TTS 25
ITALIA
Associazione Italiana della Telematica
per i Trasporti e la Sicurezza

POSITION PAPER

AI e Cybersecurity per la mobilità di persone e merci

Giugno 2026

Obiettivo

Obiettivo del presente Position Paper è di approfondire il ruolo dell'**Intelligenza Artificiale** (AI – Artificial Intelligence) nella mobilità moderna e le sue intersezioni con la **Cybersecurity**, nonché di fornire raccomandazioni per far sì che le reti di mobilità possano svilupparsi e contribuire alla crescita sostenibile del Paese.

Tale documento è stato realizzato nell'ambito del **Gruppo di Lavoro** (GdL) "*AI e Cybersecurity per la mobilità di persone e merci*", coordinato da **TTS Italia**, l'Associazione Italiana della Telematica per i Trasporti e la Sicurezza che rappresenta il settore italiano degli Intelligent Transport Systems (**ITS**) e che riunisce i principali stakeholder pubblici e privati del comparto nazionale.

Gli **ITS**, nati dall'applicazione delle tecnologie informatiche e telematiche al mondo dei trasporti, sono uno strumento fondamentale per la realizzazione della smart mobility ed è parere ormai condiviso che 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.

Ormai la trasformazione digitale sta ridisegnando la mobilità: l'Italia ha recepito la Direttiva 2023/2661/UE del 22 novembre 2023 di aggiornamento della Direttiva ITS 2010/40/UE sulla diffusione degli ITS con il Decreto del 26 gennaio 2026, pubblicato il 18 febbraio 2026 in Gazzetta Ufficiale. Inoltre l'**integrazione** degli **ITS** e dell'**AI** promette un'efficienza, sicurezza e sostenibilità senza precedenti.

Tuttavia, questa profonda interconnessione espone l'intero ecosistema a rischi cyber esponenziali ed è necessario un approccio integrato e proattivo, guidato da un quadro normativo europeo in rapida evoluzione, per trasformare le vulnerabilità in resilienza e garantire la fiducia nel futuro della mobilità.

Tutto ciò ha portato ad un confronto fra gli associati di TTS Italia, le principali associazioni e con il mondo della domanda fin da dicembre 2025, con appuntamenti serrati nel successivo semestre, per giungere così ad una formalizzazione delle architetture, ad analizzare i casi studio notevoli per giungere ad un documento tecnico e a fornire le raccomandazioni riportate in questo documento, visti anche gli esiti di parallele attività anche istituzionali, quali ad esempio l'indagine conoscitiva "*Tecnologie digitali e l'IA per le infrastrutture italiane*" svolta dal Senato della Repubblica.

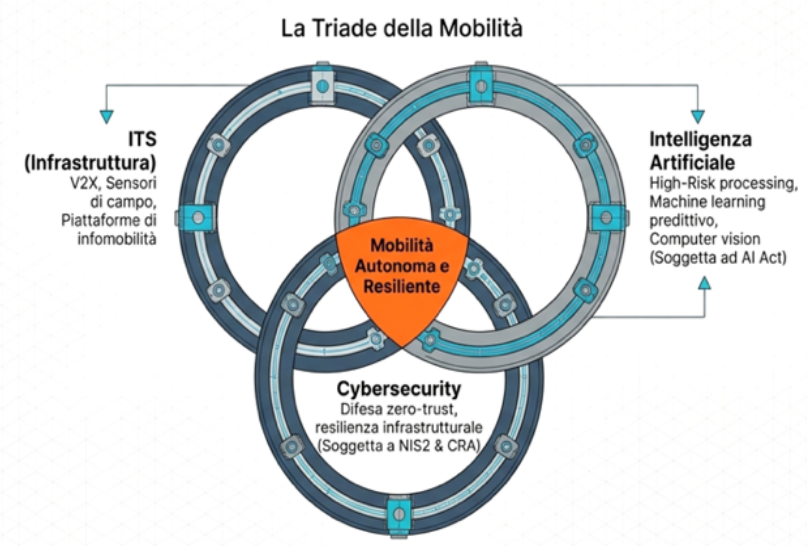
Evidenze

La mobilità sta complessivamente attraversando una trasformazione profonda grazie alla digitalizzazione, alla crescente interconnessione dei sistemi di trasporto e all'uso massivo di dati.

La prossima grande transizione tecnologica europea ed italiana vedrà dati, algoritmi e infrastrutture digitali combinarsi per rendere ogni viaggio più sicuro, pulito e inclusivo.

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.

Il veloce diffondersi dell'**AI** 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 Mobility as a Service all'anticipazione delle minacce cyber tramite "machine learning".



L'integrazione di queste tecnologie abiliterà nel futuro un ecosistema di mobilità più efficiente, sicuro, sostenibile e resiliente.

I dati delineano un mercato in forte accelerazione, dove la "Smart Mobility" è diventata una dorsale economica primaria.

