel projet. (3 points)

b) Vous proposerez plusieurs solutions technologiques pour répondre à ce besoin en précisant les critères de comparaison pour converger vers une solution unifiée. (3 points)

Question 3 (6 points)

Au regard des critères identifiés et pour répondre aux besoins d'Ingéagglo, vous êtes chargé de proposer une démarche pour mettre en place la future plateforme IoT de l'agglomération :

a) Vous proposerez une architecture technique adaptée à ce type de déploiement. (3 points)

b) Vous identifierez les principales mesures de sécurité et de gouvernance des données. (3 points)

Question 4 (4 points)

Dans une perspective de contrainte budgétaire, d'innovation, de coopération territoriale et de souveraineté numérique, vous présenterez :

- Les perspectives d'évolution de l'IoT urbain ;
- Les risques et limites à anticiper ;
- Les opportunités de mutualisation avec d'autres collectivités ou partenaires.

Liste des documents :

Document 1 : « L'IoT va devenir plus performant et plus sécurisé » - *Techniques de l'Ingénieur* - 25 octobre 2024 - 2 pages

Document 2 : « Gouvernance de la smart city et cybersécurité » - *Cahiers de la sécurité et de la justice n°56* - 15 mars 2023 - 7 pages

Document 3 : « Rennes Métropole : territoire pionnier de l'Internet des Objets (IoT) » - *synox.io* - consulté le 29 novembre 2025 - 2 pages

Document 4 : « A quelles conditions les objets connectés peuvent devenir un levier numérique pour la transition écologique » - *Lagazette.fr* - 13 juin 2025 - 3 pages

Document 5 : « Périmètre des dispositifs de l'internet des objets vis-à-vis des technologies de l'information et des communications » (extrait) - *ARCEP* - juillet 2024 - 6 pages

Document 6 : « Grâce aux objets connectés, les collectivités pourraient économiser 1,5 milliard d'euros en 2035 » - *Lagazette.fr* - 17 mars 2025 - 3 pages

Document 7 : « Souveraineté numérique, entre mythe d'indépendance et réalité industrielle » - *L'Usine Digitale* - 20 janvier 2026 - 7 pages

Document 8 : « Les territoires connectés durables » (extrait) - *Direction générale des entreprises* - octobre 2023 - 7 pages

Document 9 : « Approche SSI pour l'internet des objets industriels » - (extrait) - *ANSSI* - 30 mai 2025 - 6 pages

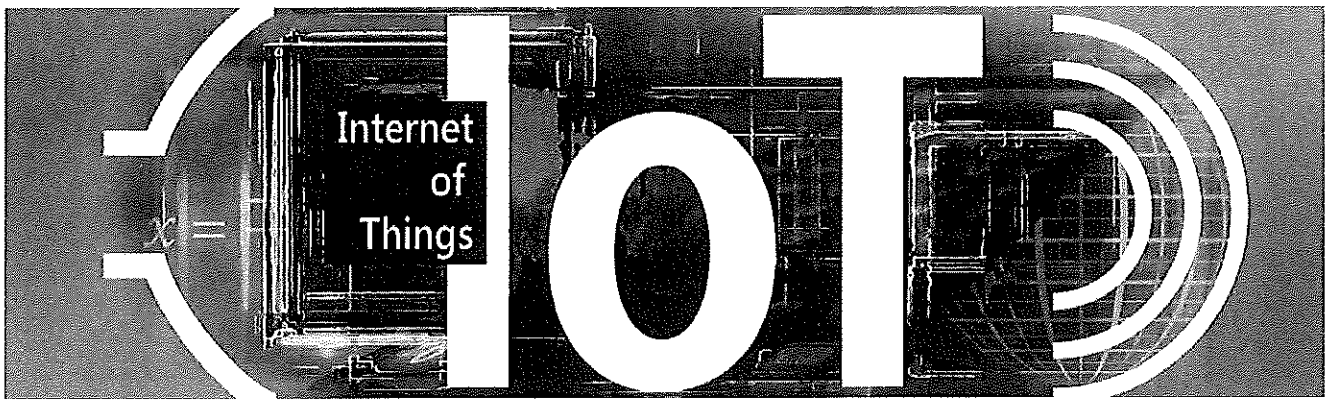
Document 10 : « Objets connectés et RGPD : comment sécuriser l'IoT ? (extrait) - *codpo.fr* - 7 octobre 2025 - 3 pages

Liste des annexes :

Annexe A : « Présentation d'Ingéagglo » - 3 pages

Dans un souci environnemental, les impressions en noir et blanc sont privilégiées. Les détails non perceptibles du fait de ce choix reprographique ne sont pas nécessaires à la compréhension du sujet, et n'empêchent pas son traitement.

DOCUMENT 1



EN CE MOMENT

L'IoT va devenir plus performant et plus sécurisé

Posté le 25 octobre 2024 par **Philippe RICHARD** dans Informatique et Numérique

L'IoT (ou l'Internet des objets) est en constante évolution. Plusieurs tendances se dessinent : l'intégration de l'intelligence artificielle, du Edge computing et de la blockchain... À la clé, des connexions plus efficaces et sûres.

L'Internet des objets (ou IoT pour « Internet of Things ») désigne un réseau de dispositifs physiques, de véhicules, d'appareils et autres objets dotés de capteurs, de logiciels et d'une connectivité réseau. Ces appareils « intelligents » peuvent collecter et partager des données, ce qui leur permet de communiquer entre eux et d'effectuer diverses tâches de manière autonome.

Le nombre de ces appareils connectés augmente rapidement. Mais la mise en œuvre de scénarios IoT se heurte encore à certaines limites et à des défis : confidentialité des données, interopérabilité, évolutivité, consommation d'énergie…

De nouveaux développements devraient accélérer et simplifier son introduction. Voici les quatre principales tendances.

1. Des systèmes IoT intelligents et réactifs grâce à l'IA

L'IA et le machine learning sont de plus en plus utilisés pour optimiser certains processus. L'IoT n'échappe pas à la règle. En analysant de grandes quantités de données, l'IA améliore les applications de l'IoT dans des domaines tels que la maintenance prédictive et la gestion de l'énergie.

La combinaison des capacités analytiques de l'IA avec les capacités de collecte et de surveillance des données de l'IoT devrait permettre de créer un écosystème où les informations opérationnelles sont recueillies plus efficacement.

Mais l'intégrité des données, basée sur l'utilisation de sources de données fiables et authentiques, est cruciale pour instaurer la confiance dans les écosystèmes...

2. Des performances améliorées grâce au Edge computing

Le Edge computing (ou informatique en périphérie) permet de traiter les données plus près de la source. Cela réduit également la quantité d'informations qui doit être envoyée à un datacenter. D'où une latence plus réduite, ce qui est important pour les applications en temps réel telles que l'automatisation industrielle. Le développement des réseaux 5G améliorera encore la communication entre ces appareils et permettra un traitement des données plus rapide et plus efficace.

3. La sécurité de l'IoT renforcée grâce à la blockchain

Ces appareils gérant de plus en plus de données, il est primordial d'assurer leur confidentialité et intégrité. La nature décentralisée de la blockchain, avec la capacité de garantir l'authenticité et la sécurité des transactions de données à travers le réseau, permet de relever ces défis.

4. Une meilleure gestion des appareils grâce à une nouvelle norme

L'eSIM SGP. 32 (eSIM pour « embedded SIM ») pour l'IoT a été créée pour répondre aux besoins des déploiements IoT. La SGP.32 est une nouvelle spécification publiée par la GSMA (Global System for Mobile Communications) en mai 2023 pour le provisionnement SIM à distance.

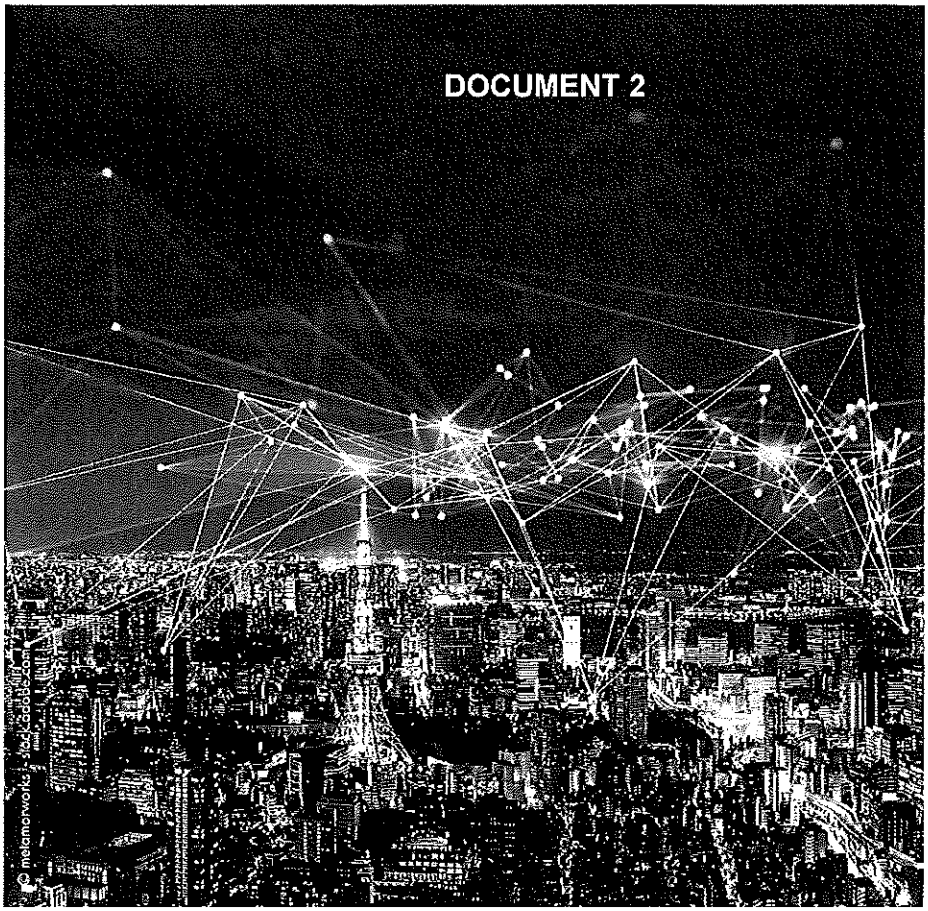
Ainsi, il ne sera plus nécessaire d'établir des connexions supplémentaires via Wi-Fi ou Bluetooth lors de la mise en service d'un appareil IoT. Cela simplifiera à la fois le matériel de l'appareil et les processus logistiques.

Les données de connexion et les paramètres requis pour la carte SIM peuvent être envoyés directement aux appareils par voie hertzienne (OTA). Cela facilite grandement le chargement, l'activation et la gestion des profils SIM des appareils IoT. Ceux-ci peuvent ainsi être gérés de manière plus efficace et plus souple tout au long de leur cycle de vie.

Gouvernance de la *smart city* et cybersécurité

Nathalie FABRY, Sylvain ZEGHNI

15 mars 2023



Introduction

Dans son roman *Blackout : Demain, il sera trop tard*, le romancier autrichien Marc Elsberg [2016] propose un thriller catastrophe axé sur le cyber-terrorisme. Un groupe de *hackers* manipule le réseau de centrales électriques européennes, plongeant l'Europe dans le chaos. La perte d'énergie entraîne par un effet domino des catastrophes allant des pénuries alimentaires à la dévaluation monétaire, en passant par les catastrophes nucléaires et l'effondrement de la société. Il n'y a pas besoin d'aller chercher dans la fiction, car l'actualité regorge d'exemples de cyber-malveillance. Déjà, en 2015, une cyberattaque a affecté le réseau électrique de l'Ukraine, compromettant la distribution d'énergie, mettant hors service l'infrastructure informatique et détruisant d'innombrables fichiers de données [Baezner, 2018]. L'actualité récente concernant la France (hôpitaux, villes, etc.) confirme la menace. Les médiatiques attaques d'hôpitaux de Rouen, Dax ou Chalon-sur-Saône et les moins médiatiques attaques des villes de Angers, Charleville-Mézières, Marseille, Martigues, Toulouse, Vincennes, qui ont eu lieu lors des deux premières vagues de la crise sanitaire de la Covid-19 en témoignent. Un exemple récent aux États-Unis est celui du Colonial pipeline en mai 2021 [CRS Report, 2021]. La menace de graves cyberattaques sur les infrastructures numériques est très réelle [World Economic Forum 2020, 2021 ; Soare *et al.*, 2020 ; Thibodeaux, 2017].

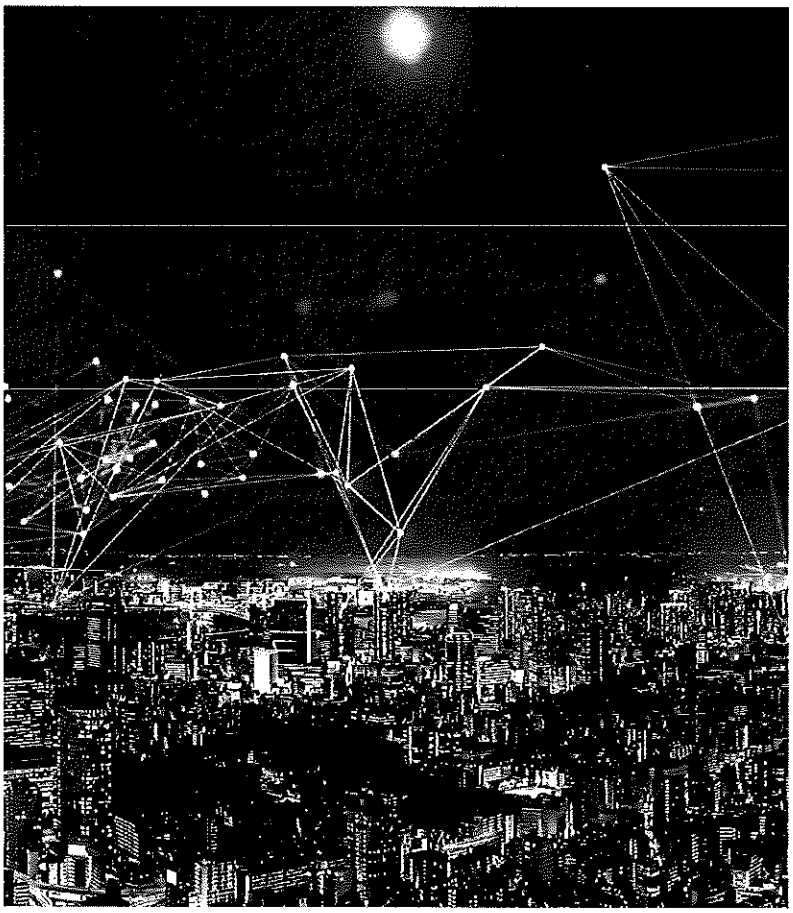
Pourquoi de telles cyberattaques sur les infrastructures ? La croissance urbaine, la transition tant écologique, numérique qu'énergétique, le besoin d'une nouvelle gouvernance démocratique, les tensions sur les finances publiques, etc. favorisent le développement des villes intelligentes. De plus en plus de villes tentent de devenir des *smart cities*. Elles adoptent des technologies intelligentes, misent sur l'interopérabilité des systèmes d'information et se reposent sur le numérique dans leur gestion du quotidien. De cela résulte le fait que les réseaux d'infrastructures numériques s'interconnectent et se complexifient chaque jour davantage. Par ailleurs, le nombre

Nathalie FABRY

Nathalie Fabry est Professeure à l'Université Gustave Eiffel. Elle a obtenu une double HDR d'abord en économie internationale à l'Université Paris-Est Marne-la-Vallée et en Sciences de l'Information et de la Communication à l'Université de Poitiers. Elle est chercheure au Laboratoire DICEN-Ile de France rattachée à la thématique « Intelligence économique, décision & Territoires ».

Sylvain ZEGHNI

Sylvain Zeghni est économiste. Il est Maître de Conférences habilité à diriger les recherches à l'Université Gustave Eiffel et membre du comité de rédaction de la revue « Mondes en Développement ».



de technologies connectées utilisées va connaître ces prochaines années une forte croissance, notamment grâce au développement de la technologie 5G, voire 6G [Damiano, 2020]. La *smart city* devient plus vulnérable aux cyberattaques, car même la plus petite vulnérabilité pourra être exploitée par les cyber-délinquants. La force des villes intelligentes dépend et dépendra de leur capacité à identifier et sécuriser leur maillon le plus faible.

Un certain nombre d'études ont présenté des analyses de la littérature sur les villes intelligentes. Cependant, la plupart de ces études semblent avoir omis de présenter une analyse significative des menaces inhérentes au développement des infrastructures urbaines intelligentes, de leurs conséquences sur le fonctionnement des villes.

L'objet de cette contribution est de s'interroger sur la place qu'occupe la sécurité dans la conception puis dans la gouvernance de la *smart city*, notamment en France. L'hypothèse que nous formulons est que la *smart city* gagne à intégrer, dès l'origine, la notion de cybersécurité. C'est ainsi que nous verrons dans un premier point ce qu'il convient d'entendre par *smart city* d'un point de vue théorique. Dans un deuxième point, nous explorerons le lien entre *smart city* et cybersécurité tel qu'il est présenté aux collectivités territoriales par la Banque des territoires, très active en matière de solutions « intelligentes » pour les collectivités en France. Nous développerons également le lien entre la *smart city*, la cybersécurité et la notion encore émergente de cyber-résilience qui appelle une gouvernance adaptée.

Qu'entendre par *smart city* ?

Le terme *smart* a émergé dans les années 1990 aux États-Unis au sein du mouvement de citoyens *Smart Growth* [Ouellet, 2006] qui proposait un ensemble de mesures alternatives à l'étalement urbain. Le terme a ensuite été généralisé par des firmes comme Cisco, IBM ou Ericsson pour mettre en évidence le développement urbain de plus en plus dépendant des technologies de l'information et de la communication (TIC), dans un contexte de mondialisation croissante. Dès le départ, la *smart city* porte en elle une ambiguïté, car pour les citoyens militants, elle est un projet de vie et de résidence, tandis que pour les entreprises, elle est une solution technologique complexe, gage de nouveaux marchés.

