Barème de Notation

Projet Edge Computing – M5Stack Tab5

UVSQ SNPI – Apprenti(e)s – Dernière année d'études

Total: 100 points (base) + jusqu'à 12 points bonus optionnels (GitHub)

Architectures Edge Computing Supportées

Sélectionnez l'architecture de votre projet:

Architecture 1: Smartphone WiFi Router + Tab5 Edge Node

☐ Mon projet utilise cette architecture

Composants Principaux:

• Smartphone: Agit en tant que routeur WiFi et capteur/client

• Tab5: Nœud edge - effectue le traitement et l'inférence

• Laptop (optionnel): Client pour afficher les résultats ou envoyer des commandes

Composants Optionnels:

☐ Capteur Filaire (GPIO, I2C, SPI): DHT22, BMP280, IMU, etc. connectés directement au Tab5

☐ Capteur Sans-fil: Température/Humidité WiFi, capteurs Bluetooth LE connectés au Tab5

☐ Module WiFi C6: Communication WiFi avancée (6 GHz, WiFi 6) au lieu du WiFi natif

☐ Module LoRa: Alternative radio longue portée pour communication edge (868/915 MHz)

Architecture 2: Tab5 + RaspberryPI API Server

☐ Mon projet utilise cette architecture

Composants Principaux:

• Tab5: Client/capteur - collecte données et fait requêtes

• RaspberryPI: API Server edge - accueille les modèles/services et traite les requêtes

• Laptop: Client pour visualiser/commander via interface web ou réseau

Composants Optionnels:

☐ Capteur Filaire (Tab5): Capteurs connectés au Tab5 via GPIO, I2C ou SPI

☐ Capteur Sans-fil: Capteurs WiFi ou BLE qui envoient données au RaspberryPI directement

☐ Module WiFi C6 sur Tab5: Pour communication Tab5→RaspberryPI en WiFi 6

☐ Module LoRa: Communiquer avec le RaspberryPI via radio LoRa longue portée

Architecture 3: Tab5 Standalone Edge Computing

☒ Mon projet utilise cette architecture

Composants Principaux:

• Tab5: Capteur, traitement ET client d'affichage - système complet

• Smartphone (optionnel): WiFi hotspot ou affichage des résultats

• Laptop (optionnel): Pour debug/monitorage via WiFi

Composants Optionnels:

☒ Capteur Filaire: Connecté directement au Tab5 (GPIO, I2C, SPI) pour acquisition données

☐ Capteur Sans-fil: BLE ou WiFi connecté au Tab5 pour captage sans câblage

☒ Module WiFi C6: Remplace WiFi natif pour WiFi 6 ou meilleure portée

☐ Module LoRa: Ajoute capacité radio LoRa pour communication longue portée

Architecture 4: Tab5 Edge + Cloud Gateway

☐ Mon projet utilise cette architecture

Composants Principaux:

• Tab5: Edge computing local (traitement, capteurs, affichage)

• Cloud Gateway: Backend cloud (AWS/Azure/Google Cloud/custom) avec API REST/gRPC

• Cloud Services: Stockage données (database), APIs 3ème partie, ML models hébergés

• Laptop/Web: Interface web pour visualisation historique et données cloud

Flux de Données:

Tab5 (processing) → WiFi → Cloud Gateway (API) → Cloud Storage/ML/APIs

Cloud → Tab5 (modèles mis à jour, configuration, résultats ML)

Composants Optionnels:

☐ Sync Périodique: Push des résultats vers cloud toutes les N minutes/heures

☐ Real-time Push: WebSocket/MQTT vers cloud pour sync temps-réel

☐ 3rd Party APIs: Intégration APIs externes (weather, forecast, business logic)

☐ ML Models Hébergés: Modèles ML lourds exécutés côté cloud, résultats renvoyés au Tab5

☐ Cold Storage: Archivage données historiques long-terme en cloud

☐ Conditional Sync: Upload des données importantes seulement (filtrage côté Tab5)

Fonctionnalités de Cybersécurité Implémentées

Sélectionnez les mesures de sécurité implémentées:

