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

AI e Cybersecurity per la mobilità di persone e merci

Giugno 2026

Executive Summary

Obiettivo del documento è di fornire Linee Guida per tutti gli associati e per gli Enti della Piattaforma degli Enti Locali di TTS Italia e approfondisce il ruolo dell'Intelligenza Artificiale (Artificial Intelligence - AI) nella mobilità moderna e le sue intersezioni con la cybersecurity ove con l'aumento di veicoli connessi, infrastrutture intelligenti e piattaforme digitali di trasporto, la superficie d'attacco cresce esponenzialmente.

Tale Documento è stato realizzato nell'ambito del Gruppo di Lavoro (GdL) "**AI e Cybersecurity nella Mobilità Intelligente**" di TTS Italia.

TTS Italia è l'Associazione Italiana della Telematica per i Trasporti e la Sicurezza che rappresenta il settore italiano degli **Intelligent Transport Systems (ITS)** e 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** e 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.

Il documento illustra le linee guida strategiche per l'integrazione tra AI, ITS e cybersecurity nel panorama della mobilità moderna.

Il percorso del GdL si è quindi concretizzato inizialmente nel comprendere le necessità di tale convergenza in un contesto estremamente mutevole con un confronto iniziale fra i soci interessati e le principali associazioni di stakeholder coinvolti a dicembre 2025 che ha prodotto un primo elenco dei contributi, poi concretizzatosi in un serrato piano di lavoro con appuntamenti mensili nel successivo semestre per giungere al presente documento.

Il testo approfondisce il quadro normativo europeo e nazionale, citando pilastri fondamentali come l'AI Act, la direttiva NIS2 e il Data Act per garantire la resilienza delle infrastrutture critiche.

Un ulteriore momento di confronto a fine marzo 2026 ha permesso di focalizzare le necessità del mondo della domanda e giungere ad una formalizzazione delle architetture. L'analisi evidenzia come la digitalizzazione dei trasporti aumenti esponenzialmente la superficie di attacco, rendendo necessari approcci di sicurezza basati sul principio della compliance by design. Attraverso l'esame di casi studio e tendenze di mercato, si sottolinea l'importanza di una governance dei dati rigorosa e di una difesa proattiva contro le minacce informatiche emergenti.

In sintesi, 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.

L'obiettivo finale è promuovere un ecosistema di trasporto che sia al contempo tecnologicamente avanzato, etico e sicuro per tutti gli utenti. Fornisce quindi raccomandazioni strategiche per garantire sistemi di mobilità resilienti e sicuri, rappresentate poi anche in forma di *Position Paper* nel corso dell'evento conclusivo dei lavori di giugno 2026.

Indice

1. Il GdL "AI e Cybersecurity per la mobilità di persone e merci": uno sguardo d'insieme

L'Italia ha recepito la Direttiva 2023/2661/UE del 22 novembre 2023 di aggiornamento della Direttiva ITS 2010/40/UE sulla diffusione degli Intelligent Transport Systems con il Decreto del 26 gennaio 2026, pubblicato il 18 febbraio 2026 in Gazzetta Ufficiale.

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

Al contempo, la trasformazione digitale del settore mobilità — con veicoli connessi, sistemi di guida assistita, flotte intelligenti, sharing mobility e infrastrutture Vehicle to Everything (V2X) — espone l'intero ecosistema a nuove superfici d'attacco. 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 mobilità sta quindi complessivamente attraversando una trasformazione profonda grazie alla digitalizzazione, alla crescente interconnessione dei sistemi di trasporto e all'uso massivo di dati. Tre pilastri risultano centrali: gli ITS, l'AI e la Cybersecurity

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. Tuttavia e come accennato, l'AI introduce nuove vulnerabilità: dati manipolabili, modelli attaccabili, sistemi decisionali sensibili.

La mobilità intelligente richiede un nuovo paradigma di cybersecurity. L'AI è sia un acceleratore di efficienza sia una nuova superficie di attacco. La cybersecurity "tradizionale" non è più sufficiente: serve un approccio integrato AI + cybersecurity, basato su robustezza dei modelli AI, difesa da attacchi "*adversarial*" [da agenti avversi], protezione dei dati sensibili usati per addestramento, architetture "zero trust", Security Operations Center (SOC) potenziati con AI, compliance normativa (UN R155, ISO 21434, AI Act, NIS2).

L'integrazione di queste tecnologie abiliterà sicuramente un ecosistema di mobilità più efficiente, sicuro, sostenibile e resiliente. I dati di mercato e i progetti reali mostrano che 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.

Obiettivo del Gruppo di Lavoro è stato quindi di effettuare una disamina delle principali opportunità e criticità, nonché formulare delle proposte e possibili raccomandazioni per le istituzioni per implementare una mobilità intelligente sicura, resiliente e conforme attraverso un documento da presentare in occasione dell'evento annuale di TTS Italia del giugno 2026.

2. Overview e fondamenti

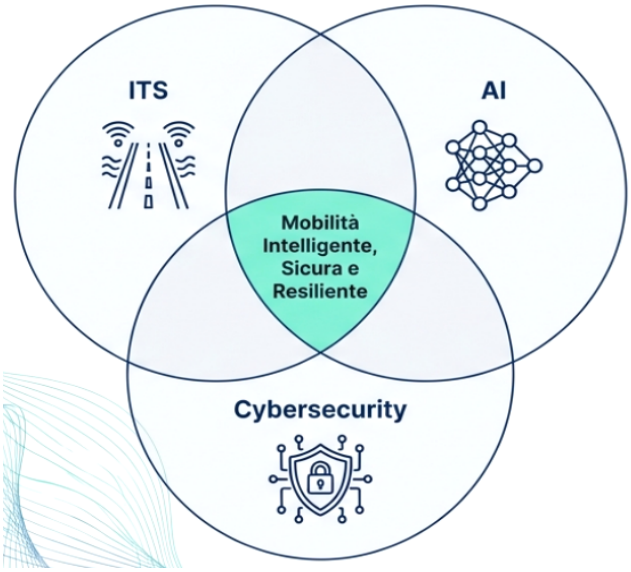
Come introdotto nel capitolo 1, la trasformazione digitale della mobilità si fonda su tre pilastri:

- ITS;
- AI;
- Cybersecurity.

La mobilità moderna è un ecosistema digitale complesso composto da veicoli connessi e autonomi, infrastrutture stradali intelligenti (ITS/RSU), comunicazioni 5G e V2X, piattaforme Mobility as a Service (MaaS) e sharing mobility, infrastrutture di ricarica smart e smart grid, algoritmi avanzati che prendono decisioni in millisecondi.

L'integrazione dell'AI nella mobilità sta trasformando radicalmente veicoli, infrastrutture, servizi digitali e sistemi energetici. Dai modelli di percezione per la guida autonoma alla predictive maintenance, dalle piattaforme MaaS all'anticipazione delle minacce cyber tramite "machine learning", l'AI è oggi un elemento critico per efficienza e sicurezza.

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



Peraltro l'AI aggiunge capacità fondamentali, ma nel contempo amplia drasticamente la superficie di attacco ed introduce nuove vulnerabilità: dati manipolabili, modelli attaccabili, sistemi decisionali sensibili.

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. Parallelamente, l'aumento della superficie di attacco richiede approcci di sicurezza "secure-by-design".

Il concetto di "secure-by-design" va approfondito, anche in riferimento ai relativi standard industriali (es. IEC 62443-4-1 e IEC 62443-4-2), per consentire di definire un approccio allo sviluppo di prodotti intrinsecamente sicuro.

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, compliance normativa (UN R155, ISO 21434, AI Act, NIS2).

Obiettivo del documento è quindi approfondire gli aspetti tecnici, operativi e normativi che guidano questa trasformazione.

2.1 I Sistemi Intelligenti di Trasporto (ITS)

Gli **ITS** svolgono un ruolo determinante per un uso più efficiente di infrastrutture, veicoli, piattaforme logistiche e per lo sviluppo sostenibile delle *smart cities*.

Nonostante la frammentarietà del nostro mercato, l'Italia è tra i leader europei nel settore degli ITS grazie a numerose aziende medio-piccole ad altissimo contenuto innovativo. Solo da qualche anno gli ITS sono stati considerati strategici per la gestione della mobilità a livello Europeo con l'emanazione della **Direttiva europea 2010/40/UE** sul "*Quadro generale per la diffusione dei sistemi di trasporto intelligenti nel settore del trasporto stradale e nelle interfacce con altri modi di trasporto*".

L'Italia ha recepito la Direttiva con l'Art.8 del Decreto-legge del 18 ottobre 2012 n. 179, e con il **Decreto del 1° febbraio 2013** del Ministero delle Infrastrutture e della Mobilità Sostenibili sulla "*Diffusione dei sistemi di trasporto intelligenti (ITS) in Italia*".

La Commissione europea ha, inoltre, pubblicato cinque **Regolamenti Delegati**, che integrano la **Direttiva 2010/40/UE** e che pertanto costituiscono norme comunitarie da rispettare nel momento in cui, come avvenuto, l'Italia ha recepito la Direttiva 2010/40/UE.

Con **Decreto del 26 gennaio 2026**, pubblicato il 18 febbraio 2026 in Gazzetta Ufficiale, l'Italia ha poi recepito la Direttiva 2023/2661/UE del 22 novembre 2023 di aggiornamento della Direttiva ITS 2010/40/UE.

Gli ITS sono sistemi di trasporto dotati di tecnologie digitali e connesse che consentono la raccolta, elaborazione e comunicazione di informazioni per ottimizzare la mobilità.

Gli ITS rappresentano l'infrastruttura digitale fondamentale per la mobilità moderna. Gli ITS combinano tecnologie di comunicazione, sensoristica, edge computing e piattaforme software per ottimizzare:

- Gestione del traffico in tempo reale;
- Sicurezza stradale tramite monitoraggio continuo;
- Mobilità multimodale e servizi MaaS.

Componenti principali sono:

- Sistemi di campo (rilevazione traffico, incidenti, condizioni atmosferiche, controllo accessi e parking, ecc);
- Sistemi di comunicazione V2X;
- Piattaforme di gestione centrale dei dati di mobilità;
- Sistemi di pagamento intelligenti (pedaggi dinamici, ticketing);
- Pannelli a messaggio variabile e servizi di infomobilità.

Gli **ITS** possono peraltro favorire l'integrazione di sistemi di trasporto, per la fornitura di dati sulla rete prioritaria urbana e per lo sviluppo di servizi innovativi di mobilità. Essi, infatti, rappresentano la declinazione dell'applicazione della tecnologia alla mobilità di merci e persone. Nel pieno della rivoluzione digitale attualmente in corso in tutti i settori industriali, anche la mobilità è diventata un campo di applicazione delle nuove tecnologie. In questo senso, la mobilità rappresenta per alcuni versi una sfida particolarmente interessante, data la natura intrinsecamente analogica del fenomeno.

Gli **ITS** sono infatti applicazioni avanzate che, senza essere dotate di intelligenza in senso proprio, mirano a fornire servizi innovativi ai diversi modi di trasporto e alla gestione del traffico e consentono agli utenti di essere meglio informati e di fare un uso più sicuro, maggiormente coordinato e più «intelligente» delle reti di trasporto.

Gli **ITS** integrano le telecomunicazioni, l'elettronica e le tecnologie dell'informazione con l'ingegneria dei trasporti al fine di pianificare, progettare, rendere operativi, sottoporre a manutenzione e gestire i sistemi di trasporto.

Occorre ricordare come gli **ITS** possono rappresentare uno strumento per l'attuazione di politiche di mobilità. In questo senso, gli ITS sono un elemento da includere nelle strategie delle città e nei programmi di investimento per raggiungere una città funzionale con una congestione e un impatto ambientale ridotti, una maggiore efficienza energetica e una maggiore sicurezza. Inoltre, gli **ITS** possono fornire accesso a dati che contribuiscono al miglioramento dello sviluppo sostenibile delle città.

Inoltre gli **ITS** richiedono investimenti molto ridotti rispetto a quelli infrastrutturali e con un tasso di ritorno molto più rapido, e che potrebbe portare i seguenti benefici:

La loro applicazione comporta una serie di benefici, fra cui:

- Riduzione della congestione ed aumento di capacità superiore al 10% a parità di infrastrutture;
- Miglioramento della sicurezza stradale e tempi di intervento più rapidi in caso di incidenti;
- Migliore qualità della vita con aumento della sicurezza, minori impatti ambientali e riduzione delle emissioni inquinanti per rendere le nostre città delle reali smart cities;
- Sviluppo di servizi per la mobilità sostenibile: pianificazione del trasporto pubblico più efficiente, mobilità elettrica, mobilità in condivisione d'uso (car pooling, car sharing, bike sharing), mobilità ciclabile.

2.1.1 Sviluppi futuri degli ITS e mercato di riferimento

La trasformazione digitale della mobilità in Europa è quindi guidata da una crescente domanda di ITS, veicoli connessi e soluzioni basate su AI, con un'attenzione sempre più stringente alla sicurezza informatica.

L'evoluzione della mobilità sta procedendo verso un ecosistema totalmente digitale, dove AI e connettività assumono un ruolo centrale. Tuttavia, questa transizione comporta rischi cyber sempre più sofisticati.

L'industria sta infatti convergendo verso una mobilità intelligente caratterizzata da:

- V2X: interazione con altri veicoli, infrastrutture, reti cellulari e cloud;
- Mobilità autonoma: algoritmi di percezione, *decision making* e controllo basati su AI;
- *Smart infrastructure*: semafori intelligenti, sistemi di monitoraggio del traffico, sensori ambientali;
- Fleet management automatizzato: ottimizzazione dei tragitti, anticipazione dei guasti, gestione predittiva.

I dati di mercato e i progetti reali mostrano che queste tecnologie non sono più solo sperimentali, ma stanno diventando parte integrante della mobilità urbana e interurbana.

Il mercato europeo degli ITS è stimato crescere da 7,90 miliardi di USD (2024) fino a 14,62 miliardi entro il 2033, con un Compound Annual Growth Rate (CAGR) del ~7,08% ed a livello globale, il mercato ITS potrebbe raggiungere 98,02 miliardi di USD entro il 2032, con un CAGR del 7,5%. (TTS Italia)

In Italia, il mercato della mobilità "smart" e della "connected car" ha un valore di 2,9 miliardi di euro nel 2023 (+17% rispetto al 2022) e le sole soluzioni Advanced Driver Assistance Systems (ADAS) (sistemi di assistenza alla guida) valgono 950 milioni € (+28 %) mentre la parte "smart mobility urbana" (sharing, parcheggi intelligenti etc.) 400 milioni € (+18 %).

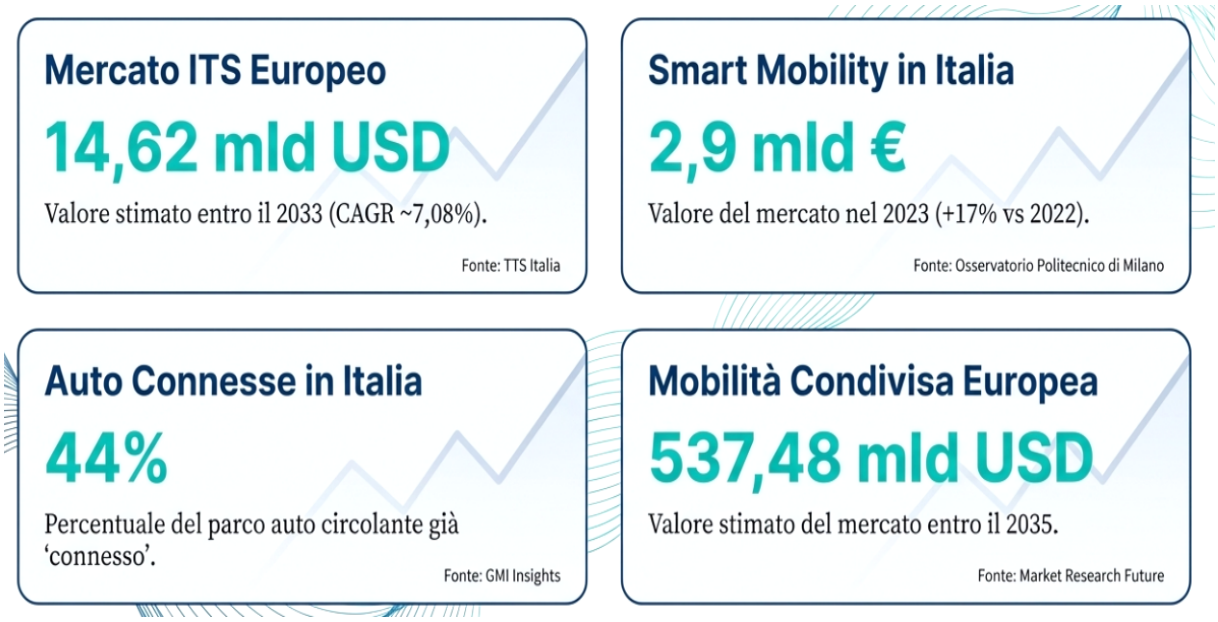
Per quanto riguarda la Mobilità Connessa (Connected Car), il 44% del parco auto circolante in Italia è "connesso" (auto con almeno una funzionalità smart) e, secondo GMI Insights, il mercato europeo delle auto connesse valeva circa 12,8 miliardi USD nel 2024, e dovrebbe arrivare a 24,8 miliardi USD entro il 2034 (CAGR ~8,3%) (Global Market Insights Inc.).

Secondo Oliver Wyman Forum, il mercato europeo della mobilità (in senso ampio: mobilità condivisa, veicoli intelligenti, ADAS) crescerà da 92 miliardi USD nel 2023 a 246 miliardi entro il 2035, con un tasso annuo atteso del 9%.

In particolare, la parte relativa agli ADAS in Europa è prevista crescere in modo esponenziale, con la domanda guidata da innovazioni tecnologiche.

Inoltre, il mercato europeo della mobilità condivisa ("*shared mobility*") è stimato raggiungere 383,84 miliardi di USD nel 2025 secondo Statista e, secondo Market Research Future il mercato shared mobility passerà da 173,02 miliardi USD nel 2025 a 537,48 miliardi entro il 2035, con un CAGR di circa il 12%.

L'Europa sta vedendo una forte adozione di veicoli elettrici Battery Electric Vehicle (BEV): secondo un report recente di Reuters, le vendite di BEV in Europa dovrebbero superare metà delle nuove immatricolazioni di veicoli leggeri entro il 2032.



Per quanto riguarda i veicoli autonomi, ci sono studi su scenari futuri per l'Europa che modellano differenti tassi di adozione dei veicoli automatizzati fino al 2050, con significativi benefici economici e sociali.

Sul fronte della sostenibilità, ricerche mostrano che la carica "smart" (*vehicle-to-grid*) può ridurre significativamente i costi del sistema energetico europeo, grazie all'integrazione dei veicoli elettrici con le reti di energia rinnovabile (fonte: arXiv).

In Italia ci sono già 21 iniziative di "Smart Road" (strade intelligenti) secondo l'Osservatorio del Politecnico di Milano e, sempre secondo il Politecnico, il 65% dei comuni italiani ha avviato almeno un progetto di smart mobility (2022-2024), ma solo il 29% sfrutta effettivamente i dati raccolti (fonte: Economyup).

Nel contesto del Piano Nazionale di Ripresa e Resilienza (PNRR), la *smart mobility* è una leva importante per l'innovazione urbana italiana: diversi progetti PNRR riguardano il traffico intelligente, la mobilità elettrica e la connettività nei trasporti.

Secondo l'Osservatorio *Connected Vehicle & Mobility* del Politecnico di Milano, nel 2024 in Italia erano 17,7 milioni le auto connesse, pari al 44% del parco auto nazionale. Entro il 2030, oltre il 70% del parco auto circolante in Europa sarà dotato di sistemi avanzati di connettività.

In generale, i numeri di mercato mostrano un forte potenziale di crescita per ITS e veicoli connessi in tutto il mondo. Le aziende e le amministrazioni che investono oggi in infrastrutture digitali e AI potranno ottenere ritorni significativi nei prossimi anni.

2.2 Lo scenario strategico dell'AI nella mobilità

I dati di mercato confermano la traiettoria di crescita del settore ITS, con investimenti che spaziano dalla smart road alla mobilità connessa. In questo ecosistema in espansione, l'AI assume un ruolo sempre più determinante.

L'AI non è più un'opzione, ma un imperativo strategico che pone il settore europeo dei trasporti di fronte a un bivio: da un lato, un potenziale di efficienza e sostenibilità senza precedenti; dall'altro, una serie di sfide infrastrutturali, etiche e competitive che ne determineranno il successo o il fallimento. Questa tecnologia sta ridisegnando le fondamenta della mobilità, con impatti diretti e misurabili sull'efficienza operativa, la sostenibilità ambientale e la competitività globale del continente. La capacità di analizzare dati in tempo reale, ottimizzare flussi complessi e automatizzare decisioni sta aprendo scenari senza precedenti per la gestione di persone e merci.

La centralità strategica di questo tema è stata confermata da iniziative di alto livello come il workshop "AI in Mobility and Transport", organizzato il 5 febbraio 2025 dalla Direzione Generale CNECT e dalla Direzione Generale MOVE della Commissione Europea ove è emersa la necessità di delineare una visione condivisa sul futuro dell'AI nella mobilità, identificando casi d'uso ad alto potenziale e affrontando le barriere che ne rallentano l'adozione.

Anche **l'indagine conoscitiva** dedicata all'**impiego delle tecnologie digitali e dell'AI nel settore delle infrastrutture**, lavoro promosso dall'8ª Commissione Senato della Repubblica e presentato il 23 aprile 2026 e che ha coinvolto istituzioni, università, centri di ricerca e operatori industriali, ha evidenziato come il digitale e l'AI siano ormai elementi imprescindibili per la progettazione, la gestione e la manutenzione delle infrastrutture strategiche del Paese.

Al tempo stesso, il quadro emerso mette in luce la necessità di accelerare sul fronte della trasformazione digitale, superando ritardi ancora presenti e rafforzando l'integrazione tra innovazione tecnologica e politiche pubbliche e propone alcune direttrici chiave per accompagnare questa trasformazione quali il potenziamento dei sistemi di monitoraggio e manutenzione predittiva, lo sviluppo di piattaforme integrate per la gestione dei dati e il rafforzamento delle competenze tecniche e digitali per costruire un ecosistema infrastrutturale più efficiente, sicuro e sostenibile, in grado di rispondere alle sfide della transizione digitale ed energetica.

Il messaggio chiave è che la trasformazione digitale delle infrastrutture non è più rinviabile. È necessario accelerare l'adozione di tecnologie innovative per colmare il divario esistente e garantire maggiore efficienza, sicurezza e competitività al sistema Paese.

L'AI permette infatti di trasformare i dati raccolti dagli ITS in azioni intelligenti, automatizzate e predittive e quindi consente agli ITS di evolvere da sistemi reattivi a sistemi predittivi e autonomi, con predizione del traffico basata su modelli Machine Learning (ML) addestrati su dati storici e real-time, riconoscimento eventi critici (incidenti, veicoli fermi, violazioni) tramite computer vision, gestione dinamica delle infrastrutture come semafori adattivi e pannelli Variable Message Sign (VMS) intelligenti.

Applicazioni chiave

A. Ottimizzazione del traffico

- Previsione della congestione tramite modelli di machine learning;
- Visualizzazione, nei pannelli VMS, dei tempi attesi di arrivo e percorrenza in real time (tenendo quindi conto delle eventuali congestioni);

- Regolazione dinamica dei cicli semaforici;
- Suggerimento di percorsi alternativi in tempo reale.

B. Trasporto autonomo

- Sistemi di percezione basati su computer vision;
- Riconoscimento pedoni, ostacoli e segnaletica;
- Pianificazione autonoma delle traiettorie.

C. Gestione della mobilità pubblica

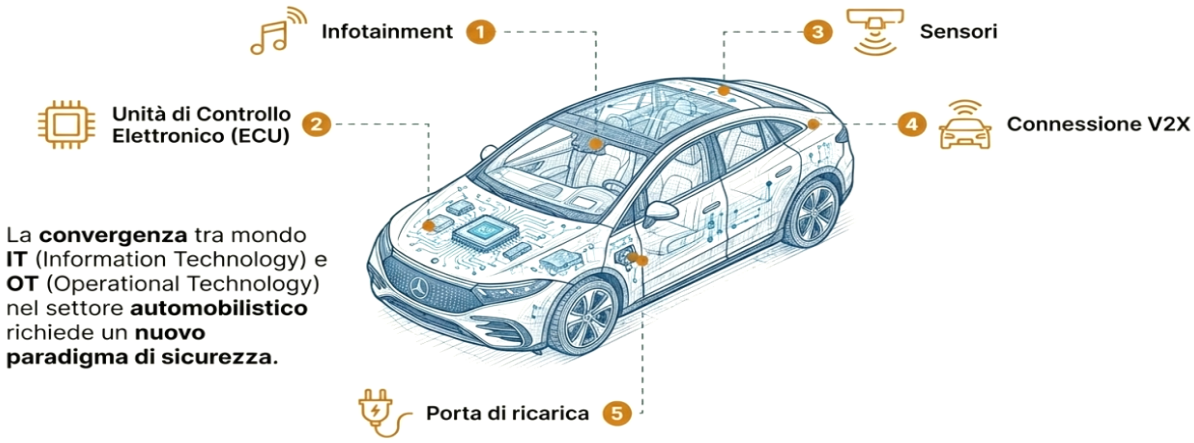
- Previsione della domanda;
- Ottimizzazione delle corse e delle frequenze;
- Allocazione dinamica delle risorse.

D. Manutenzione predittiva

- Monitoraggio continuo di veicoli e infrastrutture e dispositivi in essi integrati (es. semafori, pannelli VMS, sensori);
- Identificazione precoce di anomalie e guasti;
- Riduzione dei tempi di fermo e dei costi operativi.

Rischi

- Opacità decisionale;
- Vulnerabilità intrinseche dei modelli;
- Supply chain delle strutture di raccolta di dati (dataset e/o database).



In generale, l'uso dell'AI nei sistemi di traffico, ADAS e analisi dati sta diventando sempre più centrale per rendere la mobilità più predittiva e adattiva.

Con la diffusione di veicoli connessi e comunicazione V2X, la cybersecurity diventa critica — i dati di tali sistemi sono sensibili e vulnerabili, e servono politiche forti di protezione e standard (come PKI [Public Key Infrastructure, "infrastruttura a "chiave pubblica], crittografia, autenticazione).

2.2.1 Il potenziale trasformativo dell'AI: applicazioni concrete e benefici tangibili

Nell'analisi che segue, ci si concentrerà su applicazioni pratiche dell'AI che illustrano i benefici quantificabili che la sua adozione sta già portando al settore.

L'AI sta superando la fase di "hype" per radicarsi in applicazioni pratiche che producono valore tangibile nel settore dei trasporti e della logistica. L'enfasi si è spostata dalla speculazione tecnologica alla risoluzione di problemi concreti, con un focus sull'ottimizzazione di processi esistenti e la creazione di nuovi servizi più efficienti, sicuri e sostenibili.

Di seguito si esaminano le principali aree di applicazione in cui l'AI sta già dimostrando il suo potenziale trasformativo, analizzando i benefici specifici che derivano dal suo impiego.

Ottimizzazione dell'efficienza operativa e della logistica

- L'impatto più immediato dell'AI si manifesta nel **drastico miglioramento dell'efficienza operativa**. Sfruttando la capacità di elaborare enormi volumi di dati e di identificare pattern complessi, le aziende del settore possono ottimizzare l'intera catena del valore, dalla pianificazione strategica all'esecuzione quotidiana;
- **Ottimizzazione della logistica**: i sistemi di AI consentono di monitorare, prevedere e pianificare le operazioni in modo proattivo. Un esempio concreto è l'ottimizzazione del carico dei camion, dove gli algoritmi calcolano la disposizione ottimale delle merci per massimizzare lo spazio utilizzato, riducendo il numero di viaggi, i costi e le emissioni di CO2;
- **Ottimizzazione dinamica dei percorsi**: le aziende di corrieri stanno utilizzando l'AI generativa (GenAI) per analizzare in tempo reale variabili come traffico, condizioni meteorologiche e priorità di consegna. Questo permette di ricalcolare dinamicamente i percorsi, ottenendo una riduzione dei costi di consegna fino al 50%, con un conseguente abbattimento del consumo di carburante e dei ritardi;
- **Manutenzione predittiva**: sfruttando modelli LLM (Large Language Models) e dati provenienti da sensori, è possibile prevedere con grande accuratezza le necessità di manutenzione di veicoli e infrastrutture. Questo approccio previene guasti improvvisi, riduce i tempi di fermo e aumenta significativamente la sicurezza complessiva del sistema;
- **Automazione dei processi amministrativi**: la GenAI sta semplificando drasticamente i flussi di lavoro amministrativi. Attività come la gestione documentale, l'inserimento dati, la classificazione di contratti legali e i controlli di conformità vengono automatizzate, liberando risorse umane per compiti a maggior valore strategico;
- **Sistemi di pricing dinamici**: nel campo della logistica, l'AI sta rivoluzionando le strategie di prezzo. Attraverso la previsione accurata della domanda e l'analisi delle capacità disponibili, i sistemi possono aggiustare le tariffe in modo automatico e dinamico, ottimizzando i ricavi e la saturazione dei mezzi.

Promozione della sostenibilità e della transizione energetica

L'AI emerge come uno strumento cruciale per accelerare la transizione energetica e promuovere la sostenibilità, un obiettivo prioritario per un settore che ha un impatto ambientale significativo. A livello Europeo, i trasporti sono responsabili del 25% delle emissioni totali di gas serra, e il 70% della CO2 prodotta in ambito urbano proviene dai veicoli stradali.

Per affrontare questa sfida, le politiche di trasporto sostenibile si basano sul framework "Avoid-Shift-Improve":

* *Avoid*: ridurre la necessità di spostamenti motorizzati.

* *Shift*: incoraggiare il passaggio a modalità di trasporto più ecologiche (trasporto pubblico, ciclismo).

* *Improve*: migliorare l'efficienza energetica dei mezzi di trasporto esistenti.

L'AI contribuisce in modo concreto a questo paradigma. Il caso di gestori specializzati nella gestione di flotte aziendali, dimostra come l'applicazione di soluzioni intelligenti possa portare a risultati misurabili:

- Ottimizzazione delle strategie di elettrificazione della flotta che, in scenari ideali, può portare a una riduzione del 100% delle emissioni operative dirette (*tailpipe emissions*), con un risparmio medio documentato di 600 tonnellate di CO2 all'anno per una flotta di medie dimensioni;
- Gestione efficace della multimodalità, suggerendo agli utenti le combinazioni di trasporto più sostenibili;
- Supporto alla gestione di flotte a basse o zero emissioni e semplificazione del reporting *Environmental, Social, and Governance* (ESG), sempre più richiesto a livello normativo.

Miglioramento della sicurezza stradale

Il potenziale più dirompente dell'IA risiede nella sua capacità di migliorare radicalmente la sicurezza stradale. La stragrande maggioranza degli incidenti è, infatti, legata a fattori umani. Secondo i dati della National Highway Traffic Safety Administration (NHTSA) statunitense, una percentuale tra il 94% e il 96% degli incidenti stradali è causata, direttamente o indirettamente, dall'errore umano.

L'automazione della guida, guidata dall'AI, promette di mitigare drasticamente questo fattore di rischio.

Le analisi condotte su flotte di veicoli a guida completamente autonoma (rider-only) indicano già risultati impressionanti, con riduzioni dei tassi di incidente nell'ordine dell'80-90% in contesti urbani rispetto ai benchmark umani, seppur con variazioni sensibili per città e tipologia di sinistro. Questi dati, se confermati su larga scala, trasformano la discussione da puramente tecnologica a etica. Si delinea un vero e proprio "imperativo etico" a favore della diffusione di sistemi autonomi, una volta che questi dimostrino in modo inequivocabile di raggiungere prestazioni di sicurezza almeno equivalenti, se non superiori, a quelle di un conducente umano medio.

Tecnologie abilitanti: Digital Twin e gestione intelligente

Due concetti tecnologici chiave stanno abilitando l'applicazione avanzata dell'AI nel settore: l'Intelligent Digital Twin e l'Intelligent Digital Management:

- *Intelligent Digital Twin*: è una replica virtuale e dinamica di un processo, prodotto o sistema fisico (es. una catena di approvvigionamento, un veicolo). Sfruttando dati storici e in tempo reale, l'AI può simulare scenari futuri, prevedere colli di bottiglia, ottimizzare operazioni e testare strategie in un ambiente virtuale privo di rischi prima dell'implementazione nel mondo reale;
- *Intelligent Digital Management*: si configura come un "assistente digitale intelligente" che funge da punto di controllo centrale. Integra dati da fonti multiple, ne garantisce la qualità e utilizza l'AI per fornire informazioni e valutazioni precise, automatizzare compiti ripetitivi e supportare il processo decisionale umano attraverso interazioni intuitive.

La tabella seguente sintetizza i principali benefici e le sfide associate a queste tecnologie.

Tecnologia	Benefici	Rischi e sfide
Intelligent Digital Twin	Efficienza operativa migliorata Manutenzione predittiva Decision-making basato sui dati Maggiore agilità e flessibilità Riduzione dei costi	Costi di implementazione elevati Sicurezza e privacy dei dati Complessità di integrazione con sistemi esistenti Dipendenza dalla qualità dei dati di input Divario di competenze (Skill gaps)
Intelligent Digital Management	Automazione di compiti e processi Decision-making potenziato Tracciabilità in tempo reale Miglioramento del servizio clienti Maggiore trasparenza della supply chain	Dipendenza tecnologica e affidabilità dei sistemi Conformità normativa (es. AI Act) Sfide di integrazione con software esistenti Necessità di backup per processi manuali

L'implementazione di queste potenti tecnologie e il pieno sfruttamento dei benefici descritti dipendono, tuttavia, da fondamenta solide. Senza un accesso a dati di qualità, infrastrutture adeguate e competenze specializzate, il potenziale dell'AI rischia di rimanere un'aspirazione.

2.3 Cybersecurity nella mobilità connessa: i nuovi rischi del mondo in movimento

I benefici dell'AI nella mobilità — dall'ottimizzazione logistica alla sicurezza stradale — sono accompagnati da una corrispondente espansione della superficie di attacco, che impone un'analisi specifica dei rischi cyber nel settore. Infatti se, da una parte, è l'incessante evoluzione delle moderne tecnologie a rendere più conveniente la "migrazione" verso il digitale, dall'altra, solo la resilienza e la sicurezza delle reti e dei sistemi su cui tali servizi si basano possono garantire, nell'immediato, la sicurezza per la nostra comunità e, in prospettiva, lo sviluppo economico e il benessere dello Stato.

In particolare, la mobilità sta vivendo una rivoluzione. Non parliamo più solo di automobili e strade, ma di un ecosistema digitale complesso e interconnesso, dove veicoli, infrastrutture e servizi comunicano costantemente tra loro. Ogni elemento di questo sistema, che un tempo era puramente meccanico, è oggi un dispositivo intelligente che genera, scambia e analizza dati per rendere i nostri spostamenti più efficienti, sicuri e sostenibili.

Questo nuovo mondo in movimento è composto da diversi elementi chiave:

- **Veicoli connessi e autonomi**: automobili, bus e camion dotati di ADAS che dialogano con l'ambiente circostante;
- **Infrastrutture stradali intelligenti:** semafori, pannelli informativi e sensori stradali che gestiscono il traffico in tempo reale attraverso comunicazioni V2X;
- **Servizi digitali**: piattaforme che integrano diversi mezzi di trasporto (MaaS) e servizi di condivisione (sharing mobility);
- **Infrastrutture per la mobilità elettrica**: colonnine di ricarica intelligenti e reti elettriche (smart grid) che gestiscono l'energia in modo ottimizzato.

L'enorme vantaggio di questa digitalizzazione porta con sé una sfida altrettanto grande: la sicurezza. Nel gergo della cybersecurity, si parla di "superficie d'attacco", ovvero l'insieme di tutti i punti attraverso cui un sistema può essere violato. Con la mobilità connessa, questa superficie si è ampliata a dismisura. Ogni veicolo, ogni semaforo, ogni app sul nostro smartphone è diventata una potenziale porta d'ingresso per una minaccia informatica.

In questo settore, la cybersecurity non è più un problema che riguarda solo la protezione dei dati o la privacy. Un attacco informatico a un'auto in movimento o a un sistema di gestione del traffico può avere un "grave impatto sulla sicurezza stradale", come sottolinea la Direttiva Europea sugli ITS. Le conseguenze possono essere fisiche e immediate, mettendo a rischio la vita delle persone.

Gli ITS, essendo altamente distribuiti e connessi, presentano vulnerabilità specifiche, che possono andare dalla compromissione dei sensori stradali (telecamere, radar, LPR) alla manipolazione delle comunicazioni tra centrali operative e veicoli, agli attacchi ai sistemi di gestione del traffico, all'inserimento di dati falsi per alterare decisioni basate su AI (data injection) ed attacchi a infrastrutture edge responsabili di elaborazione locale.

L'aumento della connettività introduce nuove superfici di attacco che possono compromettere veicoli (auto, bus, treni), infrastrutture ITS, centri di controllo, servizi di pagamento e reti V2X.

La sicurezza cyber è essenziale per:

- Proteggere la sicurezza fisica degli utenti, evitando incidenti causati da manipolazioni digitali;
- Preservare i dati sensibili raccolti da veicoli e infrastrutture;
- Garantire continuità del servizio in contesti critici come trasporto pubblico, logistica e mobilità urbana;
- Mitigare attacchi su larga scala, che potrebbero compromettere intere reti di trasporto.

Come anche indicato nella "Strategia Nazionale di Cybersicurezza 2022-26" emessa dall'ACN (Agenzia per la Cybersicurezza Nazionale – vedi https://www.acn.gov.it/portale/strategia-nazionale-di-cybersicurezza), a tale realtà occorre far fronte, agendo secondo un approccio che includa l'adozione di misure di prevenzione e mitigazione del rischio volte a innalzare la resilienza delle infrastrutture digitali. Queste ultime non includono soltanto reti, sistemi e dati, ma anche, e soprattutto, utenti, la cui consapevolezza – siano essi attori istituzionali, imprese private o cittadini – va alimentata attraverso una diffusa cultura della Cybersicurezza.

Per proteggere questo nuovo ecosistema, è quindi fondamentale comprendere quali sono, concretamente, le minacce che dobbiamo affrontare.

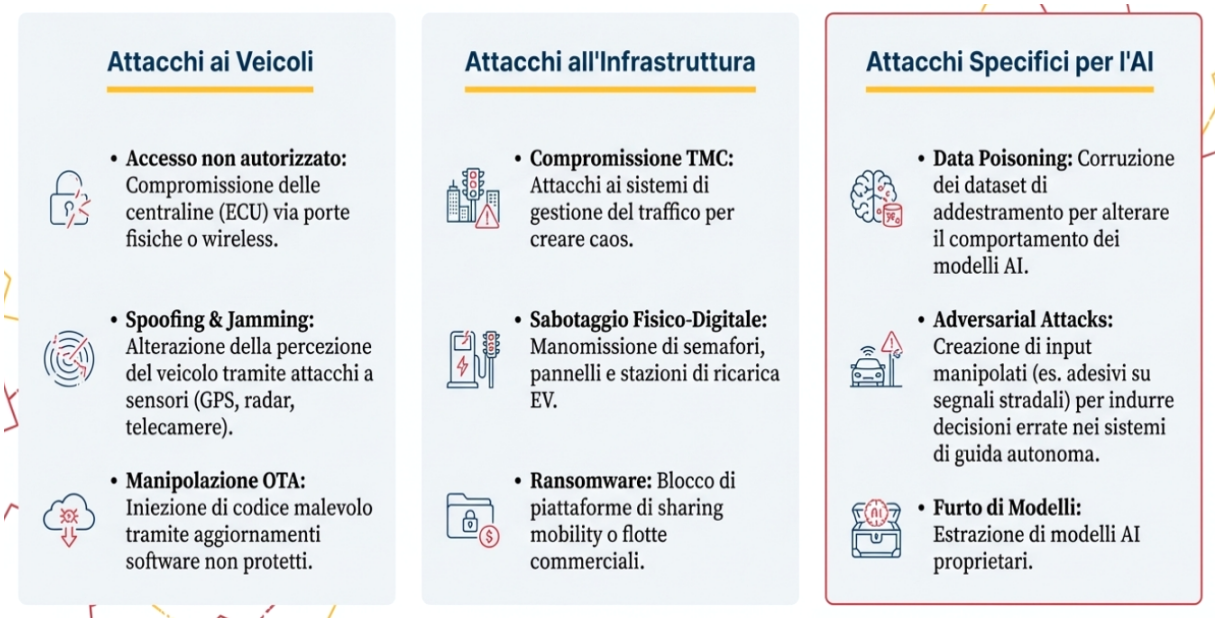
2.3.1 Il panorama delle minacce: anatomia di un cyber-attacco alla mobilità

La pressione cyber sul comparto è cresciuta in modo netto, con impatti economici rilevanti e un peso crescente della supply chain, soprattutto nel dominio stradale.

D'altro canto, l'AI è ormai uno strumento anche per l'offensiva: social engineering più credibile, deepfake, frodi basate su identità sintetiche. La stessa fonte che discute opportunità e rischi dell'AI nei trasporti richiama un caso di frode con videochiamata deepfake e sottolinea come, in infrastrutture critiche, gli effetti possano propagarsi a cascata tra sistemi interconnessi. Proteggere l'AI, in questo scenario, significa mettere sotto controllo una classe di rischi che non sempre si manifesta con un guasto evidente. La criticità sta spesso nella discrepanza tra ciò che il modello dovrebbe fare e ciò che finisce per fare quando l'input è degradato, manipolato o semplicemente diverso da quello atteso.

Nella pratica operativa, gli incidenti più onerosi seguono quattro traiettorie ricorrenti: input alterati che generano decisioni errate senza produrre errori applicativi; attacchi adattivi che aggirano difese dimensionate su test poco realistici; drift e input fuori dominio che erodono progressivamente accuratezza e affidabilità; ri-addestramenti e aggiornamenti che, se non governati, diventano un vettore di data poisoning. Il trasporto, inoltre, è esposto a un'ulteriore vulnerabilità strutturale: l'uso estensivo di segnalazioni e feedback utente provenienti da app, portali, contact center e social, spesso impiegati per addestrare o calibrare modelli NLP e sistemi di scoring legati a qualità del servizio, rilevazione disservizi e prioritizzazione interventi. In questa porzione della catena, la disinformazione non resta un tema reputazionale: diventa un fattore tecnico perché incide sui dati e può consolidarsi nel comportamento del modello.

Le minacce informatiche nel mondo della mobilità possono essere suddivise in base al bersaglio dell'attacco: il veicolo, l'infrastruttura che lo circonda o i servizi digitali che utilizziamo per spostarci. Considerazioni vanno fatte anche per attacchi a componenti dei sistemi stessi.



Attacchi al veicolo: quando l'auto non è più sicura

Un'auto moderna è un computer su ruote, con decine di centraline e reti interne. Questo la rende un bersaglio complesso e vulnerabile. Un esempio emblematico che ha reso tangibile questa minaccia è stato il famoso *hack di* una Jeep Cherokee nel 2015, in cui dei ricercatori hanno dimostrato di poter prendere il controllo remoto dello sterzo, dei freni e della trasmissione del veicolo mentre era in movimento, mostrando al mondo intero la criticità di queste nuove vulnerabilità.

Tipo di Attacco	Descrizione e rischio principale
Compromissione delle reti interne	Un hacker può accedere alla rete interna del veicolo (come la rete CAN) per inviare comandi falsi, prendendo il controllo di sterzo, freni o acceleratore. **Rischio:** perdita totale del controllo del veicolo da parte del conducente.
Manipolazione dei sensori (Spoofing)	Vengono inviati segnali falsi ai sensori del veicolo (GPS, radar, lidar). Questo può "ingannare" gli ADAS, causando frenate improvvise, accelerazioni inaspettate o manovre pericolose. **Rischio:** il veicolo reagisce a pericoli inesistenti o ignora quelli reali, provocando incidenti.
Attacchi al software di bordo	Viene iniettato un firmware (il software che fa funzionare l'hardware) malevolo, ad esempio durante un aggiornamento software non sicuro. **Rischio:** sabotaggio delle funzioni del veicolo o furto di dati sensibili (come la posizione o i dati biometrici del guidatore).

Attacchi all'infrastruttura: paralizzare il traffico

Le infrastrutture stradali intelligenti sono il "sistema nervoso" delle nostre città. Un attacco a questi sistemi può avere effetti a catena devastanti.

1. ***Attacchi ai sistemi di controllo del traffico:***
   - **Minaccia**: un attacco *ransomware* (a scopo di ottenere un riscatto) può bloccare il centro di controllo del traffico di una città, oppure un hacker può prendere il controllo remoto dei semafori, impostandoli

tutti su verde o su rosso con manipolazione dei dati in tempo reale. Ad esempio un attacco hacker che genera false informazioni sulla circolazione per condizionarla, ad esempio creare ingorghi o semplicemente criticità alla circolazione;

- **Impatto**: caos totale, ingorghi paralizzanti e aumento esponenziale del rischio di incidenti agli incroci.

2. Attacchi alle comunicazioni V2X:

- **Minaccia**: le comunicazioni tra veicoli e infrastrutture possono essere disturbate (*jamming*) o falsificate (*spoofing*). Un attaccante potrebbe inviare messaggi V2X falsi, come un avviso di "incidente imminente" o "strada libera";
- **Impatto**: i veicoli potrebbero frenare bruscamente senza motivo o ignorare un pericolo reale, causando collisioni. Questo è particolarmente critico perché i veicoli autonomi e cooperativi si basano sull'integrità di questi messaggi per prendere decisioni in frazioni di secondo su frenate, accelerazioni o cambi di corsia.

Attacchi ai servizi digitali: furto di dati e frodi

Le piattaforme MaaS e i servizi di car, bike o scooter sharing gestiscono un'enorme quantità di dati personali e finanziari, rendendoli un bersaglio molto appetibile per i criminali informatici. I rischi più comuni includono:

- Furto di credenziali e identità digitali degli utenti per accedere ai loro account;
- Abuso delle interfacce di programmazione (Application Programming Interface – API) per manipolare prenotazioni, rubare veicoli o commettere frodi sui pagamenti;
- Attacchi ransomware contro i sistemi gestionali delle aziende di trasporto per bloccarne le operazioni e chiedere un riscatto.

In questo scenario già complesso, un nuovo fattore sta cambiando le regole del gioco: l'AI. Il 2025 segna infatti l'emergere delle prime applicazioni offensive dell'AI, utilizzata per automatizzare il phishing, la ricerca di vulnerabilità e lo sviluppo di malware adattivi, aumentando ulteriormente la difficoltà di rilevamento e risposta.

Attacchi tramite parti software/hardware

Va infine considerata la minaccia geopolitica, da parte di entità statali, o legate a stati, che hanno il controllo o influenzano lo sviluppo stesso dell'hardware e del software, che così sono exploitable-by-design. Contro questo tipo di minacce la certificazione rispetto a standard non serve, perché le funzionalità di exploit non sono dichiarate, e spesso anche difficili da evidenziare in quanto implementate in firmware o addirittura cablate in hardware.

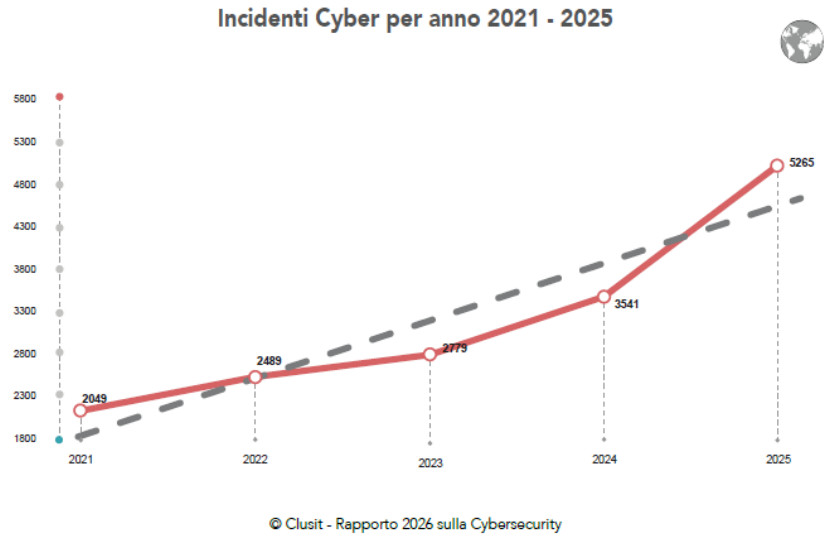
Anche queste funzionalità possono essere sfruttate da gruppi criminali una volta ne fossero venuti a conoscenza (il caso di alcune backdoor "legittime" che sono state rivelate in seguito a data theft è di pochi mesi fa).

E' quindi necessario pensare alla necessaria riforma del processo di omologazione dei veicoli e delle loro parti hardware e software per il via libera alla commercializzazione in Europa, tema molto sensibile e facilmente aggirabile soprattutto per la mancanza di uno standard unico e per buchi normativi oggi esistenti, ad esempio la mancanza di rinnovo dell'omologazione per gli aggiornamenti non solo software, quale il cambiamento di un chip in una successiva serie di un componente.

2.4 Andamento degli attacchi Cyber ai servizi di mobilità

Gli attacchi cyber sono in continua crescita, come dimostrato dai grafici seguenti di fonte CLUSIT – Rapporto 2026 sulla Cybersecurity, reperibile su https://clusit.it/rapporto-clusit/.

Nel periodo in esame, tra gennaio 2021 e dicembre 2025, sono stati censiti a livello globale un totale di 16.123 incidenti, distribuiti come mostrato nella figura successiva. Nel solo ultimo anno si sono registrati 5.265 incidenti, quota che rappresenta non solo il maggior numero registrato finora in termini assoluti, ma anche un incredibile aumento del 48,7% rispetto all'anno precedente.



Tale trend è confermato anche dal "Tinexta Cyber Threat Landscape 2025" di fine gennaio 2026 (https://www.tinextacyber.com/tinexta-cyber-threat-landscape-2025/) in cui si è evidenziato come nel 2025 il panorama delle minacce informatiche abbia raggiunto un nuovo livello di complessità, segnato dall'intensificarsi degli attacchi alla supply chain, dall'aumento dei data breach su larga scala e dal consolidamento di modelli criminali altamente strutturati basati su ransomware, infostealer e malware avanzati.

Accanto alla criminalità orientata alla monetizzazione del dato, continuano a operare attori nation-state e gruppi hacktivisti, alimentati da tensioni geopolitiche e capaci di generare impatti significativi su infrastrutture critiche, istituzioni e aziende strategiche.

In Italia, queste dinamiche si riflettono in un incremento degli attacchi verso la Pubblica Amministrazione (PA), i provider cloud e gli ecosistemi digitali complessi, con particolare evidenza sul fronte dei data breach e delle compromissioni lungo la filiera tecnologica. Allo stesso tempo, la convergenza tra gruppi criminali e la nascita di nuove alleanze operative hanno rafforzato la capacità offensiva dei Threat Actor, rendendo imprescindibili strategie di difesa proattive, cooperazione tra stakeholder e adeguamento ai nuovi quadri normativi.

Infatti il rapporto IBM X-Force Threat Intelligence Index 2025 evidenzia come a livello globale il settore trasporti sia salito al 5° posto tra i più attaccati nel 2024 (7% degli incidenti globali), rispetto all'8° posto dell'anno precedente. Il 67% degli attacchi ha preso di mira il furto di dati, il 33% ha coinvolto estorsione/ransomware. Poi il 70% di tutti i cyberattacchi nel 2024 ha colpito settori di infrastruttura critica (manifatturiero, energia, trasporti, finanza, sanità).

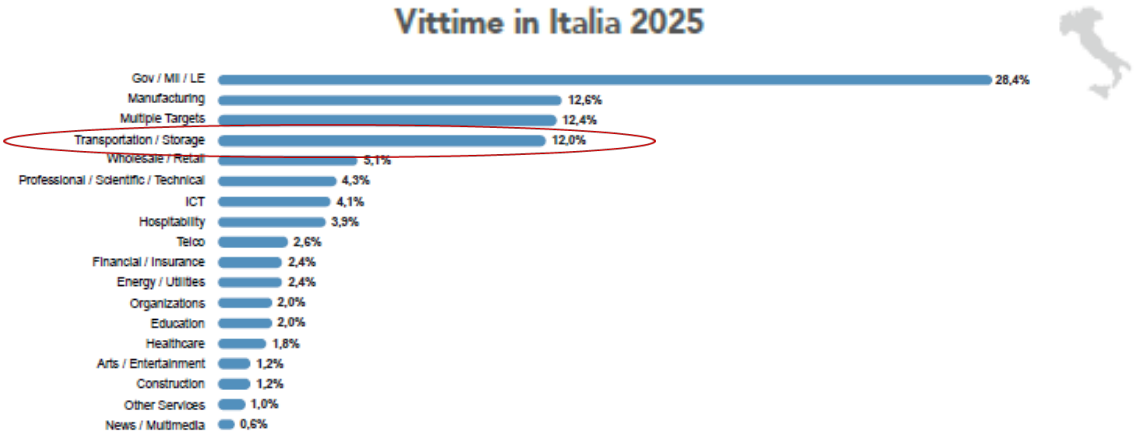
Il rapporto ENISA Threat Landscape 2025 indica come il settore trasporti è il 2° più colpito dopo la PA (11% degli incidenti). Incidenti notevoli nel 2025 hanno colpito sistemi di bigliettazione in Italia, Germania e Spagna.

Il Rapporto CLUSIT 2026 indica come la quota globale ascrivibile ai trasporti e mobilità sia pari al 3,7% in crescita importante dal 2,8% dell'anno precedente e rappresenta una crescente minaccia al settore.

© Clusit - Rapporto 2026 sulla Cybersecurity

L'analisi degli **incidenti in Italia** mostra che tra il 2021 e il 2025 il campione ha incluso 1432 incidenti noti di particolare gravità che hanno preso di mira realtà italiane. Di questi, ben 507, ovvero circa il 35% del totale, sono avvenuti nell'ultimo anno in esame. Nel 2025 l'aumento è pari al 42%, di poco inferiore al tasso di crescita globale che supera il 48%.

Il panorama degli incidenti, valutato attraverso la tipologia degli attaccanti, conferma quanto rilevato negli ultimi anni. In Italia sono principalmente attive due tipologie di attaccanti: i **Cybercriminali** e gli **Hacktivist**. L'Italia appare particolarmente vulnerabile ad incidenti di tipologia Hacktivism, che, sebbene spesso generino conseguenze



© Clusit - Rapporto 2026 sulla Cybersecurity

non particolarmente rilevanti poiché messi in atto con finalità puramente dimostrativa, vanno a segno e generano grande attenzione da parte di testate e media.

Il rapporto CLUSIT evidenzia come la distribuzione delle **vittime per categoria** mostri che nel 2025 e dopo due anni, al primo posto torna il settore governativo (Gov/Mil/LE) con oltre il 28% degli incidenti (+12 p.p.). A una discreta distanza, seguono rispettivamente il comparto Manufacturing, che resta saldamente in seconda posizione con un 12,6% degli incidenti del campione, e la categoria Multiple Targets al 12,4% (entrambe circa -4 p.p. rispetto all'anno precedente).

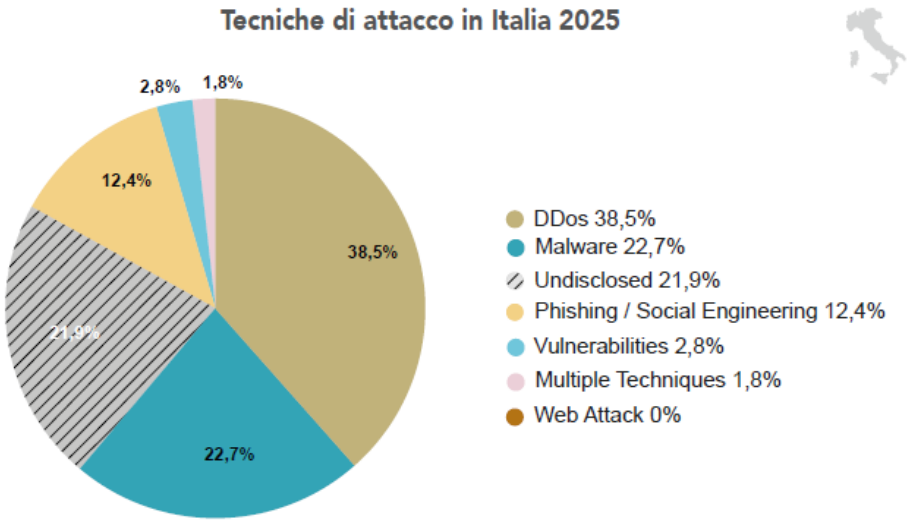
Sale di una posizione il settore **Transportation/Storage**, attestandosi al quarto posto con il 12% con un'impennata del 134,6% passando da **26 incidenti del 2024 a 61 del 2025.**

Rispetto alla classifica globale, si rilevano alcuni elementi in linea e altri che costituiscono una peculiarità italiana. Per esempio, il posizionamento elevato di Gov/Mil/LE nella classifica locale (che a livello mondo occupa la seconda posizione) è coerente, sebbene non con un differenziale rispetto alle posizioni successive così elevato come accade nel nostro Paese.

Viceversa il Financial/insurance (decimo in Italia) che a livello globale è invece sesto: questo sembra dimostrare che gli interventi derivanti dalla recente legislazione europea (i.e. Regolamento DORA in primis, che è ovviamente adottato anche in Italia) hanno contribuito efficacemente a rafforzare la capacità di difesa del settore.

Il fatto che **Transportation/Storage** dal 2022 a oggi abbia compiuto un salto rilevantissimo nel numero degli incidenti, salendo rapidamente ai primi posti della classifica, può essere ricondotto alla **volontà degli attaccanti di mettere in crisi interi settori dipendenti dalle filiere di fornitori di trasporti e logistica, nonché di generare eventi di portata elevata su più filiere di mercato contemporaneamente, limitando la loro capacità di assicurare approvvigionamenti e distribuzione degli stessi**. Ciò è verificabile dal fatto che il settore ha subito un'impennata di attacchi di matrice attivista con tecniche DDOS, nonché violazioni ad alcuni soggetti della supply-chain che hanno determinato conseguenze trasversali su più organizzazioni di questo ambito.

CLUSIT nota come in generale, la distribuzione delle tecniche di attacco mostra che il *malware* e il Distribuited Denial of Service **(DDoS**) si invertono in termini di posizione e percentuali. Il malware scende al 23% circa (dal 38% del 2024) mentre gli incidenti DDoS raggiungono il 38,5%, partendo dal 21% del 2024. Questo è coerente con l'aumento notevolissimo degli incidenti subiti dalla pubblica amministrazione (Gov/Mil/LE) e altrettanto coerente con l'impennata di incidenti di tipologia Hacktivism, in quanto spesso esiste una correlazione tra i due fenomeni. Il DDoS è infatti uno degli strumenti favoriti e più utilizzati negli attacchi dimostrativi per la sua semplicità, per l'impatto mediatico che può generare e per il valore "simbolico" (rappresenta, a suo modo, una forma di "sit-in" digitale). Una maggiore disamina degli attacchi nel caso trasporti è riportata nel capitolo 4.



