IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

INSTITUT VEDECOM

# ARCHITECTURE DISTRIBUÉE ET SÉCURISÉE POUR LES MISES À JOUR OTA DES VÉHICULES CONNECTÉS


**Tuteur entreprise : M. Arslane Hamza-Cherif**
**Tutrice école : M. Jean-Marie Bonnin**

**Présenté par : Bechir YENGUI**

**Filière Cybersécurité (CYBER)**


**Année Universitaire 2024-2025**

12/09/2025

**Stage du 1er avril au 8 septembre 2025**

# SOMMAIRE


PRÉSENTATION DE L'ORGANISME D'ACCUEIL 01

ENVIRONNEMENT DE TRAVAIL 02

CONTEXTE ET ENJEUX DU PROJET 03

SOLUTION PROPOSÉE ET TECHNOLOGIES 04

MÉTHODOLOGIE ET ARCHITECTURE 05

RÉALISATIONS ET DÉVELOPPEMENTS 06

STRATÉGIE DE MITIGATION D'UNE ATTAQUE SIMULÉE 07

ÉVALUATION DES RÉSULTATS 08

ANALYSE CRITIQUE ET PERSPECTIVES 09

IMPACTS ET BILAN PERSONNEL 10

1

# PRÉSENTATION DE L'ORGANISME D'ACCUEIL

# VEDECOM CHIFFRES CLÉS

► Fondé en 2014, institut de recherche & formation pour la mobilité durable

► 80 collaborateurs (chercheurs, ingénieurs, doctorants)

► Plus de 650 publications scientifiques

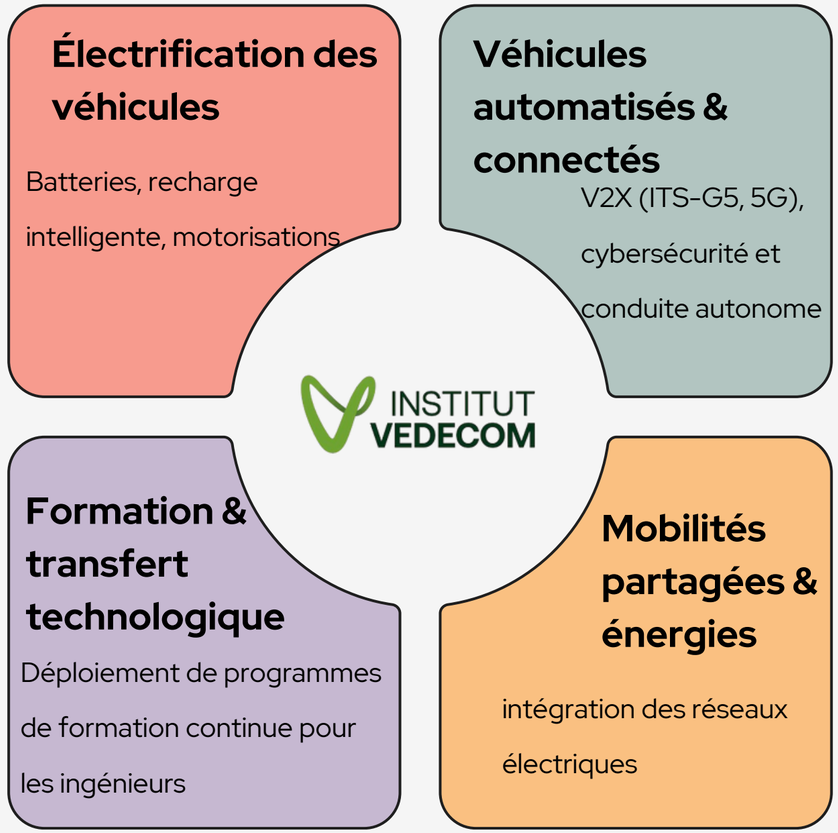
► 80 thèses encadrées

► Membre du réseau FIT (French Institutes of Technology)

► Partenariats avec 30+ acteurs industriels, académiques & institutionnels

# VEDECOM : Domaines d’expertise

- Implanté à Versailles – Satory, au cœur du pôle d’innovation Paris-Saclay
- Structure publique/privée réunissant industriels et académiques
- Mission : accélérer l’innovation dans le domaine des mobilités durables, autonomes et connectées



2

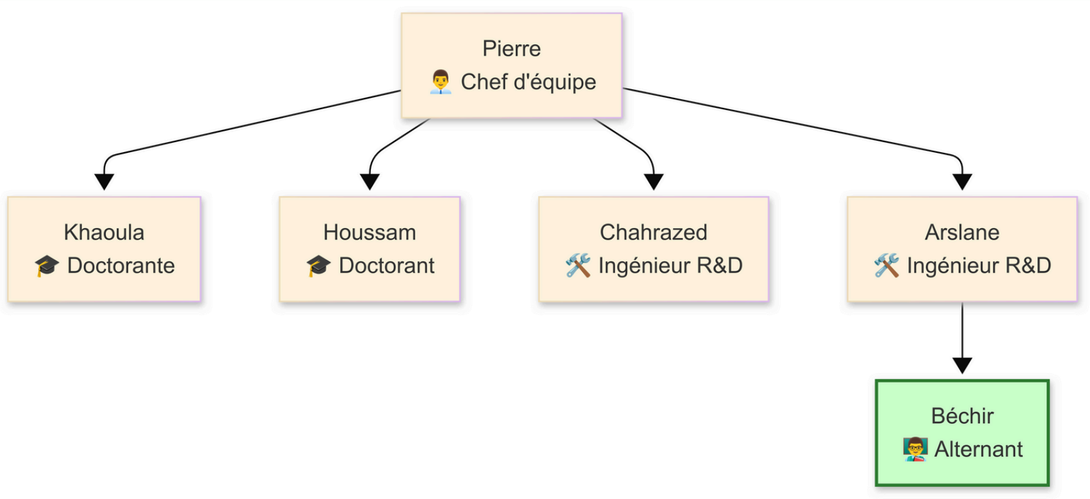
# ENVIRONNEMENT DE TRAVAIL

# ÉQUIPE ET MÉTHODOLOGIE

## MÉTHODOLOGIE ADOPTÉE :

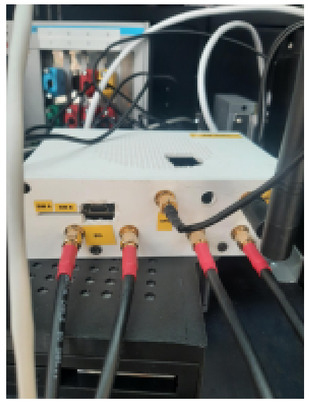
**Méthodologie de suivi et de développement :**

- Rituels hebdomadaires
  - Réunion d'équipe chaque mardi
  - Point individuel avec le tuteur entreprise chaque jeudi
  - Rapport hebdomadaire transmis chaque vendredi
- Pratiques collaboratives
  - Documentation vivante (mise à jour continue au fil du projet)
  - Revues de code systématiques via pull requests

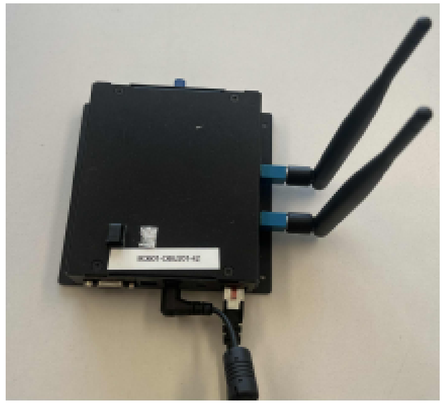


## MATÉRIEL UTILISÉ DANS L'ARCHITECTURE OTA DISTRIBUÉE

- SERVEUR CENTRAL (X86_64 LINUX)
- TCUS PIVOT/CLIENT (GATEWORKS VENICE GW7400)
- OBU (ON-BOARD UNIT ITS-G5)
- NŒUDS EDGE (PC LINUX)