Authentification & Contrôle d'Accès:

☒ Filtrage MAC Address: Whitelist/Blacklist des appareils autorisés

☐ Authentification par Mot de Passe: Credentials pour accès client

☐ Authentification par Token/API Key: JWT, Bearer tokens, API keys uniques

☐ Authentification Certificat: Certificats X.509, mTLS (mutual TLS)

☐ RADIUS Server: Authentification centralisée réseau (RADIUS protocol RFC 2865, parfait pour multi-appareils)

Chiffrement du Transport:

☒ HTTPS/TLS: Chiffrement HTTP avec certificat SSL/TLS

☐ MQTTS: MQTT sécurisé avec TLS 1.2/1.3

☐ CoAPS: CoAP sécurisé avec DTLS (Datagram TLS)

☐ VPN/Tunnel: Communication via VPN ou tunnel chiffré

Intégrité des Données:

☐ Hashing (SHA256/SHA512): Vérification d'intégrité des données

☐ CRC16/CRC32: Vérification cyclique redondance pour fichiers SD card (détecte corruption)

☐ HMAC: Authentification des messages avec clés partagées

☐ Signatures Numériques: Signature asymétrique des messages

Contrôle et Filtrage:

☒ Firewall: Filtrage des ports/protocoles (iptables, netfilter)

☐ Rate Limiting: Limitation du débit pour prévenir DDoS

☐ ACL (Access Control List): Contrôle d'accès granulaire par utilisateur/rôle

☐ Validation d'Entrée: Sanitization contre injection SQL/code

Surveillance & Audit:

☐ Logs de Sécurité: Enregistrement des tentatives d'accès/erreurs

☐ IDS/IPS: Détection/Prévention d'intrusions

☐ Monitoring en Temps Réel: Alertes sur anomalies de sécurité

Hardening & Best Practices:

☒ Désactivation des Services Inutiles: Minimiser surface d'attaque

☒ Mise à Jour des Dépendances: Patches de sécurité appliqués

☐ Secrets Management: Stockage sécurisé des clés/passwords (pas en hardcoded)

☐ Chiffrement au Repos: Données sensibles chiffrées en stockage

☐ Isolation Réseau: Segmentation, VLANs, zones démilitarisées

Sécurité Cloud & APIs (si Cloud Gateway utilisée)

Mesures de sécurité spécifiques pour intégration cloud:

Authentification Cloud & API Keys:

☐ OAuth 2.0: Authentification déléguée vers fournisseur cloud (AWS IAM, Azure

AD, Google Auth)

☐ API Keys: Clés uniques pour Tab5 générées et sécurisées côté cloud

☐ Rotating Credentials: Rotation automatique clés/tokens (ex: tous les 30 jours)

☐ mTLS vers Cloud: Certificats client pour authentification mutuelle Tab5→Cloud

Chiffrement Transport Cloud:

☐ HTTPS/TLS: Toute communication Tab5→Cloud en HTTPS avec certificats valides

☐ TLS 1.3: Utiliser TLS 1.3 minimum pour encryption forward-secure

☐ Certificate Pinning: Épingler certificat serveur cloud pour prévention man-in-the-middle

Sécurité Stockage Cloud:

☐ Encryption at Rest: Données chiffrées côté cloud (AWS KMS, Azure Key Vault, etc)

☐ Database Encryption: Chiffrement native de la base de données cloud

☐ Access Control: IAM granulaire - Tab5 ne peut accéder que ses propres données

Gestion des Secrets & Credentials:

☐ Secrets Management: Stockage API keys/credentials sécurisé (Vault, AWS Secrets Manager)

☐ No Hardcoded Secrets: Credentials JAMAIS en hardcoded dans code ou configuration

☐ Environment Variables: Credentials passées via variables d'environnement sécurisées

Monitoring & Compliance Cloud:

☐ API Rate Limiting: Limiter requêtes API pour prévention DDoS

☐ Cloud Audit Logs: Enregistrer accès et modifications de données cloud

☐ GDPR/Data Privacy: Conformité réglementaire (GDPR, CCPA) pour données stockées cloud

