

# Prévention et détection des incendies en forêt

Anthony Vasta, Evan Galli, Sacha Castillejos

*- Partie Architecture -*

Ce projet propose un système IoT pour la prévention et la détection précoce des incendies de forêt, combinant capteurs connectés, caméras intelligentes et analyse prédictive. L'architecture conçue permet une surveillance en temps réel, une transmission rapide des alertes et un meilleur usage des forces d'intervention tout en limitant l'impact environnemental.

2025-11-03

## Avant-Propos

Des outils d'intelligence artificielle ont été utilisés pour la reformulation des phrases de ce rapport

### Ubiquitous langage

| Terme                      | Définition   |
|----------------------------|--|
| Capteur                    | Dispositif IoT installé en forêt mesurant un ou plusieurs paramètres environnementaux (température, humidité, pression, gaz, vent...). Source principale de données brutes du système.       |
| Centrale météo             | Station combinant plusieurs capteurs environnementaux pour évaluer les conditions climatiques locales (humidité, vent, température, pluviométrie). Sert à l'évaluation du risque d'incendie. |
| Agrégateur forêt           | Serveur Fog dédié à une zone forestière donnée. Centralise, traite et stocke les données locales avant transmission vers le Cloud.   |
| Alerte incendie            | Notification automatique transmise au CODIS ou aux opérateurs lorsqu'un risque ou un départ de feu est confirmé. Peut être graduée selon le niveau de confiance.                             |
| Carte de risque            | Représentation dynamique (heatmap) du niveau de danger d'incendie par zone, calculée à partir des données locales et externes.   |
| CODIS                      | Centre Opérationnel Départemental d'Incendie et de Secours. Destinataire principal des alertes et interface de validation humaine des détections.  |
| Données externes           | Informations provenant de sources tierces (Météo France, satellites FIRMS, Kéranos, IGN, etc.) utilisées pour enrichir les modèles.  |
| Interface de visualisation | Application web ou mobile permettant la consultation en temps réel des alertes, cartes et historiques.   |

### Hypothèse de travail

Nous posons comme hypothèse que les tours de guet forestières bénéficient d'un accès au réseau cellulaire. Cette hypothèse est plutôt réaliste car les tours de guets sont généralement localisées à relative proximité d'axes routiers et en altitude sur des points topographiques dominants. Ce qui leur permet de capter les signaux cellulaires sans blocage des ondes dû au relief. Sur 20 tours de guet étudiées seules 4 disposaient d'une connectivité limitée (sans être nulle pour autant).

# Table des matières

|   |    |
|---|----|
| Avant-Propos .....  | 2  |
| Ubiquitous langage .....  | 2  |
| Hypothèse de travail .....  | 2  |
| 1. Description du projet .....                                      | 4  |
| 1.1. Forêt intelligente et prévention proactive .....               | 4  |
| 1.2. Analyse des risques d'incendie et cartographie dynamique ..... | 4  |
| 1.3. Détection avancée des menaces .....                            | 4  |
| 1.4. Réduction du risque de propagation .....                       | 4  |
| 1.5. Communication et alerte en temps réel .....                    | 4  |
| 1.6. Valeur ajoutée du projet .....                                 | 5  |
| 1.7. Contraintes .....  | 5  |
| 1.8. Domain Driven Design .....                                     | 6  |
| 1.8.1. Domaines principaux .....                                    | 6  |
| 1.8.2. Domaines de support .....                                    | 7  |
| 1.8.3. Domaines génériques .....                                    | 7  |
| 2. Analyse utilisateurs .....                                       | 8  |
| 2.1. Utilisateurs .....   | 8  |
| 2.2. Story telling .....  | 8  |
| 2.2.1. Scénario 1 : Détection incendie .....                        | 8  |
| 2.2.2. Scénario 2 : Prévention incendie .....                       | 8  |
| 2.2.3. Scénario 3 : Analyse des données .....                       | 8  |
| 2.3. User stories .....   | 10 |
| 3. Analyse des risques .....  | 11 |
| 3.1. Perte de données .....   | 11 |
| 3.2. Qualité des données .....                                      | 11 |
| 3.3. Cyberattaque .....   | 11 |
| 3.4. Perte de disponibilité .....                                   | 11 |
| 3.5. Faux positif ou incendie non détecté .....                     | 12 |
| 3.6. Non-acceptation .....  | 12 |
| 3.7. Risques environnementaux .....                                 | 12 |
| 4. Impacts architecturaux et fonctionnels .....                     | 13 |
| 4.1. Perte de données .....   | 13 |
| 4.2. Qualité des données .....                                      | 13 |
| 4.3. Risques de sécurité .....                                      | 13 |
| 4.4. Perte de disponibilité .....                                   | 13 |
| 4.5. Mauvaise détection ou mauvaise prévention .....                | 13 |
| 4.6. Acceptation .....  | 14 |
| 4.7. Risques environnementaux .....                                 | 14 |
| 5. Architecture .....   | 15 |
| 5.1. Déploiement .....  | 15 |
| 5.2. Transit des données .....                                      | 16 |
| 5.3. Description détaillée .....                                    | 17 |
| 5.4. Topics .....   | 19 |

# **1. Description du projet**

La prévention et la gestion des incendies de forêt représentent aujourd'hui un enjeu majeur, tant pour la protection de l'environnement que pour la sécurité des populations et des infrastructures. Un système basé sur l'Internet des Objets (IoT) permet d'apporter une réponse innovante et efficace à ces défis.

## **1.1. Forêt intelligente et prévention proactive**

L'intégration de capteurs connectés, de caméras thermiques et de systèmes de détection rend la forêt « intelligente ». Les données collectées en temps réel permettent d'identifier les signaux faibles d'un départ de feu et de déclencher des alertes immédiates avant que la situation ne devienne critique.

