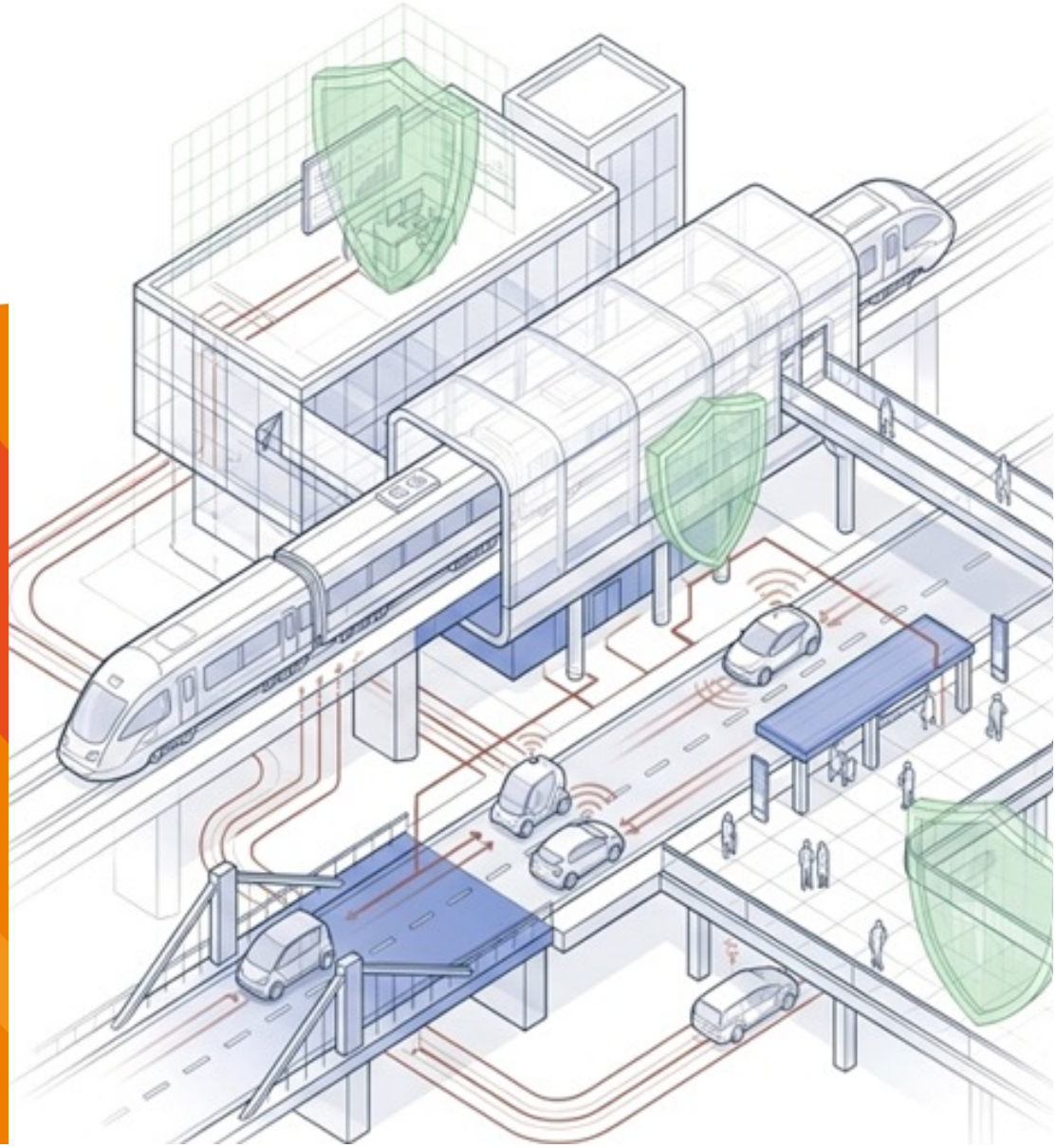
TTS ITALIA
Associazione Italiana della Telematica per i Trasporti e la Sicurezza

Position Paper

"AI & Cybersecurity per il trasporto di persone e merci"

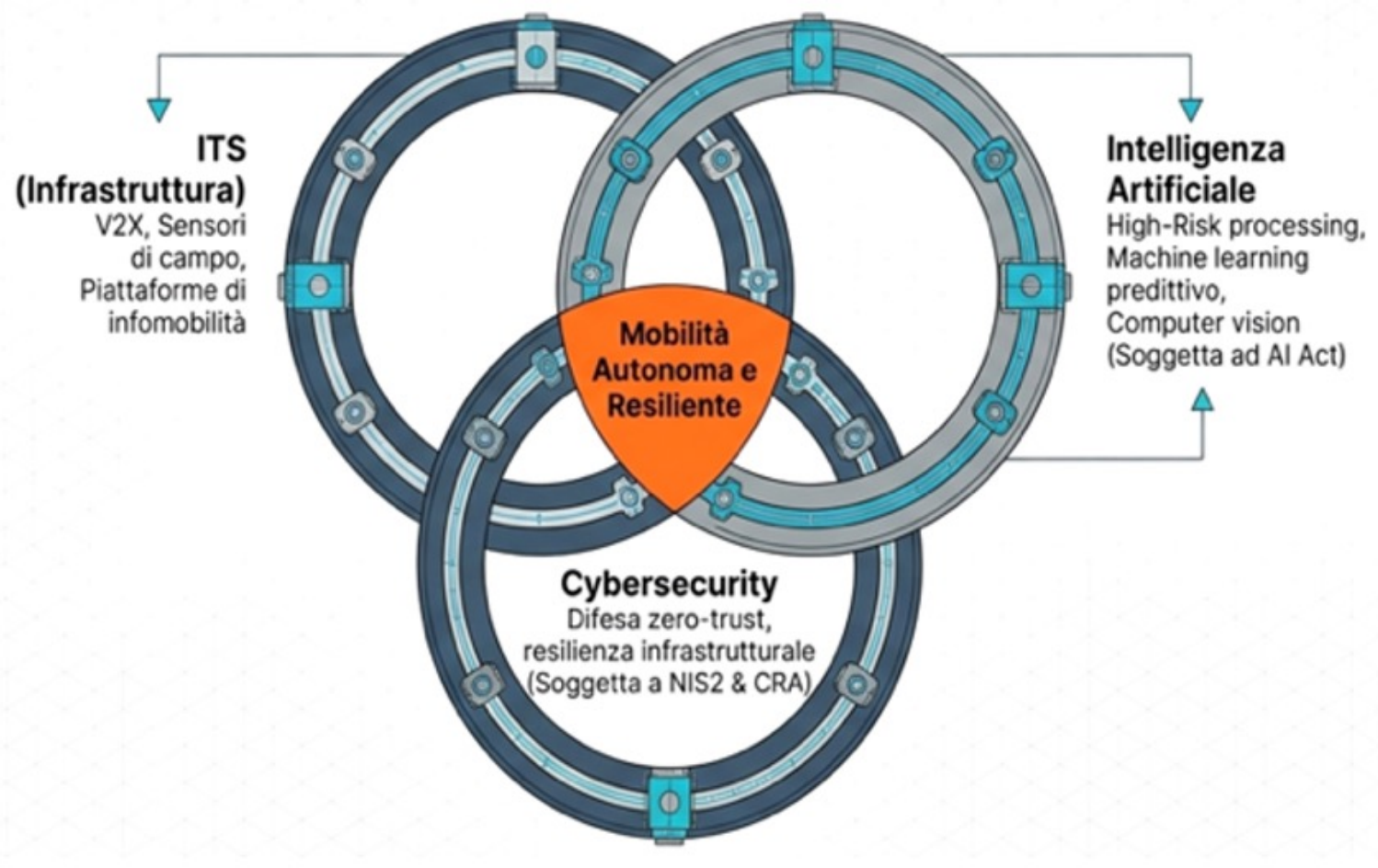
Il nuovo paradigma per una mobilità intelligente, resiliente e sicura

Fabio Nussio – Senior expert TTS Italia
Co-ordinatore GdL AI & Cybersecurity
Roma, 17 Giugno 2026



I tre pilastri

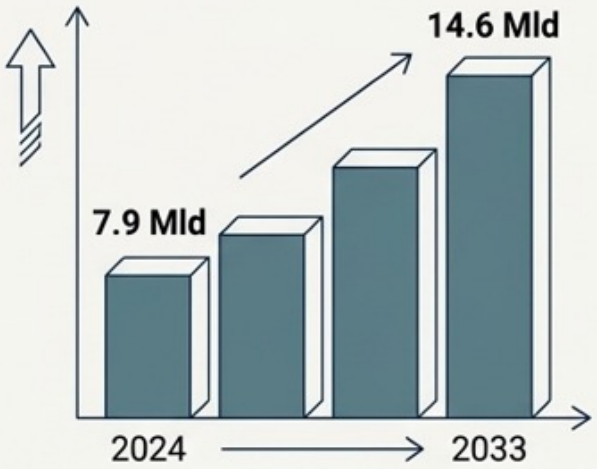
La mobilità non è più gestibile per compartimenti stagni. Solo l’integrazione nativa di questi tre pilastri garantisce la continuità operativa e la sicurezza fisica degli utenti.



