FILIÈRE INFRASTRUCTURES NUMÉRIQUES

avicca

LA CYBERSÉCURITÉ APPLIQUÉE À L'INTERNET DES OBJETS

QUELS NOUVEAUX ENJEUX POSE L'INTERNET DES OBJETS (IOT) EN CYBERSÉCURITÉ ?

Si tout projet numérique nécessite des mesures de cybersécurité, est-ce que l'arrivée de l'IoT au sein des collectivités porte de nouveaux enjeux ? Comment assurer un numérique sécurisé au cœur des projets de territoires connectés et durables ? Pour répondre à cette problématique, un groupe de travail porté par l'Avicca et le CSF IN a conduit une étude auprès de collectivités, de structures publiques de mutualisation, d'intégrateurs, d'opérateurs de réseau, de bureaux d'études, de fournisseurs de plateforme et de fabricants d'objets connectés. Cette étude a permis d'identifier des risques et des bonnes pratiques spécifiques à l'IoT.

- → Des contraintes matérielles : contrairement aux PC/serveurs, les capteurs IoT ont des ressources limitées (puissance, mémoire) qui empêchent d'installer les outils de sécurité standards.
- → Une gouvernance fragmentée : si les projets sont souvent portés par les services «métiers», la synchronisation avec les services juridiques et la DSI est essentielle et demande une coordination dédiée, y compris sur des petits volumes de capteurs.
- → Une exposition physique : le matériel n'est plus protégé dans des bureaux mais installé sur le domaine public. L'accès physique direct aux objets étend la surface d'attaque, un risque à fort impact qui est à prendre en compte dans l'analyse.
- → Un impact immédiat sur le territoire : une faille ne touche pas que des données virtuelles ; elle perturbe les services aux citoyens et dégrade la crédibilité politique de la collectivité.
- → Un écosystème complexe à piloter : la multiplication des intervenants et fournisseurs rend l'inventaire des ressources, de leur provenance (traçabilité des capteurs) et les audits globaux beaucoup plus difficiles que dans un projet IT classique. En parallèle, les différents acteurs publics impliqués dans la mutualisation doivent aligner leurs exigences et cahier des charges.

DES RISQUES MULTIPLES MAIS IDENTIFIÉS

CAPTEURS	L'achat d'équipements non vérifiés (par exemple hors UE) ou physiquement isolés expose le territoire à des fuites de données. Les remontées aberrantes s'expliquent souvent par des malfaçons matérielles, des défauts de paramétrage plutôt que par de véritables cyberattaques.
TRANSMISSION	Attaques principales connues et documentées. En revanche, c'est lors de la transmission qu'il est possible de repérer des flux non conformes générés par des capteurs. Ces flux peuvent se détecter et se bloquer dès le cœur de réseau grâce à des outils de supervision mis en place par l'opérateur, auprès duquel il est conseillé de se renseigner en amont.
PLATEFORME DE DONNÉES	Les serveurs et les plateformes des éditeurs constituent des cibles critiques nécessitant une grande vigilance. Le risque majeur est de déployer des solutions qui n'intègrent pas la sécurité dès leur conception (absence de Security by design).
SYSTÈME GLOBAL	La multiplication des acteurs et des projets métiers initiés sans la DSI élargit la surface d'attaque. Une faille systémique à ce niveau entraîne une perte de crédibilité massive vis-à-vis des usagers et des élus.
HUMAIN ET ORGANISATIONNEL	Identifié comme principal facteur de risque *Exemple de pratiques à risque : faible authentification (mettre à jour les mots de passe par défauts, mauvaise gestion des interventions terrain, négligence de sécurité (sessions laissées ouvertes), droits d'accès trop larges (partage de mots de passe en clair...)*

COMMENT DÉPLOYER DE MANIÈRE SÉCURISÉE ?