Pour nombre d'auteurs, la *smart city* est un concept valise [Anthopoulos *et al.*, 2018 ; Caragliu et Del Bo, 2017 ; Lim *et al.*, 2018 ; Tompsom, 2015] destiné à mettre l'accent sur le lien entre le territoire urbain et l'innovation portée par le numérique [Yigitcanlar *et al.*, 2018]. C'est aussi un concept en évolution qui a d'abord été envisagé d'un point de vue strictement technologique et qui désormais est compris comme une ville en quête de haute qualité de vie et de services. Si la *smart city* fait controverse [Eveno 2019], elle ne se décline pas en un modèle unique, ce qui permet le développement de monographies de type *success stories* [Henriot *et al.*, 2018 ; Leprêtre, 2018 ; Simonofski *et al.*, 2021], d'études comparatives [Camboim *et al.*, 2019], de classements divers[1]. L'Union européenne s'est positionnée dès 2011 sur ce thème dans le cadre de politiques de développement régional axées sur le numérique, la gestion efficiente des ressources, la réduction des émissions carbone, l'accompagnement des populations dans un contexte de métropolisation croissante, sous l'intitulé de *smart cities initiative*[2].

(1) Par exemple à l'initiative d'entreprises du secteur des TIC et des réseaux (Juniper research et Intel, 2017), d'universités (IMD Business School de Singapour : https://www.imd.org/research-knowledge/reports/imd-smart-city-index-2019/), de *Think thanks* (World Economic Forum : https://www.weforum.org/platforms), d'institutions internationales (Nations unies, UNESCO).

(2) Commission européenne : https://digital-strategy.ec.europa.eu/en/policies/smart-cities-and-communities

La *smart city* n'est pas un statut, mais un processus qui focalise les ambitions territoriales pour le futur [Angelidou, 2015 ; Fabry et Blanchet, 2019 ; OCDE, 2020]. Le seul point commun aux variantes locales est l'architecture de la *smart city* qui est atypique, complexe, et à ce titre, vulnérable. Dans un dernier point, nous verrons les enjeux en termes de sécurité, de gouvernance et de résilience.

La smart city comme processus et ambition pour le futur

La *smart city* doit affronter de nombreux enjeux : l'augmentation de la population urbaine, l'urgence écologique et la transition énergétique, les contraintes sur les finances publiques, le besoin de réinventer le lien entre le service public et l'usager, la quête des habitants pour augmenter leur confort de vie, etc. En réponse, la *smart city* doit créer une synergie entre différents domaines tels que la gestion intelligente du trafic, le développement de nouveaux modes de transports, l'optimisation de la consommation d'énergie et de la gestion des déchets, la protection des biens et des services, la domotique, etc.

La première réponse a été de gérer de manière optimale les flux, les réseaux et les infrastructures urbaines grâce à un suivi et un *monitoring* en temps réel des pannes, accidents et encombrements, ainsi que la mise en place d'une maintenance préventive [Camero et Alba, 2019 ; Ismagilova *et al.*, 2019 ; Maestre-Gongora *et al.*, 2019]. La *smart city* dans sa lecture technologique est un réseau de capteurs (*smart grids*) et d'objets connectés qui envoient des données et informations numériques. Ces *data* sont traitées grâce aux solutions développées par des grandes entreprises. Du point de vue des citoyens, cette ville digitale peut être perçue comme trop intrusive vis-à-vis de la vie privée et des données personnelles [CNIL, 2017] et trop organisée autour de la technologie [Plassat *et al.*, 2018 ; Rouvroy et Berns, 2013], car pouvant donner lieu à une « gouvernance algorithmique » [Gilmozzi *et al.*, 2020, p. 82].

La *smart city*, dans sa lecture actuelle, vise à économiser les ressources, tout en maintenant une qualité de vie élevée pour les habitants. Cette *smart city* déplace l'intelligence des outils et des solutions numériques vers la combinaison intelligente des ressources et des activités en vue de l'amélioration de la qualité de vie. Avec cette acception, entrent désormais dans le périmètre de la *smart city* différents domaines comme les administrations locales, les infrastructures et l'énergie, les mobilités, l'éducation, la santé et les soins, la sécurité, l'innovation, la participation citoyenne, l'urbanisation, l'éducation [Ahmadi-Assalemi *et al.*, 2020]. En devenant plus inclusive, la *smart city* devient aussi plus vulnérable aux cyberattaques en raison de son architecture complexe.

L'architecture de la smart city

Les infrastructures et leur architecture sont le fondement du développement d'une ville intelligente ; elle peut être divisée en deux catégories : physique et numérique.

L'architecture du système d'information de la *smart city* compile à la fois les contraintes d'un système d'information de gestion et celles d'un système d'information qui collecte des données au plus près de leurs sources, par le déploiement incessant d'objets connectés. La *smart city* s'apparente donc à une plateforme de données hétérogènes qui se complexifie à mesure de son développement.

Ces données émanent de fournisseurs de données du secteur public, du secteur privé et des individus. L'enjeu est de les stocker, de les mettre à disposition et de les croiser grâce à une homogénéisation des données et le développement d'API[3] qui permettent la création de nouveaux services pour les citoyens, les acteurs économiques ou les collectivités territoriales.

Une démarche *smart city* appelle le développement permanent de nouvelles fonctionnalités créatrices de valeur pour l'usager. Cela induit de gérer l'interopérabilité entre des systèmes multigénérationnels, qui empilent des nouvelles et anciennes briques technologiques. Cela implique également de maîtriser l'ouverture de son système d'information. Mais cette interopérabilité entraîne l'utilisation de protocoles disparates pouvant générer des failles de sécurité.

Les systèmes qui composent la *smart city* doivent avoir la capacité d'évoluer rapidement de manière à bénéficier des innovations des acteurs du marché. Ils doivent également répondre à des usages émergents. Ils doivent surtout prévoir des systèmes fiables, capables d'être maintenus dans le temps. Ceci pose la question du lien entre la *smart city* et la cybersécurité, notamment dans le cas des collectivités territoriales françaises.

(3) API : interface de programmation d'application.

Les enjeux en termes de sécurité, de gouvernance et de résilience

Loin d'être anecdotique, la sécurité est un enjeu transversal incluant tous les domaines de la vie quotidienne. Les enjeux autour de la propriété des données et du respect de la vie privée sont au cœur des préoccupations des usagers des villes intelligentes.

Aujourd'hui, il n'existe pas de référentiel de sécurité ou de consensus sur la gouvernance de celle-ci. Nous ne sommes encore qu'au début d'une ère numérique où le quotidien des espaces urbains sera grandement modifié. Nous pouvons toutefois noter certaines initiatives sur des sujets connexes aux *smart cities*, mais qui côtoient les mêmes enjeux.

La donnée est au cœur de la *smart city*, au point d'être devenue un véritable prérequis à son développement. Même si les différentes expérimentations actuelles démontrent déjà une certaine capacité à capter et exploiter ces données, il semble plus que nécessaire d'en accentuer la maîtrise et d'en organiser de façon pertinente la gouvernance. Les villes intelligentes ne pourront continuer à se développer sans cette démarche de redéfinition des interactions et du traitement des données entre les différents acteurs de la vie urbaine (privés, publics, consommateurs, citoyens). La gestion des données constitue donc un enjeu stratégique pour la démocratie locale, la gestion du territoire et le développement économique.

La résilience – pour les villes comme pour les organisations – est devenue une priorité à la suite de la pandémie. Le terme reflète la capacité d'une ville à assurer la continuité des services pour la ville et les citoyens en cas de catastrophe, à se reconstruire rapidement et prospérer après l'événement. Des niveaux élevés de résilience urbaine reposent sur des infrastructures de qualité, des communautés interconnectées et une bonne gouvernance. Lorsque ces éléments sont liés les uns aux autres, les villes peuvent faire face et rebondir rapidement, même après la crise la plus difficile.

La *smart city* et la cybersécurité

La Banque des territoires est une filiale de la Caisse des dépôts et consignation dont la mission est d'accompagner les acteurs territoriaux dans l'élaboration et le déploiement de leurs projets d'avenir. Nous nous sommes donc demandé comment le lien « *smart city* et cybersécurité » est présenté aux collectivités territoriales par l'opérateur en charge de l'aide au financement et du modèle opérationnel des *smart cities* en France. Nous verrons de manière plus générale que le lien *smart city* et cybersécurité doit être repensé, ce qui conduit à introduire la notion de cyber-résilience des territoires.

Les préconisations de la Banque des territoires

Nous avons réalisé une analyse de corpus extrait du site web de la Banque des territoires[4]. Deux entrées ont été priorisées : l'entrée thématique *smart city* et l'entrée factuelle cybersécurité. Sur le site web de la thématique *smart city*, la cybersécurité est abordée dans les « enjeux de la *smart city* », rubrique « *smart* territoire : les écueils à éviter ». La cybersécurité est associée à la conception d'une infrastructure numérique résiliente et à la mise en place d'un plan de résilience numérique. L'entrée par le mot-clé cybersécurité permet d'accéder à des éléments factuels, des points d'analyse et d'actualité et à quelques documents support. Il s'agit d'articles rédigés par Localtis, le média spécialisé de la Banque des territoires. Le croisement cybersécurité et *smart city* dans ce *corpus* fait ressortir un seul article, « Menace sur la ville : la cybersécurité à l'heure de la *Smart City* de 2019 ». Finalement, huit documents ont été analysés qui permettent de faire ressortir deux grandes préconisations de la part de la Banque des territoires : sortir de la vulnérabilité et anticiper.

Sortir de la vulnérabilité revient à envisager la cybersécurité par le design de la *smart city*. Dès sa conception, la *smart city* doit veiller à sécuriser les données et les infrastructures et intégrer les nouveaux risques. Il s'agit de sécuriser les systèmes d'information par des choix techniques robustes conformément aux recommandations de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) ; par des choix d'organisation (externalisation, agilité) et par la formation et la sensibilisation des administrateurs et des utilisateurs, car l'humain est souvent le maillon faible. Il s'agit également de veiller à la sécurisation des objets connectés (IoT, capteurs, mobilier urbain connecté, etc.) qui sont les nouvelles portes d'entrée pour les pirates, grâce au développement attendu de la 5G.

(4) Le corpus comprend les textes explicatifs et les divers supports fournis par la Banque des territoires. Les extractions du site ont été réalisées le 3 mai 2021. Voir : https://www.banquedesterritoires.fr/smart-city-linnovation-ou-service-des-territoires

La deuxième préconisation est l'anticipation, car, selon la Banque des territoires, la cybersécurité devrait combiner la cyberdéfense et la résilience. Ainsi, la *smart city* doit favoriser la mise en place de procédures permanentes, notamment des tests pour sécuriser et repérer les failles des réseaux (cyberdéfense) et élaborer un plan de résilience numérique pour garantir la continuité du service en cas de cyberattaque, de sinistre ou encore de pandémie.

Nous en déduisons que le lien entre *smart city* et cybersécurité doit être repensé par les collectivités territoriales.

Repenser le lien entre smart city et cybersécurité

Les cyberattaques exploitent une ou plusieurs des vulnérabilités suivantes : la faiblesse de la sécurité dans le développement des logiciels ; l'utilisation de systèmes anciens non sécurisés et peu ou pas maintenus (superposition de technologies) ; des dispositifs numériques des villes intelligentes étendus, complexes et diversifiés, avec de nombreuses interdépendances ; de multiples vulnérabilités découlant de l'erreur humaine et de la malveillance ; hameçonnage pour collecter des informations clés qui facilitent l'accès. Ces vulnérabilités sont accentuées par un certain nombre de causes, notamment le fait qu'il est souvent difficile de savoir qui est responsable du maintien de la sécurité dans les systèmes et les infrastructures complexes lorsque plusieurs entreprises et parties prenantes collaborent à leur conception, fournissent du matériel et des logiciels, et exploitent et utilisent divers éléments. Cette situation est amplifiée en ce qui concerne la gestion urbaine, où les municipalités sont soumises à une pression croissante pour réaliser des économies.

Une récente étude de la Fédération nationale des collectivités concédantes et régies (2021) montre que 84 % des collectivités interrogées manquent de maturité. Elles ne perçoivent pas la cybersécurité comme un frein au lancement de projets de *smart city* et n'ont pas de vision d'ensemble. Repenser ce lien consiste à intégrer les aspects cybersécurité dès le *design* et démarrage d'un projet *smart city*, car le réaliser plus tard dans le projet pourrait s'avérer plus complexe et coûteux, et contraindrait probablement à ne pas pouvoir traiter tous les risques. Ceci nécessite de repenser l'organisation du projet vis-à-vis de la donnée et de la gouvernance de la sécurité très en amont. Les principes de sécurité doivent être définis à l'échelle globale du projet et pris en compte par chacun des sous-projets composant la *smart city*, en fonction de leurs contraintes. Cela est d'autant plus vrai que la *smart city* implique un grand nombre d'acteurs aux cœurs de métier, aux moyens et à la maturité en matière de cybersécurité différents. Une vision globale et partagée est indispensable pour s'assurer que chaque élément traite la donnée avec le niveau de sécurité adéquat [Deloitte, 2019 ; Efthymiopoulos *et al.*, 2016 ; Elmaghraby *et al.*, 2014 ; Laufs *et al.*, 2020].

Il convient ensuite de définir les grands principes d'architecture et d'interopérabilité, selon les contraintes inhérentes à la *smart city*, liées à l'*edge computing* et au déploiement d'objets en milieu hostile. La résilience du système doit être au cœur des exigences de sécurité, la chute ou la compromission d'un élément ne devant pas entraîner la chute de la totalité du système. Enfin, le mode de développement doit être agile [Sengan *et al.*, 2020].

La cybersécurité doit être incluse dans les processus de développement par la définition d'*Evil User Stories*, permettant d'identifier et de prendre en compte les risques à chaque évolution des services ou du système d'information, et par la nomination d'experts cybersécurité dans un rôle de support et de validation. La définition

Tableau 1 - *Smart city* et cybersécurité

A. Schéma d'intégration d'une politique de cybersécurité

Risques	Accompagnement	Contrôles
Traduire les contraintes de sécurité en besoin de sécurité pour le projet	Soutenir les équipes de développement et d'infrastructure dans la conception et l'implémentation des mesure de sécurité	Valider la résorption des risques de sécurité par des tests de sécurité

B. La protection de la smart city

I	II	III
Identifier les données et actifs critiques	Sécuriser les données	Prioriser les actions

PENSER LE LIEN *SMART CITY* ET CYBERSÉCURITÉ REVIENT À FAIRE ÉMERGER UNE NOUVELLE NOTION, LA CYBER RÉSILIENCE, QUI DEVRA PROBABLEMENT COMPTER COMME UN ÉLÉMENT FORT DE L'ATTRACTIVITÉ DES TERRITOIRES INTELLIGENTS DANS LE FUTUR.

et le maintien d'un niveau de sécurité satisfaisant passeront plus que jamais par l'intégration rigoureuse de la sécurité dans toutes les phases du projet, cela pouvant induire des investissements humains et technologiques plus importants mais nécessaires. L'accompagnement doit intégrer des *serious games*, des outils d'information intégrés.

Étant donné la propension de la *smart city* à collecter et traiter de grandes quantités de données, la protection passera en premier lieu par l'identification des données et des actifs critiques. La majorité des services proposés par la *smart city* sont à destination des citoyens. Par conséquent, des données identifiantes et ainsi potentiellement sensibles vont être collectées. Par ailleurs, une perte de disponibilité ou d'intégrité de certains services pourra avoir de graves répercussions étant donné que certaines composantes du système d'information ont une prise directe sur le monde physique. La *smart city* n'échappe pas aux réglementations, notamment au règlement général sur la protection des données (RGPD), mais aussi selon les usages au référentiel général de sécurité (RGS), à la loi de programmation militaire (LPM) ou à la directive européenne *Network and Information Security* (NIS), dont les exigences en matière de protection des données devront être intégrées dans les programmes. Des niveaux de classification de la sensibilité de la donnée doivent donc être formalisés afin de permettre la priorisation des actions et la mise en place de cadres de traitement des données critiques adaptés tels que le chiffrement et l'anonymisation. Le problème de l'accès aux données devra aussi être posé. Les acteurs de la *smart city* sont nombreux et il sera nécessaire de segmenter la « vision » qu'ils pourront avoir du système d'information. Cela passera par une phase préalable de définition des profils d'habilitations, nécessaires au respect du principe de moindre privilège, associée à une revue régulière de leurs affectations afin de s'assurer qu'elles soient toujours légitimes.

La continuité et la reprise d'activité devront être au cœur de la stratégie de sécurité. Il est nécessaire de mettre en place des plans formalisés et testés, incluant à la fois les considérations techniques, comme la résilience des différents systèmes, la capacité à restaurer des systèmes indépendamment des autres, la réalisation d'exercices de gestion de crise. Toutes les parties prenantes doivent garantir la mise en œuvre de moyens significatifs dans la protection des systèmes d'information impliqués et se conformer aux exigences de la politique de sécurité du projet. Ce qui impose un engagement contractuel, la formalisation et la mise en œuvre des plans d'assurance sécurité, notamment pour les prestataires les plus critiques, le contrôle régulier des installations, des comportements afin de s'assurer du maintien du niveau de sécurité dans le temps et adresser les futurs scénarios de risque.

Penser le lien *smart city* et cybersécurité revient à faire émerger une nouvelle notion, la cyber résilience, qui devra probablement compter comme un élément fort de l'attractivité des territoires intelligents dans le futur.