IL VALORE STRATEGICO DELLA MOBILITÀ CONNESSA

L'intelligenza artificiale trasforma i trasporti da sistemi reattivi a infrastrutture predittive. L'investimento in Al non è solo una scelta tecnologica, ma un imperativo per la competitività economica e la sostenibilità ambientale dell'Italia e dell'Europa**.**

MERCATO IN CRESCITA

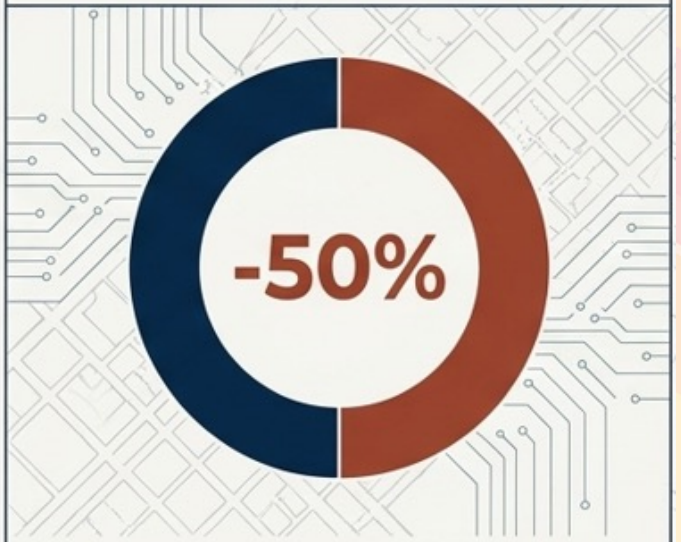


Mercato europeo ITS: da $7.9 Mld (2024) a $14.6 Mld (2033). In Italia, la smart mobility vale già **€2,9 Mld** (2023).

IMPATTO OPERATIVO

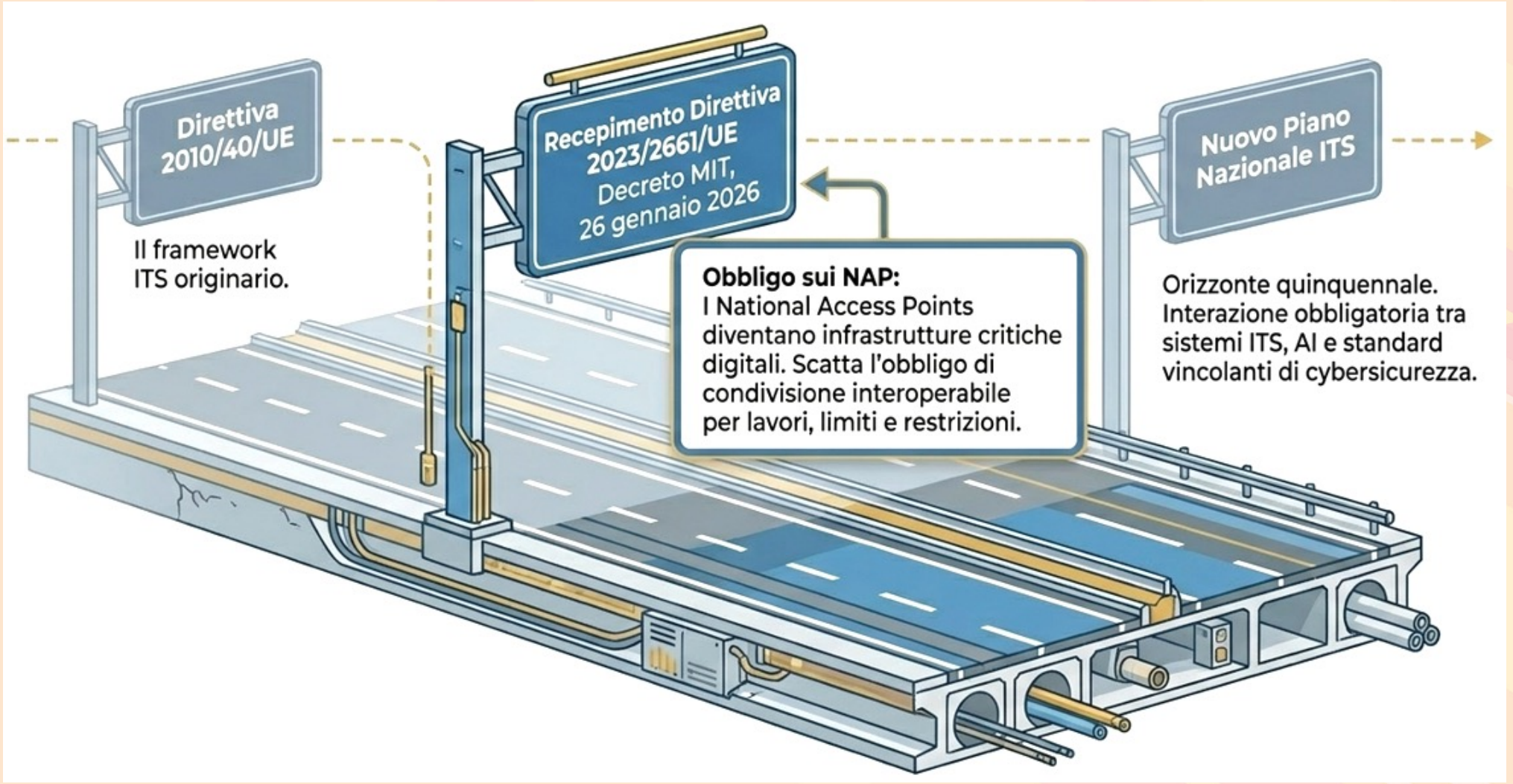
-60% ritardi per guasti grazie alla manutenzione predittiva guidata dall'Al (dati settore ferroviario).