Bonnes pratiques répertoriées par les collectivités et les entreprises

À partir de ces entretiens, le groupe de travail a recueilli des bonnes pratiques concernant chaque élément d'un projet IoT.
Chaque acteur peut jouer un rôle proactif et l'ensemble de la chaîne de valeur peut être sollicité sur l'enjeu de cybersécurité :

CAPTEURS ET DONNÉES « ABERRANTES »

- → Limiter les risques : **définir les données nécessaires**, dimensionner le nombre de capteurs au strict besoin
- → Évaluer et prioriser les risques : faire une analyse de risques, **évaluer la criticité des données et adapter l'effort**
- → Collaborer avec les services : **définir les données anormales / comportement normal du capteur avec les métiers**
- → **Tester les équipements** : rencontrer et sélectionner les fournisseurs, faire des expérimentations
- → Mises à jour : un travail de coordination entre les fournisseurs (intégrateur/équipementier/éditeurs) et les équipes terrain est nécessaire pour **garantir les mises à jour** nécessaires pour gérer les vulnérabilités. Il faut prévoir les canaux de mises à jour en amont, afin d'assurer une durée de vie maximale des capteurs.
- → Pour la structure de mutualisation, l'intégrateur/opérateur, voire pour l'éditeur de plateformes : **qualifier le matériel, vérifier les certificats de conformité, paramétrer chaque équipement avant déploiement,** voire préconiser certains capteurs (par exemple le cas de certaines structures de mutualisation)

TRANSMISSION

- → S'appuyer sur des standards de sécurité reconnus, les protocoles les plus courants
- → Pour l'intégrateur, contrôler les fournisseurs sur le respect des spécifications technologiques
- → Pour la structure de mutualisation / grande métropole, mettre en place **une supervision des flux** si la structure se positionne comme opérateur vis-à-vis d'autres communes.
- → Au-delà de la remontée de données, les actionneurs demandent une vigilance particulière. Dans la mesure du possible, séparer le réseau IoT du réseau local informatique (notamment le cas d'un réseau porté par une structure de mutualisation).
- → Certains problèmes de remontée sont le signe d'un brouillage des ondes et non d'une cyberattaque, se référer à la documentation de l'ANFR (Agence Nationale des Fréquences).

PLATEFORME DE DONNÉES

- → Exiger une conception robuste : « **security by design », ISO 27001**, attention aux solutions où la sécurité est reportée à des version ultérieures
- → Détecter les **communications anormales** au niveau de la plateforme pour protéger l'intégrité de la donnée
- → Sécuriser l'hébergement : pour les collectivités, étudier **la localisation et la redondance** du data center dès la sélection du prestataire, pour faire un choix éclairé. Définir le besoin de sauvegardes, sécuriser la possibilité de conserver des sauvegardes et en préciser le format.
- → Isoler, garantir l'intégrité des données : **une segmentation des SI (systèmes d'information) par criticité** est conseillée avec l'installation de pares-feux.
- → Documenter et planifier : l'intégrateur/opérateur se doit de livrer **un plan d'action** cartographiant l'environnement, les préconisations prioritaires (difficulté/coût/capacité), à l'éditeur de fournir **un dossier d'architecture technique** (flux, modules...)

SYSTÈME GLOBAL

- → Cadrer : les cahiers des charges doivent inclure **des clauses cyber précises** (maintien en condition de sécurité des équipements, matrice d'exigences, moyens/résultats), incluant des responsabilités et des pénalités. Il est important de challenger les prestataires et de **cibler les exigences pour ne pas le surcharger, donc prendre une approche stratégique** (niveau acceptable de risque adapté aux cas d'usage mis en place).
- → Définir une **politique cyber (PSSI) qui concerne toute la chaîne de valeur** et un Plan d'Assurance Sécurité.
- → Pour les équipementiers, il est essentiel d'appliquer les normes existantes (cf **annexe**)

HUMAIN

- → Sensibiliser : d'une part sur le **risque juridique d'acheter des équipements non sécurisés, sur la nécessité d'impliquer la DSI et la RSSI dans les projets métiers**, d'autre part au niveau des utilisateurs (formations selon le public : métiers, transverses, comité de direction pour la gestion de crise...)
- → La DSI a un rôle essentiel de coordination et de définition du cahier des charges
- → Professionnaliser, dédier des ressources : pour pérenniser la maintenance, les collectivités doivent définir un référent interne. Sur l'ensemble du projet, des métiers dédiés (responsable RSSI, data analyste...) sont à mobiliser.
- → **Tester** : organiser des simulations d'attaque/phishing, tester concrètement les crises et s'inscrire dans une logique d'amélioration continue (audits, tests d'intrusion...)