Il rapporto CLUSIT indica quindi che la capacità di determinare, anticipare e gestire le evoluzioni legate alle minacce esogene, oltre che al contesto interno dell'organizzazione, è ormai fondamentale in particolare per la PA. Il risk management non può più essere "uno strumento per pochi esperti".

Il General Data Protection Regulation (GDPR) lo ha reso necessario su tutto il perimetro dei trattamenti dei dati personali, AI Act e NIS2 ne estendono il perimetro di attuazione: è ormai ora di fare tesoro di questi adempimenti per gestire i rischi cyber nella prospettiva più specifica degli interessi e della sostenibilità del digitale da parte della singola organizzazione.

2.5 L'Intelligenza Artificiale e Cybersecurity nella mobilità

La digitalizzazione accelerata dei trasporti ferroviari e urbani, trainata dall'adozione di IoT, Cloud e AI, sta ridefinendo l'efficienza operativa di queste infrastrutture critiche. Tuttavia, l'evoluzione tecnologica espone questi settori a nuove vulnerabilità e a minacce informatiche, imponendo la necessità di strategie avanzate di cyber resilience e di una rigorosa conformità alle normative europee

L'AI ha trasformato in modo profondo la superficie digitale delle aziende e delle Istituzioni pubbliche stesse, integrandosi nei servizi ma anche nei processi di business, nei flussi di dati e nei meccanismi decisionali. A fronte di benefici evidenti in termini di efficienza e velocità, questa diffusione ha però introdotto nuove classi di rischio e modalità di attacco che sfuggono ai paradigmi di sicurezza tradizionali. L'AI è una tecnologia potentissima che, nel campo della *cybersecurity*, si sta rivelando una "spada a doppio taglio": un'arma formidabile sia per chi difende i sistemi, sia per chi li attacca.

Gli attacchi basati su AI operano su più livelli, sfruttando interazioni semantiche, manipolazione dei prompt ed orchestrazione di agenti autonomi. Questa complessità rende inefficienti i modelli difensivi pensati per minacce lineari e prevedibili, richiedendo un'evoluzione delle operazioni di sicurezza in termini di visibilità, rilevamento e risposta specifiche per l'AI.

I SOC tradizionali, già messi sotto pressione da volumi di alert crescenti e attacchi sempre più rapidi, faticano in un contesto in cui la velocità degli attaccanti supera la sola capacità di intervento umano. Al contempo però l'AI sta rivoluzionando anche la difesa informatica. I sistemi di sicurezza più avanzati, come i Security Information and

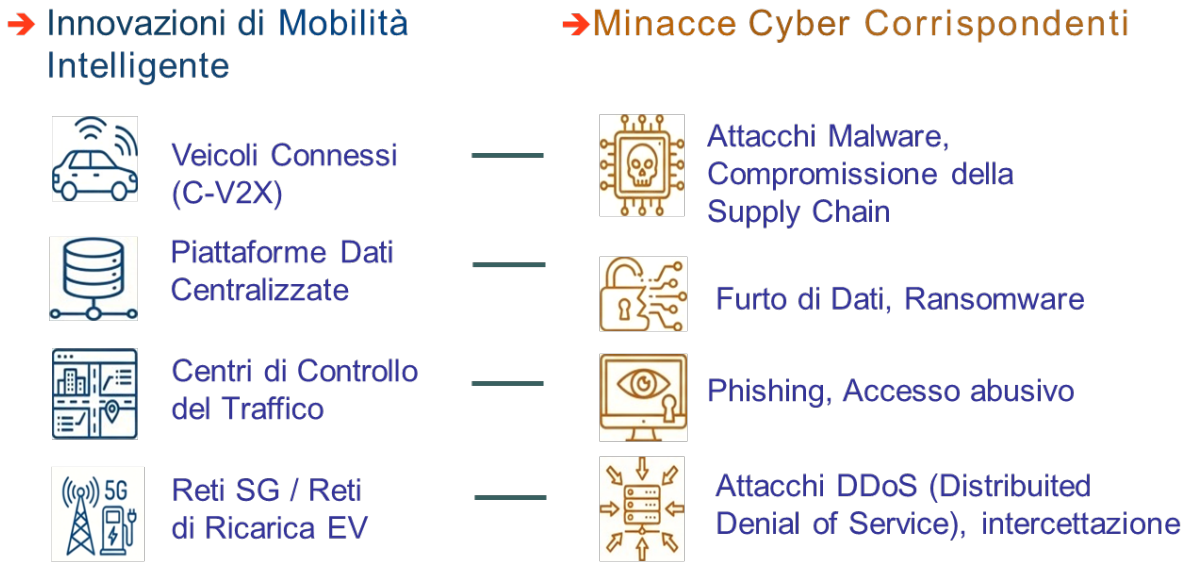
Event Management (SIEM) potenziati dall'AI, utilizzano architetture neurali profonde come le Reti Neurali Ricorrenti (RNN) per analizzare i *log* di sicurezza in tempo reale. Questo permette di identificare *pattern* di attacco sottili ad esempio nel traffico di rete dei veicoli, che i sistemi tradizionali basati su regole predefinite non riuscirebbero a cogliere. Inoltre, l'AI è in grado di analizzare enormi volumi di dati per anticipare le mosse degli attaccanti (analisi predittiva).

D'altro canto, i criminali informatici stanno sfruttando le stesse tecnologie per creare attacchi sempre più sofisticati. L'integrazione dell'AI nella mobilità intelligente, pur migliorando l'efficienza e la sicurezza, introduce un nuovo livello di minacce che espande drasticamente la superficie di attacco. Le fonti identificano diverse vulnerabilità specifiche che vanno oltre i rischi cyber tradizionali.

Ecco le principali nuove vulnerabilità introdotte dall'AI:

- **Attacchi Adversarial (Adversarial Attacks)**: questa è una delle minacce più preoccupanti per i veicoli a guida autonoma. Non si tratta semplicemente di "ingannare" l'AI, ma di sfruttare i suoi modelli matematici di percezione. Un attaccante può progettare perturbazioni quasi impercettibili, calcolate per generare errori critici. Ad esempio, un adesivo con un pattern quasi invisibile, se applicato su un segnale di STOP, può essere progettato per far sì che l'AI del veicolo lo classifichi con alta affidabilità come un segnale di "Limite di velocità 80 km/h";
- **Avvelenamento dei dati (Data Poisoning)**: questa vulnerabilità riguarda la manipolazione dei dataset utilizzati per l'addestramento dei modelli AI. Se un attaccante riesce a contaminare i dati di *training*, può compromettere l'integrità del sistema, alterando le sue prestazioni o introducendo comportamenti malevoli predefiniti che si attiveranno solo in determinate condizioni;
- **Inversione ed estrazione del modello (Model Inversion & Extraction)**: queste tecniche mirano rispettivamente a ricostruire dati sensibili utilizzati per l'addestramento partendo dagli output del sistema o a "rubare" l'architettura logica del modello AI stesso per replicarlo o studiarne i punti deboli;
- **Opacità decisionale (Black Box)**: l'AI introduce una vulnerabilità intrinseca legata alla difficoltà di interpretare il ragionamento seguito dall'algoritmo per arrivare a una determinata decisione. Questa mancanza di "spiegabilità" rende difficile prevedere come il sistema reagirà in scenari inediti o identificare se una decisione errata sia frutto di un guasto tecnico o di una manipolazione esterna;
- **Manipolazione dei flussi sensoriali**: gli attaccanti possono colpire direttamente i sensori fisici attraverso tecniche di *spoofing e jamming* (di segnali GPS, radar o telecamere) per alterare la percezione dell'ambiente da parte del veicolo AI, inducendolo a manovre pericolose;
- **Deepfake e Social Engineering**: l'AI generativa viene usata per creare email, messaggi vocali o video estremamente realistici e personalizzati (deepfake). Questi strumenti rendono le campagne di *phishing* e le truffe molto più convincenti e difficili da smascherare;
- **Dipendenza da Cloud e modelli esterni**: molti sistemi AI nella mobilità dipendono da elaborazioni da remoto. Questa connessione continua espone il sistema a interruzioni di servizio o alla compromissione dei canali di comunicazione, rendendo il veicolo vulnerabile se le sue capacità decisionali "*edge*" (locali) non sono sufficientemente autonome;
- **Democratizzazione e automazione degli attacchi**: l'AI stessa agisce come un "moltiplicatore di forza" per i cybercriminali, consentendo di automatizzare la ricerca di vulnerabilità nel software dei veicoli e di generare *malware* polimorfici capaci di adattarsi per eludere i controlli di sicurezza in tempo reale.

La tecnologia che promette efficienza è la stessa che apre le porte a nuovi rischi sistemici. La superficie d'attacco si espande con ogni nuovo nodo connesso.



In sintesi, l'AI trasforma ad esempio il veicolo in un sistema guidato da una logica probabilistica anziché deterministica: se da un lato questo lo rende più "intelligente", dall'altro lo espone a forme di inganno cognitivo precedentemente impossibili.

L'AI nella mobilità intelligente è come un pilota estremamente esperto ma che soffre di allucinazioni se indotto da segnali specifici: gli attaccanti non cercano più solo di rompere i freni (vulnerabilità fisica), ma di convincere il pilota che la strada sia libera quando invece c'è un muro (vulnerabilità cognitiva).

In questo scenario prende forma il concetto di Agentic Security Operation Center, un cambio di paradigma in cui agenti di AI assumono un ruolo attivo nel rilevare, analizzare e reagire agli incidenti, andando oltre la semplice automazione. Parallelamente diventa centrale la protezione degli stessi sistemi di AI. Con la AI Detection & Response, la sicurezza si estende a modelli, agenti e pipeline decisionali, riconoscendo l'AI sia come uno strumento di difesa sia come un asset critico da proteggere. Agentic SOC e AI Detection & Response rappresentano quindi due aspetti complementari di un'unica trasformazione: l'AI come componente centrale dell'ecosistema di sicurezza informatica.

La digitalizzazione del settore dei trasporti è inarrestabile. Eventi recenti dimostrano che gli attori malevoli non sono più costretti a compromettere le infrastrutture fisiche per generare interruzioni operative: le vulnerabilità digitali rappresentano oggi minacce ancor più concrete ed immediate per la sicurezza, la continuità del servizio e la fiducia degli utenti. Pertanto, il settore deve essere in grado di garantire la sicurezza informatica, superando le resistenze culturali, oltre ad investire in formazione e a adottare un approccio realmente integrato e proattivo.

2.6 Esigenze di Cybersecurity e AI espresse dagli attori di mobilità

Gli ITS Days nascono in TTS Italia per mettere a confronto Domanda e Offerta in un ambiente super partes, per favorire il dialogo, lasciando emergere le reali necessità del Territorio e dei suoi rappresentanti istituzionali. Con cadenza periodica, affrontano di volta in volta un diverso tema legato alla mobilità intelligente e sicura, con particolare riferimento alle aree di interesse della Direttiva ITS aggiornata.

Il primo incontro, riservato ai soci di TTS Italia, si è svolto il 18 dicembre 2024 ove si è parlato di Smart Road, e dunque della digitalizzazione delle infrastrutture di trasporto, poi altri incontri si sono focalizzati sulle tematiche dell'AI per il TPL e per la gestione della mobilità urbana.

Il quinto incontro svoltosi a fine marzo del 2026 è stato dedicato proprio al tema della "**Cybersecurity nella mobilità**". La cybersecurity vista come una componente critica per garantire la sicurezza nel settore dei trasporti, proteggendo non solo i dati degli utenti, ma l'intera infrastruttura interconnessa. Occasione quindi per parlare di sicurezza e minacce per infrastrutture, servizi di mobilità, mobilità connessa e autonoma, dati di mobilità, tra gli altri temi.

All'incontro erano presenti circa 30 partecipanti in rappresentanza degli attori della domanda e dell'offerta. È risultato evidente che la PA ha preso ormai conoscenza del problema della Cybersecurity, incrementata dall'uso dell'AI e ci sono significativi aumenti dei budget. Nel caso dei sistemi ITS ci sono problemi sul territorio, in quanto vi è la necessità di proteggere ogni punto di accesso da sistemi ITS sul territorio nonché la necessità di capacità di attrazione e mantenimento dei migliori profili da parte della PA, che si scontra con la scarsa flessibilità del lavoro all'interno di tali organizzazioni

Altra problematica è la spesa corrente più degli investimenti, in quanto molte soluzioni sono ormati trattate a livello SaaS (Software as a Service) con tariffe annuali su cloud senza vendita di sistemi ma che sono necessari a garantire la business continuity e con prezzi in continuo aumento. Ciò crea una difficile pianificazione dei costi oltra a ravvisarsi una necessità costante per fondi d'innovazione in un mercato che si aggiorna continuamente.

La protezione dei dati necessità investimenti continui e c'è un incremento continuo delle superfici d'attacco e dei dati da essi prodotti.

Ne risulta un triangolo ormai inevitabile fra digitalizzazione della mobilità, le minacce informatiche aumentate dall'AI e la Cybersecurity, con alcune tipologie di attacco sono realmente una spina nel fianco delle aziende di mobilità. Va assicurata coerenza tra digitalizzazione, infrastrutture operative e obblighi normativi.

È stata ribadita la necessità di compliance con la NIS2 anche per le organizzazioni locali e come le complesse procedure di incident report vadano recepite ed approvate dal management aziendale e dalle PA controllanti e rese operative in tempi sempre più brevi, sulla base di assessment specifici con risultati importanti anche in termini di pre-analisi e che porta a decisioni di gestione del parco macchine e delle vulnerabilità in termini di rischio aziendale.

Va costruito un approccio basato sul rischio specifico per asset per indirizzare le strategie di mitigazione ed orientare le decisioni. L'enrollment critico è un passaggio essenziale nella governance cyber delle nuove tecnologi/servizi digitali.

La Governance è necessaria per protezione dei dati, la gestione del rischio e la continuità operativa in contesti distribuiti e che integrano aziende provenienti da realtà inizialmente diverse, con gestione integrata della supply chain. Risulta quindi fondamentale il monitoraggio con KPI del rischio e quanto costerebbe l'impatto degli incidenti, sia in termini finanziari che di credibilità della struttura.

A livello di operatori urbani occorre la presa di coscienza delle necessità di spesa corrente in quanto si tratta principalmente di SaaS (Software as a Service) e non di acquisti una tantum. Occorrerà una policy coordinata fra gli attori che dovrà essere inglobata anche nel costruendo Piano ITS.

Nelle organizzazioni logistiche c'è poi una generale mancanza di consapevolezza di queste tematiche, in un mondo in cui lo scambio dati è proprio parte del processo.

Nelle smart roads e nelle autostrade è necessario segmentare tutti i collegamenti verso l'esterno e garantire l'integrità, riservatezza e utilizzo dell'informazione. Si utilizzano sistemi a più macro componenti di sistema con problemi di cybersicurezza, con decreto Smart Road che non tiene conto delle nuove problematiche. Ci sono esperienze anche innovative come ad esempio lo sviluppo di una infrastruttura quantistica per la messa in sicurezza dell'infrastruttura con chiavi quantistiche.

Ci sono stati warning durante le Olimpiadi Milano-Cortina per attacchi a sistemi ITS delle smart roads quali target come telecamere, VMS, V2X con possibili impatti su congestione e panico. Si sono quindi avviate esperienze di coordinamento fra diversi operatori (ASPI, ANAS, ecc) in maniera transnazionale con ISAC ma anche di sicurezza dei sensori diffusi (es. VMS). Vi sono state decisioni di chiudere le connessioni non necessarie e cambiare le password locali oltre ad una serie di azioni condivise fra tutti gli attori e si è evidenziata la necessità di andare oltre

le NIS2 aziendali per cooperazione fra i vari attori. Tutti gli operatori stradali sono parte di un sistema fortemente connesso e vanno superati i confini aziendali nella gestione della cybersecurity.

La complessità del perimetro cyber insieme alle limitazioni delle legacy dei sistemi OT, i rischi della supply chain e le grandi quantità di dati in gioco rischiano però di mettere a rischio cyber i processi. Ne emerge la necessità dell'aggiornamento del Decreto Smart Roads.

Il lato dell'offerta ha evidenziato come le soluzioni di agenti AI che lavorano in contesto svincolato dalla mobilità non siano già più adeguati ma come sia necessario un contesto per sviluppo applicazioni coerenti con l'azienda e come sia essenziale la creazione del digitale twin IT dell'azienda con sistemi che garantiscono l'aderenza dei sistemi aziendali a NIS2, CRA, AI Act;

Si è evidenziato come il costo medio data-breach sia già oltre 4 ML€ e come l'AI abbia cambiato il paradigma, con vantaggi operativi ma con aumentati della superficie d'attacco e l'impatto misurato. L'approccio responsabile all'AI deve prevedere 5 passi concreti: valutazione cyber, integrazione AI nella sicurezza, adozione di modello Zero Trust, unificare compliance e governance AI e progettazione resilienza dei sistemi. Infine non deve mancare la sensibilizzazione e formazione continua del personale.

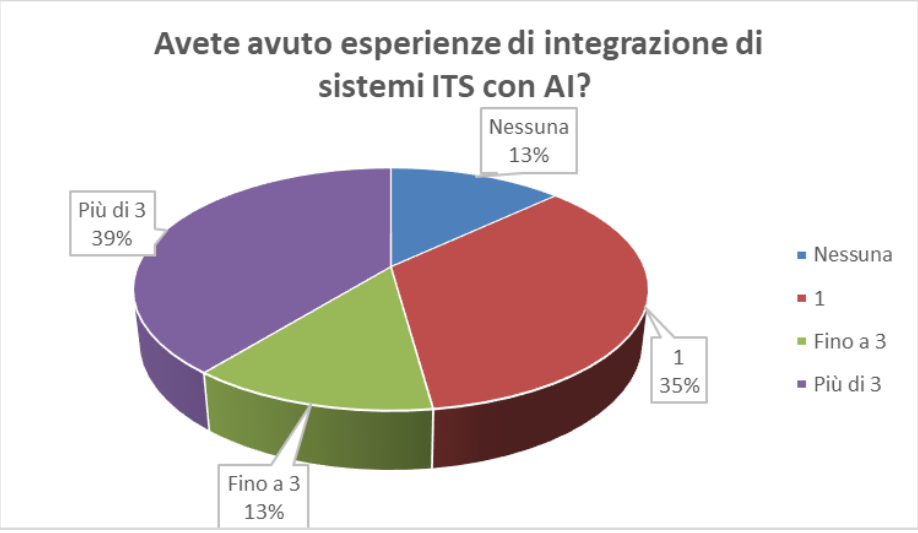
Tratti essenziali nella protezione dei trasporti sono la global security, la cyber resilience by design dei prodotti, la protezione delle infrastrutture IT/IT e l'AI-driven security. AI for remediation a metodologia RBVR in base al contesto porta importanti migliorie alle metodologie

Per quanto riguarda gli apparati di campo, la compliance by design deve partire proprio dal campo con apparati che abbiano la sicurezza come DNA nativo. Occorre partire dalla protezione del silicio con modulo crittografico, garantire l'integrità del software ed una gestione proattiva della vulnerabilità; ad esempio, nelle TVCC occorre garantire l'autenticità dei flussi video tramite firma digitale del video. Altro esempio, l'efficienza operativa può essere aumentata tramite una gestione centralizzata degli apparati di campo. La sicurezza informatica e quella fisica non sono più separate, ma un unico ecosistema di protezione e quindi la complessità normativa può essere trasformata in opportunità.

Si è poi analizzato in maniera puntuale con i seguenti spunti/domande le principali questioni sull'integrazione fra sistemi ITS, AI e Cybersecurity poste a tutti i partecipanti attraverso un tool interattivo e dove le risposte vanno intese come esperienze dirette degli attori di domanda e tramite i sistemi forniti per gli attori di offerta.

1) Avete avuto esperienze di integrazione di sistemi ITS con AI?

Le risposte riportate nel grafico seguente evidenziano un'alta familiarità dei partecipanti verso tale integrazione, dove il 39% ha dichiarato di aver avuto più di tre tali esperienze e dove soltanto il 13% non ne ha avuta nessuna.

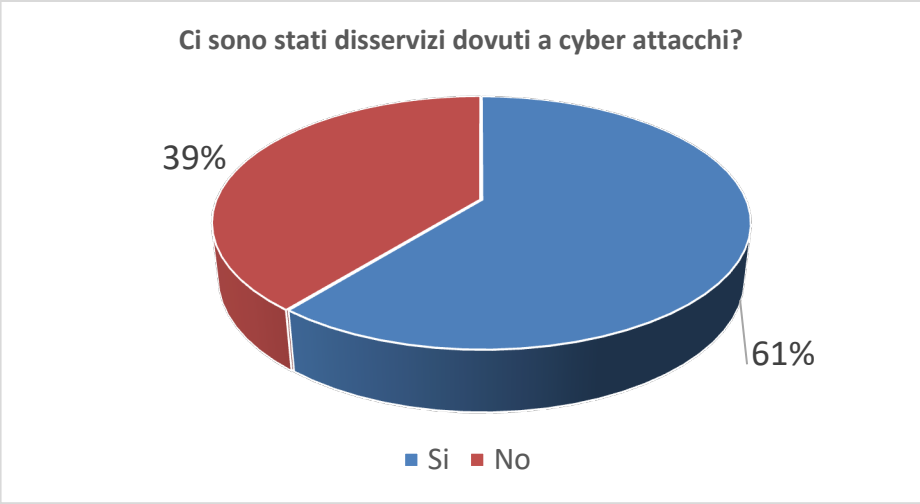


2) Ci sono stati episodi di data breach nei sistemi di vostra responsabilità?

Il grafico seguente evidenzia che ci sono già esperienze di data breach pari al 50% circa del campione e che alcuni episodi potrebbero non essere stati rilevati dai sistemi esistenti. Quindi il fenomeno è già presente sul territorio.

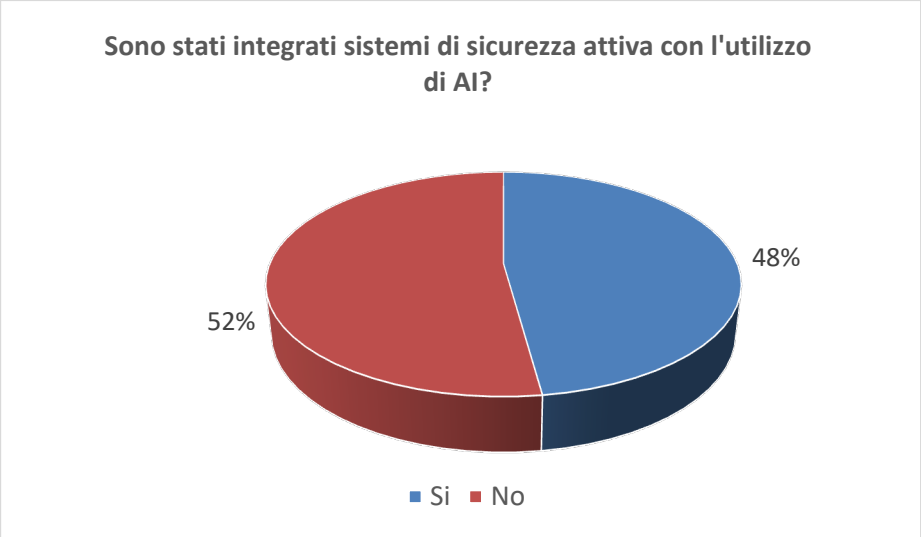
3) Ci sono stati disservizi dovuti a cyber attacchi nei sistemi da voi gestiti/forniti?

Oltre il 60% del campione ha già avuto evidenza di conseguenza dei cyber attacchi come evidenziato dal grafico seguente.



4) Sono stati integrati sistemi di sicurezza attiva con l'utilizzo di AI?

Le risposte riportate nel grafico seguente indicano che circa la metà dei votanti ha già provveduto ad integrare sistemi di sicurezza attiva con l'utilizzo di AI

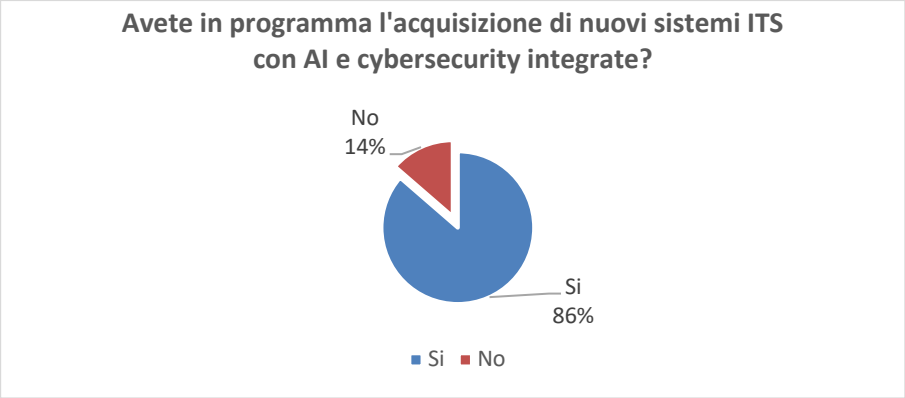


5) Sono state pianificate attività di integrazione di misure di cyber sicurezza per i sistemi ITS

Le risposte evidenziano una estrema consapevolezza della problematica e tali attività di integrazione sono state previste dalla quasi totalità dei votanti

6) Avete in programma l'acquisizione di nuovi sistemi ITS con AI e Cybersecurity integrate?

Anche in questa ultima risposta, si evidenzia una notevole consapevolezza della problematica e tali attività di acquisizione sono state previste dalla grande maggioranza dei votanti.



La giornata dedicata e le risposte a queste domande mettono in evidenza quindi la consapevolezza odierna dell'impatto dell'AI e della cyberscurity e ancor più quello previsto nel prossimo futuro sia fra gli associati di TTS Italia sia anche in importanti attori di domanda a livello nazionale.

3 Normative, standard e compliance internazionale

3.1 Il contesto strategico europeo

Per governare la complessità e mitigare i rischi, l'Unione Europea (UE) ha definito un quadro normativo integrato. Queste direttive non sono silos, ma **pilastri interconnessi** progettati per garantire interoperabilità, resilienza e affidabilità nell'era della mobilità intelligente. L'obiettivo è creare un **mercato unico digitale sicuro per i trasporti**

L'adozione dell'AI nei trasporti non avviene in un vuoto, ma si inserisce in un contesto di accesa competizione globale e di un quadro politico europeo sempre più definito. Per avere successo, l'Europa deve far leva sui propri punti di forza, consolidare il proprio quadro normativo e promuovere una cultura della collaborazione in grado di superare la frammentazione interna.

La valutazione emersa dal workshop della Commissione Europea è chiara: l'UE è attualmente in ritardo rispetto ad altre potenze globali nello sviluppo di modelli LLM di tipo generalista. Tuttavia, l'UE possiede un'opportunità unica per differenziarsi e conquistare una posizione di leadership concentrandosi sullo sviluppo di modelli e applicazioni di AI settoriali.

Sfruttando i suoi ricchi e ineguagliabili patrimoni di dati industriali, in particolare nel settore della mobilità e della manifattura, l'Europa può creare un'AI affidabile (*trustworthy AI*), specializzata e conforme ai propri valori.

Questa strategia è supportata da un solido quadro politico e normativo:

- Un chiaro mandato politico derivante dalle Linee Guida della Presidente von der Leyen, che spingono per un'accelerazione sull'uso dell'AI nel settore della mobilità;
- Una regolamentazione di riferimento a livello mondiale come l'AI Act, che mira a bilanciare innovazione e tutela dei diritti fondamentali, creando un marchio di affidabilità per l'IA europea;
- Iniziative a supporto dell'innovazione come *l'AI Innovation Package*, che include le *AI Factories* per democratizzare l'accesso al calcolo e GenAI4EU per stimolare lo sviluppo di applicazioni generative;
- Strategie mirate sui dati, come la *European Data Strategy* e la creazione di spazi di dati comuni, tra cui il *Common European mobility data space*.

Una delle principali sfide per l'Europa è il suo panorama di stakeholder, che risulta relativamente frammentato se confrontato con quello di altre regioni. Questa frammentazione richiede un'enfasi strategica sulla collaborazione per aggregare risorse, condividere conoscenze e raggiungere la massa critica necessaria per competere globalmente.

Le partnership tra centri di ricerca, industria e autorità pubbliche sono cruciali. La ricerca accademica fornisce le fondamenta scientifiche, l'industria porta la capacità di implementazione e scalabilità, e il settore pubblico definisce il quadro normativo e può agire come primo utilizzatore e facilitatore.

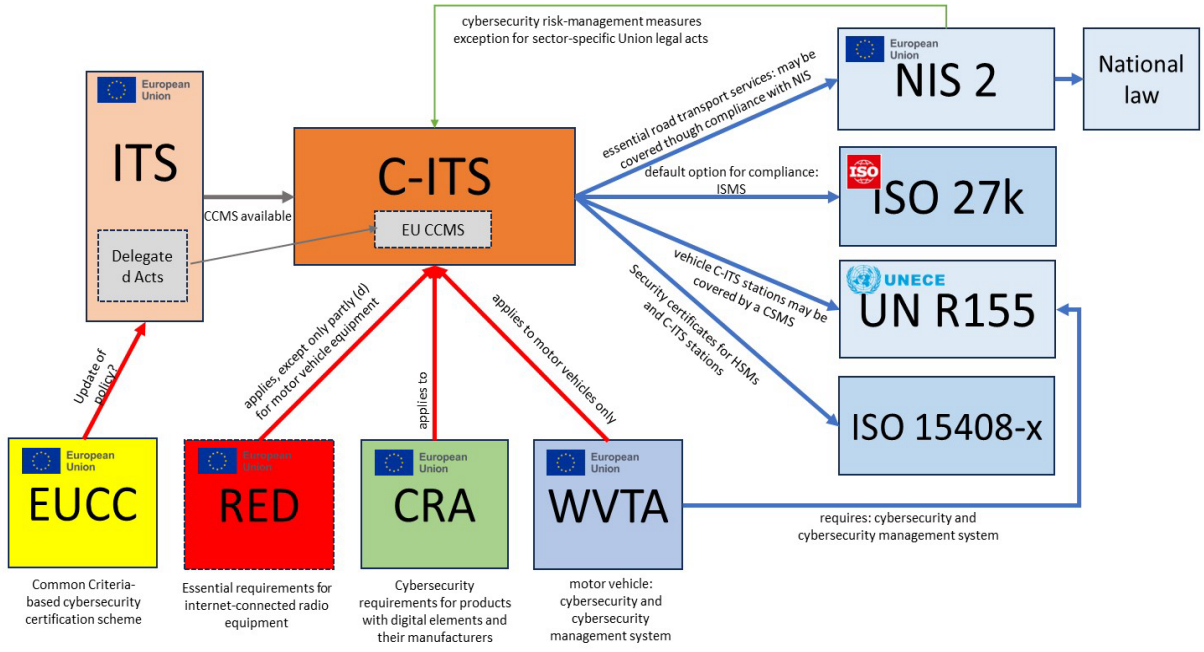
In questo contesto, l'UE ha un ruolo centrale come catalizzatore. Attraverso il supporto a progetti collaborativi, la promozione di standard tecnici comuni per garantire l'interoperabilità e l'allocazione di finanziamenti mirati, l'UE può contribuire a creare un ecosistema di innovazione più integrato e coeso, capace di trasformare le sfide della frammentazione in un'opportunità di cooperazione virtuosa.

Le Principali normative europee riflettono la convergenza fra ITS, AI e Cibersecurity, imponendo requisiti trasversali ai tre domini.

- **Direttiva ITS (UE 2023/2661):** promuove la digitalizzazione dei trasporti, modificando la direttiva ITS originaria (2010/40/UE) per aggiornare il quadro normativo alla luce delle nuove tecnologie (mobilità connessa, automatizzata, multimodale);
- **EU AI Act**: la Strategia Europea per l'AI si fonda su una visione chiara e una doppia ambizione. La strategia mira a posizionare l'Europa come un polo di eccellenza mondiale nel campo dell'AI;

- **EU Data Act e EMDS**: per trasformare il potenziale dell'AI in un vantaggio competitivo concreto, l'ecosistema europeo deve poggiare su tre pilastri strategici: la disponibilità di dati di alta qualità, l'accesso a infrastrutture di calcolo potenti e la presenza di competenze umane adeguate. Al centro di questa evoluzione vi è il vasto potenziale, ancora in gran parte non sfruttato, dei dati sulla mobilità. Per sbloccare questo valore, l'UE ha messo in campo due iniziative strategiche complementari. La prima è il Data Act, un quadro legislativo orizzontale che stabilisce regole eque per l'accesso e l'utilizzo dei dati in tutti i settori economici. La seconda è lo Spazio Comune Europeo dei Dati sulla Mobilità (EMDS);
- **Contesto GDPR e protezione della privacy;**
- **Direttiva NIS2**: estende gli obblighi di cybersecurity ai settori dei trasporti e dell'energia, imponendo misure di gestione del rischio e notifiche di incidenti gravi;
- **Cyber Resilience Act (CRA)**: stabilisce requisiti orizzontali di sicurezza per tutti i prodotti con elementi digitali durante l'intero ciclo di vita e comprende l'EUCC (European Union Cybersecurity Certification Scheme on Common Criteria);
- **Standard Automotive (UNECE R155/R156 e ISO/SAE 21434):** rendono obbligatori i sistemi di gestione della cybersecurity e degli aggiornamenti software per l'omologazione dei veicoli.

Per completezza, nella figura seguente, estratta dal TF1 di C-Roads e contestualizzata solo alla certificazione delle Fixed C-ITS Stations, sono rappresentate anche le altre norme cui il settore si deve attenere, a partire dalla normativa ITS 2010/40/UE appunto aggiornata dalla 2661/2023/UE e relativi atti delegati, oltre alle normative sull'AI. Si tenga presente che queste leggi e la loro applicabilità sono peraltro ancora in discussione.



A questa serie di normative vanno integrate le **ISO/IEC 27000**, la cui certificazione (solitamente ISO 27001) dimostra l'impegno costante dell'azienda/organizzazione verso la sicurezza. E' una famiglia di standard internazionali per la sicurezza delle informazioni, che definisce le best practice per gestire la riservatezza, l'integrità e la disponibilità dei dati. Aiuta le organizzazioni a creare un Sistema di Gestione della Sicurezza delle Informazioni (ISMS) per identificare rischi e applicare controlli adeguati. Nasce proprio con l'obiettivo di proteggere informazioni, proprietà intellettuale, dati di dipendenti e clienti. Si applica a organizzazioni di qualsiasi settore o dimensione e presenta il vantaggio di ridurre dei rischi informatici, conformità normativa (es. GDPR) e miglioramento

dell'immagine aziendale. Oltre alla 27001 e 27002, la famiglia include norme specifiche come la ISO/IEC 27005 per la gestione dei rischi e le ISO/IEC 27017/27018 per la sicurezza nel cloud.

In sintesi, la convergenza tra ITS, AI e cybersecurity trasforma la mobilità in un organismo digitale complesso. Se gli ITS sono gli organi del trasporto e l'AI è il cervello che ne coordina le funzioni, la cybersecurity rappresenta il sistema immunitario senza il quale l'intero organismo non potrebbe sopravvivere in un ambiente digitale ostile. Le citate normative principali vengono di seguito analizzate in dettaglio.

3.2 La Direttiva UE 2023/2661 e le sue implicazioni

Contesto normativo: cosa introduce la Direttiva 2023/2661

La Direttiva (UE) 2023/2661 modifica la direttiva ITS originaria (2010/40/UE) per aggiornare il quadro normativo alla luce delle nuove tecnologie (mobilità connessa, automatizzata, multimodale).

L'obiettivo è promuovere una digitalizzazione più spinta dei trasporti stradali, garantire l'interoperabilità dei dati e favorire la diffusione di servizi ITS emergenti.

La direttiva stabilisce che certi dati digitali essenziali (es. limiti di velocità, piani del traffico, restrizioni stradali, lavori stradali) devono essere resi disponibili tramite punti di accesso nazionali in formato riutilizzabile.

Prevede un'estensione geografica: gli Stati membri devono coprire una rete minima di strade per la disponibilità di questi dati.

L'entrata in vigore è relativamente rapida: gli Stati membri dovranno conformarsi entro 24 mesi dall'entrata in vigore e quindi entro il 21/12/25

Le priorità d'azione identificate nella direttiva includono, tra le altre, i servizi informativi multimodali, l'informazione sul traffico in tempo reale, i servizi di sicurezza stradale, la mobilità cooperativa e automatizzata

Implicazioni tecniche per ITS + AI + Cybersecurity

L'adozione della direttiva 2023/2661 ha impatti tecnici rilevanti su come progettare i sistemi ITS, sulle architetture dati, sulla strategia AI e sulle misure di *cybersecurity*:

Architettura dei dati

- National Access Points (NAP): gli Stati membri devono predisporre punti di accesso nazionali che permettano la condivisione di dati stradali in un formato interoperabile. Ciò richiede un'infrastruttura dati robusta: API, cataloghi dati, endpoint per dati real-time;
- Standardizzazione dei dataset ITS: i dati richiesti dalla direttiva (traffico, restrizioni, lavori, limiti di velocità, ecc.) devono rispettare formati comuni per garantire interoperabilità. Questo richiede componenti di *data ingestion* [tecniche specifiche di acquisizione massiva di dati], normalizzazione e validazione;
- Sicurezza e integrità dei dati condivisi: poiché i NAP saranno fonti critiche di dati ITS per molte applicazioni (AI, infomobilità, safety), diventa essenziale garantire che i dati pubblicati siano autenticati, protetti da manomissione e aggiornati in modo sicuro.

Mobilità connessa e automatizzata

- Cooperative ITS (C-ITS): la direttiva menziona esplicitamente i servizi per la mobilità cooperativa e automatizzata, il che implica che gli standard V2X (G5, C-V2X) e le specifiche di messaggi devono essere pienamente integrati nei piani di implementazione;
- Sicurezza V2X: per supportare i casi d'uso cooperativi e di sicurezza, le architetture dovranno includere PKI per la certificazione dei messaggi V2X, revoca di certificati e meccanismi di trust;
- Edge/fog computing: per gestire dati real-time (es. denunce di incidenti, informazioni traffico), sarà probabilmente necessario un forte uso di edge computing integrato con i punti di accesso dati.

AI & Analisi

- Modelli predittivi basati su dati condivisi: con la disponibilità di dati ricchi e interoperabili dai punti di accesso, si possono sviluppare modelli AI per previsioni di traffico, gestione dinamica del traffico e persino simulazioni cooperative tra veicoli in tempo reale;
- Servizi intelligenti basati su dati comuni: la direttiva spinge per servizi di informazione multimodale e prenotazione, il che significa che le applicazioni AI possono usare i dati condivisi (es. network multimodale) per offrire pianificatori di viaggio, raccomandazioni dinamiche, ottimizzazione delle corse.

Cybersecurity

- Protezione dei data point nazionali: i NAP diventano "infrastrutture critiche digitali" ITS: bisogna applicare misure di sicurezza per autenticazione, autorizzazione e integrità (es. TLS, API security). Si tenga comunque presente che tale categorizzazione non è automatica. In Italia infatti al momento non lo è ed inoltre i threat sono definiti da NAPCORE, le specifiche di sicurezza del NAP sono in via di pubblicazione;
- Resilienza alle minacce di integrità dati: attacchi di *spoofing* o manomissione dati (es. inserimento dati falsi sui lavori stradali) possono avere conseguenze severe su servizi safety – serve un sistema di auditing, verifica e firma dei dati;
- Compliance normativa vs sicurezza: le politiche di condivisione dei dati devono essere bilanciate con la sicurezza e la privacy. È fondamentale progettare i punti di accesso con meccanismi di access control*, policy di data governance e logging* per la tracciabilità degli usi.

Opportunità strategiche alla luce della Direttiva

Integrare la direttiva 2023/2661 nei piani strategici tecnologici può creare vantaggi competitivi e operativi quali:

Sviluppo di un Mobility Data Space nazionale / regionale

- Creare una piattaforma dati nazionale che rispetti i requisiti del NAP richiesti dalla direttiva;
- Favorire partnership pubblico-private per alimentare la piattaforma con dati ITS (infrastruttura, veicoli, traffico);
- Utilizzare il data space come base per applicazioni AI (previsione traffico, guida autonoma, servizi multimodali).

Servizi innovativi basati su AI

- Sviluppare applicazioni che sfruttano dati in tempo reale dai punti di accesso per fornire servizi di infomobilità, pianificazione multimodale, avvisi di sicurezza;
- Creare modelli predittivi con dati normalizzati: ad esempio, algoritmi che stimano i flussi di traffico in base a dati di lavori/ingressi temporanei, per ottimizzare la regolazione semaforica o veicoli cooperativi;
- Implementazione sicura di V2X;

- Costruire una PKI ITS per autenticare messaggi V2X, in linea con gli obiettivi Connected-ITS (C-ITS) della direttiva;
- Pianificare sviluppi di Road-Side Units (RSU) e On-Board Units (OBU) sicuri, con capacità di aggiornamento OTA protetto, per supportare la mobilità connessa e automatizzata.

Governance e privacy dei dati

- Definire una *policy* nazionale di *data governance* che includa la minimizzazione, la pseudonimizzazione, l'access control e il tracciamento degli accessi;
- Creare una struttura di *auditing* per garantire che i dati condivisi tramite il NAP siano usati in modo conforme alle norme europee e nazionali.

Sicurezza e resilienza

- Integrare la cybersecurity dei punti di accesso ITS nel piano di sicurezza nazionale / delle infrastrutture critiche;
- Costruire un Security Operation Center dedicato alla mobilità intelligente, con monitoraggio specifico per anomalie nei flussi di dati ITS.

3.3 L'AI Act: la strategia europea per l'intelligenza artificiale

L'approccio dell'UE all'AI si fonda su una visione chiara e una doppia ambizione. La strategia mira a posizionare l'Europa come un polo di eccellenza mondiale nel campo dell'AI, stimolando la ricerca, la capacità industriale e la competitività globale. Allo stesso tempo, e in modo inseparabile, l'UE si impegna a garantire che questa tecnologia sia sviluppata e utilizzata in modo affidabile, incentrata sull'uomo e nel pieno rispetto della sicurezza e dei diritti fondamentali. Questi due pilastri – eccellenza e fiducia – non sono obiettivi distinti, ma due facce della stessa medaglia. Anzi, la loro interdipendenza rappresenta la scommessa strategica dell'Europa: fare della fiducia un prerequisito per l'innovazione, trasformando la regolamentazione in un vantaggio competitivo. Questo approccio definisce una "terza via" rispetto al modello statunitense, più orientato al mercato, e a quello cinese, a forte guida statale, plasmando tutte le politiche dell'UE per governare il futuro digitale.

Per l'UE, "eccellenza" significa rafforzare il potenziale del continente per competere a livello globale nel campo dell'AI. Questo obiettivo si traduce in un impegno concreto per sostenere la ricerca all'avanguardia, potenziare la capacità industriale e assicurare che le innovazioni tecnologiche portino benefici tangibili a tutta la società.

L'UE persegue questo obiettivo attraverso tre azioni strategiche principali:

- Consentire lo sviluppo e l'adozione dell'AI: creare un ecosistema normativo ed economico che abbatta le barriere all'ingresso, permettendo a imprese e ricercatori di implementare soluzioni di AI su larga scala;
- Diventare il luogo in cui l'AI prospera, dal laboratorio al mercato: supportare l'intero ciclo di vita dell'innovazione, aiutando le idee nate nei centri di ricerca a trasformarsi in prodotti e servizi commercialmente validi, a beneficio delle imprese e dei consumatori europei;

- Garantire che l'AI funzioni per le persone e sia una forza positiva per la società: indirizzare lo sviluppo dell'AI verso la risoluzione di grandi sfide sociali, come la sanità, la sostenibilità ambientale e l'efficienza dei servizi pubblici, assicurando che la tecnologia migliori la qualità della vita dei cittadini.

Per sostenere questa ambizione, l'UE ha mobilitato ingenti risorse finanziarie. Attraverso i programmi Orizzonte Europa ed Europa Digitale, viene investito 1 miliardo di euro all'anno nell'AI. L'obiettivo, mobilitando anche investimenti dal settore privato e dagli Stati membri, è raggiungere un volume di investimenti annuo di 20 miliardi di euro nel corso del decennio digitale.

Tuttavia, l'eccellenza tecnologica da sola è fragile. Per trasformarla in un vantaggio competitivo duraturo, l'UE la ancora al suo **secondo pilastro**: la costruzione di un ecosistema di fiducia.

La fiducia è la pietra angolare della strategia europea per l'AI. Questo principio significa garantire che i sistemi di AI siano sicuri, trasparenti, non discriminatori e rispettosi dei diritti fondamentali e dei valori democratici dell'UE. L'obiettivo è costruire un ecosistema in cui i cittadini possano fidarsi della tecnologia che usano e le imprese possano innovare con certezza giuridica.

Per tradurre questo principio in pratica, l'UE ha creato il primo quadro giuridico completo al mondo sull'AI: l'AI Act.

Stabilendo regole chiare e prevedibili, l'UE non solo tutela i cittadini, ma crea un mercato di alta qualità che favorisce l'accettazione sociale e l'adozione su larga scala dell'AI, trasformando la fiducia in un vero e proprio vantaggio competitivo a livello globale.

Questo approccio unico, che lega indissolubilmente l'innovazione alla tutela dei valori, è supportato da iniziative specifiche volte a stimolare l'ecosistema europeo. Lanciato nel gennaio 2024, il **Pacchetto di innovazione per l'AI** è un insieme di misure concrete volte a sostenere le startup e le Piccole e Medie Imprese (PMI), che sono il motore dell'innovazione europea. L'obiettivo è fornire loro le risorse necessarie per sviluppare un'AI affidabile e competitiva a livello globale.

Il pacchetto offre tre pilastri di supporto fondamentali per le imprese innovative:

- **Supporto finanziario**: attraverso i programmi Orizzonte Europa ed Europa Digitale, la Commissione mobilita finanziamenti dedicati all'AI generativa, con l'obiettivo di generare un investimento complessivo pubblico e privato di circa 4 miliardi di euro fino al 2027;
- **Accesso privilegiato ai supercomputer**: lo sviluppo di modelli di AI avanzati richiede un'enorme potenza di calcolo. L'UE mette a disposizione delle startup la sua infrastruttura di supercalcolo leader a livello mondiale attraverso le cosiddette "Fabbriche di AI" (AI Factories), veri e propri hub di risorse per l'addestramento di modelli su larga scala;
- **Accesso ai dati**: i dati di alta qualità sono la "materia prima" essenziale per l'AI. L'UE sta accelerando lo sviluppo degli Spazi Comuni Europei di Dati, che renderanno disponibili vasti set di dati a ricercatori e imprese per addestrare e migliorare i loro modelli.

Un'iniziativa chiave di questo pacchetto è '**GenAI4EU**', che mira a stimolare l'adozione dell'AI generativa nei principali ecosistemi industriali strategici dell'UE, come robotica, sanità, biotecnologie, manifattura, mobilità, clima e mondi virtuali.

Per sviluppare l'AI serve potenza di calcolo. Moltissima. Per questo l'EU vuole dare alle PMI e alle startup un accesso privilegiato alla rete di supercomputer europei, ad esempio con il lancio di **AI Factories**, che riunisce le "materie prime" per l'AI: potenza di calcolo, dati, algoritmi e talento. Fungerà da punto di riferimento unico per le startup europee di AI, consentendo loro di sviluppare i modelli di AI e le applicazioni industriali più avanzati.

Per garantire che queste startup innovative operino in un mercato sicuro e prevedibile, il Pacchetto si integra direttamente con il quadro normativo definito dall'AI Act, che fornisce le regole del gioco per uno sviluppo tecnologico affidabile.

L'AI Act: regole chiare per un'AI sicura

L'AI Act è il primo quadro normativo completo al mondo sull'AI, un modello che l'UE spera possa generare un "effetto Bruxelles", stabilendo uno standard globale de facto. Il suo scopo è duplice: affrontare i rischi associati a specifici utilizzi dell'AI e, allo stesso tempo, promuoverne l'adozione e l'innovazione in un ambiente sicuro e affidabile.

La legge adotta un approccio basato sul rischio, classificando i sistemi di AI in quattro livelli distinti, con obblighi proporzionati al potenziale pericolo che rappresentano.

Livello di Rischio	**Descrizione**	**Esempi pratici**
Rischio inaccettabile	Sistemi di AI che rappresentano una chiara minaccia per la sicurezza, i mezzi di sussistenza e i diritti delle persone. Questi sistemi sono vietati.	Punteggio sociale (*social scoring*), manipolazione comportamentale dannosa, sfruttamento delle vulnerabilità delle persone, scraping non mirato di immagini facciali da internet o telecamere a circuito chiuso, riconoscimento delle emozioni sul posto di lavoro e negli istituti di istruzione.
Alto rischio	Sistemi di AI che possono avere un impatto negativo sulla sicurezza o sui diritti fondamentali. Sono soggetti a obblighi rigorosi prima di poter essere immessi sul mercato.	Componenti di sicurezza nei trasporti, sistemi utilizzati negli istituti di istruzione (es. per la valutazione degli esami), strumenti per la gestione dei lavoratori (es. software per lo smistamento di CV), sistemi per la gestione della migrazione e delle frontiere (es. esame automatizzato delle domande di visto), sistemi impiegati nell'amministrazione della giustizia.
Rischio di trasparenza	Sistemi di AI per i quali gli utenti devono essere informati che stanno interagendo con una macchina. Richiedono obblighi di trasparenza specifici.	Chatbot, *deep fake*, contenuti generati dall'AI (devono essere identificabili come tali).
Rischio minimo o nullo	La stragrande maggioranza dei sistemi di AI. La legge consente il loro uso senza restrizioni.	Videogiochi basati sull'AI, filtri antispam.

Per i sistemi classificati ad alto rischio quali i sistemi ADAS e di guida autonoma, impone severi requisiti di accuratezza, robustezza e sorveglianza umana ed obblighi stringenti per garantire la massima sicurezza. I più importanti includono:

1. Valutazione e mitigazione dei rischi adeguati: identificare, analizzare e ridurre i potenziali pericoli prima che il sistema raggiunga il mercato;
2. Alta qualità dei set di dati: utilizzare dati di addestramento di alta qualità per ridurre al minimo i rischi di risultati distorti e discriminatori;
3. Registrazione delle attività (*logging*): garantire la tracciabilità dei risultati e del funzionamento del sistema per poter indagare su eventuali incidenti;
4. Documentazione tecnica dettagliata: fornire tutte le informazioni necessarie sul sistema e sul suo scopo per consentire alle autorità di valutarne la conformità;
5. Informazioni chiare e adeguate all'utente: assicurare che chi utilizza il sistema possa comprenderne le capacità e i limiti;
6. Adeguata supervisione umana (*human oversight*): progettare i sistemi in modo che possano essere efficacemente supervisionati da persone, che devono poter intervenire o interromperne il funzionamento;
7. Un alto livello di robustezza, sicurezza informatica e accuratezza: garantire che i sistemi siano sicuri, resilienti e funzionino come previsto.

Per garantire che questa complessa strategia venga attuata in modo coerente in tutta l'Unione, è stato creato un organo di coordinamento centrale, **l'Ufficio Europeo per l'AI.**

Questo organo, interno alla Commissione, svolge due funzioni principali:

- Coordinare la politica in materia di AI a livello europeo: assicura che tutte le iniziative e le politiche degli Stati membri e delle istituzioni UE siano allineate, promuovendo un approccio europeo unito e coerente;
- Supervisionare l'attuazione e l'applicazione dell'AI Act: diventa l'organo di riferimento per l'applicazione delle regole, in particolare per i modelli di AI per scopi generali, e supporta le autorità nazionali.

L'Ufficio funge da braccio operativo per garantire che gli obiettivi strategici siano raggiunti in modo coeso. A supporto della sua azione, l'UE ha lanciato ulteriori iniziative chiave: il **Piano d'azione per l'AI continentale** (aprile 2025) e la strategia **Apply AI** (ottobre 2025). Questi piani mirano a consolidare la leadership europea nell'AI affidabile e a incrementarne l'adozione nei settori industriali e pubblici chiave.

L'approccio dell'UE all'AI è tale che, invece di vedere l'innovazione tecnologica e la regolamentazione come forze opposte, l'UE le considera interdipendenti e complementari, proponendo una "terza via" tra i modelli di altre potenze globali. La strategia europea cerca di trovare un equilibrio ponderato tra la spinta verso la competitività e la ferma protezione dei valori democratici e dei diritti fondamentali.

3.4 Il Data Act e l'EMDS

La digitalizzazione è il motore fondamentale che guida la duplice transizione dell'UEverso un settore della mobilità e dei trasporti che sia al contempo sostenibile e intelligente. Questa visione, delineata nella "Strategia per una Mobilità Sostenibile e Intelligente", mira a creare un sistema di trasporto multimodale realmente efficiente e interconnesso, in grado di supportare gli ambiziosi obiettivi del Green Deal Europeo e di un'Europa pronta per l'era digitale. La capacità di trasformare dati in informazioni fruibili è il perno su cui ruota questa trasformazione.

Per trasformare il potenziale dell'AI in un vantaggio competitivo concreto, l'ecosistema europeo deve poggiare su tre pilastri strategici: **la disponibilità di dati di alta qualità**, l'accesso a **infrastrutture di calcolo potenti** e la **presenza di competenze umane** adeguate. Senza un investimento coordinato su questi fattori abilitanti, il rischio è che l'innovazione rimanga confinata a pochi grandi attori, lasciando indietro le PMI e limitando l'impatto sistemico della trasformazione digitale.

Al centro di questa evoluzione vi è il vasto potenziale, ancora in gran parte non sfruttato, dei **dati sulla mobilità**. Questi dati rappresentano una risorsa strategica inestimabile per guidare l'innovazione, migliorare l'efficienza operativa, ridurre l'impatto ambientale e creare un sistema di trasporto realmente integrato per passeggeri e merci. Sfruttare appieno questo potenziale può portare a una pianificazione più resiliente delle infrastrutture, a un traffico più fluido, a catene logistiche più competitive e a viaggi transfrontalieri senza interruzioni.

Per sbloccare questo valore, l'UE ha messo in campo due iniziative strategiche complementari. La prima è il **Data Act**, un quadro legislativo orizzontale che stabilisce regole eque per l'accesso e l'utilizzo dei dati in tutti i settori economici. La seconda è lo **EMDS**, un'iniziativa settoriale mirata a superare la frammentazione specifica del panorama dei dati sui trasporti. Questa relazione analizza come la sinergia tra questi due pilastri sia cruciale per costruire un'economia dei dati europea equa, competitiva e innovativa.

L'imperativo strategico: superare la frammentazione del panorama dei dati di mobilità

La gestione attuale dei dati sulla mobilità rappresenta un significativo ostacolo strategico. Nonostante vengano generate enormi quantità di dati, spesso in risposta a requisiti legislativi dell'UE**, il panorama è caratterizzato da un'elevata frammentazione**. Questo paradosso non solo impedisce all'Unione Europea di capitalizzare appieno sulla digitalizzazione, ma rappresenta una vulnerabilità strategica che rischia di compromettere la sua competitività globale nel settore della mobilità.

Questa frammentazione si manifesta come una barriera critica all'innovazione e all'implementazione su larga scala di soluzioni basate sull'AI. Come emerso da un recente workshop sull'AI nel settore, le difficoltà nell'identificare, utilizzare e integrare dati provenienti da fonti eterogenee portano a uno spreco di risorse e ostacolano lo sviluppo di applicazioni avanzate. Molte aziende, in particolare le PMI, faticano ad accedere ai dati di cui hanno bisogno per innovare, mentre grandi aziende tecnologiche straniere utilizzano i dati europei per alimentare il proprio business.

Per affrontare questa sfida, la Strategia Europea per i Dati del febbraio 2020 ha fissato **l'obiettivo di creare un mercato unico dei dati**, garantendo che i benefici economici e sociali derivanti dal loro utilizzo siano distribuiti equamente. La necessità di un intervento strategico a livello UE è quindi imperativa per superare i silos esistenti e creare un ambiente in cui i dati possano circolare liberamente, in modo sicuro e controllato.

È in questo contesto che si inserisce la prima colonna portante della risposta dell'UE: il Data Act, un regolamento orizzontale progettato per stabilire le regole fondamentali per l'accesso e l'utilizzo dei dati in tutti i settori economici, creando le fondamenta per un ecosistema di dati più equo e competitivo.

Pilastro I: Il Data Act come Fondamento Orizzontale per l'Accesso ai Dati

Il Data Act (Regolamento sulle norme armonizzate in materia di equo accesso ai dati e di utilizzo degli stessi) rappresenta un atto legislativo intersettoriale fondamentale, destinato a plasmare il futuro digitale dell'Europa. Il suo scopo principale è creare un'economia dei dati europea che sia equa, innovativa e competitiva, stabilendo principi e linee guida applicabili a tutti i settori, inclusa la mobilità. Con la sua piena applicazione prevista a partire dal 12 settembre 2025, il regolamento mira a garantire una più equa allocazione del valore generato dai dati.

I principi fondamentali del Data Act possono essere sintetizzati come segue:

- **Controllo dell'utente**: il regolamento conferisce a consumatori e aziende un maggiore controllo sui dati generati dall'uso dei loro dispositivi connessi, come automobili, macchinari industriali o smart TV. Questo principio trasforma i dati da un sottoprodotto a un componente essenziale del prodotto stesso;
- **Obblighi di condivisione**: gli utenti acquisiscono il diritto di accedere ai dati generati e di condividerli con terze parti a loro scelta. Questo promuove una concorrenza leale, ad esempio nel mercato dei servizi post-vendita (riparazioni e manutenzione), e abilita lo sviluppo di servizi innovativi;
- **Equità contrattuale**: vengono introdotte misure specifiche per mitigare gli squilibri contrattuali e proteggere le imprese, in particolare le PMI, da clausole ingiuste imposte da controparti con una posizione di mercato significativamente più forte;
- **Interoperabilità e portabilità**: il regolamento definisce nuove norme che facilitano il passaggio tra diversi fornitori di servizi di elaborazione dati (es. cloud), con l'obiettivo di sbloccare il mercato e promuovere un quadro generale per un'interoperabilità efficiente dei dati.

I benefici pratici derivanti dall'applicazione di questi principi sono tangibili in diversi settori, come illustrato nella tabella seguente.

Settore di impatto	Beneficio concreto derivante dal Data Act
Servizi Post-Vendita	Gli utenti possono scegliere fornitori di riparazione più convenienti, prolungando la vita dei prodotti e contribuendo agli obiettivi del Green Deal.
Industria e Agricoltura	Le aziende ottengono accesso ai dati sulle prestazioni delle apparecchiature, consentendo l'ottimizzazione dei cicli operativi tramite machine learning.
Agricoltura di Precisione	Gli agricoltori possono analizzare dati in tempo reale (meteo, umidità, segnali GPS) per ottimizzare e aumentare la resa dei raccolti.
Settore Pubblico	Le amministrazioni pubbliche possono richiedere l'accesso a dati del settore privato per rispondere a emergenze pubbliche, in modo rapido, sicuro e con un onere minimo per le imprese.

Fornendo un quadro giuridico orizzontale e prevedibile, il Data Act non solo abilita, ma rende imperativa la creazione di arene settoriali come l'EMDS, dove queste nuove regole possono essere tradotte in innovazione tangibile.