## **1.2. Analyse des risques d'incendie et cartographie dynamique**

Un module de cartographie interactive évalue en continu le risque d'incendie par secteur, en prenant en compte plusieurs paramètres :

- conditions météo (humidité du sol et de l'air, vent, chaleur, sécheresse, ...),
- caractéristiques du terrain (type d'arbres, densité de végétation, éléments naturels coupe-feu, topographie),
- proximité des habitations et infrastructures sensibles,
- accessibilité pour les secours.

Cette analyse permet de hiérarchiser les zones à surveiller et de renforcer la prévention dans les secteurs les plus vulnérables.

## **1.3. Détection avancée des menaces**

Notre système offrent plusieurs couches de détection :

- caméras thermiques pour repérer les points de chaleur anormaux,
- caméras optiques pour identifier les fumées
- capteurs environnementaux pour mesurer les seuils critiques (humidité de l'air, humidité du sol, pluviométrie, température, vitesse du vent, pression de l'air, présence de gaz).

La combinaison de ces données améliore considérablement la précision des alertes.

## **1.4. Réduction du risque de propagation**

En analysant la topographie, la densité forestière, et les données météorologiques remontées par nos capteurs (telles que l'humidité et le vent) le système peut anticiper les trajectoires probables d'un incendie. De plus, il peut suggérer des actions de prévention ciblées comme le débroussaillage ou le déboisement sélectif dans des zones stratégiques pour limiter la propagation des flammes.

## **1.5. Communication et alerte en temps réel**

Un élément essentiel du projet est la capacité à notifier rapidement le centre de traitement de l'alerte (CTA) au sein du centre opérationnel départemental d'incendie et de secours (CODIS) de rattachement.

En cas de dépassement de seuil critique de risque incendie (Température > 30 °C, humidité de l'air < 30 %, Indice Forêt Météorologique (IFM)  $\geq$  40, ...) ou en cas de détection d'un départ de feu, le système alerte le CTA en lui indiquant l'ensemble des données de la zone concernée.

Cette réactivité améliore le traitement préventif des forêts et le temps nécessaire à la coordination des pompiers au travers du CODIS lors de départ d'incendie.

## **1.6. Valeur ajoutée du projet**

Le projet apporte une valeur ajoutée majeure à la prévention et à la gestion des incendies de forêt en combinant détection précoce, analyse prédictive, transmission instantanée de l'information et déclenchement automatisé d'alertes.

Grâce à notre réseau de capteurs et caméras, les départs de feu sont identifiés avant qu'ils ne deviennent incontrôlables, améliorant ainsi la réactivité des secours par conséquent les dommages.

La connaissance fine du terrain et des risques par le système permet de produire une cartographie dynamique du risque et donc d'anticiper la propagation potentielle des flammes et d'adapter les actions préventives sur les zones les plus vulnérables. En offrant une vision en temps réel de l'état de la forêt et des conditions environnementales, le système optimise la surveillance, la prise de décision et la coordination des acteurs.

## **1.7. Contraintes**

Sur le plan environnemental, l'installation de capteurs, caméras et antennes peut entraîner une pollution visuelle et être perçue comme une dégradation du paysage naturel. Les équipements introduisent également une empreinte écologique, notamment par l'utilisation de batteries et de matériaux potentiellement polluants, ou par les perturbations qu'ils peuvent provoquer sur la faune locale. Il est donc essentiel de minimiser l'impact du dispositif et de garantir sa parfaite intégration dans l'écosystème forestier.

L'énergie constitue également une contrainte majeure. Les zones forestières sont souvent difficiles d'accès, ce qui rend la maintenance et le remplacement des sources d'alimentation complexes et coûteux. Les dispositifs doivent assurer une autonomie durable, capable de supporter un fonctionnement continu sur plusieurs années. Le choix de solutions énergétiques résilientes, telles que des systèmes solaires ou des technologies basse consommation, est indispensable pour éviter toute interruption de surveillance pouvant compromettre la détection précoce des incendies.

À cette difficulté s'ajoute celle de la connectivité. Les réseaux traditionnels (comme la 4G ou la 5G) étant rarement disponibles en milieu forestier, il est nécessaire de mettre en place une infrastructure de communication dédiée. Les technologies longue portée et faible consommation (par exemple LoRaWAN) doivent garantir l'acheminement fiable des données en temps réel vers les centres de supervision. Le réseau doit rester opérationnel, même dans des conditions extrêmes telles que la dégradation des équipements causée par un incendie, ce qui nécessite des solutions robustes et redondantes.

Enfin, le projet doit relever des défis économiques et organisationnels importants. Le déploiement initial représente un investissement considérable, auquel s'ajoutent les coûts de

maintenance, de gestion des données et de renouvellement du matériel. Sa pérennité suppose ainsi un modèle financier viable, soutenu par des partenariats publics et privés.