POUR LES PETITES COMMUNES :

Il est conseillé de se rapprocher de **structures de mutualisation** qui portent les différentes couches de manière sécurisée. Cette mutualisation permet de bénéficier de ressources (formation...) et **d'optimiser les coûts** : économies sur les frais d'audits via un catalogue de services **« clé en main »**, sur les **frais de maintenance** et de mise en conformité, et diminution du **risque juridique d'achats isolés**. Il est également conseillé de participer à des groupes de travail ou des réseaux de DSI, et de recourir à un AMO mutualisé, en l'absence d'un recrutement en temps plein. Cela évite d'avoir recours à des solutions présentant des risques de souveraineté, d'interopérabilité, de pérennité comme d'évolutivité des projets.

L'AMO peut accompagner la définition du besoin et du juste dimensionnement.

Il n'existe pas de certification, il est possible de construire un catalogue d'objets « validés » par l'écosystème ou de faire certifier des objets (cela représente un coût important).

Sur des points de captation et des cas d'usage critiques, envisager un réseau de secours en cas d'attaques (par exemple redondance sur la détection de fortes crues en zone sensible).

Pour la structure de mutualisation, agir comme gestionnaire de la donnée signifie assumer la responsabilité cyber par des clauses dédiées.

L'éditeur peut proposer d'accompagner la collectivité sur la sécurisation et la redondance de l'hébergement des données.

L'intégrateur/opérateur, tout comme la structure de mutualisation, peut proposer une prestation SOC (Centre des Opérations de Sécurité), dont le niveau se définit selon les ressources humaines et financières (contrôle continu, plages horaires...).

De manière générale, se faire accompagner sur la maturité cyber sur les plans techniques et humains : l'AMO, les éditeurs, les équipementiers et les intégrateurs ont un rôle de conseil et d'accompagnement à jouer.

Les structures de mutualisation peuvent favoriser un écosystème solidaire, d'échange de bonnes pratiques, voire piloter des groupes de travail pour accompagner, auditer et sensibiliser les communes.

LA CYBERSÉCURITÉ A UN COÛT :

L'investissement cyber est estimé entre **5 et 15% du budget total**, un audit de sécurité spécifique entre 5 000 et 10 000€ HT selon le périmètre, les certifications de capteurs entre 10 000 et 30 000€ HT selon l'implication du client et la certification visée. Il est recommandé d'éviter d'exiger un niveau de sécurité maximum partout, cela double la facture sans nécessité réelle. Il faut également prendre en compte les coûts de la maintenance : mises à jour, audits de sécurité réguliers...

10 RECOMMANDATIONS
Les messages clés du groupe de travail

TROUVER LES MÉTHODES

1 **Il n'y a pas de vide méthodologique théorique** : la théorie est complète, transposable, et des recommandations, normes et standards existent (voir annexe).

2 Les nouveautés viennent du **domaine d'application** (interaction avec les métiers, surface d'exposition plus grande), de la **diversité d'acteurs**, du **niveau de maturité** de l'écosystème et de règlementation spécifique (peu existante sur les projets IoT mais à venir) qui évoluent (Intelligence Artificielle...).

INITIER UNE STRATÉGIE

3 Chaque industriel de la **chaîne de valeur** peut avoir un rôle à jouer en fonction de son niveau d'expertise et avoir anticipé proactivement des **bonnes pratiques – s'informer dès le cahier des charges**. Certains peuvent même en porter la responsabilité avec des **offres dédiées intégrées** dans l'exploitation-maintenance des capteurs/du réseau/de la plateforme de données. Cette stratégie doit s'adapter aux risques et cas d'usage locaux.

4 **Être accompagné** semble indispensable, a minima au début et pour les audits réguliers. **Une structure de mutualisation, un AMO dont l'expertise est partagée** entre des communes, sont des pistes à suivre.

BIEN ESTIMER LES COÛTS

5 Il faut anticiper un **surcoût** : d'une part dans l'accompagnement (audits, gestion de crise...), d'autre part dans l'achat des équipements et des logiciels (« security by design »).

6 **Il est toujours possible de sécuriser a posteriori** des équipements ou logiciels peu fiables mais le coût sera alors bien **plus élevé** qu'en l'anticipant dès l'achat.