Pilastro II: l'EMDS

L'EMDS è la risposta mirata e settoriale dell'UE alla sfida della frammentazione dei dati nel settore dei trasporti. È importante sottolineare che l'EMDS non è concepito come una banca dati centralizzata. Si tratta, piuttosto, di un quadro tecnico e di governance progettato per interconnettere e federare i numerosi ecosistemi di dati sui trasporti, eterogenei e spesso difficili da scoprire, che già esistono a livello nazionale e privato. L'obiettivo è rimuovere le barriere all'accesso e promuovere l'interoperabilità, basandosi sulle legislazioni intersettoriali come il Data Act.

La struttura dell'EMDS si articola attorno a componenti chiave che collaborano per creare un ambiente federato, affidabile e sicuro.

- Partecipanti e Fonti Dati: l'ecosistema include un'ampia gamma di attori. Le fonti dati provengono da domini dati esistenti dell'UE (es. ITS NAP, DTLF), da ecosistemi pubblici e privati (es. Mobility Data Space tedesco, Eona-X) e da altri spazi dati settoriali (es. energia, turismo). I partecipanti includono fornitori di dati, utenti di dati, marketplace e fornitori di servizi;
- Infrastruttura Tecnica e di Governance: il cuore operativo dell'EMDS è composto da tre elementi centrali:
  - Livello di Interconnessione (*Interlinking Layer*): definito il "nucleo" dell'EMDS, questo strato non memorizza dati ma ne facilita la reperibilità e l'accessibilità tra i vari domini, garantendo l'interconnettività tra ecosistemi esistenti ed emergenti;
  - Elementi Costitutivi (*Building Blocks)*: si tratta di componenti infrastrutturali fondamentali che forniscono le capacità tecniche per la condivisione e l'elaborazione dei dati;
  - Standard: l'adozione di standard comuni è cruciale per garantire l'armonizzazione e l'interoperabilità tecnica e semantica tra i diversi sistemi.

L'implementazione dell'EMDS promette di generare benefici significativi per tutti gli stakeholder coinvolti nel sistema della mobilità:

- Passeggeri e Viaggiatori: potranno beneficiare di un'esperienza di viaggio migliore grazie a informazioni in tempo reale più complete su traffico e ritardi, consentendo una migliore pianificazione e una maggiore integrazione multimodale;
- Stati Membri e Autorità Pubbliche: avranno accesso a dati più completi per semplificare l'elaborazione di politiche basate sull'evidenza, rafforzare la connettività transfrontaliera e prendere decisioni più consapevoli sulla pianificazione delle infrastrutture;
- Operatori di Mercato (in particolare PMI): si apriranno nuove opportunità di business per lo sviluppo di servizi innovativi. La condivisione semplificata dei dati favorirà la collaborazione tra attori pubblici e privati e consentirà di ottimizzare le operazioni, rendendole più efficienti ed economiche.

Il successo di questa ambiziosa iniziativa dipenderà intrinsecamente dalla sua capacità di integrarsi con il quadro normativo generale. È qui che il Data Act fornisce il motore giuridico necessario per trasformare la visione dell'EMDS in una realtà operativa.

Analisi delle sinergie: come il Data Act potenzia l'EMDS

La sinergia tra il quadro legislativo orizzontale del Data Act e l'iniziativa settoriale dell'EMDS è di fondamentale importanza strategica. Queste due iniziative non sono semplicemente complementari, ma creano un potente effetto moltiplicatore: il Data Act agisce come la precondizione legale che rende l'infrastruttura dell'EMDS operativamente efficace. Il Data Act fornisce le "regole del gioco" a livello di mercato, mentre l'EMDS crea l'arena specifica in cui queste regole possono essere applicate per generare valore nel settore dei trasporti.

L'interazione tra i due pilastri crea valore aggiunto attraverso diversi meccanismi:

- Fondamento Giuridico per l'Accesso: l'EMDS mira a facilitare la condivisione dei dati, ma è il Data Act a fornire la base legale e la certezza del diritto necessarie. Ad esempio, il diritto di accedere ai dati generati dai veicoli connessi, sancito dal Data Act, trasforma un principio teorico in un diritto applicabile che gli attori all'interno dell'EMDS possono esercitare per sviluppare nuovi servizi;
- Incoraggiamento alla Partecipazione: molti attori, in particolare le PMI, possono essere riluttanti a partecipare a ecosistemi di dati per timore di squilibri di potere. Le tutele del Data Act contro le clausole contrattuali abusive offrono una protezione cruciale, incoraggiando una partecipazione più ampia e diversificata all'EMDS e garantendo che anche gli attori più piccoli possano competere in modo equo;
- Abilitazione di Nuovi Servizi: il diritto di condividere i dati con terze parti, garantito dal Data Act, è il vero motore che abiliterà i casi d'uso innovativi che l'EMDS intende supportare. Servizi come la mobilità integrata (MaaS), la manutenzione predittiva basata sui dati delle prestazioni dei veicoli o i modelli assicurativi basati sull'uso dipendono direttamente da questa possibilità;
- Coerenza e Interoperabilità: costruendosi sui principi del Data Act, l'EMDS garantisce che la condivisione dei dati nel settore della mobilità sia allineata con l'approccio europeo più ampio. Questo non solo crea coerenza interna, ma facilita anche l'interoperabilità con altri spazi dati settoriali (es. energia, turismo), consentendo lo sviluppo di servizi intersettoriali, come l'ottimizzazione della ricarica dei veicoli elettrici.

Tuttavia, questa potente sinergia normativa non è di per sé sufficiente. La sua traduzione in un ecosistema fiorente si scontra con ostacoli operativi e strutturali radicati che richiedono un'analisi altrettanto strategica.

Sfide operative e ostacoli all'adozione

La transizione verso un ecosistema di dati sulla mobilità aperto e interoperabile, sebbene strategica, presenta notevoli sfide. Una visione equilibrata richiede di riconoscere questi ostacoli, poiché la loro comprensione è fondamentale per definire strategie di mitigazione efficaci e garantire che la visione del Data Act e dell'EMDS si traduca in benefici concreti. Le discussioni emerse durante il workshop sull'AI nella mobilità hanno messo in luce diverse barriere chiave.

1. Frammentazione e Interoperabilità dei Dati: nonostante l'EMDS miri a risolvere questo problema, la complessità residua a livello tecnico, semantico e legale rimane una sfida significativa. L'integrazione di dati provenienti da fonti eterogenee richiede uno sforzo collettivo per la definizione e l'adozione di standard condivisi e modelli di governance chiari, un processo che richiede tempo e collaborazione;
2. Accesso a Infrastrutture di Calcolo: lo sviluppo di applicazioni avanzate basate sui dati, in particolare quelle che utilizzano l'AI in tempo reale come la guida autonoma, richiede un accesso adeguato a calcolo ad alte prestazioni (HPC) e infrastrutture cloud/edge. Non si tratta solo di disponibilità: il loro uso deve essere proporzionato alle esigenze e user-friendly per garantire che le PMI ne traggano pieno profitto. Le "AI Factories" rappresentano un'iniziativa chiave per affrontare questa sfida;
3. Carenza di Competenze (Skills Gap): esiste un divario significativo di competenze specialistiche in ambito AI e data science. Questa carenza è particolarmente acuta tra le PMI e tra gli esperti di dominio della mobilità, i quali spesso faticano a comprendere appieno le potenzialità e i limiti delle nuove tecnologie, ostacolandone l'adozione;
4. Incentivi alla Condivisione: come dimostra l'esperienza del progetto deployEMDS, la creazione di un'infrastruttura non basta. La sfida è superare la percezione dei dati come un asset strategico da proteggere gelosamente, dimostrando che il valore generato dalla condivisione collaborativa supera quello della detenzione in silo. È fondamentale articolare chiare opportunità di creazione di valore per convincere gli attori a partecipare attivamente.

Superare queste sfide richiederà un approccio collaborativo e un sostegno mirato. L'UE sta già mettendo in campo azioni di supporto e un quadro politico evolutivo per affrontare questi ostacoli e spianare la strada verso un futuro digitale integrato.

L'addestramento e l'esecuzione di modelli di AI avanzati richiedono un'enorme potenza di calcolo. L'accesso a infrastrutture di calcolo ad alte prestazioni (HPC), connettività ad alta velocità (5G/6G) e architetture cloud/edge è quindi un prerequisito indispensabile. Per le PMI e le startup, tuttavia, il costo e la complessità di queste risorse possono rappresentare una barriera insormontabile.

L'infrastruttura deve essere non solo potente, ma anche proporzionata alle necessità e di facile utilizzo. Per affrontare questa sfida, l'UE ha lanciato l'iniziativa delle AI Factories. Questi centri non si limitano a fornire accesso alla potenza di calcolo, ma offrono un ecosistema completo di servizi pensati per le PMI:

- Supporto tecnico per l'adozione dell'AI;
- Opportunità di co-creazione con esperti;
- Programmi di up-skilling per formare il personale.

Questa combinazione di risorse tecnologiche e supporto umano è essenziale per democratizzare l'accesso all'IA e stimolare l'innovazione in tutto il tessuto economico.

Il terzo pilastro, forse il più critico, è il fattore umano. Il divario di competenze (*skills gap*) è un ostacolo maggiore, specialmente per le PMI che raramente dispongono di esperti di AI interni. Spesso manca anche una comprensione chiara delle reali possibilità e dei limiti dell'IA tra gli stessi esperti di dominio del settore trasporti. Per colmare questo divario, sono necessarie iniziative mirate di formazione e *up-skilling* della forza lavoro. Come emerso chiaramente durante il workshop europeo, i programmi più efficaci sono quelli che favoriscono un'osmosi tra mondi diversi, avvicinando gli esperti di AI e gli specialisti del settore trasporti. Solo attraverso questa collaborazione interdisciplinare è possibile sviluppare soluzioni di AI che siano tecnicamente avanzate ma anche realmente pertinenti e applicabili ai problemi specifici della mobilità e della logistica.

3.5 Direttiva NIS2 e legge di recepimento nazionale

La NIS2 è la Direttiva europea che rafforza la sicurezza delle reti e dei sistemi informativi. Classifica il settore dei trasporti come un'infrastruttura critica essenziale e impone a tutti gli operatori (gestori stradali, aziende di trasporto) di adottare misure di sicurezza adeguate e di segnalare gli incidenti gravi.

La normativa NIS2 (Network and Information Systems 2 -Direttiva UE 2022/2555), recepita in Italia con il Decreto Legislativo n. 138/2024 e entrata in vigore il 18 ottobre 2024, introduce un quadro normativo più stringente sulla cybersecurity per una serie di settori critici, compreso quello dei trasporti e della mobilità (su strada, ferroviaria, aerea, marittima e servizi logistici).

Ha impatti significativi sul settore della mobilità e dei trasporti, in particolare sotto il profilo della sicurezza informatica e resilienza operativa.

Ambito di applicazione per mobilità e trasporti

La NIS2 include il settore dei trasporti tra i settori ad alta criticità, quindi operatori e infrastrutture di trasporto pubblico e merci rientrano negli obblighi di legge se superano determinate soglie dimensionali (generalmente medio-grandi imprese) o forniscono servizi essenziali.

Anche soggetti fornitori di servizi, infrastrutture digitali o partner della supply chain ricollegabili ai trasporti possono essere soggetti indiretti agli obblighi, ad es. mediante richieste di sicurezza imposte dagli operatori principali.

Ciò significa che molte imprese e infrastrutture di questo settore rientrano nelle regole europee di cybersecurity e devono adeguarsi alle nuove norme. Settori inclusi sono:

- Trasporto aereo, ferroviario, marittimo e stradale;
- Operatori di infrastrutture critiche (es. gestione traffico, porti, aeroporti);
- Sistemi di mobilità intelligente (ITS, V2X, gestione dati in tempo reale);
- Logistica e operatori correlati potenzialmente classificati come entità "essenziali" o "importanti" a seconda di dimensione e impatto.

Obblighi di cybersecurity e gestione del rischio

La NIS2 richiede alle organizzazioni coinvolte di:

- Implementare misure di gestione dei rischi informatici e politiche di cybersecurity coerenti con la scala e la tipologia di rischi;
- Avere piani di risposta e continuità operativa per garantire resilienza in caso di attacco;
- Proteggere reti, sistemi informativi, comunicazioni e dati critici, compresi quelli di controllo del traffico e gestione infrastrutturale;
- Gestire incidenti fisici che ci possono essere nei sistemi ITS e come questi possono avere effetti su altri sistemi (e.g., notifiche ad ansfisa e CER);
- Implementare controlli di accesso avanzati e crittografia;
- Effettuare audit, test di vulnerabilità e monitoraggio continuo.

Per la mobilità e i sistemi di trasporto sempre più digitali (es. ITS, controllo ferrovia, gestione aeroportuale, veicoli connessi), questo vuol dire rafforzare tecnologie, procedure e competenze interne.

È previsto poi un obbligo di notifica rapida di incidenti significativi ai competenti *Computer Security Incident Response Team (CSIRT)* nazionali (in Italia tramite l'Agenzia per la Cybersicurezza Nazionale) entro tempistiche strette se l'incidente impatta in modo rilevante i servizi.

Il management delle entità soggette deve rispondere direttamente della conformità normativa e adottare un ruolo attivo nella cyber-governance.

Questo comporta maggiore responsabilizzazione, compresi potenziali rischi legali e sanzioni, se le organizzazioni non adottano controlli adeguati ma è fondamentale per garantire la resilienza dei servizi di mobilità e prevenire blocchi di rete o interruzioni di servizi critici.

La direttiva richiede di controllare la cybersecurity di fornitori e partner (es. IT, software, manutentori) con un impatto diretto su operatori logistici e PMI collegate. Possibile richiesta di conformità anche da parte di fornitori di livello inferiore per mantenere contratti e relazioni commerciali.

I sistemi ITS, quelli di gestione del traffico, dei controlli di volo, navigazione marittima e ferroviaria devono soddisfare standard di resilienza molto più alti rispetto al passato. La normativa impone anche di affrontare la sicurezza nelle comunicazioni real-time, critiche per la sicurezza dei passeggeri e per l'efficienza della rete.

La crescente digitalizzazione (es. veicoli connessi, ITS, gestione dati real-time) porta a una maggiore supervisione in termini di sicurezza e conformità normativa. Sistemi ITS, veicoli connessi/autonomi, controllo traffico digitale e infrastrutture di navigazione richiedono quindi particolare attenzione per proteggere dati e operatività.

Impatti pratici per operatori e imprese sono l'aumento dei costi iniziali per adeguare infrastrutture e processi alla cybersecurity, oltre a investimenti in formazione, audit, strumenti di monitoraggio e gestione del rischio. Tuttavia, la conformità può diventare un vantaggio competitivo in termini di affidabilità e fiducia del cliente.

Anche PMI che forniscono servizi o componenti a operatori maggiori possono subire l'effetto indiretto della normativa: per mantenere contratti e relazioni, potrebbero dover dimostrare standard di cybersecurity conformi.

Occorre poi considerare come le aziende non conformi siano esposte a sanzioni significative, simili a quelle GDPR, basate su fatturato globale o importi fissi elevati (Multe fino a €10 M o il 2% del fatturato globale per entità "essenziali" (trasporti inclusi se qualificati tali - Per operatori "importanti" sanzioni fino a €7 M o 1.4% del fatturato). È prevista anche la possibilità di sospensione delle attività in caso di gravi inadempienze.

In sintesi, la NIS2 ha un impatto profondo su:

- Sicurezza e resilienza dei sistemi informatici nei trasporti;
- Responsabilità ampliata per operatori, fornitori e partner (catena di fornitura);
- Adeguamenti tecnologici e gestionali con requisiti più stringenti;
- Miglioramento strutturale della cybersicurezza dell'intero comparto della mobilità.

La direttiva rappresenta quindi un salto qualitativo nella gestione dei rischi digitali per la mobilità europea e italiana, con impatti diretti su investimenti, governance e operazioni quotidiane.

3.6 Privacy e protezione dei dati personali

I sistemi di mobilità intelligente generano un volume enorme di dati personali (geolocalizzazione, video, dati biometrici), sollevando significativi rischi per la privacy. È eticamente e giuridicamente imperativo applicare i principi sanciti dal GDPR:

- *Data protection by design and by default*: la protezione dei dati deve essere integrata fin dalla progettazione;
- Minimizzazione e limitazione della conservazione: vanno raccolti solo i dati strettamente necessari per finalità legittime e conservati per il tempo minimo indispensabile.

L'AI Act europeo introduce obblighi aggiuntivi per i sistemi considerati ad alto rischio, come quelli per la gestione del traffico, imponendo una solida governance dei dati e una supervisione umana (*human oversight*). La fiducia del pubblico dipende anche dalla percezione della sorveglianza. Sistemi come i semafori intelligenti, pur offrendo benefici in termini di efficienza, possono alimentare timori di un controllo pervasivo. Per questo motivo, la trasparenza sull'uso dei dati e l'adozione di robuste misure di cybersicurezza (come richiesto dalle norme UNECE) sono condizioni non negoziabili.

Gli algoritmi di AI, se addestrati su dati storici che riflettono disuguaglianze sociali, rischiano di incorporare e amplificare tali problematiche, portando a discriminazioni sistemiche. Per analizzare e mitigare questo rischio, è utile adottare un framework strutturato come quello proposto dal National Institute of Standards and Technology (NIST), che distingue tre categorie principali di problematicità *(bias):*

1. *Bias* sistemico: radicato nelle pratiche organizzative e nelle strutture sociali in cui l'IA viene sviluppata e utilizzata;
2. *Bias* computazionale e statistico: derivante da errori sistematici nei dati (es. campioni non rappresentativi) o negli algoritmi;
3. *Bias c*ognitivo-umano: legato al modo in cui progettisti, operatori o utenti interpretano le informazioni e interagiscono con il sistema.

Gli esempi nel settore dei trasporti illustrano concretamente queste dinamiche:

- *Bias* socio-economico: uno studio sui servizi di ride-hailing a Chicago ha mostrato che gli algoritmi di prezzo dinamico tendono ad applicare tariffe più alte in aree con determinate caratteristiche demografiche, a parità di percorso, un esempio di bias sistemico e computazionale;

- *Bias* geografico e demografico: la pianificazione urbana basata esclusivamente su dati di utilizzo (es. segnalazioni via app) può sistematicamente trascurare le esigenze di aree marginali o di utenti con minor accesso tecnologico, riflettendo un bias statistico nel campionamento dei dati;
- *Bias* di genere: i modelli di mobilità delle donne sono spesso influenzati dalla percezione della sicurezza, portandole a scegliere percorsi e orari diversi. Se i dataset di addestramento non sono rappresentativi di questa eterogeneità, i sistemi di pianificazione rischiano di ignorare le loro esigenze specifiche.

Per contrastare questi rischi, è necessario un approccio di algorithmic governance. Strumenti come gli Algorithmic Impact Assessments (AIA) e l'adozione di metriche di equità *(fairness)* sono fondamentali per identificare, misurare e mitigare i *bias* in modo proattivo.

L'imperativo del controllo umano significativo (*Meaningful Human Control*)

Il concetto di *"meaningful human control"* stabilisce la necessità etica e funzionale di mantenere sempre un operatore umano consapevole, informato e in grado di intervenire efficacemente su un sistema automatizzato. Questo principio è cruciale per prevenire il fenomeno della *"moral crumple zone"*: una situazione in cui l'operatore umano diventa il capro espiatorio degli errori del sistema, pur non avendo avuto il tempo o gli strumenti per prevenirli.

Il caso del sistema Autopilot di Tesla è emblematico. Numerosi incidenti sono stati ricondotti a un'eccessiva fiducia dei conducenti nell'automazione (*overreliance*), favorita da una progettazione che non garantiva un adeguato e costante coinvolgimento del guidatore.

Questo principio etico è stato recepito a livello giuridico. L'Art. 14 dell'AI Act europeo introduce l'obbligo di human oversight per i sistemi ad alto rischio. Questa impostazione etica trova un riscontro in proposte normative avanzate, come quella delineata nel quadro giuridico italiano (ipotizzata come L. n. 132 del 23 settembre 2025), che sancirebbe che nella PA l'AI può essere usata solo come strumento di supporto, richiedendo che la decisione finale sia sempre validata da una persona fisica, che ne resta l'unica responsabile.

Questo solido quadro etico e normativo si inserisce in una più ampia strategia europea, volta a promuovere un'AI affidabile come vantaggio competitivo a livello globale.

Oltre a queste sfide di natura tecnica, infrastrutturale e umana, la transizione verso una mobilità guidata dall'AI solleva complesse questioni etiche e normative, che devono essere gestite con rigore per garantire uno sviluppo responsabile e socialmente accettabile.

La combinazione del Data Act e dello EMDS ha una portata trasformativa. Questo quadro integrato rappresenta un'opportunità unica per l'Unione Europea di affermare la propria leadership in un'economia dei dati globale, basata sui valori europei di equità, apertura e innovazione responsabile. La piena realizzazione di questa visione richiederà un impegno proattivo e coordinato da parte di tutti gli attori dell'ecosistema.

A tal fine, si formulano le seguenti raccomandazioni strategiche:

- Per le Imprese: è fondamentale avviare una valutazione proattiva delle implicazioni del Data Act sui propri modelli di business, sui flussi di dati e sulle relazioni contrattuali. Parallelamente, si consiglia di esplorare attivamente la partecipazione a iniziative pilota e progetti legati all'EMDS per acquisire esperienza pratica, sviluppare competenze e ottenere un vantaggio competitivo nel nascente mercato dei dati sulla mobilità;
- Per i Responsabili Politici: è necessario accelerare lo sviluppo e la promozione di standard comuni per garantire l'interoperabilità a livello europeo. Occorre inoltre sostenere la creazione di valore per gli attori dell'ecosistema, creando incentivi chiari per la condivisione dei dati e garantendo che i quadri normativi complementari, come l'AI Act, siano coerenti e favoriscano l'innovazione responsabile;
- Per l'Ecosistema nel suo Complesso: la collaborazione tra settore pubblico, industria e ricerca è il fattore critico di successo. Superare la frammentazione degli stakeholder e sviluppare modelli cooperativi aperti è

essenziale per affrontare sfide comuni come la carenza di competenze e la definizione di standard, creando un vantaggio competitivo unico per l'Europa.

La creazione dell'EMDS è un processo dinamico che richiederà un impegno costante e un dialogo continuo. Il forte sostegno finanziario e programmatico dell'UE, attraverso strumenti come il Programma Europa Digitale e il Meccanismo per Collegare l'Europa – Connecting Europe Facility (CEF), dimostra un chiaro impegno politico a realizzare questa visione. Questa sinergia tra legislazione e infrastruttura non è solo una strategia tecnologica, ma un vantaggio competitivo unico per l'Europa, fondato su un quadro di valori che può attrarre talenti, investimenti e guidare la prossima ondata di innovazione nella mobilità intelligente e sostenibile.

Contesto etico e privacy

L'adozione dell'AI nei trasporti deve essere guidata da un approccio "*human-centric*", che ponga al centro la dignità, la sicurezza e i diritti fondamentali della persona. Come analizzato approfonditamente da Riccardo Gentilucci, la costruzione della fiducia del pubblico e la garanzia di una legittimità sociale e giuridica per l'innovazione non sono elementi accessori, ma prerequisiti indispensabili. Questa sezione affronta i profili etici e normativi più critici che ogni sviluppatore, operatore e regolatore deve considerare.

L'imperativo etico primario è che il progresso tecnologico non comprometta, ma anzi migliori, la sicurezza di passeggeri e cittadini. Il principio di non maleficenza (primum non nocere) impone di minimizzare il rischio di incidenti causati dall'AI. Questo si traduce in approcci gestionali molto diversi:

- L'approccio prudente di Toyota: durante le Paralimpiadi di Tokyo 2021, l'azienda ha immediatamente sospeso i suoi shuttle autonomi e-Palette dopo un incidente a bassa velocità con un pedone, anteponendo la sicurezza alla sperimentazione;
- L'approccio disinvolto di Uber: la sperimentazione su strada senza adeguati controlli ha portato a un tragico incidente mortale nel 2018, evidenziando le conseguenze di una gestione del rischio inadeguata.

Un tema ampiamente dibattuto è quello dei "dilemmi di incidente inevitabile", noti come *"trolley problem"*. L'esperimento Moral Machine del Ministero delle Infrastrutture e dei Trasporti (MIT), che ha raccolto 40 milioni di decisioni da 233 Paesi, ha dimostrato l'assenza di criteri etici universali su come un veicolo dovrebbe comportarsi in tali scenari. Per superare questa impasse, la proposta più pragmatica è di ancorare il comportamento dell'AI a regole già consolidate e socialmente legittimate: un "codice della strada digitale" (*digital highway code*) basato sulle norme giuridiche esistenti, da cui l'algoritmo può discostarsi solo se strettamente necessario per evitare una collisione.

3.7 Impatti Cyber Resilience Act (CRA sulla mobilità e trasporti)

Il Cyber Resilience Act (CRA è un Regolamento UE (Regolamento (UE) 2024/2847) che introduce requisiti obbligatori di cybersecurity per i "prodotti con elementi digitali" (hardware, software, componenti con connessione di rete) immessi sul mercato europeo.

Entrato in vigore il 10 dicembre 2024, con applicazione piena prevista dal 11 dicembre 2027 e con alcune disposizioni operative già da settembre 2026 per segnalazione vulnerabilità.

Il CRA si applica a qualsiasi prodotto digitale dotato di connettività o elemento digitale che venga posto sul mercato UE. Per mobilità e trasporti include:

- Sistemi telematici di veicoli connessi;
- Componenti elettronici e sensori (IoT) installati su veicoli, infrastrutture della mobilità o logistica;
- Software di controllo, diagnostica o gestione dei dati di bordo;

- Sistemi di *infotainment* (informazione e intrattenimento) e connettività a bordo.

Tutti questi rientrano nel campo di applicazione del CRA se connessi a una rete o a un'altra macchina, sebbene alcuni prodotti già regolati da normative settoriali specifiche (ad esempio norme di sicurezza *automotive* o *aviation*) potrebbero essere esclusi o avere prescrizioni differenziate.

Il CRA prescrive una preventiva valutazione del rischio in funzione dell'architettura del sistema, in modo da poter valutare con oggettività l'impatto della vulnerabilità sul prodotto e quindi sul sistema. Al contempo però gli operatori hanno l'opportunità di semplificare molto la catena di fornitura, andando a classificare i sistemi.

Sicurezza by design e requisito "*secure-by-default*"

I produttori di sistemi digitali che si integrano nei trasporti dovranno:

- Progettare e sviluppare componenti digitali con sicurezza integrata fin dall'inizio;
- Garantire che i sistemi non presentino vulnerabilità note al momento del rilascio;
- Prevedere aggiornamenti di sicurezza per l'intero ciclo di vita previsto del prodotto (almeno 5 anni).

Ciò potrebbe richiedere revisione di processi di sviluppo, test più rigorosi e investimenti in cybersecurity specializzata. Per quanto riguarda la gestione vulnerabilità e reporting, dall'11 settembre 2026, i fabbricanti dovranno notificare vulnerabilità sfruttate attivamente e incidenti di sicurezza alle autorità competenti (inclusa ENISA).

In aggiunta a quanto sopra è richiesto una valutazione iniziale delle vulnerabilità, atto a certificare l'assenza di vulnerabilità sfruttabili sul dispositivo e il successivo monitoraggio per tutto il ciclo di vita del prodotto.

Per infrastrutture critiche o servizi di trasporto, questo significa un monitoraggio continuo e risorse dedicate per soddisfare i requisiti di *reporting* tempestivo. Nel settore trasporti (specialmente ferroviario, marittimo e infrastrutture smart), i sistemi hanno cicli di vita lunghi (10–40 anni), sono estremamente complessi e spesso vecchi, non sono stati progettati con cybersecurity integrata.

Ciò comporta difficoltà per adeguare prodotti esistenti alle nuove norme del CRA senza ritiro o aggiornamenti radicali. Per questo motivo, alcune associazioni del settore chiedono chiarezza sull'applicabilità retroattiva (p. es., escludere prodotti già in servizio).

Il CRA può aumentare costi di conformità per produttori e fornitori, esigenza di cybersecurity testing e certificazioni, impegni organizzativi per *governance* del rischio e gestione delle vulnerabilità. Questi costi possono essere significativi soprattutto per PMI o fornitori di componentistica per il settore trasporti. In pratica, il CRA rafforza il quadro della sicurezza digitale applicata a prodotti e componenti, mentre la NIS2 richiede misure di sicurezza organizzative e di sistema più ampie per operatori diretti nei trasporti.

Il CRA comporterà una trasformazione profonda nella progettazione, produzione e manutenzione di prodotti digitali utilizzati nella mobilità e nei trasporti, spingendo verso standard di sicurezza molto più elevati. Ciò rappresenta un'occasione per aumentare resilienza, affidabilità e fiducia nei sistemi connessi, ma richiede anche adeguati investimenti in competenze, processi e *governance* della sicurezza all'interno delle organizzazioni operanti nel settore.

Con l'evoluzione delle minacce informatiche, l'Unione europea ha adottato misure significative per rafforzare la sicurezza informatica in tutti i suoi Stati membri. Elemento centrale di questo impegno è il Sistema europeo di certificazione della sicurezza informatica basato su criteri comuni 'EUCC (European Common Criteria), promosso dall'Agenzia dell'Unione europea per la cibersicurezza (European Union Agency for Cybersecurity – ENISA). Pubblicato all'inizio del 2024, l'EUCC mira a creare un parametro di riferimento unificato per la sicurezza dei prodotti e servizi ICT (tecnologie dell'informazione e della comunicazione).

Il primo schema lanciato nell'ambito del quadro ENISA, l'EUCC, si rivolge ai prodotti ICT come hardware, software e componenti. Avviato il 31 gennaio 2024, questo schema istituisce un processo di valutazione strutturato e

trasparente per consentire ai fornitori di ICT di certificare le funzionalità di sicurezza informatica dei loro prodotti. Alcune di queste funzionalità possono includere l'autenticazione degli utenti, la crittografia, la sicurezza di rete, la sicurezza del software e il controllo degli accessi.

L'EUCC è volontario e si basa sul quadro di valutazione dei criteri comuni SOG-IS, già utilizzato da 17 Stati membri dell'UE. L'EUCC fa parte del CRA, che si concentra sulla sicurezza della raccolta, dell'archiviazione e del trasferimento dei dati in tutta l'UE. Il CRA includerà in futuro altri componenti come il cloud computing (EUCS) e le reti mobili 5G (EU5G). La certificazione europea di cybersicurezza vuole fornire una certificazione unificata riconosciuta in tutta l'UE. L'obiettivo è semplificare l'accesso al mercato, ridurre i costi e consentire a sviluppatori e fornitori di servizi di raggiungere un pubblico più ampio con un'unica certificazione.

Una volta entrato in vigore, ogni Paese UE avrà l'autorità di rilasciare certificazioni di sicurezza informatica ai sensi del Regolamento europeo sui servizi informatici (EUCC). I certificati saranno riconosciuti uniformemente in tutta l'Unione. Il risultato sarà un quadro normativo molto più semplice per i produttori. L'EUCC mira a garantire che i prodotti e i servizi ICT soddisfino standard di sicurezza uniformi, con l'obiettivo finale di proteggere le infrastrutture critiche e le informazioni sensibili. L'Agenzia ENISA ha anche condotto uno studio di fattibilità sui requisiti EUCC per AI. Questi sforzi riflettono una strategia più ampia volta a coprire diversi ambiti tecnologici e ad affrontare le emergenti sfide in materia di cybersicurezza.

3.8 Le norme e gli standard per l'automotive e l'AI

Governi, enti di normazione e case automobilistiche stanno collaborando per creare un quadro di regole e standard tecnici in grado di garantire un livello minimo di sicurezza per tutti.

I principali standard di cybersecurity automotive oggi rilevanti in UE e a livello globale sono UNECE R155, UNECE R156 e ISO/SAE 21434.

UNECE R155 – Cyber Security Management System (CSMS)

Regolamento ONU vincolante per l'omologazione dei veicoli (UE inclusa) che impone ai costruttori di adottare un Sistema di Gestione della Cybersecurity.

Il suo obiettivo è garantire che i veicoli siano protetti contro le minacce cyber lungo tutto il ciclo di vita, con focus su governance, processi e organizzazione. Destinatari sono gli OEM (costruttori).

Requisiti chiave sono l'implementazione di un CSMS aziendale, l'identificazione e gestione dei rischi cyber, la protezione dei veicoli in fase di progettazione, in produzione, in esercizio e post-produzione.

Finalizzata alla gestione di minacce, vulnerabilità e incidenti con coinvolgimento della supply chain.

Tempistiche di applicazione:

- Dal 2022: obbligatorio per nuove omologazioni di tipo;
- Dal 2024: per tutti i veicoli nuovi immessi sul mercato UE.

UNECE R156 – Software Update Management System (SUMS)

Regolamento ONU che disciplina la gestione sicura degli aggiornamenti software dei veicoli, inclusi gli Over-The-Air.

Il suo obiettivo è garantire che gli aggiornamenti software siano sicuri. non compromettano la sicurezza funzionale o cyber e siano tracciabili e verificabili. Il focus è su aggiornamenti software e *lifecycle management* (gestione a vita intera). Destinatari sono OEM e fornitori software.

Requisiti chiave sono l'implementazione di un SUMS di controllo di integrità del software, autenticità degli aggiornamenti, gestione del rischio cyber legato agli *update*, documentazione e *logging* degli aggiornamenti, protezione contro *update* non autorizzati.

Tempistiche di applicazione: obbligatorio insieme a R155 per l'omologazione.

ISO/SAE 21434 – Road Vehicles – Cybersecurity Engineering

Standard internazionale tecnico (non regolatorio) che definisce come progettare e sviluppare veicoli e componenti cyber-sicuri.

Il suo obiettivo è integrare la cybersecurity nel processo di engineering automotive. Focus sono i metodi tecnici e ingegneristici. Destinatari sono OEM, Tier-1, Tier-2, sviluppatori HW/SW.

Requisiti chiave sono la Cybersecurity by design, Threat Analysis and Risk Assessment, requisiti di sicurezza cyber, progettazione, verifica e validazione, gestione vulnerabilità post-produzione, integrazione con ISO 26262 (safety).

L'applicazione non è obbligatoria per legge, ma di fatto necessaria per dimostrare conformità a R155/R156.

Confronto sintetico

Norma	**UNECE R155**	**UNECE R156**	**ISO/SAE 21434**
Tipo	Regolamento	Regolamento	Standard
Obbligatorietà UE	SI	SI	No (ma essenziale)
Ambito	Cybersecurity veicolo	Aggiornamenti software	Ingegneria cybersecurity
Approccio	Gestione / governance	Gestione update	Tecnico / progettuale
Ciclo di vita	Completo	Software lifecycle	Completo
Supply chain	✓	✓	✓(dettagliato)

Questi standard sono oggi centrali per veicoli connessi, autonomi ed elettrici, e rappresentano anche la base di allineamento con il CRA europeo. In sostanza, normative come UN R155 e ISO/SAE 21434 sono risposte dirette alle minacce di compromissione delle reti e di iniezione di firmware malevolo.

Infine, la norma **ISO/IEC 42001:2023** (spesso citata come ISO 42000 o ISO 42001) è il primo standard internazionale che definisce i requisiti per un Sistema di Gestione dell'AI (AIMS - AI Management System).

In sintesi, fornisce alle organizzazioni un quadro strutturato per sviluppare, implementare, mantenere e migliorare continuamente l'uso dell'AI, garantendo etica, trasparenza, sicurezza e responsabilità. Il suo scopo è supportare le aziende nell'adozione responsabile dell'AI, gestendo rischi e opportunità, con l'obiettivo di creare fiducia nell'uso dell'AI, assicurando che i sistemi siano etici, sicuri e trasparenti.

Essa si rivolge a qualsiasi organizzazione, indipendentemente dalle dimensioni, che sviluppa o utilizza tecnologie AIe e le aiuta a prepararsi alle normative attuali e future, come l'AI Act dell'Unione Europea. Definisce chiaramente ruoli e responsabilità nell'uso dell'AI ed identifica e mitiga i rischi specifici legati all'AI, aumentando così la fiducia di clienti e stakeholder.

3.9 Il contesto normativo nazionale

La legislazione nazionale sugli ITS

Solo da qualche anno gli ITS sono stati considerati strategici per la gestione della mobilità a livello Europeo con l'emanazione della **Direttiva europea 2010/40/UE** sul "*Quadro generale per la diffusione dei sistemi di trasporto intelligenti nel settore del trasporto stradale e nelle interfacce con altri modi di trasporto*".

L'Italia ha recepito la Direttiva con l'Art.8 del Decreto-legge del 18 ottobre 2012 n. 179, e con il **Decreto del 1° febbraio 2013** del Ministero delle Infrastrutture e della Mobilità Sostenibili sulla "*Diffusione dei sistemi di trasporto intelligenti (ITS) in Italia*".

La Commissione europea ha, inoltre, pubblicato cinque **Regolamenti Delegati**, che integrano la **Direttiva 2010/40/UE** e che pertanto costituiscono norme comunitarie da rispettare nel momento in cui, come avvenuto, l'Italia ha recepito la Direttiva 2010/40/UE. Tali Regolamenti Delegati riguardano:

- Il servizio di chiamata di emergenza (eCall) (Regolamento n. 305/2013 del 26/11/2012);
- I servizi d'informazione per aree di parcheggio sicure per gli automezzi pesanti e i veicoli commerciali (Regolamento n. 885/2013 del 15/5/2013);
- I dati e le procedure per la fornitura di informazioni minime universali di traffico gratuite per la sicurezza stradale (Regolamento n. 886/2013 del 15/5/2013);
- I servizi di informazione sul traffico in tempo reale (Regolamento n. 962/2015 del 18/12/2014);
- I servizi di informazione sulla mobilità multimodale (Regolamento n. 1926/2017 del 31/5/2017).

La continuità dell'azione legislativa dimostra la rilevanza strategica del settore ITS per l'UE e per il nostro Paese.

Dopo il recepimento della Direttiva 2010/40/UE, nel 2014 in Italia è stata adottato il **Piano d'Azione ITS Nazionale** che riprende i contenuti della Direttiva UE e definisce, sulla base di 4 settori prioritari della Direttiva stessa, una serie di azioni prioritarie alla base dello sviluppo e degli ITS in Italia.

Con **Decreto del 26 gennaio 2026** pubblicato sulla Gazzetta Ufficiale n.40 del 18-2-2026, il Ministero delle Infrastrutture e dei Trasporti, di concerto con il Ministero dell'Interno e di quello dell'Università e della Ricerca ha **recepito la direttiva 2023/2661/UE del 22 novembre 2023**, che modifica la direttiva 2010/40/UE sul quadro generale per la diffusione dei sistemi di trasporto intelligenti nel settore del trasporto stradale e nelle interfacce con altri modi di trasporto.

Il MIT, ai sensi dell'art. 12 del citato Decreto del 26 gennaio 2026 pubblicato sulla Gazzetta Ufficiale n.40 del 18-2-2026, dovrà comunicare con cadenza triennale alla Commissione europea la relazione sull'attuazione della direttiva 2661/2023 UE, nonché sulle attività e sui progetti nazionali principali riguardanti i settori prioritari e la disponibilità dei dati e dei servizi di cui agli allegati III e IV della direttiva.

Inoltre, il MIT dovrà adottare quanto prima il **nuovo Piano nazionale di azione sugli ITS** con orizzonte temporale quinquennale, anche in base ai risultati del programma di lavoro della Commissione europea e che dovrà necessariamente prestare attenzione al nuovo quadro integrato dei sistemi ITA e delle loro interazioni con le applicazioni AI anche agentica nonché garantire la cybersicurezza delle infrastrutture e sistemi critici di trasporto, mobilità e logistica.

Normativa AI per mobilità e trasporti in Italia

La normativa italiana sull'AI, con un focus su mobilità, trasporti e ambiti connessi. In Italia la disciplina AI si compone principalmente di:

- Normativa Europea principale: AI Act (Regolamento UE 2024/1689), principale quadro giuridico europeo sull'IA, applicabile direttamente in tutti gli Stati membri e già discusso precedentemente;
- Nuova legge nazionale sull'AI (Legge n. 132/2025) in vigore da ottobre 2025.

L'Italia ha approvato infatti la prima normativa organica nazionale sul tema – Legge 132/2025, che completa e allinea l'attuazione dell'AI Act con regole e principi propri del contesto italiano.

Questa legge quindi non sostituisce l'AI Act europeo, ma lo integra e declina a livello nazionale principi, obblighi e regole, con alcune specificità italiane.

La legge italiana pone come valori fondamentali:

- Centralità e dignità della persona nell'uso dell'AI;
- Trasparenza e responsabilità umana nelle decisioni automatizzate;
- Protezione dei diritti fondamentali (privacy, non discriminazione, sicurezza dei dati).

Riprendendo l'approccio europeo, la legge nazionale considera e richiama le categorie di rischio dell'AI Act:

- Sistemi vietati;
- Sistemi ad alto rischio;
- Sistemi a rischio limitato o minimo.

Obblighi e novità principali introdotti dalla legge sono:

- Trasparenza e informazione: chi utilizza sistemi AI deve assicurare informazione chiara e documentata su scopo, funzioni e risultati (ad es. nei servizi al pubblico o nei contratti con utenti);
- Human oversight (supervisione umana): le decisioni critiche non possono essere completamente automatizzate senza supervisione umana, specialmente in contesti ad alto rischio — rilevante per la gestione dei trasporti intelligenti o veicoli autonomi;
- Governance e responsabilità aziendale: le imprese devono istituire strutture interne di governance dell'AI, definire ruoli e responsabilità per la gestione dei rischi legali e sociali, e documentare accuratamente ogni fase di sviluppo e impiego dei sistemi AI.

La legge introduce anche nuove fattispecie di reato e sanzioni sia amministrative sia penali (es. uso illecito dell'AI o diffusione di contenuti generati/manipolati in modo dannoso, come deepfake).

Inoltre ai lavoratori deve essere comunicato e garantito come e quando sistemi di AI sono impiegati nel loro lavoro. Questo può riguardare anche l'uso di AI in servizi di mobilità erogati dal settore pubblico o da operatori privati.

Implicazioni specifiche per mobilità e trasporti

Sebbene la legge italiana non contenga un capitolo "mobilità" esplicito, gli obblighi generali su AI si applicano pienamente anche in questo settore, in particolare:

Sistemi di guida autonoma e ADAS: qualsiasi funzione di guida automatizzata che influisce su sicurezza e decisioni di movimento rientra negli ambiti "alto rischio" del AI Act e quindi soggetta a valutazioni di conformità, test, monitoraggio continuo e trasparenza.

ITS: sistemi che utilizzano AI per gestione del traffico, predizione del flusso veicolare, ottimizzazione di semafori o percorsi intelligenti devono essere progettati con requisiti di sicurezza, robustezza e supervisione umana. Questi stessi sistemi rientrano nei modelli di governance e responsabilità previsti dalla legge nazionale.

Servizi digitali di mobilità e piattaforme: algoritmi che gestiscono servizi MaaS, ottimizzazione delle flotte, pricing dinamico o raccomandazioni agli utenti, devono rispettare trasparenza, diritti degli utenti e controllo umano.

Dati, privacy e sicurezza: essendo l'AI fortemente basata su dati, le regole italiane e europee si intrecciano con GDPR e con i requisiti di trasparenza della legge nazionale: gli utenti devono essere informati sull'uso dei loro dati e su come gli algoritmi influenzano servizi e decisioni.

Tempistiche e attuazione

L'AI Act europeo ha scadenze progressive per l'adeguamento dei sistemi AI, con obblighi più stringenti per quelli ad alto rischio che diventano pienamente applicabili entro 36 mesi dall'entrata in vigore. La Legge 132/2025 prevede però deleghe al Governo per adottare decreti attuativi su aspetti come:

- Trattamenti dati;
- Responsabilità civile e penale;
- Standard tecnici specifici.

Ci sono poi normative e regolamenti settoriali collegati all'AI nei trasporti a partire dai già discussi Regolamenti e strategie ITS, dove è in corso il recepimento dell'aggiornamento della direttiva sui ITS che include ora esplicitamente tecnologie digitali e dati in tempo reale, inclusa l'AI nel quadro della mobilità connessa e autonoma.

Regolamenti amministrativi specifici (es. ART)

Autorità di regolazione dei Trasporti e altre autorità competenti stanno adottando regole interne sull'uso di strumenti di AI generativa e algoritmi per le proprie attività di controllo, supervisione e regolazione dei mercati (es. regolamento interno sull'uso di AI generativa da parte dell'Autorità di Regolazione dei Trasporti).

L'AI in mobilità viene infatti vista non solo come tecnologia ma come servizio critico con requisiti normativi specifici:

Servizi TPL e ottimizzazione: pianificazione percorsi, ottimizzazione flotte, previsione domanda e offerta tramite algoritmi di AI devono rispettare obblighi di trasparenza e governance.

Veicoli autonomi e sistemi assistiti: la guida autonoma e gli ADAS saranno soggetti a standard di sicurezza europei e requisiti AI-Act integrati nel Codice della Strada e regolamenti specifici (con supervisione umana).

Gestione dati e interoperabilità: l'uso dei dati di mobilità per piattaforme interoperabili deve rispettare privacy GDPR, AI Act e principi nazionali di correttezza, sicurezza e trasparenza.

In sintesi:

Elemento normativo	Ambito	Rilevanza per mobilità/trasporti
AI Act (UE)	Regolamento europeo	Principale riferimento, obblighi per AI nei trasporti
Legge italiana n. 132/2025	Normativa nazionale	Complementa e attua AI Act, trasparenza, responsabilità, controllo umano
Normative ITS e regolamenti	Settore trasporti	Applicazioni specifiche (autonomi, gestione traffico, dati)
Regole ART e PA	Atti amministrativi	Uso AI generativa e algoritmi nel controllo settoriale

Quadro normativo integrato per la cybersecurity nei trasporti

Il settore dei trasporti è al centro di una rete normativa europea in rapida evoluzione, dove regolamenti sulla cybersecurity, sull'AI e sulla resilienza digitale convergono creando obblighi sovrapposti per operatori, costruttori e gestori di infrastrutture. Le sezioni seguenti descrivono i principali strumenti normativi nazionali e la loro applicazione specifica al settore dei trasporti.

L'architettura di difesa integrata descritta nelle sezioni precedenti non opera in un vuoto istituzionale: la sua progettazione e implementazione sono vincolate da un quadro regolatorio europeo che ne definisce requisiti minimi, scadenze e responsabilità.

Appare opportuno che questa sezione integri i già descritti principali strumenti normativi europei che disciplinano la cybersecurity e l'AI nel settore trasporti con quanto previsto a livello nazionale in maniera da presentare una disamina completa e che possa essere di reale aiuto per l'applicazione diretta al settore degli ITS: dal quadro

regolatorio orizzontale (NIS2, AI Act, Cyber Resilience Act) agli standard settoriali (IEC 62443, UNECE R155/R156), fino alle strategie di compliance integrata e al ritorno dell'investimento della convergenza AI-cybersecurity.

Come si è descritto in questo capitolo, gli operatori del settore trasporti si confrontano oggi con un quadro regolatorio europeo stratificato e interconnesso, nel quale la cybersecurity non è più oggetto di una singola disciplina settoriale, ma il risultato della convergenza di normative operanti su piani distinti e complementari. A livello di entità e governance organizzativa, la NIS2 (Dir. (UE) 2022/2555) impone misure di gestione del rischio e obblighi di notifica; a livello di prodotto, il Cyber Resilience Act (CRA, Reg. (UE) 2024/2847) introduce requisiti di sicurezza by design, gestione delle vulnerabilità e marcatura CE per i prodotti con elementi digitali; a livello di AI, il AI Act Act (Reg. (UE) 2024/1689) stabilisce obblighi differenziati per i sistemi ad alto rischio, categoria in cui ricadono specificamente i sistemi AI per la gestione del traffico stradale e ferroviario (Annex III, Punto 2) e i componenti di sicurezza dei veicoli (Annex I, Section B).

A questi tre pilastri orizzontali si aggiungono normative settoriali specifiche: il regolamento UNECE R155 per la cybersecurity dei veicoli (CSMS), obbligatorio per tutti i nuovi veicoli M, N e O in Europa dal luglio 2024; lo standard IEC 62443 per la sicurezza dei sistemi di automazione e controllo industriale (IACS), la cui edizione 2.0 della parte 2-1 (agosto 2024) ha introdotto un modello di maturità ristrutturato; la specifica tecnica CENELEC CLC/TS 50701 per il dominio ferroviario, in evoluzione verso lo standard internazionale IEC 63452 la cui pubblicazione è prevista a luglio 2026 e che colma il gap tra IEC 62443 e le specificità del dominio ferroviario; il regolamento EASA (UE) 2023/203 per la sicurezza informatica nell'aviazione e U-space, applicabile dal 22 febbraio 2026.

Infine, la legislazione nazionale italiana integra e in alcuni casi amplia il perimetro europeo, con il D.Lgs. 138/2024 (recepimento NIS2) e la Legge 132/2025 (prima legge nazionale sull'AI nell'Unione Europea).

La complessità di questo mosaico normativo impone un'analisi preliminare delle gerarchie applicative. L'articolo 4 della NIS2 stabilisce il principio di lex specialis: qualora atti giuridici settoriali dell'Unione impongano ai soggetti essenziali o importanti l'adozione di misure di gestione del rischio di cybersicurezza o la notifica di incidenti significativi, e tali requisiti siano «al meno equivalenti per effetto» a quelli della NIS2, le disposizioni di quest'ultima non si applicano. Le Linee Guida della Commissione Europea del settembre 2023 sulla valutazione di tale equivalenza hanno fissato un'asticella elevata: l'atto settoriale deve coprire hardware, firmware e software, richiedere un approccio all-hazards comprensivo di minacce naturali e cibernetiche, includere la sicurezza della catena di approvvigionamento, la crittografia e il controllo degli accessi, e prevedere un regime di notifica multi-livello (24 ore, 72 ore, un mese).

NIS2 e il recepimento italiano: D.Lgs. 138/2024

Tra le normative che compongono questa rete, la Direttiva NIS2 costituisce il pilastro centrale per la cybersecurity delle infrastrutture critiche, con implicazioni dirette per gli operatori di trasporto italiani.

Il Decreto Legislativo 4 settembre 2024, n. 138, entrato in vigore il 16 ottobre 2024, è una delle trasposizioni più complete della NIS2 nell'Unione Europea. Il decreto attribuisce all'Agenzia per la Cybersicurezza Nazionale (ACN) il ruolo di autorità nazionale competente NIS (Art. 10 D.Lgs. 138/2024) e di CSIRT Italia (Art. 15), mentre il Ministero delle Infrastrutture e dei Trasporti (MIT) è designato come autorità settoriale per i trasporti (Art. 11). Questa architettura istituzionale assicura sia una governance centralizzata della cybersecurity nazionale sia una supervisione settoriale specializzata per ciascun dominio critico.

I trasporti figurano nell'Allegato I del decreto come settore ad alta criticità, articolato in quattro sotto-settori:

- Aereo: vettori aerei, gestori aeroportuali, controllo traffico aereo (per l'analisi dell'enforcement ACN e l'impatto operativo sugli operatori di trasporto italiani, si veda il §5.4.4 — ACN e l'enforcement NIS2 nei trasporti);
- Ferroviario: imprese ferroviarie, gestori infrastruttura, ERTMS;
- Marittimo e fluviale: compagnie di navigazione, enti di gestione portuale, VTS;
- Stradale: autorità che gestiscono ITS, operatori di pedaggi.

Un aspetto particolarmente rilevante per il contesto italiano è **l'Allegato IV del decreto**, che costituisce un'estensione tutta italiana rispetto al testo della Direttiva europea. L'Allegato IV include esplicitamente gli operatori del Trasporto Pubblico Locale (TPL) come soggetti importanti, indipendentemente dalle dimensioni dell'impresa, qualora rientrino nel campo di applicazione del D.Lgs. 175/2016 (TUSP, Testo Unico in materia di Società a Partecipazione Pubblica). **Questa disposizione estende in modo sostanziale il perimetro NIS2 a un'ampia platea di aziende di trasporto pubblico locale, incluse le PMI partecipate da enti locali**, configurando un onere di compliance che altre nazioni europee non hanno previsto per operatori di analoga dimensione.

Le specifiche tecniche di attuazione sono definite dalla Determinazione del Direttore Generale dell'ACN n. 379907 del 18 dicembre 2025, applicabile dal 15 gennaio 2026 (che sostituisce la precedente Det. 164179 del 14 aprile 2025). La determinazione articola le misure di sicurezza baseline in quattro allegati tecnici: l'Allegato 1 prevede 37 misure e 87 requisiti per i soggetti importanti; l'Allegato 2 ne prevede 43 con 116 requisiti per i soggetti essenziali; gli Allegati 3 e 4 definiscono rispettivamente gli incidenti significativi baseline per soggetti importanti (IS-1, IS-2, IS-3) e per soggetti essenziali (IS-1, IS-2, IS-3, IS-4, quest'ultimo relativo ad accesso non autorizzato o abuso di privilegi). Le misure sono sviluppate in coerenza con il Framework Nazionale per la cybersecurity e la Data Protection e richiedono il coinvolgimento diretto degli organi di amministrazione e direttivi ai sensi dell'Art. 23 del D.Lgs. 138/2024.

Il regime di notifica degli incidenti, disciplinato dall'Art. 25 del D.Lgs. 138/2024, prevede un meccanismo a tre livelli: pre-notifica al CSIRT Italia entro 24 ore dall'evidenza dell'incidente, notifica completa con valutazione di gravità e impatto entro 72 ore, e relazione finale comprensiva di root cause analysis, misure di attenuazione e valutazione dell'impatto transfrontaliero entro un mese dalla notifica. Per le entità strategiche nazionali incluse nel Perimetro di Sicurezza Nazionale Cibernetica (PSNC, D.L. 105/2019), il termine di pre-notifica è ulteriormente ridotto a un'ora, configurando un doppio regime che richiede agli operatori di trasporto strategici capacità di rilevamento e comunicazione nettamente più avanzate.

La maturità della cybersecurity nel settore trasporti presenta marcate disparità tra sotto-settori, come documentato dal report ENISA NIS360 2024 pubblicato nel marzo 2025 — la prima valutazione sistematica della maturità cybersecurity per i sotto-settori NIS2. L'aviazione si colloca nel livello più alto di maturità, beneficiando di decenni di regolamentazione safety e security consolidata (EASA, ICAO). Il settore ferroviario si posiziona al limite della «rischio zone», con una transizione digitale rapida (ERTMS, FRMCS) non accompagnata da una corrispondente maturità cyber. Il marittimo si trova nella «rischio zone» — una delle motivazioni alla base della scelta di focalizzare l'esercitazione paneuropea Cyber Europe 2026 proprio sui settori ferroviario e marittimo. Il trasporto stradale registra un punteggio «notably lower», risultando il sotto-settore meno maturo tra i quattro: la frammentazione degli operatori e l'assenza di standard specifici di cybersecurity contribuiscono a questa valutazione.

Strategia Nazionale di Cybersicurezza 2022-26

La "**Strategia Nazionale di Cybersicurezza 2022-26**" emessa dall'Agenzia per la Cybersicurezza Nazionale (ACN) – vedi https://www.acn.gov.it/portale/strategia-nazionale-di-cybersicurezza) mira a rendere il Paese più sicuro e resiliente di fronte alle nuove sfide poste dall'incessante sviluppo tecnologico e dalla trasformazione digitale.

Per fare questo, la Strategia individua tre **obiettivi**:

- **Protezione**: la protezione degli asset strategici nazionali basata su un approccio sistemico, orientato alla gestione del rischio, tramite il mantenimento di un quadro normativo coerente e l'applicazione di misure, strumenti e controlli di sicurezza;
- **Risposta**: la risposta a minacce, incidenti e crisi di natura cibernetica attraverso l'impiego delle capacità nazionali di monitoraggio, rilevamento, analisi e risposta, nonché l'attivazione delle procedure di allertamento con il coinvolgimento di tutti gli attori dell'ecosistema nazionale di cybersicurezza;
- **Sviluppo**: lo sviluppo consapevole e sicuro di tecnologie digitali, il sostegno alla ricerca e il rafforzamento della competitività industriale, per rispondere alle esigenze del mercato attraverso l'azione sinergica di istituzioni, accademia, centri di eccellenza e imprese.

e due **fattori abilitanti**:

- **Cooperazione**: tanto sul versante nazionale, a livello istituzionale e nel rapporto pubblico-privato, quanto in ambito internazionale, in seno a consessi europei o internazionali, la cooperazione si rivela un fattore di fondamentale importanza per garantire la sicurezza e l'efficace implementazione delle policy;
- **Formazione e cultura della cybersicurezza:** la creazione di una solida forza lavoro tramite percorsi formativi mirati e l'innalzamento della consapevolezza dei rischi che promanano dalla dimensione digitale rappresentano elementi essenziali per innalzare i livelli di sicurezza e resilienza cibernetica del Paese.

Il Piano di Implementazione, correlato alla Strategia, trasforma obiettivi e fattori abilitanti in 82 misure da realizzare coinvolgendo tutta la Pubblica Amministrazione e – a cascata – le imprese e i cittadini.

Per raggiungere le 82 misure previste dal Piano di implementazione, le Amministrazioni responsabili dell'attuazione possono far ricorso a fondi dedicati all'attuazione della Strategia. In particolare, l a legge di bilancio per il 2023 (legge n. 197/2022) ha istituito il **fondo per l'attuazione della Strategia nazionale di cybersicurezza**, destinato a finanziare gli investimenti per il conseguimento dell'autonomia tecnologica in ambito digitale, nonché l'innalzamento dei livelli di cybersicurezza dei sistemi informativi nazionali, e il **fondo per la gestione della cybersicurezza**, volto ad assicurare copertura economica alle attività di gestione operativa.

È l'Agenzia per la cybersicurezza nazionale ad occuparsi della rilevazione dei **fabbisogni finanziari** delle Amministrazioni responsabili dell'attuazione delle misure. L'Agenzia, di concerto con il Ministero dell'Economia e delle Finanze, propone l'adozione di uno o più provvedimenti per la ripartizione dei fondi. L'ACN, a cui è affidato un ruolo di impulso e coordinamento, assicura le necessarie attività volte al monitoraggio periodico dello stato di attuazione della Strategia.

AI Act e classificazione dei trasporti ad alto rischio

Se la NIS2 disciplina la sicurezza delle reti e dei sistemi informativi a livello di entità, l'AI Act interviene su un piano complementare: la regolamentazione dei sistemi di AI in funzione del livello di rischio.

Il Regolamento (UE) 2024/1689 sull'AI (AI Act), in vigore dal 1° agosto 2024, introduce il primo framework normativo organico per i sistemi AI nell'Unione Europea. A differenza della NIS2 che opera a livello di entità, l'AI Act si concentra sul sistema AI in sé, classificandolo in base al livello di rischio. Per il settore dei trasporti, la norma prevede un'implementazione graduale (phased enforcement) che distingue tra sistemi AI per la gestione del traffico e sistemi AI integrati nei veicoli, con tempistiche e obblighi differenziati.