SICUREZZA E AMBIENTE



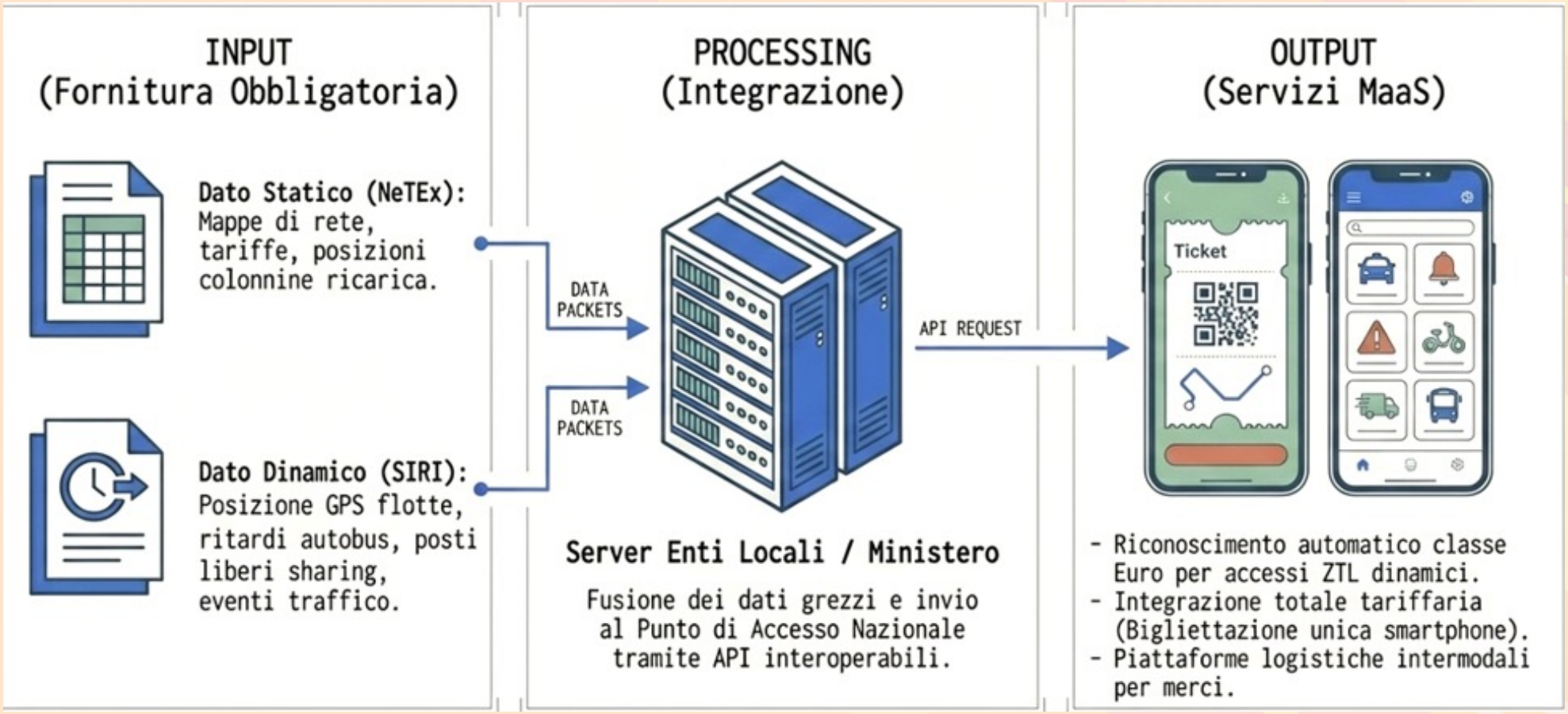
Prevenzione incidenti e ottimizzazione dinamica delle flotte (-50% costi di consegna con routing dinamico).

Il catalizzatore normativo: la direttiva ITS ed i Decreti di recepimento del MIT



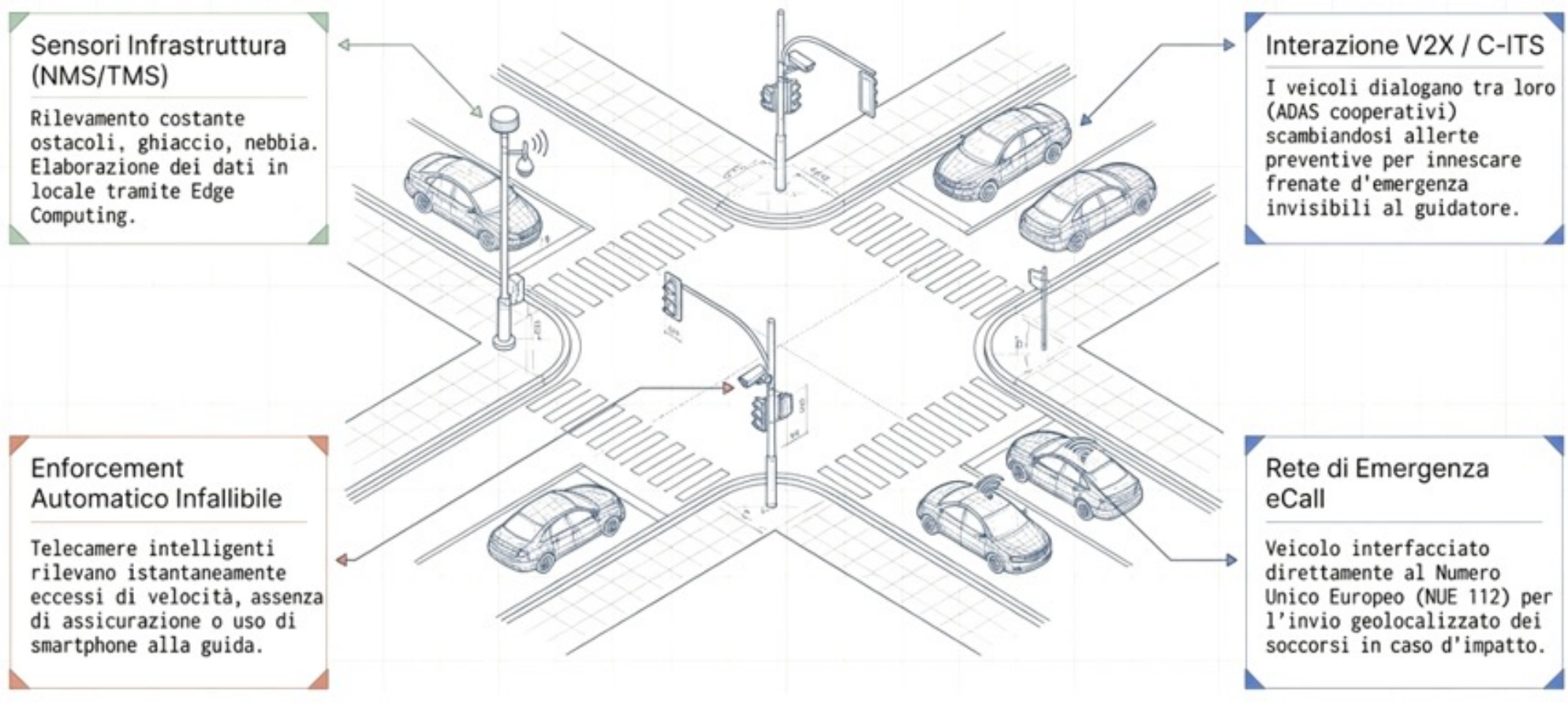
Il Decreto 40/2026 di recepimento del MIT. I 4 Settori di Azione Prioritari

Settori 1 &2: dal formato dati al servizio visibile al cittadino



Il Decreto 40/2026 di recepimento del MIT. I 4 Settori di Azione Prioritari

Settori 3 & 4: Il veicolo diventa un nodo della rete stradale



LA SUPERFICIE D'ATTACCO IN ESPANSIONE

L'iper-connettività dissolve i confini fisici. Ogni veicolo autonomo, colonnina di ricarica o sensore stradale è una potenziale porta d'ingresso. Il settore trasporti è oggi sotto un assedio digitale senza precedenti.

Gli attacchi cyber sono in continua crescita. A livello globale nel 2025 + 48,7% rispetto al 2024 (CLUSIT 2026).

In Italia, il settore Transportation/Storage è al **quarto posto con il 12% e + 134,6% degli incidenti** rispetto al 2024 (61 vs. 24).

Distribuited Denial of Service (DDoS) è la tecnica d'attacco preferita (38,5%) per semplicità, impatto mediatico (forma di "sit-in" digitale, seguita dal **malware** (23%)

Test di cyber-esercitazione a livello UE su risposta ad attacchi a reti ferroviarie e marittime

Giu 11, 2026

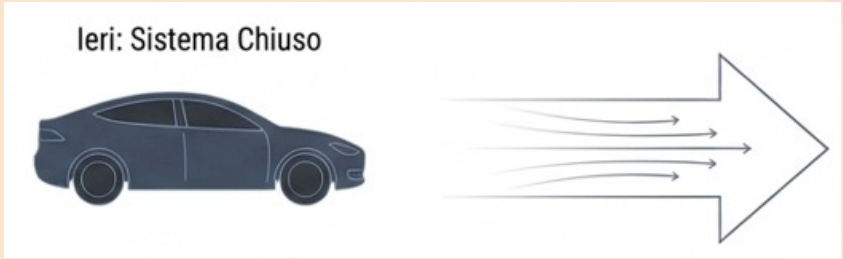
(FERPRESS) – Roma, 11 GIU – Circa 5 000 esperti hanno partecipato a un'esercitazione informatica a livello dell'UE il 10 e 11 giugno per verificare come l'Europa risponderebbe agli attacchi alle infrastrutture critiche di trasporto. Cyber Europe 2026 è stato anche il primo test a livello dell'UE del piano dell'UE per il ciberspazio 2025, che chiarisce ruoli e responsabilità in caso di crisi.