(a) TCU



(b) OBU

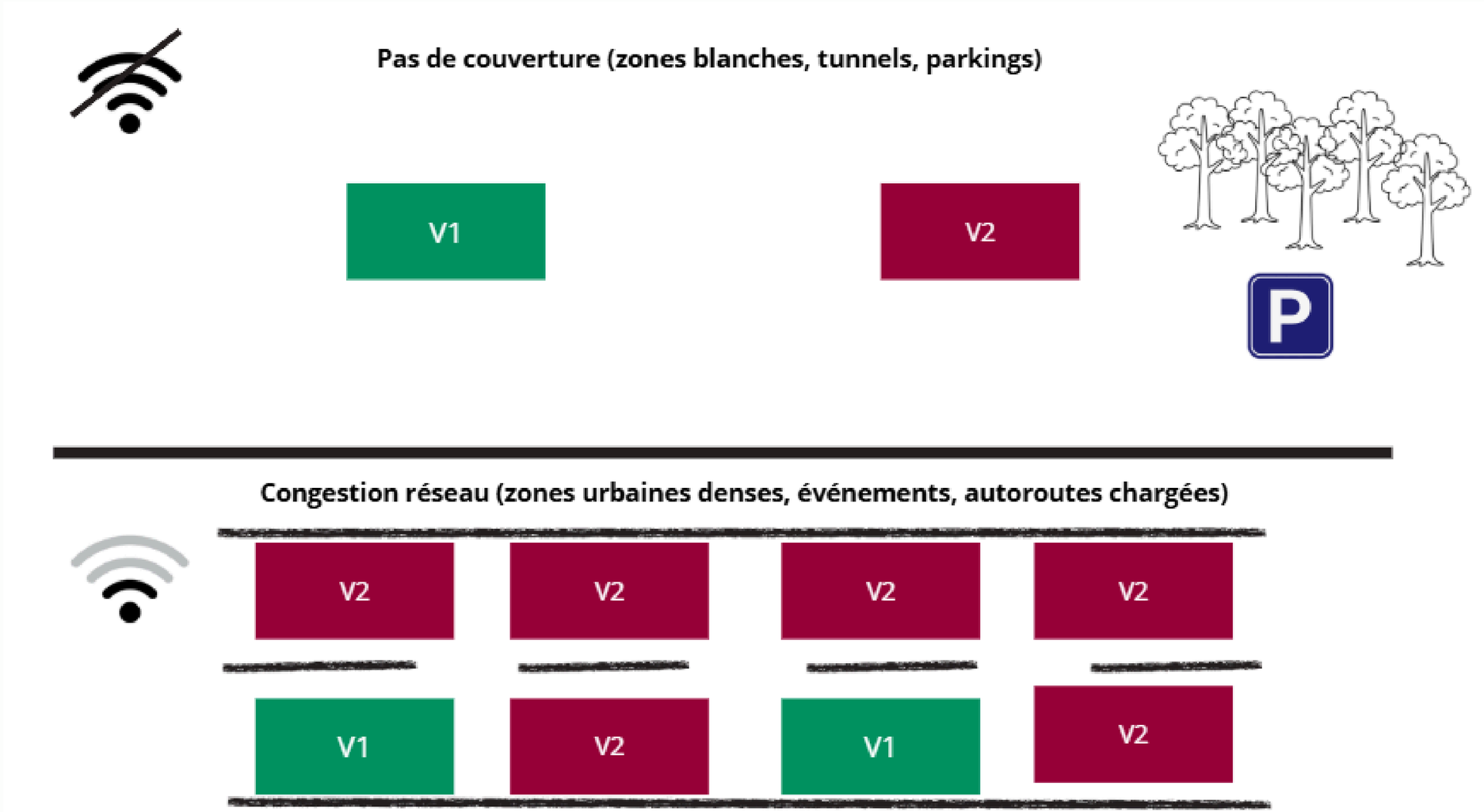
## ENVIRONNEMENT

- **Lieu :** Laboratoire de VEDECOM
- **Domaine :** Mobilités automatisées & connectées
- **Encadrants :** M. A. Hamza-Cherif et M. J-M. Bonnin
- **Projet :** HY5 – Hybrid 5G Vehicular Connectivity
- **Méthodologie :** prototypage industriel + recherche + Développement

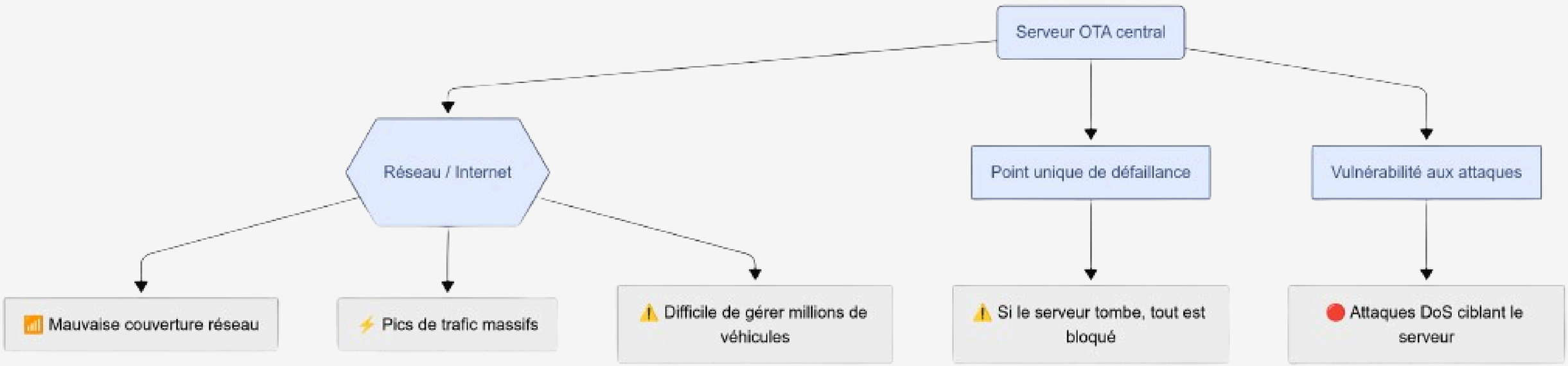
3

# CONTEXTE ET ENJEUX DU PROJET

# Scénarios de mise à jour



## LES LIMITES DES ARCHITECTURES OTA CENTRALISÉES



4

# SOLUTION PROPOSÉE ET TECHNOLOGIES

Transformation du secteur automobile (SDV) :

permet d'intégrer facilement de nouvelles fonctions sans dépendre d'un serveur central unique

**Sécurité** :

protection contre les attaques DoS/MITM grâce à la distribution décentralisée

**OTA DISTRIBUÉE**

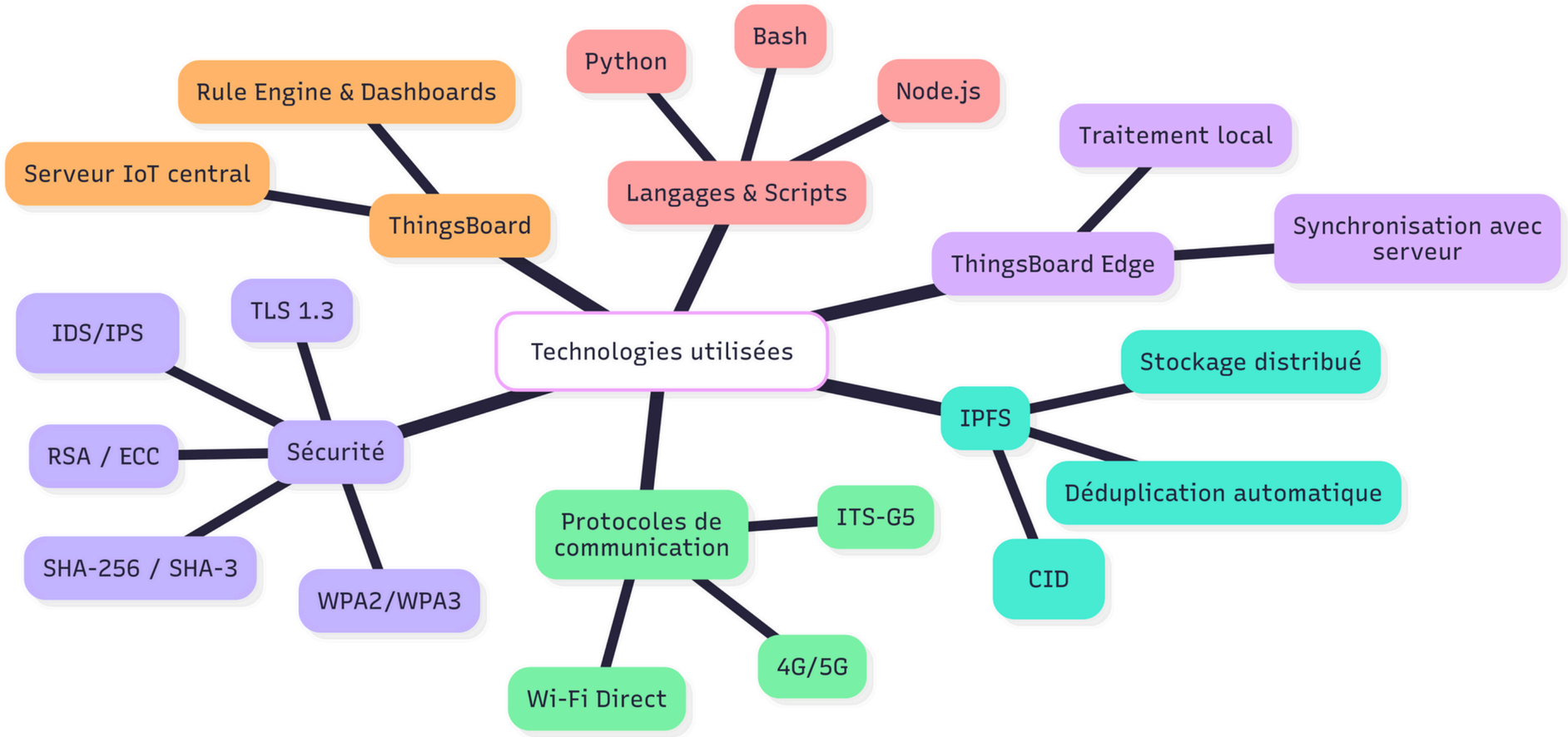
**Fiabilité** :

pas de dépendance à un serveur central, meilleure résilience dans les zones à faible couverture réseau (V2V / V2X)

**Réduction des coûts** :

optimisation de la bande passante et partage de charge entre véhicules/edges → moins d'infrastructures centrales nécessaires.