L'implementazione dell'AI Act segue quattro fasi successive: dal 2 febbraio 2025 sono operativi i divieti sulle pratiche AI inaccettabili (Art. 5) e l'obbligo di AI literacy (Art. 4); dal 2 agosto 2025 si applicano gli obblighi per i modelli GPAI (Artt. 51-56) e il regime sanzionatorio; dal 2 agosto 2026 entrerà in vigore la disciplina per i sistemi ad alto rischio classificati nell'Annex III, che include al Punto 2 i sistemi AI per la gestione e l'operazione del traffico stradale e ferroviario; infine, dal 2 agosto 2027 si applicheranno gli obblighi per i sistemi ad alto rischio dell'Annex I Section B, che comprende i componenti di sicurezza dei veicoli, inclusi ADAS e sistemi di guida autonoma. (per le iniziative europee di ricerca sulla conformità AI Act nei trasporti, si veda il §5.3 — Progetti EU e finanziamenti)

La **classificazione dei trasporti nell'AI Act** si articola su due livelli distinti con implicazioni operative differenti. L'Annex III, Punto 2 identifica come ad alto rischio i «sistemi AI destinati ad essere utilizzati come componenti di sicurezza nella gestione e nell'operazione delle infrastrutture digitali critiche, del traffico stradale»: questa categoria comprende i sistemi di Traffic Management Center (TMC), i sistemi di controllo semaforico intelligente, le piattaforme di gestione del traffico ferroviario e i sistemi di mobilità predittiva. L'Annex I, Section B copre invece i componenti di sicurezza dei veicoli regolamentati, ovvero i sistemi ADAS, la guida autonoma e i sistemi di frenata d'emergenza basati su AI, per i quali il regime normativo previsto dalla UNECE R155 mantiene la prevalenza sulla conformity assessment dell'AI Act.

Un elemento di forte incertezza nella pianificazione della compliance è rappresentato dalla **proposta Digital Omnibus**, presentata dalla Commissione Europea il 19 novembre 2025. La proposta prevede un meccanismo di

differimento condizionato delle scadenze per i sistemi ad alto rischio: qualora adottata, gli obblighi per i sistemi Annex III (inclusa la gestione del traffico) sarebbero applicabili sei mesi dopo la conferma della disponibilità degli standard armonizzati da parte della Commissione, con un termine ultimo (backstop) fissato al 2 dicembre 2027 anziché al 2 agosto 2026. Analogamente, per i sistemi Annex I Section B (veicoli), il termine sarebbe differito a dodici mesi dalla disponibilità degli standard, con backstop al 2 agosto 2028 invece del 2 agosto 2027. Il CEN-CENELEC JTC 21, responsabile della standardizzazione AI, ha indicato che gli standard armonizzati completi difficilmente saranno disponibili prima di dicembre 2026, rendendo probabile un effettivo slittamento delle scadenze operative.

La proposta Digital Omnibus introduce inoltre un nuovo Art. 60a specificamente rilevante per il settore dei trasporti. La disposizione proposta creerebbe una base giuridica per i fornitori di sistemi AI ad alto rischio sotto l'Annex I Section B — che **include esplicitamente i prodotti per la regolazione del traffico e della mobilità** in aviazione, strada, ferrovia, trasporto agricolo e marittimo — per condurre test in condizioni reali (real-world testing) attraverso accordi volontari tra Stati membri e Commissione. Qualora adottata, questa disposizione faciliterebbe la sperimentazione di sistemi AI per la mobilità autonoma e la gestione intelligente del traffico in un quadro regolatorio definito, riducendo l'incertezza giuridica che attualmente frena l'innovazione nel settore.

Cyber Resilience Act e prodotti digitali per i trasporti

Mentre l'AI Act regola i sistemi di AI in base alla loro classificazione di rischio, il Cyber Resilience Act completa il quadro normativo intervenendo sui prodotti con elementi digitali, dal sensore IoT alla piattaforma ITS.

Il CRA, già analizzato nel §3.3, impone requisiti specifici ai prodotti digitali utilizzati nei sistemi di trasporto. A differenza della NIS2, che opera a livello di entità imponendo obblighi organizzativi di governance e resilienza, il CRA agisce a livello di prodotto, richiedendo sicurezza by design, gestione delle vulnerabilità, SBOM (Software Bill of Materials) machine-readable e marcatura CE. **Le due normative sono complementari e operano su layer distinti**: un produttore ITS può essere simultaneamente soggetto alla NIS2 come operatore di servizio essenziale, al CRA come fabbricante di prodotti digitali e all'AI Act se tali prodotti incorporano sistemi AI ad alto rischio.

La timeline di applicazione del CRA prevede milestone ravvicinate che richiedono una pianificazione immediata da parte dei produttori di componenti ITS. L'11 giugno 2026 scade il termine per la notifica degli organismi di valutazione della conformità; il 30 agosto 2026 devono essere disponibili gli standard armonizzati orizzontali; l'11 settembre 2026 entra in vigore l'obbligo di reporting delle vulnerabilità attivamente sfruttate e degli incidenti gravi relativi ai prodotti, con notifica al CSIRT nazionale e ad ENISA entro 24 ore attraverso la Single Reporting Platform (SRP) che ENISA sta sviluppando; il 30 ottobre 2026 è la scadenza per gli standard armonizzati verticali; infine, l'11 dicembre 2027 segna la data di compliance piena per tutti gli obblighi CRA.

L'applicabilità del CRA al settore dei trasporti segue una regola cardine: i veicoli soggetti a omologazione tipo sono esclusi dal CRA e rimangono nel regime UNECE R155, mentre i componenti infrastrutturali e i dispositivi standalone sono in scope. Nello specifico, i veicoli delle categorie M, N e O (autovetture, veicoli commerciali, rimorchi) sono esclusi in quanto già coperti da R155 per la cybersecurity. I veicoli L-category (motocicli, scooter) saranno analogamente esclusi con l'estensione di R155 alla categoria L, prevista dall'11 dicembre 2027. I veicoli agricoli e forestali (categorie T, R, S) costituiscono eccezione perché non coperti da R155, ricadono pienamente nel CRA.

Standard settoriali e convergenza normativa globale

Accanto alle normative orizzontali dell'Unione europea, il quadro regolatorio per la cybersecurity nei trasporti comprende standard settoriali che operano come layer tecnico-operativo specializzato. Nel settore automotive, il Regolamento UNECE R155 stabilisce l'obbligo di un CSMS certificato per l'omologazione dei veicoli. Dal luglio 2024, il R155 è obbligatorio per tutti i veicoli nuovi delle categorie M, N e O (autovetture, veicoli commerciali, rimorchi e autobus) immessi sul mercato europeo, coprendo l'intero ciclo di vita del veicolo dalla progettazione alla dismissione. Il regolamento complementare R156 disciplina il SUMS, imponendo requisiti di validazione dell'integrità, protezione anti-rollback e tracciabilità per tutti gli aggiornamenti software, sia over-the-air (OTA) sia in officina.

Il Supplement 3 al R155, in vigore dal 10 gennaio 2025 (Reg. UE 2025/5), ha esteso in modo rilevante il perimetro di applicazione ai veicoli multistage, coinvolgendo carrozzieri, costruttori di rimorchi e produttori di autobus e coach che operano come second-stage manufacturer. Il supplemento chiarisce le responsabilità cybersecurity nella catena produttiva dal costruttore del veicolo base (base vehicle) al costruttore della carrozzeria (body builder), stabilendo che ciascun attore della catena deve assicurare che le modifiche apportate non compromettano le proprietà di cybersecurity del veicolo originale. L'estensione ai veicoli L-category (motocicli, scooter) è in corso tramite il regolamento di implementazione UE C(2025) 4842, con nuove omologazioni tipo previste dall'11 dicembre 2027 e obbligo per tutti i veicoli nuovi dall'11 giugno 2029. Lo standard ISO/SAE 21434 fornisce il framework ingegneristico strutturato a supporto della conformità R155, con una metodologia TARA (Threat Assessment and Remediation Analysis) a 9 step per la gestione dei rischi cyber nell'intero ciclo vita del veicolo.

Il quadro UNECE R155 opera nell'ambito del WP.29, il Forum mondiale per l'armonizzazione dei regolamenti sui veicoli, che comprende 54 parti contraenti. Sebbene il regolamento non sia ancora obbligatorio in tutte le giurisdizioni, si sta delineando una convergenza normativa globale sulla cybersecurity veicolare. Nell'Unione europea, il R155 è pienamente operativo per tutte le categorie M, N e O dal luglio 2024. La Cina ha adottato un approccio parallelo con lo standard nazionale GB 44495-2024, obbligatorio per le nuove omologazioni tipo dal gennaio 2026 e per tutti i veicoli nuovi dal gennaio 2028. La Corea del Sud ha emanato un regolamento nazionale CSMS con obbligo per le nuove omologazioni tipo dal 14 agosto 2025. L'India ha predisposto le bozze AIS-189 e AIS-190, derivate da R155 e R156, con un'entrata in vigore prevista indicativamente nel 2027.

Lo standard cinese GB 44495-2024 presenta differenze strutturali rispetto al R155 che i costruttori operanti su entrambi i mercati devono considerare attentamente. Mentre il R155 adotta un approccio prevalentemente orientato ai processi, valutando la maturità del CSMS dell'organizzazione, lo standard cinese pone un'enfasi marcata sulla verifica tecnica concreta, richiedendo evidenze specifiche di test e risultati di validazione. Il GB 44495-2024 introduce inoltre regole stringenti per l'estensione delle approvazioni cybersecurity tra modelli di veicoli (model extension testing), limitando la possibilità di estendere una certificazione ottenuta su un modello ad altri modelli della stessa piattaforma senza verifica supplementare. Lo standard companion GB 44496-2024 disciplina gli aggiornamenti software, analogamente al R156 in ambito UNECE. Per i costruttori europei che esportano verso la Cina, la compliance R155 non garantisce automaticamente la conformità a GB 44495-2024: è necessaria un'analisi gap e l'adeguamento alle specificità tecniche dello standard cinese.

Cybersecurity Act 2.0: la proposta di riforma della certificazione europea

L'interazione tra standard settoriali e normative orizzontali sollecita un meccanismo unificato di certificazione: la proposta di Cybersecurity Act 2.0 mira a colmare questa esigenza ridisegnando il framework europeo di certificazione della cybersecurity.

Il 20 gennaio 2026, la Commissione europea ha presentato la proposta di regolamento COM(2026) 11, denominata **Cybersecurity Act 2.0 (CSA2)**, che prevede l'abrogazione e sostituzione integrale del Regolamento (UE) 2019/881 (Cybersecurity Act originale). La proposta, attualmente in fase di procedura legislativa ordinaria (2026/0011/COD), si articola su tre pilastri portanti: la sicurezza della supply chain ICT, con un regime di valutazione dei fornitori critici che, qualora approvato, consentirebbe alla Commissione di designare fornitori ad alto rischio e disporre il ritiro dal mercato di prodotti ICT; l'espansione del framework europeo di certificazione cybersecurity (ECCF), con l'introduzione di certificati di «cyber-postura» che costituirebbero presunzione di conformità ai requisiti NIS2; e il rafforzamento del mandato di ENISA, con maggiore autonomia operativa e capacità di coordinamento cross-settoriale, incluse competenze in materia di security alerts e coordinated vulnerability disclosure.

Per il settore dei trasporti, la proposta CSA2 avrebbe un impatto diretto su molteplici dimensioni operative. Le regole sulla sicurezza della supply chain ICT, qualora adottate, si applicherebbero a tutti i settori classificati «ad alta criticità» dalla NIS2, includendo pertanto i fornitori di sistemi SCADA, ERTMS, ITS e V2X che costituiscono la catena di approvvigionamento tecnologica dei trasporti. I certificati di cyber-postura proposti potrebbero fornire agli operatori di trasporto una via preferenziale per dimostrare la conformità NIS2, semplificando l'onere di compliance per le entità soggette a molteplici regimi normativi. La proposta prevede inoltre sanzioni fino al 7% del fatturato

annuo mondiale, nettamente superiori alle sanzioni NIS2 (2% ai sensi dell'Art. 38 del D.Lgs. 138/2024) e allineate con le sanzioni AI Act per le violazioni più gravi.

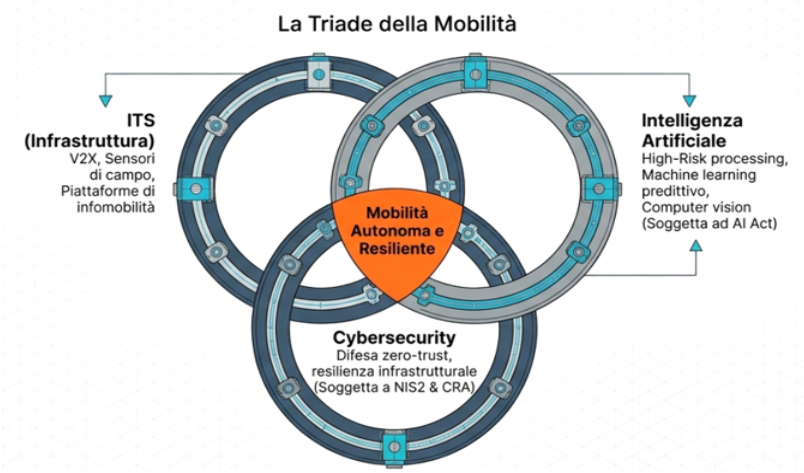
Cronologia normativa per la cybersecurity nei trasporti

Norma	Ambito trasporti	Scadenza chiave	Status
NIS2 (D.Lgs. 138/2024)	Operatori trasporto essenziali/importanti	Apr 2025 (registrazione ACN)	In vigore
EU AI Act (Reg. 2024/1689)	Sistemi AI alto rischio (Annex III, Punto 2)	Ago 2026 (conformità)	In vigore parziale
Cyber Resilience Act	Prodotti digitali per ITS	Set 2026 (obblighi fabbricanti)	Pubblicato dic 2024
UNECE R155/R156	CSMS/SUMS veicoli M, N, O	Lug 2024 (in vigore)	Obbligatorio
IEC 63452	Cybersecurity ferroviaria	Lug 2026 (previsto)	In sviluppo
L. 132/2025	Prima legge AI nazionale (Italia)	Ott 2025 (in vigore)	In vigore
eFTI Regulation	Piattaforme digitali logistica	Lug 2027 (piena obbligatorietà)	In fase attuativa

Un riferimento di rilievo per il settore ferroviario è il nuovo standard IEC 63452, attualmente in fase di finalizzazione presso il comitato TC 9/WG 49 con pubblicazione prevista per luglio 2026. Lo standard definisce requisiti specifici di cybersecurity per le applicazioni ferroviarie, colmando il gap tra la IEC 62443 (orientata all'automazione industriale generica) e le esigenze peculiari del segnalamento e del controllo ferroviario. La IEC 63452 introduce un ciclo di vita della cybersecurity allineato alle fasi CENELEC (V-model) e un approccio risk-based calibrato sulle specificità del dominio ferroviario (Rapporto Clusit 2026, p. 257).

Sul fronte della sicurezza della supply chain per i Veicoli Connessi e Autonomi (Connected and Automated Vehicles – CAV), la Commissione Europea ha pubblicato nel marzo 2026 l'ICT Supply Chain Security Toolbox dedicato ai CAV. Il toolbox fornisce linee guida operative per gli operatori del settore automotive sulla gestione dei rischi cyber lungo la catena di fornitura ICT, con particolare attenzione ai componenti software di terze parti, ai firmware e ai servizi cloud integrati nei veicoli di nuova generazione.

In sintesi e da quanto precede, la trasformazione digitale della mobilità e l'integrazione dei suoi tre pilastri ITS, AI e Cybersecurity abiliterà nel futuro un ecosistema di mobilità più efficiente, sicuro, sostenibile e resiliente ove si consideri che l'integrazione non è un'opzione tecnica, ma un pilastro di sicurezza nazionale come mostrato dalla figura seguente.



4. Architetture di sicurezza e tecnologie

4.1 Human-centric AI e transizione socio-organizzativa nella mobilità intelligente

L'introduzione crescente dell'AI nella mobilità rappresenta non solo una trasformazione tecnologica, ma anche una transizione socio-organizzativa che coinvolge operatori, decisori di policy e l'utente finale. Accanto ai benefici già evidenziati in termini di efficienza, sicurezza e sostenibilità, emerge infatti la necessità di integrare una prospettiva umanocentrica, capace di considerare l'impatto delle innovazioni sulle competenze, sulla fiducia e sulla percezione del rischio da parte delle persone che interagiscono con tali sistemi. Le applicazioni di AI, infatti, richiedono processi di accompagnamento e partecipazione consapevole degli utenti affinché il cambiamento sia produttivo.

Per questo motivo, nel contesto europeo, l'approccio alla "trustworthy AI" sottolinea come l'adozione efficace delle tecnologie intelligenti dipenda non solo dalla robustezza tecnica e dalla cybersecurity, ma anche dalla capacità di traghettare la transizione digitale attraverso percorsi di inclusione e comprensione condivisa. Nel settore della mobilità, questo si traduce nell'esigenza di affrontare un duplice digital divide: da un lato quello sociale, legato alla fiducia degli utenti verso sistemi automatizzati e servizi basati su dati; dall'altro quello organizzativo, che riguarda l'evoluzione delle competenze nelle filiere del trasporto e della logistica.

Le resistenze all'innovazione non devono essere interpretate esclusivamente come ostacoli, ma come indicatori utili per individuare bisogni formativi, criticità operative e aspetti etici ancora percepiti come incerti. In molti casi, le preoccupazioni espresse dagli operatori riflettono timori concreti legati alla trasformazione dei ruoli professionali, alla crescente complessità dei sistemi digitali e alla necessità di mantenere un controllo umano significativo nei processi decisionali automatizzati. Parallelamente, esistono percezioni distorte che associano l'automazione a una sostituzione totale del lavoro umano, senza considerare le opportunità di ridefinizione delle mansioni e di creazione di nuove competenze.

Integrare una prospettiva socio-organizzativa nella strategia di cambiamento, significa quindi rafforzare la resilienza complessiva dell'ecosistema della mobilità intelligente. Comprendere come persone e organizzazioni percepiscono e adottano l'AI consente infatti di progettare sistemi più sicuri, inclusivi e sostenibili nel lungo periodo, contribuendo a una diffusione equilibrata dell'innovazione e a una maggiore accettazione delle soluzioni tecnologiche da parte della società.

In questa prospettiva, si ricorda come i grandi processi di innovazione digitale e di automazione nella storia dei trasporti si siano sempre sviluppati in modo progressivo, attraverso fasi di adattamento tecnologico e socio-culturale. Anche le soluzioni più avanzate, infatti, esprimono il proprio potenziale solo quando vengono comprese, accettate e integrate dall'utente finale e dagli operatori del sistema: senza un percorso di accompagnamento umano

e organizzativo, il rischio è che l'innovazione rimanga confinata al piano progettuale, senza tradursi pienamente in valore per l'ecosistema della mobilità.

In questo contesto assumono un ruolo centrale gli attori di coordinamento e mediazione dell'ecosistema ITS, chiamati a facilitare il dialogo tra innovazione tecnologica, esigenze operative e aspettative sociali.

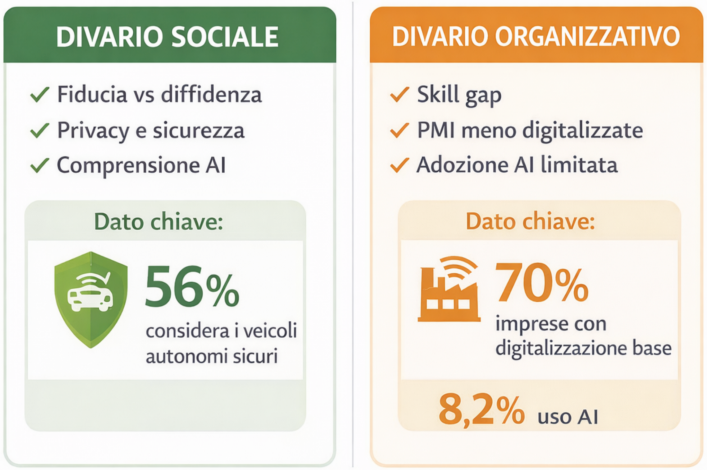
Il doppio digital divide nella mobilità

Andando ad approfondire il divario nella sua dicotomia sociale-organizzativo, si riporteranno ora degli esempi accompagnati da casi d'uso specifici.

Sul piano sociale, le percezioni degli utenti verso l'automazione e la mobilità connessa mostrano un quadro complesso e non uniforme. Studi europei evidenziano come la fiducia nei sistemi autonomi sia strettamente legata alla percezione di sicurezza e alla comprensione del ruolo umano nei processi decisionali automatizzati. Un'indagine di Allianz ha rilevato che circa il 56% dei cittadini intervistati considera i veicoli autonomi sicuri o almeno quanto la guida umana (https://www.allianz.com/en/mediacenter/news/media-releases/251028-allianz-motor-day-2025.html) , mentre una quota significativa continua a manifestare prudenza e bisogno di maggiori garanzie. Questo dualismo tra aspettative positive e diffidenza rappresenta uno degli elementi chiave del digital divide sociale: non una semplice resistenza all'innovazione, ma una richiesta implicita di trasparenza, accompagnamento e comprensione delle tecnologie emergenti.

Sul piano organizzativo, il digital divide si manifesta in modo evidente nella struttura produttiva italiana ed europea, caratterizzata da una forte presenza di PMI nelle filiere della mobilità e della logistica. Secondo i dati ISTAT e Digital Intensity Index, circa il 70% delle imprese italiane raggiunge solo un livello base di digitalizzazione, mentre appena il 26% delle PMI presenta livelli elevati, evidenziando un gap significativo rispetto alle grandi aziende (https://www.istat.it/comunicato-stampa/imprese-e-ict-anno-2024/). Ancora più marcata è la distanza nell'adozione di tecnologie avanzate: nel 2024 solo l'8,2% delle imprese con almeno 10 addetti utilizza soluzioni di AI, dato che riflette una trasformazione ancora disomogenea nelle catene del valore logistiche e nei servizi di mobilità. Questo scenario contribuisce a generare un divario organizzativo non solo tecnologico, ma anche culturale, dove parte della forza lavoro si trova a interagire con sistemi digitali senza averne piena consapevolezza operativa.

L'analisi congiunta di questi due livelli suggerisce come il digital divide nella mobilità intelligente non sia riconducibile esclusivamente a fattori tecnologici, bensì a una combinazione di competenze, fiducia e maturità organizzativa. I casi d'uso riportati di seguito mostrano come l'adozione dell'AI nei contesti logistici e nei servizi CCAM possa generare benefici concreti solo quando l'evoluzione tecnologica viene accompagnata da processi di formazione, comunicazione e partecipazione degli utenti e degli operatori.



Percezioni e timori nell'adozione dell'automazione

Per fornire una panoramica completa delle motivazioni che alimentano il divario digitale, di seguito viene proposta una breve analisi delle principali percezioni e criticità associate all'automazione e all'AI. Tali dinamiche riguardano sia l'utente finale, chiamato a interagire con sistemi sempre più autonomi, sia gli operatori delle filiere produttive della mobilità e della logistica, coinvolti in processi di trasformazione organizzativa e tecnologica.

Sul piano sociale, numerosi studi europei evidenziano come la fiducia nei sistemi automatizzati sia caratterizzata da una forte ambivalenza: aspettative positive in termini di sicurezza e sostenibilità convivono con timori legati alla privacy, alla responsabilità decisionale e alla perdita di controllo umano. Ricerche condotte su cittadini europei mostrano infatti atteggiamenti generalmente favorevoli verso i benefici dell'automazione, ma più critici rispetto alla gestione dei dati e alla sicurezza informatica (https://cordis.europa.eu/article/id/434335-how-do-europeans-feel-about-self-driving-cars/it). Analogamente, indagini sulla guida autonoma in Italia evidenziano come, pur registrando livelli di fiducia significativi, oltre la metà degli intervistati mantenga preoccupazioni sul corretto funzionamento e sull'integrazione tra sistemi automatizzati e guida umana. Queste percezioni indicano che la resistenza non deriva necessariamente da una contrarietà ideologica alla tecnologia, ma dalla richiesta di maggiore trasparenza e comprensione delle sue implicazioni.

Percezione / Timore	Bisogno reale sottostante
Perdita di controllo umano	Trasparenza decisionale
Automazione = Perdita lavoro	Reskilling e nuovi ruoli
Opacità algoritmica	Explainable AI (IA comprensibile)
Rischio sicurezza	Cybersecurity e governance

Dal punto di vista organizzativo e occupazionale, le paure si concentrano prevalentemente sulla trasformazione dei ruoli e sulla necessità di aggiornamento continuo delle competenze. Studi recenti stimano che circa 10,5 milioni di lavoratori italiani siano esposti in misura significativa agli effetti dell'automazione, evidenziando come la transizione tecnologica sia già percepita come concreta e non futura (https://www.orizzontescuola.it/intelligenza-artificiale-e-mercato-del-lavoro-italiano-105-milioni-di-occupati-rischiano-lautomazione/). Nel settore della logistica, che rappresenta quasi il 18,6% degli annunci di lavoro nazionali, emerge inoltre una crescente difficoltà nel reperire personale con competenze adeguate alla digitalizzazione dei processi (https://www.uominietrasporti.it/centonumeri/flussi-in-movimento/1-ogni-5-annunci-e-la-domanda-di-lavoro-espressa-dalla-logistica-in-italia-spesso-rimasta-senza-risposta/). A questo si aggiunge il dato secondo cui oltre il 52% delle aziende individua nella carenza di cultura digitale uno dei principali ostacoli all'adozione tecnologica, mentre il 48% segnala un deficit di competenze (https://www.corrierecomunicazioni.it/digital-economy/competenze-digitali-nel-2026-in-italia-gap-di-2-milioni-di-lavoratori/).

Inoltre, in molti contesti logistici e operativi, le resistenze non riguardano esclusivamente l'introduzione della tecnologia, ma il modo in cui essa ridefinisce il significato stesso del lavoro e dell'identità professionale.

L'analisi congiunta di questi elementi suggerisce come le paure associate all'automazione non rappresentino semplicemente un freno all'innovazione, ma costituiscano indicatori utili per individuare bisogni formativi e criticità sistemiche. Comprendere tali percezioni consente di progettare strategie di adozione più efficaci, orientate non solo

allo sviluppo tecnologico, ma anche alla costruzione di fiducia e alla gestione consapevole della transizione digitale nella mobilità intelligente. Ciò evidenzia come la transizione tecnologica richieda non solo aggiornamento delle competenze, ma anche strategie di comunicazione e coinvolgimento degli operatori.

Le dinamiche di transizione socio-organizzativa descritte in questa sezione trovano un inquadramento metodologico nelle Social Sciences and Humanities (SSH), il cui contributo è riconosciuto dal programma Horizon Europe come requisito trasversale per i progetti del Cluster 5 (Climate, Energy and Mobility). L'approccio SSH consente di affiancare all'analisi tecnica strumenti quali l'analisi delle percezioni di rischio, lo studio dei processi decisionali in contesti di incertezza e la valutazione dell'impatto sociale delle tecnologie di automazione. Il framework europeo di Responsible Research and Innovation (RRI) traduce questi principi in pratiche operative — co-design con gli utenti finali, inclusività, trasparenza, anticipazione degli impatti — direttamente applicabili alla progettazione di sistemi ITS sicuri e accettati dalla comunità di riferimento.

In questo contesto, le resistenze e le percezioni documentate nei paragrafi precedenti non rappresentano solo vincoli progettuali, ma dati di ricerca SSH che informano la progettazione di sistemi di mobilità intelligente realmente human-centric: sistemi che integrano la cybersecurity non come imposizione tecnica, ma come elemento di fiducia percepita dall'utente e di resilienza organizzativa per l'operatore.

4.2 Etica della sicurezza

Il tema dell'etica legata all'AI è estremamente attuale ed al tempo stesso critico per le istituzioni e le aziende stesse.

Quali regole e principi possono esser prese decisioni di intervento in caso di sospetto o certezza di attacco cyber? Quali sono i margini ed i limiti di intervento?

A quali logiche di rispetto della privacy, dell'interesse comune o semplicemente della pubblica sicurezza vanno ricondotte certe scelte?

La discussione etica si appoggia ai pilastri del Trustworthy AI riconosciuti a livello europeo (EU AI Act, Art. 9–15) e internazionale, e si articola attorno a tre direttrici principali: regole di intervento, privacy e sicurezza pubblica.

Sul piano delle regole di intervento, l'EU AI Act (Reg. UE 2024/1689) classifica i sistemi AI per la gestione del traffico e la sicurezza dei veicoli come "ad alto rischio" (Allegato III, Punto 2; Allegato I, Sezione B), con conformità obbligatoria entro il 2 agosto 2026. L'Art. 14 definisce quattro modelli di supervisione umana — Human-in-Command, Human-in-the-Loop, Human-on-the-Loop e Human-out-of-the-Loop — richiedendo i primi due per i sistemi safety-critical nei trasporti. In Italia, la L. 132/2025, prima legge nazionale sull'AI nell'UE (in vigore dal 10 ottobre 2025), attribuisce ad AgID il ruolo di autorità di notifica e ad ACN la sorveglianza di mercato.

Sul piano della privacy, i dati di mobilità pongono rischi specifici e quantificabili: la ricerca di De Montjoye et al. (Nature, 2013) dimostra che 4 punti spazio-temporali sono sufficienti a identificare il 95% degli individui in un dataset di mobilità. I sistemi V2X raccolgono dati di posizionamento, velocità e comportamento di guida che, senza adeguata protezione, possono consentire la sorveglianza di massa. Lo standard ETSI TS 102 941 affronta questa sfida attraverso certificati pseudonimi con rotazione periodica, implementati nel sistema europeo CCMS/CPOC operativo in 18 stati membri.

Sul piano della sicurezza pubblica, l'EU AI Act impone una tripla valutazione per i sistemi AI nei trasporti: DPIA (GDPR, Art. 35), gestione del rischio (AI Act, Art. 9) e valutazione dell'impatto sui diritti fondamentali — FRIA (AI Act, Art. 27). L'Art. 86 sancisce il diritto a "spiegazioni chiare e significative" per le persone interessate dalle decisioni algoritmiche. Il NIST AI Risk Management Framework (AI 100-1) propone un ciclo strutturato Govern-Map-Measure-Manage, con un crosswalk del 60–70% rispetto ai requisiti dell'EU AI Act, facilitando la conformità per operatori attivi in più giurisdizioni.

Per sostenere l'implementazione di questi principi, la comunità open-source offre strumenti consolidati sotto la Linux Foundation AI & Data, tra cui AI Fairness 360 e Adversarial Robustness Toolbox (descritti in dettaglio nel §4.2.9).

Lo standard ISO/IEC 42001 (2023) fornisce un sistema di gestione dell'AI certificabile, integrabile con i framework già adottati dagli operatori dei trasporti.

In questa prospettiva, l'AI in ambito cybersecurity non si configura come un mero strato tecnologico sovrapposto ai processi esistenti, ma come leva di evoluzione organizzativa: come osservato da Giuliano Noci (Il Sole 24 Ore, 11 aprile 2026), «la tecnologia è disponibile, non è nascosta, non è proibita: semplicemente non viene incorporata», e adottarla significa ripensare processi, responsabilità e gerarchie — evoluzione necessaria, non restyling.

Nuovi ruoli professionali e programmi di formazione per AI e cybersecurity nella mobilità

L'evoluzione organizzativa richiamata implica nuovi ruoli professionali che le organizzazioni del settore devono acquisire o sviluppare. L'AI Risk Officer è responsabile della valutazione e gestione dei rischi associati ai modelli di AI, inclusi bias, robustezza e conformità all'AI Act. L'OT Security Specialist presidia la sicurezza dei sistemi di controllo industriale e delle infrastrutture operative (ITS, SCADA, segnalamento ferroviario). Il Data Steward governa qualità, provenienza e compliance dei dati lungo la filiera. Il V2X Security Architect progetta architetture di comunicazione sicure per gli ecosistemi veicolo-infrastruttura.

I programmi di formazione continua devono coprire sia la dimensione tecnica (percorsi certificati in cybersecurity OT come IEC 62443, in sicurezza AI come NIST AI RMF e ISO/IEC 23894, in gestione delle identità digitali come eIDAS e SCMS) sia quella di governance (NIS2, CRA, AI Act, responsabilità in caso di incidente). Per le organizzazioni di dimensioni minori — comuni, aziende TPL, PMI della filiera logistica — la formazione può essere sostenuta attraverso i Competence Center italiani per l'Industria 4.0 e le EDIH (European Digital Innovation Hubs).

4.3 Privacy-by-Design nei sistemi ITS

L'integrazione della privacy fin dalla progettazione (Privacy-by-Design) nei sistemi di trasporto intelligente costituisce un requisito imprescindibile, sia per la conformità al GDPR e all'EU AI Act, sia per la fiducia degli utenti nei servizi di mobilità connessa. Tre pilastri tecnici sostengono questo approccio: la pseudonimizzazione delle comunicazioni V2X, il Federated Learning per l'addestramento distribuito dei modelli AI, e la minimizzazione dei dati nei flussi ITS.

Pseudoanonimizzazione delle comunicazioni V2X. Lo standard ETSI TS 102 941 definisce un'architettura di sicurezza per i sistemi cooperativi ITS basata su certificati pseudonimi (pseudonym certificates), che consentono ai veicoli di trasmettere messaggi autenticati senza rivelare l'identità del conducente. Il meccanismo europeo CCMS (Cooperative Credential Management System), coordinato attraverso il CPOC (Certificate Policy Operations Centre) della C-ITS Security Credential Management, prevede la rotazione periodica dei certificati pseudonimi — tipicamente ogni cinque minuti in condizioni operative — per impedire il tracciamento longitudinale dei veicoli.

Questa architettura bilancia due esigenze in tensione: la privacy del conducente e la responsabilità per la sicurezza stradale, poiché l'autorità di certificazione (Root CA) conserva la capacità di risalire all'identità in caso di incidente grave o indagine giudiziaria, come previsto dalla Direttiva 2010/40/UE e dal Regolamento Delegato (UE) 2019/1789.

Federated Learning per la cybersecurity collaborativa. Il Federated Learning (FL) consente l'addestramento di modelli di rilevamento delle minacce su dati distribuiti tra più operatori di trasporto, senza centralizzare i dataset e senza esporre informazioni sensibili sulle infrastrutture. In un'architettura FL applicata agli ITS, ciascun operatore (ferroviario, autostradale, portuale) addestra localmente un modello di anomaly detection sui propri flussi di rete, trasmettendo al server di aggregazione solo i gradienti del modello.

L'integrazione con tecniche di crittografia omomorfica (Homomorphic Encryption) e Secure Multi-Party Computation (SMPC) consente di proteggere anche i gradienti durante l'aggregazione, prevenendo attacchi di model inversion. L'European Data Protection Supervisor (EDPS), nel TechDispatch #1/2025 dedicato al Federated Learning, ha riconosciuto il potenziale di questa tecnica per la conformità al principio di minimizzazione dei dati (Art. 5(1)(c)

GDPR), pur evidenziando rischi residui di re-identificazione attraverso l'analisi dei gradienti, raccomandando l'adozione congiunta di differential privacy.

Minimizzazione dei dati nei flussi ITS. Il principio di minimizzazione (Art. 5(1)(c) GDPR) applicato ai sistemi ITS richiede che la raccolta di dati sia limitata allo stretto necessario per la finalità dichiarata. Per le comunicazioni V2X, ciò implica l'anonimizzazione o l'aggregazione dei dati di mobilità prima dell'ingestione nei sistemi di analisi centralizzata, la definizione di policy di data retention differenziate per tipologia di dato (telemetria veicolare, dati biometrici per l'autenticazione, log di accesso), e l'esecuzione sistematica di Data Protection Impact Assessment (DPIA) per i trattamenti ad alto rischio, come previsto dall'Art. 35 GDPR e dall'Art. 9 dell'EU AI Act per i sistemi di AI ad alto rischio nel settore trasporti (Annex III, Punto 2).

L'adozione di tecniche di k-anonimizzazione e l-diversità per i dataset di mobilità, combinata con differential privacy per le query aggregate, consente di preservare l'utilità analitica dei dati riducendo il rischio di re-identificazione a livelli conformi ai requisiti del Garante per la Protezione dei Dati Personali.

4.4 Metodi di AI Security

L'AI Security nei trasporti riguarda l'uso dell'AI per prevenire incidenti, attacchi informatici, frodi e minacce fisiche, migliorando al tempo stesso affidabilità e resilienza dei sistemi di mobilità.

La scelta e la combinazione dei diversi approcci dipendono dal contesto applicativo, dal livello di criticità del servizio e dalla posizione del sistema all'interno dell'architettura complessiva (edge, comunicazioni, backend, piattaforme).

L'efficacia dell'AI Security emerge quindi non dall'adozione di singole tecniche, ma dalla loro integrazione coerente all'interno di architetture sicure by design, come descritto nei capitoli successivi.

L'AI generativa introduce una superficie d'attacco qualitativamente nuova per i sistemi di mobilità. Il rischio di prompt injection (OWASP LLM01, 2025) è particolarmente critico nei sistemi di gestione del traffico che integrano interfacce in linguaggio naturale: un sistema LLM-based di supporto decisionale potrebbe essere indotto a generare raccomandazioni operative errate.

L'avvelenamento dei dati di addestramento (OWASP LLM04) minaccia i modelli di manutenzione predittiva, dove la corruzione dei dati telemetrici storici potrebbe mascherare il deterioramento reale dei componenti. Il periodo 2025-2026 segna un punto di inflessione: gli attacchi GenAI hanno completato la transizione da sperimentazione accademica a capacità operativa verificata, con malware costruiti interamente tramite modelli generativi rilevati in operazioni reali (CrowdStrike, 2025). Le difese devono evolvere dalla detection basata su firme alla detection comportamentale, capace di identificare anomalie nell'uso delle API e nei pattern di interazione dei sistemi AI.

L'evoluzione dei SOC verso architetture potenziate dall'AI rappresenta la risposta difensiva alla crescente sofisticazione delle minacce. I SOC di nuova generazione integrano capacità SOAR (Security Orchestration, Automation and Response) con piattaforme XDR (Extended Detection and Response) che correlano telemetria proveniente da endpoint, rete, cloud e sistemi OT in un'unica console.

Lo studio IDC/Splunk documenta risultati significativi per l'approccio unificato: il 64% di identificazione più rapida delle minacce, il 55% di risoluzione più rapida degli incidenti e un ROI del 304%. Per gli operatori di trasporto, la sfida principale risiede nella convergenza OT/IT: un SOC settoriale deve integrare dati SCADA, protocolli industriali, telemetria veicolare e sistemi di bigliettazione. Il gap di 4,8 milioni di professionisti cybersecurity a livello globale (ISC2, 2024) rende l'automazione delle attività di triage e investigazione non un'opzione ma una necessità operativa.

L'adozione di metodi AI per la cybersecurity richiede un approccio strutturato alla governance del ciclo di vita dei modelli — un paradigma definito Secure ML Lifecycle o MLSecOps. Questo approccio prevede il versionamento rigoroso dei modelli con tracciabilità dei dataset di addestramento, la validazione continua delle prestazioni e la rilevazione del model drift, il testing adversariale sistematico prima e durante il deployment, e l'audit periodico di equità e spiegabilità.

L'ecosistema di strumenti open-source sotto la Linux Foundation AI & Data — tra cui AI Fairness 360, AI Explainability 360 e Adversarial Robustness Toolbox, descritti nel §4.2.9 — supporta operativamente questo approccio. Per i sistemi AI nei trasporti, classificati ad alto rischio dall'EU AI Act (Allegato III, Punto 2), il MLSecOps è prerequisito per la conformità ai requisiti di gestione del rischio (Art. 9) e supervisione umana (Art. 14).

L'evoluzione verso architetture multi-agente nei sistemi ITS introduce rischi di failure cascading: un errore in un singolo agente può propagarsi attraverso la catena di pianificazione, esecuzione e memoria, amplificandosi ad ogni passaggio. La prima tassonomia empirica dei failure mode (MAST, marzo 2025) ha identificato 14 modalità di fallimento su oltre 1.600 tracce di esecuzione, con il 32,3% attribuibile a disallineamento inter-agente.

Per i sistemi di trasporto safety-critical, le strategie di mitigazione prevedono circuit breaker tra agenti, confini di isolamento e fallback deterministici certificati secondo gli standard di sicurezza funzionale (EN 50126, ISO 26262).

4.4.1 Analisi delle minacce 2025

Prima di esaminare i metodi difensivi, è necessario comprendere la portata e la tipologia delle minacce che il settore dei trasporti affronta nel contesto attuale.

Il settore dei trasporti è il secondo comparto più esposto in UE: secondo l'ENISA Threat Landscape 2025 (ottobre 2025, v.1.2), i trasporti rappresentano il 7,5% degli incidenti su 4.875 eventi (luglio 2024 – giugno 2025), dopo la Pubblica Amministrazione (38,2%). La disaggregazione mostra concentrazione in aviazione (58,4%) e logistica (20,8%); marittimo, ferroviario e stradale sono caratterizzati qualitativamente. La quota dell'edizione 2024 era dell'11% su oltre 11.000 eventi: la riduzione apparente è attribuibile al cambio di metodologia ENISA (agosto 2025) e non a una diminuzione reale degli attacchi.

Il quadro italiano è particolarmente grave: secondo il Rapporto CLUSIT H1 2025 (Security Summit, novembre 2025), trasporti e logistica rappresentano il 17% degli attacchi rilevati in Italia, secondo settore dopo governo e difesa (38%). Il volume degli incidenti gravi nel solo H1 2025 è pari a 1,5 volte l'intero 2024 (+150%, 280 incidenti gravi). L'Italia rappresenta il 10,2% degli attacchi cyber globali e oltre il 25% degli attacchi globali al settore trasporti. ENISA conferma l'Italia come secondo Paese UE più colpito (11,33%, dopo la Germania). Bechelli (CLUSIT) attribuisce la crescita alla volontà di colpire intere filiere logistiche.

L'ACN conferma l'escalation. La Relazione Annuale 2024 del CSIRT Italia documenta 1.411 eventi cyber gestiti e 573 incidenti confermati (+89,1% rispetto ai 303 del 2023); le vittime uniche sono raddoppiate (da 566 a 1.260), le comunicazioni di allerta cresciute da 20.825 a 53.470. Il settore trasporti ha registrato 214 vittime nel 2024. Il Riepilogo Operativo H2 2025 (febbraio 2026) rileva 1.253 cyber event (+30%) e 304 incidenti confermati: la stabilizzazione degli incidenti a fronte della crescita degli eventi indica miglioramento della rilevazione e maggiore efficacia di risposta. ACN evidenzia un pattern ricorrente di «fornitori di servizi web compromessi che causano un effetto domino» sui clienti (cfr. §5.1 e §5.4 per la risposta dell'ecosistema italiano).

La vulnerabilità specifica del settore trasporti rispetto ad altri comparti risiede nella convergenza tra sistemi informatici (IT) e sistemi operativi (OT). Un attacco che compromette i sistemi IT — biglietteria, email, piattaforme MaaS — può propagarsi tramite lateral movement verso i sistemi OT safety-critical: segnalamento ferroviario, sistemi SCADA, controllo semaforico, gestione delle porte di banchina. L'ENISA avverte che il ransomware targetizzerà sempre più i sistemi OT con potenziali conseguenze cyber-kinetic. A questo si aggiungono l'infrastruttura legacy diffusa nel settore, i cicli di vita pluridecennali dei sistemi ferroviari e marittimi, e l'espansione della superficie d'attacco determinata dall'adozione massiva di IoT, telematica e comunicazioni V2X.

Il periodo 2025-2026 segna un punto di inflessione nella natura stessa della minaccia cyber: gli attacchi potenziati dall'AI (AI) generativa hanno completato la transizione da sperimentazione accademica a capacità operativa verificata in campo. CrowdStrike, nel Threat Hunting Report 2025 (agosto 2025), ha valutato che le capacità offensive basate su GenAI sono «no longer theoretical», sulla base di malware come FunkLocker e SparkCat costruiti interamente tramite modelli generativi e rilevati in operazioni reali. Questa valutazione segna un cambio di paradigma rispetto alla percezione prevalente nel 2023-2024, quando tali capacità erano considerate un rischio emergente ma non ancora concretizzato.

Il caso più rilevante è LAMEHUG, il primo malware pubblicamente documentato con integrazione operativa di un modello linguistico di grandi dimensioni (LLM). Scoperto dal CERT-UA tra il 10 e il 17 luglio 2025 e attribuito con confidenza moderata ad APT28 (Fancy Bear, unità 26165 del GRU russo), LAMEHUG utilizza il modello Alibaba Qwen2.5-Coder-32B-Instruct tramite API HuggingFace per generare dinamicamente comandi Windows attraverso prompt predefiniti. La rilevanza per la cybersecurity è duplice: da un lato, la detection basata su firme risulta inefficace poiché ogni esecuzione produce output differenti; dall'altro, il traffico di rete verso le API LLM appare indistinguibile dall'uso legittimo di servizi di machine learning, rendendo necessario un approccio di analisi comportamentale per l'identificazione della minaccia.

L'analisi GreyNoise (gennaio 2026) documenta la scala industriale della minaccia: 91.403 sessioni di attacco contro infrastrutture LLM tra ottobre 2025 e gennaio 2026, di cui 80.469 in 11 giorni da soli 2 IP, con probing su oltre 73 endpoint (GPT-4o, Claude, Llama, DeepSeek, Gemini, Mistral, Qwen, Grok). Parallelamente, il vishing è cresciuto del +442% tra H1 e H2 2024 (CrowdStrike Global Threat Report 2025) e il phishing AI-enhanced rappresenta oltre l'80% del social engineering globale (ENISA ETL 2025), confermando l'operatività su larga scala dell'AI generativa offensiva.

Il rischio non proviene esclusivamente da attori esterni. L'adozione non governata dell'AI generativa all'interno delle organizzazioni — fenomeno denominato shadow AI — introduce un vettore di rischio endogeno quantificabile: secondo l'IBM Cost of a Data Breach Report 2025, le organizzazioni con presenza di shadow AI registrano un sovrapprezzo medio di 670.000 dollari per incidente di data breach (4,63 milioni di dollari contro una media di 3,96 milioni). Gartner prevede che entro il 2027 il 17% dei cyberattacchi coinvolgerà componenti GenAI, mentre entro il 2028 il 25% dei breach enterprise sarà riconducibile ad abuso di agenti AI autonomi.

Nel contesto dei trasporti, dove le piattaforme MaaS, i sistemi di fleet management e le chatbot di assistenza passeggeri integrano progressivamente componenti GenAI, il rischio di shadow AI si aggiunge a quello degli attacchi esterni, generando una superficie di esposizione che richiede governance specifica.

L'operazione FAMOUS CHOLLIMA, documentata nel CrowdStrike Global Threat Report 2025, è il primo caso di utilizzo full-lifecycle dell'AI generativa in un'operazione di infiltrazione: il gruppo nordcoreano ha impiegato identità sintetiche generate da AI per infiltrare oltre 320 aziende (+220% anno su anno), utilizzando l'AI dall'iniziale creazione dell'identità fittizia fino alla raccolta di intelligence interna. Questo schema operativo corrisponde ai rischi ASI01 (Agent Goal Hijacking) e ASI04 (Identity and Access Abuse) della classificazione OWASP Top 10 for Agentic Applications 2026, a conferma che le minacce ai sistemi AI agentici non sono più scenari futuri ma pattern già operativi.

Sebbene a febbraio 2026 non risultino ancora attacchi documentati in cui l'AI generativa sia stata impiegata come vettore primario contro infrastrutture OT o ITS dei trasporti, **la convergenza tra l'elevato profilo di rischio del settore e la maturità operativa degli strumenti offensivi GenAI produce un rischio convergente di alta probabilità**. L'AI può automatizzare la ricognizione delle infrastrutture ITS esposte, generare comunicazioni deepfake indirizzate al personale di controllo del traffico ferroviario o marittimo, e condurre scansioni automatizzate delle vulnerabilità di endpoint V2X e telematici. Il caso Arup (gennaio 2024, 25,6 milioni di dollari sottratti tramite videoconferenza deepfake) dimostra l'applicabilità concreta di queste tecniche al settore delle infrastrutture, rendendo la preparazione difensiva non più opzionale.

Profili di rischio per sotto-settore

L'analisi aggregata del panorama delle minacce consente di delineare profili di rischio specifici per ciascun sotto-settore dei trasporti. L'ENISA ETL 2025 fornisce per la prima volta una disaggregazione quantitativa degli incidenti per modo di trasporto, con differenze strutturali nette nella distribuzione delle minacce, nelle motivazioni degli attaccanti e nelle conseguenze operative. La rassegna che segue esamina in dettaglio i profili di minaccia dell'aviazione e del settore ferroviario, i due sotto-settori con il maggior volume di incidenti documentati e la casistica più rilevante nel periodo di riferimento.

Sotto-settore	% incidenti (ENISA 2025)	Minaccia dominante	Attori principali	Fattore critico
Aviazione	58,4%	DDoS (87,6% del totale trasporti)	NoName057(16), gruppi pro-Russia	Supply chain software
Ferroviario	n.d. (crescita documentata)	DDoS hacktivista, ransomware supply chain	Gruppi pro-Russia	Convergenza IT/OT
Stradale/Automotive	+39% incidenti YoY (Upstream 2025)	Attacchi telematica (66%) e API (17%)	Attori opportunistici e APT	Superficie d'attacco in espansione
Marittimo	OT risk score 98/100 (Cyble)	APT state-nexus, GNSS jamming	8 gruppi APT identificati	Infrastruttura legacy
Logistica/Merci	20,8%	Ransomware (+132% YoY)	CL0P (24%), Qilin (15%)	Effetto cascata supply chain

L'aviazione si conferma il sotto-settore dei trasporti con il più elevato volume di incidenti cyber documentati. Secondo l'ENISA ETL 2025, l'aviazione rappresenta il 58,4% di tutti gli incidenti attribuiti al settore trasporti nel periodo luglio 2024 – giugno 2025, consolidando una posizione di primato che riflette sia l'ampia superficie digitale del comparto sia la sua rilevanza come obiettivo strategico per attori state-nexus e gruppi hacktivisti. Gli attacchi DDoS dominano il panorama delle minacce nell'aviazione, con il sotto-settore che assorbe l'87,6% di tutti gli attacchi DDoS diretti al comparto trasporti, prevalentemente condotti da gruppi pro-Russia come NoName057(16), responsabile del 36,4% dell'attività DDoS nel settore manifatturiero e trasporti.

Le minacce all'aviazione si articolano su tre direttrici principali oltre al DDoS: il ransomware, che costituisce oltre l'80% del cybercrime nel comparto trasporti; il furto di dati, con obiettivi che spaziano dai dati personali dei passeggeri delle compagnie aeree alla proprietà intellettuale degli OEM aeronautici; e le campagne di spionaggio condotte da gruppi state-nexus, con attori Russia-nexus e Cina-nexus che prendono di mira il comparto aereo come parte di più ampie operazioni di intelligence sui trasporti e sulla logistica occidentali. Colpisce che, nonostante l'elevato volume di attacchi, solo il 2% degli incidenti DDoS nell'aviazione ha causato una disruption operativa effettiva, indicando una resilienza operativa del settore superiore a quella di altri comparti.

L'incidente Collins Aerospace MUSE (settembre 2025) illustra le conseguenze concrete di un attacco alla supply chain dell'aviazione civile. Un attacco ransomware a un fornitore terzo ha compromesso il software di check-in e boarding utilizzato in diversi aeroporti europei, tra cui Heathrow, Bruxelles e Berlino, causando code, ritardi e cancellazioni. L'incidente conferma la dipendenza dell'aviazione civile da catene di fornitura software complesse, dove la compromissione di un singolo componente può propagarsi a scala continentale, e la necessità di estendere i requisiti di cybersecurity ai fornitori terzi lungo l'intera catena del valore.

Il panorama delle minacce all'aviazione include inoltre l'attacco ransomware Rhysida al Port of Seattle/Sea-Tac Airport (agosto 2024), che ha compromesso i sistemi di smistamento bagagli, e le campagne DDoS ricorrenti condotte da gruppi hacktivisti pro-Russia contro aeroporti e compagnie aeree dell'Unione Europea, con particolare intensità nei confronti dei paesi che hanno espresso sostegno all'Ucraina. Queste campagne, sebbene raramente in grado di causare disruption operativa duratura, contribuiscono a erodere la fiducia pubblica nei servizi di trasporto aereo e impongono un onere difensivo rilevante alle organizzazioni colpite.

Il settore ferroviario presenta un profilo di minaccia strutturalmente diverso dall'aviazione, caratterizzato dalla prevalenza di attacchi DDoS hacktivisti e dalla criticità della convergenza IT/OT come fattore di rischio specifico. Sebbene l'ENISA ETL 2025 non fornisca una percentuale disaggregata per il sotto-settore ferroviario, i dati qualitativi attestano una crescita costante degli attacchi DDoS condotti da gruppi hacktivisti pro-Russia, con campagne

sistematiche dirette contro le ferrovie di Belgio, Repubblica Ceca, Romania e altri paesi dell'Europa orientale e centrale. Il fattore scatenante di queste campagne è esplicitamente collegato al sostegno dell'Unione Europea all'Ucraina.

L'attacco alla Ukrzaliznytsia (marzo 2025), l'operatore ferroviario nazionale ucraino, è stato un caso paradigmatico di attacco cyber in contesto bellico: descritto dalle autorità ucraine come «sistematico, complesso e multi-livello», ha reso inoperativo il sistema di vendita biglietti online, unico canale di acquisto per il servizio passeggeri nazionale. I treni hanno tuttavia continuato a circolare grazie a protocolli di backup pre-stabiliti, dimostrando il valore della preparazione operativa per scenari di degradazione dei sistemi IT. In un contesto diverso ma complementare, l'attacco al sistema ferroviario polacco (agosto 2023) ha messo in luce una vulnerabilità di natura radicalmente differente: l'iniezione di frequenze radio nel sistema di comunicazione analogico non crittografato ha attivato la funzione di arresto di emergenza su circa 20 treni, dimostrando come tecnologie legacy a basso costo possano essere sfruttate con equipaggiamento radio economico e senza competenze cyber avanzate.

L'incidente DSB Danimarca (ottobre 2022) rimane un riferimento chiave per il settore: la compromissione del server del subappaltatore Supeo ha disabilitato l'applicazione utilizzata dai macchinisti per le informazioni operative, causando il fermo dell'intera rete ferroviaria nazionale danese. Si è trattato del primo caso documentato in cui un attacco ransomware ha provocato l'interruzione totale di un servizio ferroviario nazionale, mettendo in luce il rischio sistemico della dipendenza da fornitori terzi per componenti operativi critici. Le campagne DDoS contro operatori ferroviari europei condotte da gruppi pro-Russia hanno interessato nel periodo 2024-2025 le ferrovie di Belgio, Repubblica Ceca e Romania, con impatto prevalentemente limitato ai portali web e ai servizi informativi per i passeggeri.

Nonostante il quadro di minaccia in evoluzione, **il settore ferroviario mostra segnali di maturità difensiva**. L'analisi NIS360 2024 dell'ENISA classifica il settore ferroviario come relativamente avanzato in termini di maturità cyber rispetto ad altri sotto-settori dei trasporti. Un elemento ricorrente nei casi analizzati è la tenuta della segmentazione IT/OT: nell'attacco a Ukrzaliznytsia e nella quasi totalità degli incidenti ferroviari documentati, la separazione tra reti informatiche e reti operative ha impedito che la compromissione dei sistemi IT si propagasse ai sistemi di segnalamento, trazione e controllo del traffico. Questa evidenza empirica conferma la segmentazione IT/OT come il singolo fattore protettivo più rilevante per la continuità operativa del settore ferroviario.

Il settore stradale e automotive registra la *più rapida espansione della superficie d'attacco* tra tutti i sotto-settori dei trasporti. Il Global Automotive cybersecurity Report 2025 di Upstream Security documenta 409 incidenti di cybersecurity pubblicamente riportati nel solo 2024, con una crescita del +39% rispetto all'anno precedente. Il dato più allarmante riguarda la scala degli attacchi: gli incidenti classificati come "massive-scale" — capaci di coinvolgere migliaia o milioni di veicoli contemporaneamente — sono triplicati dal 5% al 19% del totale, segnalando una transizione strutturale da attacchi opportunistici individuali a campagne sistematiche contro intere flotte connesse.

L'analisi dei vettori di attacco rivela la **concentrazione del rischio sulla telematica veicolare e sulle interfacce API**. La telematica è il 66% della superficie d'attacco totale degli incidenti automotive, consolidando il proprio ruolo di vettore dominante. Gli attacchi tramite API sono cresciuti del 30% circa, raggiungendo il 17% degli incidenti totali nel 2024. Questa evoluzione riflette la crescente dipendenza dell'ecosistema automotive da servizi cloud connessi, aggiornamenti OTA (Over-The-Air) e piattaforme fleet management che espongono interfacce programmatiche come punto d'ingresso per attori malevoli.

I dati dell'IBM X-Force Threat Intelligence Index 2025, basati sugli incidenti 2024, collocano il settore trasporti al 7% degli attacchi globali (quinto settore più colpito a livello mondiale), con una quota che sale all'11% nella regione Asia-Pacifico, dove i trasporti costituiscono il terzo settore per volume di attacchi dopo manifattura e finanza. A livello globale, il 70% degli attacchi registrati nel 2024 ha colpito infrastrutture critiche, e nel settore trasporti il 67% degli incidenti ha avuto come obiettivo il furto di dati. Il costo medio di un data breach nel 2025, secondo l'IBM Cost of a Data Breach Report, si attesta a 4,44 milioni di dollari (in calo del 9% rispetto al 2024), con un risparmio medio di 2,22 milioni di dollari per le organizzazioni che adottano soluzioni di sicurezza basate su AI.

La superficie d'attacco del settore stradale si estende ben oltre il singolo veicolo. Le reti di comunicazione V2X (Vehicle-to-Everything), in fase di deployment attraverso progetti pilota come C-Roads Italy, introducono nuovi

vettori di spoofing e jamming dei messaggi cooperativi. L'infrastruttura di ricarica elettrica presenta vulnerabilità significative: il protocollo OCPP (Open Charge Point Protocol), utilizzato dalla maggioranza delle stazioni di ricarica, è soggetto a rischi di autenticazione e manipolazione. L'edizione 2025 della competizione Pwn2Own Automotive ha evidenziato vulnerabilità critiche nei caricatori e nei sistemi di infotainment, confermando che la filiera della mobilità elettrica costituisce un'estensione concreta della superficie d'attacco automotive.

Come evidenziato nella sezione §4.3.1, i dati CLUSIT H1 2025 confermano la centralità del settore trasporti nel panorama delle minacce cyber italiane, con una sovraesposizione che riflette sia l'elevata digitalizzazione delle infrastrutture sia una persistente carenza di investimenti in cybersecurity nel settore.

Marittimo, logistica e trasporto merci

Il settore marittimo, responsabile di circa il 90% del commercio globale, è diventato un target prioritario per gruppi APT (Advanced Persistent Threat) a matrice statuale. Il report Cyble Maritime di luglio 2025 documenta oltre 100 cyberattacchi contro il settore marittimo, con un OT risk score di 98 su 100 — il più elevato tra tutti i sotto-settori dei trasporti. Otto gruppi APT sono stati identificati come attivamente operativi contro infrastrutture marittime:

- SideWinder (Sud Asia, targeting porti in Egitto, Gibuti e Sri Lanka);
- Lazarus Group (Corea del Nord, attacchi supply chain contro operatori logistici);
- APT41 (Cina, targeting sistemi di gestione portuale e logistica);
- APT28 e Sandworm (Russia, operazioni contro infrastrutture marittime NATO e del Mar Nero);
- FIN7 (cybercrime finanziario evoluto in espionage con targeting operatori marittimi);
- APT33 (Iran, targeting settore energetico e marittimo del Golfo Persico);
- ScarCruft (Corea del Nord, targeting intelligence marittima);
- UNC3886 (Cina, targeting tecnologie di edge networking e virtualizzazione utilizzate nei sistemi portuali).