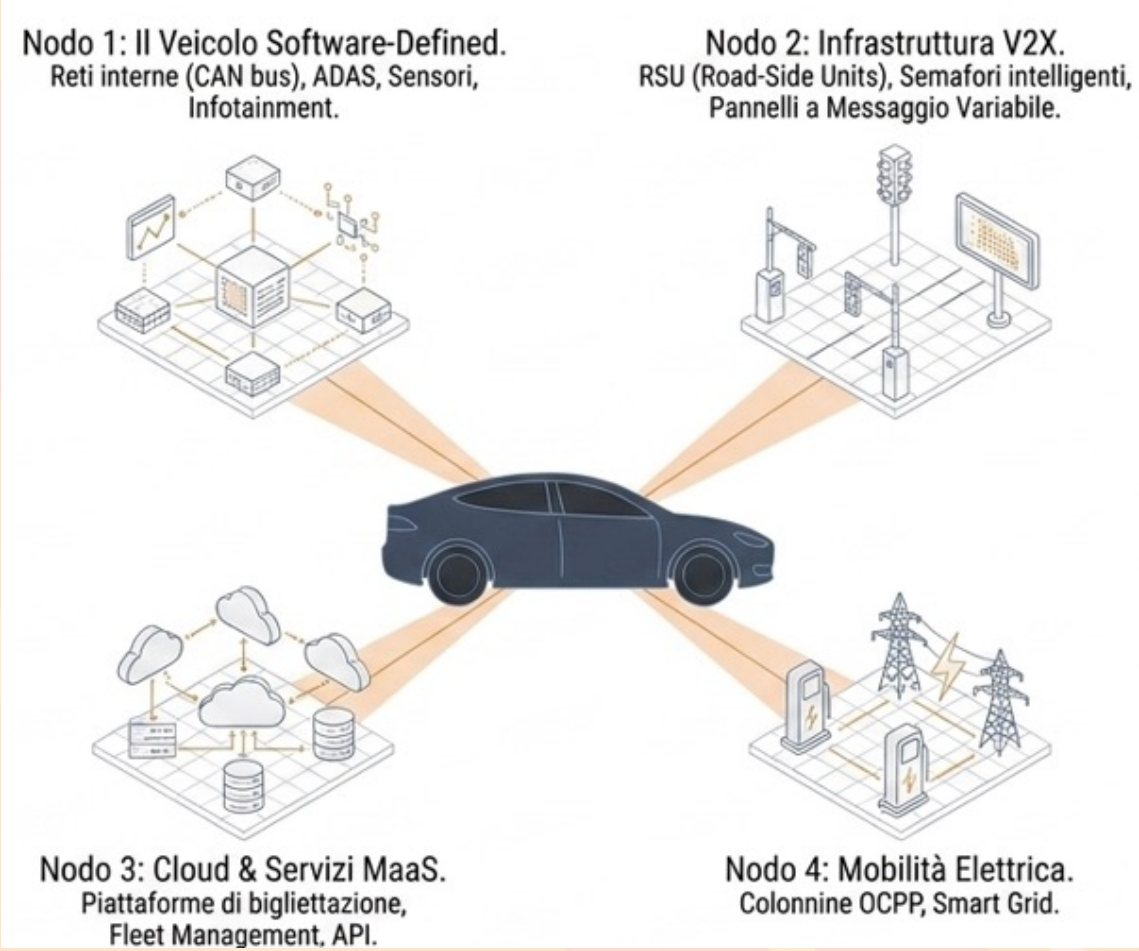
Organizzato dall'Agenzia dell'UE per la cibersicurezza (ENISA), l'esercitazione ha simulato un attacco informatico alle reti ferroviarie e marittime europee. Lo scenario ha causato gravi perturbazioni operative e si è trasformato in una vera e propria crisi di cibersicurezza. Tra i partecipanti figuravano specialisti della cibersicurezza del settore pubblico e privato, responsabili politici, istituzioni dell'UE, industria e paesi partner (Regno Unito, Norvegia, Svizzera e Ucraina).
Henna Virkkunen, Vicepresidente esecutiva per la Sovranità tecnologica, la sicurezza e la democrazia, ha dichiarato: "I trasporti sono essenziali per la nostra economia e la nostra vita quotidiana, ma sono anche un obiettivo per le minacce informatiche. Quando i porti o le ferrovie sono colpiti, gli effetti possono andare ben oltre i trasporti, perturbando il commercio, la mobilità militare e la risposta alle crisi. Poiché le minacce ibride sfumano il confine tra infrastrutture civili e militari, la preparazione non è facoltativa. Le minacce informatiche attraversano i confini in pochi secondi. L'Europa deve essere in grado di agire altrettanto rapidamente, insieme ai suoi partner più stretti."

L'esercitazione ha inoltre testato la riserva per la cibersicurezza, creata nell'ambito del regolamento sulla cibersolidarietà per sostenere le risposte agli incidenti di cibersicurezza. Gli insegnamenti tratti da Cyber Europe 2026 contribuiranno a consolidare il piano dell'UE per la cibersicurezza e a integrare la gestione delle crisi informatiche nei più ampi quadri di preparazione e risposta alle emergenze dell'Unione.

Il veicolo ieri ed oggi

Ogni nodo aggiunto per aumentare l’efficienza apre una **nuova potenziale porta d’ingresso**. Non proteggiamo più un involucro d’acciaio, ma un **ecosistema distribuito basato su API e dati in tempo reale**.



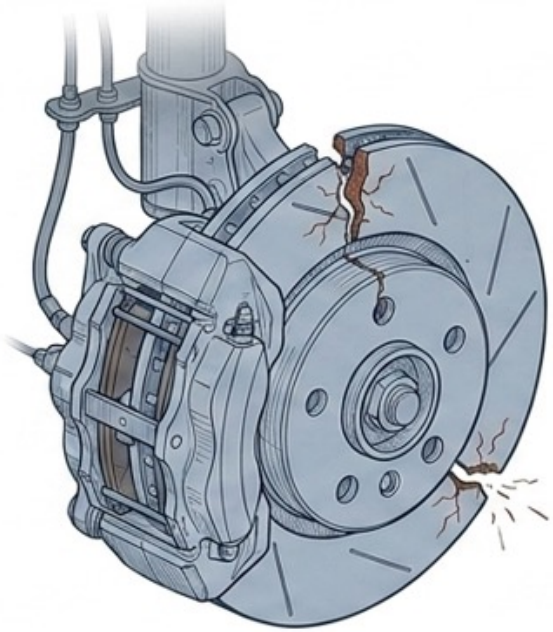


L'INTELLIGENZA ARTIFICIALE: UN'ARMA A DOPPIO TAGLIO

Le stesse tecnologie matematiche che rendono i veicoli intelligenti li espongono a forme di inganno cognitivo. Gli hacker non tagliano più i freni; convincono l'AI che la strada sia libera.

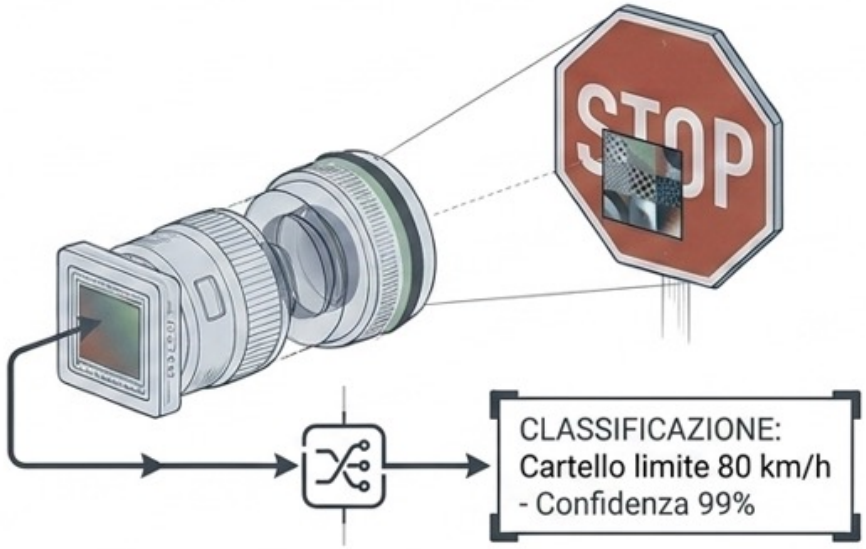
Ieri ed oggi

Ieri: La Rottura Fisica



Guasti meccanici o compromissione hardware diretta.
Determinabili, testabili, fisicamente evidenti.