Une piste pour l'avenir : la cyber résilience

La cybersécurité joue un rôle essentiel dans l'atténuation des chocs et des stress en protégeant la confidentialité, l'intégrité et la disponibilité des données et des infrastructures activées par les données. Cependant, la sécurité seule ne suffit pas. La cyber-résilience va encore plus loin en veillant à ce que les systèmes TIC continuent de fournir des services en cas de faille de sécurité. Pour les villes, la cyber-résilience peut être comprise à travers leur capacité de préparation, de réponse et de réinvention. Les efforts visant à renforcer la cyber-résilience sont essentiels pour survivre et même potentiellement prospérer face aux cyberattaques ou aux catastrophes physiques.

Les villes ne seront jamais « sécurisées » à 100 % et ne pourront éviter complètement le danger. Mais elles peuvent être résilientes face à un large éventail de stress et de chocs en faisant les bons investissements, à la fois dans les domaines physiques et cybernétiques, pour se préparer aux crises, réagir pour rétablir la normalité, apprendre du nouveau *statu quo* et s'y adapter.

La cyber-résilience est la capacité des parties prenantes de la *smart city* non seulement à être préventives ou répondre à des événements de piratage et de violation de données, mais aussi à s'adapter et survivre rapidement à l'attaque [Baig *et al.*, 2017]. Pour faire face à de telles situations, les organisations doivent rendre leurs systèmes d'information suffisamment résilients pour qu'ils puissent résister et

rebondir après une attaque, par exemple en changeant ou modifiant en permanence les mécanismes de fourniture des services [Ahmadi-Assalemi *et al.*, 2020 ; Al Dairi *et al.*, 2017 ; Chen *et al.*, 2021].

La stratégie de cyber-résilience favorise la flexibilité et la robustesse des parties prenantes de la *smart city* et lui garantit de pouvoir résister aux cyberattaques, aux pannes et aux défaillances et continuer à fonctionner même dans un état dégradé ou affaibli.

La mise en œuvre de la cybersécurité et de la résilience de la *smart city* est complexe et devrait faire partie d'une planification préalable de la part des dirigeants. Une feuille de route pour la sécurité et la résilience doit être élaborée qui doit intégrer la vision et les valeurs de l'initiative globale de la *smart city* et déterminer les objectifs, les stratégies et les actions qui garantissent la sécurité, la résilience et la protection des données sur le territoire. Elle établit des structures et des processus pour une collaboration et une coordination solide dans la gouvernance.

La feuille de route aborde en outre les obstacles potentiels et détermine les étapes à franchir pour suivre et communiquer les progrès réalisés au cours de la mise en œuvre. Les éléments clés d'une feuille de route devraient inclure les sept étapes suivantes :

1. Définir une vision de la *smart city* ;
2. Assurer une large participation des parties prenantes ;
3. Cartographier les risques critiques et les interdépendances au sein de l'écosystème ;
4. Atténuer les risques et garantir la réalisation des avantages ;
5. Définir des niveaux adéquats de sécurité et de résilience ;
6. Adapter les structures de gouvernance ;
7. Garantir des décisions d'investissement éclairées.

Chaque ville est différente. Comprendre les menaces de cybersécurité importantes et uniques pour une ville particulière, ainsi que leur impact potentiel, est essentiel pour garantir que la ville puisse y répondre efficacement. Chaque ville s'appuie sur des services critiques et des informations sensibles qui, si elles étaient compromises, endommagées ou détruites, auraient un impact dramatique sur la capacité de la ville à fonctionner. Celles-ci doivent être identifiées puis hiérarchisées, ce qui implique souvent des compromis difficiles, mais il est essentiel que la ville puisse réagir efficacement en cas de crise. Par exemple, aux États-Unis, le National Institute of Standards and Technology (NIST) propose des ressources faisant autorité, notamment les *Standards for Security Categorization of Federal Information and Information Systems* et le cadre *Protecting Critical Infrastructure Cybersecurity.*

Une fois les menaces et les services critiques identifiés, la ville doit définir sa vision de la cyber-résilience. Sur cette base, elle peut s'engager dans un effort de collaboration pour fixer des objectifs qui décrivent les objectifs spécifiques qu'ils souhaitent atteindre. Ces objectifs peuvent inclure de garantir que la ville dispose d'une plate-forme de données ouvertes efficaces qui peut fournir des informations aux premiers intervenants en cas d'urgence (chocs aigus) ou d'aider les organismes sans but lucratif à mieux répondre aux besoins des résidents de la ville au quotidien (facteurs de stress constants).

Conclusion

Il est essentiel qu'une collaboration ait lieu entre les fournisseurs, les fabricants d'appareils et les gouvernements pour élaborer une réglementation plus stricte en matière de sécurité des technologies intelligentes. Les opérateurs des villes intelligents doivent chercher à comprendre bien en amont les problèmes de sécurité auxquels sont confrontés leurs environnements et systèmes s'ils veulent atténuer les risques avant que les incidents ne se produisent. Ce n'est qu'en gardant une longueur d'avance que les municipalités pourront pleinement profiter des avantages de la *smart city*, prévenir les défaillances techniques et se défendre contre la cybercriminalité.

En termes de résilience, pour les villes comme pour les organisations, la capacité à assurer la continuité des services pour la ville et les citoyens en cas de catastrophe, à se reconstruire rapidement et à prospérer après l'événement est devenue une notion vitale. La cyber-résilience va encore plus loin en veillant à ce que les systèmes continuent de fournir des services en cas de sinistre majeur.

La responsabilité de la mise en œuvre des *smart cities* incombera aux maires. Pourtant, leur expérience pratique en matière de gestion des systèmes complexes est faible. La coopération et la collaboration entre les villes et les États s'avéreront essentielles pour le bon fonctionnement des villes intelligentes, ainsi que pour l'acceptation et la confiance du citoyen dans la vision de la ville intelligente. Gageons que la cyber-résilience sera une composante forte de l'attractivité des territoires dans les prochaines années [Abusaada et Elshater, 2021] ■

DOCUMENT 3

synox.io - consulté le 29 novembre 2025

Rennes Métropole : territoire pionnier de l'Internet des Objets (IoT)

Rennes Métropole, pionnière de l'IoT depuis 2014, franchit un cap en 2025 avec le passage à l'échelle industrielle. En partenariat avec Synox qui a remporté l'appel d'offre public, la collectivité structure une plateforme souveraine pour piloter les bâtiments, gérer les crues et améliorer la qualité de l'air. Ce projet IoT multi-usages favorise l'interopérabilité, la mutualisation et l'autonomie des communes. Rennes s'affirme comme un modèle de territoire connecté, durable et résilient.

Industrialisation et passage à l'échelle

Rennes Métropole a pris très tôt le virage des objets connectés. Dès 2014, la collectivité a expérimenté un premier réseau LoRa baptisé « LoRa Fabian » *(oui, vous avez bien lu !)*, avant de basculer, dès 2016, en **portage métropolitain**, avec un objectif clair : démocratiser la donnée pour mieux piloter les services publics.

"On est sortis du cadre expérimental le 1er janvier 2025. On passe en mode industriel avec une offre de service structurée : d'un côté la connectivité, de l'autre un accompagnement clé en main pour les communes, centré sur la gestion bâtimentaire." – Pierre Renault, Chef de projet Data à Rennes Métropole

Des ambitions fortes pour un projet à impact

La gestion technique des bâtiments publics a été le point d'entrée. Mais très vite, les cas d'usage se sont diversifiés pour répondre à d'autres enjeux stratégiques : **efficacité énergétique, qualité de l'air, prévention des risques naturels...**
Avec Synox, Rennes Métropole s'appuie sur une **plateforme IoT interopérable et souveraine**, capable d'agréger des données issues d'un large écosystème (LoRa, Enedis, GRDF, GTB/GTC...). "L'enjeu clé, c'est de donner aux communes une vision unifiée de leur patrimoine, en consolidant une multitude de sources de données trop souvent cloisonnées."

98% des communes n'ont pas la capacité de gestion en interne. Il y a donc un réel sujet d'accompagnement de l'acteur public.

Anticiper les risques et généraliser l'usage de l'IoT

L'actualité climatique a confirmé l'importance d'une approche territoriale. Les crues majeures de 2024, inédites depuis 60 ans, ont déclenché une accélération des projets.

"On travaille à la mise en place d'un système d'alerte intelligent, en croisant nos données internes avec celles de Vigicrues. Et surtout, on veut rendre ces outils accessibles aux directions métiers."

Une démarche mutualisée avec l'écosystème breton

Fidèle à sa culture collaborative, Rennes Métropole échange régulièrement avec d'autres territoires pilotes, comme Lorient Agglomération ou Montpellier Méditerranée Métropole. La collectivité s'inscrit également dans les dynamiques de la **FNCCR**, et du **SDEF** en quête de retours d'expérience concrets.

Trois grands axes structurants

1. **Interopérabilité & standardisation des données** : pour gérer les données provenant de sources multiples.
2. **Transparence et communication** : pour valoriser les usages auprès des élus et citoyens.
3. **Montée en charge & consolidation** : pour généraliser l'IoT au-delà du bâtimentaire.
   "Aujourd'hui, nous avons entre huit et dix ans de recul. L'enjeu, c'est d'essaimer, massifier, et faire boule de neige avec les communes. On vise un déploiement multiplié par 100 en nombre de capteurs sur le réseau métropolitain, déjà conséquent."

Une collaboration stratégique avec Synox

Avec Synox, la métropole mise sur une **architecture souveraine et sécurisée**, couplée à une plateforme d'hypervision multi-cas d'usage. "On a besoin de partenaires capables de s'adapter à nos cas d'usage très concrets, et de nous aider à passer à l'échelle sans sacrifier la qualité ou l'interopérabilité."

Et demain ?
Qualité de l'air, gestion énergétique, confort des usagers, crues, stationnement... Rennes Métropole voit l'IoT comme un **vecteur de transition numérique, écologique et sociale**. Une approche pragmatique, fondée sur l'usage, la mutualisation et la réversibilité.

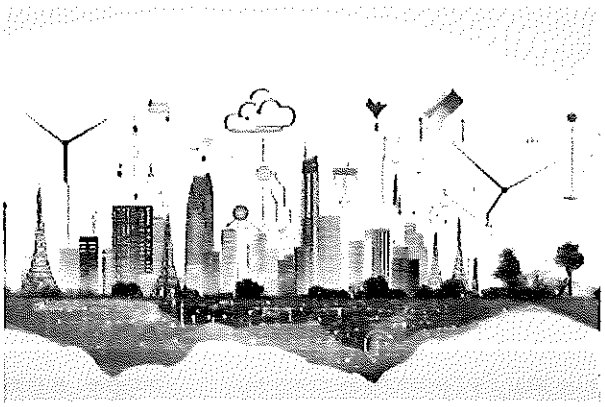
"L'IoT, ce n'est pas qu'un sujet technologique. C'est un levier de transformation publique, au service d'un territoire plus résilient et plus efficace."

la gazette·fr

DOCUMENT 4

A quelles conditions les objets connectés peuvent devenir un levier numérique pour la transition écologique

Publié le 13/06/2025



Adobe Stock

Vision politique et mutualisation doivent présider à la conception des réseaux d'objets connectés (IoT) déployés par les collectivités. Le but : faire du numérique un fil conducteur qui irrigue toutes les politiques publiques locales.

Sobriété énergétique des bâtiments, télérelève de la consommation d'eau ou d'électricité, gestion du stationnement et de l'éclairage public, gestion des flux touristiques, prévention des risques de submersion marine ou d'inondation, détection des feux de forêt… Les réseaux d'objets connectés (ou IoT pour « Internet of Things ») offrent des usages sans cesse plus nombreux et sont sources d'économies potentielles. En mars, le second Observatoire des territoires connectés et durables a montré qu'en déployant des solutions numériques reliées aux objets connectés, les collectivités pourraient économiser jusqu'à 1,5 milliard d'euros en 2035.

Mais « l'internet des objets, ce n'est pas seulement un outil technologique, expose Xavier Grawitz, vice-président du syndicat mixte Manche numérique, en ouverture de la première Biennale des objets connectés, le 4 juin à Granville (Manche). Se lancer dans un projet IoT est aussi un acte politique. C'est une nouvelle manière d'exercer nos compétences, qui rend notre action plus précise, plus réactive, plus durable, et c'est une opportunité d'égalité territoriale, en offrant des services adaptés aux réalités de terrain ».

Pour le département de la Manche, à dominante rurale et au territoire littoral maritime très étendu, Xavier Grawitz cite plusieurs exemples : optimiser la gestion de l'eau qui est précieuse dans les zones agricoles, alerter sur le niveau de remplissage des bennes à ordures pour rationaliser les tournées de collecte, suivre la consommation énergétique des bâtiments publics ou encore mieux orienter les investissements et réduire les charges pour les ports. Il convient d'adopter une « vision politique claire » et de considérer le numérique comme un fil conducteur qui irrigue toutes les politiques : eau, déchets, mobilité, santé, éducation, transition écologique…

Mutualisation poussée

Loin d'être un gadget connecté, c'est un enjeu de gouvernance territoriale, de méthode et de coopération, estime l'élu qui prône aussi une mutualisation poussée : infrastructures, plateformes de collecte et de traitement des données, compétences juridiques, capacité à expérimenter... Sans soutien, une collectivité isolée aura du mal à lancer un projet d'objets connectés durable.

Mais, « portée par un syndicat mixte comme Manche numérique qui est une structure fédératrice, chaque intercommunalité peut bénéficier d'une feuille de route claire, d'un accompagnement sur mesure et surtout, d'un modèle économique soutenable », argumente le vice-président.

« Partout en France, on est exposés à des problématiques de stress hydrique, de gestion et d'optimisation de ressources », explique Morgan Hervé, directeur de Haute-Garonne numérique, à la tête du projet de réseau IoT bas débit Ligam (« lien » en occitan). « Le réseau peut être la pierre angulaire pour repenser les politiques publiques », autour des crises climatiques ou de la modernisation des services publics notamment.

« Et il faut un vrai portage politique », pour montrer qu'il ne s'agit pas de gadgets, conclut Morgan Hervé, affirmant qu'il est nécessaire de « transformer les décideurs pour qu'ils prennent conscience de l'importance de ces projets ».

Avec l'aide d'Ubicité, qui l'accompagne depuis cinq ans, Manche numérique a voté à l'unanimité un schéma directeur des objets connectés (SD-Roc) qui analyse le côté technique, le business plan, la faisabilité et l'acceptabilité du projet.

Car comprendre ces sujets techniques n'est pas toujours simple pour les élus communaux et intercommunaux. C'est pourquoi « il faut leur parler leur langage », estime Xavier Grawitz. C'est-à-dire, leur expliquer l'utilité concrète du réseau : usages et économies envisageables, amélioration du service public. Tout en leur offrant « un cadre clair et fédérateur ».

Même position pour Jérémie Gachelin, responsable innovation, données et usages à Lorient agglomération (25 communes, 213 310 habitants), pour qui « il faut voir les cas d'usage avec les élus et inscrire le projet dans une politique de territoire ».

Plan « France territoires durables et connectés »

Ce que confirme Ariel Turpin, délégué général de l'Avicca : « la technologie doit se mettre au service d'un projet politique de territoire, pour plus de sobriété, d'efficience et de mieux-vivre. Nous profitons de chaque occasion pour marteler la nécessité de baser un projet IoT sur la mutualisation, car aucun acteur ne porte toutes les stratégies. Il faut mobiliser les élus et les convaincre de l'efficacité et de l'intérêt économique du réseau ».

L'Avicca travaille sur le sujet depuis 2016, et propose des ateliers dédiés à ses adhérents. Convaincue que c'est la vision politique qui compte, l'association d'élus a rapidement compris qu'il fallait « sortir d'un discours techno-centré pour revenir à plus de pragmatisme ». En effet, « la standardisation et la normalisation avancent plus vite que les usages et les services et elles sont souvent internationales, et donc en décalage avec le terrain », a poursuivi Ariel Turpin.

Le défi consiste maintenant à passer de l'expérimentation à la généralisation, notamment dans les territoires peu denses. L'Avicca porte, auprès de l'État et de l'écosystème numérique, une proposition de plan « France territoires durables et connectés », sur le modèle du plan France très haut débit. Objectif : donner la priorité à des usages qui allient transition écologique et transformation numérique, avec un guichet ouvert en permanence (au lieu d'appels à projets multiples), un cahier des charges précis qui prenne en compte les dernières avancées techniques au fil de l'eau et une gouvernance partagée État-collectivités.

L'Avicca espère que le futur programme Transformation numérique des territoires inclura des thèmes tels que la cybersécurité, les infrastructures, les données (data), le numérique responsable... L'information devrait être donnée lors d'un « Roquelaure du numérique » — initialement prévu le 10 juin, il a été reporté *sine die*.

« Périmètre des dispositifs de l'internet des objets vis-à-vis des technologies de l'information et des communications » (extrait)

(...)

2.1.2. Dispositifs connectés et dispositifs IoT

a) Dispositifs connectés

Les dispositifs connectés sont des appareils électroniques grand public, des appareils électroménagers et d'autres équipements, y compris à des fins industrielles, qui peuvent interagir avec leur environnement distant ou proche. Si, jusqu'à récemment, seuls quelques dispositifs étaient généralement connectés aux réseaux de communication, une variété croissante de dispositifs, d'appareils et d'infrastructures grand public et industriels dans tous les secteurs sont connectés à Internet et entre eux, ce qui est rendu possible par la diffusion généralisée de l'Internet haut débit, ainsi que de l'accès sans fil et mobile.