L'interferenza GNSS nel settore marittimo ha raggiunto livelli critici nel 2025. Lo studio GPSPATRON/Gdynia Maritime University documenta oltre 820 episodi di jamming registrati dalla Lettonia, attribuiti ad attività russa persistente, con oltre 5.800 navi colpite nel solo secondo trimestre 2025. Nel Mar Baltico, il posizionamento GNSS è risultato indisponibile al largo di Danzica per il 17% del tempo nei mesi di giugno-luglio 2025, e i ricercatori hanno identificato un "sistema di interferenza distribuito multi-nodo" — una rete di guerra elettronica con trasmettitori multipli sincronizzati. Analoga escalation interessa il Mar Nero (471 navi colpite, frequenza quasi giornaliera nella primavera 2025) e lo Stretto di Hormuz, dove l'interferenza elettronica su chokepoint strategici rende le navi effettivamente "cieche" in alcune delle acque più trafficate al mondo.

Il contesto normativo marittimo è in rapida evoluzione. La Circolare 177/2025 del MIT (Direzione Generale per la Vigilanza sulle Autorità Portuali) stabilisce requisiti specifici di cybersecurity per le facility portuali italiane, mentre a livello internazionale le linee guida BIMCO v5 e le risoluzioni IMO aggiornano il framework di cybersecurity per le operazioni navali. Con l'entrata in vigore della Direttiva NIS2 (Network and Information Security), porti e operatori logistici marittimi sono classificati come entità essenziali, soggetti a obblighi stringenti di gestione del rischio e notifica degli incidenti. Si rileva tuttavia una carenza di dati pubblicamente disponibili sulla postura di cybersecurity dei porti italiani: le informazioni specifiche sugli incidenti e sulle misure implementate rimangono largamente riservate, limitando la possibilità di un'analisi quantitativa dettagliata del sotto-settore a livello nazionale.

Due incidenti illustrano l'impatto concreto degli attacchi a infrastrutture portuali. L'attacco ransomware LockBit 3.0 al Port of Nagoya (luglio 2023) ha sospeso le operazioni container per circa 2,5 giorni nel porto che gestisce un decimo del volume commerciale giapponese, con effetti a cascata sulle supply chain automotive. L'incidente DP World Australia (novembre 2023) ha messo offline quattro porti responsabili del 40% del traffico import/export australiano, con 30.137 container bloccati per tre giorni. Questi casi, oggetto di analisi approfondita nella sezione dedicata ai casi studio, confermano come la compromissione di un singolo sistema portuale possa generare disruption a cascata su intere catene logistiche regionali.

Il settore della logistica e del trasporto merci presenta un *profilo di minaccia strutturalmente diverso dal trasporto passeggeri*: il ransomware domina rispetto al DDoS hacktivista, la supply chain funge da vettore amplificatore primario e le conseguenze economiche si propagano a cascata su interi comparti industriali. Secondo l'ENISA ETL 2025, la logistica costituisce il 20,8% degli incidenti nel settore trasporti, il secondo sotto-settore dopo l'aviazione. Il report Cyble Transport & Logistics 2025 documenta un'escalation senza precedenti del ransomware: 283 attacchi registrati nel 2025, con un incremento del +132% rispetto ai 122 dell'anno precedente. I gruppi CL0P (24% degli attacchi) e Qilin (15%) guidano questa offensiva, con il 71% delle vittime concentrate nel segmento trucking e servizi freight.

Tra le minacce ibride cyber-physical nel trasporto merci, i dati Verisk CargoNet 2025 segnalano perdite stimate per furto di carico di 725 milioni di dollari nel 2025, con un incremento del +60% rispetto all'anno precedente, a fronte di 2.646 furti confermati (+18%). Il valore medio per furto è salito a 273.990 dollari (+36%), indicando un targeting sistematico verso carichi di alto valore. Il report NMFTA 2026 Transportation Industry cybersecurity Trends documenta la convergenza tra compromissione digitale e furto fisico: identity fraud, FMCSA account hijacking e load-board impersonation sono diventati strumenti standard per le reti criminali. La weaponizzazione di tool Remote Monitoring and Management (RMM) come AnyDesk e ConnectWise — deployati come first-stage payload per movimento laterale senza triggerare allarmi tradizionali — e il GPS spoofing per la deviazione di carichi completano il quadro di una minaccia in rapida sofisticazione.

Il rischio supply chain nel settore freight è amplificato da un effetto cascata che è proprio di questo sotto-settore: la compromissione di un singolo nodo logistico può paralizzare intere filiere industriali. Gli incidenti DP World Australia e Port of Nagoya (cfr. §4.2.1 per l'analisi dettagliata) rappresentano casi paradigmatici di questa dinamica. Il World Economic Forum conferma la rilevanza sistemica di questo rischio: il 54% delle grandi organizzazioni identifica le interdipendenze supply chain come la maggiore barriera alla cyber resilience.

La distinzione tra minacce al trasporto persone e al trasporto merci emerge come chiave interpretativa essenziale per l'analisi del panorama delle minacce. Mentre il trasporto passeggeri subisce prevalentemente attacchi DDoS di matrice hacktivista con impatto sulla continuità dei servizi digitali, il trasporto merci è strutturalmente esposto a ransomware e attacchi supply chain con conseguenze economiche dirette e immediate. L'entrata in vigore della NIS2 introduce obblighi specifici per gli operatori logistici come entità essenziali, richiedendo l'implementazione di misure di gestione del rischio e la notifica tempestiva degli incidenti. Il quadro complessivo dei cinque sotto-settori analizzati conferma che il settore trasporti è sottoposto a una pressione cyber senza precedenti, con tendenze convergenti di aumento della frequenza, della scala e della sofisticazione degli attacchi.

Casistica e analisi strutturale

I casi seguenti illustrano la varietà e l'impatto degli attacchi al settore trasporti a livello globale. Non intendono costituire un inventario esaustivo, bensì una selezione rappresentativa degli incidenti che, per scala, vettore d'attacco o conseguenze operative, hanno segnato il biennio 2023-2025.

Nel settembre 2024, Transport for London è stata vittima di un attacco attribuito al gruppo Scattered Spider, che ha compromesso i sistemi IT dell'operatore del trasporto pubblico londinese. L'incidente ha comportato la compromissione dei dati bancari di circa 5.000 clienti e la necessità di resettare le credenziali in presenza di 30.000 dipendenti. I sistemi di bigliettazione Oyster card hanno subito disservizi, mentre il ripristino completo di tutti i servizi IT ha richiesto diverse settimane.

Come analizzato nella sezione precedente (§4.2.1), gli incidenti DP World Australia (2023) e Port of Nagoya (2023) confermano la vulnerabilità delle infrastrutture portuali e logistiche agli attacchi ransomware, con effetti a cascata sulle supply chain globali.

Il quadro è completato da ulteriori incidenti che confermano l'ampiezza geografica e settoriale della minaccia. L'attacco ransomware al Port of Nagoya (luglio 2023, cfr. §4.2.1) ha confermato la vulnerabilità degli scali commerciali. Nel settembre 2025, il ransomware al sistema MUSE di Collins Aerospace ha causato disservizi ai processi di check-in e imbarco negli aeroporti di Heathrow, Bruxelles e Berlino. Sul fronte ferroviario, l'attacco al subappaltatore danese Supeo (ottobre 2022) ha rappresentato il primo ransomware a fermare l'intera rete

ferroviaria nazionale di un paese europeo, mentre l'iniezione di frequenze radio nella rete polacca (agosto 2023) ha dimostrato la vulnerabilità dei sistemi analogici non cifrati ancora in esercizio.

La casistica analizzata **conferma la segmentazione IT/OT come il controllo protettivo più efficace documentato**. l'attacco a Ukrzaliznytsia del marzo 2025 e molteplici episodi precedenti presentano un pattern ricorrente: laddove la segregazione tra sistemi informativi e sistemi operativi era implementata, le operazioni di trasporto sono proseguite nonostante la compromissione IT. Questa evidenza empirica rafforza la centralità delle architetture di difesa in profondità, della segmentazione di rete e degli approcci Zero Trust trattati nelle sezioni successive.

4.4.2 Tassonomia dei rischi per applicazioni LLM: OWASP Top 10 2025

Il panorama delle minacce delineato nella sezione precedente documenta la portata e la sofisticazione crescente degli attacchi al settore trasporti. Per tradurre questa consapevolezza in strategie di difesa efficaci, è necessario adottare tassonomie strutturate che classifichino i rischi in modo sistematico. L'OWASP Foundation, organizzazione internazionale no-profit di riferimento per la sicurezza applicativa, ha sviluppato classificazioni specifiche per le applicazioni basate su Large Language Model (LLM), aggiornate nel 2025 per riflettere l'evoluzione rapida di queste tecnologie e la loro crescente adozione in contesti operativi critici, inclusi i sistemi di trasporto intelligente.

La OWASP Top 10 for LLM Applications 2025 (versione 2025.1) identifica i dieci rischi di sicurezza più critici per i sistemi basati su modelli linguistici di grandi dimensioni. Rispetto alla prima edizione del 2023, la lista ha subito un marcato riordinamento che riflette l'esperienza operativa accumulata in due anni di deployment su larga scala: LLM01 Prompt Injection rimane al primo posto come rischio principale; LLM02 Sensitive Information Disclosure sale dalla sesta posizione, riflettendo la gravità crescente delle fughe di dati sensibili; LLM03 Supply Chain sale dalla quinta posizione con un ambito ampliato alla filiera dei componenti AI; LLM04 Data and Model Poisoning ridefinisce il precedente Training Data Poisoning estendendolo all'avvelenamento dei modelli stessi; LLM05 Improper Output Handling scende dalla seconda posizione.

Nel contesto dei trasporti, il **rischio di Prompt Injection (LLM01) diventa particolarmente critico nei sistemi di gestione del traffico e di logistica** che integrano interfacce in linguaggio naturale. Un sistema LLM-based di supporto alle decisioni operative in un centro di gestione del traffico (TMC) potrebbe essere indotto, attraverso l'inserimento di istruzioni malevole nei flussi di dati elaborati, a generare raccomandazioni operative errate — ad esempio suggerendo la chiusura di corsie non necessaria o la modifica dei cicli semaforici in modo da creare congestione artificiale. La ricerca documenta che le tecniche di prompt injection multi-turn raggiungono tassi di successo fino al 97% in cinque turni di interazione, rendendo le difese basate esclusivamente su filtri statici insufficienti.

Il **rischio di Data and Model Poisoning (LLM04) è particolarmente insidioso per i sistemi di manutenzione predittiva e anomaly detection** impiegati nel settore trasporti. Un attaccante che riuscisse a corrompere i dati di addestramento di un modello di manutenzione predittiva ferroviaria — ad esempio manipolando i dati telemetrici storici relativi a vibrazioni, temperature o usura dei componenti — potrebbe alterare le soglie di allarme del sistema, mascherando il deterioramento reale dei componenti e ritardando interventi di manutenzione critici per la sicurezza. Analogamente, l'avvelenamento delle baseline comportamentali di un sistema di anomaly detection potrebbe consentire ad un attaccante di rendere invisibili le proprie attività malevole, eliminando la capacità del sistema di rilevare intrusioni future.

Il nuovo **rischio Vector and Embedding Weaknesses (LLM08)** è direttamente rilevante per i sistemi RAG (Retrieval-Augmented Generation) che stanno emergendo nel settore trasporti per la consultazione automatizzata di normativa e procedure operative. Un sistema RAG utilizzato per supportare la conformità normativa — ad esempio per la consultazione di requisiti NIS2, IEC 62443 o UNECE R155/R156 — potrebbe essere compromesso attraverso l'inserimento di embedding manipolati nel database vettoriale, inducendo il sistema a fornire interpretazioni errate dei requisiti normativi o a omettere requisiti critici di sicurezza. La natura vettoriale della manipolazione rende questo tipo di attacco particolarmente difficile da rilevare con approcci di sicurezza tradizionali, poiché le alterazioni avvengono nello spazio delle rappresentazioni matematiche piuttosto che nel testo visibile.

Il red-teaming AI è emerso come pratica essenziale per la validazione proattiva della sicurezza dei sistemi LLM. Il mercato del red-teaming AI è stimato a 1,43 miliardi di dollari nel 2024 con una proiezione a 4,8 miliardi entro il 2029. Strumenti come Microsoft PyRIT (open-source, febbraio 2024, con evoluzione ad AI Red Teaming Agent nell'aprile 2025) e NVIDIA Garak (circa 100 vettori di attacco, fino a 20.000 prompt per esecuzione) consentono la simulazione sistematica di scenari di attacco contro modelli LLM, fornendo agli operatori dei trasporti la capacità di valutare la robustezza dei propri sistemi AI prima del deployment in ambienti operativi.

L'evoluzione dall'AI verso architetture agentiche — sistemi in grado di operare autonomamente, pianificare sequenze di azioni e interagire con strumenti esterni senza supervisione umana continua — introduce una superficie d'attacco qualitativamente diversa da quella dei modelli LLM tradizionali. Tre caratteristiche distintive separano i sistemi agentici:

- **Autonomia operativa**: gli agenti agiscono su molteplici step e sistemi senza conferma umana ad ogni passaggio, implicando che una singola decisione compromessa può propagarsi attraverso una catena di azioni irreversibili;
- **Accesso a strumenti esterni (tool use)**: gli agenti invocano API, interrogano database, eseguono codice ed interagiscono con servizi di terze parti, dove ogni tool diventa un potenziale vettore di attacco o di esfiltrazione dati;
- **Memoria persistente e contesto condiviso**: i sistemi multi-agente mantengono stati conversazionali e memorie condivise attraverso sessioni, creando repository di dati sensibili che possono essere avvelenati o esfiltrati se non adeguatamente protetti.

OWASP Top 10 for Agentic Applications 2026 si fonda su tre principi architetturali. Minima Agenzia (Least-Agency) estende il principio del minimo privilegio all'autonomia: gli agenti ricevono solo l'autonomia strettamente necessaria al compito. Osservabilità Forte (Strong Observability) richiede visibilità completa su azioni, motivazioni, strumenti invocati, con log degli stati obiettivo, pattern di tool-use e percorsi decisionali. Checkpoint Deterministici prevede punti di verifica obbligatori per le azioni ad alto impatto, in particolare quelle safety-critical nei sistemi di trasporto (cfr. §5.1.3 e §5.4.1 per applicazioni Hitachi Rail e SOC Gruppo FS).

ASI01 – Agent Goal Hijack è l'evoluzione a livello di sistema della prompt injection (LLM01). Quando un agente AI opera autonomamente su molteplici fonti dati, contenuto malevolo in email, PDF, feed o web può alterare gli obiettivi o il percorso decisionale. Nel traffico urbano, dati avvelenati nei feed in tempo reale o nelle comunicazioni V2X potrebbero deviare il routing verso percorsi congestionati o allontanare i veicoli da percorsi di evacuazione. In un sistema ERTMS che integri componenti agentiche, il dirottamento potrebbe alterare le decisioni di distanziamento tra convogli con implicazioni dirette sulla sicurezza ferroviaria.

ASI02 – Tool Misuse and Exploitation riguarda l'uso improprio di strumenti legittimi per prompt ambigui, privilegi eccessivi o input manipolati. Gli agenti interagiscono con database, API, esecuzione di comandi e scrittura su sistemi di produzione. Nel ferroviario, un agente con accesso a interfacce SCADA potrebbe essere indotto, tramite descrittori di tool avvelenati, a modificare parametri operativi del segnalamento — soglie di frenatura automatica in CBTC o velocità massime su tratte specifiche. La mitigazione richiede scoping rigoroso dei permessi, esecuzione in sandbox, validazione degli argomenti e policy control su ogni invocazione, coerentemente con il principio di Minima Agenzia.

ASI08 – Cascading Failures è uno dei rischi più critici per il settore trasporti: un errore in un singolo agente può propagarsi attraverso pianificazione, esecuzione, memoria e sistemi downstream. In un ITS integrato, un errore nell'agente di gestione semaforica può propagarsi agli agenti di routing, priorità mezzi di emergenza e gestione parcheggi, causando congestione a cascata. Lo studio MAST (arXiv 2503.13657, oltre 1.600 tracce di esecuzione) ha identificato 14 modalità di fallimento in tre categorie — System Design (44,2%), Inter-Agent Misalignment (32,3%) e Task Verification (23,5%). Le mitigazioni richiedono confini di isolamento, rate limit, circuit breaker e testing pre-deployment di piani multi-step.

La rilevanza operativa dei rischi agentici è confermata da casi documentati. Il threat group FAMOUS CHOLLIMA, affiliato alla DPRK (Corea del Nord), utilizza GenAI per l'intero ciclo di vita delle operazioni di infiltrazione tramite falsi lavoratori IT: generazione di CV, preparazione ai colloqui, comunicazione aziendale e coding assistito, con oltre

320 aziende infiltrate e un aumento del 220% anno su anno (CrowdStrike Global Threat Report 2025). Questo caso dimostra come i rischi ASI01 (Goal Hijack — gli agenti GenAI operano con obiettivi nascosti) e ASI04 (Supply Chain — l'identità stessa del lavoratore è falsificata tramite AI) siano già sfruttati operativamente. Le aziende del settore trasporti — OEM, system integrator, fornitori di infrastruttura — che assumono personale IT remoto sono esposte allo stesso vettore: un lavoratore infiltrato con accesso a sistemi SCADA, fleet management o infrastruttura C-ITS costituisce un insider threat persistente.

I tre principi architetturali **OWASP — Minima Agenzia, Osservabilità Forte e Checkpoint Deterministici** — forniscono un framework operativo per la progettazione sicura dei sistemi AI agentici nel settore trasporti. L'applicazione del principio di Minima Agenzia ai sistemi di **trasporto** implica che un agente AI per la gestione semaforica debba avere accesso esclusivamente ai parametri dei cicli semaforici della propria area di competenza, senza possibilità di modificare configurazioni di rete, accedere a dati dei passeggeri o interagire con sistemi di segnalamento ferroviario. L'Osservabilità Forte richiede che ogni azione di un agente AI su infrastrutture critiche di trasporto sia tracciata in log immutabili, con registrazione dello stato obiettivo, del reasoning e degli strumenti invocati — un requisito coerente con le prescrizioni di logging della direttiva NIS2 (Art. 21.2f) e con i requisiti di trasparenza dell'AI Act (Art. 13).

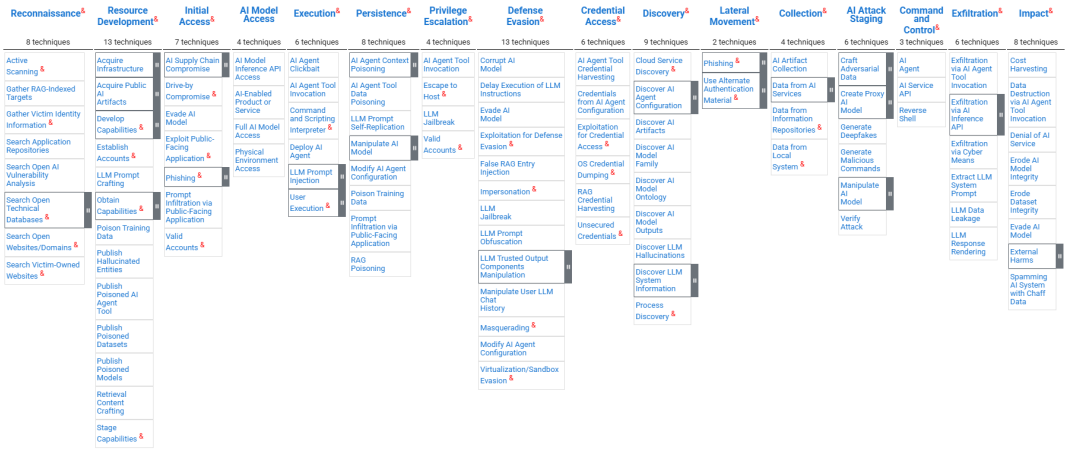
I Checkpoint Deterministici assumono particolare rilevanza nei sistemi di trasporto safety-critical: ogni azione di un agente AI che influisce sulla sicurezza operativa — modifica di parametri di segnalamento, variazione di piani di traffico, intervento su sistemi di frenatura — deve prevedere un punto di verifica obbligatorio che consenta la validazione umana o automatizzata prima dell'esecuzione. Questo principio è direttamente allineato con il concetto di human oversight dell'AI Act (Art. 14), che richiede che i sistemi AI ad alto rischio consentano la supervisione umana effettiva durante il periodo di utilizzo, e con il requisito IEC 62443 di Safety Integrity Level (SIL) per le funzioni di sicurezza nei sistemi di controllo industriale.

4.4.3 MITRE ATLAS: tassonomia strutturata degli attacchi AI

Se le classificazioni OWASP analizzate nelle sezioni precedenti rispondono alla domanda «quali rischi prioritizzare?», il framework MITRE ATLAS (Adversarial Threat Landscape for Artificial Intelligence Systems) risponde a una domanda complementare: «come si sviluppano concretamente gli attacchi contro i sistemi AI?».

ATLAS è una base di conoscenza strutturata di tattiche, tecniche e procedure (TTP) avversarie specifiche per i sistemi di AI, sviluppata e mantenuta dal MITRE Corporation — la stessa organizzazione che ha creato il framework ATT&CK, divenuto lo standard de facto per la modellazione delle minacce nella cybersecurity tradizionale.

La struttura di ATLAS ricalca intenzionalmente quella di ATT&CK: le tattiche rappresentano gli obiettivi strategici dell'avversario (reconnaissance, resource development, initial access, execution, evasione, esfiltrazione), le tecniche descrivono il «come» operativo di ciascuna tattica, e i case study documentano evidenze reali di attacchi osservati in ambiente operativo.



Matrice MITRE ATLAS: tattiche e tecniche di attacco ai sistemi AI (Fonte: MITRE Corporation, atlas.mitre.org)

Per gli operatori, ATLAS scompone ciascun attacco nelle singole azioni tecniche, consentendo difese mirate per fase. Un Red Team che valuta un sistema AI di gestione del traffico può simulare sequenze realistiche dalla ricognizione (modelli ML in uso, dataset di training, API esposte) all'accesso iniziale (manipolazione input), all'impatto finale (evasione del modello, esfiltrazione dati, degradazione prestazioni). Questa granularità rende ATLAS particolarmente utile per le valutazioni di rischio richieste dall'AI Act (Art. 9) e per i penetration test specifici dei sistemi AI.

NIST AI 100-2 E2025 è un aggiornamento sostanziale rispetto alla versione E2023, da tassonomia teorica a documento operativo che incorpora scenari reali e nuove categorie 2024-2025: clean-label poisoning, indirect prompt injection cross-context, energy-latency attacks, e i vettori specifici per agenti AI (riconosciuti come categoria distinta). Il documento NIST funziona da lingua franca: quando un operatore italiano segnala un incidente all'ACN e uno tedesco al BSI, la tassonomia comune consente classificazione e confronto delle minacce a livello internazionale.

4.4.4 Maturità operativa degli attacchi basati su GenAI

I framework OWASP (§4.2.2-§4.2.3) e MITRE ATLAS (§4.2.4) classificano i rischi AI; questa sezione esamina come **l'AI generativa sia passata da strumento sperimentale a vettore d'attacco operativo** — un'evoluzione che trasforma radicalmente il landscape delle minacce per il settore trasporti.

L'adozione incontrollata dell'AI generativa all'interno delle organizzazioni — il fenomeno noto come **shadow AI** — funge da amplificatore critico della superficie d'attacco. I dati disponibili delineano un quadro preoccupante: secondo il Cost of Data Breach Report 2025 di IBM, le organizzazioni che utilizzano shadow AI affrontano un costo medio delle violazioni superiore di 670.000 dollari rispetto alla media del settore (4,63 milioni contro 3,96 milioni di dollari). Check Point ha rilevato nel novembre 2025 che 1 prompt su 35 inviato a sistemi GenAI comporta rischio di data leakage, con l'87% delle organizzazioni che riportano problematiche di sicurezza legate all'uso di AI generativa. Gartner stima che oltre il 40% delle implementazioni AI nelle imprese coinvolga shadow AI — strumenti e modelli utilizzati senza la supervisione del dipartimento IT — e prevede che entro il 2030 oltre il 40% delle imprese subirà incidenti di sicurezza originati da sistemi AI non governati.

Di fronte a questa evoluzione, i sistemi di rilevamento basati su firme (signature-based detection), che costituiscono ancora la dorsale della sicurezza in molte infrastrutture ITS, risultano strutturalmente inadeguati. Un malware con integrazione LLM come LAMEHUG genera comandi dinamicamente ad ogni esecuzione: il codice prodotto è diverso ogni volta, rendendo impossibile la costruzione di firme statiche. Il traffico di rete verso le API dei modelli linguistici — come le chiamate di LAMEHUG verso HuggingFace — appare indistinguibile dalle comunicazioni legittime verso

servizi cloud di machine learning, che un numero crescente di sistemi ITS utilizza per la manutenzione predittiva, l'analisi del traffico e l'ottimizzazione operativa. Il phishing generato con GenAI è polimorfico e contestualizzato: ogni messaggio è unico, adattato al destinatario e privo delle anomalie linguistiche che i filtri tradizionali utilizzano come indicatori.

L'accelerazione delle capacità offensive GenAI sta generando un'asimmetria crescente tra la velocità di adozione delle tecniche di attacco e la velocità di implementazione delle difese corrispondenti. Le previsioni Gartner indicano che il 29% delle organizzazioni ha già subito attacchi alla propria infrastruttura GenAI nel 2025, e che oltre l'80% delle campagne di phishing a livello globale sfrutta già tecniche AI-enhanced. Per gli operatori del settore trasporti — che gestiscono infrastrutture critiche con cicli di vita ventennali e processi di aggiornamento necessariamente graduali — questa asimmetria richiede un'azione immediata: non è possibile attendere che le soluzioni di difesa AI-native raggiungano piena maturità prima di iniziare ad adottarle.

4.4.5 Failure cascading nei sistemi multi-agente

Le architetture multi-agente analizzate in precedenza introducono rischi specifici quando più agenti AI autonomi collaborano, si delegano compiti e condividono contesti operativi di rischi qualitativamente diversa: i failure cascading, in cui un errore o una compromissione in un singolo agente si propaga attraverso l'intero sistema, amplificandosi ad ogni passaggio. L'OWASP Top 10 for Agentic Applications ha classificato questo rischio come ASI08 (Cascading Failures), descrivendone i meccanismi nella sezione 4.2.3: un planner che produce task errati li distribuisce a multipli agenti esecutori; uno stato avvelenato si propaga attraverso agenti di deployment e policy; feedback loop tra agenti che consumano reciprocamente output corrotti generano divergenze incontrollate.

La prima tassonomia empirica dei failure mode nei sistemi multi-agente basati su LLM è stata sviluppata da Cemri, Pan, Yang e colleghi (MAST — Multi-Agent System Failure Taxonomy, marzo 2025). Lo studio ha analizzato oltre 1.600 tracce di esecuzione annotate attraverso 7 framework multi-agente tra i più diffusi, utilizzando 4 modelli linguistici di riferimento (GPT-4, Claude 3, Qwen2.5, CodeLlama), con un accordo inter-annotatore $\kappa = 0{,}88$ — un valore elevato che indica una tassonomia robusta e riproducibile. L'analisi ha identificato 14 failure mode distinti, raggruppati in tre categorie principali: System Design Issues (44,2% dei failure osservati), Inter-Agent Misalignment (32,3%) e Task Verification Issues (23,5%).

La categoria predominante — System Design Issues (44,2% dei failure) — comprende errori di scomposizione dei task, assegnazione dei ruoli e definizione delle interfacce tra agenti. Esempio nel trasporto: un sistema multi-agente di gestione integrata del traffico fallisce perché l'ottimizzazione semaforica viene assegnata a un agente privo di informazioni sui flussi pedonali. La seconda categoria — Inter-Agent Misalignment (32,3%) — documenta agenti con obiettivi formalmente compatibili ma risultati conflittuali nella pratica. La terza — Task Verification (23,5%) — riguarda la qualità degli output e la propagazione degli errori, con allucinazioni accettate acriticamente da agenti downstream.

Per le **infrastrutture di trasporto intelligenti**, le implicazioni dei failure cascading sono amplificate dall'interconnessione tra sottosistemi e dalla dimensione safety-critical delle decisioni. Si consideri uno scenario di gestione integrata del traffico urbano basata su agenti AI: un agente di analisi dei flussi produce una valutazione errata della congestione in un corridoio principale, basandosi su dati sensoriali degradati; l'agente di gestione semaforica, che riceve questa valutazione come input, modifica i cicli semaforici del corridoio; gli agenti di routing delle flotte di trasporto pubblico reagiscono alla nuova configurazione semaforica deviando i percorsi; l'agente di gestione delle emergenze, ricevendo informazioni contraddittorie sulla viabilità, potrebbe ritardare l'instradamento di mezzi di soccorso. In questo scenario, un singolo errore di valutazione si propaga attraverso quattro livelli del sistema, con un impatto che cresce ad ogni passaggio — e potenzialmente con conseguenze sulla sicurezza delle persone.

4.4.6 SOC potenziati dall'AI: automazione e accelerazione della difesa

La terza generazione — il SOC agentico — segna un salto qualitativo: agenti AI autonomi che analizzano alert, correlano evidenze cross-domain, conducono investigazioni multi-step ed eseguono azioni di risposta secondo playbook approvati con guardrail. A differenza dei playbook SOAR tradizionali, basati su sequenze predefinite e trigger specifici, gli agenti AI ragionano su contesti non previsti e adattano la strategia investigativa. Particolarmente rilevante per i trasporti: la convergenza OT/IT genera scenari cross-domain (segnalamento ferroviario, bigliettazione, V2X, fleet management) che superano le capacità di un analista singolo o di un playbook statico.

L'adozione di **architetture SOC potenziate dall'AI** e guidata da fattori convergenti che rendono insostenibile il modello tradizionale basato sulla capacita umana. Il primo fattore e il *volume degli alert*: un SOC tradizionale di un grande operatore ferroviario o autostradale può ricevere migliaia di alert giornalieri dai propri sistemi di monitoraggio — reti IT aziendali, sistemi SCADA, piattaforme cloud, dispositivi IoT infrastrutturali, sistemi di bigliettazione, reti di comunicazione operativa — di cui la stragrande maggioranza sono falsi positivi o eventi a bassa priorita che tuttavia richiedono triage umano.

Il secondo fattore, strettamente correlato, e la *velocita degli attacchi moderni*: le tecniche GenAI documentate nella sezione 4.2.5 consentono agli attaccanti di generare varianti di malware in tempo reale e di condurre campagne di phishing personalizzate a scala industriale, comprimendo la finestra di risposta da giorni a minuti. L'interazione tra questi due fattori crea una pressione insostenibile sugli analisti umani, che devono processare volumi crescenti di alert in tempi sempre piu ristretti.

Il terzo fattore — il piu strutturale — è la *carenza globale di professionisti di cybersecurity*. Secondo l'ISC2 2024 Cybersecurity Workforce Study, la forza lavoro globale in cybersecurity ammonta a 5,5 milioni di professionisti, con una crescita dello 0,1% anno su anno — una stagnazione di fatto. Il gap tra domanda e offerta ha raggiunto 4,8 milioni di professionisti necessari ma non disponibili, con un aumento del 19% rispetto all'anno precedente. Il 90% delle organizzazioni intervistate riporta carenze di competenze cybersecurity, e il 58% ritiene che queste carenze comportino un rischio concreto per la propria sicurezza. Per gli operatori di trasporto, questa carenza e amplificata dalla competizione per talenti con settori tradizionalmente piu attrattivi — servizi finanziari, tecnologia, difesa — e dalla necessita di competenze ibride OT/IT raramente disponibili sul mercato del lavoro.

La cybersecurity degli ITS può essere rafforzata tramite AI avanzata anche con modelli predittivi per identificare comportamenti anomali, per la correlazione eventi che unisce dati da telecamere, scambi V2X e reti stradali e per automazione delle risposte con il seguente schema di massima.

Rilevamento delle intrusioni con AI

- Machine learning per anomaly detection sui dati di rete e dei sensori;
- Analisi predittiva per anticipare *pattern* sospetti e prevenire incidenti;
- Adaptive *Intrusion detection systems* (IDS) in grado di aggiornarsi dinamicamente.

Protezione dei modelli AI

- *Adversarial training* per migliorare la robustezza contro perturbazioni malevole;
- *Defensive distillation* per rendere il modello più resistente agli attacchi;
- Monitoraggio *runtime* dei modelli per identificare output anomali;
- *Continual learning* per affrontare minacce emergenti e scenari non previsti.

Security Automation

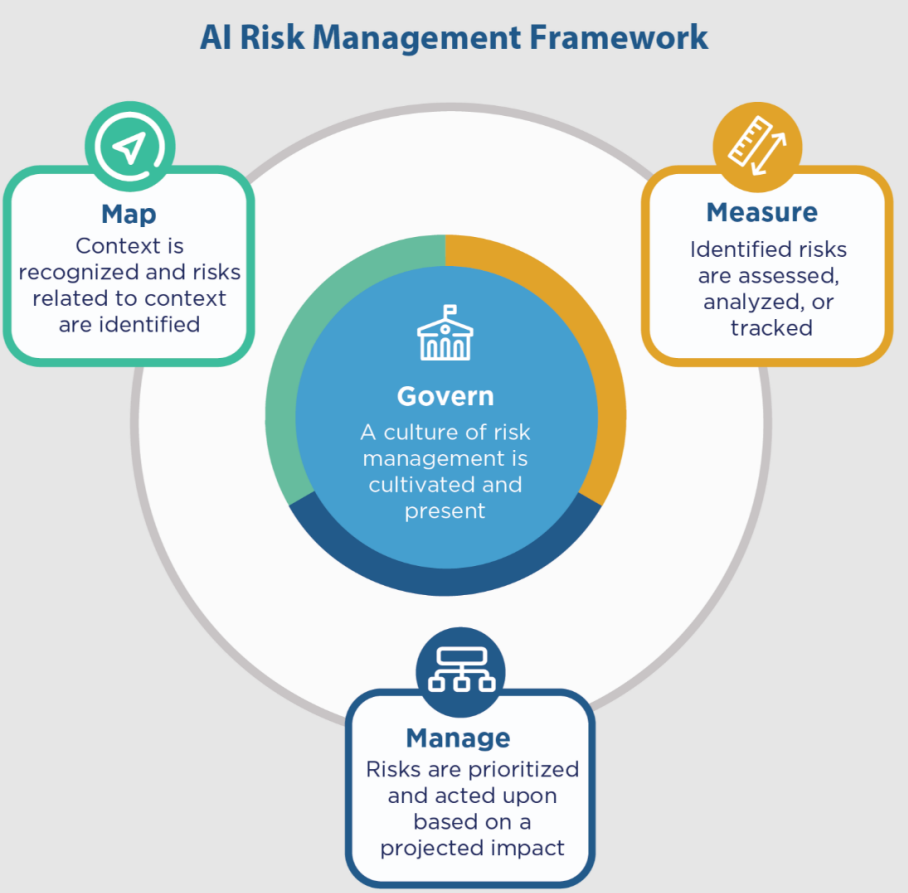
- Automated Incident Response (AIR): attivazione automatica di contromisure;
- AI-driven threat intelligence, basata su correlazioni tra grandi volumi di dati;
- Automazione della gestione degli aggiornamenti (patch) a valle di un'analisi del rischio che determina un livello di sicurezza inadeguata, con l'obiettivo di ridurre al minimo le finestre di vulnerabilità.

L'AI Security nei trasporti riguarda quindi l'uso dell'AI per prevenire incidenti, attacchi informatici, frodi e minacce fisiche, migliorando al tempo stesso affidabilità e resilienza dei sistemi di mobilità.

4.4.7 Metodi AI per la cybersecurity nei trasporti: capacità, limiti e applicazioni

Questa sezione presenta gli **otto metodi AI principali per la cybersecurity nei trasporti**, organizzati come schede operative. Per ciascun metodo sono indicate: tecniche AI sottostanti, applicazioni concrete nel settore trasporti e vantaggi documentati con fonti istituzionali.

I SOC potenziati dall'AI (cfr. §4.4.7) rappresentano il nucleo operativo della difesa automatizzata; le capacità di detection, triage e response che li definiscono trovano applicazione concreta nei metodi descritti.



Funzioni core del NIST AI Risk Management Framework: Govern, Map, Measure, Manage (Fonte: NIST AI 100-1)

Di seguito una panoramica chiara dei principali metodi utilizzati, con esempi pratici.

	Metodo	Tecniche chiave	Applicazioni ITS	Vantaggio
1	Computer Vision	CNN, YOLO, Faster R-CNN	Rilevamento ostacoli, monitoraggio stazioni	Riduzione tempo risposta incidenti
2	Anomaly Detection	ML non supervisionato, Autoencoder, LSTM	Guasti veicoli, manomissioni sensori	Prevenzione incidenti anticipata
3	Cybersecurity AI	IDS con AI, Deep Learning, RL	Protezione V2X, difesa SCADA	Sicurezza dinamica adattiva
4	Sicurezza veicoli autonomi	Sensor fusion, modelli predittivi	Prevenzione collisioni, anti-spoofing GPS	Affidabilità decisionale
5	Predictive Maintenance	ML supervisionato, time-series	Previsione guasti, monitoraggio infrastrutture	-60% ritardi per guasti
6	Gestione traffico/emergenze	RL, modelli predittivi	Ottimizzazione flussi, evacuazione intelligente	Riduzione tempi intervento
7	Sicurezza dati e Privacy	Federated Learning, Differential Privacy, XAI	Protezione dati passeggeri, audit modelli	Conformità GDPR
8	Contrasto frodi/minacce interne	Behavioral analytics, Graph ML	Frodi biglietti, insider threat	Riduzione perdite economiche

1. Computer Vision per la sicurezza fisica

Metodo

- Reti neurali convoluzionali (CNN);
- Object detection (YOLO, Faster R-CNN);
- Video analytics in tempo reale (la supply chain security dei modelli AI, tema trasversale che collega MLSecOps — §4.2.6 — all'ecosistema delle startup specializzate, è analizzata nel §5.2 — Ecosistema startup per la cybersecurity nei trasporti);

Applicazioni

- Rilevamento di ostacoli su strade e ferrovie;
- Monitoraggio stazioni, aeroporti e porti;
- Individuazione di comportamenti anomali (intrusioni, abbandono di oggetti);
- Controllo automatico dei binari e delle infrastrutture.

Vantaggio: riduzione del tempo di risposta agli incidenti. I modelli YOLO ottimizzati per edge computing raggiungono latenze compatibili con i requisiti operativi delle stazioni ad alto traffico, con TRL 7-9 per applicazioni standard di sorveglianza (OWASP, 2025).

2. Anomaly Detection (rilevamento anomalie)

Metodo

- Machine learning non supervisionato
- Autoencoder, Isolation Forest, LSTM

Applicazioni

- Individuazione di guasti nei veicoli
- Rilevamento di manomissioni su sensori
- Monitoraggio del traffico anomalo su reti di trasporto intelligenti

Vantaggio: prevenzione di incidenti prima che si verifichino. Il framework MARIS-ADS per la rete CAN ferroviaria raggiunge un'accuratezza del 99,3% con un tempo di inferenza di 0,31 millisecondi su hardware resource-constrained, consentendo il rilevamento di intrusioni nei sistemi di segnalamento CBTC in tempo reale.

3. Cybersecurity basata su AI

Metodo

- AI per intrusion detection systems (IDS)
- Deep learning per traffic analysis
- Reinforcement Learning per difesa adattiva

Applicazioni

- Protezione dei veicoli connessi (V2X)
- Difesa delle infrastrutture critiche (semafori intelligenti, SCADA)
- Rilevamento di attacchi zero-day

Vantaggio: sicurezza dinamica contro minacce in evoluzione. L'approccio di detection comportamentale è particolarmente rilevante contro il malware con integrazione LLM, i cui output polimorfi rendono inefficace la detection basata su firme (CrowdStrike, 2025).

4. AI per la sicurezza dei veicoli autonomi

Metodo

- Sensor fusion (LiDAR, radar, telecamere)
- Modelli predittivi del comportamento
- Redundant AI systems (Sistemi AI sovradimensionati)

Applicazioni

- Prevenzione collisioni
- Rilevamento di spoofing GPS
- Validazione delle decisioni del sistema di guida

Vantaggio: aumento dell'affidabilità decisionale. L'adversarial robustness dei modelli di percezione è critica e può essere valutata sistematicamente con strumenti come l'Adversarial Robustness Toolbox (cfr. §4.2.9).

5. Predictive Maintenance

Metodo

- Machine learning supervisionato
- Time-series analysis (Analisi dell'evoluzione temporale)

Applicazioni

- Previsione guasti su treni, autobus, aerei, strade, infrastrutture e dispositivi in essi integrati

- Monitoraggio di freni, motori e infrastrutture

Vantaggio: riduzione dei costi e aumento della sicurezza operativa. I risultati documentati nel settore ferroviario indicano riduzioni del 60% dei ritardi correlati a guasti e del 30% delle fermate impreviste, con ROI medio tra 12 e 24 mesi.

6. AI per la gestione del traffico e delle emergenze

Metodo

- Reinforcement Learning
- Modelli predittivi

Applicazioni

- Ottimizzazione dei flussi di traffico
- Gestione prioritaria dei mezzi di soccorso
- Evacuazione intelligente in caso di emergenza

Vantaggio: riduzione dei rischi e dei tempi di intervento. Nei sistemi multi-agente per la gestione integrata del traffico, i meccanismi di circuit breaker e fallback deterministici prevengono la propagazione a cascata di errori tra agenti interconnessi.

7. Sicurezza dei dati e Privacy-by-Design

Metodo

- Federated Learning
- Differential Privacy
- AI explainability (XAI)

Applicazioni

- Protezione dei dati dei passeggeri
- Conformità a GDPR
- Audit dei modelli AI per decisioni critiche

Vantaggio: fiducia degli utenti e conformità normativa. Il federated learning consente la formazione collaborativa di modelli di intrusion detection tra operatori europei senza centralizzazione dei dati operativi sensibili, come riconosciuto dall'EDPS (TechDispatch #1/2025).

8. AI per il contrasto a frodi e minacce interne

Metodo

- Behavioral analytics
- Graph-based machine learning

Applicazioni

- Rilevamento frodi nei biglietti
- Individuazione di insider threat

- Monitoraggio accessi non autorizzati

Vantaggio: riduzione delle perdite economiche e dei rischi interni

- Anomaly detection: accuracy documentata fino al 99,3%, deployment operativi in fleet management e monitoraggio reti, TRL 6-8 per applicazioni veicolari
- Computer vision per sorveglianza: già operativa in stazioni, porti e aree logistiche con track record pluriennale, TRL 7-9 per applicazioni standard
- Manutenzione predittiva: ROI medio del 30% documentato da operatori ferroviari, aeroportuali e logistici, TRL 7-8 per veicoli e infrastrutture

Al livello di **readiness media** — tecnologie in fase pilota o con limitazioni specifiche per il settore trasporti — si collocano:

- Cybersecurity AI-based per intrusion detection: matura per reti IT enterprise ma con customizzazione rilevante necessaria per reti OT ferroviarie e portuali, TRL 5-7 per OT
- NLP per threat intelligence: efficace per analisi automatizzata di report e feed di minacce ma con sfide di dominio specifiche per il vocabolario tecnico dei trasporti
- Federated learning per flotte condivise: promettente per fleet analytics senza centralizzazione dei dati ma con overhead computazionale e complessità di coordinamento tra operatori
- Simulazione multi-agente e digital twin: validata in ambienti di ricerca ma con gap tra fedeltà della simulazione e complessità dei sistemi di trasporto reali, TRL 4-6 per scenari complessi

9. Observability avanzata come abilitatore della threat detection nella mobilità

L'observability avanzata rappresenta un salto di paradigma rispetto al monitoraggio tradizionale: non si limita a raccogliere metriche, ma costruisce una comprensione in tempo reale dell'intero ecosistema cyber-fisico della mobilità. L'architettura sottostante si basa su una pipeline scalabile e distribuita che raccoglie e normalizza dati eterogenei — telemetria IoT da sensori, CAN bus e GPS, eventi applicativi, log di sicurezza, tracce distribuite e output dei modelli AI — lungo tutto lo stack, dall'edge ai gateway fino al cloud. Standard aperti come OpenTelemetry si stanno affermando come riferimento de facto per l'interoperabilità, affiancati da piattaforme come Grafana, Prometheus e Loki che consentono di costruire viste integrate e dinamiche su domini tradizionalmente separati.

È l'integrazione nativa con l'AI a rendere questo approccio realmente proattivo. Algoritmi di machine learning analizzano i flussi di telemetria per identificare pattern anomali, anticipare guasti attraverso la predictive maintenance e rilevare segnali deboli di attacchi informatici prima che si manifestino in modo evidente. Diversi operatori del settore hanno già adottato questo modello su larga scala: Uber monitora in tempo reale milioni di eventi attraverso piattaforme di observability avanzata; Deutsche Bahn ha integrato queste capacità nei propri processi di manutenzione predittiva e resilienza operativa; Volvo combina telemetria e monitoring avanzato per analizzare il comportamento dei veicoli in condizioni reali.

Un contributo significativo viene dall'integrazione della Explainable AI (XAI) nei sistemi di rilevamento delle intrusioni. Gli IDS tradizionali basati su AI operano come scatole nere, rendendo difficile comprendere il fondamento delle segnalazioni; la XAI li trasforma in strumenti trasparenti, permettendo agli analisti di identificare quali parametri — una latenza anomala, firme digitali sospette, una frequenza inattesa nei messaggi CAN — hanno attivato l'allarme. Questa comprensibilità non è solo un vantaggio operativo: riduce concretamente i falsi positivi e, sul piano dell'incident forensics, consente di ricostruire la catena decisionale di un veicolo in caso di incidente, facilitando la conformità all'AI Act e alla direttiva NIS2.

Una dimensione sempre più rilevante è quella della AI observability, che estende il monitoraggio dall'infrastruttura al comportamento stesso dei modelli: drift dei dati, variazioni di accuratezza, bias emergenti. Si crea così un ponte diretto tra observability e MLSecOps, dove la salute dei modelli diventa un oggetto di sorveglianza continua al pari dei sistemi che li ospitano. In prospettiva, l'evoluzione naturale è verso architetture self-healing, in cui il sistema non si limita a segnalare un problema ma attiva autonomamente contromisure — isolare un nodo compromesso,

ribilanciare il traffico, aggiornare un modello AI — trasformando l'observability da strumento di visibilità a motore attivo di resilienza.

10 Incident Response: coordinamento multiattore e comunicazione nella mobilità

Le capacità di SOC e threat detection devono essere completate dalla dimensione organizzativa della gestione degli incidenti. Nella mobilità, dove un attacco cyber può tradursi in rischio fisico immediato, sono necessari playbook specifici per settore: protocolli predefiniti che guidano la risposta a scenari tipici — compromissione di un ITS urbano, ransomware a una rete ferroviaria, manomissione telematica in una flotta logistica — coprendo contenimento, isolamento, comunicazione interna ed esterna, ripristino e analisi post-incidente. La risposta coinvolge gestori dell'infrastruttura, operatori del trasporto, PA, CSIRT nazionali e settoriali, forze dell'ordine e autorità (ANSF, ANSFISA, ENAC). La NIS2 impone obblighi specifici di notifica e coordinamento. Esercitazioni tabletop e red team congiunte sono indispensabili per validare i playbook. I playbook dovrebbero includere template di comunicazione pre-approvati e ruoli chiari per la gestione mediatica: messaggi contraddittori tra operatori e autorità erodono la fiducia più dell'incidente stesso.

4.4.8 La Protezione dei modelli AI

La protezione dei modelli AI nei sistemi di mobilità si articola su quattro dimensioni operative complementari: (1) robustezza avversariale del data layer, (2) protezione del modello in produzione (drift detection, sicurezza del deployment), (3) guardrails per l'AI generativa, (4) controllo della filiera dati. Le sezioni seguenti analizzano ciascuna dimensione, mappandola ai requisiti dell'AI Act (Art. 9 risk management, Art. 15 accuratezza e robustezza) e fornendo indicazioni operative per gli operatori di trasporto.

Il primo passaggio, quando si parla di protezione, è rendere osservabile e misurabile ciò che si pretende dal modello AI di mobilità. Senza una definizione chiara del perimetro di robustezza, ogni discussione sulle difese rischia di restare dichiarativa. La robustezza, qui, è la stabilità del modello rispetto a perturbazioni plausibili o intenzionali; non è una proprietà assoluta, ma una prestazione condizionata dal threat model e dal budget di perturbazione. In questo quadro si colloca l'adversarial training: la tecnica consiste nell'inserire in addestramento esempi avversari generati con attacchi controllati e nell'ottimizzare il modello affinché mantenga performance accettabili anche nel caso peggiore, entro un'intensità definita.

Robustezza avversariale dei modelli AI: gli attacchi avversariali racppresentano una minaccia concreta per i sistemi AI nella mobilità: la manipolazione di segnali stradali tramite perturbazioni visive impercettibili, l'avvelenamento dei dati di training per sistemi di previsione del traffico, e l'estrazione di modelli proprietari sono scenari documentati nella letteratura. L'Adversarial Robustness Toolbox (ART) è una libreria Python open-source (Linux Foundation AI) per la valutazione e difesa dei modelli ML contro attacchi avversariali, che supporta 4 categorie di attacco: evasion, poisoning, extraction, inference, è compatibile con TensorFlow, PyTorch, scikit-learn, XGBoost e altri framework. Applicazione ITS può essere per testare la robustezza dei modelli di riconoscimento della segnaletica, classificazione dei veicoli, e anomaly detection nei flussi di traffico. HEART (Hardened Extension of ART): estensione per workflow di test & evaluation strutturati

L'uso della distillation: la defensive distillation addestra un modello secondario sui soft labels (distribuzioni di probabilità) prodotti dal modello primario, anziché sulle hard labels: ne risulta una superficie decisionale più regolare, con gradienti meno sfruttabili dagli attacchi adversarial basati su perturbazione (Papernot et al., 2016). Nel contesto della mobilità, la tecnica trova applicazione nei modelli di percezione a bordo veicolo e negli anomaly detector sui flussi V2X, dove la stabilità rispetto a input manipolati è un requisito di safety. La distillation va però considerata anche come vettore di attacco: un avversario che interroga ripetutamente un modello in produzione può estrarne una copia surrogata (model extraction), aggirando la proprietà intellettuale e abilitando attacchi adversarial in white-box sul surrogato. Le contromisure operative includono rate limiting delle query, watermarking del modello, monitoraggio dei pattern di interrogazione anomali e logging coerente con i requisiti di tracciabilità dell'AI Act (Art. 12).

La protezione del modello durante il suo utilizzo

In esercizio, il modello AI di mobilità richiede protezione su tre fronti complementari. Il primo è l'integrità degli artefatti: firma digitale dei pesi, verifica del digest al caricamento, secure enclave per l'inferenza on-edge tramite TEE o moduli HSM integrati nelle unità ITS, in modo che un attaccante con accesso al filesystem non possa sostituire il modello con una variante compromessa. Il secondo è il controllo di runtime: input validation con rilevamento di perturbazioni avversariali e di campioni out-of-distribution, output filtering per coerenza con vincoli operativi (velocità ammissibili, traiettorie fisicamente plausibili, range di parametri di segnalamento) e fallback deterministico in caso di esito non affidabile. Il terzo è il monitoraggio continuo del drift, sia statistico (covariate shift, label shift su validation rolling) sia comportamentale (degrado di accuracy, aumento dell'incertezza calibrata), con trigger automatici di retraining o rollback. Il NIST AI RMF (funzione MEASURE) e l'AI Act (Art. 15) inquadrano questi controlli come requisiti per i sistemi ad alto rischio, fra cui rientrano molti dei sistemi AI applicati al trasporto.

Sicurezza dell'AI Generativa: Con la crescente adozione di modelli di AI generativa anche nel settore mobilità (assistenti virtuali per operatori, generazione di report, analisi di scenario), emergono nuove superfici di attacco: prompt injection, jailbreak, allucinazioni, e data leakage. I framework di guardrail per la GenAI implementano il rilevamento automatizzato di contenuti dannosi, dati personali esposti, tentativi di jailbreak e allucinazioni, in conformità con i requisiti dell'EU AI Act per i sistemi ad alto rischio (Art. 9, 15). L'ecosistema open-source offre diverse soluzioni mature: NeMo Guardrails (NVIDIA) per flussi conversazionali programmabili, LlamaFirewall (Meta, 2025) con riduzione del 90% del tasso di successo degli attacchi, e Guardrails AI con oltre 24 validatori per PII, tossicità e bias. Le piattaforme di governance dell'AI consentono la discovery degli asset AI non censiti (shadow AI), l'automazione del red-teaming tramite strumenti come PyRIT (Microsoft) e Garak (NVIDIA), e la validazione della conformità rispetto ai principali framework normativi. Il NIST AI RMF (AI 100-1) struttura queste capacità nelle funzioni GOVERN, MAP, MEASURE e MANAGE, mentre l'EU AI Act (Art. 9) impone un sistema di gestione del rischio continuo per i sistemi ad alto rischio.

Il controllo delle filiere dati

Sul piano organizzativo, nel 2026 restano centrali due vincoli: l'aumento degli attacchi e la pressione sulla supply chain, e l'evoluzione dei requisiti di compliance. Come già esaminato nel cap. 3, la NIS2, recepita con il D.Lgs. 138/2024 e con scadenze operative già fissate nel 2025, spinge ulteriormente verso processi dimostrabili e ripetibili: tracciabilità, audit, response plan e controlli su dati e modelli.

Data provenance e integrità dei dati AI tramite Blockchain/DLT

Blockchain e DLT sono tecnologie fondamentali per la protezione dei dati in ecosistemi distribuiti; esse forniscono un trust fabric che garantisce immutabilità, auditabilità e non ripudio: eventi critici e metadati vengono ancorati a un registro distribuito tramite hash crittografici, mentre i dati operativi restano off-chain. La DLT deve essere integrata con meccanismi di trusted data ingestion e secure hardware (TPM, secure enclave), poiché certifica l'immutabilità ma non la veridicità all'origine.

Adversarial attacks documentati e testing XAI nella mobilità

Nel 2018 ricercatori dell'Università di Berkeley dimostrarono come un adesivo nero su un cartello di STOP potesse indurre un sistema di visione artificiale a classificarlo come limite di velocità con probabilità superiore al 90%. Nel 2020 Google Brain estese questi risultati ai sistemi di object detection per veicoli autonomi, ingannabili attraverso pattern visivi proiettati su superfici urbane. Tesla riporta una riduzione del 95% degli errori causati da input manipolati nei test interni grazie ad adversarial training con scenari avversariali e filtri Randomized Smoothing. BMW utilizza il federated learning per migliorare i sistemi di assistenza alla guida senza raccogliere dati sensibili dei clienti, dimostrando la privacy by design.

Le tecniche XAI SHAP e LIME offrono capacità specifiche per il testing di sicurezza automotive, a complemento di ART e HEART. SHAP (SHapley Additive exPlanations) assegna un valore di importanza a ogni input per una specifica decisione: nei sistemi IDS aiuta a capire quali parametri V2X hanno spinto il modello a segnalare un attacco e a verificare l'assenza di combinazioni che causino manovre errate. LIME crea modelli semplificati attorno a singole decisioni, evidenziando quali pixel o bit V2X hanno causato un errore. Durante le fasi di Software-in-the-Loop (SIL), SHAP e LIME identificano i punti ciechi degli algoritmi prima della messa su strada, supportando la certificazione ISO 21434 e UNR155.

Sul piano della protezione del modello come asset, meccanismi di confidential computing consentono inferenze all'interno di enclave sicure (SGX, TrustZone), riducendo model stealing e esfiltrazione. Il watermarking dei modelli rileva copie non autorizzate. Piattaforme come Darktrace monitorano in tempo reale il traffico di rete dei veicoli connessi, identificando attacchi prima che raggiungano i sistemi safety-critical. Il progetto europeo SAIM (Securing AI for Mobility), con Volvo, Siemens e l'Università di Eindhoven, ha prodotto un framework di certificazione per modelli AI destinati ai veicoli autonomi e un database condiviso di attacchi avversariali. Amazon ha implementato modelli Isolation Forest nei magazzini automatizzati, riducendo del 40% gli errori di gestione delle scorte causati da data poisoning.

Il consorzio MOBI (Ford, GM, BMW, Renault, IBM, Bosch) standardizza l'identità veicolare su blockchain, consentendo ai veicoli di dimostrare in modo crittograficamente verificabile il proprio stato prima di interagire con infrastrutture critiche. Un progetto congiunto MOBI+DARPA garantisce la tracciabilità immutabile delle decisioni AI nei veicoli autonomi: ogni azione critica (frenata, cambio di corsia) viene registrata on-chain con timestamp crittografico, con comunicazioni crittografate e verificabili contro attacchi man-in-the-middle. IOTA, DLT a grafo aciclico (DAG) ottimizzata per IoT, abilita comunicazioni V2X tamper-proof a bassa latenza con validazione AI edge-native.

IBM Food Trust combina blockchain e sensori IoT per tracciare in tempo reale la catena del freddo durante il trasporto di alimenti deperibili: algoritmi AI analizzano i pattern dei dati IoT per distinguere tra guasti operativi e tentativi di manomissione deliberata, con evidenze integre e verificabili a posteriori. TradeLens (Maersk + IBM) ha dimostrato come la condivisione sicura e verificabile di documenti tra spedizionieri, dogane e porti possa ridurre i tempi di sdoganamento da giorni a minuti e abbattere il rischio di frodi documentali — contraffazione di polizze di carico e certificati di origine, un vettore d'attacco che costa miliardi di euro all'anno nel commercio marittimo.

4.5 Vantaggi strategici della convergenza ITS–AI–Cybersecurity

I domini della mobilità connessa — veicoli, infrastrutture ITS, comunicazioni V2X, piattaforme MaaS, sistemi energetici e supply chain — non possono più essere considerati silos indipendenti.

Dal punto di vista della cybersecurity, essi costituiscono un ecosistema interconnesso in cui una vulnerabilità locale genera impatti sistemici: l'attacco a CDK Global (giugno 2024) ha bloccato 15.000 concessionari per tre settimane con danni superiori a 1 miliardo di dollari (CNBC, 2024).

I principali domini architetturali della mobilità intelligente vanno quindi visti come componenti di un'unica catena di valore digitale, ponendo le basi per una visione architetturale integrata.

Per abilitare questa catena del valore, è fondamentale superare la logica dei silos tecnologici adottando un livello di integrazione digitale che disaccoppi i sistemi di backend dai canali di fruizione. Questa architettura consente di aggregare i dati provenienti da fonti eterogenee (sensori, veicoli, database) rendendoli disponibili in tempo reale e 24/7, garantendo al contempo che i sistemi critici sottostanti rimangano protetti.

La frammentazione degli strumenti di sicurezza rappresenta una sfida operativa significativa: secondo Gartner (2024), le organizzazioni gestiscono in media 45 soluzioni di cybersecurity, con il 65% che consolida attivamente per migliorare la postura di rischio. Le ricerche sulla convergenza delle piattaforme di sicurezza (Palo Alto Networks,

2025, n=1.000) mostrano un ROI del 101% per le organizzazioni con approccio integrato, contro il 28% di quelle con strumenti frammentati.