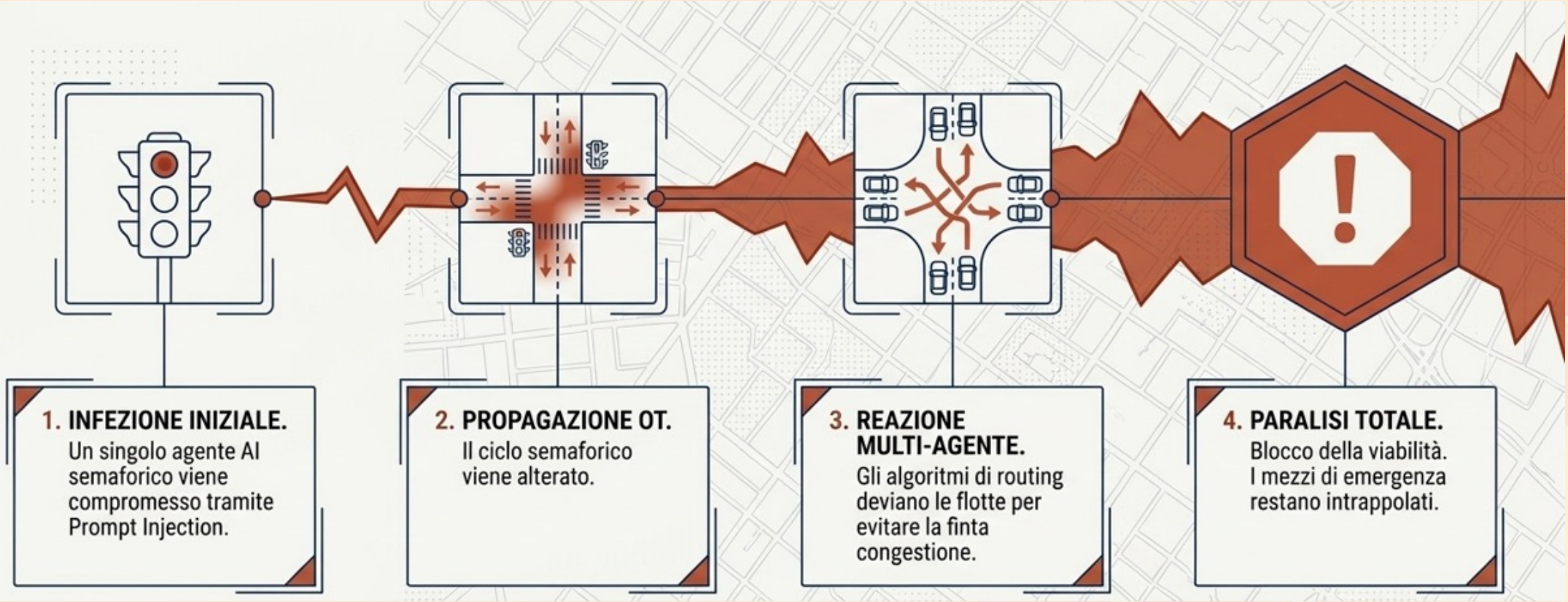
Oggi: L'Inganno Cognitivo (Adversarial Attack)



Perturbazioni invisibili all'occhio umano. Il sistema non è guasto, è stato indotto a prendere una decisione critica fatale manipolando la sua logica matematica di percezione.

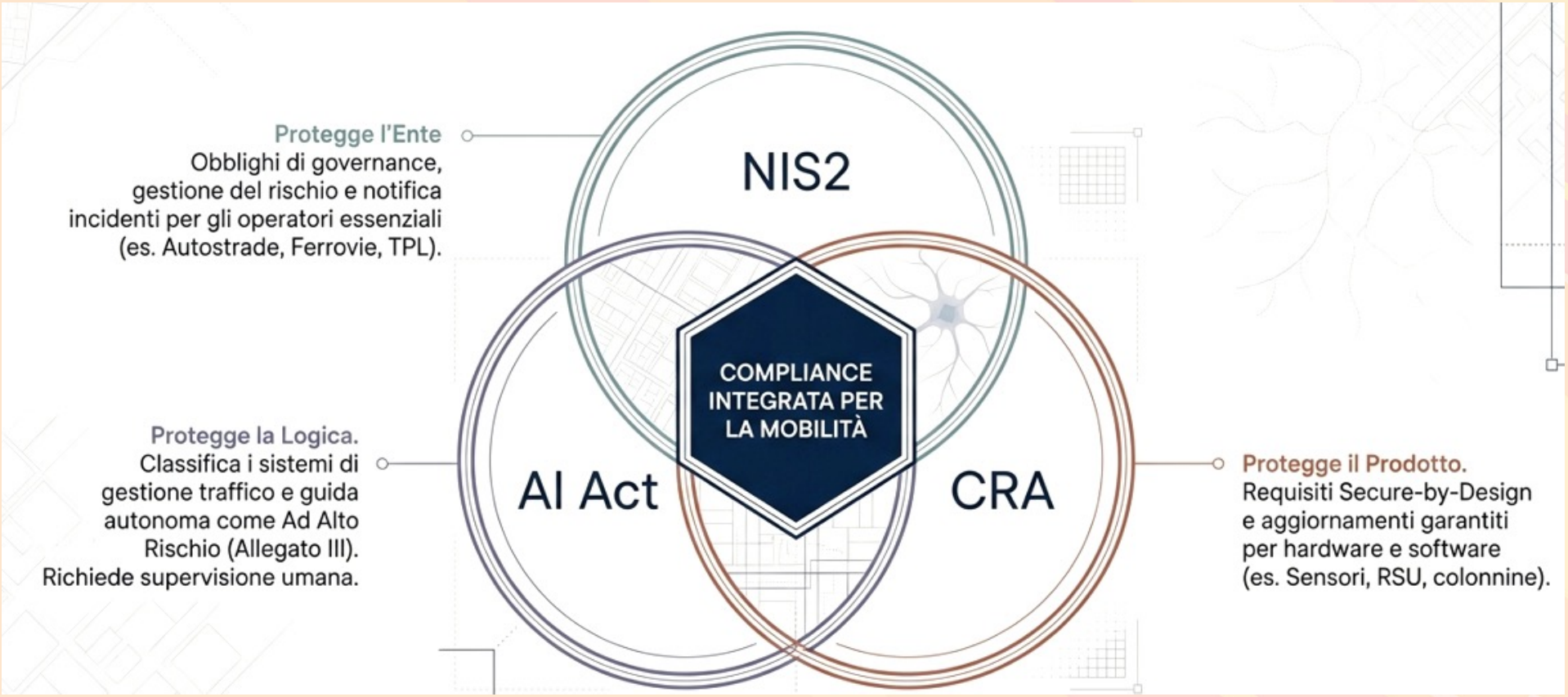
ANATOMIA DI UN FALLIMENTO A CASCATA (Cascading Failure)

Nei sistemi multi-agente, un errore locale si propaga e si amplifica. Il rischio non è più solo il furto di dati, ma la paralisi fisica delle infrastrutture critiche e il blocco dei servizi di emergenza.



LO SCUDO NORMATIVO EUROPEO

Le normative non sono silos isolati, ma pilastri interconnessi. L'Unione Europea ha creato un mercato unico digitale sicuro: conformarsi significa acquisire un vantaggio competitivo globale.



LA ROADMAP DELLA RESILIENZA

Trasformare l'adeguamento normativo da onere burocratico a proprietà intrinseca del sistema. Chi progetta oggi con sicurezza integrata dominerà il mercato di domani.

IL PARADIGMA COMPLIANCE BY DESIGN

Invece di rincorrere le singole scadenze, gli operatori devono **integrare i controlli di sicurezza** (**ISO 27001, IEC 62443**) direttamente **nell'architettura ingegneristica**.

