

SECTOR PACKAGE · INDUSTRY AND OT

Machine commands under control, plants that keep running

Control, local continuity and verifiable evidence for commands to machinery, remote maintenance and vendor intervention in OT environments.

In OT, a failure is not a data leak: **it is a plant shutdown or a dangerous physical state**. Remote maintenance, integrators and vendors act on systems that cannot stop, and automation reaches deeper every year. *Who authorizes each command to the machine, with which operational context, and what evidence remains of each intervention?*

WHAT VELANTIA BRINGS TO THIS SEGMENT

GATE — authorizes each command and each intervention with **operational context**: which asset, which state, which time window, which vendor — and blocks what does not belong.

SENTINEL — observes activity on plant assets, **detects anomalous behavior** and attributes each action to its origin.

EVIDENCE — preserves the **traceability of every intervention**: who acted on which equipment, with which authorization and with what outcome.

AUTONOMY — governs robots, industrial automation and agents operating on the plant floor, with **explicit limits and revocation**.

WHAT YOU CAN DO WITH IT

- ▶ **Authorize remote maintenance** per vendor, equipment, task and time window — and nothing more.
- ▶ **Operate locally when the central connection drops**: essential functions continue under previously defined policies.
- ▶ **Bound the damage of a compromised credential**: it can only do the little its permission allows, and everything is recorded.
- ▶ **Prove every intervention** to customers, insurers or regulators, without rebuilding scattered records from each manufacturer.

Ultimate control stays in the plant and with its owner — with evidence of every executed command.

DEPLOYMENT

Built for the plant floor: the **INDUSTRIAL 500R** appliance (available for pre-order), with ruggedized hardware and local operation, governed from **VELANTIA ONE** together with the rest of the deployment. Also software, virtual machine or private cloud where applicable. It integrates with your industrial systems **without replacing what exists**.

WHY NOW

IT/OT convergence widens the attack surface just as industrial-cybersecurity obligations tighten, and automation reaches assets with physical impact. Whoever does not govern the commands to their machines today will only investigate the shutdown tomorrow.

Next step: an initial meeting and a demonstration.

Full flow in a controlled or simulated environment: command → policy → approval or block → evidence, without acting on the real plant. A scoped pilot proposal is available, 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