I benefici economici della convergenza sono quantificabili: secondo il Cost of a Data Breach Report (Ponemon Institute, 2025), le organizzazioni con AI security estensiva risparmiano in media 1,9 milioni di dollari per incidente e riducono il ciclo di vita delle violazioni di 80 giorni. Il costo medio di una violazione nel settore trasporti raggiunge i 3,98 milioni di dollari (Ponemon Institute, 2025). I SOC potenziati dall'AI registrano riduzioni del 64% nei tempi di identificazione e ROI stimato al 304% (IDC/Splunk).

In generale, l'integrazione sinergica di questi tre pilastri consente: maggiore sicurezza stradale grazie a sistemi predittivi; riduzione delle interruzioni operative causate da attacchi cyber; ottimizzazione del traffico e riduzione dei costi; maggiore fiducia degli utenti e delle istituzioni.

In particolare si hanno vantaggi importanti anche in specifici settori della mobilità quali:

- **Veicoli autonomi** — sistemi di percezione resilienti a dati alterati, verifica di integrità dei sensori, monitoraggio più affidabile sullo stato del veicolo;
- **Smart mobility urbana** — coordinamento sicuro tra trasporto pubblico, micromobilità e infrastrutture, sistemi di risposta rapida a incidenti cyber tramite AI, ottimizzazione predittiva del traffico;
- **Flotte commerciali** — dashboard di rischio in tempo reale, AI per la manutenzione predittiva con integrazione cyber, segmentazione della rete e protezione dei sistemi di gestione.

4.6 Applicazione del quadro normativo per la cybersecurity nei trasporti

4.6.1 Il quadro regolatorio europeo: una rete normativa interconnessa

Il quadro regolatorio europeo per la cybersecurity nei trasporti si articola su tre pilastri orizzontali — NIS2, AI Act e CRA — già analizzati in dettaglio nel Capitolo 3 di questo documento (cfr. §3.2 NIS2, §3.3 AI Act, §3.7 CRA). Questa sezione si concentra sulle implicazioni mobility-specific. Gli operatori del settore trasporti devono applicare simultaneamente la NIS2 (sicurezza delle reti e dei sistemi informativi a livello di entità), l'AI Act (conformità dei sistemi AI classificati come ad alto rischio nella gestione del traffico, della segnaletica intelligente, della manutenzione predittiva e dei sistemi di pagamento dei pedaggi) e il CRA (prodotti digitali integrati nei sistemi di trasporto). A questi pilastri si aggiungono le normative settoriali UNECE R155/R156 per i veicoli omologati e gli standard IEC 62443 e CLC/TS 50701 per le infrastrutture industriali e ferroviarie.

La gerarchia applicativa è regolata dall'Art. 4 della NIS2, che riconosce la prevalenza di atti settoriali quando questi prevedano requisiti di sicurezza «al meno equivalenti»: ad oggi solo il regolamento DORA per il settore finanziario ha ottenuto questo riconoscimento, mentre per i trasporti la NIS2 rimane il framework di riferimento generale. L'implicazione operativa è che gli operatori devono progettare programmi di compliance integrati capaci di gestire requisiti potenzialmente sovrapposti, con notifiche di incidente verso autorità diverse (CSIRT nazionale per NIS2, autorità di vigilanza del mercato per AI Act, ENISA per il CRA). Il principio di Compliance by Design (cfr. §4.6.8) consente di trasformare questa complessità in vantaggio strategico, integrando i controlli sin dalla progettazione delle architetture e dei processi.

4.6.2 NIS2 e il recepimento italiano: D.Lgs. 138/2024

La Direttiva NIS2 e il D.Lgs. 138/2024 di recepimento italiano costituiscono il pilastro centrale della cybersecurity per le infrastrutture critiche di trasporto; il quadro generale è analizzato nel Capitolo 3 (cfr. §3.2). Per il settore mobilità, l'Allegato I del decreto qualifica i trasporti come settore ad alta criticità articolato in quattro sotto-settori: aereo (vettori, gestori aeroportuali, controllo del traffico aereo), ferroviario (imprese ferroviarie, gestori

dell'infrastruttura, ERTMS), marittimo e fluviale (compagnie di navigazione, enti di gestione portuale, VTS) e stradale (gestori di ITS e operatori di pedaggi). Un'estensione tutta italiana è contenuta nell'Allegato IV del D.Lgs. 138/2024, che amplia il perimetro degli operatori soggetti rispetto al testo della direttiva.

Le specifiche tecniche di attuazione sono fissate dalla Determinazione del Direttore Generale ACN n. 379907 del 18 dicembre 2025. Il regime di notifica degli incidenti (Art. 25) prevede un meccanismo a tre livelli — pre-notifica al CSIRT entro 24 ore, notifica entro 72 ore, relazione finale entro un mese — che richiede infrastrutture di rilevamento e comunicazione automatizzate. La maturità della cybersecurity nel settore varia significativamente tra sotto-settori, come documentato dal report ENISA NIS360 2024: il marittimo italiano è collocato nella «risk zone», con conseguente priorità di investimento. Il regime sanzionatorio (Art. 38) prevede sanzioni fino a 10 milioni di euro o al 2% del fatturato globale per le entità essenziali. La timeline di compliance per gli operatori italiani è serrata: registrazione sul portale ACN entro il 28 febbraio 2025, applicazione delle misure di sicurezza dal 16 ottobre 2025.

4.6.3 AI Act e classificazione dei trasporti ad alto rischio

L'AI Act (Reg. UE 2024/1689) interviene su un piano complementare alla NIS2: regola la conformità dei sistemi di AI in funzione del loro livello di rischio. Il quadro generale è descritto nel Capitolo 3 (cfr. §3.3). Per il settore della mobilità, la classificazione si articola su due livelli con implicazioni operative differenti. L'Annex III, Punto 2 dell'AI Act qualifica come ad alto rischio i sistemi AI utilizzati nella gestione e nell'esercizio di infrastrutture critiche di trasporto stradale, ferroviario e per la fornitura di acqua, gas, riscaldamento ed elettricità. Sono inclusi i sistemi AI per il controllo del traffico, la segnaletica intelligente, la manutenzione predittiva di infrastrutture critiche, i sistemi di pagamento elettronico dei pedaggi e i sistemi di sorveglianza aeroportuale e ferroviaria.

La timeline applicativa è scandita: dal 2 febbraio 2025 sono operativi i divieti sulle pratiche AI inaccettabili (Art. 5); dal 2 agosto 2025 si applicano gli obblighi su general-purpose AI; dal 2 agosto 2026 entrano in vigore gli obblighi per i sistemi ad alto rischio (Art. 16-29), inclusi sistema di gestione del rischio (Art. 9), governance dei dati di training (Art. 10), documentazione tecnica (Art. 11), tracciamento (Art. 12), trasparenza e supervisione umana (Art. 14), accuratezza e robustezza (Art. 15). Un elemento di incertezza è la proposta Digital Omnibus della Commissione (autunno 2025), che potrebbe modificare l'Annex III; il nuovo Art. 60a proposto introdurrebbe inoltre un sandbox regolamentare per il settore trasporti.

Sul piano nazionale, la Legge 132/2025 (in vigore dal 10 ottobre 2025) costituisce la prima legge italiana sull'AI con disposizioni specifiche su responsabilità civile e penale. L'interazione AI Act–NIS2 è particolarmente rilevante: l'Art. 9 dell'AI Act sul risk management può essere integrato nei processi di gestione del rischio NIS2, evitando duplicazioni. Per gli operatori di trasporto italiani la pianificazione deve essere differenziata in base alla tipologia di sistema AI utilizzato e alla data di immissione sul mercato.

4.6.4 Cyber Resilience Act e prodotti digitali per i trasporti

Il Cyber Resilience Act (Reg. UE 2024/2847), descritto nel Capitolo 3 (cfr. §3.7), completa il quadro normativo introducendo requisiti di security-by-design per i prodotti con elementi digitali immessi sul mercato europeo. Per il settore trasporti, l'applicabilità del CRA segue una regola cardine: i veicoli soggetti a omologazione tipo (UNECE R155, automobili e veicoli commerciali) sono esclusi dal CRA e rimangono nel regime UNECE; sono invece pienamente soggetti al CRA i componenti dell'infrastruttura di trasporto. Le Roadside Unit (RSU) per la comunicazione V2X, i sistemi di pagamento elettronico dei pedaggi, i sistemi di gestione del traffico, i dispositivi IoT per il monitoraggio strutturale di ponti e gallerie, le telecamere e i sensori per la sorveglianza, i sistemi SCADA e ICS per il controllo della segnaletica e i dispositivi mobili per il personale operativo di trasporto rientrano tutti nel perimetro del CRA.

Sebbene l'uso del CRA come strumento sia attualmente in fase di valutazione da parte della Commissione, va ricordato come la timeline di applicazione preveda milestone ravvicinate: dall'11 dicembre 2027 entrano in vigore gli obblighi sostanziali (security-by-design, vulnerability handling, SBOM, notifica incidenti). La relazione tra CRA e NIS2 è di complementarità non di sovrapposizione: il CRA disciplina i prodotti, la NIS2 le entità che li utilizzano. Le

notifiche di incidente seguono trigger distinti — ENISA per il CRA (vulnerabilità sfruttate), CSIRT nazionale per la NIS2 (incidenti significativi). Il CRA prevede un meccanismo di semplificazione della compliance duale: per i prodotti che incorporano sistemi AI ad alto rischio, la conformità ai requisiti CRA può essere riconosciuta come adempimento parziale degli obblighi AI Act sulla cybersecurity (Art. 15 AI Act). Un punto critico per i produttori di componenti ITS è l'attuale assenza di standard armonizzati verticali specifici, che impone il ricorso agli standard generali ETSI EN 303 645 e IEC 62443 in attesa della pubblicazione della normativa di settore.

4.6.5 Standard settoriali e convergenza normativa globale

Accanto alle normative orizzontali europee, la cybersecurity nei trasporti si fonda su un articolato sistema di standard settoriali a livello internazionale. I regolamenti UNECE R155 (Cybersecurity Management System) e R156 (Software Update Management System), già richiamati nel Capitolo 3 (cfr. §3.5), costituiscono il framework di riferimento per i veicoli a motore omologati. Il Supplement 3 al R155, in vigore dal 10 gennaio 2025 (Reg. UE 2025/5), ha esteso il perimetro applicativo ai veicoli pesanti, agli autobus e ai veicoli specializzati, oltre alle automobili e ai veicoli commerciali leggeri originariamente coperti. Il quadro UNECE opera nell'ambito del WP.29 (Forum mondiale per l'armonizzazione dei regolamenti sui veicoli, 54 paesi membri), garantendo riconoscimento internazionale delle omologazioni.

Lo standard cinese GB 44495-2024 introduce requisiti specifici di test di penetrazione, certificazione obbligatoria di laboratori cinesi e localizzazione dei dati di sicurezza, imponendo ai costruttori operanti su entrambi i mercati di progettare programmi di compliance dual-track. Il confine tra i regimi R155 e CRA è centrale per gli operatori: i veicoli omologati restano nel perimetro UNECE, mentre i loro componenti e i sistemi di infrastruttura ricadono nel CRA.

Nel dominio delle infrastrutture industriali e dei sistemi OT (Operational Technology), la serie IEC 62443 costituisce il framework di riferimento globale. Gli aggiornamenti recenti rafforzano gli strumenti operativi in cui la IEC 62443-3-2 (giugno 2020) definisce la metodologia di assessment del rischio per zone e conduit.

Si tenga presente che i concetti di Zone (Aree di sicurezza), Conduit (Canali di comunicazione) e Zero Trust costituiscono i pilastri della moderna sicurezza informatica, sia in ambito IT (reti aziendali) che OT (sistemi industriali). Le **Zone** infatti sono i raggruppamenti di dispositivi o risorse digitali che condividono requisiti di sicurezza simili mentre i **Conduit** sono i canali o percorsi circoscritti che collegano e regolano il traffico tra le diverse Zone, proteggendo i dati in transito. Il concetto **Zero Trust** descritto nel paragrafo successivo impedisce a utenti, app o dispositivi di accedere automaticamente a una rete o a una zona, richiedendo continue autenticazioni. Unire questi tre elementi significa costruire un sistema dove ogni area della rete è isolata e monitorata.

Nella prassi industriale e nelle analisi tecniche di settore, la serie IEC 62443 è riconosciuta come framework appropriato per dimostrare il rispetto degli obblighi NIS2 di gestione del rischio nei sistemi OT, in quanto fornisce metodologie consolidate per la segmentazione tramite zone e conduit, la defense in depth e la calibrazione dei Security Level proporzionati al profilo di minaccia. Pur non costituendo essa stessa un atto giuridico equivalente ex Art. 4 NIS2 — riconoscimento ad oggi formalizzato solo per DORA nel settore finanziario — la sua adozione è coerente con le indicazioni operative della ENISA NIS2 Technical Implementation Guidance v1.0 (giugno 2025) e con la prassi consolidata di settore (cfr. DNV, «Leverage IEC 62443 for EU NIS2 Directive compliance», 2024).

L'interazione tra standard settoriali e normative orizzontali configura un quadro coerente: la IEC 62443 fornisce gli strumenti operativi per la cybersecurity industriale; le specifiche CENELEC e ferroviarie ne contestualizzano l'applicazione settoriale; le normative orizzontali (NIS2, AI Act, CRA) impongono i requisiti vincolanti a livello di entità o prodotto. Per gli operatori di trasporto, la strategia di compliance integrata prevede l'adozione degli standard settoriali come riferimento tecnico per l'implementazione dei requisiti normativi orizzontali.

4.6.6 Cybersecurity Act 2.0: la proposta di riforma della certificazione europea

L'interazione tra standard settoriali e normative orizzontali sollecita un meccanismo unificato di certificazione, oggetto della proposta Cybersecurity Act 2.0 (CSA2). Il 20 gennaio 2026, la Commissione europea ha presentato

la proposta di regolamento COM(2026) 11, denominata Cybersecurity Act 2.0, con l'obiettivo di rafforzare il ruolo di ENISA, ampliare lo schema di certificazione europea (EUCC) e introdurre meccanismi di mutual recognition tra schemi nazionali. Per il settore dei trasporti, la CSA2 avrebbe un impatto diretto su molteplici dimensioni: le regole sulla sicurezza degli operatori di trasporto verrebbero allineate ai criteri ENISA, con possibili semplificazioni delle procedure di assessment per i prodotti ITS già certificati a livello nazionale. La proposta potrebbe inoltre introdurre uno schema di certificazione specifico per i prodotti ad alto rischio AI Act, completando il quadro applicativo dell'Art. 15 dell'AI Act. Lo stato dell'iter legislativo richiede appropriata cautela: a febbraio 2026 la proposta è in prima lettura presso il Parlamento europeo e il Consiglio, con tempistiche di approvazione attese non prima del 2027. Gli operatori di trasporto dovrebbero seguirne l'evoluzione per anticipare gli adeguamenti necessari ai propri programmi di certificazione e governance.

4.6.7 Cronologia integrata e strategia di compliance unificata

La convergenza delle scadenze normative nel periodo 2026-2027 impone agli operatori di trasporto un calendario serrato di adeguamento. Il quadro complessivo, già richiamato nel Capitolo 3 (cfr. §3.8), si articola in quattro ondate principali. La prima ondata (gennaio-luglio 2026) include l'entrata in vigore degli obblighi NIS2 sostanziali per le entità essenziali registrate sul portale ACN, l'applicazione del Supplement 3 al R155 per veicoli pesanti e specializzati, e l'obbligo di pre-notifica incidenti al CSIRT entro 24 ore. La seconda ondata (estate 2026), particolarmente impattante, concentra le scadenze più critiche: il 2 agosto 2026 entrano in vigore gli obblighi sostanziali per i sistemi AI ad alto rischio (Art. 16-29 dell'AI Act), inclusi quelli utilizzati nella gestione del traffico e nelle infrastrutture critiche di trasporto. La terza ondata (autunno 2026) concentra le scadenze più dense per la governance complessiva: entro il 10 ottobre 2026 dovranno essere completate le notifiche degli operatori di servizi essenziali sotto la NIS2, le designazioni delle autorità competenti e i piani di gestione del rischio cyber. La quarta ondata (2027) completa il quadro con le scadenze a più lungo termine: l'11 dicembre 2027 segna la piena obbligatorietà degli obblighi sostanziali del CRA per i prodotti immessi sul mercato europeo.

La complessità del quadro non è ingestibile se affrontata con una strategia di compliance unificata: il principio di Compliance by Design (cfr. §4.6.8) consente di sfruttare le sovrapposizioni parziali tra framework, integrando i controlli sin dalla progettazione delle architetture e dei processi. La gestione integrata di rischio, documentazione tecnica e governance riduce significativamente il costo complessivo della compliance e ne aumenta la robustezza. Permangono tuttavia gap normativi rilevanti: a febbraio 2026 non esiste una guida ENISA specifica per l'applicazione integrata di NIS2, AI Act e CRA al settore trasporti; gli standard armonizzati settoriali per il CRA sono in fase di definizione; il riconoscimento di equivalenza degli standard IEC 62443 ai sensi dell'Art. 4 NIS2 non è ancora formalizzato. Gli operatori di trasporto dovrebbero pianificare un programma di compliance multi-anno, con priorità alle scadenze immediate del 2026 e con piena integrazione tra i diversi requisiti normativi.

4.6.8 Il concetto di Compliance by design

Il concetto di «Compliance by Design» va collegato esplicitamente alla timeline normativa e cioè NIS2 (già in vigore, con liste di entità essenziali entro aprile 2025), CRA (reporting obbligatorio da settembre 2026, piena conformità da dicembre 2027) e AI Act (conformity assessment per sistemi ad alto rischio da agosto 2026). Il quadro normativo europeo (EU AI Act, NIS2, CRA, UN R155/R156) non deve essere percepito solo come onere ma come opportunità di differenziazione. L'adozione proattiva di un approccio «Compliance by Design» consente agli operatori di trasformare gli obblighi regolatori in vantaggio competitivo.

Il principio di Compliance by Design trasforma l'adeguamento normativo da esercizio reattivo a proprietà intrinseca dell'architettura di sistema. Per gli operatori del trasporto, questo significa integrare i requisiti di NIS2, AI Act e CRA fin dalla fase di progettazione, sfruttando le sovrapposizioni tra i framework per ridurre la complessità di conformità (per la cronologia dettagliata delle scadenze, cfr. §4.4.7).

La sovrapposizione parziale dei requisiti tra i diversi framework normativi rende possibile e conveniente un approccio unificato: la gestione del rischio richiesta dalla NIS2 (Art. 21) soddisfa in larga parte i requisiti di risk management dell'AI Act (Art. 9); le procedure di vulnerability handling del CRA si allineano con gli obblighi di incident reporting

della NIS2; le certificazioni IEC 62443 possono essere riutilizzate come evidenze di conformità sia per la NIS2 sia per i framework settoriali (come descritto nel Capitolo 3). Un operatore del trasporto che implementa oggi un framework di governance integrato sarà pronto per tutte queste scadenze, riducendo i costi di compliance e accelerando il time-to-market dei nuovi servizi digitali.

L'automazione della compliance attraverso strumenti di continuous monitoring e framework machine-readable come NIST OSCAL (CSWP 53, dicembre 2025) consente la verifica continua della conformità, trasformando la compliance da esercizio periodico a proprietà intrinseca del sistema.

4.6.9 ROI della convergenza AI e cybersecurity

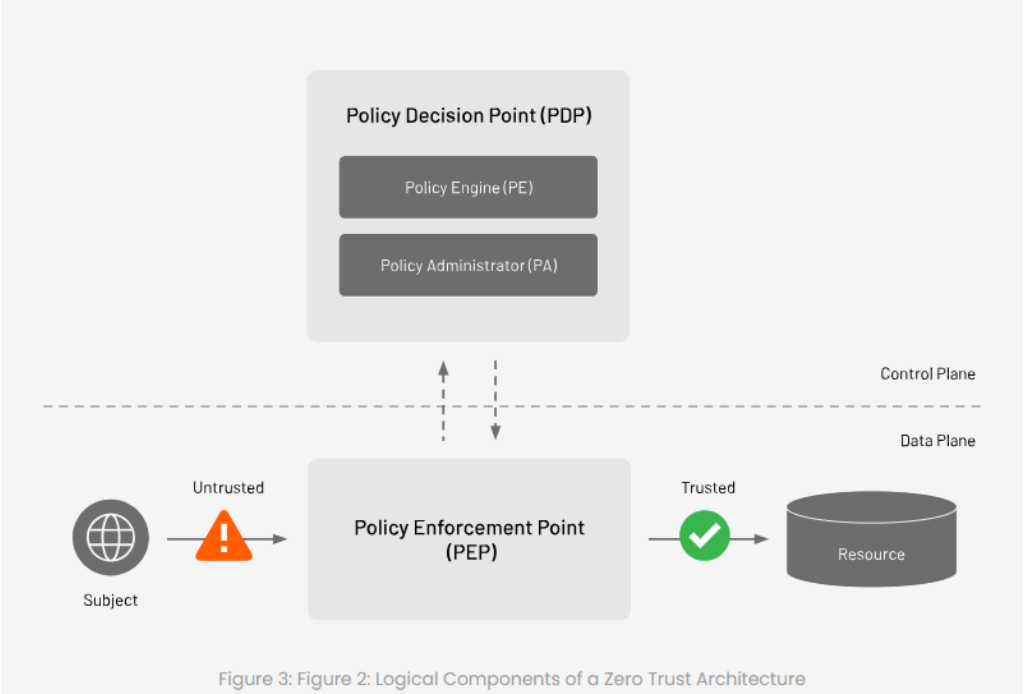
Per gli operatori di trasporto, il calcolo del ROI della convergenza AI-cybersecurity si articola su tre dimensioni complementari. La prima è il risparmio diretto derivante dall'evitamento dei costi di breach: le organizzazioni con AI security estensiva documentano risparmi medi di 2,22 milioni di dollari per incidente rispetto a quelle prive di automazione (Ponemon Institute, 2025). La seconda dimensione è l'efficienza operativa generata dall'automazione del triage e dell'investigazione, che libera risorse qualificate in un contesto di carenza strutturale del settore. La terza è la riduzione dei costi di compliance derivante dall'approccio unificato ai diversi framework normativi, dove la sovrapposizione dei requisiti NIS2, AI Act e CRA consente economie di scala nella governance. Secondo le analisi di settore, **l'adozione di piattaforme integrate riduce i tempi di rilevamento e risposta di oltre il 70% e i costi operativi di sicurezza del 30–40%.**
A complemento delle metriche MTTD/MTTR già documentate, indicatori specifici per i sistemi AI completano il quadro: tasso di drift dei modelli (frequenza e ampiezza delle deviazioni), tasso di falsi positivi e negativi nei sistemi di anomaly detection, copertura dei test avversariali (percentuale degli scenari di attacco noti effettivamente testati), tempo medio di aggiornamento dei modelli in produzione. In ecosistemi con trust scoring dinamico, il trust score medio della flotta, la frequenza delle degradazioni e il tempo di recupero offrono una visione aggregata dello stato di affidabilità. Per i decisori pubblici, il costo per punto percentuale di riduzione del rischio e il rapporto tra investimento in sicurezza e riduzione attesa delle perdite supportano le decisioni di allocazione. Dashboard integrate alimentate dai sistemi di observability consentono una gestione del rischio dinamica e data-driven.

Nel settore ferroviario, i tempi di rientro dell'investimento per soluzioni integrate di manutenzione predittiva e cybersecurity si attestano tra 12 e 24 mesi, confermando la sostenibilità economica dell'approccio anche per operatori di medie dimensioni. Lo studio IDC/Splunk documenta un ROI del 304% per le piattaforme di sicurezza unificata, con il 64% di identificazione più rapida delle minacce e il 55% di risoluzione più rapida degli incidenti.

4.7 Architetture sicure per la mobilità intelligente

4.7.1 Architettura Zero Trust per ITS e sistemi OT

Il paradigma Zero Trust, formalizzato nel NIST SP 800-207 (agosto 2020 - https://csrc.nist.gov/publications/detail/sp/800-207/final), si fonda sul principio «*never trust, always verify*»: nessun componente del sistema — utente, dispositivo, rete o applicazione — è considerato affidabile a priori, indipendentemente dalla sua posizione nella topologia di rete. Ogni richiesta di accesso è valutata dinamicamente sulla base di identità, contesto, postura di sicurezza del dispositivo e policy definite. Nei sistemi ITS, questo principio si traduce nell'eliminazione della fiducia implicita tra componenti tradizionalmente considerati «interni»: RSU, OBU, controllori semaforici, sistemi SCADA di segnalamento ferroviario e piattaforme di gestione flotte. Il mercato Zero Trust Architecture vale 19,2 miliardi di dollari (2024), con proiezione verso 69-84 miliardi entro il 2032 (CAGR 17,4%).



Architettura logica Zero Trust con Policy Engine, Policy Administrator e Policy Enforcement Point (Fonte: NIST SP 800-207)

L'applicazione di Zero Trust ai trasporti richiede un adattamento sostanziale rispetto al contesto IT tradizionale. I sistemi OT di trasporto operano con vincoli strutturali specifici: requisiti di latenza hard real-time (sub-100 millisecondi per messaggi V2X safety-critical), dispositivi legacy con cicli di vita di 20-30 anni privi di capacità di autenticazione moderna, protocolli proprietari non compatibili con gli stack di sicurezza standard, e connettività intermittente in ambienti mobili. Ciononostante, il principio di verifica continua è applicabile: la micro-segmentazione delle reti V2X, l'autenticazione basata su certificati per ogni componente e il monitoraggio comportamentale dei dispositivi sono implementazioni concrete del modello Zero Trust nel dominio trasporti.

Il **CISA Zero Trust Maturity Model versione 2.0** (aprile 2023 - https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf) articola il percorso di maturità Zero Trust in cinque pilastri, ciascuno con applicazioni specifiche nel contesto dei sistemi di trasporto intelligente. Il pilastro Identity gestisce l'autenticazione di veicoli, utenti e infrastrutture tramite PKI (Public Key Infrastructure) e certificati digitali; nel contesto V2X, il framework D-IM (Decentralized Identity Management) basato su blockchain (Hyperledger Iroha) ha dimostrato una riduzione del 65% delle superfici di attacco con overhead contenuto (degradazione PRR inferiore al 7% in scenari urbani, latenza aggiuntiva inferiore a 0,06 secondi per comunicazioni C-V2X).

La validazione empirica dell'approccio Zero Trust per i sistemi Internet of Vehicles (IoV) è supportata da risultati promettenti: il framework SIoV-DS raggiunge il 99,78% di accuratezza nella rilevazione di anomalie su dataset IoV, con spiegabilità SHAP integrata per gli analisti SOC — elemento che risponde al requisito di trasparenza dell'AI Act per i sistemi ad alto rischio nel dominio trasporti (Annex III, Punto 2). Inoltre, l'87% dei professionisti OT riconosce Zero Trust come l'approccio corretto per la sicurezza operativa (Palo Alto Networks, 2024), segnalando un consenso settoriale ampio nonostante le sfide implementative nei sistemi legacy.

Il documento «Zero Trust for Operational Technology Activities and Outcomes», pubblicato dal Department of Defense (DoD) Chief Information Officer (CIO), il 18 novembre 2025 (https://dodcio.defense.gov/Portals/0/Documents/Library/ZT-OperationalTechnologyActivitiesOutcomes.pdf), costituisce il riferimento più maturo per l'applicazione di Zero Trust agli ambienti OT. Il framework definisce 105 attività distribuite su sette pilastri (User, Device, Network/Environment, Application/Workload, Data, Visibility/Analytics, Automation/Orchestration): 84 attività sono classificate come Target (da completare entro

FY2030) e 21 come Advanced (entro FY2033). A differenza del CISA ZTMM v2.0, che riconosce esplicitamente il proprio gap nella copertura OT, il documento DoD è progettato specificamente per sistemi di controllo industriale e include i sistemi di trasporto nel proprio perimetro applicativo.

Il settore ferroviario offre l'esempio più avanzato di implementazione Zero Trust nel dominio trasporti, attraverso uno stack normativo integrato che collega sicurezza funzionale (safety) e cybersecurity. La norma EN 50159:2010+A1:2020 definisce il modello di sicurezza delle comunicazioni ferroviarie articolato in tre categorie: Categoria 1, rete chiusa senza accesso esterno (ad esempio bus di interlocking interni); Categoria 2, rete aperta con accesso controllato (ad esempio GSM-R con autenticazione SIM); Categoria 3, rete aperta con accesso non controllato (ad esempio internet pubblico o future reti 5G/FRMCS). Per ciascuna categoria, la norma identifica sette minacce principali — ripetizione, cancellazione, inserimento, risequenziamento, corruzione, ritardo e mascheramento — e prescrive otto difese: numero di sequenza, marca temporale, timeout, identificatore sorgente/destinazione, messaggio di feedback, procedura di identificazione, codice di sicurezza e tecniche crittografiche.

La specifica tecnica CLC/TS 50701:2023 costituisce il ponte tra la sicurezza funzionale di EN 50159 e la cybersecurity industriale di IEC 62443, mappando il modello zone/conduit di IEC 62443 sulla topologia ferroviaria. Questa integrazione consente di definire livelli di sicurezza (Security Level 1-4 secondo IEC 62443) per ciascuna zona della rete ferroviaria, dalle sale apparati agli impianti di linea, dal bordo treno ai sistemi di terra. La specifica è in corso di internazionalizzazione come IEC 63452, la cui pubblicazione è attesa nel corso del 2026 [DA VERIFICARE], consolidando il modello di cybersecurity ferroviaria a livello globale e facilitando l'adozione da parte di operatori e fornitori extra-europei.

L'attuale protocollo Euroradio, utilizzato per le comunicazioni ERTMS/ETCS di Categoria 2 e 3 secondo EN 50159, impiega l'algoritmo 3DES con chiavi a 192 bit e codici MAC per l'autenticazione dei messaggi di segnalamento. Questo algoritmo presenta una vulnerabilità teorica nota: dopo circa 2^32 blocchi cifrati (circa 32 gigabyte di dati per sessione), la probabilità di collisione diventa rilevante. Nel contesto ferroviario operativo, questa vulnerabilità è mitigata dalla rotazione delle chiavi di sessione e dal volume limitato di dati trasmessi per sessione, che resta ordini di grandezza inferiore alla soglia critica. Tuttavia, l'obsolescenza progressiva di 3DES — deprecato dal NIST nel 2023 e previsto per dismissione entro il 2025 nel contesto IT — costituisce una delle motivazioni architetturali per la migrazione verso FRMCS (Future Railway Mobile Communication System), che adotta nativamente la suite crittografica 5G comprensiva di 5G-AKA, privacy SUPI/SUCI e TLS 1.3.

Le sfide dell'**implementazione Zero Trust nei sistemi OT di trasporto** restano consistenti: dispositivi legacy installati decenni fa senza capacità di autenticazione robusta, requisiti di latenza hard real-time incompatibili con processi di verifica complessi, protocolli proprietari non supportati dagli stack di sicurezza standard, e connettività intermittente in ambienti mobili come treni, veicoli e droni. I report Fortinet «State of Operational Technology and cybersecurity» documentano tuttavia un'evoluzione positiva della convergenza IT/OT: nel survey 2024, il 73% delle organizzazioni aveva subito almeno un breach con impatto sui sistemi OT (era 49% nel 2023); nel survey 2025, il 52% delle organizzazioni ha registrato zero intrusioni nell'ultimo anno (era 6% nel 2022). Questi dati, che misurano metriche differenti in periodi differenti, non sono contraddittori ma documentano un percorso: la consapevolezza del problema (73% breach) precede e motiva le contromisure che producono risultati (52% zero intrusioni).

Un indicatore chiave di questa maturità è l'evoluzione della governance: la responsabilità della sicurezza OT è passata dal 16% al 52% sotto il CISO/CSO, con il 78% delle organizzazioni che ha consolidato i fornitori di sicurezza a 1-4 vendor e l'80% che prevede di spostare la governance OT sotto il CISO. Per le organizzazioni al livello di maturità 4 (il più alto nella scala Fortinet), la quota con zero intrusioni raggiunge il 65%. Questi dati indicano che l'implementazione progressiva di principi Zero Trust e la convergenza organizzativa IT/OT producono risultati misurabili, anche in ambienti OT complessi come quelli dei trasporti — a condizione che l'approccio sia sistematico, sostenuto dal vertice aziendale e integrato con le specificità operative del settore.

Principi base

In un ecosistema senza perimetri definiti, la sicurezza non può più basarsi sulla difesa di un confine. Sembra necessario un approccio olistico, integrato fin dalla progettazione e basato su principi di massima diffidenza e verifica continua i cui principi sono:

Defense in Depth: sicurezza a strati. Molteplici livelli di controlli di sicurezza (hardware, software, comunicazioni, cloud) sono implementati per garantire che la compromissione di un singolo strato non pregiudichi l'intero sistema. Il modello di riferimento è definito dalla serie IEC 62443 con il concetto di zone e conduit: ciascuna zona operativa (veicolo, stazione, centro di controllo) è isolata da confini logici, con i conduit che regolano i flussi informativi tra zone secondo livelli di sicurezza graduati (Security Level 1–4). Per le infrastrutture di trasporto, i livelli si articolano in: sicurezza hardware (secure elements, HSM conformi ai profili EVITA, moduli TPM); sicurezza software e firmware (sandboxing, hypervisor sicuri, validazione del codice); protezione delle comunicazioni V2X (crittografia, autenticazione, anti-replay); edge computing sicuro per ridurre latenza ed esposizione del dato.

Secure by Design: la sicurezza è integrata, non aggiunta. Le considerazioni di cybersecurity sono parte integrante di ogni fase del ciclo di vita, dalla progettazione e sviluppo fino alla dismissione, riducendo le vulnerabilità a monte.

AI-Assisted Security — SOC intelligente per la mobilità: rappresenta un'area ad alto potenziale dove l'AI diventa strumento attivo di difesa.

Architetture Resilienti per ITS + AI

L'adozione di piattaforme in grado di aggregare dati da più fonti ed esporre secondo i formati richiesti quanto normato è cruciale per rispettare i requisiti dell'ITS. La convergenza IT/OT nei trasporti richiede il superamento di paradigmi di sicurezza storicamente separati: i sistemi IT privilegiano riservatezza e integrità, mentre i sistemi OT priorizzano disponibilità e sicurezza funzionale. Per garantire resilienza è necessario:

- Adottare architetture Zero Trust per tutte le comunicazioni;
- Segmentare la rete ITS per contenere attacchi;
- Utilizzare firmware e software firmati digitalmente;
- Implementare digital twin per testare scenari e possibili vulnerabilità;
- Assicurare che modelli AI siano explainable e monitorati costantemente.

Quantum-Safe Cryptography per la mobilità del futuro: le infrastrutture ITS hanno cicli di vita decennali. I veicoli e le RSU installati oggi saranno operativi nel 2035–2040, quando i computer quantistici potrebbero essere in grado di violare la crittografia attuale. La minaccia Harvest Now, Decrypt Later (HNDL) — la raccolta preventiva di comunicazioni cifrate da parte di gruppi APT per decrittarle quando i computer quantistici saranno operativi — rende urgente l'adozione di crittografia post-quantistica già in fase di progettazione. L'architettura di riferimento descrive il percorso di migrazione.

Integrazione AI + Cybersecurity

- Modelli AI integrati direttamente nei sistemi di controllo per difesa in tempo reale;
- Threat modeling specializzato per architetture basate su AI;
- Digital twin di sicurezza per simulare attacchi e testare resilienza.

Architettura di riferimento per la convergenza ITS–AI–Cybersecurity

La crescente complessità dei sistemi di mobilità intelligente richiede un'evoluzione delle architetture di sicurezza, che non possono più essere concepite come elementi accessori o perimetrali, ma come componenti strutturali dell'intero ecosistema ITS.

In uno scenario caratterizzato da veicoli connessi, infrastrutture distribuite, piattaforme digitali e modelli di AI operanti in tempo reale, la sicurezza deve essere affrontata come una proprietà emergente dell'architettura, non come una funzione isolata.

Questa architettura di riferimento non rappresenta un modello rigido, ma una cornice evolutiva che consente a Pubbliche Amministrazioni, gestori di infrastrutture e operatori industriali di progettare sistemi adattabili alle specificità del proprio contesto operativo e alle evoluzioni normative in corso. L'accelerazione regolatoria — con la NIS2 applicabile dal 15 gennaio 2026 (determinazioni ACN), l'AI Act in vigore graduale dal 2025 al 2027, e il CRA dal dicembre 2027 — impone un'architettura capace di incorporare nuovi requisiti senza riprogettazione strutturale.

Il Gruppo di Lavoro propone quindi una architettura di riferimento basata sulla convergenza di tre domini tecnologici:

- ITS, come infrastruttura digitale distribuita della mobilità;
- AI, come motore di analisi, previsione e supporto decisionale;
- Cybersecurity, come sistema immunitario dell'ecosistema.

Tale architettura si fonda su alcuni principi chiave:

Security by Design e by Default

Da quanto sin qui illustrato appare necessario integrare Security by Design fin dalla fase di progettazione, nonché adottare modelli AI trasparenti e spiegabili (XAI).

La sicurezza deve essere integrata fin dalle fasi di progettazione di veicoli, infrastrutture e piattaforme digitali, lungo l'intero ciclo di vita del sistema, riducendo l'esposizione a vulnerabilità strutturali e facilitando la conformità normativa.

Zero Trust applicato alla mobilità

In un contesto privo di perimetri definiti, nessun attore — veicolo, infrastruttura, applicazione o utente — può essere considerato affidabile a priori. Ogni interazione deve essere autenticata, autorizzata e monitorata in modo continuo.

Architettura multilivello e distribuita

La sicurezza deve essere implementata in modo coerente su più livelli:

- Edge (veicoli, sensori, RSU), per garantire reazioni rapide e continuità operativa, con moduli HSM e secure elements per la protezione crittografica nel silicio;
- Comunicazioni (V2X, 5G, reti IP), per proteggere integrità e autenticità dei flussi informativi tramite crittografia end-to-end e certificati pseudonimi conformi a ETSI TS 103 097;
- Backend e cloud, per analisi avanzate, orchestrazione e correlazione degli eventi tramite SOC AI-driven che integrano telemetria IT, OT e veicolare in un'unica piattaforma di correlazione;
- Livello dati, per garantire protezione, qualità e governance delle informazioni utilizzate dai modelli AI.

Preparazione post-quantum: le infrastrutture ITS, con cicli di vita di 15–20 anni, devono adottare un percorso di migrazione verso la crittografia post-quantum per contrastare la minaccia Harvest Now, Decrypt Later (HNDL). L'approccio ibrido — che affianca algoritmi tradizionali ai nuovi standard post-quantum del NIST — consente una transizione graduale senza interruzione dei servizi operativi, proteggendo fin da oggi le comunicazioni V2X e i flussi SCADA destinati a restare in esercizio per decenni.

Integrazione tra AI e cybersecurity

I modelli di AI devono essere sia protetti sia utilizzati come strumenti di difesa, abilitando:

- Rilevamento precoce di anomalie e comportamenti anomali;
- Analisi predittiva delle minacce;
- Supporto automatizzato alla risposta agli incidenti.

Declinazioni settoriali e simulazione

L'architettura di riferimento deve essere poi declinata ed integrata per soddisfare le necessità dei differenti settori della mobilità (automotive, logistica, ecc).

In ottica MaaS e NIS2 è poi importante garantire un censimento centralizzato degli asset che garantisca governance e un approccio di "Compliance by Design": l'utilizzo di meccanismi automatici (come scorecard di conformità) all'interno delle piattaforme di sviluppo consente di verificare in tempo reale se le tecnologie aderiscono alle regole, bloccando preventivamente il rilascio di software non conforme e individuando azioni correttive su quanto già in produzione

4.7.2 Crittografia post-quantum per le infrastrutture di trasporto

Il modello Zero Trust garantisce la verifica continua di identità e autorizzazioni a livello logico; tuttavia, la sicurezza crittografica su cui si fonda l'intera catena di fiducia è oggi minacciata dall'emergere del computing quantistico.

Il 13 agosto 2024 il **NIST ha finalizzato i primi tre standard di crittografia post-quantum**, segnando il passaggio dalla fase di ricerca alla standardizzazione operativa. FIPS 203 definisce machine learning-KEM (Module-Lattice-Based Key-Encapsulation Mechanism), basato sul problema Module Learning With Errors (MLWE) per l'incapsulamento delle chiavi; FIPS 204 definisce Module-Lattice-Based Digital Signature Algorithm (ML-DSA) per le firme digitali, anch'esso basato su reticoli; FIPS 205 definisce Stateless Hash-Based Digital Signature Algorithm (SLH-DSA), che adotta un approccio basato su funzioni hash per fornire diversità crittografica rispetto agli algoritmi lattice-based. Tre dei quattro algoritmi originariamente selezionati nel processo di standardizzazione includono contributi di ricercatori IBM.

A marzo 2025 il NIST ha selezionato Hamming Quasi-Cyclic (HQC) come quinto algoritmo di backup per il key encapsulation, basato su error-correcting codes anziché reticoli, garantendo diversità algoritmmica in caso di vulnerabilità future nei costrutti lattice-based. FIPS 206, che standardizzerà FN-DSA (Fast Fourier lattice-based compact signatures, precedentemente noto come Falcon), si trova attualmente in fase di Initial Public Draft in clearance presso NIST/DoC, con pubblicazione finale attesa per fine 2026 o inizio 2027. Ai fini della pianificazione della migrazione PQC nelle infrastrutture di trasporto, la priorità operativa rimane sui tre standard già finalizzati (FIPS 203, 204, 205), che forniscono una base completa per l'avvio della transizione.

La minaccia Harvest Now, Decrypt Later (HNDL) è il vettore più insidioso per le infrastrutture di trasporto: gruppi APT state-sponsored stanno già raccogliendo comunicazioni cifrate — incluse comunicazioni V2X, flussi SCADA ferroviari e dati di gestione flotta — con l'obiettivo di decrittarle quando i computer quantistici crittograficamente rilevanti (CRQC) saranno operativi. La probabilità di realizzazione di un CRQC capace di violare RSA-2048 supera il 50% entro il 2035 secondo le stime del settore. A maggio 2025, il team Google Quantum AI ha pubblicato una stima aggiornata secondo cui RSA-2048 potrebbe essere violato con meno di 1 milione di qubit rumorosi, una riduzione del 95% rispetto alle stime del 2019, accelerando in misura netta la timeline della minaccia quantistica.

Il disallineamento tra i cicli di vita delle infrastrutture ITS e la timeline della minaccia quantistica crea un'urgenza strutturale unica nel settore trasporti. I semafori intelligenti hanno cicli di vita di circa 20 anni, i sistemi di segnalamento ferroviario superano i 30 anni: le infrastrutture installate oggi saranno operative fino al 2040-2055, ben oltre la potenziale finestra di disponibilità dei CRQC. Questo significa che ogni decisione crittografica presa oggi

per le infrastrutture di trasporto deve già considerare la minaccia quantistica, non come scenario futuro ma come parametro di progettazione attuale.

Il **NIST IR 8547**, pubblicato a novembre 2024, stabilisce il calendario formale per la deprecazione degli algoritmi crittografici classici: RSA-2048 e ECC-256 saranno deprecati (sconsigliati per nuovi sistemi) entro il 2030 e proibiti (non più accettati per nessun utilizzo) entro il 2035. Questa timeline non è un'aspirazione ma un requisito tecnico che influenzerà la conformità dei prodotti digitali per i trasporti, con implicazioni dirette per il CRA (cfr. Cap. 4.3) che richiede il rispetto degli standard crittografici riconosciuti per i prodotti con elementi digitali. (i bandi Digital Europe DEPLOY-CYBER-07, con 31 milioni di euro per la transizione PQC, sono analizzati nel §5.3.2 — ECCC e bandi Digital Europe 2025-2027)

Il **programma Cryptographic National Security Algorithm Suite 2.0** (CNSA 2.0) della NSA, aggiornato a maggio 2025, impone requisiti ancora più stringenti: dal 1° gennaio 2027 tutte le nuove acquisizioni per i sistemi di sicurezza nazionale devono essere conformi CNSA 2.0, con transizione completa entro il 2035. Gli algoritmi approvati CNSA 2.0 sono gli stessi standard NIST (machine learning-KEM, machine learning-DSA, SLH-DSA), creando convergenza globale. Sebbene il requisito CNSA 2.0 sia formalmente vincolante per i sistemi di sicurezza nazionale statunitensi, la sua applicazione per analogia è rilevante per il settore trasporti europeo: la data del 1° gennaio 2027 stabilisce un benchmark globale per le nuove acquisizioni che influenzerà le catene di fornitura internazionali.

Il 23 giugno 2025 la Commissione Europea e gli Stati membri hanno pubblicato il **Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography**, documento di attuazione della Raccomandazione (UE) 2024/1101 dell'11 aprile 2024. La roadmap stabilisce una timeline vincolante a tre fasi per la migrazione dell'intera Unione verso la crittografia quantum-safe, con il settore trasporti esplicitamente classificato tra i settori ad alto rischio.

La timeline a **tre fasi della roadmap EU** definisce scadenze progressive: la Fase 1, con scadenza al 31 dicembre 2026, richiede che ogni Stato membro adotti una strategia nazionale PQC e completi gli inventari crittografici delle proprie infrastrutture critiche; la Fase 2, con scadenza al 31 dicembre 2030, richiede che le infrastrutture critiche e i sistemi classificati ad alto rischio completino la migrazione a crittografia quantum-safe; la Fase 3, con scadenza al 31 dicembre 2035, prevede la transizione completa di tutti i sistemi. I settori classificati ad alto rischio — reti elettriche, telecomunicazioni, trasporti, difesa, finanza — sono soggetti alla scadenza della Fase 2, che per il settore trasporti implica la migrazione dei sistemi critici (segnalamento ferroviario, infrastruttura V2X, sistemi SCADA) entro il 2030.

Le sfide della migrazione PQC nel settore trasporti sono strutturalmente diverse da quelle di altri settori critici. Nel dominio V2X, i messaggi di sicurezza veicolare (BSM, CAM) devono essere verificati entro 100 millisecondi per garantire la safety-of-life. Le firme machine learning-DSA (FIPS 204) producono output di circa 4.627 byte contro i circa 64 byte di ECDSA, un incremento di circa 70 volte che impone frammentazione IP e potenziali effetti DDoS-like su veicoli legacy che non supportano le dimensioni PQC. Le attuali specifiche dei certificati V2X (IEEE 1609.2, ETSI TS 103 097) non includono forward compatibility per algoritmi PQC, una lacuna critica dato che i veicoli connessi in fase di deployment oggi opereranno fino al 2040 e oltre. Le soluzioni proposte dalla letteratura includono schemi PKI ibridi (classico + PQC durante la transizione) e protocolli come qSCMS.

Nel dominio ferroviario, i sistemi di segnalamento hanno cicli di vita superiori a 30 anni e non sono stati progettati per la sostituzione crittografica in campo. La crypto-agility — capacità di aggiornare gli algoritmi crittografici senza sostituzione dell'hardware — emerge come requisito architetturale essenziale per ogni nuova installazione. I sistemi ERTMS/ETCS Level 2, che utilizzano il protocollo Euroradio con MAC basato su 3DES (come discusso nella sezione Zero Trust), dovranno affrontare una doppia transizione: dalla crittografia simmetrica legacy alla crittografia moderna, e da questa alla crittografia quantum-safe. L'architettura FRMCS (Future Railway Mobile Communication System), in fase di sviluppo come successore di GSM-R, integra nativamente TLS 1.3 e supporto per algoritmi aggiornabili, ma le prime installazioni operative sono attese non prima del 2027 con piena maturità oltre il 2030.

La convergenza di tre framework globali — EU PQC Roadmap, NIST IR 8547 e NSA CNSA 2.0 — crea una finestra di migrazione unitaria per il periodo 2025-2030, con il 2027 come primo checkpoint critico (CNSA 2.0 per nuove acquisizioni) e il 2030 come scadenza intermedia per i sistemi critici dei trasporti. Per supportare questa

transizione, sono disponibili strumenti dedicati: il portfolio IBM Quantum Safe (Explorer per la scansione del codice e generazione di CBOM crittografiche, Advisor per l'analisi della postura crittografica, Remediator per il deployment di configurazioni quantum-safe), la suite PQShield PQPlatform per implementazioni hardware e software ottimizzate, la piattaforma ISARA Advance Crypto Agility per la gestione del ciclo di vita crittografico, e le soluzioni Thales CipherTrust per la gestione centralizzata delle chiavi quantum-safe. L'IBM Quantum Readiness Index 2025 indica un punteggio globale di 28 su 100, in progresso di 6 punti dal 2023 ma ancora criticamente basso, a conferma del divario tra urgenza normativa e preparazione operativa.

4.7.3 Defense in depth per infrastrutture di trasporto

I digital twin consentono di testare la resilienza di ciascun layer dell'infrastruttura; il principio che guida la progettazione di questi layer è la defense in depth, ovvero la protezione multilivello che garantisce la tenuta complessiva anche in caso di compromissione parziale.

L'approccio defense in depth per le infrastrutture di trasporto si fonda sul **principio di protezione multilivello — fisico, rete, applicazione, dati** — dove la compromissione di un singolo layer non consente l'accesso all'intera infrastruttura. Il modello di riferimento è definito dalla serie IEC 62443, che introduce il concetto di zone e conduit per la segmentazione delle reti industriali. Una zona raggruppa asset con requisiti di sicurezza omogenei (ad esempio, i controllori di un segmento ferroviario o i PLC di un'area portuale), mentre i conduit definiscono i canali di comunicazione autorizzati tra zone, ciascuno con controlli specifici. Lo standard definisce quattro Security Level (SL 1-4), che scalano dal misuso non intenzionale (SL 1) fino ad attacchi state-level con risorse elevate (SL 4), consentendo agli operatori di trasporto di calibrare le difese in proporzione al profilo di minaccia dell'infrastruttura.

Il livello hardware della defense in depth si articola intorno a moduli di sicurezza dedicati e trust anchor fisici. Nel dominio automotive, il framework EVITA (E-safety Vehicle Intrusion Protected Applications) definisce tre profili di HSM (Hardware Security Module): il profilo Full, con crittografia asimmetrica hardware-accelerata, è destinato alle applicazioni V2X dove la verifica delle firme dei messaggi di sicurezza deve rispettare vincoli di latenza stringenti; il profilo Medium è ottimizzato per i sistemi powertrain; il profilo Light è progettato per sensori e attuatori con vincoli di risorse. AUTOSAR 4.3 integra la gestione degli HSM attraverso il Crypto Service Manager, fornendo un'interfaccia standardizzata per le operazioni crittografiche. Il TPM 2.0 (Trusted Platform Module) funge da trust anchor nei gateway edge delle infrastrutture stradali e ferroviarie, garantendo l'integrità del firmware e l'autenticazione dei dispositivi.

La certificazione di sicurezza dei dispositivi edge per i trasporti registra progressi importanti. Eurotech ReliaGATE 10-14 è il primo edge AI gateway certificato IEC 62443-4-2 specificamente per il trasporto stradale e il fleet management, stabilendo un benchmark per i dispositivi di campo che devono combinare capacità di elaborazione AI con requisiti di sicurezza industriale. Nel dominio V2X, Autotalks SECTON e CRATON2 sono i primi chipset V2X a ottenere la certificazione Common Criteria con HSM embedded (settembre 2024), integrando la sicurezza hardware direttamente nel silicio delle comunicazioni veicolari. Queste certificazioni dimostrano la maturità dell'ecosistema hardware per la defense in depth nei trasporti e forniscono ai system integrator componenti con garanzie di sicurezza verificate indipendentemente. (il modello defense in depth è implementato dal Gruppo FS attraverso la segmentazione IT/OT e il C-SOC dedicato — si veda il §5.4.1 — Gruppo FS e la resilienza della supply chain)

Il livello software della defense in depth si fonda sugli hypervisor automotive, un mercato in crescita da 541,6 milioni di dollari (2023) a 3,2 miliardi entro il 2030, con un CAGR del 29%. Gli hypervisor Type 1 bare-metal, che detengono il 57-62% del mercato, forniscono isolamento hardware tra i domini funzionali del veicolo: il dominio safety-critical (ADAS, frenata), il dominio infotainment, e il dominio comunicazioni (V2X, telematics). BlackBerry QNX domina il segmento premium, Green Hills INTEGRITY è il riferimento per le applicazioni safety-critical con i livelli di certificazione più elevati, e Xen è adottato da Tesla, Jaguar Land Rover e Boeing 787 come soluzione open-source. Le tecnologie ARM — PAC (Pointer Authentication Code), BTI (Branch Target Identification), MTE (Memory Tagging Extension) e TrustZone — forniscono ulteriori meccanismi di isolamento a livello hardware, creando un'architettura di sicurezza stratificata dal silicio al software.

Gli standard IEC 62443-4-1 e IEC 62443-4-2 definiscono rispettivamente i requisiti per il ciclo di vita sicuro dei prodotti industriali e i requisiti tecnici di sicurezza dei componenti. IEC 62443-4-1 specifica i processi di secure product development con quattro livelli di maturità, dalla gestione base della sicurezza (Maturity Level 1) all'ottimizzazione continua (Maturity Level 4). IEC 62443-4-2 definisce oltre 140 requisiti tecnici organizzati in sette Foundational Requirements — identificazione e autenticazione, controllo dell'utilizzo, integrità del sistema, riservatezza dei dati, restrizione del flusso dati, risposta tempestiva agli eventi, e disponibilità delle risorse — ciascuno declinato sui quattro Security Level. Per il settore trasporti, la certificazione IEC 62443 è la garanzia di base che i componenti embedded (controllori di segnalamento, RSU, PLC portuali, centraline veicolari) siano stati progettati e verificati secondo standard di sicurezza riconosciuti a livello internazionale. Siemens Mobility detiene la certificazione IEC 62443 worldwide largest-scope (TÜV SÜD), dimostrando l'applicabilità dello standard all'intero portafoglio di prodotti ferroviari.

Il framework STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege), applicato ai veicoli autonomi SAE 4-5, genera un catalogo di minacce specifiche:

- Spoofing: falsificazione dei segnali GPS, dei messaggi V2X e delle identità dei sensori;
- Tampering: manipolazione dei dati sensoriali in transito, alterazione dei modelli machine learning di percezione;
- Repudiation: impossibilità di attribuire azioni in sistemi multi-agente con decisioni distribuite;
- Information Disclosure: esfiltrazione di dati di percorrenza, abitudini degli utenti, mappe HD proprietarie
- Denial of Service: saturazione delle interfacce V2X, blocco dei sistemi di aggiornamento OTA, degradazione dei sensori LiDAR tramite interferenza ottica;
- Elevation of Privilege: escalation dall'infotainment ai bus CAN/Ethernet automotive, accesso non autorizzato ai domini safety-critical.

4.7.4 FRMCS: sicurezza by-design per le comunicazioni ferroviarie di nuova generazione

I principi di defense in depth trovano una declinazione specifica nelle architetture di comunicazione di nuova generazione per il settore ferroviario, dove il Future Railway Mobile Communication System (FRMCS) integra la sicurezza fin dalla fase di progettazione.

Il Future Railway Mobile Communication System (FRMCS) incarna il paradigma di sicurezza by-design per le comunicazioni ferroviarie, strutturato su un'architettura a tre strati di sicurezza con perimetri distinti. Il Railway Application Stratum ospita le applicazioni critiche ferroviarie — ETCS (European Train Control System), ATO (Automatic Train Operation) e TCMS (Train Control and Monitoring System) — ciascuna con requisiti di sicurezza e safety specifici. Il Service Stratum adatta i servizi 3GPP MCX (Mission Critical Services) al dominio ferroviario, includendo MCPTT (Mission Critical Push-To-Talk) per le comunicazioni vocali operative, MCData per lo scambio dati tra treno e terra, e MCVideo per la videosorveglianza in tempo reale. Il Transport Stratum si basa su una rete 5G SA (Standalone) con tecnologia NR (New Radio), Mobile Edge Computing (MEC) per l'elaborazione a bassa latenza, e network slicing per l'isolamento logico del traffico ferroviario dal traffico commerciale.

Ciascuno strato implementa meccanismi di sicurezza nativi. Il Railway Application Stratum eredita i requisiti di sicurezza funzionale definiti da EN 50129 (Safety-related electronic systems for signalling) e integra la protezione delle comunicazioni secondo EN 50159, con l'obiettivo di superare le limitazioni del protocollo Euroradio attuale — basato su cifratura 3DES con chiavi a 192 bit, soggetto a vulnerabilità di collisione dopo 2^32 blocchi, mitigata dalla rotazione delle chiavi di sessione ma comunque insufficiente per le esigenze di sicurezza a lungo termine (cfr. sezione Zero Trust, EN 50159). Il Service Stratum applica i meccanismi di sicurezza MCX definiti da 3GPP TS 33.180, includendo mutua autenticazione tra utenti e servizi, cifratura end-to-end delle comunicazioni e gestione centralizzata delle identità. Il Transport Stratum beneficia della sicurezza nativa 5G: protocollo 5G-AKA (Authentication and Key Agreement) per l'autenticazione reciproca, protezione dell'identità dell'abbonato tramite SUPI/SUCI (Subscription Permanent/Concealed Identifier), e TLS 1.3 per le comunicazioni tra le funzioni di rete.

La pubblicazione dello standard ETSI TS 103 764 V1.1.1 nel gennaio 2026 segna una pietra miliare per l'architettura di sicurezza FRMCS, definendo il modello dei trust domain — ovvero i confini di fiducia tra gli attori del sistema (operatore ferroviario, fornitore di rete, produttori di equipaggiamento) e le relazioni di trust necessarie per garantire l'integrità delle comunicazioni critiche. Questo standard si inserisce nel contesto più ampio della standardizzazione FRMCS condotta da ETSI TC-RT (Technical Committee on Railways Telecommunications), in coordinamento con 3GPP per gli aspetti radio e servizio, e con ERA (European Union Agency for Railways) per i requisiti operativi e di interoperabilità. Il progetto FP2-MORANE-2, finanziato dall'Europe's Rail Joint Undertaking con 13,5 milioni di euro, coordina lo sviluppo del sistema FRMCS includendo la validazione dei requisiti di sicurezza e la definizione delle specifiche di interoperabilità.

La maturità del sistema FRMCS è stata validata attraverso il 5° ciclo di Plugtests FRMCS, condotto nell'ottobre 2025, che ha registrato un tasso di successo di interoperabilità del 95,5% tra i diversi fornitori partecipanti. Questo risultato dimostra che le specifiche di sicurezza sono implementabili in modo coerente da produttori diversi — un prerequisito essenziale per un sistema che dovrà operare su reti multi-vendor in tutta Europa. Le aree testate includono l'autenticazione reciproca tra i terminali a bordo treno e la rete 5G, il funzionamento dei servizi MCX in condizioni di handover tra celle, e l'isolamento del traffico ferroviario tramite network slicing. Il programma di lavoro 2026 dell'Europe's Rail Joint Undertaking prevede il proseguimento delle attività di validazione e il finanziamento di dimostratori su corridoi TEN-T, incluse le demo pianificate a Genova.