## 1.8. Domain Driven Design

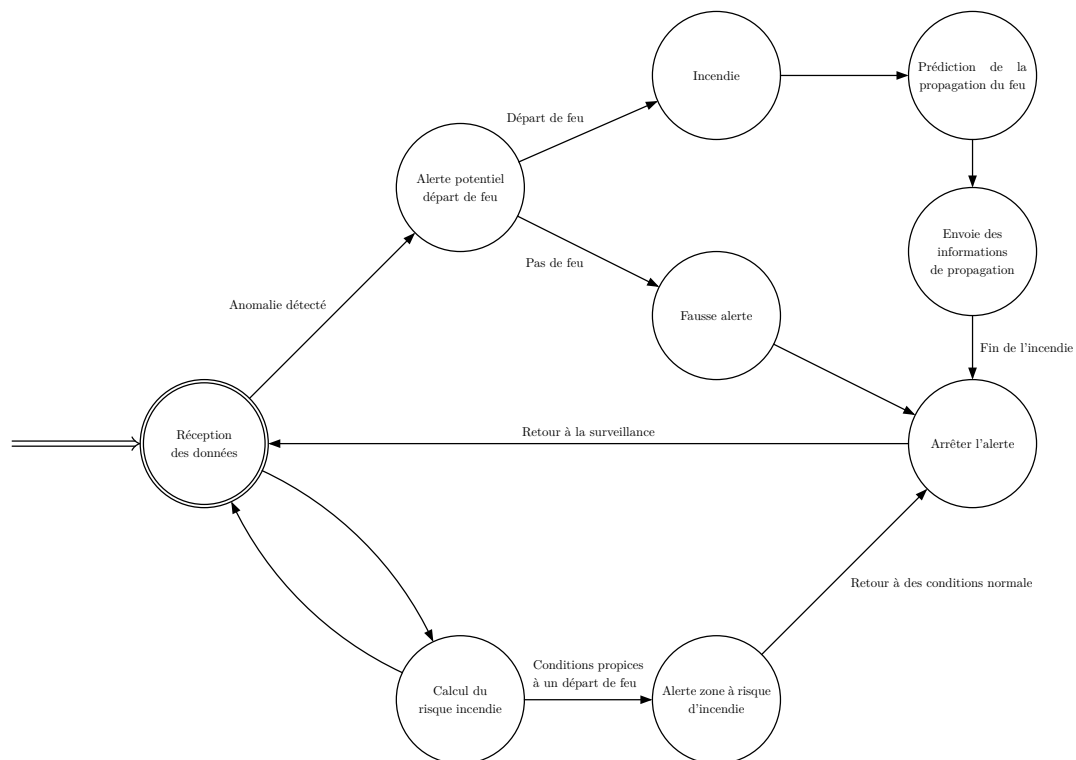


Fig. 1. – Machine à état métier

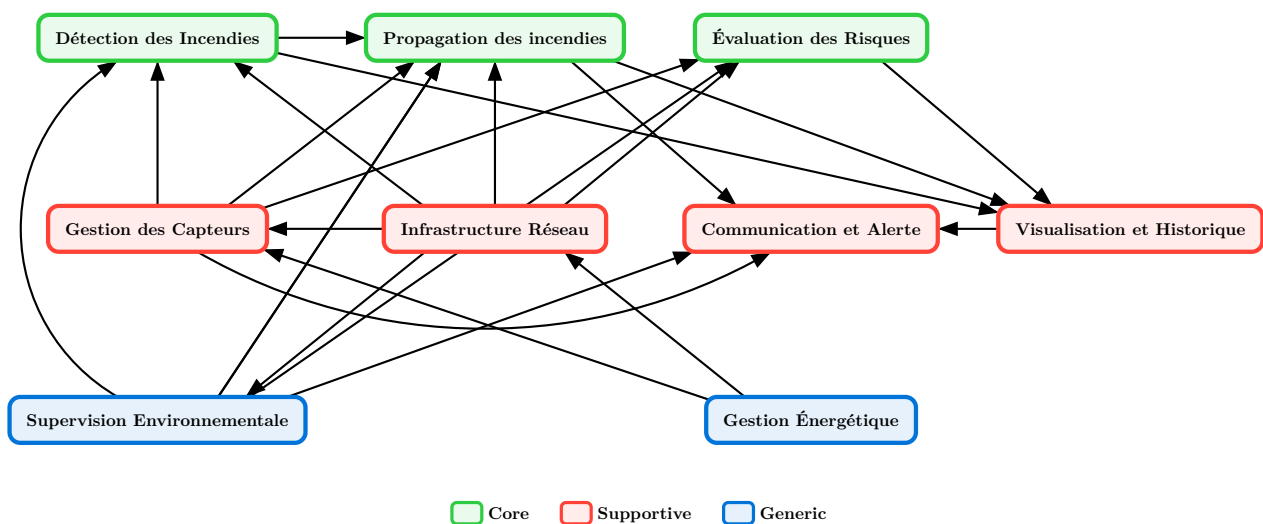


Fig. 2. – Context map

### 1.8.1. Domaines principaux

- **Détection d'incendie** : Analyse en temps réel des données remontées pour identifier les signes précurseurs d'un départ de feu et déclencher des alertes précises dès qu'un seuil critique est atteint .
- **Propagation de l'incendie** : Anticipe la trajectoire et la vitesse de propagation des flammes en analysant la topographie, la densité de végétation et la direction du vent. Aide à identifier les zones à risque afin de planifier les interventions et l'évacuation des zones menacées.

- Évaluation du risque d'incendie : Calcule dynamiquement le niveau de risque incendie par zone forestière en tenant compte de multiples paramètres : conditions météorologiques, sécheresse, type de sol, végétation, proximité d'habitations ou de routes. Cette analyse prédictive offre une vision dynamique et hiérarchisée du niveau de danger.

### **1.8.2. Domaines de support**

- Gestion des capteurs : Un mécanisme d'auto-diagnostic identifie automatiquement les capteurs défectueux ou déconnectés afin d'assurer la continuité et la qualité des données collectées.
- Visualisation et historique : Les informations issues du réseau IoT (données des capteurs et des images capturées par les caméras) sont centralisées dans une interface permettant leur exploitation par les autorités, chercheurs ou opérateurs. Cette base de données facilite le suivi en temps réel et l'analyse historique des phénomènes.
- Communication et alertes : Lorsqu'un risque ou un incendie est détecté, le système émet des alertes automatiques à destination des gardes forestiers et du CODIS, avec la localisation exacte du danger.
- Infrastructure Réseau : Garantit la connectivité fiable en milieu forestier via des technologies LoRaWAN. Assure la redondance et la résilience des communications même en conditions extrêmes.