☐ Offline Queue: Queue locale si connexion cloud perdue (sync automatique au retour)

Sélectionnez les protocoles de transport utilisés pour la communication edge:

☐ MQTT: Protocole publish/subscribe très léger, idéal pour IoT, faible bande passante, connexion instable

☒ HTTP/HTTPS: API REST classique, facile à déboguer, overhead supérieur, standard web

☐ CoAP: Protocole ultra-léger pour appareils contraints (low power IoT), alternative MQTT

☐ RS485: Communication série filaire industrielle, longue portée (1200m), multi-master

☐ Modbus (RTU/TCP): Protocole industriel standard, acquisition capteurs, simple et robuste

☒ WebSocket: Communication bidirectionnelle temps-réel, push/pull, interface web interactive

☐ TCP/UDP: Transport bas-niveau custom, performance maximale, nécessite implémentation custom

☐ Protocole Custom: Implémentation propriétaire adaptée aux besoins spécifiques

☐ Plusieurs protocoles: Hybridation de protocoles (ex: MQTT + RS485, HTTP + CoAP)

Note: Votre architecture, vos composants (capteurs, modules radio), protocoles de transport et mesures de cybersécurité doivent être clairement documentés dans la documentation et expliqués lors de la soutenance. Le choix de ces éléments affecte directement la complexité, les performances et la sécurité du projet.

1. Implémentation Edge Computing et Architecture -- 25 points

Points	Critères
23-25	**Excellent** Architecture edge computing bien pensée et clairement documentée. Choix justifiés de l'architecture (avec ou sans cloud gateway), des composants optionnels et du protocole de transport. Protocole bien choisi et implémenté. Mesures de cybersécurité robustes implémentées (HTTPS/MQTTS, authentification tokens/certificats/RADIUS, hashing/CRC pour SD card, firewall, rate limiting, validation d'entrée). Si cloud gateway utilisé: authentification cloud robuste (OAuth/API keys sécurisées), chiffrement TLS 1.3+, certificate pinning, encryption at rest, gestion des secrets sécurisée. Architecture sécurisée documentée. Intégration des capteurs filaires/sans-fil, modules radio, et services cloud correctement implémentée. Déploiement efficace sur Tab5 avec gestion optimale des ressources. Scalabilité et maintenabilité démontrées. Gestion des pannes cloud (offline queue, retry logic).
18-22	**Bon** Architecture correcte et fonctionnelle. Choix architectural (local ou avec cloud), protocole et sécurité clairement décrits et justifiés. Plusieurs mesures de sécurité implémentées (TLS, authentification MAC/RADIUS, hashing/CRC). Si cloud: authentification cloud et chiffrement transport implémentés. Composants optionnels bien intégrés. Déploiement réussi avec gestion adéquate des ressources. Quelques optimisations possibles.
13-17	**Acceptable** Architecture fonctionnelle de base. Déploiement réalisé avec quelques inefficacités. Description de l'architecture et du protocole présente mais incomplète. Mesures de sécurité minimales ou partiellement implémentées. Intégration des composants optionnels partielle.
0-12	**Insuffisant** Architecture insuffisante ou non-fonctionnelle. Déploiement incomplet. Protocole de transport absent ou mal implémenté. Sécurité ignorée ou non-implémentée. Intégration des composants problématique.

2. Optimisation des Performances et Gestion des Ressources -- 15 points

Points	Critères
14-15	**Excellent** Optimisations multiples démontrées et documentées (latence réseau, consommation mémoire RAM, utilisation CPU, consommation électrique, surtout important si capteurs sans-fil ou modules radio). Benchmarks avec résultats. Gestion efficace des ressources avec monitoring. Techniques d'optimisation appliquées (compression, quantization, caching).
11-13	**Bon** Optimisations adéquates appliquées. Mesures de performance documentées. Gestion des ressources correcte et efficace.
8-10	**Acceptable** Quelques optimisations basiques. Mesures partielles de performance. Gestion des ressources satisfaisante mais peu détaillée.
0-7	**Insuffisant** Peu ou pas d'optimisations. Performance non mesurée ou non documentée.

