mobility magazine

N. 525 - 26 maggio 2026

Verso una "AI-Native Security".
Intervista a Panero di TTS Italia ▪
Rapporto Fermerci 2026 ▪
Rapporto CER-Confcommercio ▪
Biodiversità a Firenze ▪
Liguria GO in Braille ▪ ROAD ▪
GTT ▪ ATM ▪ Rhenus ▪
F-Ingegneria

Rossella Panero (TTS Italia)

Intervista

Verso una "AI-Native Security": la ricetta di TTS Italia per i trasporti del futuro: Intervista a Rossella Panero

In occasione dell'imminente convegno che TTS Italia ha organizzato a Roma sul tema "AI e Cybersecurity per la mobilità di persone e merci", Mobilitypress ha intervistato la presidente Rossella Panero.

L'adozione delle tecnologie digitali nei settori delle infrastrutture e della logistica è destinata a incidere in profondità sulla progettazione, realizzazione, gestione e manutenzione delle opere pubbliche e dei nodi della mobilità. Al contempo, l'Intelligenza artificiale è ormai entrata nelle nostre vite. Qual è l'utilizzo e l'impatto dei sistemi di Intelligenza Artificiale nel settore della mobilità di passeggeri e merci?

Gli ITS, nati dall'applicazione delle tecnologie informatiche e telematiche al mondo dei trasporti, sono uno strumento fondamentale per la realizzazione della smart mobility. L'Associazione è convinta che gli ITS possano apportare benefici importanti sia per il settore pubblico, attraverso la riduzione delle esternalità, sia per il settore privato, attraverso la creazione di opportunità di business, sia soprattutto per l'utente del sistema dei trasporti che può usufruire di servizi di mobilità più confortevoli, più efficienti e più rispettosi dell'ambiente.
L'Italia ha recepito con Decreto del 26 gennaio 2026 pubblicato il 18 febbraio 2026 in Gazzetta Ufficiale, la Direttiva 2023/2661/UE del 22 novembre 2023 di aggiornamento della Direttiva ITS 2010/40/UE sulla diffusione degli ITS. Le infrastrutture stradali e i veicoli stanno diventando nodi intelligenti di un ecosistema integrato, capace di generare valore tramite dati in tempo reale, automazione e capacità predittiva.
La mobilità sta quindi complessivamente attraversando una trasformazione profonda grazie alla digitalizzazione, alla crescente interconnessione dei sistemi di trasporto e all'uso massivo di dati. Il veloce diffondersi dell'AI (Artificial Intelligence) in tutti i campi e la sua integrazione nella mobilità sta trasformando radicalmente veicoli, infrastrutture, servizi digitali e sistemi energetici. Dai modelli di percezione per la guida autonoma alla "predictive maintenance" [manutenzione preventiva], dalle piattaforme MaaS (Mobility as a Service) all'anticipazione delle minacce cyber tramite "machine learning", l'AI è oggi un elemento critico per efficienza e sicurezza, ma l'integrazione di queste tecnologie abilite-

TTS ITALIA
Associazione Italiana della Telematica per i Trasporti e la Sicurezza

rà nel futuro un ecosistema di mobilità più efficiente, sicuro, sostenibile e resiliente.

Quali invece i rischi e le vulnerabilità dell'Intelligenza Artificiale nei trasporti? Come affrontarli?

L'adozione dell'intelligenza artificiale nel settore dei trasporti presenta un duplice profilo: da un lato, il potenziale per migliorare efficienza, sostenibilità e sicurezza; dall'altro, sfide tecniche, infrastrutturali, umane ed etiche che ne condizionano lo sviluppo.
Un quadro etico ben calibrato non è un ostacolo all'innovazione: ne è la condizione necessaria per garantire legittimità e accettazione sociale. È fondamentale ribadire che l'etica dell'AI non riguarda le presunte intenzioni morali delle macchine, che sono strumenti matematici, ma le scelte umane che guidano la loro progettazione, il loro addestramento e il loro impiego. La responsabilità risiede negli esseri umani che definiscono i dati, gli obiettivi e i criteri di valutazione dei sistemi.
L'intelligenza artificiale è comunque un imperativo strategico che eleva gli ITS a sistemi auto-apprendenti. Tuttavia, la sua adozione introduce un dualismo pericoloso: se da un lato l'IA agisce come "moltiplicatore di efficienza", dall'altro crea una classe di rischi "silenti" che non si manifestano con guasti tecnici evidenti, ma con derive decisionali che potrebbero essere catastrofiche. La gestione di questo dualismo richiede un passaggio dalla cybersecurity "tradizionale" a una "AI-Native Security", dove la robustezza del modello è monitorata durante l'intero ciclo di vita.
La trasformazione digitale del settore mobilità — con veicoli connessi, sistemi di guida assistita, flotte intelligenti, sharing mobility e infrastrutture V2X — pur offrendo benefici sistemici senza precedenti espone l'intero ecosistema a nuove superfici d'attacco. Ogni nuovo nodo connesso — dal sensore stradale al veicolo autonomo — diventa un potenziale punto di ingresso per