DÉFINIR LES RESPONSABILITÉS

7 **Il est nécessaire de définir la responsabilité de chaque acteur de la chaîne de valeur dès le cahier des charges, et de la contractualiser**. Certains recommandent un découpage par domaine d'expertise : l'éditeur de plateforme responsable de la plateforme, l'intégrateur des capteurs, l'opérateur du LNS (cœur de réseau)...

NB : Cela ne dispense pas d'une **analyse complète** des risques cyber en amont de la mise en œuvre du projet.
NB : La collectivité **demeure responsable en cas d'impact sur les données** (fuites...), car elle est propriétaire des données. Lorsque la collectivité est une structure de mutualisation pour d'autres, elle devient exploitante de la donnée et est responsable des données que les communes lui ont confiées. Au-delà du risque juridique, **le risque pour l'image de la collectivité et la poursuite d'autres projets IoT est crucial.**

APRÈS LA MISE EN PLACE

8 **Tout ne peut pas être anticipé**, il y aura toujours des risques et des attaques. Une bonne politique cyber permet de **détecter, retarder, limiter les impacts, de réagir de manière proportionnée à l'impact réel**.

9 **Une crise cyber peut aussi être un déclencheur d'une politique cyber plus robuste,** à condition de cartographier les bons interlocuteurs avec la DSI et d'avoir un plan de crise.

10 **Le facteur humain et organisationnel** est une vulnérabilité clé. Il faut veiller à la coordination avec les DSI dès le début du projet, puis à la formation sur le temps long de l'ensemble des parties prenantes.

RETOUR D'EXPÉRIENCE : TESTER LA CYBERSÉCURITÉ EN PRATIQUE

La métropole de Montpellier a lancé son expérimentation de projet de territoire durable et connecté dès 2016. Aujourd'hui, la métropole compte plus de 50 000 objets connectés (45 000 sur la seule télérelève de l'eau). Ceux-ci communiquent sur un réseau LoRa (Long Range, « longue portée ») propriétaire grâce à une trentaine de Gateway (une quarantaine à terme) en couvrant 100% des 31 communes. Gestions des points d'apports volontaires pour les déchets, capteurs pour la qualité de l'air, d'humidité et de températures dans les musées pour la préservation des œuvres d'art, de surveillance et des gestions des crues... remontent leurs données sur un système d'information centralisé et sécurisé.

Cette sécurisation est assurée 24/7 par un SOC (Centre des Opérations de Sécurité) **mis en œuvre par une société externe**. De plus, une autre entreprise réalise **des simulations d'attaques depuis 8 ans**, notamment sur l'IoT. **Des tests d'intrusions sur le réseau LoRa** ont également été menés régulièrement, par exemple à l'occasion de **hackathons menés par des étudiants**. Enfin, **un réseau de secours** est prévu en cas d'indisponibilité de l'infrastructure LoRa pour les données sensibles.

RETOUR D'EXPÉRIENCE : QUESTIONNER SES PRESTATAIRES

Afin de renforcer la maîtrise des solutions numériques, le SIEEEN a mis en place un **questionnaire pour ses prestataires**. Cette démarche vient d'un besoin identifié : bénéficier d'une base de discussion solide face aux prestataires, afin de conserver un pouvoir de décision. L'objectif reste une sensibilisation, de pousser la maturité de l'écosystème (notamment en anticipation de la directive NIS 2). Ce questionnaire est partagé dès le sourcing.

L'objectif est d'ajouter aux questions techniques usuelles (fonctionnalité, ergonomie...) une dimension dépassant le métier : cybersécurité, souveraineté, redondance... Quelques exemples de questions : les serveurs utilisés, les API (interface de programmation d'application) disponibles, les droits d'accès aux bases de données, le lieu d'hébergement, la capacité à sauvegarder en propre en parallèle (par exemple pour de plus longues durées de rétention), le déroulé des mises à jour, la présence d'un PAS (Plan d'Assurance Sécurité)...

Utilisé depuis 2 ans, cet outil mène à une note de qualité et ouvre la possibilité pour les prestataires de proposer des alternatives. Il sert avant tout à interroger et échanger, en définissant une base de discussion qui nourrit les aller-retours avec les décideurs et les interlocuteurs techniques. Certains éléments sont ensuite sécurisés contractuellement, par convention ou marché public.

