

SECTOR PACKAGE · CRITICAL INFRASTRUCTURE

Decisions with physical impact, controlled and provable

Control with operational context, continuity and verifiable evidence for energy, water, transport, telecommunications, healthcare, ports and airports.

For an essential operator, a failure is not a data leak: **it is a supply that gets cut or a service that stops**. Operators, vendors, systems and automations act on assets that cannot fail. *Who authorizes each action on the essential asset, with which context, and what evidence remains for the regulator and the investigation?*

WHAT VELANTIA BRINGS TO THIS SEGMENT

GATE — authorizes with **operational context** before acting on the essential asset: state, risk, time window, responsible party — and blocks what would endanger the service.

SENTINEL — observes activity on the infrastructure, **detects anomalies** and attributes each action to its origin: person, vendor, system or agent.

EVIDENCE — preserves the **verifiable trail** the regulator and incident investigation will demand: decision, approval, execution and outcome.

AUTONOMY — governs the automation reaching physical assets, with **explicit limits, human approval and revocation**.

WHAT YOU CAN DO WITH IT

- ▶ **Authorization with context before executing** on essential assets — not just a valid credential.
- ▶ **Local continuity on loss of connection**: essential functions keep operating under defined policies.
- ▶ **Bound the damage of compromised credentials or agents**: only what the permission allows, with a record of everything.
- ▶ **Answer the regulator with evidence**, not reconstructions: every incident with its coherent history.

No command — however well authenticated — should be able to force a dangerous state of the service.

DEPLOYMENT

Depending on the environment: **SOVEREIGN 700** for sovereign operation and **INDUSTRIAL 500R** for plant and OT (both available for pre-order), governed from **VELANTIA ONE**. Also software, virtual machine or the operator's private cloud. It integrates with existing systems **without replacing them**.

WHY NOW

Cybersecurity obligations for essential operators tighten year after year, threats against infrastructure grow and automation reaches assets with physical impact. The ability to prove the applied control stops being desirable: **it becomes mandatory**.

Next step: an initial meeting and a demonstration.

Full flow in a controlled or simulated environment, without acting on real infrastructure. A sovereignty and critical-infrastructure pilot proposal is available, scoped and with metrics.

Agustín López Mayor — Inventor · Co-founder · **Stephan Hoof** — Co-founder · International Expansion

contact@velantia.io · velantia.io · Villajoyosa (Alicante, Spain) · Weikersheim (Germany) · Ruse (Bulgaria)

Nine patent applications filed with the Spanish Patent and Trademark Office (OEPM) · pending · Strategic presentation document