DOSSIER DE SÉCURITÉ ET CONFORMITÉ

Sécurité, souveraineté des données et conformité réglementaire

Architecture de sécurité du système, conformité avec TS 50701 et EN 50155, gestion des identités, souveraineté des données de l'opérateur et conformité au Règlement européen sur l'IA (AI Act) et au RGPD.

Document	IN-SIGHT-SC-001 · Version publique 1.0
Date	Juin 2026
Organisation	Ingérop Espagne — Division Transports (T3)
Programme	IN³ Saison IV
Audience	Directions techniques, responsables de cybersécurité (CISO), DPO, conseil juridique

1. La sécurité commence par l'architecture : non-intrusivité

La décision de conception la plus importante d'IN-SIGHT du point de vue de la sécurité n'est pas une contre-mesure : c'est l'architecture elle-même. Le système **ne se connecte à aucun bus de données du véhicule** (MVB, CANbus, Ethernet véhiculaire), n'accède ni au TCMS ni à aucun ordinateur embarqué, et fonctionne avec une alimentation et des communications totalement indépendantes. La conséquence directe : la surface d'attaque vers les systèmes de contrôle, traction, freinage ou signalisation du véhicule est nulle par construction. Il n'existe aucune voie physique ni logique d'IN-SIGHT vers un quelconque système de sécurité fonctionnelle.

> **Implication pour l'homologation**
> Ne modifiant ni n'interagissant avec aucun système certifié, l'installation d'IN-SIGHT n'altère pas le dossier de certification de sécurité fonctionnelle du véhicule. Le kit est considéré comme un équipement embarqué indépendant, ce qui simplifie drastiquement l'évaluation des risques de l'opérateur et élimine le principal obstacle à l'adoption des solutions de surveillance intégrées.

2. Conformité avec la réglementation ferroviaire

Norme	Champ d'application	Application dans IN-SIGHT
TS 50701	Cybersécurité dans les applications ferroviaires	L'architecture est conçue conformément à la TS 50701 dès le premier jour : segmentation des zones et des conduits, gestion des vulnérabilités, et traçabilité des événements de sécurité. Conçue pour évoluer vers la future EN 50701.

Norme	Champ d'application	Application dans IN-SIGHT
EN 50155	Équipements électroniques embarqués dans le matériel roulant	Sélection des composants, plages thermiques, essais de vibration et de choc, et connecteurs industriels M12 conformes à la norme. Plan de certification formel financé par les premiers déploiements commerciaux.
EN 13715	Profils de roue	Référence pour les conditions de validité du protocole Golden Run (tolérances de roulement certifiées par l'opérateur).
CEM ferroviaire	Compatibilité électromagnétique	Critère d'acceptation du pilote : zéro interférences avec les systèmes de signalisation et de communications. Numérisation du signal à la source (ESP32-S3 dans le pod) pour minimiser le câblage analogique susceptible aux EMI.

3. Chiffrement de bout en bout

État des données	Protection	Détail
En transit	TLS 1.3	Toutes les communications du système : MQTT du pod vers le cloud, requêtes du tableau de bord et du portail, ainsi que le trafic interne entre services cloud. Suites de chiffrement modernes, sans rétrogradation.
Au repos	AES-256	Chiffrement automatique de toutes les données stockées (Storage Service Encryption). Support des clés gérées par le client (CMK) dans Azure Key Vault pour les opérateurs qui en ont besoin.
Clés et certificats	Azure Key Vault	Cycle de vie complet des certificats de dispositif et des clés de chiffrement dans un module géré, avec rotation et audit des accès.

Chaque dispositif embarqué s'authentifie individuellement auprès de la plateforme avec une identité propre et des identifiants révocables par unité : la compromission hypothétique d'un kit n'affecte pas le reste de la flotte.

4. Identité, accès et isolation entre opérateurs

- **Microsoft Entra ID B2B** comme fournisseur d'identité : le personnel de l'opérateur accède avec ses propres comptes d'entreprise Microsoft, sans identifiants supplémentaires à gérer ni mots de passe partagés. L'ajout et la suppression du personnel sont automatiquement hérités de la gestion des identités de l'opérateur lui-même.
- **Authentification multifactorielle (MFA) obligatoire** pour tout accès humain à la plateforme.
- **Contrôle d'accès par rôles (RBAC)** : profils différenciés de visualisation, d'opération de maintenance et d'administration, avec privilège minimum par défaut.
- **Row-Level Security (RLS)** au niveau de la couche de présentation : dans les déploiements multi-opérateurs, chaque organisation voit uniquement et exclusivement les données de sa flotte. L'isolement s'applique au niveau des données, pas à celui de l'interface.
- **Enregistrement auditable** : toute action ayant un effet sur le système — reconnaissance et clôture des alertes, approbation des baselines, modifications de seuil — est enregistrée avec l'utilisateur, la date et un commentaire.