Dans son rapport « *Digitalization & Energy* » [AIE – 2017], l'AIE emploie la classification suivante pour les dispositifs connectés : « *En parlant de la consommation d'énergie des dispositifs connectés (en tant que segment des TIC), il est utile de distinguer deux types de dispositifs connectés : les « équipements électroniques de périphérie », dont la fonction principale est le stockage / l'utilisation des données, tels que les ordinateurs portables et les smartphones, et « d'autres équipements de périphérie », dont les fonctions principales ne sont pas liées aux données, tels que les appareils de cuisine et les voitures connectés* ».

b) Dispositifs IoT

Selon [UIT-T Y.2060], en ce qui concerne l'Internet des objets, un dispositif IoT est un équipement doté de capacités de communication obligatoires et de capacités facultatives de détection, d'actionnement, de saisie de données, de stockage et de traitement de données.

Le facteur déterminant d'un dispositif IoT est qu'il peut effectuer un certain type de traitement numérique et, grâce à ses capacités de communication, peut être identifié et intégré dans des réseaux de communication. C'est ce qui le distingue des appareils physiques (électroniques) ordinaires qui ne sont dotés que de quelques circuits et éventuellement d'une pile ou batterie. Parmi ces dispositifs IoT citons les stimulateurs cardiaques, les terminaux de point de vente, les réfrigérateurs intelligents, les vélos intelligents, les moniteurs d'activité, les compteurs électriques intelligents, les terminaux de stationnement intelligents, etc.

NOTE 1 : Bien que les termes systèmes IoT / dispositifs IoT soient parfois utilisés de manière interchangeable, les dispositifs IoT font partie d'un système plus vaste pour un cas d'utilisation donné. En permettant à un stimulateur cardiaque de communiquer avec le monde extérieur via une passerelle, par exemple en transmettant des données de rythme cardiaque à une base de données centrale, tous ces biens (y compris le réseau) se transforment en un système IoT.

NOTE 2 : Les capacités de communication d'un dispositif IoT peuvent être utilisées par le dispositif pour se connecter à Internet ou non. Les capacités de communication peuvent inclure la communication via des réseaux sans fil ou fixes (tels qu'Ethernet, Profibus, Profinet).

Les étapes générales de fonctionnement d'un terminal IoT, en ce qui concerne les données, comprennent l'acquisition, le traitement, le stockage et la transmission des données. La première et la dernière étape existent sur tout dispositif IoT, tandis que le traitement et le stockage peuvent exister ou non dans certaines applications.

[UIT-T Y.4460] dérive des modèles de référence architecturaux pour les trois types d'équipements IoT mentionnés dans la Figure 3. Les modèles de référence architecturaux définissent les principales entités fonctionnelles du dispositif IoT et peuvent servir de conception de référence pour la mise en œuvre du dispositif IoT.

NOTE : Les modèles de référence architecturaux définissent les principales entités fonctionnelles « logiques » du dispositif IoT et peuvent servir de conception de référence pour la mise en œuvre du dispositif IoT. Cependant, d'un point de vue

matériel, ces entités « logiques » fonctionnelles doivent être mappées sur des entités « matérielles » fonctionnelles (car différentes entités « logiques » fonctionnelles peuvent être exécutées par la même entité « matérielle » ou une entité fonctionnelle « logique » donnée peut être exécutée par plus d'une entité « matérielle »).

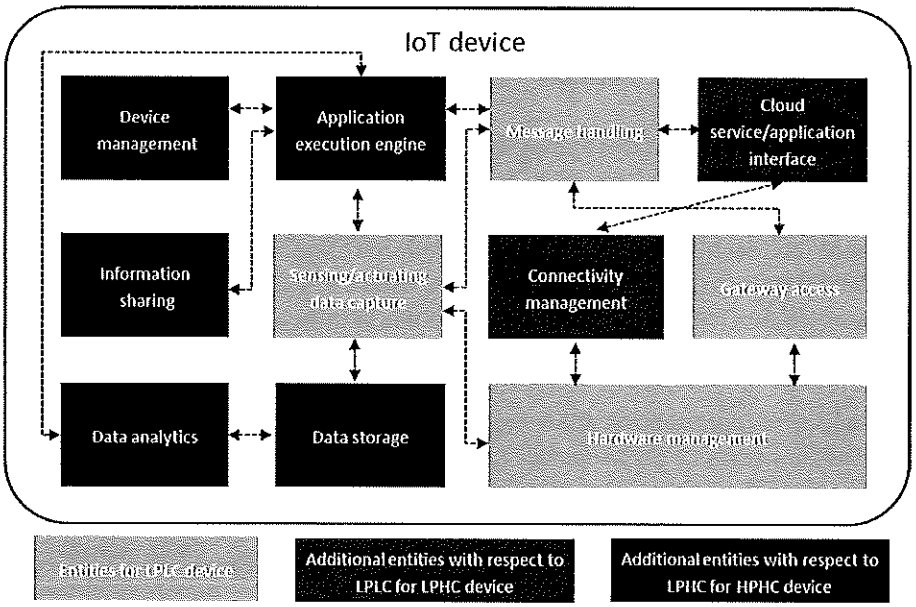


Figure 3 – Modèle de référence architectural montrant les entités logiques fonctionnelles des trois types d'équipements IoT du point de vue de leurs capacités de traitement et de communication selon la norme [UIT-T Y.4460].

Exigences pour la qualification IoT

La Figure 4 illustre une architecture générique de haut niveau d'un dispositif connecté au sein de l'IoT interagissant avec l'infrastructure TIC (réseaux et centres de données). Un dispositif connecté est constitué d'un dispositif d'hébergement (par exemple l'appareil électroménager) embarquant un ou plusieurs dispositifs IoT, qui peuvent être représentés de manière modulaire (*firmware* du dispositif IoT / logiciel embarqué, module microcontrôleur, module de détection, alimentation, ...). Le module de connectivité est composé de plusieurs puces de communication et d'un micrologiciel de connectivité. Dans la Figure 4, les réseaux de communication offrent des capacités de transfert de données fiables et efficaces. L'infrastructure du réseau IoT peut être réalisée par le biais de réseaux existants, tels que les réseaux TCP / IP conventionnels, et / ou de réseaux évolutifs, tels que les réseaux de nouvelle génération (RNG) [b-UIT-T Y.2001].

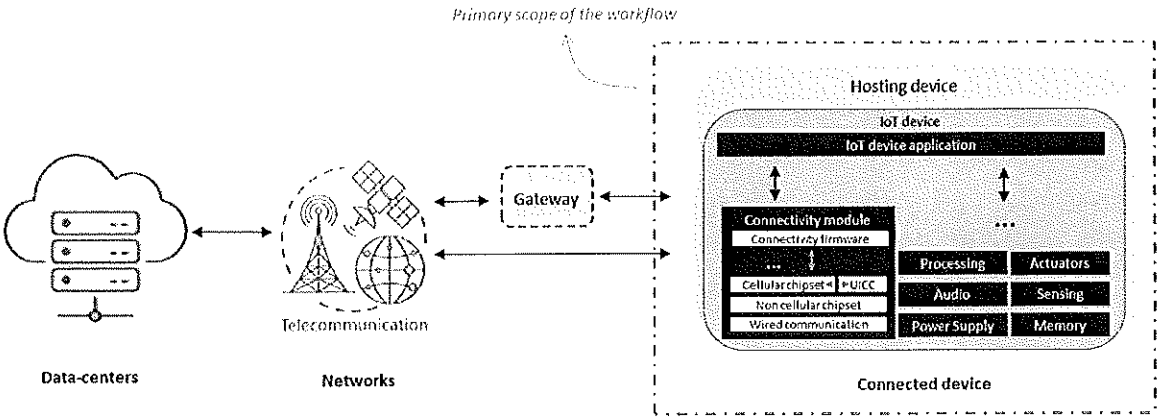


Figure 4 – Illustration d'un dispositif connecté au sein de l'IoT

Modèle de référence IoT [UIT-T Y.2060] : La Figure 5 présente le modèle de référence de l'IoT. Ce modèle comprend quatre couches auxquelles sont associées des capacités de gestion et de sécurité. Les quatre couches sont les suivantes :

- Couche application ;
- Couche de prise en charge des services et des applications ;
- Couche réseau ;
- Couche dispositif.

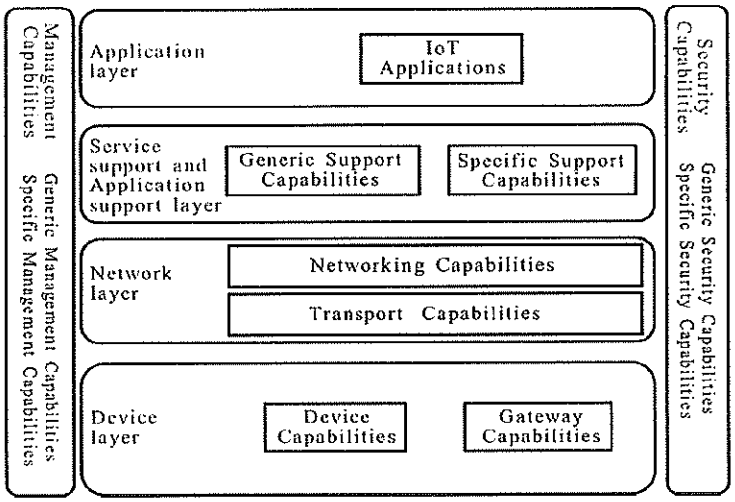


Figure 5 – Modèle de référence de l'IoT [UIT-T Y.2060]

Conformément à la [UIT-T Y.2060], une infrastructure IoT comprend les éléments essentiels suivants, ce qui permet une caractérisation initiale d'une solution IoT :

(1) L'application de dispositif IoT et l'application IoT hébergée sur une plateforme de services IoT (par exemple, un serveur situé dans un centre de données) ou au sein d'un équipement d'exposition des capacités (*Device Capabilites Exposure* (DCE)) du dispositif IoT interagissent ensemble dans le cadre de la couche application de la solution IoT.

(2) Réseau de communication reliant la plateforme de services IoT soit directement au dispositif connecté à l'IoT, soit à une passerelle, qui effectue la traduction nécessaire entre les protocoles utilisés dans le réseau de communication et ceux utilisés par le dispositif IoT. Ce réseau de communication fait partie de la couche réseau de la solution IoT et doit être

conforme ou similaire à la couche 3 du modèle OSI[6] (par exemple, le transfert et le routage de paquets utilisant généralement l'IP avec éventuellement des technologies d'accès radio comme la 4G, la 5G).

(3) Connectivité basée sur l'identification : La connectivité entre un objet (c'est-à-dire IoT) et l'IoT est établi en fonction de l'identifiant (unique) de l'objet.

NOTE : L'identification est une caractéristique importante pour être qualifié de dispositif IoT. Dans le cadre de la version 19, le 3GPP travaille sur l'intégration de dispositifs IoT basés sur l'alimentation ambiante dans les réseaux cellulaires 5G / 6G (appelés « Ambiant IoT ») avec des capacités et des cas d'utilisation équivalents aux terminaux RFID / NFC.

(4) Différentes topologies et structures de réseau peuvent être envisagées sous l'égide de l'IoT, notamment : les réseaux ad-hoc, les réseaux de dispositifs avec communications directes, les réseaux de dispositifs limités isolés ou connectés, etc. Dans le cas d'un réseau de dispositifs contraint tel que spécifié dans la [UIT-T Y.4451], une « couche d'adaptation » dans la pile de protocoles est nécessaire pour émuler les fonctions généralement liées aux architectures de réseau et aux caractéristiques de réseau (telles que la compression d'en-tête de paquet, la fragmentation de paquets, l'adressage de réseau...).

(5) Selon la norme UIT Y.2060, « les dispositifs IoT peuvent, par exemple, communiquer avec d'autres dispositifs au moyen d'une liaison directe sur un réseau local (c'est-à-dire un réseau assurant une connectivité locale entre les dispositifs eux-mêmes et entre ceux-ci et une passerelle, comme un réseau ad-hoc) ». Dans ce cas, la solution doit être conforme à l'architecture de référence de l'IoT DCE telle que spécifiée dans la Recommandation UIT-T Y.4115 [UIT-T Y.4115].

L'ensemble complet des exigences communes de l'IoT est détaillé dans la Recommandation UIT-T Y.2066[7]. Outre les Recommandations UIT-T susmentionnées, le praticien peut se référer à des exigences plus spécifiques pour les cas d'utilisation liés aux :

- Dispositifs portatifs IoT (IoT grand public) : Se référer à la Recommandation UIT-T Y.4117[8].
- Dispositifs IoT industriels : Se référer à la Recommandation UIT-T Y.4003[9].
- Dispositifs IoT pour l'automobile et les systèmes de transport intelligent (ITS) : Se référer à la Recommandation UIT-T Y.2281[10].
- Dispositifs IoT communiquant par lumière visible : Se référer à la Recommandation UIT-T Y.4465[11] et à la Recommandation UIT-T Y.4474[12].

[6] Modèle d'interconnexion des systèmes ouverts

[7] https://www.itu.int/rec/T-REC-Y.2066-201406-I / en

[8] https://www.itu.int/rec/T-REC-Y.4117-201710-I / en

[9] https://www.itu.int/rec/dologin_pub.asp?lang=s&id=T-REC-Y.4003-201806-I!!PDF-E&type=items

[10] https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-Y.2281-201101-I!!PDF-E&type=items

[11] https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-Y.4465-202001-I!!PDF-E&type=items

[12] https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-Y.4474-202008-I!!PDF-E&type=items

Catégories d'équipements IoT

Les dispositifs IoT peuvent être classés selon différentes perspectives :

- Les dispositifs IoT peuvent être classés en fonction **de la manière dont un dispositif interagit avec les objets physiques** (équipement d'accueil). Selon la [UIT-T Y.2060], 4 types canoniques sont identifiés : dispositifs porteurs de données, dispositifs de capture de données (exemples : lecteurs infrarouges, lecteurs de cartes, lecteurs de codes-barres...), dispositifs de détection et d'actionnement (exemples : capteurs et actionneurs) et dispositifs généraux (où des capacités de communication et de traitement sont intégrées dans le dispositif), y compris les équipements et les appareils pour différents domaines d'application de l'IoT, tels que les machines industrielles, les appareils électroménagers et les smartphones.

Figure 6 illustre les 4 types mentionnés et leur relation avec l'objet physique.

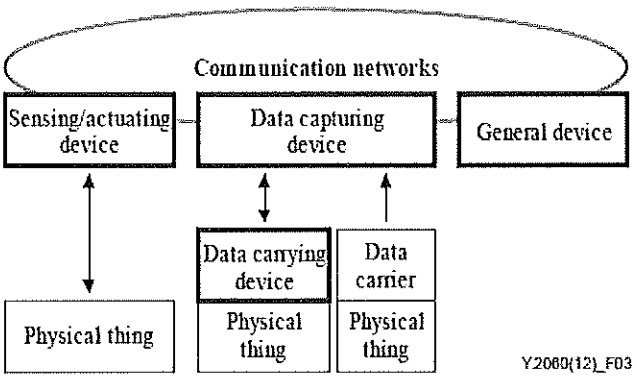


Figure 6 – Les différents types de dispositifs et leurs relations avec les objets physiques [UIT-T Y.2060]

- Les dispositifs IoT peuvent être classés, **d'un point de vue architectural, en fonction de la puissance de traitement (calcul) et de la communication**, deux capacités qui sont parmi les plus essentielles. En corrélant ces deux capacités, la norme UIT-T Y.4460 identifie 3 types de dispositifs : les dispositifs à faible capacité de traitement et à faible connectivité (LPLC – par exemple, les capteurs contraints), les dispositifs à faible capacité de traitement et à haute connectivité (LPHC – par exemple, les dispositifs dans les applications domestiques intelligentes) et les dispositifs à capacité de traitement élevée et à haute connectivité (HPHC – par exemple, une caméra de surveillance à IA intégrée).

NOTE 1 : Comme la capacité de connectivité dépend également de la capacité de traitement, la combinaison d'une capacité de traitement élevé et d'une faible connectivité n'est pas usuelle (car en général, un dispositif qui a déjà une capacité de traitement élevée aura également des capacités de connectivité élevées) conformément à la [UIT-T Y.4460].

NOTE 2 : En ce qui concerne l'Internet des objets, les dispositifs sans capacité de traitement sont des dispositifs IoT passifs (terminaux à faible coût sans microcontrôleurs) tels que les étiquettes d'identification basées sur NFC / RFID.

L'IoT au sein de l'ensemble plus large des dispositifs connectés

Il convient de noter que tous les produits connectés ne sont pas des produits IoT. Les produits TIC, les produits M&D, les produits IoT et les produits connectés peuvent se chevaucher mais font référence à des types de produits distincts, comme illustré dans Figure 7.

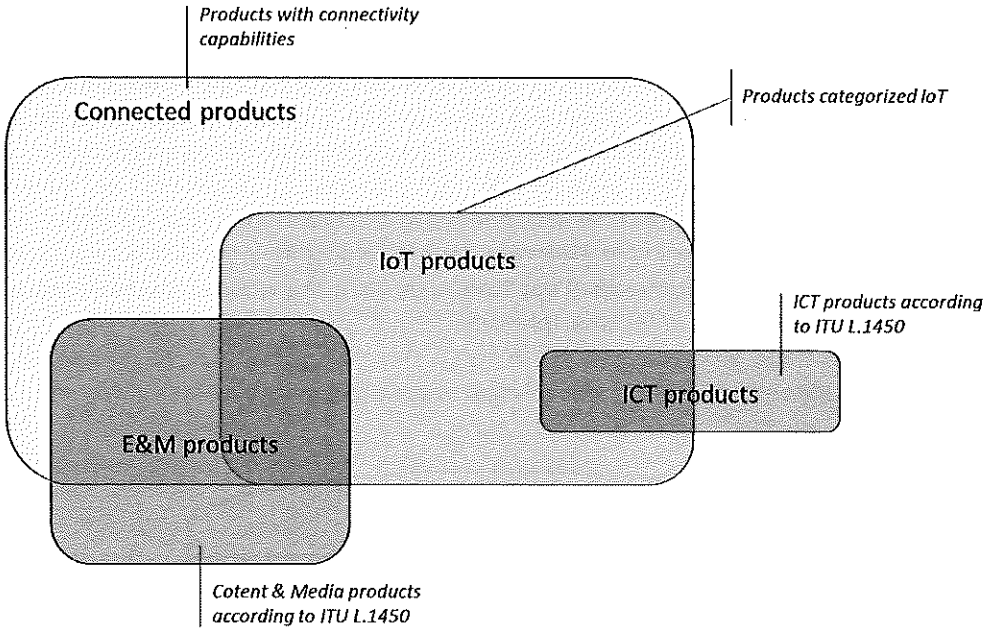


Figure 7 – Cartographie des différents types de produits : produits connectés, produits IoT, produits TIC et produits M&D (la taille de chaque article ne reflète pas la taille du marché concerné)

NOTE : Fixer le périmètre exact des secteurs des TIC et du M&D en ce qui concerne les produits IoT et les produits connectés est complexe. Au moment de la publication de la Recommandation UIT-T L.1450 (2014), il a été considéré comme « facultatif » d'inclure la connectivité intégrée dans le périmètre des TIC, mais à mesure que ce secteur se développe, cela pourrait faire l'objet d'un examen plus approfondi.