### **1.8.3. Domaines génériques**

- Gestion énergétique : Maximise la durée de vie des batteries et gère les sources d'énergie alternatives (solaire). Prédit les besoins de maintenance énergétique.
- Supervision Environnementale : Mesure et archive en continu les paramètres environnementaux. Fournit les données brutes aux autres sous-systèmes.

## **2. Analyse utilisateurs**

### **2.1. Utilisateurs**

- Gardes-forestier
- Centre Opérationnel Départemental d'Incendie et de Secours (CODIS)
- Police scientifique
- Scientifique
- Équipe de maintenance

### **2.2. Story telling**

#### **2.2.1. Scénario 1 : Détection incendie**

Je suis opérateur au CODIS, en charge de la surveillance et de la coordination des secours dans le département.

Je reçois une notification d'alerte automatique indiquant une hausse anormale de la température et la présence de fumée dans une zone forestière.

Je visualise immédiatement la zone concernée sur la carte fournie par l'application du système.

La zone suspecte apparaît en rouge, accompagnée des informations précises de localisation et des relevés des capteurs environnants.

J'accède ensuite au flux en direct de la caméra optique installée à proximité du foyer détecté.

Les images confirment la présence d'un départ de feu actif.

Le système me fournit automatiquement une analyse prédictive de propagation, indiquant les zones alentour vers lesquelles le feu est susceptible de se déplacer, en tenant compte du vent, de la température et de la topographie.

Je déclenche la procédure d'intervention et dépêche immédiatement les équipes de sapeurs-pompiers les plus proches sur place.

#### **2.2.2. Scénario 2 : Prévention incendie**

De fortes chaleurs sévissent depuis plusieurs jours et certains bois sont très sec.

Je suis le garde forestier en charge de la zone

Le système me notifie lors du dépassement de certains seuil et me propose une carte des zones à risque

Il me propose des zones à débroussailler de manière préventive et à interdire d'accès

Je prend les mesures nécessaires sur la zone et je suis particulièrement vigilant

#### **2.2.3. Scénario 3 : Analyse des données**

Un incendie semblant être d'origine criminelle a eu lieu dans une zone forestière équipée du système de prévention.

En tant que membre de la police scientifique, je suis chargé d'analyser les données enregistrées par le système au moment de l'incident.



J'accède à l'historique des images capturées par les caméras situées à proximité du point de départ du feu.

Je consulte également les données des capteurs (température, CO<sub>2</sub>, fumée, etc...) collectées durant la même période.

En croisant ces informations, je peux reconstituer les événements et identifier la zone exacte d'origine du feu.

Les éléments visuels et les données capteurs sont utilisées pour étoffer les informations de l'enquête.

## 2.3. User stories

En tant qu'opérateur chez le CODIS, je veux que le système m'indique les zones à risque, afin d'agir en conséquences

---

En tant qu'opérateur chez le CODIS, je veux être notifié en cas d'incendie et pouvoir visualiser la ou les zones concernées par l'alerte, afin de pouvoir confirmer qu'un incendie a bien lieu et dépêcher une équipe de pompier sur place.

---

En tant qu'opérateur chez le CODIS, je veux pouvoir prédire les zones sur lesquelles le feu risque de se propager, afin d'anticiper l'évolution du front de feu, et d'orienter les équipes d'interventions pour faciliter le travail des pompiers

---

En tant qu'opérateur chez le CODIS, je veux que le système s'adapte en cas de perte de données, afin de conserver une couverture sur l'ensemble de la zone

---

En tant que garde forestier, je veux que le système m'alerte au plus vite en cas d'augmentation du risque incendie pour une zone de la forêt afin de pouvoir limiter son accès et programmer un débroussaillage préventif.

---

En tant que garde forestier, je veux que le système m'alerte au plus vite en cas de détection d'un début d'incendie, afin que je puisse me rendre sur place pour assurer la sécurité des personnes et l'éteindre si son ampleur me le permet.

---

En tant que police scientifique, je veux avoir accès aux données enregistrées par le système, afin pouvoir mener des recherches sur l'origine d'un incendie

---

En tant que chargé de la maintenance, je veux être informé en cas de défaillance capteurs, afin de pouvoir planifier son remplacement

---

En tant que développeur du système, je veux avoir accès aux données historiques, afin de pouvoir faire évoluer le modèle en fonction des remontés du terrain.

### 3. Analyse des risques

La mise en place d'un système IoT pour la prévention des feux de forêt comporte plusieurs risques techniques et organisationnels qui peuvent compromettre son efficacité.

|               | MINEUR | MODÉRÉ                                  | MAJEUR                                   | CATASTROPHIQUE         |
|---------------|--------|---|--|------------------------|
| Très fréquent |        |   |  |                        |
| Fréquent      |        | Perte de données<br>Qualité des données |  |                        |
| Possible      |        |   | Faux positifs<br>non conformité<br>légal | Incendie non détecté   |
| Rare          |        | Cyberattaque                            |  | Perte de disponibilité |

Tableau 1. – Matrice de risques

#### 3.1. Perte de données

Un premier risque concerne la perte de données, qui peut survenir en cas de dégradations matérielles (par des animaux ou des actes de vandalisme), de pannes réseau (interférences locales ou coupure globale) ou encore de problèmes électriques (panne d'alimentation, court-circuit, surtension). L'architecture du réseau doit donc prévoir des mécanismes de redondance (réseau maillé, plusieurs passerelles, priorisation des flux critiques).