L'ARCHITETTURA IMMUNITARIA: ZERO TRUST

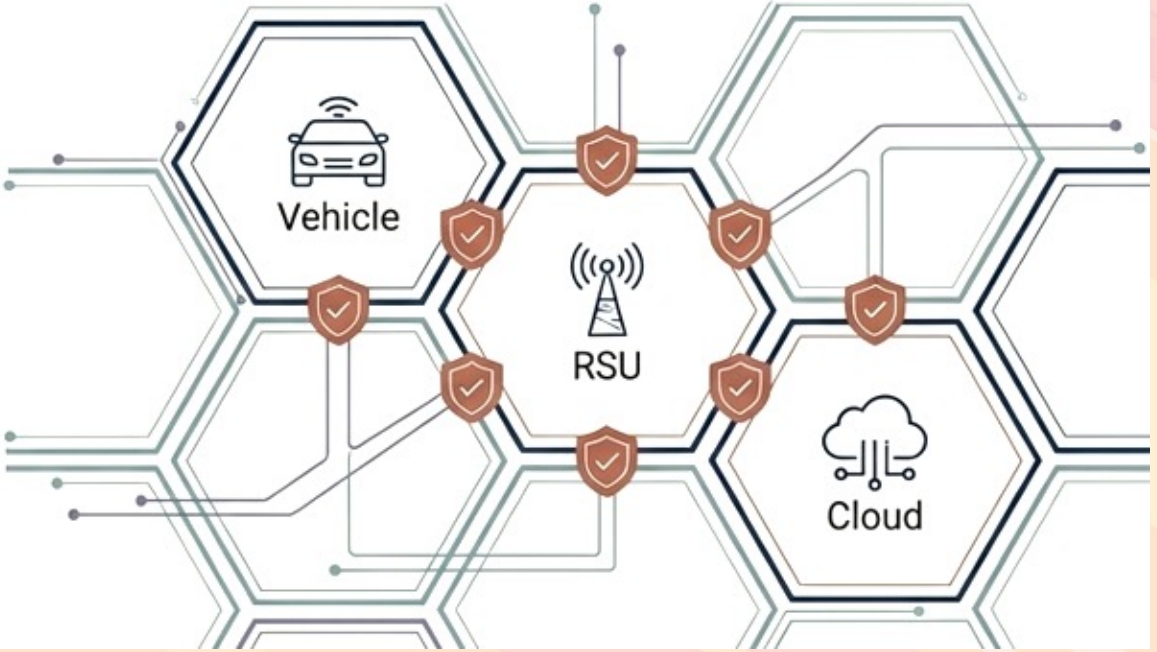
Nei trasporti connessi non esiste più un perimetro da difendere. Il nuovo paradigma è Zero Trust: nessun veicolo, sensore o utente è affidabile a priori. Ogni singola transazione dati viene autenticata, verificata e micro-segmentata.

IL PASSATO: CASTELLO E FOSSATO

Fiducia implicita all'interno della rete. Vulnerabile al movimento laterale se il perimetro viene bucato.

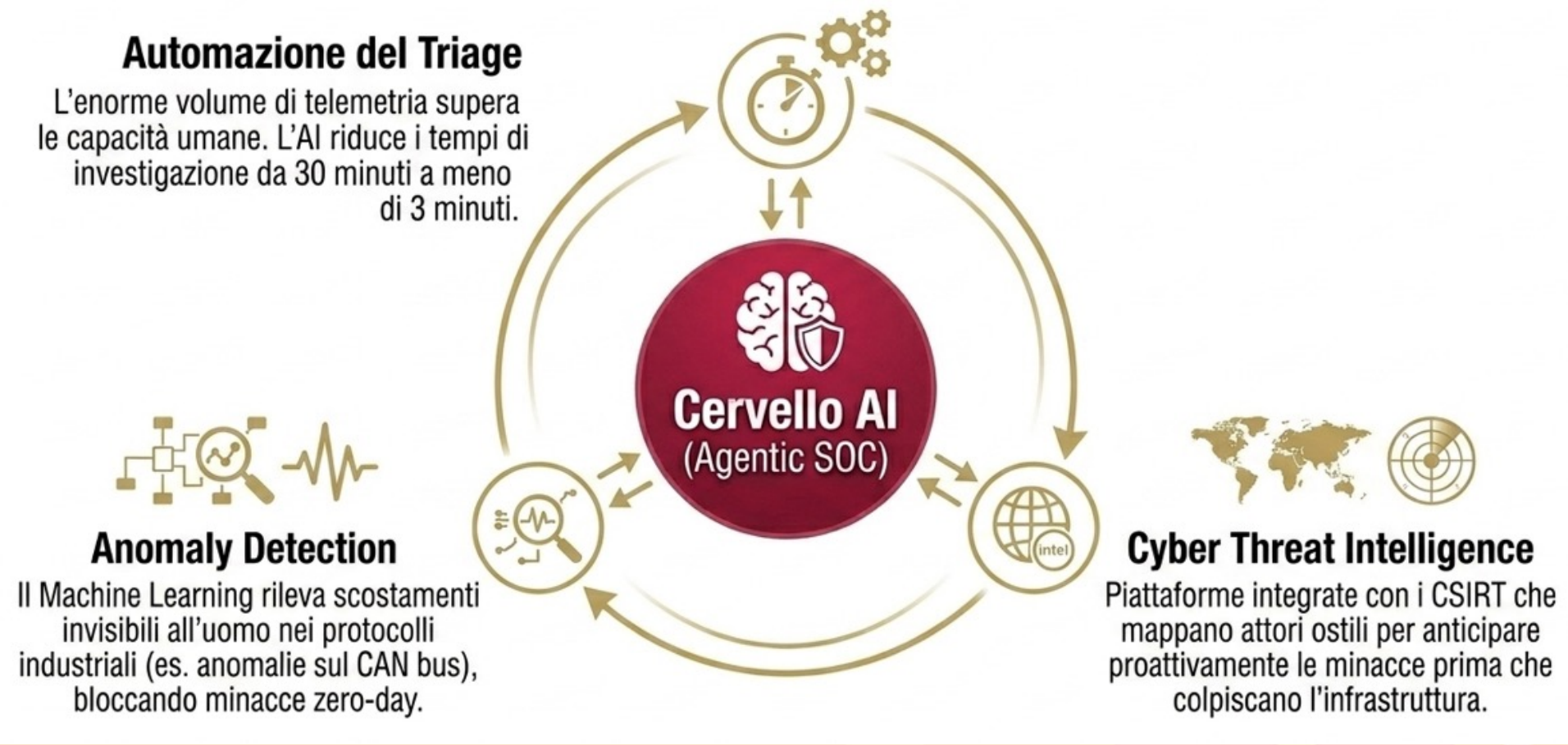
IL PRESENTE/FUTURO: ZERO TRUST & DEFENSE IN DEPTH (IEC 62443)

Micro-segmentazione e verifica continua su ogni singola connessione.



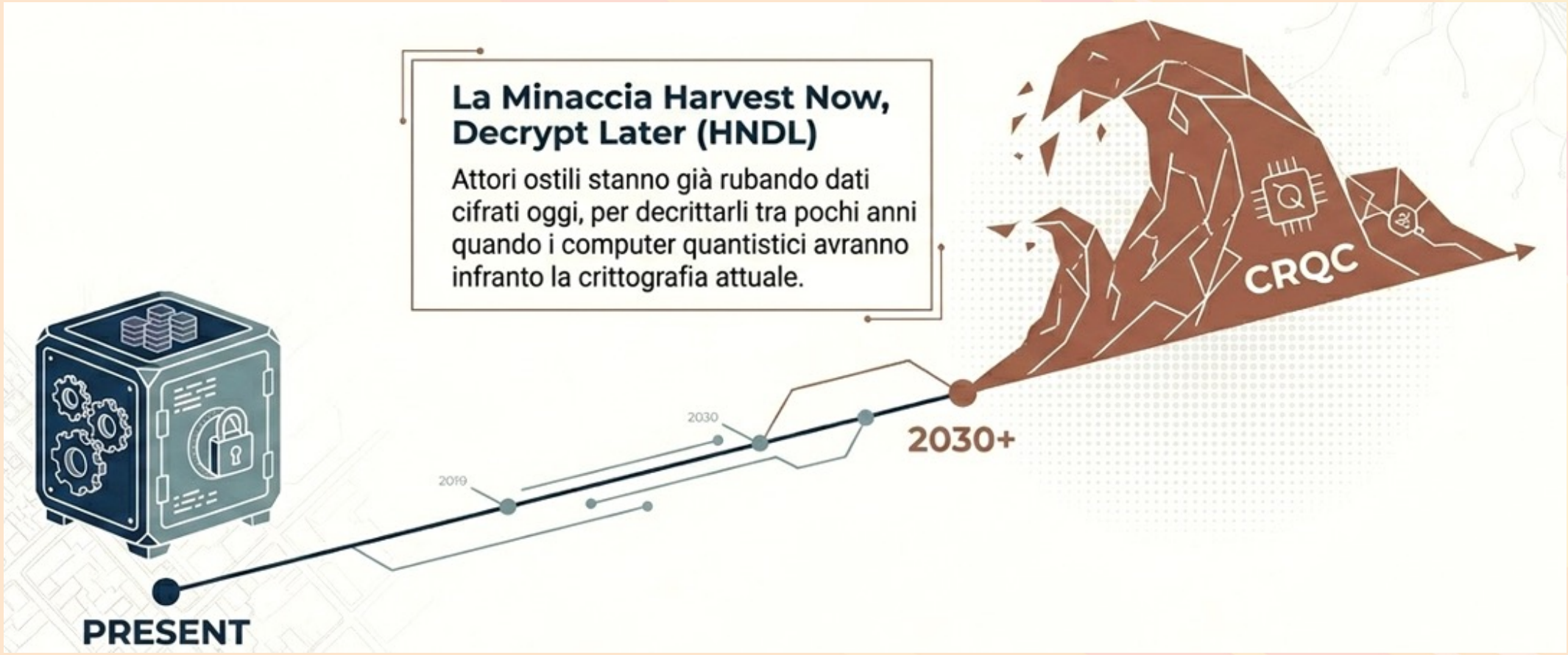
AI-Driven SOC (Security Operations Centre)