2.1.3. Produits connectés et systèmes de produits connectés : l'importance de fixer le périmètre

Comme le montre la cartographie de la Figure 7, il existe de nombreuses sous-catégories possibles pour un produit connecté (M&D et IoT, uniquement IoT mais ni M&D ni TIC, etc.). En outre, comme indiqué dans l'introduction du présent rapport, la numérisation croissante peut conduire à des systèmes complexes composés de plusieurs produits connectés. Ainsi, lorsqu'il aborde un système de produits connectés, le praticien doit prendre soin des limites utilisées car cela peut avoir un impact sur le résultat de la classification.

2.2. Approche méthodologique

Le flux de travail s'effectue selon les étapes suivantes :

(1) Décrire les approches suivies de cinq études sélectionnées pour la catégorisation des dispositifs connectés (par rapport au secteur TIC ou aux secteurs TIC/M&D) et les choix d'allocation pour la comptabilité carbone ;

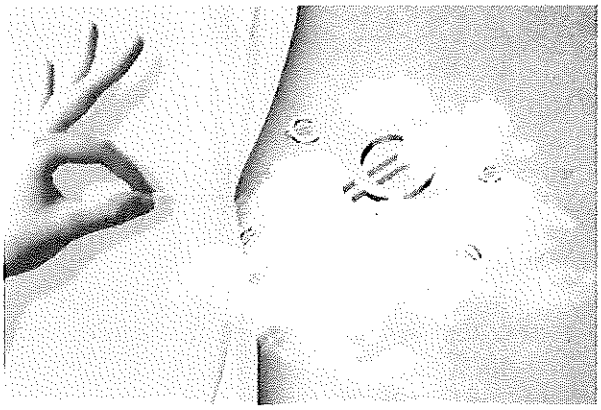
(...)

la gazette.fr

DOCUMENT 6

Grâce aux objets connectés, les collectivités pourraient économiser 1,5 milliard d'euros en 2035

Publié le 17/03/2025



sergey-nivens-adobestock

Chiffres à l'appui, le second Observatoire des territoires connectés et durables, présenté le 17 mars, montre l'impact des solutions numériques sur les transitions écologique et économique des collectivités. À condition que des structures de mutualisation incitent un maximum de communes à les adopter.

Les solutions numériques reliées aux objets connectés (IoT) pourraient accélérer la transition écologique et optimiser la dépense publique, selon l'Observatoire des territoires connectés et durables 2025, présenté le 17 mars à Paris. Pour cette seconde édition, la Fédération nationale des collectivités concédantes et des régies (FNCCR) et InfraNum se sont projetés à l'horizon 2035. Avec, pour objectif, de tenter d'évaluer les bénéfices dans cinq secteurs prioritaires : eau, déchets, éclairage public, gestion énergétique des bâtiments, détection des incendies.

L'étude, réalisée par les cabinets Tactis et Releaf Carbon, simule les gains économiques et environnementaux attendus à l'échelle nationale à travers plusieurs scénarios, combinant la capacité d'un territoire à mener un projet « intelligent » et le nombre de départements impliqués à terme.

« Connecter les territoires permet des économies dans le temps pour le service public, diminue l'empreinte carbone et accompagne les engagements d'impact environnemental, précise Ilham Djehaich, présidente d'InfraNum et directrice générale d'Altitude Infra THD. En 2024, le premier observatoire visait à justifier que le numérique était la technologie qui permettait aux territoires de se connecter et de développer leurs usages. Depuis un an, les projets se sont multipliés. L'observatoire 2025 montre de manière chiffrée qu'on peut faire plus avec moins, sur deux volets, l'économie et l'empreinte environnementale ».

Les résultats apportent une vision concrète du retour sur investissement. « Par exemple, entre les coûts évités et les bénéfices obtenus grâce à la télé-relève des compteurs d'eau, les simulations montrent que, chaque année, 320 piscines olympiques pourraient être économisées par département », illustre Ilham Djehaich. Quant à la détection des incendies, elle préserverait 42 500 hectares de forêt, offrirait entre 1 et 5% de gain de temps par an aux pompiers, sans compter l'impact humain.

Au total, en prenant l'hypothèse de vingt-cinq départements concernés en 2035, les économies pourraient atteindre près d'un milliard et demi d'euros pour les cinq cas d'usage analysés :

1. télé-relève des compteurs d'eau,
2. mesure en temps réel de la consommation énergétique des bâtiments,
3. pilotage de l'éclairage public à distance,
4. optimisation des points d'apport volontaires (sondes de remplissage, mesures à distance),
5. détection des incendies par des caméras installées sur des points hauts.

Mutualiser les infrastructures

L'étude montre aussi l'importance de mutualiser les projets de territoires connectés et durables pour inciter les collectivités, en particulier les communes, à adopter ces solutions numériques territoriales. Une mutualisation qui passe par des infrastructures et services largement accessibles, afin de réduire les coûts, limiter la multiplication des réseaux et garantir « un numérique sécurisé et maîtrisé ».

« L'extrapolation de l'observatoire, à l'échelle nationale et à dix ans, peut toutefois masquer certaines dynamiques locales sur le plan qualitatif », constate Loïc Haÿ, conseiller technique à la FNCCR. Très attaché à la nécessité de mutualiser les infrastructures, il explique que la démarche peut s'engager dès l'échelon intercommunal : une métropole peut lancer un projet pour couvrir ses besoins, avant d'entraîner l'ensemble des communes, pour des cas d'usage qui correspondent à leurs propres compétences.

Ainsi, Rennes métropole développe, dans le cadre du réseau privé bas débit LoraWan du Pays rennais, une offre de gestion énergétique des bâtiments destinée aux collectivités. La métropole a créé un premier réseau de capteurs pour satisfaire ses besoins métiers : points d'apport volontaires, consommations d'énergie (gaz, électricité), qualité de l'air intérieur, confort thermique des locaux... Dans un second temps, elle ouvre son réseau aux communes et acteurs publics locaux, à travers le dispositif Ecodata. Une offre « clé en main », avec un accompagnement technique. Actuellement constitué de 5 000 capteurs, installés sur du mobilier urbain et des bâtiments publics et connectés à 72 antennes, le réseau devrait en compter 57 000 en 2035.

« La question se pose de l'échelle pertinente pour déployer et généraliser une offre numérique. C'est sans doute dans un projet commun piloté par des structures d'envergure départementale que l'on pourrait embarquer l'ensemble des acteurs métiers d'un territoire », explique Loïc Haÿ. À la manœuvre : un syndicat numérique, un syndicat énergie ou encore un syndicat à double casquette numérique et énergie. « C'est à cette échelle départementale, avec des syndicats métier, que l'approche mutualisée a le plus de chance d'entraîner un maximum d'acteurs et d'avoir le plus grand impact économique », confirme le conseiller technique de la FNCCR.

Avec, pour déclencheur, le fait de disposer d'une infrastructure bas débit mutualisée, maîtrisée par la puissance publique. En effet, « la valeur des territoires connectés et

durables n'est pas technologique. Elle est dans l'usage et dans la démultiplication des usages métiers qui entraînent le maximum d'acteurs d'un territoire où la mutualisation sera d'autant plus gagnante », ajoute Loïc Haÿ.

Avancer pas à pas, de manière itérative

Pour mener un projet de territoire connecté durable mutualisé, il faut avancer « pas à pas de manière itérative » et non avec un marché global à très long terme. La mutualisation doit se faire « main dans la main entre le public et le privé », ainsi qu'entre acteurs publics selon une approche pragmatique, adaptée aux besoins, en adéquation avec les moyens de la ou des collectivités qui portent les projets et celles qui en bénéficient.

Mais attention, prévient Loïc Haÿ, il convient d'avoir la pleine maîtrise des solutions et des données territoriales utilisées (souveraineté). « L'IoT est une nouvelle source de données à intégrer dans la stratégie data des territoires. Il faut bétonner les aspects cyber, gestion de la donnée et interopérabilité des systèmes de données ».

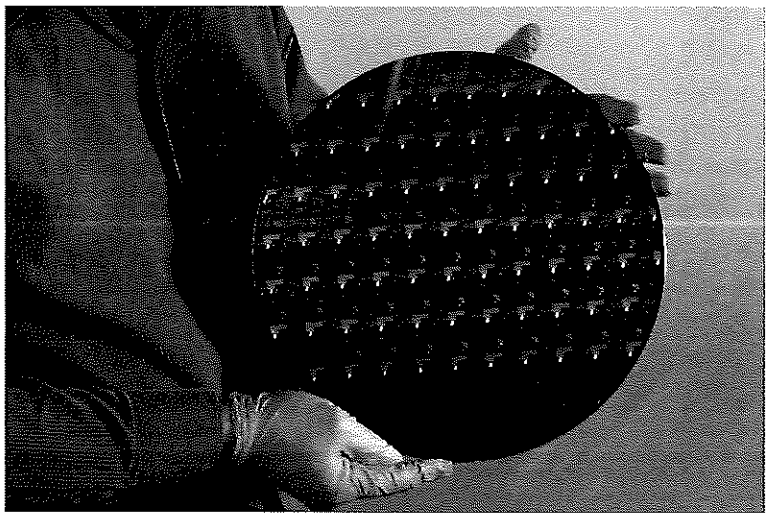
Focus

Évaluation simplifiée

Avec la méthode d'évaluation simplifiée de l'Observatoire, les collectivités peuvent identifier immédiatement la pertinence d'un projet : impacts économiques, environnementaux et sociaux. Les analyses prospectives reposent sur des données terrain, collectées lors d'entretiens et de séances de concertation, menés auprès de collectivités et d'industriels. Une quinzaine d'entretiens et des comités d'experts, composés de collectivités et d'industriels, ont permis de définir les hypothèses-clés du modèle.

Souveraineté numérique, entre mythe d'indépendance et réalité industrielle

Si la souveraineté numérique était totale, elle commencerait dans une mine et finirait dans nos appareils électroniques. Car derrière l'injonction à "l'indépendance numérique", il y a une réalité industrielle faite de chaînes d'approvisionnement mondialisées et de rapports de force économiques. Dans un contexte international explosif, cette évidence prend une dimension nouvelle. L'Usine Digitale propose un état des lieux.



IBM

L'Europe est un grain de sable dans l'industrie mondiale des nouvelles technologies. Mais le sable qui compte, celui du silicium, elle en maîtrise très peu. Pour les semi-conducteurs, l'Europe représente moins de 10% de la production mondiale, loin derrière l'Asie et les Etats-Unis. Sur les métaux critiques nécessaires à l'électronique, le constat est le même : la Chine concentre près de 70% de l'extraction mondiale.

Pour des métaux, comme le cobalt, essentiel à la fabrication des batteries et de certaines puces, plus de 70% de la production mondiale vient de la République démocratique du Congo. Même le lithium, surnommé "l'or blanc", est majoritairement extrait en Australie et en Amérique du Sud.

La chaîne industrielle échappe à l'Europe

Et ce n'est que la première étape. La fabrication et la transformation de ces matières premières échappent largement à l'Europe. Ainsi, la quasi-totalité du raffinage des terres rares et des métaux critiques se fait en Chine. Et les usines de fabrication de puces les plus avancées - indispensables entre autres pour l'intelligence artificielle - sont massivement situées à Taïwan et en Corée du Sud.

La dépendance est tout aussi massive sur le software. En Europe, plus de 70% du marché du cloud est capté par trois géants américains : Amazon Web Services (AWS), Microsoft Azure et Google Cloud. Et que dire des applications elles-mêmes ? Que vous préféreriez Android ou iOS, Windows ou MacOS (ou même Red Hat), Office 365 ou Google Workspace, Salesforce ou HubSpot... Vous utilisez des technologies américaines.

Les chiffres sont édifiants : 80% des dépenses européennes en logiciels et services cloud à usage professionnel sont réalisées auprès d'entreprises américaines, soit un volume d'environ 264 milliards d'euros par an. Ces flux économiques correspondent à près de 2 millions d'emplois directs, indirects et induits aux États-Unis.

Le software massivement américain

Autrement dit, l'Europe importe non seulement les matières premières essentielles à ses industries numériques mais elle ne maîtrise pas non plus les étapes industrielles les plus sensibles de leur transformation, et à la fin est même dépendante de logiciels étrangers. Dans ces conditions, parler de souveraineté numérique "totale" n'a pas de sens : sans contrôle sur les composants matériels et sans contrôle sur les briques logicielles, il n'y a pas d'autonomie numérique possible.

L'essor du Software-as-a-Service (SaaS) n'a pas arrangé les choses. A l'époque des licences perpétuelles, des sanctions imposées à la va-vite puis retirées trois jours plus tard (comme se plaît à le faire le gouvernement américain) n'auraient pas eu de réel impact sur les entreprises clientes. Aujourd'hui, un fournisseur SaaS pourrait se retrouver forcé de couper l'accès à tous ses clients, sans contournement possible pour ces derniers.

Le contexte international le montre tous les jours et avec encore plus de force ces derniers temps. Les Etats-Unis utilisent de plus en plus ouvertement les droits de douane, les restrictions d'exportation et les contrôles technologiques comme des instruments de politique étrangère.

La Chine en fait de même sur les terres rares et certains métaux critiques. Depuis 2023, elle a instauré des contrôles sur l'exportation de gallium et de germanium, deux métaux essentiels aux semi-conducteurs, dont elle contrôle l'essentiel de la production mondiale.

Une réalité face à laquelle il faut composer

Face à cette réalité, les entreprises européennes doivent composer. Pour OVHcloud, cela signifie contrôler le "stack" logiciel et matériel de l'infrastructure cloud. "*La souveraineté technologique, c'est qui maîtrise la technologie de la solution que je vais utiliser*", détaille Caroline Comet-Fraigneau, chief revenue officer au sein de l'entreprise roubaisienne, à *L'Usine Digitale*.

OVHcloud a ainsi investi dans deux sites de fabrication de serveurs - l'un à Croix dans le nord de la France, l'autre au Canada - afin de conserver une autonomie industrielle dans l'intégration des composants. Mais l'entreprise reconnaît les limites de cette

autonomie : "*nous ne sommes pas complètement souverains parce qu'à un moment, nous sommes bien obligés d'acheter des composants électroniques*".

Protéger les données des autorités étrangères

OVHcloud met aussi en avant la souveraineté des données stockées. "*La souveraineté des données, c'est où sont localisées mes données... mais aussi à quelles lois extraterritoriales elles sont potentiellement soumises*", note Caroline Comet-Fraigneau. "*By design, en tant qu'entreprise européenne, on propose une souveraineté sur toutes nos offres*", poursuit-elle.

Cette revendication vise directement des lois comme le CLOUD Act, une réglementation américaine autorisant - sous certaines conditions - les autorités de surveillance à accéder aux données stockées par les fournisseurs américains quelle que soit leur localisation.

SecNumCloud, de la cyber à la souveraineté

Pour attester qu'une offre n'est pas soumise à des lois étrangères, la France s'est dotée d'un label : SecNumCloud. Il s'agit d'un visa de sécurité délivré par l'Agence nationale de la sécurité des systèmes d'information (Anssi). C'est sa version actualisée en mars 2022 (version 3.2) qui intègre la nécessité de protéger contre les législations extraterritoriales.

A l'origine, l'objectif de SecNumCloud était de créer un label de confiance pour répondre au constat suivant : début 2010, les administrations et les entreprises critiques (opérateur d'importance vitale et opérateur de service essentiel) hésitent à passer au cloud par peur pour la confidentialité de leurs données.

Après une première phase d'expérimentation en 2014, la première version du label voit le jour en 2016. Progressivement, en particulier depuis sa version actualisée, SecNumCloud a glissé dans le débat public pour devenir un substitut de "cloud souverain". Or, ce raccourci est trompeur : SecNumCloud garantit certes un niveau de sécurité élevé mais pas une indépendance industrielle. D'ailleurs, si cette qualification devait certifier une souveraineté au sens strict, aucun acteur ne pourrait aujourd'hui l'obtenir.

Le compromis de S3NS et Bleu

Les offres franco-américaines S3NS - qui vient d'obtenir le visa de sécurité - et Bleu illustrent ainsi une souveraineté par délégation partielle. L'Europe ne contrôle pas la technologie au cœur de solution, mais elle en encadre l'usage. Elle ne possède pas le stack, mais elle en sécurise l'exploitation. C'est une réponse pragmatique à court terme, mais qui ne règle la question de la dépendance industrielle de long terme.