## LES TECHNOLOGIES



# CAHIER DES CHARGES

## OBJECTIFS TECHNIQUES :

► Architecture distribuée & sécurisée pour OTA

► Garantir : disponibilité, intégrité (CID, signatures), résilience

► Optimiser : bande passante (IPFS/V2V)

## CONTRAINTES DE L'ARCHITECTURE :

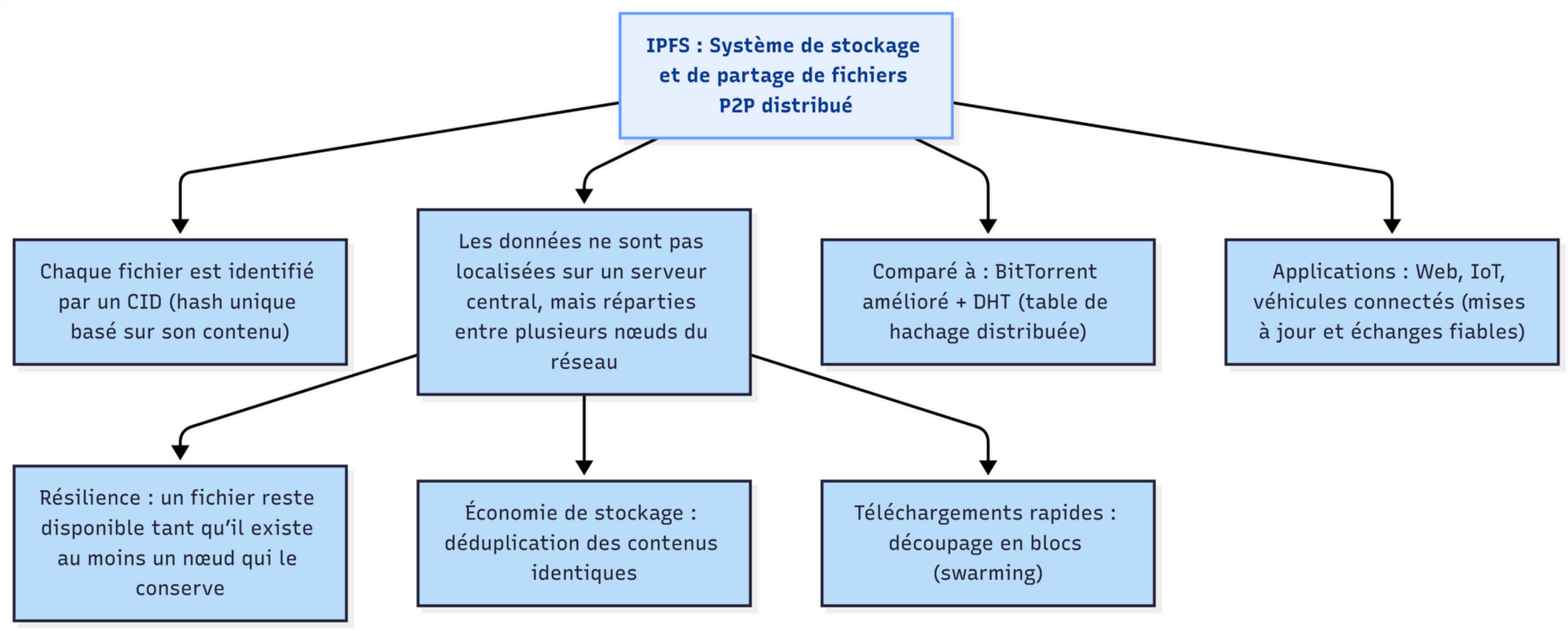
► Support de plusieurs technologies : ITS-G5, Wi-Fi direct, 4G/5G

► Gestion des zones blanches

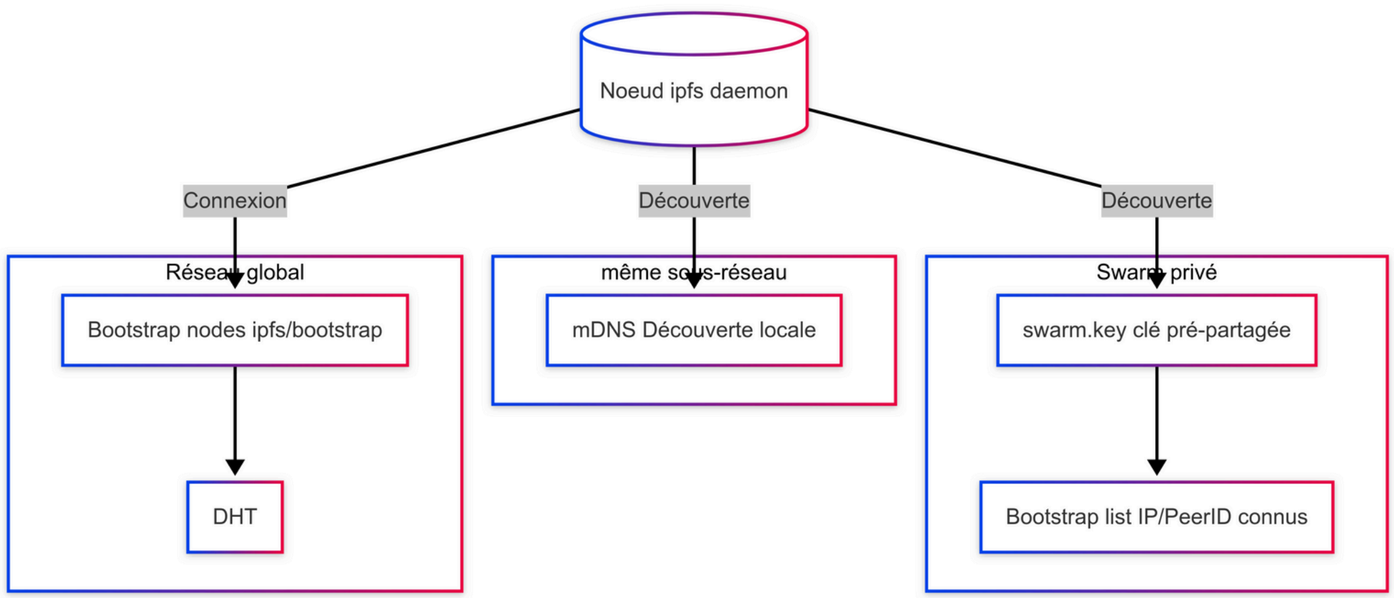
► Contraintes matérielles : CPU, RAM, stockage limités sur TCU

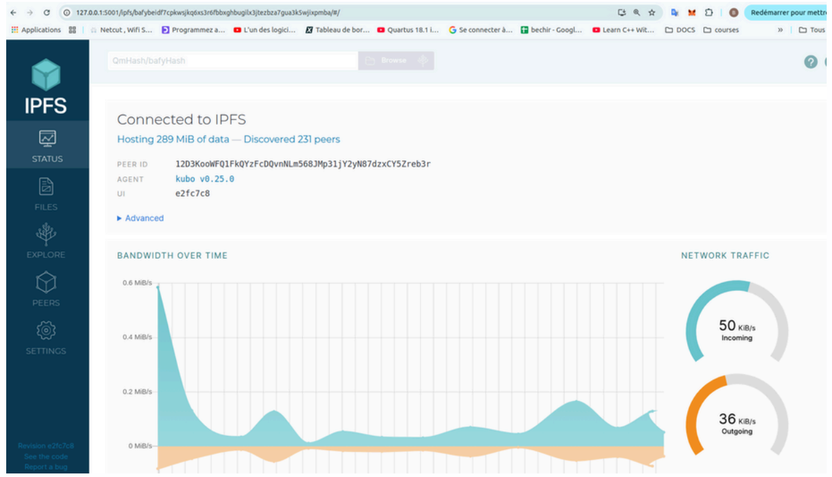
► Éviter les points uniques de défaillance (architecture hiérarchique : Serveur → Edge → Véhicule pivot → V2V)

# IPFS : SYSTÈME DE STOCKAGE PAIR-À-PAIR DISTRIBUÉ



# IPFS : LA RÉCUPERATION DES FICHIERS



# THINGSBOARD

**DÉFINITION GÉNÉRALE :**
PLATEFORME IOT OPEN SOURCE POUR LA GESTION D'ÉQUIPEMENTS CONNECTÉS.
FOURNIT DES SERVICES DE COLLECTE DE DONNÉES, SUPERVISION ET AUTOMATISATION

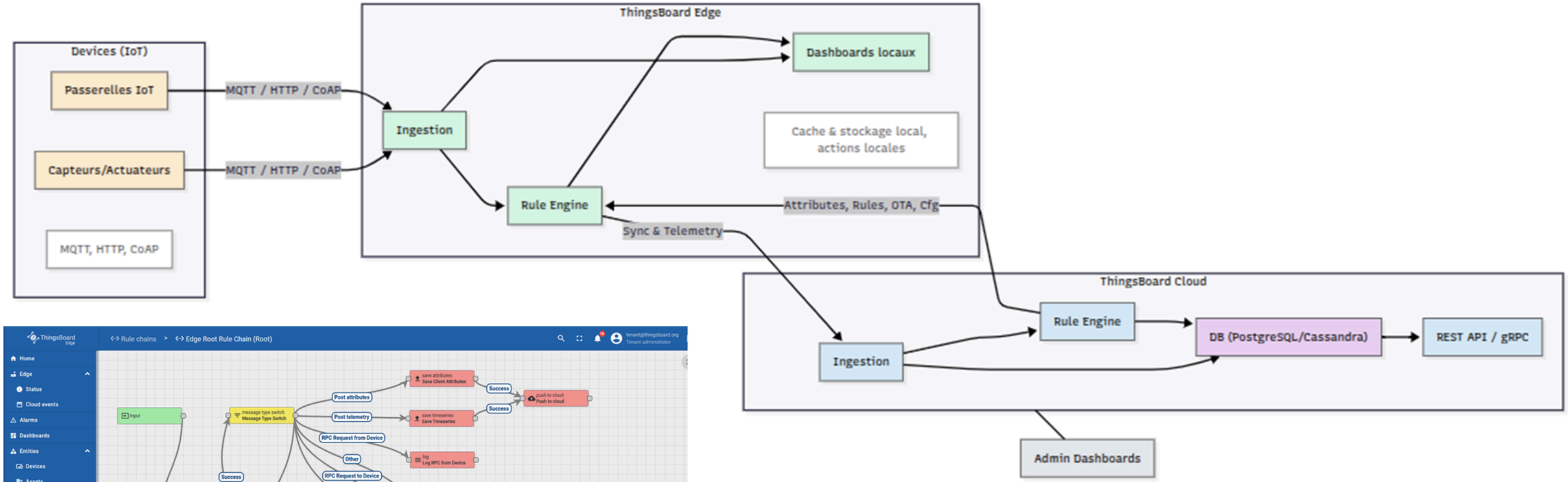
**Supervision : tableaux de bord dynamiques pour visualiser télémétrie, logs,alertes**