L'Intelligenza Artificiale come Difesa Data la carenza globale di esperti cyber e la velocità degli attacchi automatizzati, la risposta umana non basta più. I SOC potenziati dall'AI analizzano milioni di eventi, isolano le minacce in millisecondi e orchestrano la difesa delle infrastrutture critiche.



L'Orizzonte Post-Quantistico

Le infrastrutture ITS (es. semafori, reti ferroviarie) hanno cicli di vita di 15-30 anni. L'hardware installato oggi deve supportare la Crittografia Post-Quantum. L'UE impone la transizione delle infrastrutture critiche entro il 2030. Pianificare oggi evita la rapida obsolescenza domani.



Il Fattore Umano: Etica e Controllo

L'intelligenza artificiale nei trasporti deve essere human-centric. La tecnologia supporta, ma la responsabilità etica e legale dell'intervento in contesti critici deve rimanere saldamente umana.

AI logic

Human Oversight Checkpoint

Action

Ethics by Design

Valutazioni di impatto etico obbligatorie per evitare bias e garantire trasparenza.

Human-in-the-Loop (Art. 14 AI Act)

Le decisioni ad alto rischio non possono essere totalmente delegate alla macchina. Serve responsabilità umana inequivocabile (Legge 132/2025).

Competenze Ibride

Necessità di formare team multidisciplinari (AI Risk Officers, OT Security Specialists) per comprendere sia il trasporto che il codice.

Casi d’uso: piattaforme su larga scala

Settore Ferroviario (Alstom & Hitachi)

Alstom: Metodologia FENCE (EBIOS + IEC 62443 + CLC/TS 50701) per risk assessment nativo. Gateway unidirezionali hardware.

Hitachi Rail: Piattaforme AI e cybersecurity integrate nativamente nei treni di nuova generazione.

Smart Roads (ANAS / Gruppo FS)

Investimento di ~ 1 Miliardo €.

Edge AI per la classificazione di anomalie in tempo reale.

Protezione comunicazioni tramite Security Fabric.

Rete Autostradale (CAV)

Piattaforma STRIVE: Predizione delle anomalie di traffico tramite AI.

Prevenzione incidenti in infrastrutture critiche (gallerie, viadotti).

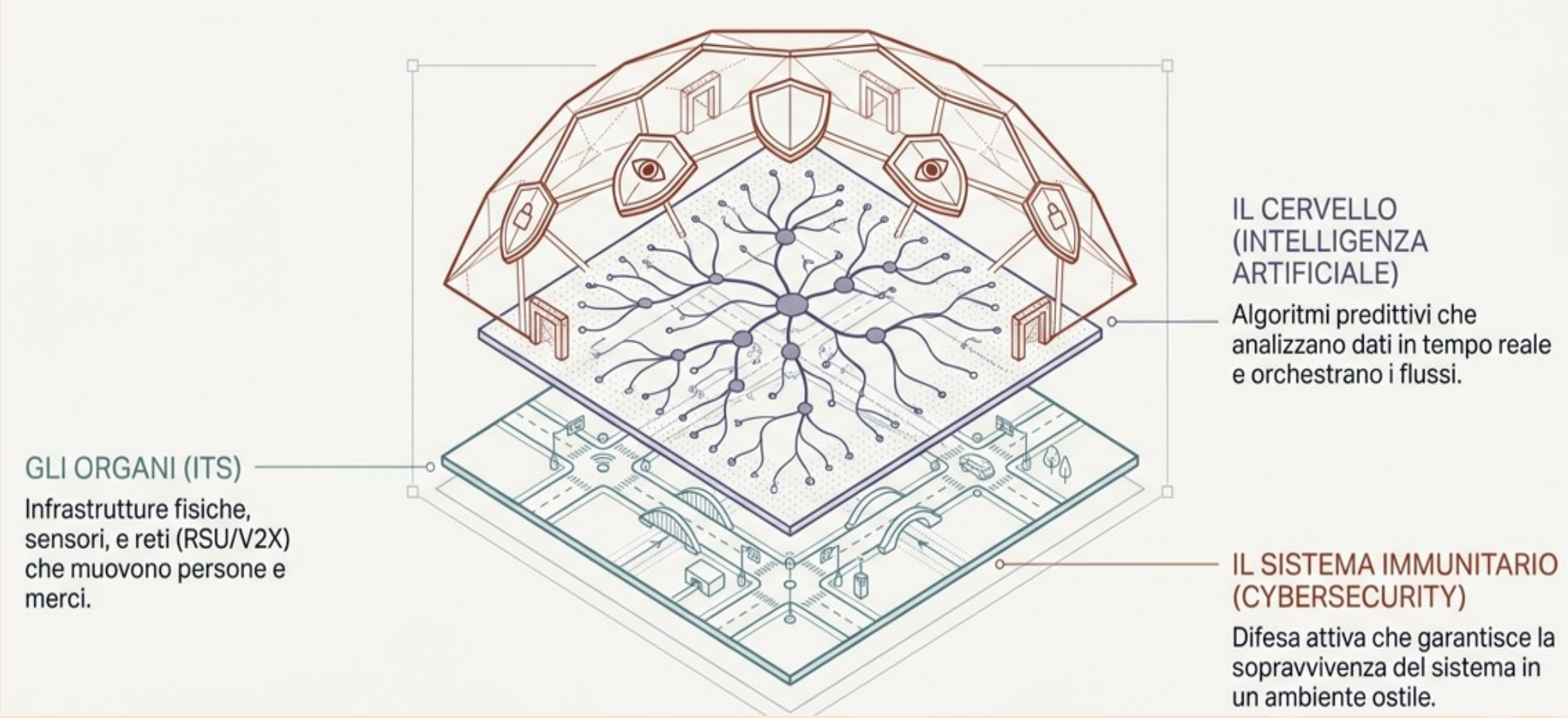
C-Roads Italy & Pedaggiamento

Implementazione architettura PKI armonizzata europea.

AI per profilazione sagoma/assi e riduzione errori ai caselli, con transazioni inviolabili.