La roadmap di deployment FRMCS prevede i primi dispiegamenti operativi nel periodo 2027-2028, con un'architettura di coesistenza dual-mode GSM-R/FRMCS che garantirà la continuità operativa durante la transizione. Il sunset di GSM-R è stimato intorno al 2035, con variazioni marcate tra i diversi gestori di infrastruttura europei in funzione dello stato della rete esistente e dei cicli di investimento. La sicurezza by-design di FRMCS si articola su quattro pilastri: mutua autenticazione nativa (5G-AKA) che supera la semplice autenticazione SIM di GSM-R, cifratura end-to-end delle comunicazioni critiche a ogni strato dell'architettura, isolamento del traffico ferroviario tramite network slicing dedicato, e sicurezza edge attraverso MEC (Mobile Edge Computing) per l'elaborazione locale dei dati sensibili. Questa architettura posiziona FRMCS non come un semplice aggiornamento tecnologico di GSM-R, ma come una riprogettazione completa della sicurezza delle comunicazioni ferroviarie, in coerenza con i principi Zero Trust.

4.7.5 Sicurezza V2X: standard ETSI e architettura PKI

Se il FRMCS definisce l'architettura di sicurezza per le comunicazioni ferroviarie, il **dominio stradale** richiede un framework analogo per le comunicazioni veicolo-infrastruttura: lo standard C-V2X, con la propria architettura PKI, risponde a questa esigenza.

Lo stack di sicurezza ITS di ETSI costituisce l'infrastruttura a chiave pubblica (PKI) che protegge le comunicazioni V2X a livello applicativo. Lo standard ETSI TS 102 940 definisce l'architettura complessiva di sicurezza ITS, strutturata su una gerarchia di Certificate Authority: la Root CA come ancora di fiducia al vertice, le Enrolment Authority (EA) per l'iscrizione iniziale dei dispositivi ITS e l'emissione dei certificati di lunga durata, e le Authorization Authority (AA) per l'emissione dei certificati pseudonimi a breve termine utilizzati nelle comunicazioni operative. Questa separazione tra enrolment e authorization è progettata per proteggere la privacy: la EA conosce l'identità del veicolo ma non i suoi messaggi operativi, mentre la AA emette certificati pseudonimi senza conoscere l'identità reale del richiedente.

In ambito ETSI per i sistemi di trasporto intelligenti (C-ITS) è importante introdurre i Service Specific Permissions (SSP) che sono campi contenuti nei certificati di sicurezza che definiscono i permessi precisi di una stazione ITS (ITS-S) per una specifica applicazione. In pratica, fungono da livello di autorizzazione granulare e garantiscono che un dispositivo, anche se autorizzato a partecipare alla rete C-ITS, possa inviare solo i messaggi coerenti con il suo ruolo. Vengono verificati durante la ricezione di un messaggio per confermare che il mittente abbia effettivamente il diritto legale/tecnico di inviare quelle informazioni specifiche. In sintesi, gli SSP sono il meccanismo che impedisce a un utente non autorizzato di inviare messaggi critici per la sicurezza, come la segnalazione falsa di un veicolo di emergenza in arrivo.

Lo standard ETSI TS 102 941 specifica i flussi di trust and privacy management, dettagliando le procedure di enrolment (registrazione iniziale del dispositivo ITS nella PKI), authorization (richiesta e rinnovo dei certificati pseudonimi), e revoca (distribuzione delle Certificate Revocation List). I formati dei certificati e degli header di sicurezza sono definiti da ETSI TS 103 097, progettato per la compatibilità con lo standard IEEE 1609.2 utilizzato in Nord America — garantendo l'interoperabilità transatlantica delle comunicazioni V2X. I certificati pseudonimi vengono ruotati periodicamente per impedire il tracciamento dei veicoli: un singolo veicolo utilizza certificati diversi nel corso della giornata, rendendo impossibile a un osservatore esterno ricostruire gli spostamenti completi. Il sistema di misbehavior detection, standardizzato in ETSI TS 103 759, consente la segnalazione e la revoca di entità che inviano messaggi anomali o malevoli, completando l'architettura di fiducia con un meccanismo di difesa post-deployment.

Le sfide di sicurezza C-V2X derivano dalla natura broadcast del PC5 sidelink: a differenza delle comunicazioni cellulari, le trasmissioni broadcast non prevedono autenticazione AS — ogni veicolo nel raggio riceve i messaggi senza verifica del mittente a livello radio. La protezione è interamente affidata ai certificati applicativi: ogni messaggio BSM (Basic Safety Message) o CAM (Cooperative Awareness Message) è firmato con certificato pseudonimo valido. La ricerca sulla sicurezza NR-V2X ha identificato la vulnerabilità CVD-2024-0098 (febbraio 2025) sui meccanismi di allocazione delle risorse radio. Nel dominio hardware, i chipset Autotalks SECTON e CRATON2 sono i primi V2X con HSM Common Criteria (settembre 2024), che consentono la verifica delle firme nel silicio (cfr. §5.3.1 per il pilota C-Roads Italy).

Il deployment dell'architettura C-V2X in Italia procede attraverso il **progetto C-Roads Italy**, pilota nazionale che testa i servizi cooperativi Day 1 (safety: hazardous location notification, road works warning) e Day 1.5 (traffic management: signal phase and timing, green light optimisation) su arterie ad alta intensità di traffico. La sicurezza delle comunicazioni nel pilota segue gli standard della C-Roads Platform europea per la gestione dei certificati PKI e la validazione dei messaggi. Una sfida emergente per l'architettura di sicurezza V2X riguarda la compatibilità con la crittografia post-quantum: i certificati definiti da ETSI TS 103 097 e IEEE 1609.2 utilizzano attualmente algoritmi a curva ellittica (ECDSA) con firme di circa 64 byte, mentre gli algoritmi post-quantum come machine learning-DSA producono firme di circa 4.627 byte — un incremento di circa 70 volte che pone sfide rilevanti per le comunicazioni V2X, dove i messaggi BSM/CAM devono essere trasmessi e verificati entro finestre temporali di 100 millisecondi. Questa transizione è una delle sfide architetturali più complesse per la sicurezza dei trasporti connessi nel prossimo decennio.

4.7.6 Architetture di sicurezza settoriali

Dopo aver esaminato le architetture trasversali — Zero Trust, crittografia post-quantum, SOC AI-driven, digital twin, defense in depth — e i framework di comunicazione sicura (FRMCS, C-V2X), la trattazione si concentra sulle architetture specifiche per ciascun sotto-settore della mobilità.

Veicoli e mobilita delle persone

Nel dominio automotive, l'architettura di sicurezza è strutturata attorno al CSMS imposto dal regolamento UNECE R155 (cfr. §4.3.4), obbligatorio per tutti i veicoli di categoria M, N e O dal luglio 2024. Lo standard ISO/SAE 21434 (agosto 2021) fornisce il framework di cybersecurity engineering che supporta la conformità R155, coprendo l'intero ciclo di vita del veicolo dalla progettazione alla dismissione. Il rischio dominante è la safety-of-life: un attacco ai sistemi di percezione o decisione di un veicolo connesso o autonomo ha conseguenze potenzialmente letali, distinguendo il dominio automotive da tutti gli altri settori di trasporto. Le certificazioni 2024-2025 documentano la maturazione dell'ecosistema hardware di sicurezza: Infineon SLI37 con certificazione Common Criteria EAL6+ (primo secure element automotive a questo livello), Arm Platform Security Architecture con certificazione ML3 rilasciata da exida, Synopsys con la prima certificazione IP product da SGS-TÜV Saar, e lo schema settoriale ENX Vehicle cybersecurity (VCS) lanciato nel giugno 2024 per la gestione della sicurezza lungo la supply chain automotive.

Il **pattern architetturale chiave per il dominio automotive** è la difesa a strati del veicolo connesso: Hardware Security Module (HSM) con profili EVITA (Full/Medium/Light) per la protezione crittografica nel silicio, hypervisor bare-metal per l'isolamento dei domini di sicurezza (safety-critical, infotainment, connettività), e infrastruttura PKI per le comunicazioni V2X. La sicurezza degli aggiornamenti over-the-air (OTA) è un elemento architetturale critico: i meccanismi includono Trusted Execution Environment (TEE) per l'esecuzione protetta del processo di aggiornamento, firma end-to-end con algoritmi RSA-2048 o ECC per la verifica di autenticità e integrità del firmware, e protezione anti-rollback con meccanismo "ratchet" che impedisce il downgrade a versioni precedenti vulnerabili. Autotalks SECTON e CRATON2 sono i primi chipset V2X con HSM certificato Common Criteria (settembre 2024), integrando la verifica dei certificati V2X direttamente nel silicio — un approccio che consente prestazioni compatibili con i vincoli di latenza delle comunicazioni safety-of-life. (l'ecosistema delle startup specializzate per ciascun sotto-settore — ferroviario, OT/difesa, automotive — è analizzato nel §5.2).

Nel **dominio del Trasporto Pubblico Locale e Mobility-as-a-Service** [PERSONE], il rischio dominante è la combinazione di data breach dei dati passeggeri e disruption del servizio pubblico — con implicazioni che vanno oltre il danno economico, impattando la fiducia dei cittadini nei servizi di mobilità digitale. Il mercato dei sistemi AFC (Automatic Fare Collection) è valutato a 20,67 miliardi di dollari (2024) con proiezione a 59,79 miliardi entro il 2032, e l'attacco a Oahu Transit Services (2024) ha dimostrato la vulnerabilità concreta dei sistemi di bigliettazione, disabilitando l'intera fare collection. La normativa primaria è il D.Lgs. 138/2024 (trasposizione NIS2), che all'Allegato IV include esplicitamente i gestori del trasporto pubblico locale — un'estensione italiana rispetto alla direttiva europea. Il progetto MaaS4Italy (MIT), con sperimentazioni a Torino, Milano, Roma, Bari, Napoli e Piemonte, introduce l'identità digitale SPID/CIE come trust anchor per la federazione di servizi di mobilità eterogenei, centralizzando la distribuzione dati attraverso la piattaforma nazionale DSRM (Data Sharing & Service Repository for MaaS).

Logistica, marittimo e merci

Nel **dominio freight e logistica** [MERCI], il ransomware domina come vettore primario con una pressione in rapida escalation: 283 attacchi ransomware documentati nel 2025 verso il settore transport & logistics (Cyble 2025), il 71% dei quali diretti a flotte trucking e servizi freight. Il rischio distintivo è il cyber-enabled cargo theft: cartelli criminali utilizzano strumenti di Remote Monitoring and Management (RMM) per ottenere visibilità in tempo reale sui movimenti merci, combinandoli con GPS spoofing per mascherare deviazioni di rotta non autorizzate — con perdite stimate a 725 milioni di dollari nel 2025 (+60% anno su anno, CargoNet/Verisk) e valore medio per furto di 273.990 dollari (+36%, CargoNet 2025). Il Transportation Management System (TMS) è il target primario: la sua compromissione paralizza la visibilità sulla supply chain, impedendo tracciamento spedizioni, gestione ordini e ottimizzazione rotte. La normativa primaria comprende NIS2 per gli operatori logistici essenziali, il Cyber Resilience Act per i prodotti digitali della supply chain, e il Regolamento (UE) 2020/1056 (eFTI) che impone la piena obbligatorietà delle informazioni elettroniche sul trasporto merci dal 9 luglio 2027, con requisiti di autenticità, integrità, tracciabilità e disponibilità per le piattaforme certificate.

Nel **dominio marittimo e portuale** [MERCI], l'architettura di sicurezza deve gestire la convergenza tra sistemi OT storicamente isolati e infrastrutture IT moderne, in un contesto di escalation drammatica delle minacce: oltre 100 cyberattacchi al settore marittimo nell'anno fino a luglio 2025 (+150%, Cyble 2025), con 12 e più gruppi APT attivi (SideWinder, Mustang Panda, APT41, APT28) e un risk score OT compromise di 98 su 100 (Cyble 2025). L'architettura portuale organizza i sistemi in zone funzionali secondo il modello IEC 62443: zona crane automation (STS, RTG, PLC/SCADA) con il rischio di manipolazione dei movimenti e sabotaggio fisico; zona VTMS (radar, AIS, VHF) esposta a false data injection e disruption della navigazione; zona terminal operations (TOS, gate automation, RFID/OCR) con rischi di manipolazione del tracking container; e zona reti IT (ERP, billing) esposta a ransomware e data exfiltration. Il framework normativo marittimo si articola su tre livelli: le linee guida aggiornate IMO MSC-FAL.1/Circ.3/Rev.3 (23 aprile 2025), allineate al NIST CSF 2.0; l'obbligatorietà di integrazione della cybersecurity nel ISM Code (MSC.428(98), in vigore dal 1 gennaio 2021); e le linee guida settoriali BIMCO v5 (14 novembre 2024) con la più ampia coalizione di stakeholder marittimi.

Il GPS spoofing marittimo ha raggiunto dimensioni critiche nel 2025: GPSPatron documenta oltre 13.000 navi impattate globalmente, con 3.000+ disrupted nel Golfo Persico e nello Stretto di Hormuz in meno di due settimane e un'escalation nel Baltico da 1.225 a oltre 5.800 navi tra Q1 e Q2 2025. Il pattern architetturale integra: navigazione multi-constellation GNSS con validazione incrociata inerziale e anomaly detection AI; digital twin portuale (Port of Rotterdam: replica 42 km con rete LTE privata; Port of Antwerp: 5G SA per drone e automazione); separazione dei cinque livelli OT/IT con monitoring real-time per zona. Il codice ISPS, focalizzato sulla sicurezza fisica, non contiene cybersecurity esplicita nella Parte A vincolante — gap normativo che richiederebbe l'emendamento della Sezione 16.

Infrastrutture, mobilita elettrica e analisi trasversale

Nel dominio della **mobilità elettrica** [ENTRAMBI persone e merci], l'architettura di sicurezza ruota attorno ai protocolli veicolo–stazione di ricarica. OCPP 2.0.1 prevede tre profili: Profile 1 (HTTP Basic, deprecato), Profile 2 (TLS con autenticazione server, minimo accettabile pubblico), Profile 3 (mutual TLS con certificati X.509 bidirezionali, raccomandato). La CVE-2025-12357 in ISO 15118-2 (CISA ICSA-25-303-01, CVSS 8.3) ha dimostrato vulnerabilità del protocollo SLAC per il pairing veicolo–stazione, mitigata da ISO 15118-20 con TLS obbligatorio. Pwn2Own Automotive ha registrato un'escalation dei zero-day da 49 (2025) a 76 (2026, +55%), con targeting diretto dei charger via charging gun (Alpitronic HYC50, premio singolo $60.000). Il CRA è applicabile a wallbox e backend CSMS; i veicoli type-approved sotto R155 sono esclusi.

L'ecosistema italiano delle infrastrutture intelligenti di trasporto è coordinato **dall'Osservatorio Tecnico Smart Road del MIT** e si articola su tre piattaforme nazionali complementari. ANAS Smart Road (Gruppo FS) investe circa un miliardo di euro (2018-2025) per l'infrastruttura C-ITS su rete TEN-T e autostradale con sensori IoT, fibra ottica dedicata e analytics AI/Big Data, con piloti operativi sulla A2 Fisciano-Sala Consilina, Roma-Fiumicino e Smart Road Dolomiti (80 km). C-Roads Italy, consorzio che include ANAS, A22, A4 Brescia-Padova, Stellantis e Politecnico di Milano, testa il deployment armonizzato dei servizi cooperativi C-ITS Day 1 e Day 1.5 con architettura PKI conforme alla piattaforma C-Roads europea, su corridoi A22, A4, A28 e aree urbane di Torino, Verona e Trento. MaaS4Italy, promosso dal MIT e dal Dipartimento per la Trasformazione Digitale, sperimenta l'integrazione di servizi di mobilità con identità digitale SPID/CIE su scala nazionale. Queste piattaforme rappresentano il substrato infrastrutturale su cui le architetture di sicurezza descritte in questa sezione dovranno essere implementate — la loro evoluzione determinerà la resilienza del sistema dei trasporti italiano nei prossimi decenni.

Questa architettura di riferimento non è un modello rigido, ma una cornice evolutiva che consente a Pubbliche Amministrazioni, gestori di infrastrutture e operatori industriali di progettare sistemi.

L'AI è simultaneamente moltiplicatore di difesa e sfida di sicurezza. Le piattaforme SOC AI-driven riducono i tempi di investigazione da 30 a meno di 3 minuti (Prophet Security); i digital twin consentono testing di scenari senza impatto operativo, con riduzioni del 33% nei tempi di detection e del 43% nel containment (WEF 2025); l'anomaly detection raggiunge accuratezze superiori al 99% su dataset specifici per il trasporto. La crittografia post-quantum impone una visione di lungo periodo: ITS con cicli di vita 15-30 anni, installati oggi, saranno operativi fino al 2040-2055 — oltre la probabilità superiore al 50% di un computer quantistico crittograficamente rilevante (CRQC) entro il 2035. La EU PQC Migration Roadmap (23 giugno 2025) classifica i trasporti come settore ad alto rischio, con obbligo di migrazione critica entro il 31 dicembre 2030 (Fase 2).

4.7.7 Integrazione Cyber Threat Intelligence

La crescita della superficie d’attacco nei sistemi di mobilità richiede strumenti in grado di supportare la prevenzione e la comprensione delle minacce. In tale contesto, le piattaforme di Cyber Threat Intelligence (CTI) costituiscono una componente del pilastro Cybersecurity, in quanto consentono di raccogliere, organizzare e rendere utilizzabili informazioni su attori ostili, campagne malevole, vulnerabilità, indicatori tecnici, esposizione degli asset e rischi per la continuità operativa.

La funzione della CTI è trasformare dati eterogenei in informazioni utili per la sicurezza. Indicatori di compromissione, vulnerabilità note, report di settore, segnalazioni istituzionali, eventi rilevati dai sistemi di sicurezza e dati relativi alla superficie esterna di attacco acquisiscono valore quando vengono messi in relazione con il contesto dell'organizzazione. Nel settore della mobilità, questo significa valutare le minacce rispetto a infrastrutture ITS, sistemi OT, centrali di controllo, apparati di campo, piattaforme digitali, reti V2X, fornitori e servizi essenziali.

Una piattaforma CTI permette quindi di integrare l'analisi delle minacce nei processi di sicurezza. L'obiettivo non è soltanto sapere che una minaccia esiste, ma comprendere se possa interessare il proprio perimetro, quali asset risultino esposti, quali vulnerabilità siano prioritarie e quali conseguenze possano prodursi sulla continuità del servizio.

Nel settore dei trasporti, questa impostazione è utile perché un incidente cyber può generare impatti che vanno oltre il piano informatico. La compromissione di un sistema di bigliettazione, di una centrale operativa, di un'infrastruttura OT, di una piattaforma MaaS o di un fornitore può incidere sulla regolarità del servizio, sulla sicurezza degli utenti, sulla fiducia nei sistemi digitali e sulla stabilità della filiera logistica.

Le piattaforme CTI non devono essere interpretate come semplici archivi di feed o indicatori. La raccolta automatizzata da fonti Open Source INTelligence (OSINT), bollettini pubblici, repository tecnici o feed commerciali è utile, ma non sufficiente. La qualità dell'intelligence dipende dalla verifica delle informazioni, dall'attribuzione di livelli di attendibilità, dal collegamento con gli asset esposti e dalla distinzione tra rumore informativo ed elementi utili per la sicurezza. L'automazione può accelerare raccolta, normalizzazione e correlazione, ma non sostituisce il processo analitico.

Anche quando vengono impiegati strumenti avanzati o modelli di AI, la CTI mantiene una funzione distinta rispetto all'AI Security. La piattaforma appartiene al dominio della cybersecurity e può dialogare con SOC, CSIRT, sistemi di vulnerability management e strumenti di analisi, ma il suo valore resta legato alla qualità delle fonti, alla validazione e alla conoscenza del contesto operativo. Le piattaforme di Cyber Threat Intelligence possono essere integrate nell'architettura di sicurezza degli operatori della mobilità a supporto delle attività di prevenzione, rilevamento, risposta agli incidenti, gestione delle vulnerabilità e protezione della catena di fornitura.

Dal punto di vista funzionale, una piattaforma CTI consente di aggregare informazioni provenienti da fonti tecniche, fonti aperte, canali istituzionali, reti settoriali, CSIRT, ISAC, vendor advisory, report di threat landscape, eventi SOC e dati di contesto. Queste informazioni vengono organizzate in modo da poter essere interrogate, correlate e utilizzate nei processi decisionali.

Nel contesto della mobilità, la piattaforma assume valore quando consente di collegare minacce e vulnerabilità agli asset. Centrali di controllo, sistemi ITS, apparati di campo, reti V2X, sistemi di bigliettazione, piattaforme MaaS, ambienti cloud, sistemi edge, fornitori e manutentori non hanno tutti lo stesso livello di esposizione né lo stesso impatto sul servizio. La **CTI aiuta a stabilire priorità più aderenti al rischio**.

Dalla raccolta automatizzata all'intelligence contestualizzata

La disponibilità di grandi quantità di dati non equivale automaticamente a una maggiore capacità di difesa. Una piattaforma CTI può raccogliere molti indicatori, ma tali indicatori sono utili solo se vengono verificati, classificati e contestualizzati.

Nel settore della mobilità, la stessa informazione può assumere peso diverso a seconda del contesto. Una vulnerabilità che per un'organizzazione ha impatto limitato può essere significativa per un operatore che utilizza quel componente in un'infrastruttura essenziale. Allo stesso modo, una campagna osservata in altri settori può diventare rilevante se coinvolge tecnologie, fornitori o servizi utilizzati anche nel trasporto pubblico, nella logistica o nella gestione stradale.

Per questo motivo, **la CTI deve integrare automazione e analisi**. Gli strumenti automatici supportano la velocità del processo, mentre la qualificazione dell'intelligence richiede criteri di attendibilità, livelli di confidenza, correlazione con fonti indipendenti e valutazione del contesto.

Una piattaforma deve quindi aiutare a distinguere tra informazione disponibile e informazione utile. Questo passaggio serve a ridurre falsi positivi, evitare priorità non coerenti con il rischio e orientare le attività di mitigazione. Accanto a fonti aperte, feed commerciali, bollettini istituzionali, vendor advisory e report di settore, la CTI può anche integrare informazioni provenienti da fonti qualificate non sempre accessibili o interpretabili attraverso strumenti automatizzati.

Nel contesto della Cyber Threat Intelligence, l'arricchimento informativo può includere dati provenienti da ambienti digitali ostili o semi-chiusi, quali forum underground, marketplace criminali, leak site riconducibili a gruppi ransomware, canali di scambio di credenziali compromesse, infrastrutture di phishing, ambienti del dark web e altre fonti utili alla comprensione delle minacce.

In tale quadro, la componente riconducibile alla Human Intelligence (HUMINT) deve essere intesa come attività specialistica di raccolta, analisi e qualificazione delle informazioni svolta a supporto del patrimonio informativo della piattaforma CTI. Non si tratta di raccolta affidata al personale dell'organizzazione che utilizza la piattaforma, ma di un'attività condotta da analisti specializzati nell'osservazione e interpretazione di fonti che richiedono competenze umane, conoscenza degli ambienti criminali digitali, capacità linguistiche e valutazione del contesto.

La HUMINT applicata alla CTI come attività regolamentata, documentata e svolta entro limiti legali ed etici definiti può contribuire all'identificazione di credenziali compromesse, dati aziendali esposti, riferimenti a fornitori o infrastrutture del settore, campagne in preparazione, strumenti malevoli in circolazione, vulnerabilità discusse in ambienti criminali o segnali preliminari di interesse verso specifici comparti.

Queste informazioni, una volta validate e correlate con fonti tecniche, OSINT, eventi SOC, segnalazioni CSIRT, dati di threat landscape e indicatori disponibili nella piattaforma, consentono di arricchire il dataset CTI con elementi che la sola automazione potrebbe non rilevare, non contestualizzare correttamente o acquisire con sufficiente tempestività.

Le informazioni raccolte da una piattaforma CTI non dovrebbero essere utilizzate in modo indifferenziato. È necessario distinguere tra dato grezzo, segnalazione, evidenza verificata e intelligence utilizzabile. Il dato grezzo è un'informazione non ancora verificata. La segnalazione è un elemento potenzialmente rilevante, ma da approfondire. L'evidenza verificata è un'informazione confermata da riscontri tecnici, operativi o documentali. L'intelligence utilizzabile è invece un'informazione contestualizzata, correlata e idonea a supportare una decisione, una misura di mitigazione o una priorità di intervento.

Questo processo è importante quando le informazioni provengono da fonti non automatizzate o da segnalazioni operative. Tali informazioni possono avere valore, ma richiedono criteri chiari di valutazione: attendibilità della fonte, prossimità all'evento osservato, competenza del soggetto che segnala, datazione, coerenza con altre evidenze, possibilità di riscontro tecnico e rilevanza rispetto agli asset.

Una piattaforma CTI deve quindi permettere di tracciare il ciclo di vita dell'informazione: origine, fonte, livello di confidenza, correlazioni, utilizzo operativo e aggiornamenti successivi. Questa tracciabilità migliora l'analisi e riduce il rischio di decisioni fondate su elementi non verificati.

Integrazione con SOC, CSIRT, ISAC e processi di rischio

La piattaforma CTI deve integrarsi con i principali processi di sicurezza dell'organizzazione e dell'ecosistema settoriale. In particolare, può alimentare SOC, CSIRT, vulnerability management, incident response, business continuity, risk management e attività di protezione della supply chain.

Per i SOC, la CTI consente di arricchire alert e casi di indagine con informazioni su attori, campagne, tecniche, vulnerabilità sfruttate, asset esposti e segnali provenienti da fonti diverse. Per i CSIRT, supporta la ricostruzione della catena di attacco, la valutazione dell'impatto e la comunicazione verso gli stakeholder coinvolti.

Per il vulnerability management, la CTI permette di superare una logica basata solo sulla gravità tecnica. Una vulnerabilità va valutata anche rispetto all'esposizione effettiva, alla probabilità di sfruttamento, all'interesse degli attori ostili e alla criticità del servizio impattato.

La CTI può inoltre rafforzare la cooperazione con ISAC, autorità competenti, associazioni di settore e altri operatori della mobilità. La condivisione controllata di informazioni consente di individuare campagne che non colpiscono un singolo soggetto, ma intere filiere o sotto-settori: trasporto pubblico locale, infrastrutture autostradali, ferroviarie, portuali, aeroportuali, logistica e servizi digitali di mobilità.

Benefici attesi per l'ecosistema della mobilità

Una piattaforma CTI aggiornata, validata e arricchita da fonti differenziate può rafforzare la postura cyber dell'ecosistema della mobilità. Il primo beneficio è la capacità di anticipare le minacce, individuando correlazioni e segnali prima che si traducano in incidenti rilevanti.

Il secondo beneficio riguarda la qualità delle decisioni. La CTI permette di superare la semplice raccolta di indicatori tecnici e di costruire una visione più aderente al rischio: asset esposti, vulnerabilità prioritarie, fornitori critici, campagne compatibili con il settore e misure da adottare.

Il terzo beneficio riguarda la supply chain. Molte minacce ai trasporti transitano attraverso fornitori, manutentori, piattaforme terze, servizi cloud, componenti software e apparati di campo. Una piattaforma CTI può contribuire a intercettare criticità distribuite lungo la filiera e a migliorare il coordinamento tra operatori.

Infine, la CTI rafforza la consapevolezza organizzativa perché consente di integrare nei processi interni informazioni sulle minacce già raccolte, validate e contestualizzate dalla piattaforma. In questo modo, l'organizzazione può orientare meglio attività di monitoraggio, priorità di mitigazione, formazione, gestione degli incidenti e protezione della supply chain.

In sintesi, una piattaforma CTI rappresenta una tecnologia cyber a supporto di una difesa proattiva. Il suo obiettivo è collegare dati, persone, processi e decisioni, trasformando la conoscenza delle minacce in azioni utili a proteggere continuità, resilienza e affidabilità dei servizi di mobilità.

La CTI resta tuttavia distinta dall'AI: può utilizzare strumenti automatici o modelli avanzati, ma il suo valore dipende dalla qualità delle fonti, dalla validazione delle evidenze, dalla raccolta di informazioni anche non automatizzate e dalla capacità di trasformare segnali in decisioni operative.

4.7.8 Digital Twin e simulazione

L'uso di ambienti di simulazione e digital twin consente di testare scenari operativi e di attacco, valutare l'impatto di nuove minacce e migliorare la resilienza complessiva del sistema prima della messa in esercizio. Secondo il World Economic Forum (marzo 2025), l'adozione di digital twin per la sicurezza consente una riduzione del 33% dei tempi di rilevamento degli incidenti e del 43% dei costi di risposta, confermando il valore della simulazione proattiva per gli operatori di infrastrutture critiche.

Le implementazioni operative dimostrano la maturità della tecnologia a scala industriale. Deutsche Bahn, in collaborazione con NVIDIA, ha sviluppato un digital twin a scala nazionale che replica 5.700 km di rete e oltre 5.000 asset, consentendo la simulazione di scenari operativi e la manutenzione predittiva con riduzione documentata del 60% dei ritardi correlati a guasti.

L'Italia partecipa attivamente a questo sviluppo. Il progetto SAFETY4RAILS (H2020, €7,7M) ha sviluppato la piattaforma S4RIS con 18 strumenti integrati, conducendo esercitazioni cyber-fisiche a Roma con il coinvolgimento di ATAC e STASY. Il laboratorio del Politecnico di Milano (PoliCyber) opera un cyber range dedicato alla mobilità connessa, con simulazioni di attacco a reti V2X e sistemi ADAS.

Sul piano europeo, l'esercitazione Cyber Europe 2026 (giugno 2026) sarà la prima esercitazione paneuropea focalizzata specificamente sui trasporti, con scenari dedicati a ferroviario e marittimo (ENISA, novembre 2025). Nel dominio portuale, il Porto di Rotterdam ha implementato un digital twin dell'intero complesso di 42 chilometri, alimentato da dati sensoristici in tempo reale e protetto da una rete LTE privata, consentendo la simulazione di scenari di attacco dalla compromissione dei sistemi di gestione delle gru alla manipolazione dei dati AIS delle navi.

L'intersezione tra digital twin per la cybersecurity e manutenzione predittiva genera sinergie operative rilevanti: la validazione dei controlli di sicurezza in ambiente virtuale prima del deployment consente di ridurre sia i rischi operativi sia i costi di integrazione.

Un approccio emergente è il «digital shadow»: una replica basata esclusivamente su dati storici, senza connessione in tempo reale all'infrastruttura operativa. Questo modello, proposto dal Connected Places Catapult (Regno Unito, 2025), consente il testing di cybersecurity senza introdurre nuovi vettori di attacco attraverso le connessioni real-time, risultando particolarmente adatto per la valutazione iniziale della postura di sicurezza di infrastrutture legacy. L'investimento in cyber range e ambienti di simulazione dedicati alla mobilità rappresenta una priorità strategica per rafforzare le competenze operative di tecnici e decisori del settore.

Un altro approccio già applicato nella citata soluzione italiana presente sul mercato prevede l'utilizzo di tre tools. un primo tool analizza la rete target attraverso sniffer commerciali: si tratta di una soluzione avanzata per il monitoraggio della superficie di attacco. Diversamente dai tradizionali strumenti di vulnerability scanning come Nessus, questa agisce come una sonda intelligente che non si limita a rilevare vulnerabilità, ma le integra direttamente nel modello di rischio dell'organizzazione, offrendo una visione più completa e contestualizzata aggiornando con continuità il digital twin nella topologia, nei legami logici e regole di filtraggio e routing.

Un secondo tool costruisce un modello matematico della rete target e identifica i possibili cammini di attacchi noti: creazione del Digital Twin, definizione degli obiettivi da proteggere, scelta del livello di confidenza e accuratezza per eseguire le simulazioni, la simulazione degli attacchi, scelta delle contromisure all'interno di un menu dedicato, lista delle contromisure per neutralizzare il rischio.

Attività. Presenta un archivio "Export Vulnerability scanning" di vulnerabilità individuate nei vari componenti hardware, software e firmware della infrastruttura target dell'assessment", Cammini di Attacco generati da ogni attaccante modellato e permette la creazione database storico dei Digital Twin dell'infrastruttura, delle vulnerabilità, di tutti i percorsi di attacco abilitati dalle vulnerabilità, delle remediation da applicare per mitigare il rischio cyber ed eventuali what-if simulati

Un terzo tool esegue un monitoraggio ed intervento real time: consente di analizzare in modo avanzato le correlazioni tra eventi di sicurezza e di prevedere l'evoluzione delle minacce nel tempo. Grazie a modelli predittivi basati su algoritmi di machine learning, questo tool identifica pattern di attacco ricorrenti e segnali deboli che possono anticipare potenziali violazioni. Permette l'analisi predittiva delle minacce emergenti con una dashboard interattiva per il monitoraggio in tempo reale delle correlazioni e la generazione di report predittivi con raccomandazioni per la mitigazione proattiva.

L'integrazione di un approccio Cybersecurity Digital Twin predittivo offre vantaggi strategici per la conformità alla Direttiva NIS2, trasformando la difesa da reattiva a proattiva attraverso la simulazione e l'analisi dei dati in tempo reale, in quanto l'utilizzo di gemelli digitali permette di soddisfare i pilastri fondamentali della nuova normativa europea. Il Digital Twin crea una replica virtuale dell'infrastruttura IT/OT per simulare scenari di attacco senza impattare la produzione reale e consente l'identificazione precoce di vulnerabilità e percorsi di attacco non autorizzati attraverso simulazioni basate su dati reali e AI, supportando l'obbligo NIS2 di mantenere l'operatività aziendale testando l'efficacia dei piani di incident response e disaster recovery in un ambiente sicuro.

Permette poi di valutare l'impatto di modifiche o patch di sicurezza prima della loro implementazione effettiva e fornisce ai vertici aziendali prove tangibili e basate su evidenze (non supposizioni) per l'approvazione delle misure di sicurezza, rispondendo alla responsabilità diretta del management introdotta dalla NIS2.

5. Use Cases e scenari futuri

Gli use cases e gli scenari descritti nel presente capitolo non rappresentano esempi isolati o soluzioni puntuali, ma applicazioni concrete dell'architettura di riferimento per la convergenza ITS–AI–Cybersecurity descritta nel Capitolo precedente.

In ciascun caso, l'efficacia delle soluzioni proposte deriva dall'adozione di principi comuni quali sicurezza by design, architetture distribuite, integrazione tra AI e cybersecurity e gestione resiliente dei dati e delle comunicazioni.

Gli use cases sono pertanto da intendersi come istanze operative di un approccio architetturale coerente, replicabile e adattabile ai diversi contesti territoriali e infrastrutturali.

In questo contesto, al fine di rendere ancora più esplicita la lettura e l'analisi dei casi d'uso, è possibile adottare una chiave interpretativa basata su un modello architetturale multilivello.

Lettura architetturale multilivello dei casi d'uso

Al fine di garantire che le soluzioni presentate risultino coerenti, scalabili e replicabili, ogni caso d'uso viene analizzato attraverso un modello architetturale articolato su tre livelli:

- **Livello Edge:** sensori e sistemi di campo che raccolgono e pre-elaborano i dati direttamente alla fonte;
- **Livello Comunicazioni e Piattaforme:** le reti e le infrastrutture centrali preposte alla trasmissione, all'analisi e alla correlazione dei flussi informativi;
- **Livello Servizi e Controllo:** i sistemi decisionali e le interfacce per gli operatori e gli utenti finali.

Tale strutturazione definisce con chiarezza le responsabilità e il percorso dei dati lungo l'intera catena del valore. Sfruttando l'elaborazione distribuita (*edge computing*), si migliora la tempestività e la qualità delle informazioni, riducendo contestualmente la superficie d'attacco cibernetico. Questo approccio permette inoltre di legare in modo trasparente le scelte tecnologiche ai risultati operativi, facilitando la misurazione dell'efficacia e della sicurezza di ogni singola implementazione.

5.1 Partnership OEM strategiche e piattaforme su larga scala

La crescente pressione normativa europea (NIS2, Cyber Resilience Act, AI Act) e l'escalation documentata delle minacce cyber stanno trasformando la cybersecurity da funzione accessoria a componente strategica per i costruttori (OEM). L'industria ha maturato una consapevolezza: la sicurezza informatica per i trasporti richiede competenze ultra-specialistiche (dalla threat detection AI/ML alla valutazione del rischio IEC 62443) che si devono integrare con l'expertise ingegneristica tradizionale. Nonostante le differenze architetturali, i leader di mercato convergono verso la platformization: gli OEM stanno transitando da semplici venditori di treni fisici a fornitori di piattaforme digitali e servizi di cybersecurity che gestiscono l'intero ciclo di vita del prodotto.

5.1.1 Alstom e il modello risk assessment integrato

Alstom ha sviluppato la rete di partnership più articolata tra gli OEM ferroviari, puntando sull'integrazione nativa della cybersecurity nel proprio ciclo ingegneristico. La partnership con Airbus Protect ha generato una metodologia di risk assessment "field-tested" (presentata a InnoTrans 2024) che unisce tre framework: EBIOS Risk Manager, IEC 62443 e la specifica ferroviaria CLC/TS 50701. Lo strumento operativo è **FENCE**, un database centralizzato che

permette la tracciabilità delle decisioni di mitigazione e il riutilizzo delle valutazioni. Sul fronte operativo, l'investimento di 7 milioni di dollari in Cylus ha permesso di integrare algoritmi di Machine Learning per il monitoraggio delle reti di segnalamento (come nella Tel Aviv Red Line). Infine, l'approccio alla difesa delle reti fisiche è garantito da Waterfall Security tramite gateway hardware unidirezionali che azzerano gli attacchi di penetrazione remota.

5.1.2 Siemens Mobility e il monitoraggio fleetwide

L'approccio di Siemens Mobility trasforma la cybersecurity da funzione isolata a dimensione integrata nella gestione operativa della flotta. Questo è reso possibile dall'integrazione di **RazorSecure Delta** nell'ecosistema **Railigent X**. RazorSecure, operante su oltre 3.200 veicoli, funziona come un Network Intrusion Detection System (IDS) specifico per il *rolling stock*, mappando la rete di bordo e identificando anomalie. I dati confluiscono nello stesso cruscotto della manutenzione predittiva, portando a riduzioni tangibili: 40% in meno di tempi di fermo imprevisti e 30% in meno di costi di manutenzione. Siemens affianca al monitoraggio valutazioni periodiche tramite il dispositivo **SIESTA** e detiene la certificazione IEC 62443 con il raggio d'azione più ampio al mondo, utilizzando *digital twin* per abbattere del 60% i tempi di testing.

5.1.3 Hitachi Rail: piattaforma AI e cybersecurity integrata

Hitachi Rail ha intrapreso il percorso più ambizioso creando una piattaforma "full-stack" proprietaria. Dopo l'acquisizione di Thales GTS (€1,66 miliardi), ha presentato **HMAX**, una piattaforma unificata basata su quattro paradigmi di AI: Perception, Generativa, Agentica e Physical AI. L'ecosistema si regge su alleanze titaniche: l'infrastruttura cloud e le analisi ML sono fornite da **Google Cloud**; la simulazione virtuale di sistemi fisici complessi è alimentata da **NVIDIA**; il monitoraggio OT/IoT è garantito da **Nozomi Networks**. Tutti i dati convergono nei SOC gestiti da Hitachi Cyber. Sebbene questo modello offra una *detection* formidabile, introduce rischi strutturali di integrazione complessa e un potenziale *vendor lock-in*.

5.1.4 SBB e i contratti di interlocking digitale

Le strategie degli OEM trovano il loro massimo banco di prova nel programma delle Ferrovie Federali Svizzere (SBB/FFS). Nell'ottobre 2025, SBB ha assegnato contratti per 1,5 miliardi di euro per la migrazione al *digital interlocking*. Hitachi e Siemens si sono aggiudicate in parallelo il Lotto 1, mentre Stadler il Lotto 2. La transizione al digitale espande criticamente la superficie d'attacco, trasformando sistemi chiusi in reti connesse. I fornitori sono obbligati contrattualmente alla conformità IEC 62443 e CLC/TS 50701, garantendo un ciclo di manutenzione e sicurezza di ben 25 anni. La scelta di usare fornitori paralleli riflette i principi di diversificazione del rischio della NIS2.

5.1.5 NotPetya e Maersk — cascading failure nella logistica globale (2017)

Nel giugno 2017 il malware NotPetya colpì Maersk compromettendo l'intera infrastruttura IT: 49.000 laptop, 3.500 server, comunicazioni con terminal portuali in 76 paesi. Per dieci giorni Maersk operò senza sistemi informatici, con perdite stimate tra 250 e 300 milioni di dollari. L'unica copia integra dell'Active Directory fu recuperata da un server in Ghana rimasto offline durante l'attacco. Le lezioni: la dipendenza da un singolo fornitore software (M.E.Doc) evidenziò la criticità della supply chain security; l'assenza di segmentazione di rete permise la propagazione laterale; la mancanza di backup offline rallentò il ripristino. L'episodio accelerò l'adozione di observability avanzata basate su AI e blockchain per il monitoraggio delle catene logistiche.

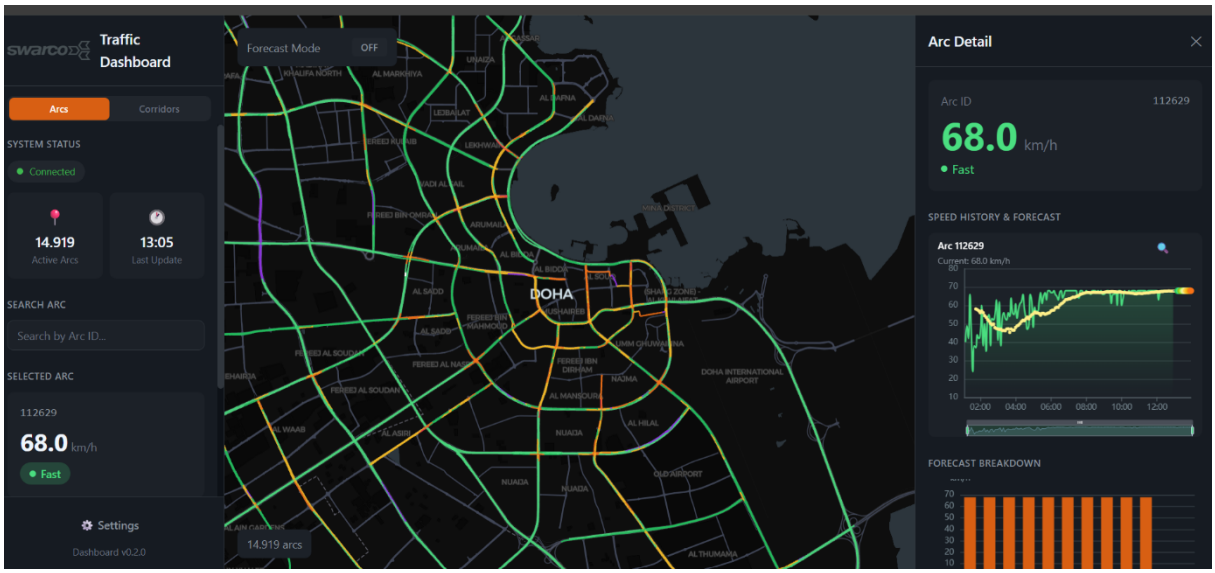
5.1.6 Caso d'Uso – AI predittiva per la gestione proattiva della mobilità (Doha, Qatar)

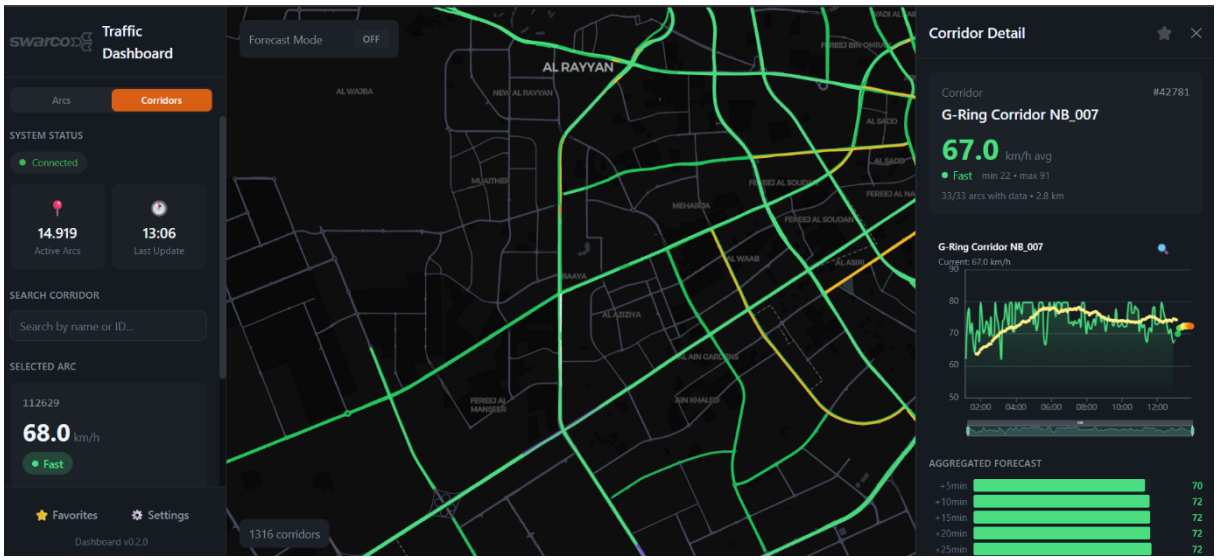
Questo caso rappresenta il benchmark internazionale di come le piattaforme AI su larga scala (simili a quelle proposte dai grandi OEM) possano gestire infrastrutture critiche complesse.

- **Descrizione:** il sistema monitora 6000 km di strade e 15.000 archi stradali tramite oltre 20.000 sensori connessi, elaborando 10 GB di dati giornalieri. L'architettura cloud integra un agente di *forecasting* che genera previsioni sul traffico fino a 60 minuti. Il modello combina machine learning supervisionato con componenti ibride fisico-statistiche;
- **Risultati**: il sistema è passato da una gestione reattiva a una proattiva. Identifica l'insorgere di saturazioni e genera raccomandazioni operative sui pannelli a messaggio variabile (VMS). L'accuratezza è validata tramite l'indicatore MAPE (Mean Absolute Percentage Error):

$$MAPE = \frac{1}{n}\sum_{t=1}^{n} \left|\frac{y_t - \hat{y}_t}{y_t}\right| \times 100$$

- **Ruolo dell'AI e della Cybersecurity:** l'AI effettua un cross-check tra fonti eterogenee (Floating Car Data e sensori). A livello cyber, l'infrastruttura (considerata critica per il Qatar) prevede API sicure, comunicazioni crittografate e rigorosa segregazione tra l'ambiente di training dei modelli AI e l'ambiente di produzione;
- **Benefici**: maggiore stabilità dei flussi e prevenzione del rischio in blackspots critici tramite integrazione di dati meteo. È un modello replicabile in Europa a supporto della Direttiva ITS 2023/2661.





5.1.7 Chiave di lettura architetturale

I modelli analizzati confermano l'orientamento verso ecosistemi digitali in cui la **cybersecurity** non è un modulo addizionale, ma una proprietà strutturale integrata *by design*. In tale architettura, il livello **Edge** agisce come primo presidio per la validazione del dato alla fonte, laddove le infrastrutture centrali ne permettono l'orchestrazione e l'elaborazione massiva. La convergenza fluida tra questi domini garantisce l'integrità informativa e l'affidabilità operativa, in piena aderenza ai paradigmi di *Zero Trust* e ai requisiti di resilienza sistemica richiesti dalla moderna mobilità intelligente.

5.2 Ecosistema startup per la Cybersecurity e Smart Mobility

L'ecosistema delle startup di cybersecurity ha registrato una crescita marcata, con investimenti globali balzati a 18 miliardi di dollari nel 2025 (+26%). Questa dinamica riflette la convergenza tra la spinta normativa, l'espansione della superficie d'attacco e la forte domanda di soluzioni verticali. Nel settore dei trasporti, le startup hanno ampiamente superato la fase prototipale, diventando componenti critici integrate direttamente negli ecosistemi dei grandi costruttori industriali.

5.2.1 Startup ferroviarie: dalla protezione del segnalamento al monitoraggio fleetwide

Questo segmento ha raggiunto la produzione su larga scala. L'israeliana **Cylus** (57 milioni di dollari di funding) addestra la propria AI a riconoscere i protocolli *safety-critical* specifici del segnalamento (CBTC ed ETCS). A maggio 2025 ha rafforzato la propria offerta integrandosi nei gateway ruggedizzati di duagon (D527). Parallelamente, la britannica **RazorSecure** si concentra sui sistemi operativi e sulle reti di bordo (informazione passeggeri, gateway IT/OT), gestendo la complessità di protocolli eterogenei. Entrambe le realtà compensano la mancanza di dataset sugli attacchi storici ferroviari utilizzando tecniche avanzate di *anomaly detection* non supervisionata basate sul machine learning.

5.2.2 Startup OT e difesa: dalla cybersecurity militare ai trasporti civili

Questo segmento prospera sul trasferimento tecnologico: architetture nate per proteggere asset militari vengono riadattate per la mobilità civile. **Shift5** ($260M di finanziamenti) è l'esempio più strutturato. Progettata

originariamente per la difesa USA, garantisce massima affidabilità in assenza di connettività. Nel febbraio 2025, ha stretto una partnership globale con Boeing per fornire un *Compliance Module* capace di automatizzare la verifica di conformità normativa aeronautica (ANSP), analizzando automaticamente i file di log. Questo pattern di trasferimento tecnologico dalla difesa accomuna anche realtà come Nozomi Networks, Claroty e Dragos.

5.2.3 Startup automotive: piattaforme per veicoli connessi

Con una proiezione di crescita a 28 miliardi di dollari entro il 2036, il segmento automotive è trainato dai Software-Defined Vehicles (SDV) e dalla normativa UNECE R155. Le startup si focalizzano su piattaforme cloud (XDR). **Upstream Security** protegge oltre 25 milioni di veicoli connessi (il 60% degli incidenti coinvolge flotte massicce tramite server telematici e API). L'investimento strategico di Cisco in Upstream dimostra la transizione verso il modello "Vehicle SOC", dove le soluzioni verticali automotive si integrano nelle grandi reti enterprise e comunicano con le infrastrutture cittadine.

5.2.4 Caso d'Uso – Gestione flussi e prevenzione "Phantom Jams" (Milano Serravalle / Smart Cities)

L'applicazione pratica delle tecnologie di startup e vendor specializzati per la Smart Mobility urbana.

- **Descrizione:** reti di telecamere intelligenti dotate di capacità di calcolo *Edge* monitorano i flussi su snodi critici (es. Milano Serravalle e Tangenziali). I sensori non si limitano a registrare video, ma estraggono metadati in tempo reale sulle traiettorie veicolari;
- **Risultati:** ottimizzazione dei cicli semaforici e drastica riduzione della congestione. L'impiego di queste tecnologie permette in particolare l'analisi e la prevenzione dei cosiddetti *phantom traffic jams* (ingorghi fantasma), ovvero le onde d'urto causate da frenate improvvise o cambi di corsia non necessari che paralizzano il traffico senza cause apparenti (incidenti o cantieri);
- **Ruolo dell'AI e della Cybersecurity:** l'AI a bordo camera rileva i micro-comportamenti che innescano le onde d'urto. La Cybersecurity garantisce che i feed video e i metadati raccolti siano cifrati e non manipolabili, tutelando la privacy dei conducenti (oscuramento automatico) e la continuità del servizio.
- **Benefici:** integrazione con piattaforme MaaS, rendendo la città di Milano metropoli più sicura e reattiva, in perfetta coerenza con gli standard ITS.

5.2.5 Chiave di lettura architetturale

L'approccio innovativo delle startup si concentra prioritariamente su moduli iper-specializzati dell'architettura, quali l'AI, la **Cybersecurity** delle comunicazioni o i framework di advanced analytics. Ciononostante, il valore strategico di tali soluzioni si manifesta appieno solo attraverso un'**integrazione interoperabile** e senza soluzione di continuità all'interno di ecosistemi di mobilità più vasti e complessi.

5.3 Progetti EU, finanziamenti e infrastrutture (TEN-T)

I programmi di finanziamento europei costituiscono la vera infrastruttura abilitante, articolandosi su tre livelli: *ricerca pre-competitiva* (Horizon Europe), *deployment delle tecnologie mature* (Digital Europe Programme) e *costruzione di capacità infrastrutturale* (CEF Digital). Sebbene i trasporti competano per questi fondi orizzontali con energia e finanza, hanno generato un portafoglio di progetti cruciali che traducono i framework normativi in strumenti operativi.

5.3.1 Progetti finanziati con partecipazione italiana

La ricerca pre-competitiva vede un posizionamento italiano eccellente. **CitySCAPE** (€5M) ha creato un toolkit di risk assessment multimodale testato sul trasporto pubblico genovese. **SAFETY4RAILS** ha analizzato la resilienza agli attacchi cyber-fisici con RFI. **CARAMEL** ha sviluppato protezioni anti-jamming GPS per veicoli autonomi, mentre **CYRail** ha generato i *Protection Profiles* per lo standard ferroviario CLC/TS 50701. Decisivo per l'implementazione pratica della NIS2 è **CYRUS** (Digital Europe Programme), coordinato da Deep Blue, che ha formato oltre 500 dipendenti del Gruppo FS sulle pratiche di igiene informatica.

5.3.2 ECCC e i bandi Digital Europe 2025-2027

L'European Cybersecurity Competence Centre (ECCC) ha stanziato 390 milioni di euro per il triennio 2025-2027. I bandi recenti mirano a coprire lacune cruciali: il DEPLOY-CYBER-06 (€40M) finanzia l'uso della *GenAI* nei SOC per sopperire alla carenza globale di analisti; il DEPLOY-CYBER-07 (€31M) accelera la migrazione alla crittografia Post-Quantum (PQC), vitale per infrastrutture con cicli di vita di 30 anni; il DEPLOY-CYBER-08 finanzia strumenti di *threat intelligence*. Il limite è la natura orizzontale dei fondi, che costringe i trasporti a competere con altri settori critici.

5.3.3 Mobilità connessa e automazione urbana (IN2CCAM)

Il progetto europeo IN2CCAM nasce per accelerare l'integrazione di soluzioni di mobilità connessa, cooperativa e autonoma (CCAM) nei sistemi di trasporto urbano. Attraverso l'integrazione di infrastrutture fisiche, digitali e operative, l'iniziativa mira a elevare gli standard di sicurezza, efficienza del traffico e sostenibilità ambientale. In questo scenario, la creazione di Living Lab europei funge da banco di prova per validare nuovi modelli di mobilità e definire quadri di governance scalabili, capaci di trasformare la gestione dei flussi urbani in contesti reali.

5.3.4 Caso d'Uso – Integrazione e adozione di soluzioni CCAM: Living Lab Torino

La sperimentazione di veicoli autonomi e strategie dinamiche di gestione del traffico per l'ottimizzazione dell'ecosistema urbano.

- **Descrizione**: implementazione di un caso pilota nel Living Lab di Torino focalizzato sull'integrazione di navette autonome in ambito urbano reale. Il progetto ha previsto il test di tecnologie CCAM e lo sviluppo di servizi innovativi di gestione del traffico tramite comunicazione Vehicle-to-Infrastructure (V2I). TTS Italia ha coordinato le attività operative, gestendo l'autorizzazione tecnica con il MIT, l'ottenimento della polizza assicurativa e facilitando il coinvolgimento degli stakeholder per la scalabilità delle soluzioni;
- **Risultati**: Torino ha dimostrato la capacità di ricalcolare dinamicamente i percorsi delle navette sulla base dei dati in tempo reale. Le analisi hanno evidenziato una riduzione dei tempi di percorrenza totali fino all'11% e dei ritardi fino al 22% in condizioni di traffico intenso. In scenari critici, il ritardo medio per viaggio è stato ridotto fino al 37%, confermando l'efficacia dei meccanismi di bilanciamento del carico per ridistribuire il traffico dalle aree congestionate;
- **Ruolo dell'AI e della Cybersecurity:** l'AI abilita il controllo adattivo del traffico e l'ottimizzazione dei percorsi, permettendo alla navetta di evitare aree sature e migliorare indirettamente il flusso dei veicoli non connessi. La Cybersecurity è centrale nella piattaforma *Ohmio Lift*, progettata con sistemi di controllo isolati per impostazione predefinita. La connettività esterna (per diagnostica remota, integrazione con semafori o gestione del trasporto a richiesta tramite *PADAM Mobility*) è limitata e controllata caso per caso per bilanciare funzionalità e protezione contro accessi non autorizzati;
- **Benefici**: miglioramento della sicurezza e della sostenibilità ambientale attraverso la riduzione della congestione locale. Il comportamento ottimizzato del veicolo autonomo (adeguamenti precoci del percorso) genera benefici misurabili per l'intera rete stradale. Il progetto ha inoltre prodotto un quadro di governance scalabile per l'adozione di soluzioni CCAM a livello nazionale ed europeo.

5.3.5 AI affidabile e accettazione sociale della mobilità autonoma (AI4CCAM)

Il passaggio verso la mobilità automatizzata richiede non solo innovazione tecnologica, ma un framework di "AI affidabile" (trustworthy-by-design) che metta al centro la sicurezza degli utenti vulnerabili della strada (VRU), come pedoni e ciclisti. Il progetto europeo AI4CCAM (Horizon Europe) affronta questa sfida integrando linee guida etiche e tecniche avanzate di anticipazione del comportamento. L'obiettivo è superare la diffidenza verso i veicoli automatizzati, trasformando la percezione dell'AI da "scatola nera" a strumento trasparente, inclusivo e capace di interagire in modo naturale e sicuro nel contesto urbano.

5.3.6 Caso d'Uso – Validazione dell'accettazione utente per veicoli CAV (AI4CCAM)

Lo sviluppo di un ambiente aperto per l'integrazione di modelli di AI affidabili e la ricerca sull'interazione tra auto autonome e utenti vulnerabili.

- **Descrizione:** coordinato da Simula Research Laboratory e con la responsabilità di TTS Italia per il Caso d'uso 3, il progetto sviluppa modelli per l'anticipazione del comportamento di pedoni e ciclisti basati sulla stima dello sguardo e sulla predizione delle traiettorie. La sperimentazione utilizza un sistema centralizzato per focus group europei, indagini stated-choice ed esperimenti immersivi in realtà virtuale che simulano scenari urbani complessi (incroci, rotatorie, aree dense). Un elemento chiave è il test di sistemi di comunicazione non verbale, come i digital eyes montati sul veicolo per fornire feedback visivo ai pedoni;
- **Risultati:** produzione di una metodologia per l'AI affidabile applicata alla mobilità (D1.1) e rilascio del Participatory AI4CCAM Space, una piattaforma partecipativa per coinvolgere cittadini ed esperti nella definizione dei requisiti etici. È stata inoltre creata una libreria di scenari di simulazione sul simulatore CARLA (D4.4). I risultati includono l'identificazione dei fattori determinanti per l'accettazione sociale e una tabella di marcia per superare le barriere alla diffusione dei veicoli automatizzati. I casi d'uso sono consultabili al link: https://www.youtube.com/watch?v=luiUiCqnz5w;
- **Ruolo dell'AI e della Cybersecurity:** l'AI è il motore del progetto attraverso modelli di deep learning per la percezione e pianificazione spiegabile a bordo veicolo. Vengono utilizzate reti generative avversarie (GAN) e metamorphic testing per generare scenari sintetici e individuare distorsioni (bias) nei dati, garantendo robustezza in condizioni critiche. La Cybersecurity è declinata secondo l'approccio trustworthy-by-design, focalizzandosi sulla protezione dei dati personali raccolti nei focus group (GDPR), sulla tracciabilità dei dataset di addestramento e sulla difesa del Participatory Space da manipolazioni o minacce informatiche;
- **Benefici**: fornitura di strumenti integrati per industria e regolatori europei per progettare soluzioni di mobilità autonoma inclusive e trasparenti. La creazione di un Long-Term Advisory Board dopo la chiusura del progetto (aprile 2026) assicurerà il mantenimento dei modelli e dei dataset prodotti, consolidando un ecosistema europeo per lo sviluppo di IA affidabile applicata alla mobilità cooperativa e automatizzata.