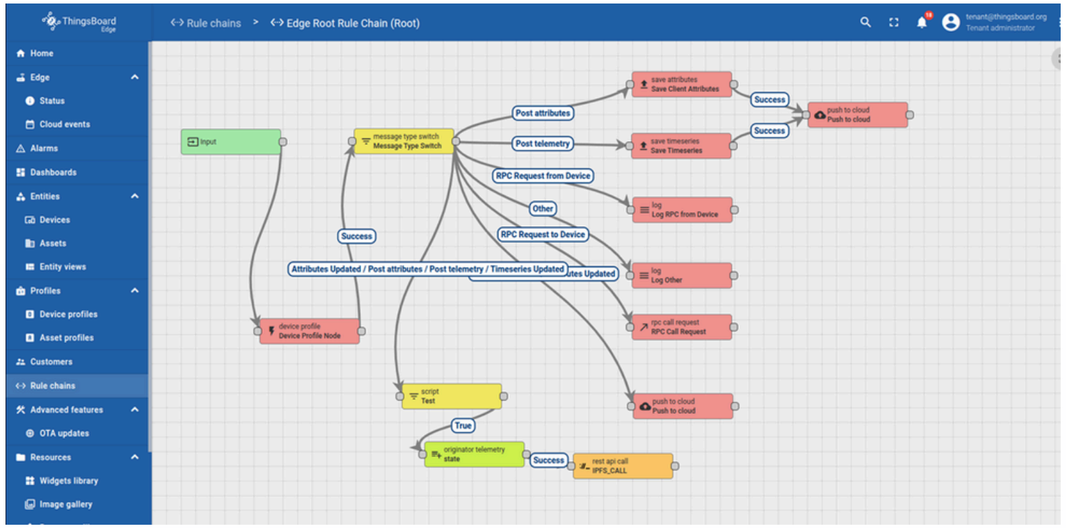
**Moteur de règles (Rule Engine): permet de créer des workflows**

**Protocoles supportés : MQTT, CoAP, HTTP → communication standardisée avec les objets connectés**

**•THINGSBOARD CLOUD → ADMINISTRATION CENTRALISÉE**
**•THINGSBOARD EDGE → FONCTIONNE LOCALEMENT PUIS SYNCHRONISE**

# THINGSBOARD

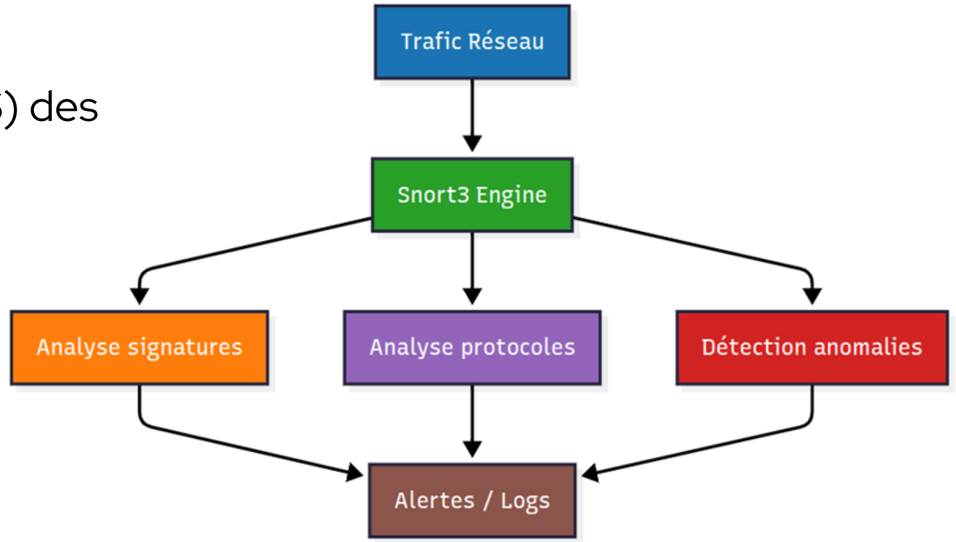


# SNORT

**Rôle :**

- Surveille le trafic réseau en temps réel pourdétecter (IDS) et bloquer (IPS) des attaques.




**Modes :**

- IDS (passif) : génère des alertes.
- IPS (inline) : bloque via nftables/iptables →NFQUEUE.

**Pipeline :**

- Décodage des paquets → préprocesseurs (flux/normalisation) → moteur de règles (signatures/patterns) → actions (alert/log/drop)

# STACK TECHNOLOGIQUE : JUSTIFICATIONS

**ThingsBoard (Serveur IoT central)**

✔ Open-source, extensible, compatible protocoles IoT (MQTT/HTTP/CoAP)

✔ Rule Engine puissant + dashboards pour supervision en temps réel

✘ Alternatives (AWS IoT, Azure IoT Hub) : dépendance cloud, coûts élevés, manque de souveraineté

**ThingsBoard Edge (traitement local)**

✔ Fonctionne même en cas de perte de connectivité → synchronisation différée

✔ Réduction de la latence, décisions locales autonomes

✘ Alternatives (edge propriétaire) : verrouillage fournisseur, intégration limitée avec IPFS

**ITS-G5 & Wi-Fi direct (communications V2V)**

✔ ITS-G5 : faible latence, , standard européen

✔ Wi-Fi direct : haut débit point-à-point pour le transfert de données OTA

✘ Alternative 5G seule : forte dépendance opérateur, zones blanches, coût plus élevé

**Stack sécuritaire (RSA/ECC, SHA-256, TLS 1.3, Snort3 IDS)**

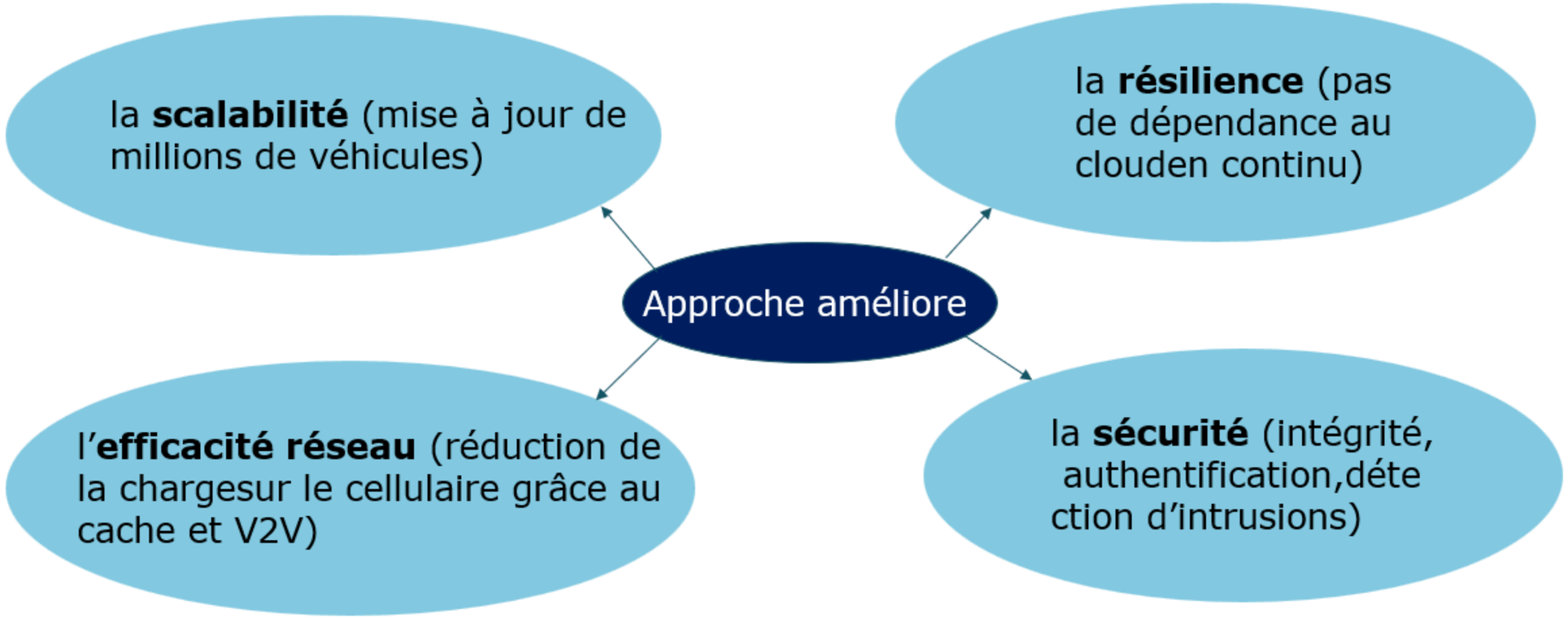
✔ IDS (Snort3) pour détection proactive des attaques (DoS, injection)

✘ Alternatives (protocole custom) : non standard, non certifiable, faible interopérabilité

5

# MÉTHODOLOGIE ET ARCHITECTURE

## APPROCHE

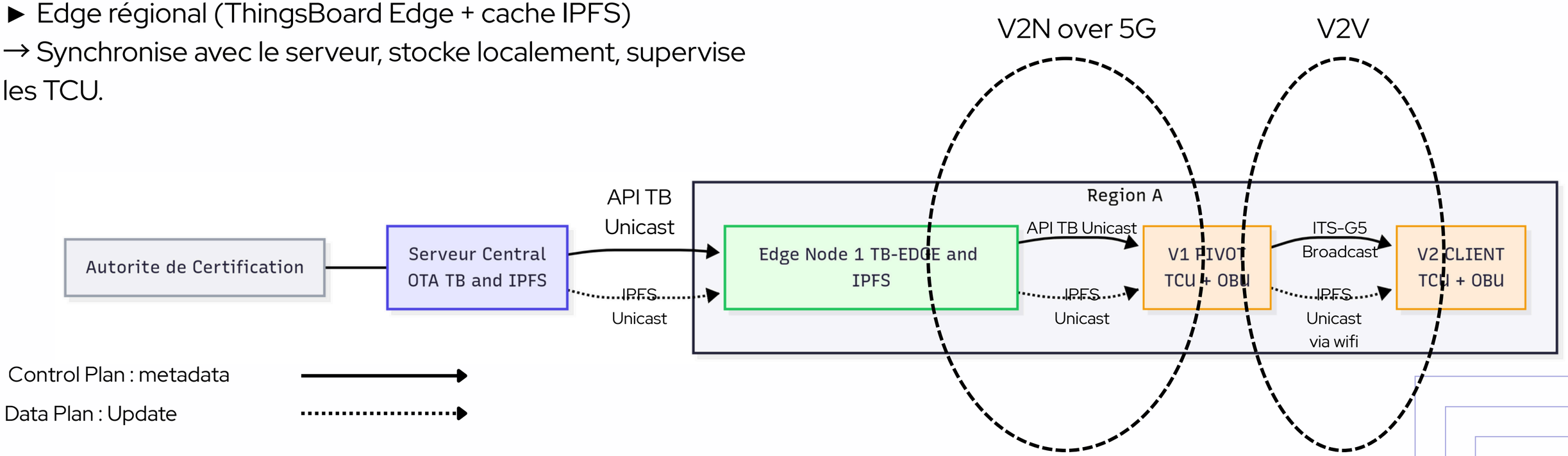

la **scalabilité** (mise à jour de millions de véhicules)
la **résilience** (pas de dépendance au clouden continu)
Approche améliore
l'**efficacité réseau** (réduction de la chargesur le cellulaire grâce au cache et V2V)
la **sécurité** (intégrité, authentification,détection d'intrusions)

## ARCHITECTURE (VUE PAR COUCHES)

► Serveur central (Cloud ThingsBoard + IPFS bootstrap)
→ Préparation, signature et publication des mises à jour.