#### 3.2. Qualité des données

Avoir des capteurs opérationnels ne suffit pas : encore faut-il que les données remontées soient fiables. Or, en pleine forêt, la qualité des relevés peut rapidement se détériorer. Avec le temps, des branches, de la poussière ou de la mousse peuvent obstruer les capteurs ; certains équipements peuvent dériver ; des capteurs peuvent être en dehors de leur plage de fonctionnement (tension électrique par exemple) et fournir de mauvaises valeurs. À cela s'ajoute le risque de recevoir de mauvaises données issues de sources externes (par exemple de l'API météo).

#### 3.3. Cyberattaque

Tout système connecté est une cible potentielle, et celui-ci ne fait pas exception. Une attaque de type « Man-in-the-Middle » pourrait par exemple intercepter ou modifier les données en transit. Un attaquant pourrait injecter de fausses alertes... ou en masquer de vraies. Une compromission de la base centrale permettrait même de modifier les historiques ou les seuils d'alerte. Sans protection suffisante, un tel scénario pourrait remettre en question la crédibilité du système.

#### 3.4. Perte de disponibilité

Même sans attaque, un système peut devenir inutilisable à cause d'une surcharge ou d'un simple bug serveur. Les problèmes serveurs constituent une menace majeure : attaque par

DoS, surcharge, panne ou mauvaise configuration. Ces problèmes peuvent entraîner une perte de disponibilité ou une altération de l'intégrité des données. Si la plateforme centrale tombe en panne, le système ne peut transmettre d'alerte en temps réel, ce qui annule tout l'intérêt du dispositif.

### 3.5. Faux positif ou incendie non détecté

Un système de détection automatisé n'est jamais parfait, et deux erreurs opposées peuvent se produire : ne pas détecter un incendie réel (faux négatif), ou déclencher régulièrement des fausses alertes (faux positif). Le premier cas est évidemment le plus critique, mais le second ne doit pas être négligé, car un système qui alerte trop souvent finit par ne plus être pris au sérieux par les équipes terrain.

### 3.6. Non-acceptation

Même avec une technologie performante, le système peut échouer si les utilisateurs finaux ne l'adoptent pas réellement. Plusieurs scénarios peuvent poser problème : des opérateurs qui ignorent ou contournent une alerte parce qu'ils n'ont pas confiance dans l'outil, des équipes terrain qui ne sont pas formées à l'interprétation des indicateurs, ou encore un manque de coordination entre les différents acteurs. Le risque n'est pas technique ici, mais lié à l'usage : un mauvais alignement entre les procédures existantes et les nouvelles fonctionnalités peut entraîner une incompréhension, voire un rejet.

### 3.7. Risques environnementaux

Installer des capteurs, caméras ou antennes en forêt n'est pas neutre. Certaines zones protégées comme les réserves naturelles ou les espaces classés Natura 2000 imposent des restrictions strictes sur les installations permanentes. Enfin, l'ajout d'équipements physiques peut être perçu comme une pollution visuelle ou une perturbation écologique, notamment pour certaines espèces sensibles aux perturbations lumineuses ou électromagnétiques.

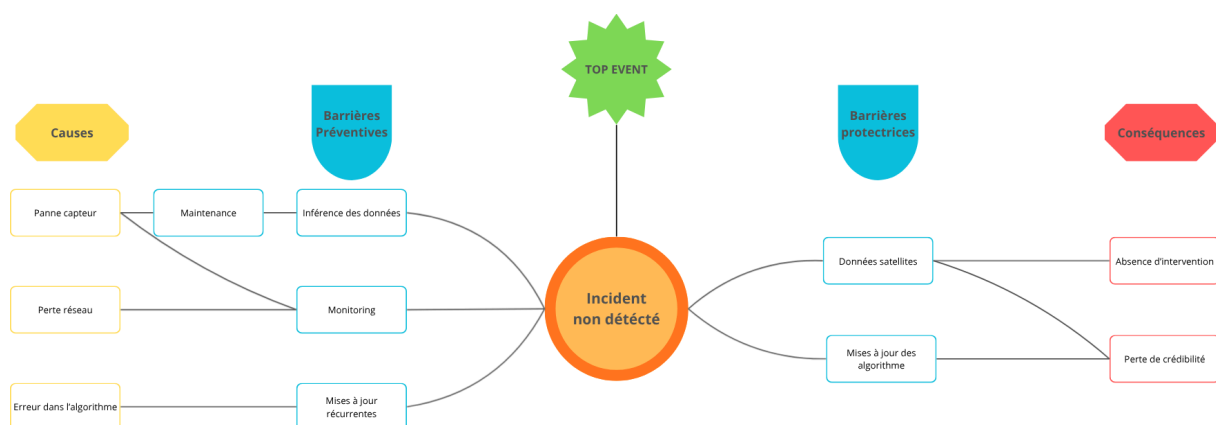


Fig. 3. – Bow tie

## **4. Impacts architecturaux et fonctionnels**

### **4.1. Perte de données**

Pour éviter la perte de données le protocole de transmission que nous avons choisi (LoRaWAN) permet le routage des messages par plusieurs passerelles, ce qui est utile en cas de défaillance de l'une d'elles.

Nous prévoyons aussi une double alimentation au niveau des passerelles (batterie + solaire) pour éviter la perte de transmission liée à une panne énergétique.

Pour éviter une perte d'énergie au niveau des stations capteurs, nous transmettons le niveau des batteries, ce qui permet d'être alerté avant qu'elles ne se vident.

Nous effectuons aussi un suivi de l'absence de perte de données grâce à une vérification automatique des paquets transmis.