RETOUR D'EXPÉRIENCE : METTRE EN PLACE UN PROCESSUS D'AGRÉMENT

Dès 2014, Rennes a expérimenté un réseau bas débit longue portée open source baptisé « LoRa Fabian ». Après cette phase expérimentale, la collectivité est passée, début 2025, à la généralisation de la gestion technique des bâtiments publics, de l'efficacité énergétique, de la qualité de l'air, des risques de crues, des points d'apports volontaires de déchets, de l'éclairage public ou la relève des compteurs d'eau, etc.

La plateforme IoT vise l'interopérabilité par l'agrégation et la standardisation de données issues de ce large écosystème pour nourrir des superviseurs métiers. Il s'agit désormais de massifier les cas d'usages et de multiplier le nombre de capteurs (5000 actuellement pour 72 antennes LoRa) sur l'ensemble du territoire métropolitain, en accompagnant ses 43 communes.

Comment assurer la cybersécurité des 57 000 capteurs prévus à l'horizon 2030 ? Tout part de la **stratégie numérique responsable rennaise et d'une PSSI initiée dès 2020**. La métropole a fait appel à un AMO **pour l'analyse cyber et risque qui est ensuite assurée par la RSSI**, avec un contrôle interne et un suivi précis de tous les prestataires impliqués. Chaque projet est examiné à la fois par le DPO et le RSSI, via un **PMO et un comité de suivi des systèmes industriels** (systèmes d'assainissement, Gestion Technique Batimentaire...). Rennes a aussi mis en place **un processus d'agrément par capteur et par cas d'usage**. Cette exigence a conduit le principal prestataire à mettre au point une offre renforcée baptisée CyberPlus. Ces processus, imposés aux fabricants de capteurs, sont vertueux pour la métropole comme pour ses prestataires.

ANNEXE : LES STANDARDS

- **Cadre réglementaire et législatif** : RGPD, NIS 2, IA Act, Data Act
- **Évolution européenne à l'horizon 2027 (CRA)** : Anticipation du Cyber Resilience Act qui imposera aux fabricants des obligations de sécurité native pour tous les produits numériques
- **Normes de management** : ISO 27001/27002 pour structurer la gouvernance cyber et exiger un PAS
- **Standards techniques IoT et industriels** : norme ETSI EN 303 645, IEC 62443 pour la sécurisation des automates et des systèmes urbains, ISO 15408, FIPS 140

Guides & livres blancs :

- **ANSSI** : Méthode EBIOS Risk Manager, guide PSSI, recommandations Objets connectés (2021), méthode de classification des systèmes industriels (2025)
- **CNIL** : PIA pour les objets connectés (2018), Pack conformité pour les compteurs communicants (2014)
- **SBA** : La cyber sécurisation des bâtiments tertiaire (2023)
- **ANFR** : Enquête sur le brouillage des ondes (2024)

Comité Stratégique de Filière Infrastructures Numériques

Le 22 novembre 2018, le Conseil national de l'industrie a labellisé le Comité stratégique de filière relatif aux infrastructures numériques. Quatre fédérations sont à l'initiative de ce contrat lequel a été renouvelé en 2023. Aujourd'hui, la filière Infrastructures numériques rassemble les fabricants de composants et d'équipements réseaux, les opérateurs d'infrastructures fixe et mobile et de services de communications électroniques, les fabricants de matériels et câbles de communication/très haut débit et les industriels des réseaux d'initiative publique. Elle peut également compter sur de nombreux centres de recherche et pôles de compétitivité pour favoriser son essor économique et développer les activités de R&D.

Groupe de travail Territoires connectés et durables

Dans le cadre du CSF Infrastructures numériques, un groupe de travail a été créé en 2020 pour construire une vision commune des « territoires connectés et durables » avec l'ensemble des parties prenantes. A ce titre, plusieurs associations de collectivités contribuent à ce groupe de travail. Les résultats sont le fruit de la concertation entre fédérations d'industriels, associations de collectivités et partenaires institutionnels.

Référents : Luc Derriano - Avicca, Agnès le Meil - InfraNum

Conception : Astrid Voorwinden, Hichem Midoun et Paola Ropele - InfraNum

Contributeurs : Montpellier, SIEL 42, SIEEEN, SIPPEREC, Berry Numérique, Rennes, Artelia, ON-X, Orange, Sogetrel, Synox, Eridanis, Lacroix, Tektelic, Ubicité