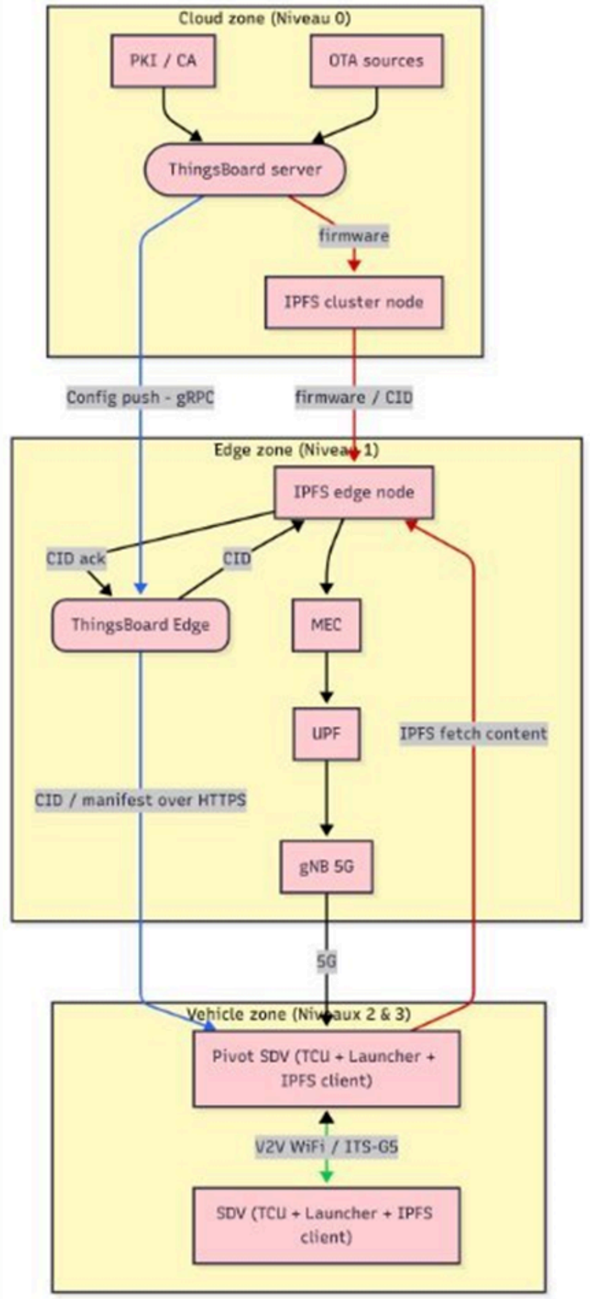
► Edge régional (ThingsBoard Edge + cache IPFS)
→ Synchronise avec le serveur, stocke localement, supervise les TCU.

► Véhicules (TCU pivot + clients) Pivot : reçoit la mise à jour (cellulaire/Edge), diffuse en V2V (ITS-G5, Wi-Fi direct).

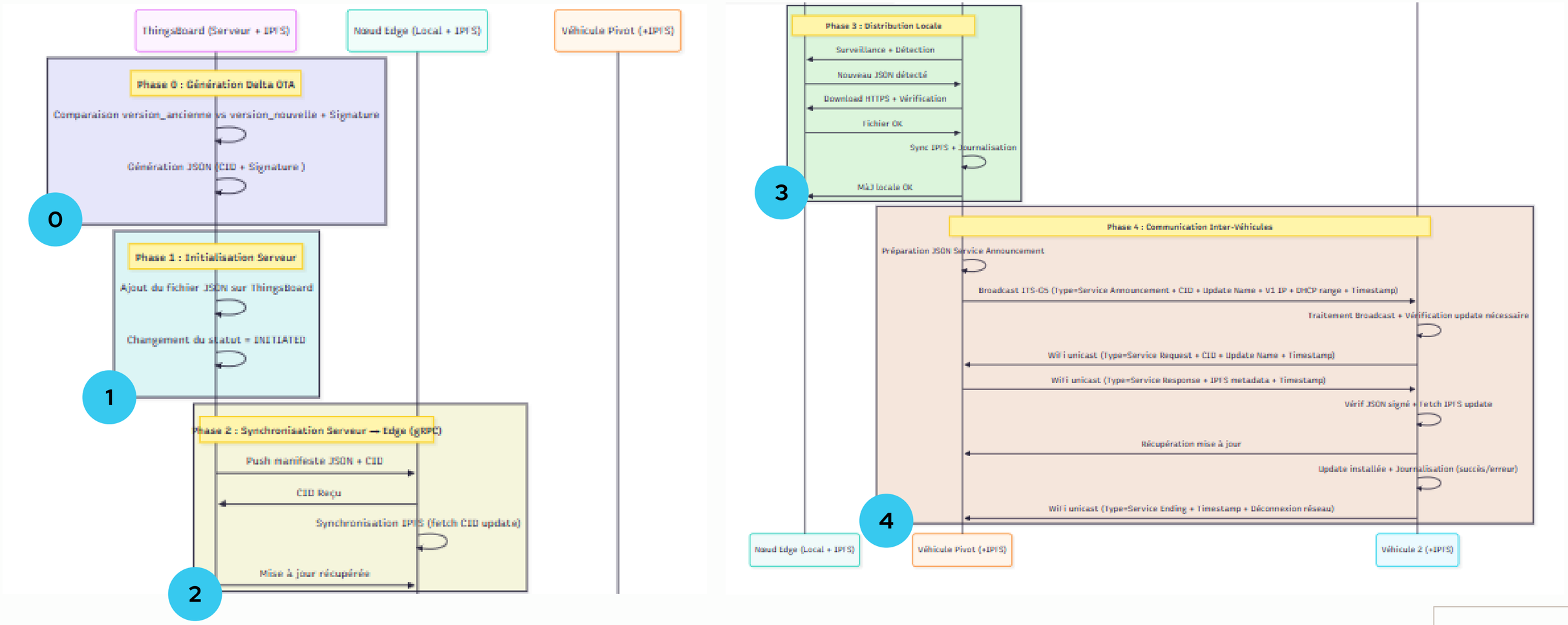


## DÉROULEMENT DE LA MISE À JOUR

- Génération & signature du delta OTA (JSON signé, CID IPFS). Publication sur IPFS → CID unique.
- Synchronisation : Edge télécharge via IPFS, valide l'intégrité.
- Distribution locale : Véhicules téléchargent depuis Edge (HTTPS) ou depuis pivot (Wi-Fi direct).
- Propagation V2V : pivot diffuse via ITS-G5 (annonce + hotspot Wi-Fi).
- Vérification & installation : chaque véhicule contrôle la signature, applique et journalise.