En cas de perte ou d'interruption de transmission, le système met en œuvre des mécanismes d'inférence de données permettant d'estimer les valeurs manquantes à partir des mesures précédentes ou valeurs des capteurs voisins.

### **4.2. Qualité des données**

Pour garantir la cohérence du système, nous allons intégrer des contrôles automatiques. Cela inclura la comparaison entre capteurs proches, la détection d'anomalies statistiques, l'alerte en cas de dérive importante et la surveillance de l'état du système lui-même.

### **4.3. Risques de sécurité**

Pour maîtriser les risques de sécurité, nous allons concevoir le système en intégrant la sécurité dès sa conception.

Nous mettrons en œuvre le chiffrement systématique des échanges, l'authentification forte entre les équipements, la journalisation des accès et la segmentation du réseau pour contenir d'éventuelles compromissions.

### **4.4. Perte de disponibilité**

Pour éviter la perte de disponibilité, nous concevons un système capable de fonctionner sans cloud, grâce à un traitement sur le fog et l'envoi d'alertes push depuis celui-ci.

Les paquets LoRaWAN sont reçus par plusieurs antennes, ce qui permet de limiter l'impact de la perte de l'une d'entre-elles.

### **4.5. Mauvaise détection ou mauvaise prévention**

Pour éviter une mauvaise détection ou une mauvaise prévention, nous allons concevoir le système pour qu'il associe un niveau de confiance à ses alertes. Nous conserverons un historique des données pour affiner continuellement les algorithmes. Enfin, nous nous assurerons que toute alerte soit explicable.

## **4.6. Acceptation**

Pour assurer l'acceptation du système, nous prévoyons une phase d'accompagnement lors le déploiement. Cet accompagnement comprendra des formations, une documentation claire, des démonstrations concrètes et une écoute active des retours terrain.

## **4.7. Risques environnementaux**

Pour minimiser l'impact environnemental, nous limitons la densité de capteur à déployer. Et nous utiliserons un matériel discret, par exemple grâce à une peinture camouflage ou une intégration paysagère.

Nous anticiperons aussi les démarches administratives en amont, et nous garantirons que la collecte des données respecte strictement la réglementation en vigueur.

## 5. Architecture

### 5.1. Déploiement

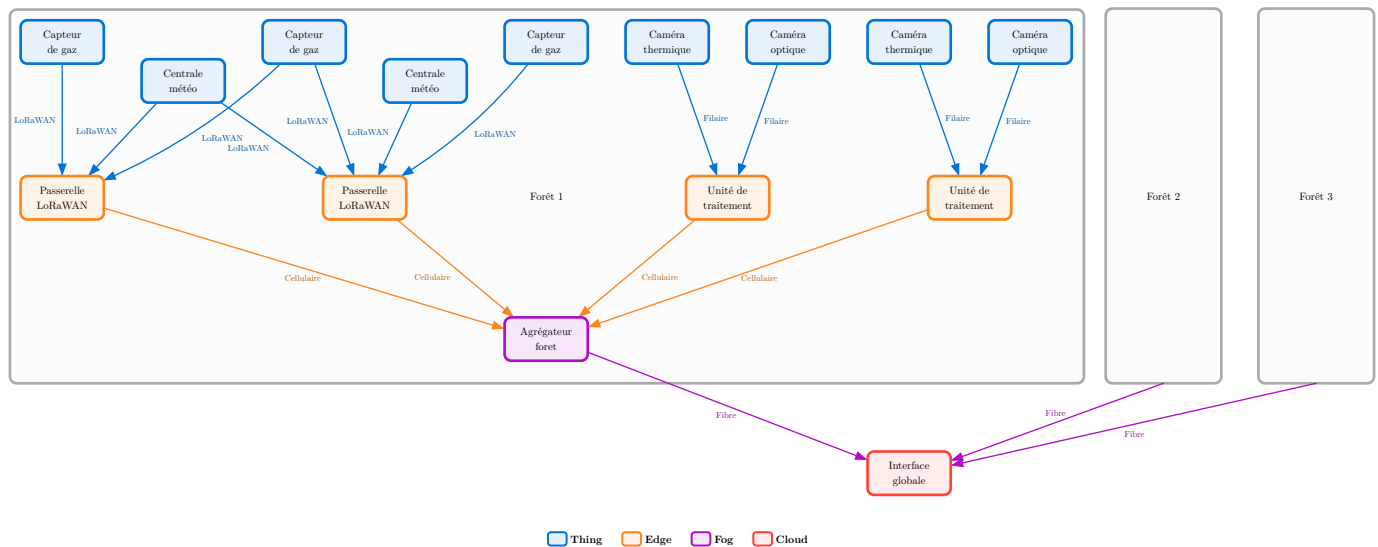


Fig. 4. – Exemple de structure de déploiement

Les capteurs de gaz sont déployés le long des zones à risques (axes routiers ou habitations par exemple). Ils fonctionnent sur batterie et envoient les données récoltées par LoRaWAN à la passerelle.

Les capteurs météo sont rassemblés en un seul appareil (dit « centrale météo ») qui sera déployé à des endroits représentatifs de la forêt. Les centrales météo fonctionnent elles aussi sur batterie et envoient leurs données par LoRaWAN.

Les passerelles LoRaWAN sont déployées dans des zones dégagées et reçoivent le réseau cellulaire. Au même endroit, les caméras optiques et thermiques seront reliées à un seul dispositif qui communiquera les flux par réseau cellulaire et fonctionnera sur batteries rechargées par panneaux solaires. L'alimentation est partagée avec les passerelles LoRaWAN.

Le serveur de gestion de la forêt (ou agrégateur) sera chargé de tous les calculs liés aux données remontées et stockera les données.