Il sistema nervoso digitale della mobilità

La trasformazione digitale del settore dei trasporti non è una somma di tecnologie, ma la nascita di un ecosistema interconnesso. Senza un sistema immunitario cyber-resiliente, l’intelligenza diventa il suo punto di rottura



Le Raccomandazioni per una strategia integrata

Pillar 1 - Governance & Dati	Pillar 2 - Sicurezza & Resilienza	Pillar 3 - Ecosistemi & Mobilità	Pillar 4 - Etica, IA & Competenze
R1. Governance Architetturale	**R2.** Security & Zero Trust	**R6.** Logistica Integrata	**R5.** AI Affidabile Settoriale
R4. Interoperabilità e Mobility Data Platform	**R3.** Integrazione AI/Cyber	**R7.** Trasporto Multimodale	**R9.** Competenze & Sandbox
R12. Riforma Omologazione	**R13.** SOC Potenziati	**R8.** Mobilità Connessa e Autonoma	**R10.** Ethics-by-Design
	R14. Cultura Cybersicurezza		**R11.** Controllo Umano

Fattore Abilitante (Enabler)	**R15.** Incentivazioni economiche per evitare ritardi strutturali di PA e Imprese

Il 1° Pillar: Governance e dati

ID Raccomandazione	Azione Strategica	Impatto Atteso
R1	Adottare una governance architetturale integrata per ITS, AI e cybersecurity.	Superamento dei silos decisionali; allineamento strategico nazionale.
R4	Rafforzare governance dati, standard aperti e supportare una Mobility Data Platform nazionale interoperabile.	Flusso di dati fluido tra attori pubblici e privati; base per servizi avanzati.
R12	Riforma del Processo di Omologazione.	Adeguamento normativo ai ritmi dell'innovazione tecnologica; go-to-market accelerato.

Il 2° Pillar: Sicurezza e Resilienza

Zero Trust Architetturale

Dominio Sicurezza	Principio Core (Raccomandazione)	Elementi Tecnologici / Operativi
Progettazione	R2. Integrare **Security by Design** e **Zero Trust** lungo l'intero ciclo di vita.	Architetture Zero Trust, validazione continua.
Resilienza di Sistema	R3. Promuovere l'integrazione tra AI e cybersecurity come fattore abilitante.	AI per rilevamento minacce, automazione risposte.
Monitoraggio Attivo	R13. Istituzione di SOC Potenziati dall'AI.	Cyber Threat Intelligence, Digital Twin, riservatezza dati.
Fattore Umano	R14. Cultura diffusa della cybersicurezza negli ITS.	Formazione mirata per PA ed imprese.

Il 3° Pillar: Sicurezza, Resilienza ed Integrazione digitale

R6. Logistica Integrata

Sviluppo di un ecosistema integrato per l'ottimizzazione del trasporto merci e delle catene di approvvigionamento tramite dati condivisi.

R7. Multimodalità

Creazione di un ecosistema digitale per il trasporto multimodale ed intermodale, garantendo transizioni fluide tra vettori.

R8. Mobilità Connessa e Autonoma

Sviluppo di veicoli autonomi e infrastrutture ITS connesse, supportato dal necessario e tempestivo adeguamento della normativa.

Il 4° Pillar: Etica, IA e Competenze

Certificazione

R5. Sviluppo Trustworthy AI

Promuovere AI Settoriale per la mobilità con un marchio distintivo di 'AI affidabile'.

Capitale Umano

R9. Competenze e Sperimentazione

Investire in competenze, collaborazione, ambienti di sperimentazione controllata (sandbox) e team multi-genere e multidisciplinari.

Progettazione

R10. Ethics-by-Design

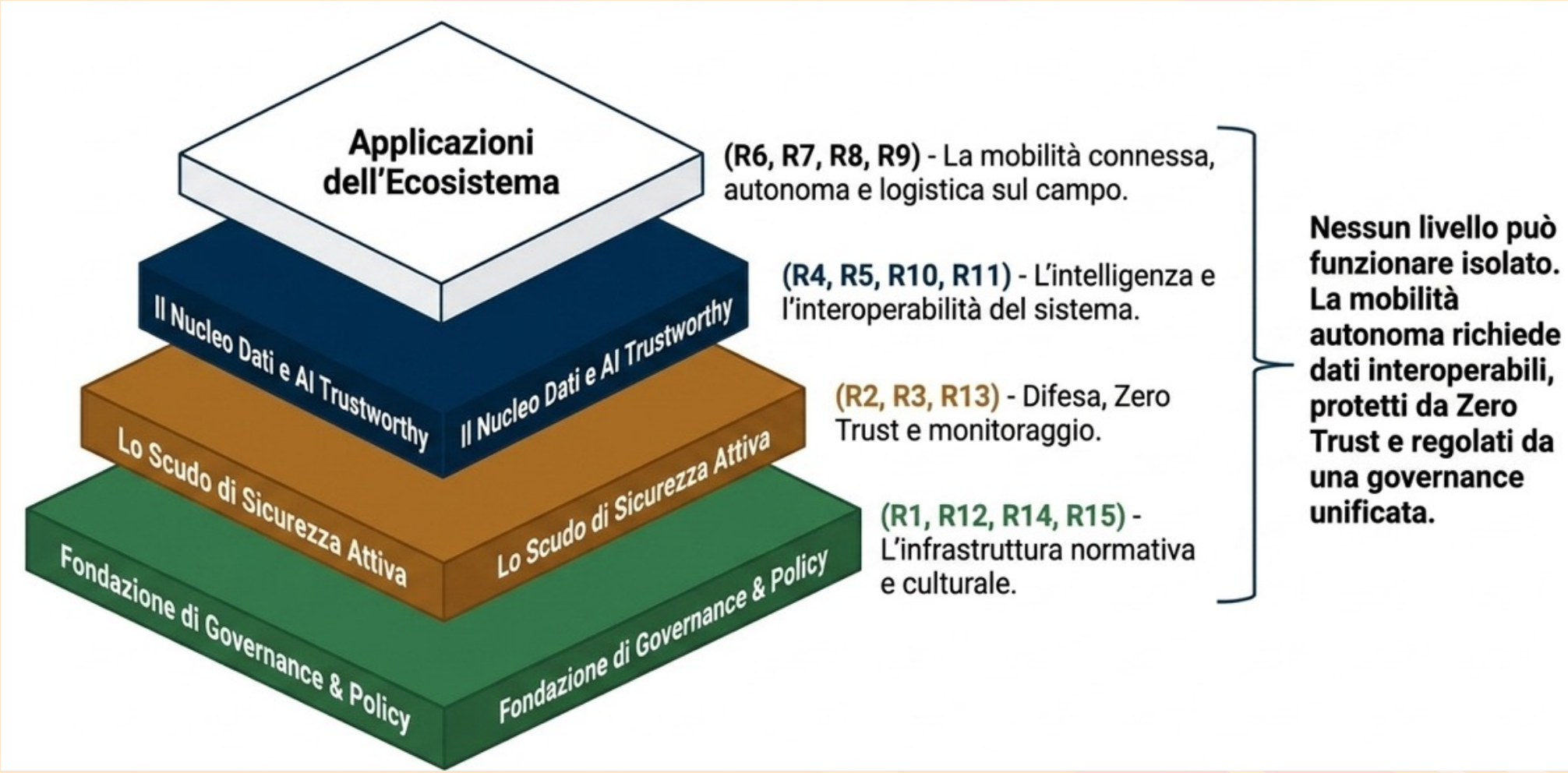
Integrare i principi etici fin dalla progettazione nei nuovi sistemi di IA critici nel settore dei trasporti.

Responsabilità

R11. Governance Umana

Garantire sempre un Controllo Umano Significativo e stabilire una Chiara Responsabilità giuridica/operativa.

La Raccomandazioni per una strategia integrata: 4 livelli di resilienza



Le Raccomandazioni in un caso reale: il veicolo autonomo

Il veicolo autonomo (R8) entra in un incrocio urbano complesso

Dati & AI	Riceve dati sul traffico dalla Mobility Data Platform (R4) e decide tramite algoritmi certificati Ethics-by-Design (R10).
Sicurezza	La connessione all'infrastruttura è validata istantaneamente tramite protocolli Zero Trust (R2) ed è monitorata dall'AI-SOC (R13).
Governance	L'intero processo è legale e assicurato perché il sistema ha superato il nuovo Processo di Omologazione (R12) sotto un'Architettura Unificata (R1).

Il fallimento di un singolo livello sottostante compromette istantaneamente l’intero ecosistema

Il Documento e le Raccomandazioni: Grazie a tutto il GdL!

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.

Il **Core-team**: Almaviva, Aesys, CinqueT, IBM, Leonardo, Mia-Platform, Openmove e Swarco Italia.

Ringraziamenti particolari agli **Ing Daniele Arangio Mazza di IBM** (coordinatore del cap. 4 – Architetture) e **Ing. Valentina Tempera di Mia-Platform** (coordinatrice cap. 5 – Casi studio).

Grazie per la vostra attenzione e…

Buona lettura!