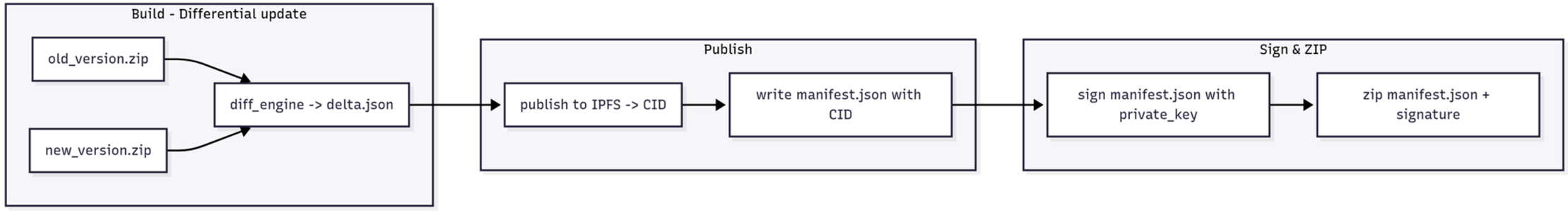
## DIAGRAMME UML DE L'ARCHITECTURE



6

# RÉALISATIONS ET DÉVELOPPEMENTS

## PH0: GÉNÉRATION DE MISE À JOUR DIFFÉRENTIELLE

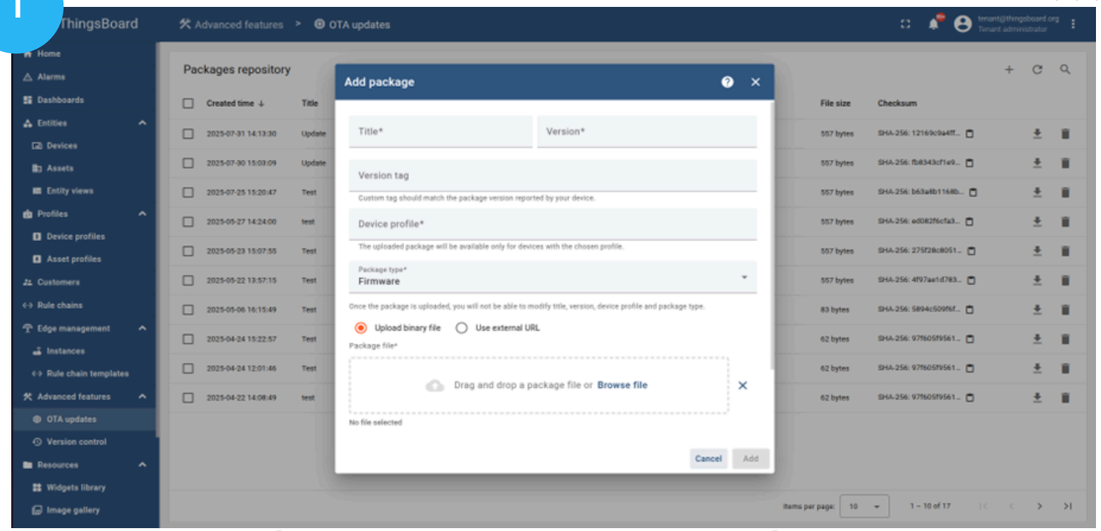



### Processus de génération et distribution du delta OTA :

- Un fichier delta.json est généré en comparant deux versions (ancienne vs nouvelle), listant les fichiers ajoutés, modifiés ou supprimés.
- Ce delta est ensuite signé numériquement (RSA/SHA-256) puis empaqueté dans une archive ZIP.
- L'archive signée est publiée sur TB, qui fournit un CID unique servant de référence aux nœuds Edge et aux véhicules pour récupérer l'artefact correct et vérifié.