5.3.7 Europe's Rail Joint Undertaking e i programmi framework

Europe's Rail JU è il principale strumento europeo verticale per il trasporto su rotaia. Un focus centrale è il passaggio al **FRMCS** (il sistema di comunicazione 5G SA), che incorpora nativamente la sicurezza (95,5% di interoperabilità nei recenti test). Iniziative come OCORA hanno prodotto la *ERORAT Guideline v3.01* (marzo 2025), che traduce lo standard IEC 62443 per i sistemi di Comando e Controllo (CCS). A chiudere il cerchio infrastrutturale interviene il CEF Digital (€47,4M), che finanzia la costruzione materiale delle reti 5G sicure lungo i corridoi logistici TEN-T.

5.3.8 Caso d'Uso – Sistema di pedaggio intelligente (Intelligent Tolling)

L'integrazione di sistemi di esazione sicuri lungo i corridoi stradali, in linea con i programmi infrastrutturali europei.

- **Descrizione:** implementazione di sistemi di pedaggio *Free Flow* ad alta velocità. Si basano su sensori IoT e telecamere intelligenti (es. architetture specializzate) che effettuano classificazione volumetrica e lettura targhe (ANPR) direttamente *on-the-edge*, integrandosi in architetture centrali sicure e resilienti;
- **Risultati:** massima efficienza operativa con abbattimento delle code ai caselli, riduzione drastica degli errori di classificazione (profilazione assi/sagoma) e maggiore tracciabilità dei flussi commerciali e privati;
- **Ruolo dell'AI e della Cybersecurity:** l'AI abilita la classificazione automatica e rileva le anomalie (es. targhe alterate o illeggibili). Operando come un sistema finanziario a tutti gli effetti, un'architettura di Cybersecurity rigorosa garantisce l'integrità, l'inviolabilità e l'auditabilità delle transazioni di pagamento;
- **Benefici:** evoluzione verso sistemi di pedaggiamento interoperabili nazionali ed europei (framework ITS), supportando futuri modelli di tariffazione dinamica (es. basata su fasce orarie o inquinamento) all'interno della mobilità integrata.

5.3.9 Chiave di lettura architetturale

Le risultanze dei progetti europei analizzati confermano come un approccio a compartimenti stagni non risulti più sostenibile. Risulta indispensabile adottare una visione sistemica: dalla generazione del dato all'**Edge** periferico fino alla sua elaborazione centralizzata, ogni livello architetturale deve essere progettato in maniera coordinata. La **cybersecurity**, l'**interoperabilità** e una rigorosa **governance** delle informazioni devono rappresentare il pilastro fondamentale dell'intera progettazione *secure-by-design*.

5.4 Ecosistema italiano per la cybersecurity nei trasporti

L'assenza di un programma europeo dedicato in via esclusiva ai trasporti rende cruciale il ruolo degli ecosistemi nazionali. L'Italia opera in un contesto dicotomico: da un lato, un mercato cyber in rapida crescita (2,48 miliardi di euro nel 2024, +15%); dall'altro, un'esposizione spaventosa, che colloca l'Italia come secondo Paese più colpito in Europa (attira oltre il 25% degli attacchi globali ai trasporti). L'ecosistema si articola su quattro pilastri: operatori (domanda), industria (offerta), ricerca (competenze) e istituzioni (enforcement normativo).

5.4.1 Leonardo e la gestione della cyber-resilienza nazionale

Leonardo SpA rappresenta un pilastro dell'offerta tecnologica nazionale, fornendo servizi e piattaforme che garantiscono il monitoraggio e la protezione predittiva di dati e asset strategici. Attraverso architetture secure-by-design, l'uso di Big Data e tecniche di supercalcolo, l'azienda ricopre un ruolo centrale nel rilevamento e nell'analisi delle minacce cibernetiche. Grazie all'acquisizione della finlandese SSH Communications Security, Leonardo ha integrato soluzioni avanzate come la crittografia quantum-safe e le architetture Zero Trust sovrane, fondamentali per la difesa delle infrastrutture critiche del Paese.

5.4.2 Caso d'Uso – Ottimizzazione del Vulnerability Management tramite AI (RBVR per ANAS)

L'applicazione dell'AI per gestire e dare priorità alle vulnerabilità software nelle infrastrutture critiche stradali.

- **Descrizione:** il progetto Risk-Based Vulnerability Remediation trasforma il tradizionale processo statico di gestione delle vulnerabilità in un modello data-driven. Utilizza modelli di AI e algoritmi di Natural Language Processing (NLP) basati su architetture Transformer per leggere e analizzare automaticamente i testi dei report di vulnerability assessment, estraendo entità rilevanti (prodotti software, versioni) e individuando relazioni tra gli interventi tecnici suggeriti;

- **Risultati:** nei perimetri dell'infrastruttura tecnologica di ANAS analizzati, il sistema AI ha identificato e raggruppato gli interventi ridondanti. Le azioni di remediation necessarie sono passate da 1068 a sole 300, ottenendo una riduzione degli interventi operativi del 71,9%. In media, ogni singola azione suggerita dall'AI ha sostituito 3,6 interventi tecnici isolati;
- **Ruolo dell'AI e della Cybersecurity**: l'AI (NLP) agisce come un analista esperto, comprendendo il testo non strutturato dei log di sicurezza e correlando i dati. La Cybersecurity ne trae un vantaggio operativo immenso: anziché basarsi solo sul punteggio teorico statico (CVSS), i team di sicurezza possono ottimizzare il patch management concentrando le loro risorse limitate sulle vulnerabilità che presentano un rischio effettivo per l'organizzazione;
- **Benefici:** drastica riduzione della complessità operativa, risparmio di ore-uomo per i team di sicurezza, facilitazione nella pianificazione degli interventi IT e una gestione nettamente più sostenibile e proattiva della cyber-resilienza in ambienti infrastrutturali altamente complessi.

5.4.3 Ricerca, formazione e competence center

Il sostrato delle competenze è garantito dal **CINI**, che tramite *CyberChallenge.IT* forma talenti e trasferisce ricerca metodologica. Il Competence Center **START 4.0** di Genova funge da cerniera operativa per i porti e la logistica del Nord-Ovest, organizzando l'evento annuale CSET. La più grande vulnerabilità del sistema Italia si riscontra nel Trasporto Pubblico Locale (TPL): mentre i grandi player sono strutturati, i numerosi operatori regionali — soggetti alla NIS2 (Allegato IV) — affrontano obblighi complessi con budget frammentati e gravi carenze di competenze. Associazioni come ASSTRA tentano di colmare questo gap strutturale.

5.4.4 ACN e l'enforcement NIS2 nei trasporti

L'Agenzia per la Cybersicurezza Nazionale (ACN), in tandem con il Ministero dei Trasporti (MIT), ha avviato le scadenze inderogabili della NIS2 (D.Lgs. 138/2024). Da gennaio 2026, gli operatori essenziali devono notificare gli incidenti entro 24 ore; entro ottobre 2026 dovranno aver adottato le misure di sicurezza baseline. La pressione è confermata dai dati del CSIRT-Italia: nel secondo semestre 2025 gli eventi cyber sono balzati del 30%, trainati da attacchi DDoS e dall'"effetto domino" delle compromissioni IT. Il MIT guida parallelamente l'innovazione infrastrutturale tramite l'Osservatorio Tecnico Smart Road.

5.4.5 Caso d'Uso – Smart Road e monitoraggio infrastrutturale (ANAS)

L'applicazione pratica degli investimenti istituzionali

- **Descrizione:** le iniziative ANAS (supportate da RTI Site e Valtellina) trasformano la rete in una Smart Road. Le telecamere Edge (es. tecnologie Axis) raccolgono e pre-elaborano i dati visivi. Soluzioni di AI specifiche (come l'AI di Waterview) permettono di misurare intensità di pioggia o presenza di neve/nebbia direttamente dall'analisi delle immagini della telecamera, trasformandola in un sensore meteo;
- **Risultati:** riduzione enorme dei tempi di rilevazione di incidenti, veicoli fermi o oggetti in carreggiata, garantendo interventi immediati e incrementando la resilienza dell'infrastruttura stradale;
- **Ruolo dell'AI e della Cybersecurity:** l'AI classifica le anomalie a livello Edge. La Cybersecurity garantisce l'integrità del dato trasmesso, l'autenticazione crittografica di migliaia di nodi sparsi sul territorio e la protezione delle comunicazioni secondo il modello di *Security Fabric*;
- **Benefici:** sviluppo di modelli predittivi del rischio meteo-stradale, supporto alla pianificazione dinamica e futura integrazione con i Digital Twin autostradali.

5.4.6 Caso d'Uso – Smart Parking e gestione accessi

La gestione dell'ultimo miglio urbano nell'ecosistema di smart mobility.

- **Descrizione:** sistemi intelligenti per la gestione dei parcheggi e delle aree di sosta basati su rilevazione automatica ottica o magnetica, capaci di fornire un monitoraggio in tempo reale dell'occupazione e della gestione dei varchi di accesso alle ZTL;
- **Risultati:** drastica riduzione del traffico indotto (le auto in cerca di sosta), ottimizzazione sistematica degli spazi urbani e netto miglioramento dell'esperienza per il cittadino;
- **Ruolo dell'AI e della Cybersecurity:** l'AI abilita la rilevazione predittiva della disponibilità di stalli e l'analisi dell'utilizzo delle aree nel tempo. La Cybersecurity è fondamentale per tutelare i dati di localizzazione, le abitudini degli utenti e impedire accessi non autorizzati all'infrastruttura cittadina;
- **Benefici:** integrazione completa con le piattaforme MaaS, supporto alle politiche di mobilità sostenibile ed evoluzione verso ecosistemi urbani pienamente interconnessi.

5.4.7 Innovazione e sicurezza nella rete autostradale (CAV)

L'evoluzione della rete autostradale italiana, caratterizzata da un traffico di oltre 86,6 miliardi di veicoli-km nel 2023 e da una complessa architettura di gallerie e viadotti, richiede un passaggio strategico verso modelli di gestione proattiva. In questo contesto, l'integrazione di dati, infrastrutture e sistemi intelligenti diventa fondamentale per rafforzare la resilienza e la capacità di prevenzione delle emergenze. La collaborazione tra Autostrade dello Stato e CAV mira a costruire un ecosistema integrato capace di anticipare i rischi, elevando gli standard di sicurezza ed efficienza dell'intera rete nazionale.

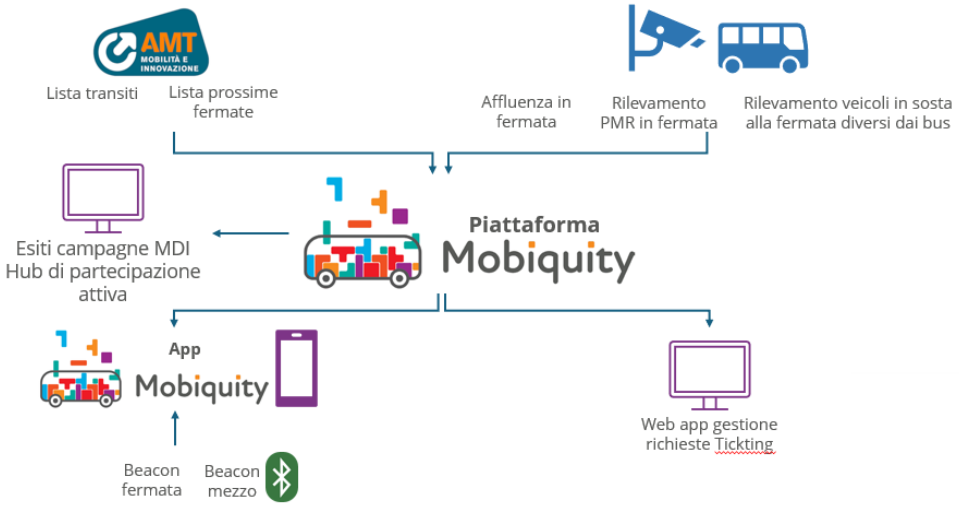
5.4.8 Caso d'Uso – Sicurezza infrastrutturale e AI: piattaforma STRIVE (CAV)

L'integrazione di sistemi di monitoraggio avanzati per la gestione proattiva delle emergenze autostradali, sviluppata da Autostrade dello Stato insieme a CAV.

- **Descrizione**: implementazione della piattaforma STRIVE, fulcro delle soluzioni innovative per il monitoraggio e la sorveglianza avanzata della rete autostradale. Il sistema utilizza telecamere smart e algoritmi addestrati per analizzare flussi video in tempo reale, individuando segnali precoci di rischio come la presenza di fumo. La sperimentazione operativa è stata condotta il 19 marzo 2026 nella galleria San Silvestro (Passante di Mestre), simulando un incendio generato da un veicolo fermo a seguito di un tamponamento;
- **Risultati**: durante la prova, la piattaforma ha rilevato tempestivamente il fumo, generato un alert sulla GUI e supportato efficacemente il processo decisionale dell'operatore. Il test ha confermato la riduzione dei tempi di individuazione delle emergenze, migliorando la qualità delle informazioni e segnando il passaggio concreto da una gestione reattiva a una proattiva e predittiva;
- **Ruolo dell'AI e della Cybersecurity**: l'AI è l'elemento abilitante che analizza i flussi video per superare la sorveglianza passiva, evolvendo nel tempo grazie all'interazione con l'operatore per ridurre i falsi positivi. La cybersecurity garantisce la solidità dell'intero sistema, proteggendo i flussi informativi, assicurando l'integrità dei dati e salvaguardando le logiche algoritmiche da potenziali manomissioni;
- **Benefici**: l'approccio incrementa la sicurezza per utenti e personale operativo attraverso un miglior coordinamento dei soggetti coinvolti. Un elemento distintivo è la tutela dei soccorritori: l'intervento è stato supportato da robot antincendio radiocomandati, che permettono di operare in ambienti ad alto rischio riducendo l'esposizione umana diretta.

5.4.9 Accessibilità e inclusione nel Trasporto Pubblico Locale (Mobiquity)

Il divario di accessibilità ai servizi essenziali rappresenta una sfida centrale per le moderne Smart City, specialmente per le Persone a Mobilità Ridotta (PMR). Ridurre questo gap significa non solo abbattere barriere architettoniche fisiche, ma anche digitali, incentivando l'autonomia e la partecipazione sociale.



Attraverso l'approccio del Co-Design for All, il progetto Mobiquity (finanziato dal PR FESR 2021-2027) ha trasformato le necessità espresse direttamente dai cittadini con disabilità in soluzioni tecnologiche concrete, definendo nuove linee guida metodologiche per un TPL realmente inclusivo e accessibile.

5.4.10 Caso d'Uso – Assistenza alla mobilità inclusiva: progetto Mobiquity (Genova)

L'integrazione di sistemi di AI e monitoraggio IoT per il supporto personalizzato alle Persone a Mobilità Ridotta (PMR) nel sistema di trasporto pubblico di Genova.

- **Descrizione**: sviluppo di un ecosistema digitale composto da un'app mobile, hardware di fermata (beacon e telecamere AI) e interfacce per i conducenti AMT. Il sistema permette agli utenti, in particolare non vedenti o con disabilità motorie, di localizzare la fermata, visualizzare l'affollamento dei bus in arrivo e prenotare la salita (segnalando la necessità della pedana) prima ancora del sopraggiungere del mezzo. L'app abilita inoltre la comunicazione diretta con l'autista durante il viaggio e la partecipazione attiva tramite l'invio di segnalazioni sull'accessibilità urbana e il calcolo del Mobility Divide Index (MDI);
- **Risultati:** realizzazione di una piattaforma integrata che supporta l'intero ciclo del viaggio e di un "Hub di partecipazione attiva" per la governance collaborativa tra cittadini e istituzioni. I test hanno validato la capacità del sistema di fornire informazioni in tempo reale (come il livello di affollamento) e di facilitare le operazioni di imbarco/sbarco, creando le basi per un modello di mobilità urbana scalabile e replicabile a livello nazionale ed europeo;
- **Ruolo dell'AI e della Cybersecurity**: l'AI utilizza algoritmi di Deep Learning e la piattaforma AI-Sphere (Aitek) per elaborare in tempo reale le immagini delle telecamere, rilevando automaticamente la presenza di PMR, posti riservati occupati o ostacoli in fermata. L'AI analizza inoltre i dati provenienti da wearable (smartwatch) per correlare i parametri fisiologici dell'utente al comfort del viaggio. La Cybersecurity protegge l'ecosistema tramite la crittografia dei flussi video, l'uso di VPN e protocolli sicuri (MQTT/REST API), garantendo l'anonimizzazione dei dati sensibili e la conformità al GDPR;
- **Benefici**: aumento significativo dell'autonomia e della sicurezza delle persone vulnerabili, migliorando la qualità dell'esperienza di viaggio. Gli operatori di TPL ottengono strumenti precisi per la pianificazione di politiche inclusive basate su dati reali, mentre l'uso di tecnologie IoT (come i beacon Bluetooth Low Energy)

assicura una navigazione precisa per i non vedenti, riducendo le barriere informative e fisiche dell'ultimo miglio.

5.4.11 Eventi, esercitazioni e cooperazione internazionale

Il 2026 rappresenta l'anno della verità: a giugno l'esercitazione continentale **Cyber Europe** dell'ENISA sarà dedicata esclusivamente ai trasporti, simulando un blocco coordinato di ferrovie e porti tramite attacchi cyber-fisici simultanei. Data l'alta incidenza di attacchi in Italia, la partecipazione del CSIRT-Italia e di operatori come FS costituirà un test di *preparedness* fondamentale. A livello istituzionale, la conferenza ERA-ENISA (dicembre 2025) ha sottolineato l'importanza dell'ER-ISAC per lo scambio confidenziale di *threat intelligence* nel trasporto ferroviario.

5.4.12 La cybersecurity nella supply chain e nella distribuzione alimentare

Nell'ambito del trasporto delle merci, il settore alimentare rappresenta un ambito che per complessità e pervasività non ha eguali in Italia ed Europa. Pur essendo unificato dall'oggetto del trasporto, in realtà si compone di divere separate linee, definite da una serie di fattori che, semplificando si possono enumerare come origine, modalità di consumo, deperibilità, natura. In particolare, si focalizza l'attenzione sulla supply chain dei prodotti deperibili freschi e freschissimi destinati alla distribuzione moderna.

Il trasporto per diverse classi di questi prodotti è obbligatoriamente effettuato con veicoli dotati di certificazione ATP (Accord Transport Perissable), un trattato internazionale in vigore dagli anni 1970 e riconosciuto in ambito ONU per il trasporto transfrontaliero. Esso prevede che a bordo dei veicoli siano presenti dei rilevatori di temperatura in grado di registrarne i livelli nel vano o nella cassa di carico durante il trasporto. La comunicazione avviene direttamente dal sensore alla destinazione, che è costituita da un sistema di tracciamento in capo al gestore del veicolo.

Oggi in Italia sono in circolazione circa 120.000 "oggetti" ATP, la cui proprietà è molto frammentata ove la più grande flotta ATP supera di poco le 2000 unità. Altro discorso per la gestione, dove esistono servizi multi-cliente, spesso in cloud, che si occupano anche di 15.000 nodi. La necessità di migliorare il monitoraggio delle temperature sta però portando ad aumentare il numero dei sensori e quindi a centralizzare i dati del singolo mezzo per poi inviarli al centro, cui si aggiunge la bidirezionalità della comunicazione, nata per consentire la calibrazione ma che oggi permette il monitoraggio e controllo remoto del gruppo frigo.

I veicoli refrigerati stanno quindi diventando vulnerabili ad attacchi sul singolo "nodo" e sull'intera flotta, specie in momenti in cui la supervisione locale dell'autista sia assente o rilassata, per esempio nelle fasi di sosta notturna oppure alla compromissione del veicolo stesso. Anche il centro di distruzione (Ce.Di.) della grande distribuzione organizzata può essere soggetto ad attacchi, con un blocco dei rifornimenti ai punti vendita ed alla compromissione degli alimenti stoccati.

Con la nuova generazione di sensori/attuatori a bordo veicolo e con il crescente accentramento delle funzioni di monitoraggio e telecontrollo delle flotte in sistemi condivisi operanti in cloud, la cybersicurezza del trasporto di alimentari deperibili deve quindi salire di livello nell'attenzione, come pure per i Ce.Di. e la catena nel suo complesso, considerando che oggi la maggioranza dei sistemi frigoriferi viene gestita da remoto da fornitori di servizi, anch'essi attaccabili. Diventa necessario una rigorosa qualificazione dei fornitori anche dal punto di vista della cybersicurezza.

5.4.13 Chiave di lettura architetturale

L'ecosistema nazionale converge verso modelli di **integrazione profonda**, in cui sensori distribuiti, piattaforme cloud e sistemi di controllo operano in sinergia. In tale assetto cooperativo, assicurare la **sicurezza** e l'**affidabilità** del dato sin dal suo punto di origine (*Edge*) rappresenta il fondamento indispensabile per garantire la **resilienza** e l'efficacia dell'intera infrastruttura di mobilità.

6. Raccomandazioni e conclusioni

La mobilità del futuro sarà definita dalla capacità di gestire una complessità tecnologica senza precedenti. Solo un approccio integrato, proattivo e standardizzato, capace di unire ingegneria dei trasporti e resilienza cibernetica, potrà garantire che l'intelligenza dei nostri sistemi non diventi il loro punto di rottura, ma il fondamento della nostra sicurezza nazionale

Le proposte contenute in questo capitolo rappresentano l'esito coerente del lavoro svolto dal GdL di TTS Italia, visti anche gli esiti di parallele attività anche istituzionali, quali ad esempio quella dell'8° Commissione permanente del Senato della Repubblica Italiana nell'ambito dell'indagine Conoscitiva sulle Tecnologie digitali e l'AI per le infrastrutture italiane. Ciò delinea 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.

Il Nuovo Paradigma della Mobilità: convergenza strategica tra ITS, AI e Cybersecurity.

La trasformazione digitale della mobilità non è una mera evoluzione tecnologica di settore, ma rappresenta una convergenza critica di tre pilastri fondamentali che oggi definiscono il perimetro della sicurezza nazionale e della competitività economica.

Gli ITS, l'AI e la Cybersecurity non operano più in silos indipendenti, ma formano un unico ecosistema cyber-fisico.

La missione del Gruppo di Lavoro è stata quella di mappare questa integrazione, identificando come il flusso di dati e l'efficacia degli algoritmi siano i motori per garantire viaggi non solo più fluidi e puliti, ma intrinsecamente sicuri e inclusivi.

L'architettura della mobilità moderna si regge su questi tre cardini strategici:

- ITS: l'infrastruttura digitale abilitante che integra sensoristica, edge computing e comunicazioni V2X per ottimizzare la gestione del traffico e la sicurezza stradale;
- AI: il catalizzatore decisionale che sposta il paradigma da sistemi reattivi a modelli predittivi e autonomi, capaci di elaborare volumi massivi di dati in millisecondi;
- Cybersecurity: il garante della resilienza, necessario per proteggere l'integrità del sistema e la sovranità dei dati in un perimetro di rete che non conosce confini fisici definiti.

Questa evoluzione, pur offrendo benefici sistemici senza precedenti, espande drasticamente la superficie di 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.

Impatto del valore digitale

La comprensione delle metriche economiche è il presupposto per giustificare investimenti proporzionati in sicurezza e innovazione. 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. I dati del Rapporto CLUSIT 2026 e del Tinexta Cyber Threat Landscape 2025 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'AI trasforma questi numeri in capacità operativa, ma richiede una protezione che sia altrettanto dinamica e scalabile.

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 in accordo a quanto

richiesto dalle normative nazionali ed europee in essere e strategiche per il futuro della mobilità e per rafforzare l'autonomia logistica del Paese.

L'AI come catalizzatore di efficienza e nuova superficie di attacco

L'adozione dell'AI 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'AI 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'AI 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 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.

Anatomia delle minacce nella mobilità connessa

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 semaforo, app e centralina di ricarica. 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 di attori che integrano deliberatamente hardware vulnerabile nella supply chain. Questi difetti sono impossibili da rilevare con certificazioni standard e rappresentano un rischio diretto a livello nazionale oppure attacchi che, partendo da un nodo secondario, si propagano per risonanza in sistemi interconnessi, portando al collasso di intere reti di trasporto come pure l'inserimento di falsi avvisi o manipolazioni di sensori sul campo.

Questa anatomia delle minacce discussa nel presente rapporto dimostra che la conformità normativa non è un onere burocratico, ma l'unico sistema di difesa scalabile contro attacchi di magnitudo geopolitica.

Il framework normativo: da obbligo a opportunità di resilienza

I pilastri del quadro regolatorio sono:

- Direttiva ITS 2023/2661/UE (Decreto 26/01/2026): 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;
- NIS2 (D.Lgs. 138/2024): inquadra la mobilità come infrastruttura critica, imponendo obblighi severi di gestione del rischio e notifica incidenti;
- AI Act: classifica i sistemi di trasporto ad "alto rischio", richiedendo supervisione umana, trasparenza algoritmica e robustezza dei dati;
- Standard Tecnici Convergenti: è fondamentale distinguere tra la ISO 21434, focalizzata sulla gestione della cybersecurity lungo tutto il ciclo di vita del veicolo, e la IEC 62443, che disciplina la sicurezza dei componenti industriali e infrastrutturali (OT);
- CRA: impone requisiti di sicurezza per tutti i prodotti digitali (hardware e software) lungo l'intera supply chain.

L'adozione del paradigma "Compliance by Design" è l'unica via per gestire la complessità normativa europea, trasformando i vincoli in vantaggi competitivi.

6.1 Raccomandazioni strategiche e proposte

A valle delle attività del Gruppo di Lavoro, sintetizzate nel presente Rapporto, si formulano le seguenti raccomandazioni strategiche per costruire un ecosistema di mobilità resiliente, al cui rispetto potranno essere vincolati eventuali incentivazioni di legge.

Queste linee di azione sono fra loro interconnesse e nel loro insieme costituiscono un quadro strategico per guidare la trasformazione digitale del sistema infrastrutturale e logistico italiano. Esse sono appunto concepite non come misure isolate, ma come strumenti operativi di una nuova politica industriale e territoriale, fondata su sicurezza, innovazione, sostenibilità e competitività.

R1 – Adottare una governance architetturale integrata per ITS, AI e cybersecurity

La progettazione dei sistemi di mobilità intelligente dovrebbe basarsi su architetture di riferimento coerenti e condivise, che integrino fin dall'origine ITS, AI e cybersecurity. Un approccio architetturale consente di evitare soluzioni frammentate, ridurre la complessità operativa e garantire interoperabilità, scalabilità e resilienza nel tempo. La sicurezza non deve essere considerata come un requisito aggiuntivo, ma come una proprietà strutturale del sistema.

R2 – Integrare i principi di Security by Design e Zero Trust lungo l'intero ciclo di vita

È raccomandabile che i sistemi di mobilità intelligente vengano progettati secondo i principi di security by design e by default, applicando modelli Zero Trust a tutti i livelli dell'ecosistema. Ogni componente — veicolo, infrastruttura, piattaforma digitale o servizio — dovrebbe essere autenticato, autorizzato e monitorato in modo continuo, riducendo la dipendenza da perimetri statici e aumentando la capacità di risposta a minacce evolutive.

R3 – Promuovere l'integrazione tra AI e cybersecurity come fattore abilitante della resilienza

L'AI dovrebbe essere utilizzata non solo come strumento di ottimizzazione dei servizi di mobilità, ma anche come elemento attivo di difesa. L'integrazione tra AI e cybersecurity consente il rilevamento precoce di anomalie, l'analisi predittiva delle minacce e l'automazione delle risposte agli incidenti, rafforzando la resilienza operativa dei sistemi complessi e distribuiti.

R4 – Rafforzare la governance dei dati, l'interoperabilità e l'uso di standard aperti

La qualità, la sicurezza e la governance dei dati rappresentano un prerequisito fondamentale per l'efficacia dei sistemi ITS e dei modelli di AI. In linea con le indicazioni Comunitarie e nazionali, è necessario favorire l'adozione di standard aperti, modelli interoperabili e spazi di dati condivisi, in linea con le iniziative europee sullo Spazio Comune dei Dati sulla Mobilità e dell'aggiornamento della Direttiva ITS con la definizione di chiari modelli di governance ed economici che incoraggino la condivisione dei dati tra attori pubblici e privati. Si supera così la frammentazione attuale e si creerà una base comune ove reperire dati di mobilità certificati su cui costruire servizi ITS affidabili ed aggiornati. Ciò consentirà di valorizzare i dati esistenti, ridurre i lock-in tecnologici e favorire la collaborazione tra attori pubblici e privati.

R5 - Promuovere lo sviluppo di AI Settoriale e Trustworthy

A valle dell'obiettivo R5, gli investimenti e gli sforzi politici andrebbero concentrati sullo sviluppo di modelli di AI specifici per il dominio dei trasporti, creando un vantaggio competitivo distintivo, fondato sull'affidabilità, la sicurezza e la piena conformità ai valori e al quadro normativo europeo, costruendo un marchio globale di "AI affidabile", con creazione di Mobility Data Platform nazionale interoperabile con il NAP, con API garantendo così la conformità e facile replicabilità in ogni Paese UE

R6 – Ecosistema integrato di logistica

La sfida dell'autonomia logistica e della resilienza industriale va affrontata con la costruzione di un ecosistema nazionale per la logistica aumentata, facendo leva su automazione. Servizi C-ITS e CCAM, connettività e nuove competenze, affinché la logistica diventi una leva attiva di politica economica. Anticipare inoltre l'attuazione del regolamento europeo n. 2020/1056 (regolamento eFTI), dotando il Paese di un'infrastruttura digitale interoperabile, capace di integrare porti, ferrovie e logistica terrestre nel mercato unico europeo

R7 – Ecosistema digitale per il trasporto multimodale ed intermodale

Tale proposta, rafforzata alla luce del contesto europeo, mira a promuovere un ecosistema digitale per il trasporto intermodale ed intermodale. L'obiettivo è di ottimizzare l'uso delle infrastrutture stradali esistenti e ridurre la congestione attraverso la continuità dei servizi ITS per gli utenti relativi a viaggi, trasporti e la gestione del traffico per sostenere la multimodalità, l'integrazione dei modi di trasporto e l'agevolazione del trasferimento modale sulla rete di trasporto nazionale, garantendone la sicurezza nell'utilizzo di tali servizi e dei dati personali degli utenti e dei sistemi coinvolti sia per le persone che per la logistica del trasporto merci

R8 – Sviluppo della mobilità connessa ed autonoma

Risulta ormai fondamentale la creazione di un ecosistema C-ITS che permetta la cooperazione tra veicoli, infrastrutture e altri utenti della strada attraverso lo scambio sicuro di dati in tempo reale. Occorre una rivisitazione delle specifiche tecniche per lo sviluppo e l'attuazione di sistemi di trasporto intelligenti e cooperativi, in particolare per sostenere la CCAM. Le tecnologie sono mature e la riforma del codice della strada è ormai un passo necessario per adeguare la normativa nazionali a queste nuove forme di mobilità ma occorre farlo in sicurezza, ma al contempo in maniera rapida per non essere tagliati fuori da un mercato in continua evoluzione.

R9 – Investire su competenze, collaborazione, ambienti di sperimentazione controllata e team multi-genere e multidisciplinari

La complessità della convergenza tra ITS, AI e cybersecurity richiede competenze multidisciplinari e una collaborazione strutturata tra Pubbliche Amministrazioni, gestori, industria, mondo della ricerca ed università con un focus specifico sulla creazione di profili professionali ibridi, capaci di coniugare l'esperienza nel dominio dei trasporti con le competenze in ambito AI e Cybersecurity. È raccomandabile promuovere programmi di formazione continua, iniziative di condivisione delle conoscenze e l'uso di ambienti di simulazione e digital twin per testare soluzioni, scenari di rischio e modelli di governance prima della loro adozione su larga scala.

Inoltre si raccomanda di promuovere team multi-genere e multidisciplinari, favorendo la presenza femminile nella AI & cybersecurity nella mobilità nonché l'integrazione tra competenze STEM, umanistiche, giuridiche, organizzative, comunicative e di dominio. Tali tematiche non possono essere infatti affrontate solo come tema tecnico in quanto richiedono competenze diverse e complementari. La costituzione di team misti per genere e competenze può migliorare la qualità dell'analisi, ampliare le prospettive decisionali e favorire soluzioni più adatte a sistemi complessi,

nei quali sicurezza digitale, sicurezza fisica, continuità operativa, privacy, esperienza utente e fiducia pubblica sono strettamente connesse.

R10 – Integrare l'etica fin dalla progettazione (Ethics-by-Design)

Per garantire che i principi etici non siano un'aggiunta a posteriori, è necessario rendere obbligatorie valutazioni di impatto etico e algoritmico (AIA) per i nuovi sistemi di AI critici nel settore dei trasporti. Questo assicurerà che principi fondamentali come l'equità, la trasparenza, la privacy e il controllo umano siano integrati fin dalle prime fasi del ciclo di vita tecnologico.

R11 - Garantire un Controllo Umano Significativo e una chiara responsabilità

I requisiti di human oversight previsti dall'AI Act devono essere tradotti in standard tecnici e organizzativi chiari e applicabili. È essenziale definire catene di responsabilità inequivocabili che prevengano il fenomeno della "moral crumple zone", assicurando che la decisione finale in contesti critici rimanga sempre attribuibile a un essere umano e che quest'ultimo disponga degli strumenti per esercitare un controllo reale ed efficace.

R12 - Riforma del Processo di Omologazione

Tale riforma dovrebbe avere, sotto l'egida del Ministero delle Infrastrutture e delle Autorità Regolatrici, l'obiettivo di chiudere i "legal loopholes" attuali, nel senso che ogni aggiornamento Over-the-Air (OTA) critico o sostituzione di componenti hardware (chip) dovrebbe essere attuato in maniera da prevenire l'attivazione di backdoor silenti o vulnerabilità post-vendita.

R13 - Istituzione di SOC di Settore Potenziati dall'AI, con architetture Zero Trust e da piattaforme di Cyber Threat Intelligence con soluzioni tali da garantire la riservatezza dei dati

In linea con gli strumenti di attuazione della nuova Direttiva 2661/2023 e suo Decreto di recepimento, SOC di Settore Potenziati dall'AI, gestiti dagli Operatori di infrastrutture e Gestori di flotta in Partnership Strategica con ACN, dovrebbero avere l'obiettivo di implementare architetture Zero Trust che utilizzino l'IA per il rilevamento tempestivo di anomalie comportamentali, superando la difesa perimetrale statica.

Al contempo, essi dovrebbero essere potenziati da piattaforme di Cyber Threat Intelligence, intese come tecnologie per raccogliere, correlare, validare e contestualizzare informazioni sulle minacce cyber, a supporto di una postura orientata all'anticipazione degli scenari di rischio e complementari alle tecnologie di AI Security ma distinte da esse, capaci di rafforzare i e i processi di gestione del rischio.

Dovrebbe infine essere riservata attenzione a soluzioni tali da garantire la riservatezza dei dati, che puntino quindi su sviluppi integralmente certificati e non basate su prodotti le cui interazioni non siano tracciate.

R14 - Cultura diffusa della cybersicurezza negli ITS

In partnership fra MIT, Agenzia per la Cybersicurezza Nazionale e TTS Italia e la Piattaforma Enti Locali, si dovrebbe alimentare una cultura diffusa della cybersicurezza nelle Amministrazioni, nelle imprese per diffondere ed armonizzare gli standard ITS a livello nazionale, evitando la frammentazione tecnologica che espone i comuni più piccoli a rischi cyber sproporzionati, nonché con iniziative in grado di sensibilizzare anche i cittadini-utenti, trasformandoli da "anelli deboli" a sensori attivi di resilienza.

Inoltre va favorita la crescita delle competenze integrate ITS, AI e Cybersecurity sia a livello universitario che con formazione continua nelle imprese e nelle Amministrazioni, al fine di poter seguire a tutti i livelli le evoluzioni tecnologiche del settore.

R15 - Incentivazioni economiche

Il rispetto delle precedenti raccomandazioni relative all'adozione dell'AI e della Cybersecurity nel settore della mobilità comporterà costi di investimento, di gestione e di aggiornamento nonché rischi percepiti elevati. Senza strumenti economici adeguati, imprese e PA effettueranno investimenti limitati ed avranno un ritardo strutturale continuo che potrà mettere a rischio il sistema ed il governo della mobilità di persone e merci sia a livello locale che nazionale. All'interno del quadro normativo, andrà quindi individuata una chiara scala temporale di realizzazione dei singoli interventi prioritari, misurati con KPI predeterminati in grado di garantire la funzionalità e lo sviluppo del sistema di mobilità nel prossimo futuro ed a medio termine. Potrà anche essere individuato un mix di misure quali crediti fiscali per investimenti in soluzioni AI/cybersecurity degli interventi, fondi dedicati in termini di programmi di finanziamento per progetti innovativi della PA e di imprese innovative come anche la promozione di appalti innovativi, che valorizzino soluzioni tecnologiche avanzate.

6.2 Conclusioni

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.

La mobilità del futuro sarà quindi caratterizzata da sistemi altamente connessi, autonomi e intelligenti. ITS, AI e cybersecurity costituiscono un ecosistema indivisibile, dove:

- I dati diventano un asset strategico;
- La sicurezza informatica è un prerequisito fondamentale;
- Le città e i veicoli diventano sempre più digitali, efficienti e predittivi;
- Lo sviluppo di una mobilità moderna e resiliente richiede investimenti tecnologici, competenze specializzate e standard condivisi.

L'integrazione di AI e cybersecurity è il fattore critico per garantire sicurezza, affidabilità e resilienza nella mobilità intelligente.

L'integrazione tra ITS, AI e cybersecurity non è più una visione futuristica ma una realtà in rapida espansione in Europa e in Italia ed abilita un ecosistema di mobilità intelligente, predittivo e resiliente, capace di affrontare le sfide della crescente domanda di trasporto, della sicurezza stradale e della sostenibilità energetica. Le infrastrutture diventeranno piattaforme digitali, i veicoli nodi intelligenti e la gestione del traffico un processo autonomo e data-driven. Le dimensioni di mercato, le iniziative urbane, i progetti pilota e i trend tecnologici confermano che stiamo entrando in una nuova era della mobilità:

- Più connessa (veicoli + infrastrutture);
- Più intelligente (AI per prevedere e ottimizzare);
- Più sicura (protezione dai rischi cyber);
- Più sostenibile (elettrificazione + smart charging).

Per cogliere appieno queste opportunità serve una strategia integrata, con attori pubblici e privati che lavorano insieme su standard, investimenti e innovazione.

Infine, l'inserimento della Direttiva UE 2023/2661 ormai in recepimento rafforza la visione strategica: non si tratta solo di tecnologia, ma di un quadro normativo che abilita la mobilità del futuro basata su dati, interoperabilità e sicurezza.

- Integrare le sue disposizioni tecniche significa;
- Progettare sistemi ITS e infrastrutture dati coerenti con gli obblighi di condivisione;
- Sviluppare un'AI avanzata alimentata da dati standardizzati;
- Garantire un approccio solido alla cybersecurity per proteggere i dati ITS critici.

In generale, le regole non sono solo burocrazia: stanno ponendo le fondamenta tecniche e organizzative indispensabili per costruire una mobilità connessa che sia affidabile e sicura per tutti. Nell'era della mobilità connessa, la cybersecurity non è più un optional o un costo aggiuntivo, ma un requisito strutturale e imprescindibile. Non si tratta solo di proteggere la privacy degli utenti o di prevenire frodi, ma di garantire l'incolumità fisica delle persone. Ogni componente di questo ecosistema, dal singolo sensore alla piattaforma cloud, deve essere progettato, gestito e monitorato con la sicurezza come priorità assoluta.

Poiché gli attacchi sono inevitabili, l'obiettivo finale guidato dalla regolamentazione e dalla responsabilità condivisa non è solo la prevenzione, ma la costruzione di un ecosistema resiliente, in grado di resistere e riprendersi dagli incidenti informatici garantendo al contempo l'affidabilità operativa e la sicurezza fisica degli utenti. Solo così sarà possibile abilitare un futuro della mobilità che sia innovativo, sostenibile e, soprattutto, sicuro.

Risulta quindi importante avere una visione di lungo periodo che guardi ai servizi digitali in una logica strategica per lo sviluppo dell'innovazione e degli investimenti necessari in un contesto mondiale in grande evoluzione in una dimensione almeno europea, che riguardi la gestione/protezione dei dati, la cybersecurity e la resilienza delle infrastrutture

In questa visione strategica ed europea dovrebbero rientrare le normative e i finanziamenti nazionali per le tecnologie e le infrastrutture, ove sembra opportuno focalizzarsi anche sui veicoli del futuro sulla guida autonoma, ambiti in cui la cybersecurity è prioritaria. Occorrerà che a tali sviluppi si leghi anche il tema delle competenze per creare profili adeguati ad affrontare le sfide integrate sopra definite.

In sintesi, un approccio olistico — che unisca tecnologie avanzate, processi robusti, architetture scalabili, compliance normativa e formazione di base e continua — che renderà possibile abilitare il futuro della mobilità autonoma, connessa, elettrica e condivisa in modo sicuro e posizionare Enti, Amministrazioni ed imprese quali attori di riferimento nella mobilità digitale europea.

.

7. Crediti

Il presente documento è stato curato da:

- Ing. Fabio Nussio, Senior Expert TTS Italia e Responsabile del Gruppo di Lavoro AI & Cybersecurity per il trasporto di persone e merci;
- Ing. Leonardo Domanico, Responsabile dei rapporti con gli associati di TTS Italia.

Con il contributo degli associati TTS Italia e delle seguenti Associazioni di Settore: AGENS, AISCAT, ANITA, ANFIA, Cluster Trasporti, Club Italia, Freight Leaders Council, OITAF, PIARC e Women4Cyber.

Lo sviluppo del Gruppo di Lavoro ha previsto un coinvolgimento maggiore per un ristretto Core-team che hanno supportato ciascuna fase di sviluppo del presente documento, composto dai seguenti Associati: Almaviva, Aesys, CinqueT, IBM, Leonardo, Mia-Platform, OpenMove e Swarco Italia.

Specifico ringraziamento è poi rivolto all'Ing Daniele Arangio Mazza di IBM quale coordinatore del cap. 4 ed all'Ing. Valentina Tempera di Mia-Platform quale coordinatrice del cap. 5.

Allegato 1 – Principali link di riferimento e di approfondimento

Generali

- Intelligent Transport Systems in the EU: https://cinea.ec.europa.eu/programmes/connecting-europe-facility/transport-infrastructure/intelligent-transport-systems-eu_en
- ITS & ISO: https://www.iso.org/transport/its-intelligent-transportation-systems
- Intelligent Transport Systems (ITS) for Sustainable Mobility: https://unece.org/transport/publications/intelligent-transport-systems-its-sustainable-mobility-second-edition-part
- ITS Directive and Action Plan - Mobility and Transport: https://transport.ec.europa.eu/transport-themes/smart-mobility/road/its-directive-and-action-plan_en
- Sistemi di Trasporto Intelligenti (ITS): https://www.mit.gov.it/documentazione/i-sistemi-di-trasporto-intelligenti-its
- CLUSIT – Rapporto 2026 sulla Cybersecurity. https://clusit.it/rapporto-clusit/.
- MITRE ATLAS (Adversarial Threat Landscape for Artificial Intelligence Systems), MITRE Corporation: www.atlas.mitre.org
- Network and Information Systems (NIS) Cooperation Group: https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group
- OWASP Foundation - organizzazione internazionale no-profit di riferimento per la sicurezza applicativa: https://owasp.org/
- Quadro regolatorio UE sull'AI: https://digital-strategy.ec.europa.eu/it/policies/regulatory-framework-ai
- "Strategia Nazionale di Cybersicurezza 2022-26" - ACN: https://www.acn.gov.it/portale/strategia-nazionale-di-cybersicurezza
- Zero Trust Cybersecurity: 'Never Trust, Always Verify': https://csrc.nist.gov/publications/detail/sp/800-207/final
- Zero Trust Maturity Model Version 2.0: https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf
- Zero Trust for Operational Technology Activities and Outcomes: (https://dodcio.defense.gov/Portals/0/Documents/Library/ZT-OperationalTechnologyActivitiesOutcomes.pdf)

Etica e Digital Divide

- https://www.orizzontescuola.it/intelligenza-artificiale-e-mercato-del-lavoro-italiano-105-milioni-di-occupati-rischiano-lautomazione/
- https://www.uominietrasporti.it/centonumeri/flussi-in-movimento/1-ogni-5-annunci-e-la-domanda-di-lavoro-espressa-dalla-logistica-in-italia-spesso-rimasta-senza-risposta/
- https://www.corrierecomunicazioni.it/digital-economy/competenze-digitali-nel-2026-in-italia-gap-di-2-milioni-di-lavoratori/.
- https://www.allianz.com/en/mediacenter/news/media-releases/251028-allianz-motor-day-2025.html
- https://www.istat.it/comunicato-stampa/imprese-e-ict-anno-2024/

- https://cordis.europa.eu/article/id/434335-how-do-europeans-feel-about-self-driving-cars/it

Blockchain/DLT

MOBI — Mobility Open Blockchain Initiative

- Sito ufficiale: https://dlt.mobi/
- Scheda INATBA: https://inatba.org/mobility-open-blockchain-initiative/
- Paper accademico (ResearchGate): https://www.researchgate.net/publication/350080152_The_Mobility_Open_Blockchain_Initiative_Identity_Members_Technologies_and_Future_Trends

IOTA — DLT per veicoli connessi e V2X

- Mobility use case: https://www.linkedin.com/pulse/iota-new-mobility-glance-opportunities-alexander-renz-1
- Partnership Jaguar Land Rover: https://blog.iota.org/earn-as-you-drive-with-jaguar-land-rover-and-iota-3c744d8c0cba/
- Connected car apps: https://blog.iota.org/develop-connected-car-apps-using-high-mobility-and-iota-14d663c860b7/

IBM Food Trust — Blockchain per catena del freddo logistica

- Sito ufficiale: https://www.ibm.com/products/supply-chain-intelligence-suite/food-trust
- Pagina blockchain solutions: https://www.ibm.com/blockchain/solutions/food-trust
- Partnership iFoodDS: https://www.ibm.com/case-studies/blog/ifoodds-and-ibm-forge-new-path-to-food-safety-with-ibm-food-trust

TradeLens — Blockchain per logistica marittima (Maersk + IBM)

- Annuncio lancio (PR Newswire): https://www.prnewswire.com/news-releases/maersk-and-ibm-introduce-tradelens-blockchain-shipping-solution-300694642.html
- Comunicato chiusura (Maersk): https://www.maersk.com/news/articles/2022/11/29/maersk-and-ibm-to-discontinue-tradelens
- Analisi tecnica (PixelPlex): https://pixelplex.io/blog/maersk-ibm-tradelens-blockchain-supply-management/
- Post-mortem (Port de Barcelona): https://piernext.portdebarcelona.cat/en/technology/the-closure-of-tradelens/

Cybersecurity e casi di studio

NotPetya / Maersk (2017)

- Case study Columbia SIPA: https://www.sipa.columbia.edu/sipa-education/picker-center-executive-education/case-collection/notpetya-cyber-attack
- Case study MIT: https://cyberir.mit.edu/?p=2404

- Paper accademico (ResearchGate): https://www.researchgate.net/publication/346080185_The_Context_and_Impact_of_Maerk's_NotPetya_cyber_attack
- Rebuilding after NotPetya (CSO Online): https://www.csoonline.com/article/567845/rebuilding-after-notpetya-how-maersk-moved-forward.html
- Key learnings (LRQA): https://www.lrqa.com/en/insights/articles/notpetya-ransomware-attack-on-maersk-key-learnings/
- SOS Intelligence case study: https://sosintel.co.uk/case-study-maersks-response-to-notpetya-how-cybersecurity-best-practices-mitigated-a-major-cyberattack/
- Wikipedia: https://en.wikipedia.org/wiki/2017_Ukraine_ransomware_attacks

Bosch VSOC — Vehicle Security Operations Center

- Bosch Engineering (sito ufficiale): https://www.bosch-engineering.com/services/engineering-services/cybersecurity/
- Upstream vSOC platform: https://upstream.auto/solutions/vehicle-security-operations-center/
- Kaspersky — Why VSOCs: https://www.kaspersky.com/blog/secure-futures-magazine/vehicle-security-operations-center/36596/
- VSOC in CCAM (Zenodo paper): https://zenodo.org/records/14044633
- Inside the vSOC ECU to Cloud: https://multicorewareinc.com/inside-the-vsoc-securing-the-software-defined-vehicle-from-ecu-to-cloud/

AI spiegabile e adversarial attacks

AIthena — Progetto EU CCAM su Trustworthy AI

- Sito ufficiale: https://aithena.eu/
- Scheda CORDIS: https://cordis.europa.eu/project/id/101076754
- Risultati (CORDIS): https://cordis.europa.eu/article/id/457142-self-driving-technologies-need-user-friendly-ai
- Pagina CCAM Association: https://www.ccam.eu/projects/aithena/
- IRU (partner): https://www.iru.org/what-we-do/being-trusted-voice-mobility-and-logistics/eu-research-innovation-projects/aithena

Adversarial attacks su segnali stradali (Berkeley)

- Blog BAIR (Berkeley AI Research): https://bair.berkeley.edu/blog/2017/12/30/yolo-attack/
- Paper CVPR 2018 (Eykholt et al.): https://arxiv.org/pdf/1707.08945
- Survey adversarial attacks su AV (Springer): https://link.springer.com/article/10.1007/s10462-024-11014-8

Allegato 2 – Acronimi

ACN	Agenzia per la Cybersicurezza Nazionale
AI	Artificial Intelligence
AIA	Algorithmic Impact Assessments
AIR	Automated Incident Response
API	Application Programming Interface
BEV	Battery Electric Vehicle
C-ITS	Connected-ITS
CAGR	Compound Annual Growth Rate
CAV	Connected and Automated Vehicles
CCAM	mobilità connessa, cooperativa e autonoma
CEF	Connecting Europe Facility
CIO	Chief Information Officer
CNSA 2.0	Cryptographic National Security Algorithm Suite 2.0
CRA	Cyber Resilience Act
CRQC	computer quantistici crittograficamente rilevanti
CSIRT	Computer Security Incident Response Team
CSMS	Cyber Security Management System
CTI	Cyber Threat Intelligence
DDoS	Distribuited Denial of Service
DoD	Department of Defense
ECCC	European Cybersecurity Competence Centre
EDPS	European Data Protection Supervisor
EMDS	Spazio Comune Europeo dei Dati sulla Mobilità
ENISA	European Union Agency for Cybersecurity
ESG	Environmental, Social, and Governance
EUCC	European Common Criteria
FRMCS	Future Railway Mobile Communication System
GDPR	General Data Protection Regulation
HNDL	Harvest Now, Decrypt Later
HQC	Hamming Quasi-Cyclic
IDS	Intrusion Detection Systems
IoV	Internet of Vehicles
ITS	Intelligence Transport Systems
LLM	Large Language Models
MaaS	Mobility as a Service

MIT	Ministero delle Infrastrutture e dei Trasporti
ML	Machine Learning
ML-DSA	Module-Lattice-Based Digital Signature Algorithm
MLWE	Module Learning With Errors
NAP	National Access Points
NHTSA	National Highway Traffic Safety Administration
NIST	National Institute of Standards and Technology
OBU	On-Board Units
OSINT	Open Source INTelligence
OT	Operational Tecnology - uso di hardware e software per controllare i dispositivi industriali
PA	Pubblica Amministrazione
PKI	Public Key Infrastructure
PMI	Piccole e Medie Imprese
Pnrr	Piano Nazionale di Ripresa e Resilienza
RMM	Remote Monitoring and Management
RRI	Responsible Research and Innovation
RSU	Road-Side Units
SaaS	Software as a Service
SIEM	Security Information and Event Management
SLH-DSA	Stateless Hash-Based Digital Signature Algorithm
SOC	Security Operations Center
SSH	Social Sciences and Humanities
STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege
SUMS	Software Update Management System
TMC	Traffic Management Center
TPL	Trasporto Pubblico Locale
UE	Unione Europea
V2I	Vehicle-to-Infrastructure
V2X	Vehicle to Everything
VMS	Variable Message Sign
VRU	utenti vulnerabili della strada

Allegato 3 - Chi è TTS Italia

TTS Italia è **l'Associazione Nazionale della Telematica per i Trasporti e la Sicurezza** che rappresenta il settore italiano dei Sistemi Intelligenti di Trasporto (ITS), fondata nel 1999 da un gruppo di organizzazioni pubbliche e private attive sul tema, sull'esempio offerto da altre associazioni nazionali e internazionali.

Associazione no profit, TTS Italia riuniscw i principali stakeholder pubblici e privati del comparto nazionale, attualmente 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 degli ITS 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 degli ITS.

Gli ITS sono uno strumento fondamentale per la realizzazione della **smart mobility** e possono apportare benefici importanti sia per il settore pubblico, attraverso la riduzione delle esternalità, sia per il settore privato, con 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.

La **sfida** che l'Associazione si è posta fin dalla sua fondazione è di creare le condizioni normative e tecniche per la diffusione della smart mobility in Italia, obiettivo per il quale il settore pubblico è assolutamente fondamentale per creare le opportune condizioni di sviluppo.

L'Associazione è da sempre convinta che lo sviluppo diffuso degli ITS sul territorio nazionale debba passare attraverso il coinvolgimento degli Enti Locali che sono i principali attori per l'attuazione delle politiche di mobilità. A tale proposito, TTS Italia ha lanciato nel 2014 una **Piattaforma degli Enti Locali** con l'obiettivo primario di creare un tavolo tecnico di confronto sul tema degli ITS in un terreno neutro tra il mondo dell'offerta e quello della domanda rappresentato dagli Enti Locali. A dimostrazione dell'interesse dell'iniziativa, alla Piattaforma hanno aderito, a titolo gratuito, le principali città metropolitane nonché alcune delle regioni più attive ed è in continuo ampliamento.

TTS Italia nel corso della sua oramai ultra ventennale attività ha collaborato attivamente con le istituzioni, in particolare con il Ministero delle Infrastrutture e dei Trasporti (MIT), nella definizione delle principali normative che regolano tale settore in Italia. In particolare, TTS Italia ha supportato il MIT, come autorità nazionale, nel processo di elaborazione e recepimento della Direttiva 2010/40/UE, la cosiddetta Direttiva ITS che rappresenta il quadro normativo europeo del settore degli ITS. Successivamente, TTS Italia ha lavorato insieme al MIT per la redazione del Decreto ITS del 1° Febbraio 2013, nonché, su incarico del MIT, ha coordinato le attività che hanno portato alla definizione del **Piano d'Azione ITS Nazionale** adottato dal MIT stesso a Febbraio del 2014. TTS Italia ha supportato il MIT nella definizione del Decreto sulla Bigliettazione Elettronica del 27 Ottobre 2016, del Decreto sui Piani Urbani della Mobilità Sostenibile (PUMS) del 4 Agosto 2017 e del Decreto sulle Smart Road e la Guida Autonoma del 28 Febbraio 2018. Per ultimo, nel corso del 2025 ha supportato ancora il MIT per il recepimento della nuova Direttiva ITS 2661/2023/UE, avvenuto a inizio del 2026, che modifica la Direttiva 2010/40/UE.

Infine, TTS Italia fa anche parte di un **Network internazionale** costituito dalle Associazioni Nazionali per gli ITS presenti nelle più importanti Nazioni europee e mondiali e rappresenta il settore italiano degli ITS nei principali eventi internazionali.

Allegato 4 – Elenco Associati

Soci Fondatori

Soci Sostenitori

Soci Ordinari

• 4ICOM Italia • 5T • AEP Ticketing Solutions • Aesys • Anas • ANM – Agenzia Napoletana per la Mobilità • Autoroute • Autostrada Pedemontana Lombarda • Axis Communications • Berenice • BIP - Business Integration Partners • Bridge129 • Circle • Click&Find • CNR-ITAE • Concessioni Autostradali Venete – CAV • Conduent • Consorzio UnicoCampania • Cyclomedia • DataInfomobility • Digitalia • Divitech • Eltraff • Esri Italia • Famas System • FIT Consulting • GreenShare • HERE Italy • IBM Italia • IM Group • IMQ • Intellera Consulting • International Central Sat • Iveco • Kentkart • Kuba Italia • MacNil • Maggioli • MAIOR • Mia-Platform • Microrex • Mindicity/Gruppo TIM • Municipia • Octo Telematics • OpenMove • Pin Bike • PluService • Project Automation • PTV SISTeMA • PwC • QMap • Roma Servizi per la Mobilità • Safety21 • Selea • Servizi in Rete 2001 • Smart Parking Systems • Sodi Scientifica • Sprinx Technologies • T Bridge • Tattile • Tecsen - TEC Systems Engineering • Teltonika Italy • Thetis IT • Tiemme • Trafficlab • Traffic Technology • Turin Tech • Vifram • Yunex Traffic •

Amministrazioni Locali

• Comune di Rimini • Comune di Verona •

Università

• Politecnico di Bari – Dip. di Ingegneria Elettrica e dell'Informazione • Politecnico di Milano - Dip. Design, Laboratorio Mobilità e Trasporti • Politecnico di Torino - Dip. di Ingegneria dell'Ambiente, del Territorio e delle Infrastrutture • Università di Enna Kore – Facoltà di Ingegneria e Architettura • Università di Napoli "Federico II" - Dip. Ingegneria Civile Edile ed Ambientale (DICEA) • Università di Roma "La Sapienza" - Dip. Ingegneria Civile, Edile e Ambientale • Università di Roma "La Sapienza" - Dip. Statistiche • Università di Salerno - Dip. Ingegneria Industriale •

Partner Istituzionali

• Polizia di Stato •

Partnership

• Club Italia • Cluster Trasporti Italia 2020 • EIT Urban Mobility • FederDistribuzione • FLC - Freight Leaders Council • IRF Global - International Road Federation Global • Network of National ITS Associations • OITAF - Osservatorio Interdisciplinare Trasporto Alimenti e Farmaci • Open Logistics Foundation • Osservatorio Nazionale Sharing Mobility • PAVE Europe • PIARC – Associazione Mondiale della Strada, Comitato Nazionale Italiano • UNINFO •

Piattaforma Enti Locali

• Regione Emilia-Romagna • Regione Liguria • Regione Molise • Regione Piemonte • Regione Sardegna • Città Metropolitana di Cagliari • Città Metropolitana di Firenze • Città Metropolitana di Reggio Calabria • Città Metropolitana di Torino • Comune di Acquaviva delle Fonti • Comune di Ancona • Comune di Bari • Comune di Bologna • Comune di Capo d'Orlando • Comune di Cuneo • Comune di Genova • Comune di Gioia del Colle • Comune di L'Aquila • Comune di Lucca • Comune di Messina • Comune di Milano • Comune di Monza • Comune di Napoli • Comune di Palermo • Comune di Reggio Calabria • Comune di Rimini • Comune di Roma • Comune di Rutigliano • Comune di Torino • Comune di Verona •

TTS ITALIA

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

Con il supporto di

GOLDEN SPONSOR

SILVER SPONSOR