AI & Cybersecurity per la mobilità di persone e merci

AI affidabile e sovrana per la mobilità delle merci

Giuseppe Parlati

Almaviva Group

Divisione Transport & Logistics – Architecture Dept.

17 giugno 2026


Almaviva
Almaviva
KlingAI 3.0

Uno snapshot della cybersecurity nei Trasporti e AI (2025-2026)

2025 — 2026

Mar 2025

Ukrzaliznytsia (Ucraina)
biglietteria online KO
→ Protocolli di backup

Lug 2025

LAMEHUG
1° malware con LLM (APT28)
modello Alibaba su HuggingFace

Estate 2025

Baltico/Mar Nero sotto assedio
5.800 navi colpite (GNSS jamming)
100+ attacchi, 8 gruppi APT.

Set 2025

Collins Aerospace MUSE
Ransomware → aeroporti in tilt:
Heathrow, Bruxelles e Berlino

Gen 2026

GreyNoise
91.403 attacchi a
infrastrutture LLM

283
ransomware nel 2025
+132% vs 2024 (122)

71%
vittime nel segmento
trucking & freight

725 M$
furti di carico (+60%)
GPS spoofing — CargoNet

Trasporto merci: conseguenze economiche dirette e furto fisico dei carichi.

Dove l'AI è già matura nella mobilità delle merci

Ottimizzazione & pianificazione

Routing, dispatch e demand forecasting: ricerca operativa + ML, in produzione da anni con ROI ripetibile.
Es. UPS ORION (On-Road Integrated Optimization and Navigation) il più sofisticato

Manutenzione predittiva

ML sulla **telemetria** di flotte, materiale rotabile e gruppi frigo: ottimizza fermi e costi.
Es. Siemens Railigent: −40% fermi

Computer Vision

Robotica per picking e sorting nei magazzini, OCR dei codici container ai gate, lettura targhe, rilevamento danni.
Qui la computer vision è affidabile

Visibility & predictive ETA

Control tower: coordinare, monitorare e ottimizzare catene di fornitura, logistica, trasporti
Es. project44, FourKites (monitoraggio RT, visibilità end-to-end e ottimizzazione delle catene di forniture)

Frontiera: **guida autonoma in ambiente aperto**, **orchestrazione agentica cross-attore**, **GenAI sulle decisioni operative** — l’ostacolo principale non è l'algoritmo, ma sicurezza, responsabilità e integrazione tra attori.

La frontiera — autonomia e agenti — arriverà a maturità solo quando l’AI sarà sicura, governata e sovrana … by-design.

Il vero prerequisito per l’AI nella Logistica

Quantità, Qualità, Interoperabilità e fiducia tra gli attori della filiera: una è sopravvalutata, le altre tre sono una piramide.

Fiducia tra gli attori
il vero prerequisito

Interoperabilità
il dato deve fluire tra sistemi e attori

Qualità del dato
garbage in, garbage out - le fondamenta

Quantità — la più sopravvalutata: conta la bontà dei dati e non la quantità (data-centric AI). Cento dati "puliti" battono un milione di dati "sporchi".

Perché in logistica?

È un ecosistema multi-attore — spedizionieri, vettori, porti, dogane, 3PL, spesso concorrenti. Il dato attraversa i confini tra organizzazioni: nessuno condivide dati certificati e di qualità se non si fida di come saranno usati e protetti.

La fiducia non è ‘aleatoria': si progetta.

Governance · provenienza e integrità · Zero-Trust · sovranità del dato. È il modello dei data space europei (Gaia-X, IDS), dell'eFTI e degli standard aperti.

In logistica il dato non è un problema tecnico: è un problema di fiducia.

Evitare by-design che l'AI diventi una vulnerabilità

L'AI ha una doppia faccia — asset da proteggere e arma

I bersagli principali nell'AI

- **Dati:** avvelenamento di training e telemetria
- **Modello:** furto, estrazione, attacchi adversarial
- **Agenti:** prompt injection, excessive agency (OWASP)
- **Supply chain dell'AI:** shadow AI non governata,
- **Tre livelli da difendere**: dispositivi–edge–cloud.

«By-design», in concreto

- **Threat modeling dal giorno zero**, con tassonomie AI-specifiche (OWASP LLM/Agentic, MITRE ATLAS).
- **Standard** come ossatura: NIST AI RMF, ISO/IEC 42001, IEC 62443, e compliance-by-design NIS2/CRA/AI Act.
- **Zero-Trust end-to-end** e modello protetto (confidential computing); limiti agli agenti, human-in-the-loop.
- **MLSecOps + quality gate (V&V)** non negoziabile prima del go-live + human oversight (AI Act).

Sviluppo delle Applicazioni (SDLC AI Assisted)

requisiti, design, sviluppo software, code review, testing

La sicurezza si progetta, non si aggiunge — aggiungerla dopo costa di più e protegge di meno.

"Claude Mythos Preview": potenzialità e «sovranità cognitiva»

Modello AI di frontiera (Anthropic) con capacità cyber così elevate da imporre un rilascio controllato — "Project Glasswing".

Potenzialità

- **S**copre vulnerabilità zero-day
- **G**
- **P**
- **A**

Il Sole 24 Ore — Prof G. F. Italiano [10 giu '26]

Dalla sovranità digitale alla sovranità cognitiva.

«La partita del futuro non si gioca più sulla diffusione dell'AI, ma sul controllo delle sue capacità più avanzate.»

