SECURITY AND COMPLIANCE DOSSIER

Security, Data Sovereignty, and Regulatory Compliance

System Security Architecture, compliance with TS 50701 and EN 50155, Identity Management, operator Data Sovereignty, and compliance with the European AI Regulation (AI Act) and GDPR.

Document	IN-SIGHT-SC-001 · Public Version 1.0
Date	June 2026
Organization	Ingérop Spain — Transport Division (T3)
Program	IN³ Season IV
Audience	Technical management, cybersecurity officers (CISO), DPO, legal counsel

1. Security begins with architecture: non-intrusiveness

The most important design decision of IN-SIGHT from a security perspective is not a countermeasure: it is the architecture itself. The system **does not connect to any vehicle data bus** (MVB, CANbus, vehicular Ethernet), does not access the TCMS or any onboard computer, and operates with completely independent power and communications. The direct consequence: the attack surface towards the vehicle's control, traction, braking, or signaling systems is **zero by design**. There is no physical or logical path from IN-SIGHT to any functional safety system.

> **Implication for certification**
> Since it does not modify or interact with any certified system, the installation of IN-SIGHT does not alter the vehicle's functional safety certification file. The kit is considered independent onboard equipment, which drastically simplifies the operator's risk assessment and removes the main barrier to adopting integrated monitoring solutions.

2. Compliance with railway regulations

Standard	Scope	Application in IN-SIGHT
TS 50701	Cybersecurity in railway applications	The architecture is designed according to TS 50701 from day one: zone and conduit segmentation, vulnerability management, and security event traceability. Designed to evolve towards the future EN 50701.
EN 50155	Onboard electronic equipment in rolling stock	Component selection, thermal ranges, vibration and shock testing, and industrial M12 connectors according to the

Standard	Scope	Application in IN-SIGHT
		standard. Formal certification plan funded by the initial commercial deployments.
EN 13715	Wheel profiles	Reference for the validity conditions of the Golden Run protocol (rolling tolerances certified by the operator).
Railway EMC	Electromagnetic Compatibility	Pilot acceptance criterion: zero interference with signaling and communication systems. Signal digitization at source (ESP32-S3 in pod) to minimize analog wiring susceptible to EMI.

3. End-to-end Encryption

Data State	Protection	Detail
In Transit	TLS 1.3	All system communication: MQTT from pod to cloud, dashboard and portal queries, and internal traffic between cloud services. Modern encryption suites, no downgrade.
At rest	AES-256	Automatic encryption of all stored data (Storage Service Encryption). Support for customer-managed keys (CMK) in Azure Key Vault for operators who require it.
Keys and certificates	Azure Key Vault	Full lifecycle management of device certificates and encryption keys in a managed module, with rotation and access auditing.

Each onboard device authenticates individually to the platform with its own identity and revocable credentials per unit: the hypothetical compromise of one kit does not affect the rest of the fleet.

4. Identity, access, and isolation between operators

- **Microsoft Entra ID B2B as identity provider:** operator personnel access with their own corporate Microsoft accounts, without additional credentials to manage or shared passwords. Personnel onboarding and offboarding is automatically inherited from the operator's own identity management.
- **Mandatory multi-factor authentication (MFA)** for all human access to the platform.
- **Role-Based Access Control (RBAC)**: differentiated profiles for viewing, maintenance operation, and administration, with minimum privilege by default.
- **Row-Level Security (RLS) at the presentation layer**: in multi-operator deployments, each organization sees exclusively the data of its own fleet. Isolation is applied at the data layer, not at the interface layer.
- **Auditable logging**: every action affecting the system — alert acknowledgment and closure, baseline approval, threshold changes — is recorded with user, date, and comment.

5. Data Sovereignty

Unlike manufacturers' proprietary diagnostic portals — where vehicle telemetry remains under the OEM's control — in IN-SIGHT **the data belongs to the operator**. This is one of the pillars of the value proposition and is embodied in concrete commitments:

Commitment	Implementation
Data Ownership	Telemetry generated by the operator's fleet is owned by the operator. Ingérop acts as the service data processor, not as the data owner.
Residence in the EU	Cloud infrastructure deployed in European Union regions, with contractually guaranteed data residency.

Commitment	Implementation
Portability	Export of any time series in standard formats (CSV) at any time. No data lock-in: the historical data belongs to the operator even after the contract ends.
On-premise option	The architecture, defined as infrastructure as code, supports deployment in the operator's private cloud for cases that require it.

6. Compliance with the European AI Regulation (AI Act)

IN-SIGHT incorporates the principles of the AI Act by design, not as a subsequent adaptation. The diagnostic system is deliberately hybrid — rigorous physical model plus explainable machine learning — precisely to avoid black-box behavior:

- **Native explainability.** The first diagnostic stage is a physical model (Kalman filter) whose output has direct statistical interpretation; the second uses decision trees with feature contribution analysis. Each alert can be explained: which sensor, what deviation, relative to which reference condition.
- **Traceability and integrity.** SHA-256 cryptographic fingerprint of models and calibration datasets: every system decision is traceable to the exact version of the model and baseline that produced it.
- **Effective human supervision.** The system recommends; the maintenance team decides. The alert recognition and closure flow with final diagnosis keeps the human in the loop and also generates the ground-truth record that improves the system.
- **Proportional risk management.** IN-SIGHT is a maintenance support tool, without a safety function: it does not act on the vehicle nor replace any regulatory inspection. Its risk classification under the AI Act is, consequently, limited.

7. Personal data protection (GDPR)

IN-SIGHT's position regarding the GDPR is simple and robust: **the system does not capture personal data**. The telemetry is exclusively machine data — vibration, temperature, mechanical component acoustics, vehicle position. There are no cameras, no cabin microphones aimed at people, no passenger or individual driving data. The only personal data in the service are the user accounts of authorized personnel (name and corporate email), processed in accordance with the GDPR solely for access control and auditing purposes. For each deployment, the corresponding processing annex is provided and, if the operator requires, the joint impact assessment.

8. Operational resilience

Scenario	System behavior
Loss of cellular coverage (tunnels, shadow zones)	Local buffer of weeks of capacity in the embedded gateway. Automatic retroactive synchronization upon connectivity recovery (store-and-forward). No data loss.
Sensor failure	Automatic detection through signal quality monitoring; alert to the administrator. Diagnosis continues with the remaining modalities with the corresponding declared uncertainty.
Device compromise	Individual revocation of the device identity without affecting the rest of the fleet. Re-provisioning with new credentials.
Cloud unavailability	The kits continue capturing and storing locally. The service is restored without field intervention.

For a detailed security review with your team (CISO, DPO, technical management), request a technical session at **in3-insight.cloud**.