Finalement, le serveur cloud fournira une interface unifiée entre les différentes forêts gérées. Il ne stockera que les données générales (liées aux différentes cartographies proposées et aux alertes), les données plus précises seront obtenues par des requêtes au serveur agrégateur de la forêt concernée.

## 5.2. Transit des données

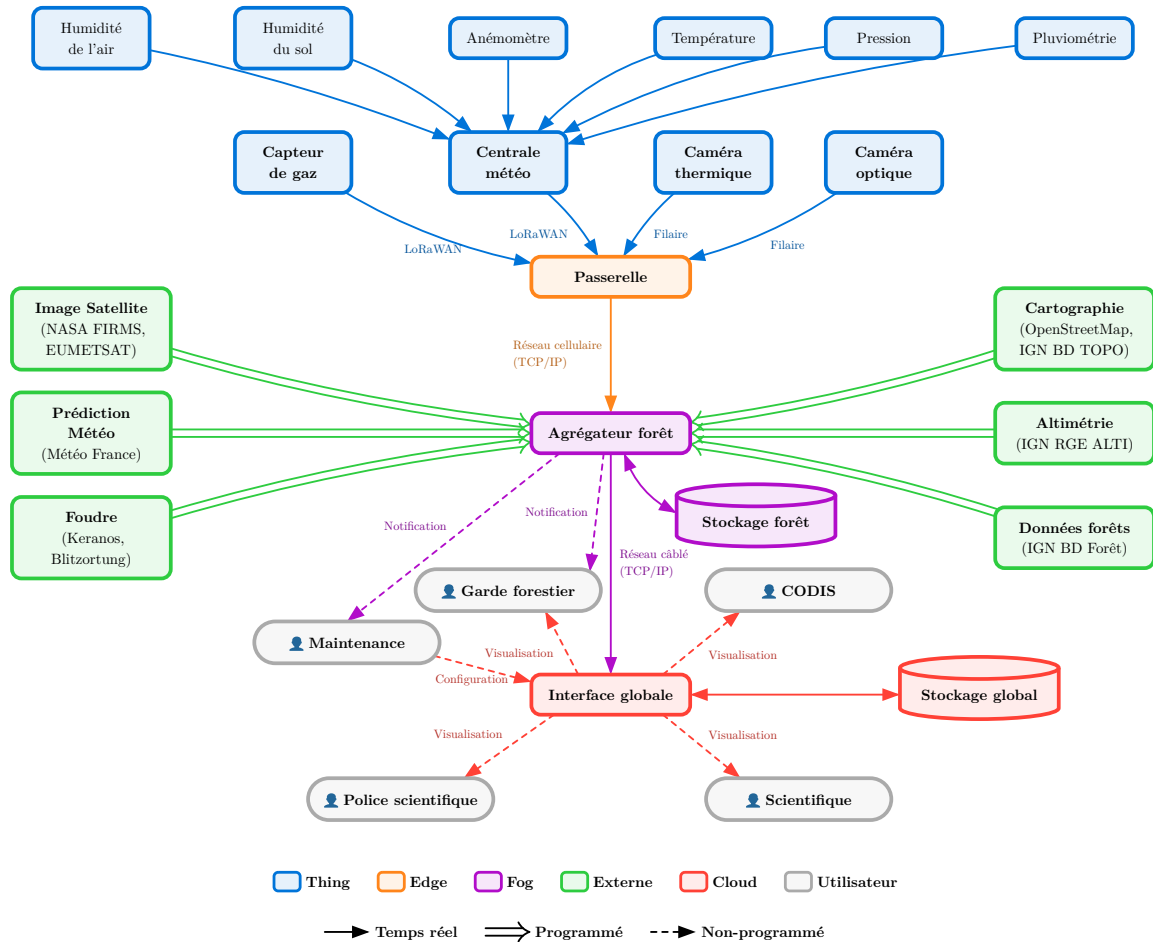


Fig. 5. – Vue des sources de données

La première étape concerne la collecte des données via des capteurs environnementaux (température, humidité, pression, gaz, etc.). Ces capteurs, connectés en LoRaWAN ou par liaisons filaires, transmettent leurs mesures à une passerelle locale qui les transmet à son tour à un agrégateur central.

L'agrégateur de forêt fusionne les données locales avec des sources externes telles que les prévisions météorologiques de Météo France, qui fournissent des données fiables sur les températures, les précipitations, la vitesse et l'orientation du vent, essentiels pour évaluer le risque d'incendie et modéliser sa propagation. Les images satellitaires, issues notamment de NASA FIRMS ou d'EUMETSAT, offrent une vue macro et permettent de détecter des points de chaleur ou des fumées naissantes à large échelle, complétant ainsi la détection locale. Les données de foudre, provenant de services spécialisés comme Kéranos ou Blitzortung, identifient les impacts de foudre susceptibles de déclencher un incendie, particulièrement dans les zones orageuses. Enfin, les données cartographiques et altimétriques de l'IGN, comme la BD TOPO ou le RGE ALTI, fournissent une modélisation fine du terrain, de la végétation et des infrastructures, permettant de contextualiser les alertes et d'affiner les prévisions de propagation.

Les données brutes sont conservées dans le fog, permettant une analyse locale rapide et un accès aux historiques. Seules les données traitées, telles que les cartes ou les alertes, sont envoyées vers le cloud.



Enfin, sur le cloud, les informations synthétisées sont accessibles via une interface globale, offrant des fonctions de visualisation, de consultation et de notification en temps réel aux gardes forestiers, CODIS et aux équipes scientifiques.

[illegible]

Les éléments déployés intègre tous un module de gestion de l'alimentation qui sera en capacité de donner les tensions et niveaux de charge des batteries, permettant ainsi de s'assurer que les capteurs sont dans des conditions normales d'utilisation et d'être alerté si un changement de batterie est nécessaire avant qu'il ne soit trop tard.