Al contempo, la trasformazione digitale del settore mobilità espone l'intero ecosistema a nuove superfici d'attacco ed ogni componente infrastrutturale è un bersaglio. Un attacco in questo dominio non è un mero furto di dati, ma un evento fisico con potenziali vittime reali. Scenari di Rischio High-Impact vedono anche minacce da hardware vulnerabile nella supply chain.

Questa esplosione del valore digitale è, tuttavia, sotto assedio. I dati degli ultimi rapporti di settore indicano un'emergenza sistemica, con un **incremento del 48,7% degli attacchi nel 2025** rispetto all'anno precedente. Questo scenario conferma che il valore economico della mobilità connessa è direttamente proporzionale alla sua vulnerabilità e richiede una protezione dinamica e scalabile.

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.

Il tutto si inquadra in un complesso quadro regolatorio, i cui pilastri sono:

- La **Direttiva ITS 2023/2661/UE**, recepita in Italia con il Decreto del MIT del 26/01/2026 e che rende obbligatoria l'integrazione di servizi digitali sicuri e la disponibilità di dati interoperabili per la gestione stradale;
- La **NIS2**, recepita con il D.Lgs. 138/2024 e che inquadra la mobilità come infrastruttura critica, imponendo obblighi severi di gestione del rischio e notifica incidenti;
- L'**AI Act** che classifica i sistemi di trasporto ad "alto rischio";
- Le normative settoriali quali il **Cyber Resilience Act** e gli **standard tecnici.**

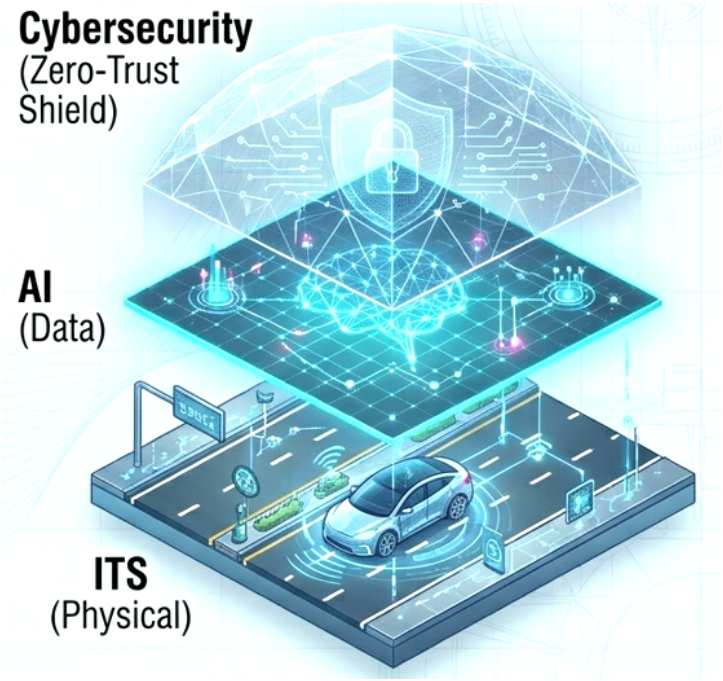
La Cybersecurity "tradizionale" non è quindi più sufficiente: serve un **approccio integrato AI + Cybersecurity**, basato su robustezza dei modelli AI, difesa da attacchi adversarial, protezione dei dati sensibili usati per addestramento, architetture "zero trust" (ossia basate sul principio "mai fidarsi, verificare sempre"), SOC potenziati con AI, compliance normativa (UN R155, ISO 21434, AI Act, NIS2) e l'adozione del paradigma "Compliance by Design".

Queste tecnologie non sono più solo sperimentali, ma stanno diventando parte integrante della mobilità urbana e interurbana.

Il futuro della mobilità dipende però dalla capacità di gestire queste crescenti complessità e di sviluppare ecosistemi resilienti. Pertanto, solo attraverso un approccio integrato, proattivo e standardizzato sarà possibile garantire sistemi di trasporto efficienti, resilienti e sicuri e che l'intelligenza dei nostri sistemi non diventi il loro punto di rottura, ma fondamento della sicurezza nazionale.

La collaborazione tra industria, istituzioni e ricerca diventa quindi essenziale per costruire ecosistemi di mobilità affidabili e sostenibili.

Emerge una forte convergenza verso alcuni nodi prioritari, quali la necessità di intervenire in modo selettivo e programmato sulle infrastrutture esistenti, di costruire un'infrastruttura pubblica del dato quale asset strategico per il futuro della mobilità e per rafforzare l'autonomia logistica del Paese.



In sintesi, **la convergenza tra ITS, AI e Cybersecurity rappresenta uno dei principali fattori abilitanti della mobilità del futuro**. In un contesto caratterizzato da crescente digitalizzazione, interconnessione e complessità, la sicurezza diventa un elemento essenziale per garantire affidabilità, continuità del servizio e tutela degli utenti. ITS, AI e Cybersecurity costituiscono un ecosistema indivisibile dove i dati diventano un asset strategico.