OVHcloud, qui commercialise plusieurs offres qualifiées, fait d'ailleurs la même distinction. "*Ce qu'apporte SecNumCloud, ce sont des garanties en termes de sécurité*, affirme la chief revenue officer. *Nous sommes plutôt sur un plan cyber que sur un axe souveraineté.*"

Cet avis est partagé par Christophe Grosbost, chief strategy officer de l'Innovation Makers Alliance (IMA), une association professionnelle qui rassemble les directions innovations de près de 165 grandes entreprises et administrations publiques. "*SecNumCloud est un label de cybersécurité, pas un label de souveraineté*", assure-t-il dans le cadre d'un échange accordé à L'Usine Digitale.

Il livre une vision assez radicale de la souveraineté : "*c'est la capacité, en cas de guerre, à continuer à avoir des capacités numériques fiables, opérationnelles, non influencées et non manipulées*". En pratique, "*si vos outils de communication peuvent être coupés de l'extérieur, si vos données sont sur des clouds soumis à une juridiction étrangère, si vos communications reposent sur une infrastructure qui peut être désactivée, alors vous n'êtes pas souverain*", poursuit-il.

L'interdépendance comme stratégie industrielle

Face à ce constat, la solution se trouve pour lui dans la notion d'interdépendance. "*Créer des briques technologiques sur lesquelles les autres ont besoin de nous, comme l'Europe l'a fait avec ASML*", explique-t-il. Pour rappel, l'entreprise néerlandaise est spécialisée dans les machines de lithographie utilisées pour fabriquer les semi-conducteurs. Concrètement, elle conçoit et produit les équipements qui permettent de graver les circuits électroniques sur les puces. Pour les technologies les plus avancées, dites EUV (Extreme Ultraviolet), ASML est aujourd'hui le seul fournisseur au monde.

A noter, et c'est une précision indispensable à faire, que les meilleurs clients d'ASML sont asiatiques et américains. Schématiquement, l'Europe dépend des Etats-Unis pour la conception des puces et de Taïwan pour leur fabrication physique. Les États-Unis eux-mêmes font d'ailleurs pression sur Taiwan Semiconductor Manufacturing Company (TSMC), qui est aujourd'hui le leader de la fabrication de puces logiques, pour qu'elle construise des usines sur son territoire, ce qu'elle est en train de faire.

Les USA disposent aussi de leur propre champion national : Intel, qui conçoit et fabrique ses puces. Longtemps leader des process de fabrication, il a été en perte de vitesse pendant une dizaine d'années mais est en train de revenir en force sur la scène à coups de dizaines de milliards de dollars d'investissement. Et l'Europe dans tout ça ? L'usine de fabrication de semi-conducteurs la plus avancée du continent se trouve en Irlande. Sortie de terre en 1989, plus de 30 milliards d'euros y ont été investis à date. Le twist ? Cette usine appartient à Intel.

L'Europe absente des chaînes essentielles de l'IA

L'Europe est quasiment absente du marché des processeurs dédiés à l'intelligence artificielle moderne. Les GPU et autres accélérateurs IA, devenus le cœur des data centers de nouvelle génération car essentiels pour faire tourner les modèles d'IA générative, sont dominés par des entreprises américaines comme Nvidia, avec ses puces comme les séries Blackwell et désormais les GPU Rubin. Les challengers se nomment AMD et Intel, sans compter les start-up qui cherchent d'autres approches : Cerebras, Unconventional AI, Oxmiq Labs... Tous sont américains.

Pour tenter de réduire sa dépendance étrangère dans le domaine des semi-conducteurs, l'Union européenne a lancé le European Chips Act en 2023. Le plan repose sur un engagement de plus de 43 milliards d'euros de financements publics et privés jusqu'en 2030 pour stimuler la recherche, la production et la résilience des chaînes de valeur européennes. L'objectif est ambitieux : doubler la part du marché européen dans la production mondiale de puces, de moins de 10% aujourd'hui à 20% d'ici 2030.

Cet effort s'appuie d'abord sur un tissu industriel déjà existant. L'Europe dispose d'acteurs solides comme STMicroelectronics, Infineon, NXP ou Bosch (nous n'incluons pas GlobalFoundries, qui est américain) capables de produire des puces indispensables pour l'automobile, l'énergie, l'industrie ou les capteurs. Ce sont des segments stratégiques, mais ce ne sont pas ceux qui structurent aujourd'hui l'économie du cloud et de l'IA. Aucun de ces industriels ne fabrique de processeurs pour data centers ou pour smartphones. Ils n'en ont pas les capacités technologiques.

Autrement dit, même si le European Chips Act réussit, il renforcera surtout une souveraineté industrielle sur des puces spécialisées. Il ne comblera pas, à court terme, l'absence européenne sur les composants les plus critiques pour le numérique contemporain. Aujourd'hui, seules trois entreprises maîtrisent la production de puces logiques avancées : TSMC, Intel et Samsung. Quant à la mémoire, ce sont les sud-coréens Samsung et SK Hynix qui dominent.

La robotique, un levier indispensable de réindustrialisation

"*L'Europe a fait une erreur stratégique en abandonnant l'industrie du hardware pendant vingt ans. Recréer cette industrie demanderait des investissements colossaux*", regrette Christophe Grosbost.

Pour lui, un levier reste pourtant décisif : la robotique. "*La guerre du hardware se joue au niveau des robots. Ce sont eux qui fabriqueront demain les puces et les infrastructures industrielles*", résume-t-il. Or le signal est inquiétant : "*Quand on voit que 60 à 70% des entreprises de robotique au CES sont chinoises, on comprend l'urgence*".

D'où son appel à une stratégie comparable à celle d'Airbus : "*une alliance industrielle européenne, un investissement massif et un protectionnisme assumé*" pour faire émerger un champion européen de la robotique, capable de redonner à l'Europe un levier réel sur ses capacités industrielles futures.

La question de la préférence européenne

Cette logique conduit, selon Christophe Grosbost, à poser une question : faut-il réserver certains secteurs du numérique à des acteurs nationaux ou européens ? Sa réponse est claire. Le droit européen le permet déjà. "*Il existe l'article 346 du traité sur l'Union européenne, qui permet de suspendre le droit à la concurrence pour des secteurs géostratégiques. Il est utilisé pour l'armement et pour le nucléaire. Nous pourrions l'utiliser pour certains secteurs du numérique.*"

L'idée est simple : lorsque des activités sont jugées vitales pour la sécurité et la continuité de l'État, elles sortent du champ du marché libre. Pour lui, le numérique est désormais dans cette catégorie. "*Nous avons trop longtemps considéré le numérique comme un simple outil. Or, il est devenu l'infrastructure stratégique centrale d'une nation. L'économie, la défense, l'information, la capacité de décision politique reposent dessus*", raconte-t-il.

L'intelligence artificielle pousse cette logique encore plus loin. "*L'IA est devenue plus stratégique que l'arme nucléaire. Si une nation ne maîtrise pas son IA, elle devient dépendante intellectuellement, économiquement et politiquement*", poursuit-il. Cela justifie, selon lui, d'assumer des choix politiques forts : restreindre l'accès à certains marchés, instaurer une préférence européenne et considérer que certaines briques numériques critiques ne peuvent être confiées qu'à des acteurs jugés pleinement maîtrisés et indépendants.

Maîtriser ses dépendances

Entre l'autarcie numérique et la dépendance totale, il existe toutefois un entre-deux. La souveraineté peut aussi se penser comme une capacité à maîtriser ses dépendances. Autrement dit, il ne s'agit pas seulement de savoir de qui l'on dépend, mais dans quelles conditions, avec quels leviers de négociation, quelles marges de manœuvre et quelles alternatives possibles.

La souveraineté devient alors moins une question d'indépendance absolue que de contrôle du destin collectif : être capable d'anticiper les ruptures, d'organiser des solutions de repli, de préserver une continuité stratégique même dans un environnement profondément interdépendant. C'est la vision défendue par Guillaume Poupard, ancien directeur général de l'Anssi ayant récemment rejoint Orange après être passé chez NumSpot.

"*Maîtriser ne signifie pas tout faire soi-même, tourner le dos à l'innovation technologique, s'enfermer dans une vision rétrograde et conservatrice. Maîtriser c'est au contraire savoir tirer profit des progrès technologiques d'où qu'ils viennent, les comprendre, savoir les mettre en œuvre de manière autonome et raisonnée*", écrivait-il.

Autrement dit, il s'agit de rester acteur de ses choix dans un monde de dépendances inévitables. Ce que l'on appelle "souveraineté" est une construction stratégique : un ensemble de choix politiques, industriels et juridiques qui rendent certaines dépendances acceptables et d'autres inacceptables. Refuser de regarder ces dépendances en face, c'est accepter une fragilité permanente sans l'assumer.

L'open source, une fausse solution ?

L'open source est souvent présenté comme une voie possible pour réduire les dépendances, parce qu'il garantit l'accès au code et la possibilité de l'exploiter sans dépendre juridiquement d'un éditeur unique. En théorie, chacun peut l'auditer, le modifier, l'héberger et l'adapter à ses besoins.

Mais, là encore, l'ouverture du code ne suffit pas à créer une souveraineté. Les briques open source centrales du cloud et de l'IA sont pour la plupart structurées par des acteurs américains, qui en financent le développement, en orientent les priorités et en concentrent l'expertise. Le logiciel est ouvert, mais la capacité à le faire évoluer, à l'industrialiser et à en tirer de la valeur reste très largement concentrée hors d'Europe. Autrement dit, l'open source réduit la dépendance contractuelle, pas la dépendance industrielle. On notera au passage que les licences open source sont généralement basées sur le droit américain.

La réglementation comme arme

L'un des principaux leviers dont dispose aujourd'hui l'Europe est finalement la réglementation. C'est par le droit qu'elle tente de rééquilibrer un rapport de force industriel qui lui est défavorable. RGPD, Digital Markets Act (DMA), Digital Services Act (DSA), Artificial Intelligence Act : l'Europe impose des contraintes là où elle ne peut pas imposer sa puissance industrielle.

Cette stratégie ne plaît ouvertement pas à Donald Trump. Durant son premier mandat, il avait déjà dénoncé les amendes infligées aux géants américains du numérique comme une "taxe déguisée" contre les États-Unis. Son retour sur la scène politique s'accompagne d'un discours encore plus frontal, assimilant les réglementations européennes à des barrières commerciales et à une forme de protectionnisme juridique.

Or, l'Europe n'est pas seulement dépendante, elle est aussi un marché majeur. Les grandes entreprises technologiques américaines ne pourraient pas se passer durablement de l'Europe sans perdre une part décisive de leurs revenus. Les 264 milliards d'euros dépensés chaque année par les entreprises européennes financent directement l'innovation et l'emploi.

L'Europe, indispensable mais pas dominante

La dépendance est donc réciproque mais elle est aujourd'hui asymétrique : l'Europe dépend de technologies qu'elle ne maîtrise pas, tandis que les États-Unis profitent d'un marché qu'ils considèrent acquis.

La souveraineté commence peut-être dans un grain de sable, mais elle se joue aussi dans la capacité à faire comprendre que ce grain de sable pèse, économiquement et politiquement, beaucoup plus qu'on ne l'admet. Mais encore faut-il que l'Union européenne ait réellement le pouvoir politique de jouer ce jeu jusqu'au bout.

DOCUMENT 8

Direction générale des entreprises - octobre 2023

Les territoires connectés durables (extrait)

(...) **2. Réunir les conditions d'un dialogue commun entre collectivités et industriels, à engager autour de 4 politiques à fort niveau de préoccupation des elus locaux et s'accordant sur 4 chantiers prioritaires**

Pour définir les usages numériques des collectivités territoriales connectées, une précision se doit d'être mentionnée : les prérogatives des collectivités locales sont exercées en faisant valoir des compétences basées sur des objectifs préalablement définis par les textes réglementaires en vigueur. Leurs élus ont également au titre de leurs fonctions des projets de transition, d'inclusion, et le numérique est pour eux un outil au service de l'accélération et l'efficacité des services publics rendus.

Le prisme retenu est donc celui d'une logique continue d'amélioration de l'efficacité de l'action publique par le biais des outils et solutions numériques qui servent la transition écologique.

Le numérique est un outil au service des politiques publiques et il permet de les objectiver. Le numérique est aujourd'hui nécessaire pour optimiser les services publics locaux existants, pour créer de nouveaux services cohérents avec les habitudes de vie des usagers, pour maintenir ou restaurer la santé financière de la collectivité, pour améliorer l'efficacité du fonctionnement des services chargés de produire et piloter les services publics locaux et s'adapter aux évolutions réglementaires.

Le nombre d'expérimentations d'usages numériques connectés menées jusqu'à présent dans les collectivités précurseurs (souvent les plus grandes) atteint plusieurs centaines. Les caractéristiques techniques et organisationnelles de ces services numériques connectés sont très variables, même pour un cas d'usage donné. Les fournisseurs se sont différenciés sur ce marché très concurrentiel en adaptant leur offre sur le plan contractuel ou technique en fonction des spécificités, des besoins et des priorités de la collectivité. Les garanties d'interopérabilité et de réversibilité ont parfois été inégalement données. Il importe de reconnaître la valeur des expérimentations et de considérer maintenant un projet plus global, fédérateur et d'ampleur pour l'ensemble des collectivités locales en métropole et outre-mer.

Les élus sont lucides sur l'état des forces et de leur pouvoir de marché. Ils revendiquent aussi le souci de la sobriété dans les manières de faire, en se limitant à des usages véritablement utiles, en repoussant le numérique « gadget » et en développant la connaissance du territoire y compris avec la donnée. Les réalisations de territoires connectés et durables sont un moyen pour les collectivités de répondre à leurs grands enjeux : transition écologique et énergétique, inclusion et cohésion sociale, aménagement territorial et développement de services publics.

Les élus des territoires ont en commun une attention de tous les instants à l'amélioration de la qualité de vie des habitants, c'est l'ADN de leur engagement, leur motivation, quelle que soit la taille de leur collectivité ; c'est à travers ce prisme empreint d'humanité et non celui du numérique que s'organise leurs actions dans les territoires.

2-1 Déployer les usages numériques autour de 4 « chantiers » prioritaires

Recommandation n°3 (R3). Structurer un cadre stratégique cohérent de déploiement des usages numériques autour d'un socle de 4 chantiers prioritaires

Pour chaque domaine de compétences aux mains des collectivités territoriales, la mission a employé un langage commun et compréhensible des élus locaux, communaux, intercommunaux,

départementaux, métropolitains et régionaux. Bien entendu la liste qui suit n'est pas exhaustive de l'ensemble des possibilités, mais si les usages numériques de cette liste sont déployés par grands domaines d'application dans les collectivités dotées de ces compétences, la mission affirme que l'on fera un grand bond en avant.

Beaucoup de territoires ont déjà implémenté des usages numériques connectés parmi cette liste (non exhaustive). Avec les intervenants privés (fournisseurs d'équipements et de prestations), les élus et les services métiers ont retenu certaines déclinaisons organisationnelles, technologiques et contractuelles souvent très différentes d'une collectivité à l'autre. La mission propose de présenter ces usages en quatre principaux regroupements :

Usages numériques et domaines de compétences des collectivités territoriales réunis en quatre regroupements :

- Exercer confortablement ses activités
- Se déplacer en sécurité
- Protéger les citoyens
- Contribuer activement à la préservation de la ressource

Exercer confortablement ses activités

Sélection d'usages numériques connectés

Compétences des collectivités territoriales par domaine d'application	Usages numériques au service quotidien des habitants
Exercer confortablement ses activités	
Gestion des bâtiments publics	
• Construction et fonctionnement des bâtiments publics territoriaux • Construction et fonctionnement des écoles maternelles et élémentaires, des collèges et des lycées • Construction et fonctionnement des équipements sportifs de proximité, dans les collèges et les lycées • Bibliothèques de prêt municipales et départementales • Protection du patrimoine • Organisation et financement des musées • Conservation et mise en valeur des archives	• Pilotage de la performance énergétique des bâtiments • Amélioration du confort des usagers (suivi de la qualité de l'air, de la température et de l'hygrométrie, visualisation des données et système d'alerte) • Surveillance du mobilier urbain • Amélioration des conditions d'activité (smart office, espaces publics mutualisés) • Amélioration de la sécurité intérieure et identification de situation à risque (notamment mesure et suivi du niveau de fréquentation des lieux publics)

Se déplacer en securité :

Sélection d'usages numériques connectés

Compétences des collectivités territoriales par domaine d'application	Usages numériques au service quotidien des habitants
Se deplacer en securité	
Aménagement du territoire	
• Élaboration du plan régional de transports • Élaboration du schéma régional de l'intermodalité et du schéma régional des infrastructures de transports • Élaboration des schémas régionaux des infrastructures et des transports définissant notamment les priorités d'actions en ce qui concerne les infrastructures routières • Identification des voies et axes routiers qui constituent des itinéraires d'intérêt régional dans le SRADDET	• Observatoire des mobilités (comptage, diagnostic et analyse des flux, fréquentation et modes de déplacement, évaluation des actions) • Amélioration de la coordination des différents flux de mobilité du territoire (meilleure évaluation et gestion des places de livraison et de covoiturage, repérage des véhicules ventouses, redirection des véhicules vers les zones moins chargées, signalétique intelligente)
Transports publics	
• Financement, organisation et fonctionnement des transports scolaires • Organisation de la mobilité, organisation des transports de personnes (hors Région Ile-de-France) et des transports non urbains, (organisation des transports publics et des services de covoiturage, autopartage, service public de location de bicyclette • Élaboration du plan de déplacements urbains • Organisation des transports ferroviaires régionaux	• Développement de l'adoption de nouveaux comportements de déplacements au service de la décarbonation du territoire (meilleure évaluation et gestion des places avec des bornes électriques, priorisation du passage des bus aux carrefours complexes, facilitation de l'accès à la mobilité douce)