3. Troubleshooting et Résolution de Problèmes -- 20 points

Points	Critères
18-20	**Excellent** Documentation complète des problèmes rencontrés (ressources insuffisantes, connectivité WiFi, communication capteurs/modules radio, problèmes protocole, timeouts, sécurité: certificats invalides, authentification RADIUS/cloud échouée, CRC mismatch SD card, chiffrement, validation entrée). Si cloud gateway: problèmes connectivité cloud, timeout API, credential rotation issues, certificate pinning failures, cloud service unavailable (offline queue behavior), rate limiting, data sync conflicts. Solutions claires avec justifications techniques. Guide GitHub complet avec tous les pièges, erreurs courantes (protocole, sécurité, cloud), et débogage. Avertissements de sécurité (RADIUS timeout, CRC mismatch, MAC filtering, API key exposure, cloud auth failures). Prévention proactive.
15-17	**Bon** Bonne documentation des problèmes et solutions, y compris enjeux sécurité (RADIUS, CRC, et si cloud: API auth, TLS, offline behavior). Guide pour éviter erreurs bien expliqué. Quelques détails manquants.
11-14	**Acceptable** Documentation partielle des problèmes et solutions. Guide basique pour éviter les erreurs. Problèmes de protocole peu documentés. Sécurité peu ou pas mentionnée.
0-10	**Insuffisant** Documentation insuffisante des problèmes. Peu ou pas de guide de prévention. Problèmes de protocole et sécurité non documentés.

Guide attendu: Section dédiée dans le README ou TROUBLESHOOTING.md listant: (1) Problèmes spécifiques à votre architecture et composants (WiFi, LoRa, capteurs filaires/sans-fil),

(2) Symptômes et diagnostics, (3) Solutions appliquées, (4) Points d'attention, (5) Common pitfalls.

4. Qualité du Code et Architecture -- 12 points

Points	Critères
11-12	**Excellent** Code bien structuré et modulaire. Gestion efficace des ressources. Documentation excellente. Absence de bugs critiques. Bonnes pratiques de codage respectées.
9-10	**Bon** Architecture correcte, fonctions bien séparées. Commentaires adéquats. Code lisible et maintenable.
6-8	**Acceptable** Code fonctionnel avec quelques problèmes d'organisation. Documentation partielle.
0-5	**Insuffisant** Code désorganisé ou peu documenté. Bugs significatifs.

5. Documentation Technique et Conception -- 13 points

Points	Critères
12-13	**Excellent** README complet avec architecture edge détaillée (choix justifiés). Diagrammes: déploiement, flux données, composants et interaction. Schémas de câblage pour capteurs filaires. Documentation complète du protocole de transport (MQTT/Mosquitto, HTTP REST, CoAP, RS485, Modbus, WebSocket). Documentation des modules radio (WiFi C6, LoRa). Documentation de sécurité détaillée: mesures implémentées (HTTPS/MQTTS, authentification MAC/RADIUS/tokens/certificats, hashing/CRC pour SD card, firewall, rate limiting), justification des choix de sécurité, configuration RADIUS, guide CRC pour SD card, directives de déploiement sécurisé, gestion des secrets/clés. Si cloud gateway utilisé: architecture cloud détaillée (services, base données, APIs), authentification cloud (OAuth flow, API keys, credentials management), chiffrement transport (TLS 1.3, certificate pinning), encryption at rest, offline queue behavior, rate limiting API, data privacy (GDPR), backup/recovery strategy. Guide d'installation étape-par-étape sécurisé. Configuration réseau, protocole, cloud et sécurité documentée. API bien documentée avec exemples sécurisés. Cas d'usage et exemples.
10-11	**Bon** Documentation adéquate avec schémas d'architecture. Instructions de déploiement claires. Documentation du protocole et des composants présente. Mesures de sécurité documentées avec justifications. Si cloud: cloud integration documentée (endpoints, auth basics, offline behavior mentionnés).
7-9	**Acceptable**

Points	Critères
	Documentation basique. Quelques schémas ou diagrammes. Documentation du protocole incomplète. Mesures de sécurité peu documentées.
0-6	**Insuffisant** Documentation insuffisante. Schémas absents ou peu clairs. Protocole de transport non documenté. Sécurité ignorée.