minacce che possono tradursi in impatti fisici immediati, rendendo imperativa un'analisi rigorosa del valore di mercato contrapposta alla magnitudo dei rischi.
I dati delineano un mercato in forte accelerazione, dove la "Smart Mobility" è diventata una dorsale economica primaria.
Tuttavia, la crescita segnala un'espansione della superficie digitale talmente rapida da rischiare di superare le capacità di difesa dei budget di manutenzione legacy delle infrastrutture critiche. Questa esplosione del valore digitale è, tuttavia, sotto assedio.
Gli ultimi dati (es. Rapporto CLUSIT 2026) e indicano un'emergenza sistemica, con un incremento del 48,7% degli attacchi rispetto all'anno precedente. Questo scenario conferma che il valore economico della mobilità connessa è direttamente proporzionale alla sua vulnerabilità.
L'IA trasforma questi numeri in capacità operativa, ma richiede una protezione che sia altrettanto dinamica e scalabile.

L'adozione di sistemi autonomi e di intelligenza artificiale nei trasporti impone di ripensare sicurezza, privacy, responsabilità. A che punto siamo a livello normativo?

L'ecosistema V2X ha trasformato ogni componente infrastrutturale in un bersaglio. La superficie d'attacco non è più limitata al centro di controllo, ma è distribuita su ogni impianto periferico, app o centralina di ricarica. Un attacco in questo dominio non è un mero furto di dati, ma un evento fisico con potenziali vittime reali.
Le esigenze di cybersecurity si articolano su più livelli: proteggere veicoli e infrastrutture connesse, garantire comunicazioni sicure e affidabili (preservando l'integrità, la disponibilità e la riservatezza dei dati), difendere piattaforme e servizi digitali, mettere in sicurezza infrastrutture di ricarica ed energia, rafforzare la supply chain, rispettare normative e standard internazionali e implementare strategie di sicurezza "by design" e monitoraggio continuo.
La cybersecurity "tradizionale" non è più sufficiente: serve un approccio integrato AI + cybersecurity, basato su robustezza dei modelli AI, difesa da attacchi adversarial, protezione dei dati sensibili usati per addestramento, architetture "zero trust" [Zero Trust, ossia basato sul principio "mai fidarsi, verificare sempre"], SOC potenziati con AI e una assoluta compliance normativa.
La conformità normativa non è infatti un onere burocratico, ma l'unico sistema di difesa scalabile contro attacchi di magnitudo geopolitica e costruisce di fatto un'opportunità di resilienza.
Suoi pilastri ne sono la Direttiva ITS 2023/2661/UE (Decreto 26/01/2026) che rende obbligatoria l'integrazione di servizi digitali sicuri e la disponibilità di dati interoperabili per la gestione stradale. Il successivo Piano d'Azione ITS nazionale, atteso entro il corrente anno, definirà le priorità implementative e ne chiarirà eventuali fondi disponibili.
La normativa NIS2 (D.Lgs. 138/2024) inquadra la mobilità come infrastruttura critica, imponendo obblighi severi di gestione del rischio e notifica incidenti.
L'AI Act individua i sistemi di trasporto come ad "alto rischio", richiedendo supervisione umana, trasparenza algoritmica e robustezza dei dati.
Il Cyber Resilience Act (CRA) impone requisiti di sicurezza per tutti i prodotti digitali (hardware e software) lungo l'intera supply chain e gli standard Tecnici, dalla ISO 21434, focalizzata sulla gestione della cybersecurity lungo tutto il ciclo di vita del veicolo, alla IEC 62443, che disciplina la sicurezza dei componenti industriali e in-frastrutturali.

Quali proposte/raccomandazioni proponete come TTS Italia per migliorare il coordinamento tra istituzioni e imprese nella difesa dalle minacce ibride nel settore trasporti?

La convergenza tra ITS, AI e cybersecurity rappresenta la base della mobilità del futuro. Solo attraverso un approccio integrato, proattivo e standardizzato sarà possibile garantire sistemi di trasporto efficienti, resilienti e sicuri.
La collaborazione tra industria, istituzioni e ricerca diventa quindi essenziale per costruire ecosistemi di mobilità affidabili e sostenibili.
A valle di un complesso lavoro svolto dall'Associazione in collaborazione con tutti i suoi associati e con le altre principali associazioni di settore, ci sentiamo di poter oggi individuare alcuni punti chiave fra loro interconnessi e che possono guidare la trasformazione digitale del sistema infrastrutturale e logistico italiano.
Il risultato del lavoro svolto sarà presentato **il 17 giugno al convegno nazionale organizzato da TTS Italia** dove si svolgerà un confronto con gli attori del settore ed i rappresentanti delle istituzioni competenti.
Ci auguriamo che il contributo della nostra associazione possa servire da stimolo per cogliere questa grande opportunità nella piena consapevolezza dei rischi che devono essere gestiti.

Intervista di Giulia Ratini