Giuseppe F. Italiano, Il Sole 24 Ore

conta l'accesso e il controllo

10 giu: Anthropic lancia Fable 5 (basato su Mythos 5) - 12 giu il governo US lo blocca

Comunicato Antropic:

The US government, citing national security authorities, has issued an export control directive to suspend all access to Fable 5 and Mythos 5 by any foreign national, whether inside or outside the United States, including foreign national Anthropic employees. The net effect of this order is that we must abruptly disable Fable 5 and Mythos 5 for all our customers to ensure compliance. Access to all other Anthropic models will not be affected.

We received the directive from the government today at 5:21pm (ET). The letter did not provide specific details of its national security concern. …

https://www.anthropic.com/news/fable-mythos-access

Esempio in 2 settimane, 371 vulnerabilità individuate e corrette in Firefox (Mozilla); ai vertici nei test Capture-the-Flag vs altri modelli di frontiera.

Time-to-Exploit → minuti

da settimane/mesi a pochi minuti: la finestra tra scoperta e sfruttamento si azzera → rischio sistemico.

Dal perché al come

AI affidabile, sicura by-design e sovrana.

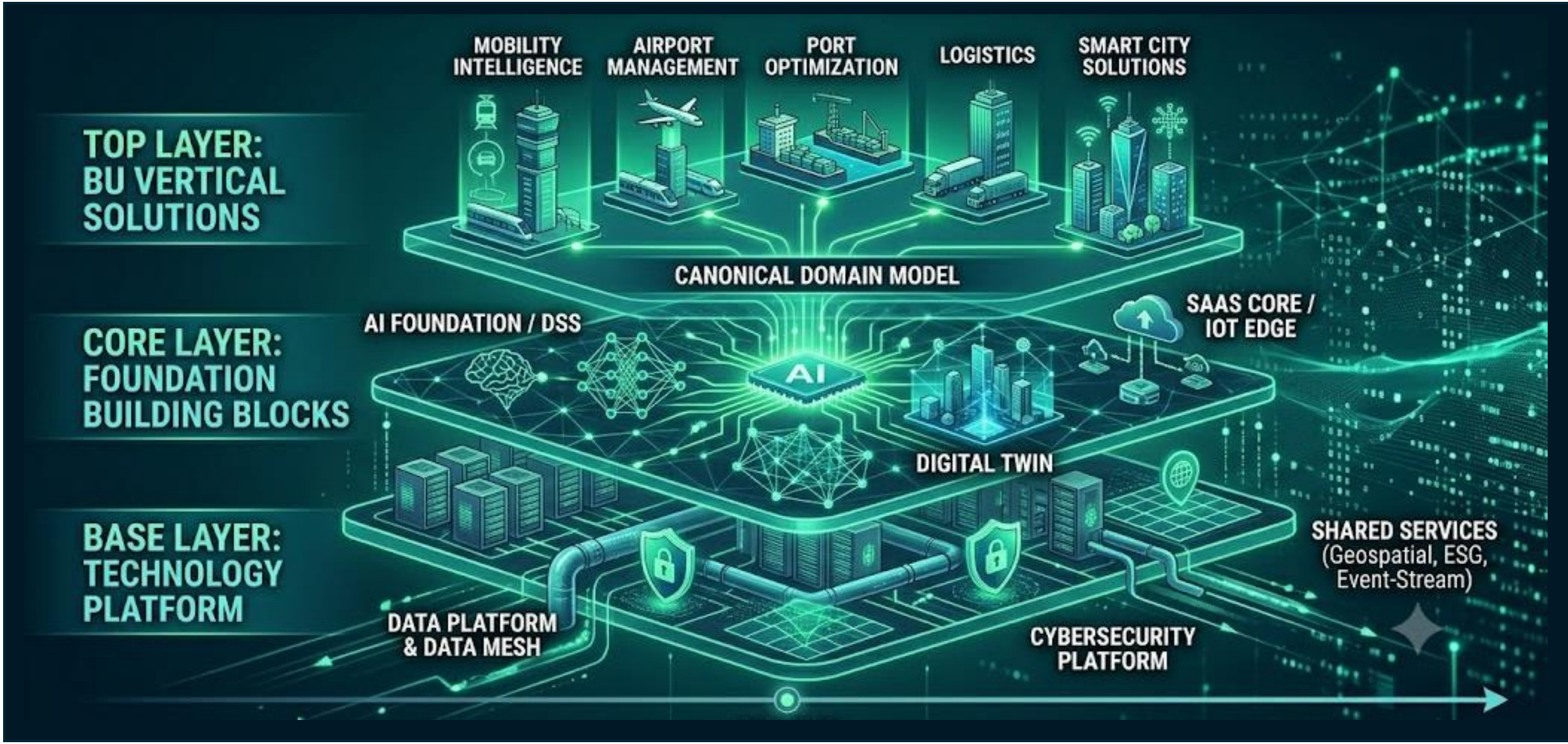
In Almaviva come la costruiamo in pratica?

Visione Strategica AI: Tecnologia, Tool e GOVERNANCE

1:30’

T&L Foundation Platform

1:30’



In conclusione

L'AI nella logistica scalerà solo dove sarà sicura, governata e sovrana.

Almaviva: un'azienda italiana al 100%, con respiro internazionale
- sicurezza, governance e sovranità del dato sono centrali -

Q&A

Grazie

Giuseppe Parlati
www.linkedin.com/in/giuseppeparlati/

Almaviva
Group