Protéger les citoyens

Sélection d'usages numériques connectés

Compétences des collectivités territoriales par domaine d'application	Usages numériques au service quotidien des habitants
Protéger les citoyens	
Tranquillité publique et protection civile	
• Police municipale • Pouvoir de police portant sur des objets particuliers (circulation, stationnement, ...)	• Maintenance des infrastructures / gestion de la voirie (état et accidentologie) • Amélioration de la sécurité routière : • Mise en place d'alertes dynamiques (signalétique) de danger en amont des zones à risques • Sécurisation dynamique des mobilités actives aux abords des carrefours complexes • Gestion de l'éclairage public de nuit aux intersections à risques • Diagnostic amont de zones à risque par IA (alertes de pré-accident), ... • Participation citoyenne à travers une solution de signalement mobile d'incidents
• Exercice du devoir d'alerte et de veille sanitaire par le signalement sans délai des menaces imminentes pour la santé de la population et par la transmission à l'Institut de veille sanitaire d'informations nécessaires à l'exercice de ses missions ;	• Détection en temps réel ou de manière prédictive des incendies, des inondations, des submersions ou des tempêtes, alerte des populations et coordination des services de secours
Action sociale et santé	
• Les pouvoirs de police municipale en matière de sécurité et de salubrité, ainsi que certaines dimensions de la politique de l'habitat (résorption de l'insalubrité et des immeubles menaçant ruine ...) • Le devoir d'alerte et de veille sanitaire par le signalement sans délai des menaces imminentes pour la santé de la population et par la transmission à l'Institut de veille sanitaire d'informations nécessaires à l'exercice de ses missions • Élaboration et la mise en œuvre des schémas départementaux d'organisation sociale et médico-sociale • Co-pilotage du plan d'alerte et d'urgence au profit des personnes âgées, des personnes	• Observatoire environnemental • Contribution à l'amélioration de la qualité de l'air en extérieur • Amélioration des niveaux et de la qualité de l'eau, notamment dans les bassins de rétention • Contrôle des exutoires et trappes • Surveillance de la chaîne du froid • Détection des ouvrants • Anticipation et alerte des zones à risque en fonction du climat (observatoire de la santé sur les îlots de chaleur, le pollen, ...) • Détection en temps réel ou de manière prédictive des canicules, alerte des populations et coordination des services de secours

handicapées ou en perte d'autonomie en cas de risques exceptionnels • Surveillance et le contrôle des établissements et services d'accueil des enfants de moins de six ans	• Participation citoyenne à travers une solution d'entraides citoyennes/signalement d'incidents • Surveillance de la chaîne du froid • Détection des ouvrants

Contribuer activement à la préservation de la ressource

Sélection d'usages numériques connectés

Compétences des collectivités territoriales par domaine d'application	Usages numériques au service quotidien des habitants
Contribuer activement à la préservation de la ressource	
Environnement	
• Schéma régional d'aménagement durable du territoire • Schémas interrégionaux du littoral et de massif • Délimitation du périmètre d'intervention pour la protection et la mise en valeur des espaces agricoles et naturels périurbains	• Cartographie en temps réel grâce aux capteurs de sol et météo pour optimiser les déplacements en vue d'arroser, de fertiliser, ... • Observation du territoire pour tester de nouvelles techniques d'agriculture (cf. INRIA) • Observation de l'impact du climat sur l'évolution de la biodiversité : niveau d'eau des fleuves, observation des arbres en ville (pour sélection de nouvelles espèces plus adaptées), ... • Analyse des flux pour maîtriser et contrôler l'accès aux espaces protégés
Déchets	
• Collecte et traitement des ordures ménagères • Plan régional de prévention et de gestion des déchets	• Suivi du niveau de remplissage des containers pour optimiser les tournées et déclencher des alertes • Optimisation du tri sélectif et réduction des erreurs de tri • Accès aux déchetteries • Détection des dépôts sauvages • Gaspillage alimentaire
Eau et assainissement	
• Distribution publique de l'eau potable et élaboration du schéma de distribution d'eau potable (+ options : production, transport et stockage de l'eau potable) • Assainissement • Gestion des eaux fluviales	• Mesure de la consommation d'eau • Mesure de la qualité de l'eau : eaux pluviales, rivière, ... • Arrosage intelligent en fonction du taux d'humidité des sols et la prise en compte des prévisions météo

• Aménagement, entretien et exploitation des cours d'eau, canaux, lacs et plans d'eau • Gestion des milieux aquatiques et de prévention des inondations	• Détection des fuites avec capteurs acoustiques au niveau des canalisations • Amélioration des niveaux de la qualité de l'eau, notamment dans les bassins de rétention
Energie / éclairage	
• Autorités organisatrices de distribution d'électricité et de gaz • Aménagement, exploitation et installation de production d'énergie de sources renouvelables • Création d'infrastructures de charges nécessaires à l'usage de véhicules électriques ou hybrides • Aménagement de réseaux de chaleur alimentés par des installations utilisant le pouvoir calorifique des résidus et déchets collectés • Plan lumière • Mise en place d'actions tendant à maîtriser la demande d'énergie • Schéma Régional d'Aménagement, de Développement Durable et d'Egalité des Territoires (comprend notamment le Schéma Régional Climat-Air-Energie)	• Observatoire énergétique du territoire : suivi du bilan énergétique du territoire (consommation et production), à travers l'agrégation et l'analyse des données énergétiques, en fonction d'usage et localisation différentes, du mix énergétique • Optimisation de la consommation en énergie fossile liée aux déplacements en permettant de les réduire • Smart grid : gestion dynamique des flux d'énergies entre producteurs et consommateurs • Optimisation de l'éclairage public (allumage, gradation de la lumière ou extinction en fonction de la présence ou du passage d'usagers)

Source : DGCL, travaux de la filière Infrastructures numériques, retraitement par la mission

Autour de ce cadre de référence, chaque collectivité territoriale pourra *a minima* développer l'un des quatre chantiers prioritaires suivants, essentiels pour la transition écologique des territoires et pour lesquels les bénéfices de l'utilisation du numérique en tant que moyen sont démontrés, avec des financements publics principalement ouverts aux demandes portant sur :

- L'éclairage public ;
- La gestion de l'eau ;
- La gestion des risques climatiques ;
- La rénovation énergétique des bâtiments.

La mission insiste sur les atouts d'une telle structuration des déploiements d'usages numériques qu'elle considère indispensable à sa montée en puissance :

- Les 4 politiques de déploiement des usages numériques sont complémentaires et interdépendantes : elles permettent de satisfaire la double exigence de nos concitoyens d'un accroissement de la qualité de vie de chacun et d'un mieux vivre ensemble en préservant nos ressources.
- Quel que soit le chantier prioritaire choisi pour démarrer, la collectivité est assurée de la cohérence du déploiement des usages numériques car il existe des passerelles naturelles entre les 4 chantiers, comme il en existe entre les 4 axes de la stratégie.

Il est ainsi entendu que le déploiement de ces chantiers prioritaires permet au territoire d'envisager plus facilement l'adoption progressive de nouveaux cas d'usages, et tendre ainsi vers le développement d'une offre numérique aboutie correspondant à ses besoins.

Le passage d'un usage numérique au prochain se fera plus aisément et s'alignera avec la cohérence d'ensemble, pour massifier les volumes au niveau national pour les industriels tout en respectant les choix des priorités des élus.

R3 | Action n°1. *Structurer la montée en puissance des usages numériques dans les territoires avec les 4 chantiers prioritaires consensuels que sont l'éclairage public, la gestion de l'eau, la prévention et la gestion des risques climatiques et la rénovation énergétique des bâtiments publics.*

Chantier n°1 L'éclairage public

Le premier chantier prioritaire énuméré par la mission concerne l'éclairage public inscrite dans la compétence de police municipale et régie par le Code général des collectivités territoriales (art. L2212-2). Au fil des entretiens, la mission a relevé que ce service (ce chantier) rassemble un éventail large des défis à relever.

Fondamentalement, il illustre surtout la capacité qu'auront l'État, les collectivités et l'écosystème d'entreprises à s'organiser autour d'un objectif partagé et atteignable : passer rapidement à l'échelle de manière significative en s'adressant à toutes les localités de métropole et d'outre-mer. Ce mouvement collectif est totalement aligné avec les transitions que les collectivités veulent mener. Les expérimentations qui mobilisent les solutions numériques connectées révèlent que ce potentiel pour les transitions énergétique et écologique est à la portée des collectivités, incluant les petites localités du bloc communal.

En premier lieu, un interlocuteur faisait observer à la mission que la diffusion géographique du service de l'éclairage public matérialise l'empreinte humaine sur l'espace naturel originel. Ce service historique s'accompagne de nombreuses normes techniques et nécessite une grande expertise pour être finement calibré.

L'évolution que connaît l'éclairage public est amplifiée par les contraintes qui pèsent sur les budgets des collectivités, par l'urgence de la sobriété énergétique et la limitation nécessaire des nuisances lumineuses. Cette évolution a des conséquences sur la conception, la définition du niveau de service et sa production (autoconsommation, points lumineux auto-alimentés).

Ce service soulève également des questions autour de l'évaluation de sa valeur globale, depuis sa part dans les dépenses (41 % des consommations d'électricité des collectivités territoriales), sa valeur d'usage compte tenu des dépenses investies et sa contribution à la stratégie territoriale sur trois plans au moins :

- Au niveau économique, pour restaurer la capacité d'investissement de la collectivité ;
- Au niveau social, pour maintenir la qualité du service rendu aux usagers ;
- Au niveau environnemental, pour accélérer la lutte contre les pollutions.

La mission retient en première approche que l'éclairage agit sur le confort global du territoire et étend les durées des activités humaines sur l'espace public au fil des semaines et des saisons.

L'éclairage assure une fonction inclusive puisqu'il accompagne le quotidien de toutes les populations : les piétons de tous les quartiers d'une collectivité, les usagers de moyens de locomotion

(...)

DOCUMENT 9
ANSSI - 30 mai 2025

« Approche SSI pour l'internet des objets industriels » (extrait)

(...)

3 Impacts de l'introduction de l'IIoT sur le modèle de sécurité de l'usine

La génération et le traitement de la donnée IIoT reposent sur un nouveau système composé notamment des capteurs IIoT et de la chaîne de traitement des données IIoT. S'il existe quelques spécificités dues au capteur et à la communication sans fil associée, la faible adhérence du reste des équipements de la chaîne IIoT à des technologies spécifiques aux systèmes industriels permet d'appliquer les bonnes pratiques de la SSI à la chaîne IIOT, et de les inscrire dans les schémas de gouvernance existants au sein des organisations.

Il est recommandé de réaliser ou de mettre à jour une analyse de risque SSI s'appuyant sur la méthode EBIOS RM en incluant dans son périmètre le système IIoT. L'objectif pour l'entité est de pouvoir adapter les mesures de sécurité en fonction des menaces retenues et des évènements redoutés associés aux valeurs métiers du système industriel.

L'analyse doit englober à la fois les nouveaux scénarios susceptibles de déclencher des événements redoutés déjà identifiés dans le système industriel via le système IIoT, ainsi que les scénarios pouvant engendrer de nouveaux événements redoutés spécifiques à la chaîne IIoT. En particulier, il est nécessaire de traiter les scénarios de risques impactant :

- la disponibilité et/ou l'intégrité du système industriel (à partir du système IIoT);
- la confidentialité des données de la chaîne de collecte du système IIoT;
- la disponibilité et/ou l'intégrité de la chaîne de collecte du système IIoT;
- la disponibilité et/ou l'intégrité de la chaîne de traitement du système IIoT.

Information

Certains systèmes de maintenance préventive pour les machines tournantes sont entièrement intégrés au système industriel et connectés directement aux automates. Ces systèmes matérialisent à l'extrême le modèle des systèmes IIoT traité dans ce document. Par conséquent, pour ces systèmes, une étude poussée doit être menée et mise à jour régulièrement. De manière générale, toute interconnexion IT/OT ne s'appuyant pas sur la zone DMZ (couche 3.5 du modèle de Purdue) doit être étudiée avec soin.

3.1 Les scénarios de risques portant atteinte à la disponibilité et/ou l'intégrité du système industriel

Les deux principaux éléments à prendre en compte dans les scénarios de risques pouvant impacter la disponibilité et l'intégrité du système industriel sont les suivants :

- **Attaques par latéralisation :** la mise en œuvre d'un système IIoT augmente la surface d'attaque du système industriel en créant de nouvelles interconnexions et donc la possibilité de latéralisation d'un attaquant vers le système industriel. Un soin particulier doit être apporté au cloisonnement entre ces deux systèmes. Dans de nombreux cas, ils n'ont pas besoin de communiquer : il est donc inutile de les interconnecter.
- **Attaques de l'homme du milieu (*Man-in-the-middle Attacks*) :** les consignes intelligentes pourraient être supprimées, modifiées et/ou rejouées entre le système IIoT et le système industriel. Il est important de considérer des mesures de protection en intégrité et authenticité sur les flux transportant les consignes intelligentes et/ou sur la passerelle d'interconnexion entrante vers le système industriel.

Par exemple, selon les cas d'usage et l'adhérence entre l'IIoT et le système industriel, ces menaces pourraient mener à un arrêt durable d'exploitation du système (via latéralisation et prise de contrôle du système industriel à partir de l'IIoT) ou à un comportement erratique du procédé industriel par la réception de consigne intelligente non intègre et non authentifiée.

3.2 Les scénarios de risques portant atteinte à la confidentialité des données de la chaîne de collecte du système IIoT

La centralisation des données du système industriel au sein du système IIoT augmente les potentiels impacts sur le système industriel en cas de divulgation de celles-ci. Dans ce cas de figure, les principaux éléments à prendre en compte sont :

- **Attaque par administration non autorisée de l'infrastructure hébergeant les données :** il est important de prendre en compte, en cas d'infogérance, la capacité de l'infogérant d'accéder aux données et aux traitements.
- **Attaque par accès non autorisés aux données par un utilisateur tiers :** en cas de mutualisation des moyens avec d'autres clients (par exemple dans un contexte *cloud*), le niveau de confiance dans l'infogérant, comme par exemple un *Cloud Service Provider* (CSP), et le niveau de cloisonnement des données doivent être pris en compte pour évaluer le risque associé.
- **Attaque par exfiltration de données :** en cas de compromission de l'espace de stockage par un attaquant malveillant, l'ensemble des données pourrait être exfiltré. Il est donc important de s'assurer du niveau de sécurité de cet espace de stockage, d'envisager des mécanismes de chiffrement des données au repos et de contrôler que seules les données autorisées y sont remontées via la passerelle d'interconnexion sortante.

Selon le domaine industriel d'application et les données choisies pour les nouveaux cas d'usage, une perte de confidentialité des données peut avoir par exemple des impacts sur l'avantage concurrentiel lié au savoir-faire de l'entité.

3.3 Les scénarios de risques portant atteinte à la disponibilité et l'intégrité des données sur la chaîne de collecte du système IIoT

Les traitements réalisés par le système IIoT sont naturellement très dépendants de l'intégrité et de la disponibilité des données remontées par la chaîne de collecte IIoT. Les principales menaces à considérer sont :

- **Attaque par modification ou prise de contrôle des équipements IIoT depuis la zone entreprise (voire depuis Internet) :** la modification ou perte d'intégrité des capteurs de collecte de données (c.-à-d. les capteurs IIoT) peut impacter la disponibilité et/ou l'intégrité des données traités par le système IIoT. Les mesures à envisager sont l'authentification et le contrôle d'intégrité des commandes qui ont pour destination le système IIoT, l'utilisation des capteurs IIoT embarquant des fonctions de sécurité et disposant de certifications ou qualifications de sécurité.
- **Attaque physique sur les capteurs IIoT :** notamment le changement du positionnement du capteur dans l'usine peut impacter l'intégrité des mesures [13].

Les impacts de ce type de menaces peuvent par exemple inclure une indisponibilité du système industriel faute de déclenchement d'actions préventives de maintenance en l'absence d'alerte émise par le système IIoT, ou alors des pertes économiques induites par le déclenchement trop fréquent de d'actions préventive de maintenance.

Information

Dans l'évaluation des risques, s'ajoute la particularité des communications entre le capteur IIoT et le point de concentration local à l'usine. Ces communications peuvent être portées par un réseau étendu à basse consommation (ex. : LPWAN). Dans ce cas, le niveau de sécurité cryptographique de ces communications est limité par la contrainte de faible consommation électrique des capteurs. La majorité des produits proposés sur le marché aujourd'hui offrent un niveau de protection cryptographique insuffisant.

De fait, les communications entre le capteur IIoT et le point de concentration local sont vulnérables en raison de faiblesses inhérentes au protocole. Si les risques associés sont considérés inacceptables au regard des usages et de la menace, il est recommandé de ne pas recourir à l'IIoT. Il faut par ailleurs encourager une montée du niveau de sécurité des équipements chez les constructeurs, par exemple en indiquant clairement le niveau minimal de sécurité pour l'achat et l'emploi de l'IIoT dans un contexte donné.

13. Notamment a) un capteur situé dans une zone accessible de l'usine pourrait être déplacé, sa mesure ne refléterait plus la valeur attendue (ex. : capteur de température d'un environnement clos déplacé en extérieur) ou b) un capteur dont l'interface de maintenance, accessible depuis le terrain, pourrait être réétalonné afin de fournir une valeur faussée.

3.4 Les risques sur la disponibilité et l'intégrité des fonctions de la chaîne de traitement du système IIoT

Sur la chaîne de traitement du système IIoT, il est important de prendre en compte le risque de non-fiabilité de la donnée d'entrée, en particulier dans le cas de l'utilisation d'algorithmes de traitements reposant sur l'analyse statistique ou sur l'intelligence artificielle. Ces principales menaces d'origine accidentelle sont :

- **les biais statistiques dans les modèles de traitements des données :** ceux-ci peuvent produire des résultats erronés et donc biaiser les prises de décisions. Ces biais peuvent être dus au fait que :
  - > l'entraînement des modèles sur la base d'un jeu de données incomplet induit des corrélations incomplètes et donc des causes infondées,
  - > il y a un décalage entre le modèle travaillé dans un environnement de laboratoire et ce même modèle déployé en environnement réel,
  - > une confiance excessive est placée dans un indicateur donné,
  - > de nombreuses variables peuvent être oubliées dans le calcul final (contraintes d'environnement physique, etc.);
- **l'usage d'un ensemble de données parcellaires :** cela peut fausser les résultats d'un modèle de simulation;
- **l'usage d'un ensemble de données erronées/non intègres :** par exemple l'achat ou la vente de stock pourrait mener à une perte de disponibilité et des pertes financières.