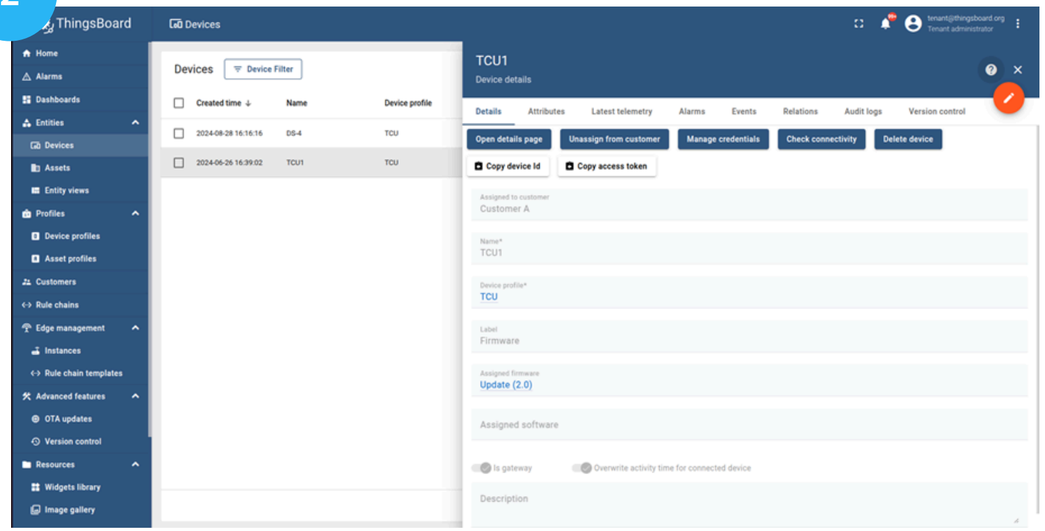
## PH1: INITIALISATION SERVEUR

1



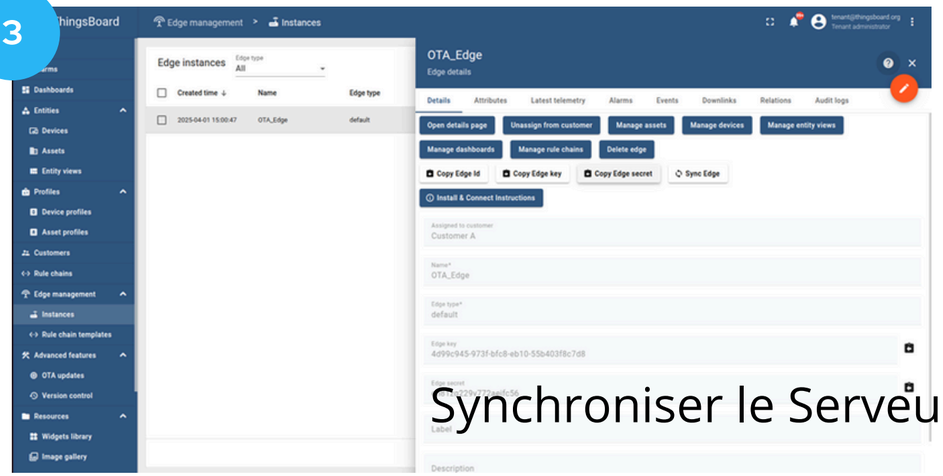

Crée le package de mise à jour

2



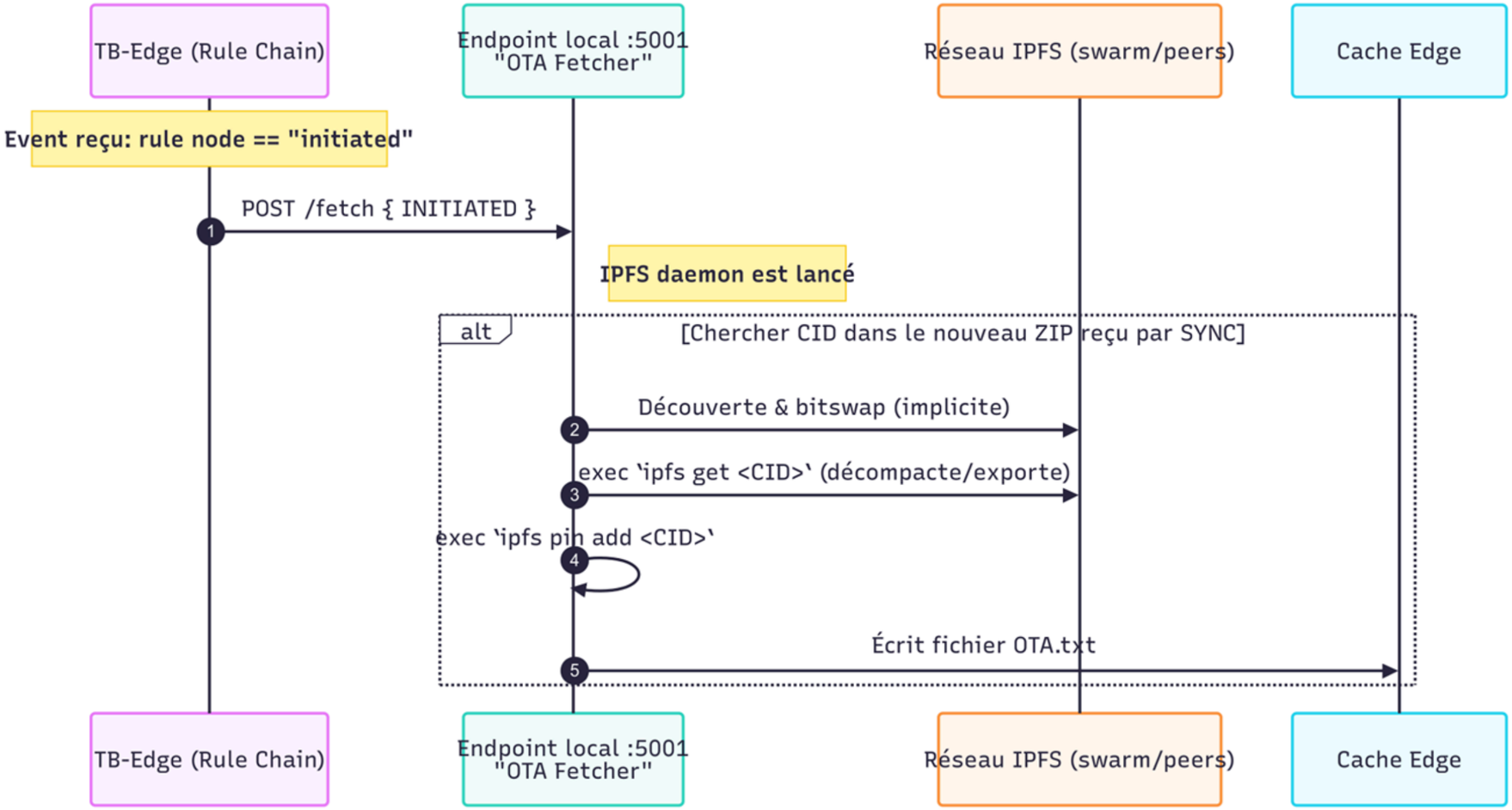

Affécter le MAJ à un TCU choisit

3

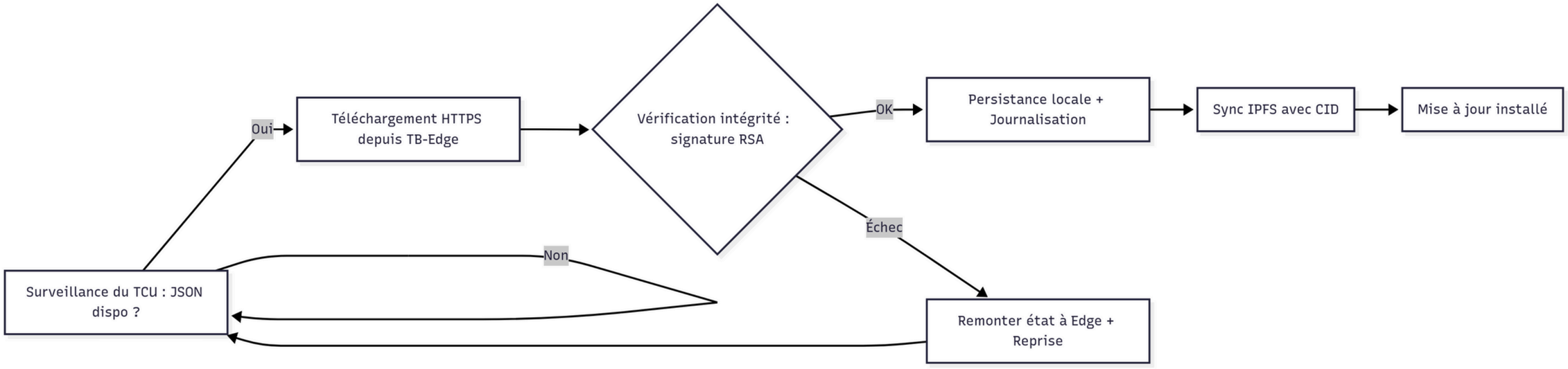


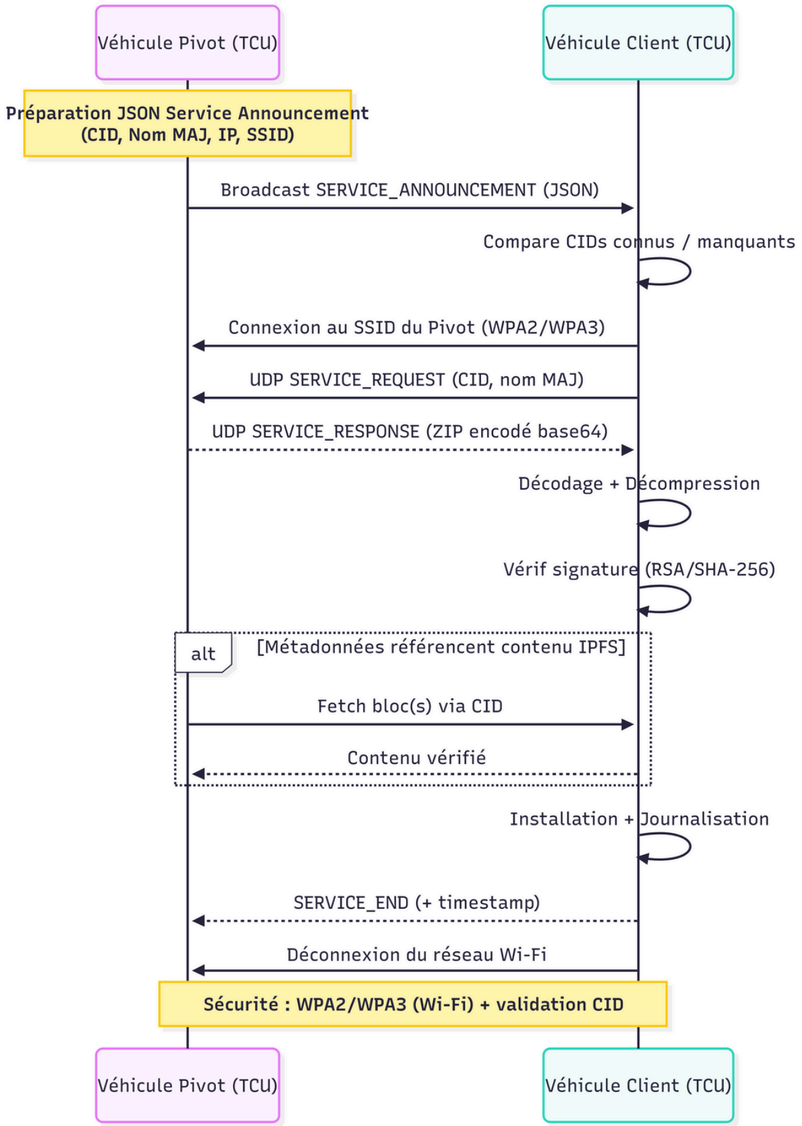

Synchroniser le Serveur avec le Edge

## PH2: SYNCHRONISATION SERVEUR / EDGE



## PH3: DISTRIBUTION LOCALE





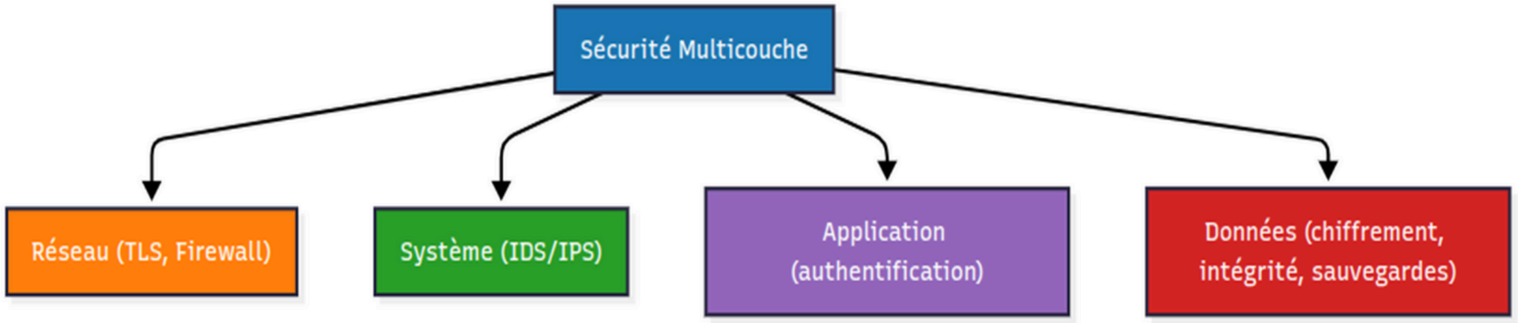

## PH4: COMMUNICATION INTER-VÉHICULE

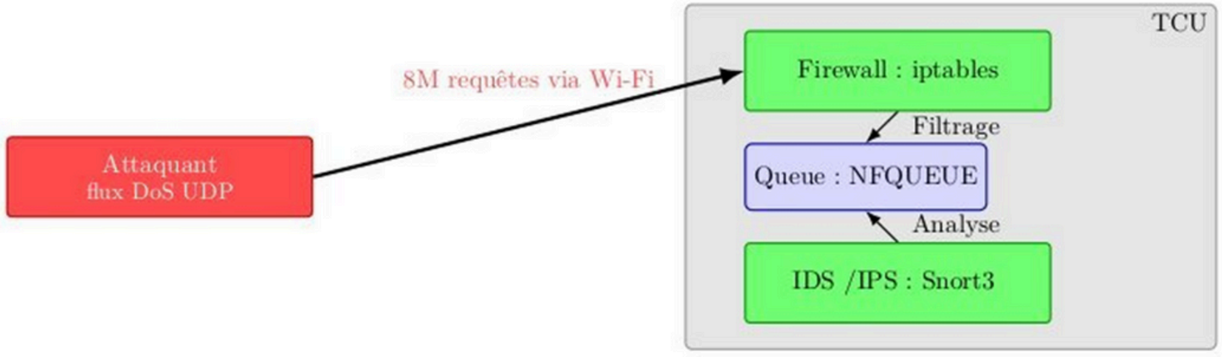
Header ITS-G5 :

| Mac source (6B) | Mac Destination (6B) | Ethertype : 0x8947 (2B) |
|---|---|---|

7

# STRATÉGIE DE MITIGATION D'UNEATTAQUESIMULÉE




**Contexte :**

- Attaque simulée : DoS (flood UDP) visant le TCU pivot.
- Objectif : saturer les ressources (CPU, mémoire, bande passante)

**Contre-mesure mise en place :**

- Déploiement de Snort 3 (IDS/IPS) sur le TCU.
- Détection en temps réel des paquets malveillants (flood UDP).
- Règles personnalisées pour classifier et bloquer le trafic.
- Intégration avec nftables/NFQUEUE pour mitigation active.

8

# ÉVALUATION DES RÉSULTATS

**Data Plan = contenu : téléchargement de l'artefact via IPFS**

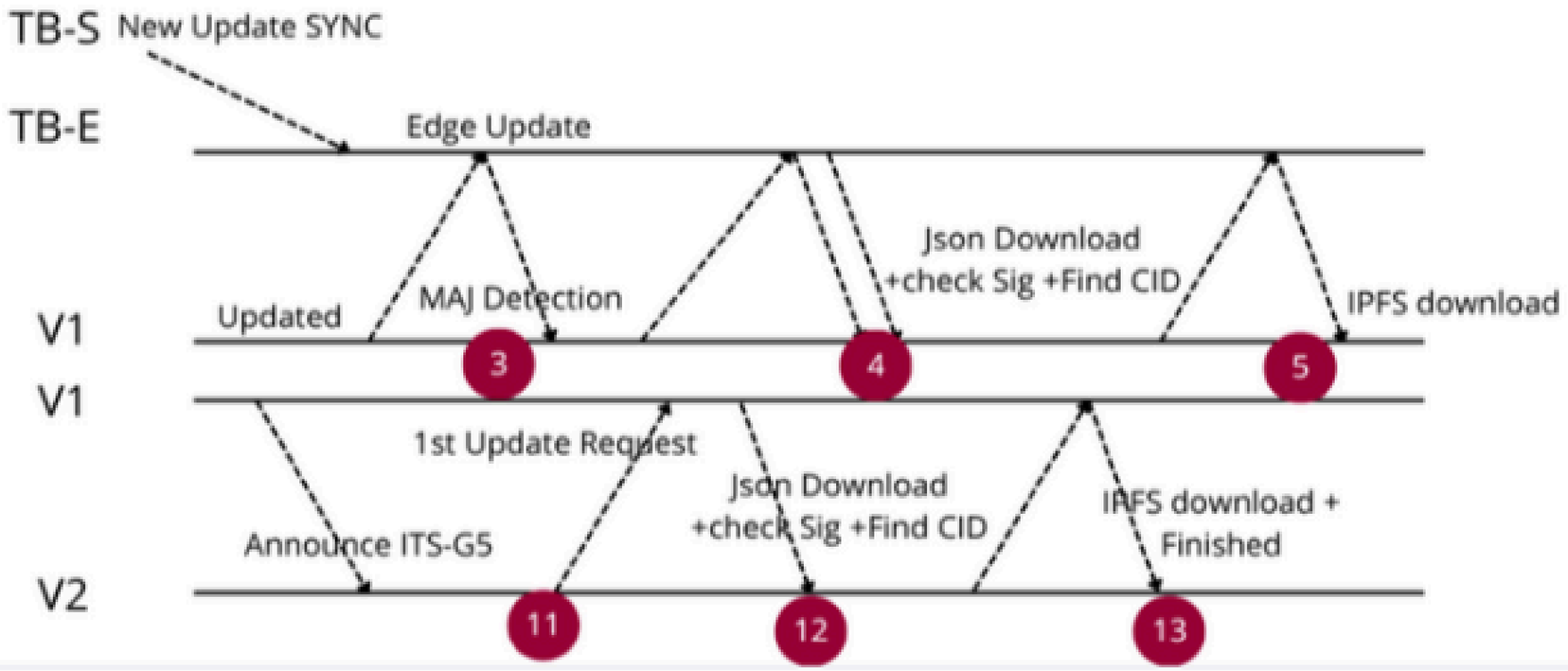
**Control Plan = tout ce qui est métadonnées**