Il settore trasporti è diventato il quinto più attaccato a livello globale. L'emergere dell'AI generativa (GenAI) ha trasformato minacce teoriche in capacità offensive operative (malware polimorfi, deepfake, prompt injection).

L'Europa e l'Italia hanno definito un perimetro legale complesso (AI Act, NIS2, Data Act, Cyber Resilience Act) che impone obblighi di compliance rigorosi e responsabilità dirette per il management.

La transizione richiede non solo investimenti tecnologici, ma un'evoluzione culturale e organizzativa per colmare il "digital divide" e lo "skills gap" nelle Pubbliche Amministrazioni (PA) e nelle PMI.

Raccomandazioni strategiche

Quanto precede ha delineato le potenzialità trasformative delle tecnologie digitali, ma anche le criticità sistemiche che oggi ostacolano l'adozione diffusa e coordinata dell'innovazione nel settore della mobilità e come l'integrazione di AI e Cybersecurity sia il fattore critico per garantire sicurezza, affidabilità e resilienza della mobilità intelligente.

Le **raccomandazioni strategiche** per costruire un ecosistema di mobilità resiliente, risultato del confronto tra i principali stakeholder che hanno partecipato al GdL di TTS Italia sul tema sono riportate di seguito:

- *R1 – Adottare una governance architetturale integrata per ITS, AI e cybersecurity;*
- *R2 – Integrare i principi di Security by Design e Zero Trust lungo l'intero ciclo di vita;*
- *R3 – Promuovere l'integrazione tra AI e cybersecurity come fattore abilitante della resilienza;*
- *R4 – Rafforzare la governance dei dati, l'interoperabilità e l'uso di standard aperti", supportato da Mobility Data Platform nazionale interoperabile;*
- *R5 - Promuovere lo Sviluppo di AI Settoriale e Trustworthy della mobilità con marchio di "AI affidabile;*
- *R6 – Ecosistema integrato di logistica;*
- *R7 – Ecosistema digitale per il trasporto multimodale ed intermodale;*
- *R8 – Sviluppo della mobilità connessa ed autonoma con adeguamento della normativa;*
- *R9 – Investire su competenze, collaborazione, ambienti di sperimentazione controllata e team multi-genere e multidisciplinari;*
- *R10 – Integrare l'etica fin dalla progettazione (Ethics-by-Design) nei nuovi sistemi di AI critici nel settore dei trasporti;*
- *R11 – Garantire un controllo umano significativo e una chiara responsabilità;*
- *R12 – Riforma del Processo di Omologazione;*
- *R13 – Istituzione di SOC Potenziati dall'AI con Zero Trust e Cyber Threat Intelligence;*
- *R14 – Cultura diffusa della cybersicurezza negli ITS nelle Amministrazioni ed imprese;*
- *R15 – Incentivazioni economiche, per evitare ritardi strutturale delle imprese e PA.*

Costituiscono linee di azione fra loro interconnesse e che rappresentano un quadro strategico per guidare la trasformazione digitale del sistema infrastrutturale e logistico italiano.

Sono quindi concepite non come misure isolate, ma come strumenti operativi di una politica industriale e territoriale, fondata su sicurezza, innovazione, sostenibilità e competitività.

Chi è TTS Italia

TTS Italia è l'Associazione Nazionale della Telematica per i Trasporti e la Sicurezza fondata nel 1999 da un gruppo di organizzazioni pubbliche e private attive nel settore della smart mobility.

TTS Italia è un'associazione no profit e rappresenta il settore italiano della mobilità intelligente, riunendo i principali stakeholder pubblici e privati del comparto nazionale.

Attualmente TTS Italia annovera oltre 90 associati tra aziende del settore industriale, agenzie della mobilità, aziende di trasporto pubblico, operatori autostradali, Enti Locali, enti di ricerca e dipartimenti universitari.

La missione di TTS Italia è promuovere lo sviluppo e l'implementazione delle tecnologie per trasporti più sicuri, efficienti e sostenibili per tutte le modalità (strada, ferrovia, mare, aereo), anche fornendo un supporto tecnico agli organi istituzionali sia centrali che locali nella definizione delle politiche e delle strategie per il settore della smart mobility.

TTS Italia fa anche parte di un Network internazionale costituito dalle Associazioni Nazionali per la mobilità intelligente presenti nelle più importanti Nazioni europee e mondiali e rappresenta il relativo settore italiano nei principali eventi internazionali.

TTS ITALIA

Via Flaminia 388 – 00196 Roma
ttsitalia@ttsitalia.it
www.ttsitalia.it

Con il supporto di

GOLDEN SPONSOR

SILVER SPONSOR