6. Soutenance Orale (10 min individuelles) -- 15 points

Clarté et Pédagogie -- 5 points

Points	Critères
4.7-5	Excellente clarté et pédagogie. Explications fluides et progressives. Adapte le discours au public. Engageant et captivant.
3.75-4.6	Bon. Exposé clair et organisé. Logique facile à suivre. Bon débit de parole.
2.5-3.74	Acceptable. Exposé compréhensible mais quelques passages peu clairs. Rythme parfois irrégulier.
0-2.4	Insuffisant. Exposition peu claire. Difficile à suivre.

Maîtrise Technique & Répondre aux Questions -- 5 points

Points	Critères
4.7-5	Maîtrise complète du projet. Réponses précises et détaillées. Justifie choix architecturaux, composants, protocole de transport et mesures sécurité (RADIUS, CRC, MAC filtering, TLS). Si cloud: explique choix architecture cloud (local vs cloud sync, APIs 3ème partie), authentication cloud robuste, offline queue behavior, API rate limiting, data privacy. Explique optimisations et compromis. Débat technique fluide sur protocole et sécurité (et cloud si applicable). Peut expliquer trade-offs latence/bande passante/puissance/sécurité/coûts cloud. Démontre compréhension profonde des vulnérabilités et mitigations (RADIUS timeout, SD card corruption detection, certificate validation, API key compromise, cloud service unavailable).
3.75-4.6	Bonne compréhension du projet. Répond correctement à la plupart des questions. Concepts clés bien maîtrisés (protocole, architecture, sécurité incluant RADIUS/CRC, et si cloud: authentification cloud, offline behavior). Justifie choix de protocole et mesures sécurité.
2.5-3.74	Compréhension partielle. Réponses avec quelques imprécisions. Lacunes sur certains concepts (protocole peu expliqué, sécurité mal comprise).
0-2.4	Maîtrise insuffisante. Réponses vagues ou incorrectes. Protocole ou sécurité mal compris.

Qualité Visuelle du Support & Démonstration -- 5 points

Points	Critères

Points	Critères
4.7-5	Support visuellement excellent (schémas architecture, diagrammes flux données, schémas capteurs/modules, diagramme protocole, architecture sécurité, diagramme RADIUS si utilisé, schéma CRC SD card, et si cloud: diagramme architecture cloud avec services/APIs/storage). Démonstration complète réussie. Vidéo ou live demo fluide montrant tous composants, protocole fonctionnant, et mesures sécurité activées (certificats valides, authentification réussie, chiffrement observable, RADIUS successful auth si utilisé, CRC validation si utilisé). Si cloud: démontre Tab5→Cloud communication en HTTPS/TLS, API call successful avec résultats, offline queue behavior (optionnel).
3.75-4.6	Support bon avec schémas utiles et diagrammes. Démonstration réussie du protocole et de la sécurité (RADIUS/CRC si applicable). Si cloud: cloud integration documentée et fonctionnelle. Globalement professionnel.
2.5-3.74	Support acceptable mais peu polished. Quelques schémas. Démonstration du protocole partielle. Sécurité peu ou pas démontrée.
0-2.4	Support peu attrayant. Peu de visuels. Démonstration absente ou protocole/sécurité non-fonctionnel.

Bonus Optionnels -- jusqu'à +12 points

GitHub Contribution Bonus

10 points bonus: Projet livré via GitHub avec repository public/partagé et README clair. Aucun commit minimum requis.

+2 points supplémentaires: Historique de commits réguliers et bien documentés (minimum 15-20 commits significatifs).

Résumé de Notation

Plage de Points	Niveau	Interprétation
95-112	**A+ Excellent**	Projet exceptionnel
90-94	**A Très Bon**	Très bonne qualité
85-89	**B+ Bon**	Bon niveau
80-84	**B Satisfaisant**	Compétences validées
70-79	**C Acceptable**	Minimum requis
< 70	**F Insuffisant**	À réviser