ARCHITECTURE 17

Un module d'annotation se chargera de construire le message contenant les données capteurs ainsi que les méta-données mentionnées précédemment (id station, date, niveau de batterie).

Dans le cadre des capteurs environnementaux (centrale météo ou capteurs de gaz), le message est transmis par un module de communication en utilisant LoRaWAN à une passerelle. Le protocole LoRaWAN a été choisi pour sa faible consommation énergétique et sa longue portée, tout deux étant nécessaires pour des systèmes déployés en forêt sur batteries. La passerelle se chargera de retransmettre le message au serveur fog au travers d'MQTT.

Pour les caméras, la transmission se fait en deux parties, le module de communication envoie les données batteries sur le topic MQTT dédiée et les flux caméras sont eux envoyés par RTP (Real-time Transport Protocol). Ce mécanisme en deux composantes était nécessaire car un flux image est trop lourd pour MQTT. RTP est un protocole particulièrement adapté pour ce genre de tâche, puisqu'il permet le streaming quasi-temps réel de flux de données importants. Nous avons tout de même conservé une communication MQTT pour les batteries pour unifier le traitement de celles-ci.

MQTT est utilisé en interface avec les dispositifs edge mais c'est en suite Redpanda, une alternative à Kafka, plus moderne et performante qui prend la relève pour le traitement. Redpanda Connect est utilisé pour faire le pont entre les deux plateformes.

Les données caméras sont archivées dans un data lake MinIO. Nous avons choisi MinIO car il constitue un équivalent open-source à S3 d'AWS et permet le stockage de masse de données de type objet. Ces données sont aussi traitées au fur et à mesure par deux services intégrant un modèle d'IA. Un service sera dédié à la reconnaissance de fumée sur le flux optique, l'autre se chargera de déterminer les zones anormalement chaudes pouvant indiquer la présence d'un incendie. Les résultats seront envoyés sur le topic dédiés aux données traitées (voir Chapitre 5.4).

Un service se charge de vérifier que les stations répondent et le niveau de batterie indiqué et émet des alertes en cas de problème.

Des données sont récupérées régulièrement depuis des acteurs externes par un service dédié qui stocke ces informations dans une base InfluxDB. Cette base InfluxDB est aussi utilisée pour sauvegarder les différentes données qui circulent de sorte à conserver un historique. Cet historique pourra être récupéré grâce à une API proposée par le fog. Elle permettra l'accès à l'historique vidéo, capteurs et d'analyse. L'API sera aussi utilisée pour la configuration à la fois du fog et des stations edge au travers d'un service dédié. Ce service stockera les données dans la base MinIO sous format JSON et effectuera un envoi minimal vers les stations si une mise à jour de leur configuration est demandée (le reste des informations de la station est obtenue par MinIO grâce à l'id de station).

Les données collectées et traitées sont utilisées par trois services qui correspondent à notre cœur métier:

- Le service de détection agrège les données pour identifier les anomalies et notifier d'un départ de feu

- Le service d'analyse de la propagation utilise les données topographiques (altimétrie, végétation, direction du vent) pour estimer la trajectoire probable du feu et les zones menacées à court terme
- Le service de prédiction combine les informations météorologiques (issues de services externes et des stations locales) et les données de terrains (altimétrie, végétation, présence de zone à plus forte activité humaine) afin de calculer un indice de risque d'incendie dynamique.

Un service de communication est chargé de réceptionner les alertes et les résultats d'analyse. Il est capable d'émettre des notifications push pour plus de réactivité. Il retransmet aussi ces infos à un cluster cloud Redpanda.

Celui-ci se charge d'agréger les informations générales de chaque forêt pour permettre une gestion plus aisée.

Des services se chargent de mettre en forme les données reçus en vue d'être affichées (génération de GeoJSON par exemple).

Les données sont stockées dans une base MinIO accessible depuis l'extérieur via une API sur laquelle vont se greffer nos interfaces de visualisation (site web et application mobile).

Les données plus détaillées (flux caméra ou données de station par exemple), peuvent être obtenues au travers de l'API du cloud qui communiquera avec celle du fog.

## 5.4. Topics

*Les messages échangés sont décrits plus en détail dans le rapport dédié aux données.*

- `/captors` : Topics liés aux stations terrains
  - `/captors/{type_station}` : Topics liés à un type précis de stations terrains (cameras, meteo, gaz)
  - `/captors/{type_station}/{id_station}` : Topics liées à une station précise
    - `/captors/{type_station}/{id_station}/raw` : Permet la remontée « crue » (non-traitée) des données capteurs de la station. Contient à minima les méta-données de la station telles que la date et le niveau de batterie.
    - `/captors/{type_station}/{id_station}/config` : Permet de configurer la station (id, date)
    - `/captors/{type_station}/{id_station}/data` : Les données traitées y transitent. Elles sont annotées avec l'id de station, la position de la station, la zone de rattachement, la date et l'heure de collecte et la confiance en la donnée.
- `/maps` : Topics liés aux sorties d'une analyse
  - `/maps/{type}` : Topics liés aux sorties d'une analyse spécifique
    - `fire` pour la détection d'incendie,
    - `evol` pour la prédiction de déplacement de l'incendie
    - et `risk` pour le risque de déclenchement d'incendie
  - `/maps/{type}/{area}` : Sortie d'une analyse spécifique d'une zone de forêt donnée
- `/alerts` : Topics liés aux différentes alertes

- `/alerts/{type}` : Alertes de type spécifique
  - `/alerts/{type}/{equipement}` : Alertes de type spécifique relative à un équipement
- `/config` : Configuration générale pour le traitement