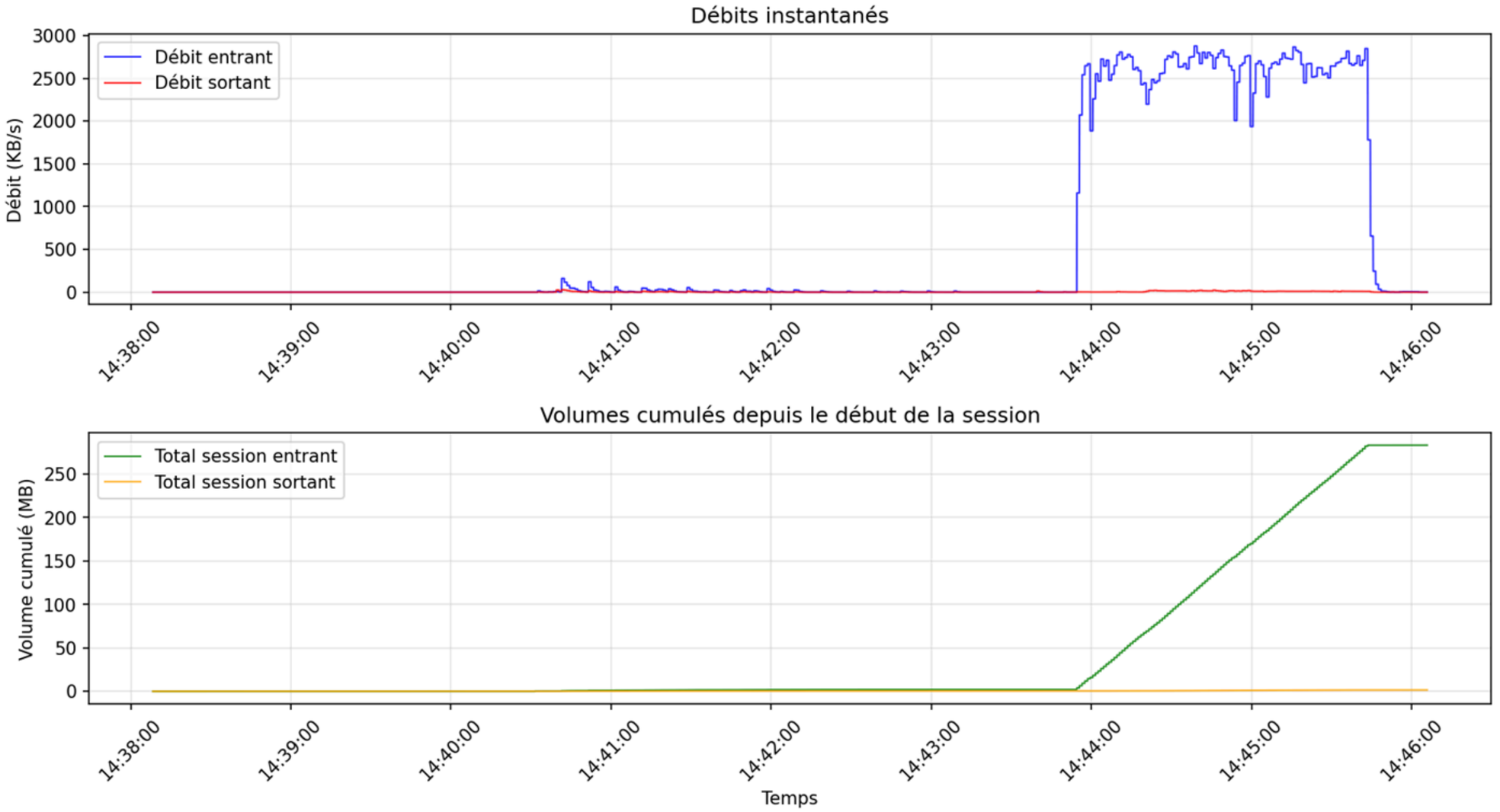
# Métriques

**Update Duration**

| | Control Plan | Data Plan | Total | Size | |
|---|---|---|---|---|---|
| V1 Pivot | 4 - 3 | 5 - 4 | 5 - 3 | Json.zip files + IPFS file → | CSV1 |
| V2 Client | 11 - 12 | 13 - 12 | 13 - 11 | Json.zip files + IPFS file → | CSV2 |

**Bandwidth** Courbe Pendant la MAJ via IPFS → Courbe + CSV3 in V1 and V2




Débits instantanés
Débit entrant
Débit sortant
Débit (KB/s)
3000
2500
2000
1500
1000
500
0
14:38:00
14:39:00
14:40:00
14:41:00
14:42:00
14:43:00
14:44:00
14:45:00
14:46:00
Volumes cumulés depuis le début de la session
Total session entrant
Total session sortant
Volume cumulé (MB)
250
200
150
100
50
0
Temps

9

# ANALYSE CRITIQUE ET PERSPECTIVES

# ANALYSE CRITIQUE

**POINTS D'AMÉLIORATION IDENTIFIÉS :**

► Gestion manuelle du cycle PKI (certificats).

► Centralisation et corrélation des logs encore limitées.

**SOLUTIONS MISES EN ŒUVRE ET RECOMMANDATIONS :**

► Ajouter rollback automatique.

► Tester 5G-V2X pour portée/scalabilité.

► Intégrer un SIEM (Wazuh/ELK) pour corrélation globale (collécte des données via Thingsboard Edge )

► Industrialisation : conteneurisation Docker, pipelines CI/CD, supervision centralisée par métriques.

►Intégration possible de Blockchain pour :

- Garantir immutabilité et horodatage des mises à jour/journaux
- Assurer traçabilité distribuée sans tiers de confiance.

CONCLUSION

10

# IMPACTS ET BILAN PERSONNEL

# Conclusion

## BILAN PERSONNEL ET DÉVELOPPEMENT COMPÉTENCES :

- ▶ Montée en compétences en réseaux , embarquée , sécurité et R&D.
- ▶ Autonomie, rigueur et gestion d'un projet complexe.
- ▶ Collaboration avec équipes académiques et industrielles
- ▶ Leadership technique et conduite projet.
- ▶ Analyse critique et résolution problèmes complexes.
- ▶ Déploiement expérimental multi-TCU (ITS-G5, Wi-Fi direct) et développement logiciel
- ▶ Maîtrise d'architectures distribuées (IPFS, Edge, OTA)

## APPORTS INSTITUTIONNELS :

- ▶ La contribution à une publication scientifique
- ▶ Valorisation du projet HY5 & Software-Defined Vehicle

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

INSTITUT VEDECOM

# MERCI POUR VOTRE ATTENTION


**Bechir Yengui**

**Filière Cybersécurité (Cyber)**

**IMT Atlantique • Vedecom**


**Année Universitaire 2024-2025**

**Stage du 1er avril au 8 septembre 2025**

0

# BACKUP SLIDE

## 💶 Dimension économique

Moins de rappels & coûts opérationnels [Allied Market Research, 2024](https://www.alliedmarketresearch.com/software-defined-vehicle-market-A12956)

Optimisation bande passante IPFS/V2V [Benet, 2014](https://ipfs.io/ipfs/QmR7GSQM93Cx5eAg6a6yRzNde1FQv7uL6A4Q1dX2n4mQJd)

Cycles OTA plus courts : cas Tesla [Case Study](https://www.tesla.com/updates)

## 🌱 Dimension environnementale

Réduction $CO_2$ : -1500 t/an (100k véhicules) [EPA](https://www.epa.gov/greenvehicles/greenhouse-gas-emissions-typical-passenger-vehicle)

Optimisation réseaux : -40 à -60% data centers [IEA](https://www.iea.org/reports/data-centres-and-data-transmission-networks)

Déduplication IPFS : moins de transferts redondants [Benet, 2014](https://ipfs.io/ipfs/QmR7GSQM93Cx5eAg6a6yRzNde1FQv7uL6A4Q1dX2n4mQJd)

Économie circulaire : allongement durée de vie véhicules [EU Report](https://ec.europa.eu/environment/circular-economy/)

## 🌍 Dimension sociétale

Équité d'accès : sécurité pour tous [UNR155](https://unece.org/transport/vehicle-regulations/un-regulation-no155-cybersecurity) & [UNR156](https://unece.org/transport/vehicle-regulations/un-regulation-no156-software-updates)

Sécurité accrue : corrections rapides vulnérabilités [ISO/SAE 21434](https://www.iso.org/standard/70918.html)

Acceptabilité sociale : confiance véhicules connectés [McKinsey, 2021](https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/over-the-air-updates)