3.5 Synthèse des risques liés à l'IIoT

L'utilisation de l'IIoT induit de nombreuses menaces qui doivent être prises en compte. Cela est plus particulièrement vrai dans des contextes d'utilisation où un fort niveau de dépendance existe entre l'IIoT et le système industriel. Par exemple, un procédé industriel dont la maintenance prédictive repose entièrement sur l'IIoT pourrait engendrer un arrêt (maîtrisé ou non) inacceptable.

Il est donc important de mettre en place des mesures SSI adaptées afin d'assurer un niveau de confiance suffisant dans la chaîne de collecte des données et donc des traitements effectués. Un cas d'usage en particulier doit être traité avec vigilance. Il s'agit de l'utilisation de consignes intelligentes à partir de données industrielles (IIoT et non IIoT) au travers d'algorithmes de traitement statistique ou d'intelligence artificielle pour optimiser le procédé. Pour mettre en œuvre cet usage, il est nécessaire de traiter les points suivants :

- le stockage hors système industriel des données provenant du système industriel;
- les algorithmes permettant de calculer la consigne intelligente;
- le transport de la consigne intelligente vers le système industriel.

La figure 7 ci-après illustre la boucle d'asservissement intelligente.

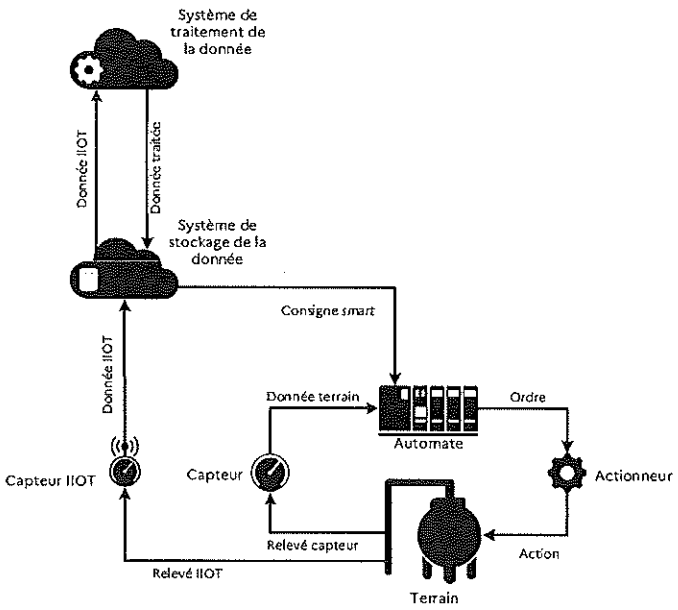


FIGURE 7 – La boucle d'asservissement intelligente

La branche intelligente de la boucle :

- Le capteur IIoT mesure une grandeur sur le terrain (par exemple une pression).
- La donnée IIoT est envoyée dans le système de stockage des données.
- Le système de traitement de la donnée calcule une consigne à partir des données présentes dans le système de stockage des données (données IIoT, données industrielles, données externes).
- La consigne intelligente est envoyée à l'automate.

La branche locale de la boucle :

- Le capteur mesure une grandeur sur le terrain (par exemple une température).
- Le capteur envoie à l'automate une donnée reflétant la valeur mesurée.

- En fonction de la donnée du capteur et de la consigne (un objectif à atteindre, par exemple 60 °C), l'automate calcule un ordre (par exemple, chauffer).
- L'ordre est envoyé à l'actionneur.
- L'actionneur réalise l'action associée et modifie le procédé (par exemple, la température augmente).
- Le procédé change sous l'effet de l'actionneur. De nouvelles grandeurs sont mesurées, la boucle intelligente calcule une nouvelle consigne intelligente, l'automate recalcule un ordre, etc.

L'apparition dans le système industriel d'une consigne intelligente calculée en dehors du système industriel ou importée d'un système tiers ne découle pas strictement de l'IIoT. Cependant, il serait tentant, à des fins d'optimisation des coûts, d'adapter la chaîne IIoT pour le calcul et la redescente de la consigne intelligente dans le procédé et, en particulier, le serveur d'échange de données situé dans la DMZ en zone de production. Cette architecture exposerait le procédé à un risque important en cas de consignes intelligentes non-intègres et non-authentifiées pouvant modifier le comportement du système industriel et mener à un arrêt d'exploitation.

Les besoins de sécurité de l'interconnexion IT vers OT (consigne intelligente) et ceux relatifs à l'interconnexion OT vers IT (IIoT) sont différents et doivent donc faire l'objet de canaux distincts.

Il est nécessaire de traiter deux points structurants pour limiter les risques avant de mettre en place la consigne intelligente en répondant aux questions suivantes :

- Est-il acceptable, du point de vue de la sûreté de fonctionnement, de piloter la procédé avec la consigne intelligente ?
- Comment mettre en place de manière sécurisée la chaîne de communication associée ?

(...)

DOCUMENT 10

codpo.fr

Objets connectés et RGPD : comment sécuriser l'IoT ? (extrait)

Blog - 07/10/2025

Pourquoi l'IoT est un sujet RGPD et cyber

Les objets connectés collectent, transmettent et croisent des données parfois très sensibles : localisation, habitudes de vie, données de santé ou usages industriels. Cette **explosion de données** crée un double enjeu : garantir la **conformité au RGPD** et renforcer la **sécurité des systèmes**. La CNIL souligne que sécuriser les objets connectés et leurs écosystèmes – applications, cloud, API – est essentiel pour préserver la vie privée et limiter les risques d'intrusion.

Les principes du RGPD appliqués aux objets connectés

Le RGPD repose sur plusieurs **principes fondamentaux** qui s'appliquent pleinement aux systèmes IoT :

- **Licéité, loyauté et transparence** : l'utilisateur doit être informé de façon claire et compréhensible des traitements effectués par l'objet connecté.
- **Minimisation des données** : seules les informations strictement nécessaires doivent être collectées.
- **Exactitude et limitation de conservation** : les données doivent être tenues à jour et supprimées une fois leur finalité atteinte.
- **Intégrité et confidentialité** : les traitements doivent être sécurisés de bout en bout, depuis le capteur jusqu'au cloud.

La **sécurité des données** est un pilier majeur : mots de passe, chiffrement, protocoles, API et applications doivent être conçus selon les recommandations de la CNIL et de l'ANSSI.
L'**analyse d'impact (AIPD ou DPIA)** devient obligatoire dès qu'un traitement présente un risque élevé, par exemple en cas de surveillance à distance, de traitement de données de santé ou d'utilisation à grande échelle.

Le cadre réglementaire à connaître (2024–2027)

1. Norme ETSI EN 303 645

C'est la norme européenne de référence pour les objets connectés grand public. Elle fixe les bonnes pratiques : mots de passe uniques, mises à jour logicielles sécurisées, divulgation responsable des vulnérabilités, chiffrement des échanges et approche « privacy by design ».

2. Cyber Resilience Act

Entré en vigueur en décembre 2024, ce règlement européen impose aux fabricants de produits numériques (dont les objets connectés) d'intégrer la sécurité dès la conception. Les obligations principales s'appliqueront à partir de décembre 2027, mais certaines, comme la notification des vulnérabilités, entreront en vigueur dès 2026.

3. Directive NIS2

La directive NIS2 renforce les exigences de cybersécurité pour les secteurs critiques et les fournisseurs de services essentiels. Sa transposition en France prévoit des obligations accrues en matière de gestion des incidents, de gouvernance et de contrôle technique.

Choisir la base légale adaptée et maîtriser le consentement

Chaque traitement de données lié à un objet connecté doit reposer sur une **base légale claire** :

- **Exécution du contrat** : lorsque le traitement est nécessaire pour fournir le service attendu (par exemple, un thermostat connecté qui ajuste la température).
- **Intérêt légitime** : pour des finalités non intrusives comme l'amélioration de la sécurité ou la maintenance.
- **Consentement** : pour les traitements non indispensables tels que la publicité personnalisée ou le partage de données avec des partenaires.

Le **consentement** doit être libre, spécifique, éclairé et révocable à tout moment. Les systèmes multi-terminaux (appareils, applications, plateformes) doivent garantir la cohérence du choix de l'utilisateur sur tous les supports.

Réaliser une AIPD (Analyse d'Impact sur la Protection des Données)

L'AIPD est indispensable dès qu'un traitement présente un **risque élevé** pour les droits et libertés des personnes. C'est souvent le cas dans les projets IoT liés à la santé, à la géolocalisation, à la surveillance ou au profilage.

Les étapes clés d'une AIPD efficace :

1. **Cartographier** les flux de données : capteurs, applications, serveurs, API, tiers.
2. **Identifier les risques** : exfiltration, manipulation, indisponibilité, perte d'intégrité, détournement de finalité.
3. **Évaluer leur gravité** et la probabilité d'occurrence.
4. **Définir les mesures** techniques et organisationnelles pour les réduire (chiffrement, authentification, mises à jour, cloisonnement réseau, clauses contractuelles).
5. **Documenter et suivre** l'évolution du risque dans le temps.

Mesures techniques de sécurité à mettre en œuvre

Sécurisation des produits et logiciels

- Éliminer les mots de passe par défaut et forcer leur modification lors de la première utilisation.
- Utiliser des mécanismes de chiffrement modernes (TLS 1.2 minimum).
- Signer et vérifier les mises à jour logicielles.
- Mettre en place un système de démarrage sécurisé (secure boot) et un contrôle d'intégrité.
- Journaliser les événements de sécurité pour détecter les anomalies.

Architecture et infrastructure réseau

- Segmenter les réseaux : séparer le trafic IoT du reste du système d'information.
- Appliquer le principe du moindre privilège pour limiter l'accès aux ressources.
- Sécuriser les API et contrôler l'accès par des clés et des jetons renouvelables.
- Héberger les données dans des environnements conformes, avec chiffrement des sauvegardes et limitation de la rétention.

Protection des données personnelles

- Activer les paramètres de confidentialité les plus protecteurs par défaut.
- Fournir une information claire dans les notices, les interfaces et les applications.
- Offrir une procédure simple d'accès, de rectification et de suppression des données.
- Anonymiser ou agréger les données lorsqu'une identification n'est pas nécessaire.

(...)

Gouvernance et documentation : être prêt à prouver sa conformité

Un projet IoT conforme au RGPD doit pouvoir démontrer, à tout moment, sa conformité documentaire. Voici les éléments indispensables :

- **Registre des traitements** décrivant les flux et les sous-traitants.
- **Notices d'information** destinées aux utilisateurs, intégrées aux supports physiques et numériques.
- **Contrats** avec les sous-traitants, incluant des clauses de sécurité, de maintenance et de gestion des incidents.
- **Procédures internes** de gestion des droits des personnes, de conservation des données et de notification en cas de violation.
- **Politique de mise à jour et de support** pour les produits connectés.

Les erreurs fréquentes à éviter

- **Penser que le cloud garantit la conformité** : l'hébergeur ne détermine pas la base légale ni la durée de conservation.
- **Négliger la fin de vie de l'objet** : sans effacement ou réinitialisation, les données restent accessibles.
- **Sous-estimer les API** : elles sont souvent la porte d'entrée des attaques.
- **Oublier l'AIPD** alors que des données sensibles sont traitées.

ANNEXE A

« Présentation d'Ingéagglo »

Ingéagglo est une **communauté d'agglomération de 180 000 habitants**, regroupant **28 communes**, dont :

- Une ville-centre de 80 000 habitants,
- Cinq communes de plus de 10 000 habitants,
- Et vingt-deux communes périurbaines et rurales.

Depuis plusieurs années, Ingéagglo s'est engagée dans une **dynamique de transformation numérique et écologique** à travers son **Plan d'Aménagement Numérique du Territoire (PANT 2024-2030)**. Ce plan vise à garantir l'égalité d'accès aux infrastructures numériques et à favoriser les usages innovants au service des politiques publiques locales.

Les principales réalisations à ce jour sont :

- **Couverture intégrale du territoire en fibre optique (FTTH)**, finalisée en 2024, en partenariat avec le syndicat départemental numérique.
- **Expérimentations IoT sectorielles** menées par plusieurs directions métiers :
  - Sondes de qualité de l'air dans la ville-centre et sur les grands axes,
  - Éclairage public intelligent sur trois quartiers pilotes,
  - Suivi du remplissage des bennes et conteneurs enterrés sur cinq sites,
  - Capteurs de température et d'humidité dans les écoles, équipements sportifs et quelques ilots de chaleur urbains identifiés dans la ville centre.
- **Mise en place d'un réseau bas débit LoRaWAN** sur dix antennes, actuellement géré par un opérateur privé, sans interconnexion entre services.

L'agglomération dispose par ailleurs d'un **système d'information géographique (SIG)** mutualisé et d'une **direction du numérique et des systèmes d'information (DNSI)**, qui assure le support technique, la cybersécurité des infrastructures et le pilotage et la maintenance des SI de gestion pour les villes de l'agglomération ayant mutualisé le numérique (c'est le cas de la ville-centre et de 16 autres communes de l'EPCI, 11 communes n'ayant pas mutualisé leur système d'information).

En 2025, la présidence d'Ingéagglo souhaite engager la définition d'une **stratégie IoT unifiée**, intégrée au futur **schéma directeur du numérique et du territoire intelligent**, afin de :

- Garantir **l'interopérabilité** entre dispositifs existants et futurs,
- Assurer un **pilotage global et sécurisé** des données territoriales,
- Et définir un **modèle de gouvernance et de financement** cohérent pour la généralisation des usages connectés.

Réseau et connectivité d'IngéAgglo

- Le territoire d'Ingéagglo bénéficie d'une **couverture intégrale en fibre optique FTTH**, finalisée en 2024.
- Le backbone communautaire repose principalement sur de la **fibre optique noire** mise à disposition via le syndicat départemental numérique, permettant à la collectivité de maîtriser ses interconnexions inter-sites.
- Certaines liaisons secondaires utilisent de la fibre activée (fibre blanche) opérée par des tiers.
- Un réseau **LoRaWAN** composé de **10 antennes** couvre environ 65 % du territoire (ville-centre et principales communes urbaines).
- Ces antennes sont raccordées en fibre au réseau métropolitain.
- Le réseau est aujourd'hui exploité par un **opérateur privé**, sans interconnexion technique avec les autres systèmes communautaires.
- Les objets utilisent majoritairement le protocole **LoRaWAN classe A**, avec remontées périodiques de données (15 min à 1 heure selon usage).
- Les dispositifs d'éclairage intelligent reposent sur une solution propriétaire incluant un **back-office SaaS opéré par une start-up basée à Barcelone (Espagne)**, avec hébergement hors du territoire national.
- Il n'existe **aucune interconnexion directe** entre la plateforme LoRaWAN actuelle et le **SIG communautaire**.
- En revanche, le patrimoine d'éclairage public (points lumineux, armoires, réseaux) est intégré au SIG via un **import FME quotidien**, désynchronisé (mise à jour par lot chaque fin de journée).
- Une réflexion avancée est engagée pour internaliser la gestion du réseau LoRaWAN, y compris la reprise de la gestion des clés.

Données et supervision

- Les données issues des capteurs LoRaWAN sont actuellement accessibles via la plateforme opérateur.
- Les données issues du SaaS éclairage sont récupérables via une **API REST propriétaire du fournisseur**, mais :
  - L'EPCI n'a pas encore développé le demi-connecteur d'intégration (capacité interne de développement faible)
  - Aucune synchronisation automatisée vers le SI communautaire n'est en place au-delà des imports FME quotidien. La conduite d'exploitation est réellement opérée et dépendante du SaaS du fournisseur
- Aucun standard commun d'API ou de modèle de données n'a été imposé aux fournisseurs.

- Conformément au RGPD, les nouveaux marchés intègrent des clauses précisant :
- les durées de conservation,
- les modalités d'anonymisation,
- les obligations contractuelles des sous-traitants.
  Les durées de conservation sont conformes à la réglementation pour les dispositifs récents.

Sécurité et exploitation

- Les clés d'activation LoRaWAN sont aujourd'hui gérées par l'opérateur privé.
- Les mises à jour firmware des capteurs ne sont pas supervisées par la DNSI pour l'éclairage public. Les capteurs des bennes sont propriétaires et ne sont pas mis à jour (le fournisseur historique a fait une cessation d'activité). Les capteurs d'humidité et de température utile encore le réseau cuivre historique pour communiquer, réseau qui sera décommissionné sur le territoire en décembre 2027. (Annoncé par Orange)
- Aucun PCA/PRA spécifique n'est encore défini pour les services IoT
- La maintenance terrain est assurée soit par les services métiers, soit par les prestataires (quand l'équipement est encore sous garantie).

Infrastructure du SI communautaire

- L'agglomération dispose de **deux hébergeurs communautaires (HC)** sur deux sites géographiquement distincts.
- L'infrastructure repose majoritairement sur :
  - des clusters VMware vSphere,
  - quelques baremetal pour usages spécifiques,
  - une baie de stockage mutualisée
- Une DMZ est en place pour les services exposés vers l'extérieur.
- La supervision de sécurité est assurée par un **SOC externalisé**, comprenant :
  - surveillance des flux réseau,
  - corrélation d'événements,
  - détection d'intrusions (IDS/IPS),
  - gestion des incidents critiques 24/7.
- Les dispositifs IoT ne sont pas encore intégrés au périmètre de supervision SOC.