5. Souveraineté des données

Contrairement aux portails de diagnostic propriétaires des fabricants — où la télémétrie du véhicule reste entre les mains de l'OEM —, dans IN-SIGHT **les données appartiennent à l'opérateur**. C'est l'un des piliers de la proposition de valeur et cela se traduit par des engagements concrets :

Engagement	Mise en œuvre
Propriété des données	La télémétrie générée par la flotte de l'opérateur est la propriété de l'opérateur. Ingérop agit en tant que sous-traitant du traitement du service, non en tant que propriétaire des données.
Résidence dans l'UE	Infrastructure cloud déployée dans des régions de l'Union Européenne, avec résidence des données garantie contractuellement.
Portabilité	Exportation de toute série temporelle aux formats standards (CSV) à tout moment. Sans verrouillage des données : l'historique appartient également à l'opérateur à la fin du contrat.
Option on-premise	L'architecture, définie comme infrastructure en tant que code, permet un déploiement dans le cloud privé de l'opérateur pour les cas qui le nécessitent.

6. Conformité au Règlement européen sur l'IA (AI Act)

IN-SIGHT intègre les principes de l'AI Act dès la conception, et non comme une adaptation ultérieure. Le système de diagnostic est délibérément hybride — modèle physique rigoureux plus apprentissage automatique explicable — précisément pour éviter le comportement de boîte noire :

- **Explicabilité native.** La première étape du diagnostic est un modèle physique (filtre de Kalman) dont la sortie a une interprétation statistique directe ; la seconde utilise des arbres de décision avec analyse de contribution par caractéristique. Chaque alerte peut être expliquée : quel capteur, quelle déviation, par rapport à quelle condition de référence.
- **Traçabilité et intégrité.** Empreinte cryptographique SHA-256 des modèles et des jeux de données de calibration : chaque décision du système est traçable à la version exacte du modèle et du baseline qui l'a produite.
- **Supervision humaine effective.** Le système recommande ; la décision revient à l'équipe de maintenance. Le flux de reconnaissance et de clôture des alertes avec diagnostic final maintient l'humain dans la boucle et génère en outre un enregistrement terrain qui améliore le système.
- **Gestion de risque proportionnée.** IN-SIGHT est un outil d'aide à la maintenance, sans fonction de sécurité : il n'agit pas sur le véhicule et ne remplace aucune inspection réglementaire. Sa classification de risque selon le AI Act est, par conséquent, limitée.

7. Protection des données personnelles (RGPD)

La position d'IN-SIGHT vis-à-vis du RGPD est simple et robuste : **le système ne capture pas de données personnelles**. La télémétrie est exclusivement machine — vibration, température, acoustique des composants mécaniques, position du véhicule —. Il n'y a pas de caméras, pas de microphones de cabine orientés vers des personnes, pas de données sur les passagers ni sur la conduite individuelle. Les seules données à caractère personnel du service sont les comptes utilisateurs du personnel autorisé (nom et courriel professionnel), traitées conformément au RGPD avec pour seule finalité le contrôle d'accès et l'audit. Pour chaque déploiement, l'annexe de traitement correspondante est fournie et, si l'opérateur le demande, l'évaluation d'impact conjointe.

8. Résilience opérationnelle

Scénario	Comportement du système
Perte de couverture cellulaire (tunnels, zones d'ombre)	Tampon local de plusieurs semaines de capacité dans la passerelle embarquée. Synchronisation rétroactive automatique lors de la récupération de la connectivité (store-and-forward). Sans perte de données.
Défaillance d'un capteur	Détection automatique par la propre surveillance de la qualité du signal ; alerte à l'administrateur. Le diagnostic se poursuit avec les modalités restantes en déclarant l'incertitude correspondante.

Scénario	Comportement du système
Compromission d'un dispositif	Révocation individuelle de l'identité du dispositif sans affecter le reste de la flotte. Réapprovisionnement avec de nouvelles identités.
Indisponibilité du cloud	Les kits continuent de capturer et de stocker localement. Le service est rétabli sans intervention sur site.

Pour une revue de sécurité détaillée avec votre équipe (CISO, DPO, direction technique), demandez une session technique sur **in3-insight.cloud**.