Computers & Security 160 (2026) 104729

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

Full Length Article

A quantitative methodology for systemic impact assessment of cyber threats in connected vehicles

Don Nalin Dharshana Jayaratne [a,b,c], Qian Lu [a,*], Abdur Rakib [a], Muhamad Azfar Ramli [c], Rakhi Manohar Mepparambath [c], Siraj Ahmed Shaikh [b], Hoang Nga Nguyen [b]

[a] Centre for Future Transport and Cities (CFTC), Coventry University, United Kingdom
[b] Systems Security Group (SSG), Department of Computer Science, Swansea University, United Kingdom
[c] Institute of High Performance Computing (IHPC), Agency for Science, Technology and Research (A*STAR), Singapore

ARTICLE INFO

Keywords:
Connected vehicles
Automotive cybersecurity
Threat analysis and risk assessment
Impact assessment
Simulation

ABSTRACT

The increasing integration of digital technologies in connected vehicles introduces cybersecurity risks that extend beyond individual vehicles, with the potential to disrupt entire transportation systems. Current practice (e.g., ISO/SAE 21434 TARA) focuses on threat identification and qualitative impact ratings at the vehicle boundary, with limited systemic quantification. This study presents a systematic, simulation-based methodology for quantifying the systemic operational and safety impacts of cyber threats on connected vehicles, evaluating cascading effects across the transport network. Three representative scenarios are examined: (I) telematics-induced sudden braking causing a cascading collision, (II) remote disabling on a motorway (M25) segment, and (III) a compromised Roadside Unit (RSU) spoofing Variable Speed Limit (VSL) and phantom lane closure messages to connected and automated vehicles (CAVs). The results highlight the potential for cascading safety incidents and systemic operational degradation, as evidenced by the defined systemic operational and safety vectors, factors that are insufficiently addressed in the current scope of the ISO/SAE 21434 standard, which primarily focuses on individual vehicle-level threats. The findings underscore the need to incorporate systemic evaluation into existing frameworks to enhance cyber resilience across connected vehicle ecosystems. The framework complements ISO/SAE 21434 by supplying quantitative, reproducible evidence for the impact rating step at a systemic scale, reducing assessor subjectivity and supporting policy and operations, enabling more data-driven evaluations of systemic cyber risks.

1. Introduction

In an increasingly interconnected world, advanced digital technologies have become integral to road transportation infrastructure (Perallos et al., 2013; Joseph, 2006). These technologies enhance traffic management, road safety, and transportation efficiency while reducing environmental impacts (Deka et al., 2018; Centre for Connected and Autonomous Vehicles, 2020; Shladover, 2018). However, as these systems evolve, they introduce new cybersecurity challenges due to the integration of complex and interconnected digital components (Lamssaggad et al., 2021; Chowdhury et al., 2020; Dibaei et al., 2020a; Vellinga, 2022). Each technological advancement potentially exposes additional attack surfaces (Plappert et al., 2021).

1.1. Cybersecurity threats in connected vehicles

Modern road transport networks comprising connected vehicles (CVs) and infrastructure encounter an increasing array of cyber vulnerabilities (Upstream Security, 2024). Exploitable flaws in Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications present risks such as data breaches, traffic manipulation, and disruptions to cooperative driving functions (Lamssaggad et al., 2021; Sun et al., 2021). Similarly, autonomous vehicle perception systems such as LiDAR

* Corresponding author.
E-mail addresses: jayaratned@uni.coventry.ac.uk (D.N.D. Jayaratne), ad5271@coventry.ac.uk (Q. Lu), ad9812@coventry.ac.uk (A. Rakib), ramlimab@ihpc.a-star.edu.sg (M.A. Ramli), rakhimm@ihpc.a-star.edu.sg (R.M. Mepparambath), s.a.shaikh@swansea.ac.uk (S.A. Shaikh), h.n.nguyen@swansea.ac.uk (H.N. Nguyen).

https://doi.org/10.1016/j.cose.2025.104729
Received 2 June 2025; Received in revised form 12 September 2025; Accepted 20 October 2025
Available online 27 October 2025

(Light Detection and Ranging) and cameras are vulnerable to cyber interference, with attackers leveraging laser-based spoofing techniques to distort sensor data, causing phantom braking, unintended lane changes, or complete sensor blindness (Thompson, 2022; Ji et al., 2021).While integrating cyber systems with physical operations improves efficiency, it simultaneously expands the attack surface and introduces cyber–physical pathways that threaten privacy, operational safety, and network resilience.

The complex software systems governing CVs are susceptible to manipulation, leading to potential disruptions in traffic flow and increased public safety risks. Notable incidents, such as the Miller-Valasek Jeep Cherokee hack and the Tesla Model S hack by Tencent Keen Security Lab, have demonstrated the real-world implications of these vulnerabilities (Miller and Valasek, 2015; Nie et al., 2016). In the 2015 Jeep Cherokee hack, white-hat hackers Miller and Valasek remotely exploited a vehicle's infotainment system, gaining control over its brakes and acceleration, leading to the recall of 1.4 million vehicles (Miller and Valasek, 2015). Similarly, in 2016, Keen Security Lab remotely hacked a Tesla Model S, manipulating braking, doors, mirrors, and infotainment via vulnerabilities in the Controller Area Network (CAN) bus and web browser (Nie et al., 2016). Such remote attacks are particularly concerning due to their scalability and ability to be executed without direct physical access, making them highly effective vectors for large-scale disruptions.

Recent years have seen a sharp rise in remote cyberattacks targeting vehicle control systems, undermining the safety and integrity of road transportation networks (Upstream Security, 2024). Attackers have exploited multimedia CAN bus vulnerabilities to hijack infotainment systems (Costantino and Matteucci, 2022; Kulandaivel et al., 2021), while weaknesses in Wi-Fi chips have been leveraged to breach telematics boxes, granting unauthorised remote access to vehicle operations such as door locking, engine control, and security system deactivation (Lab, 2021). More concerningly, remote attacks capable of affecting multiple vehicles simultaneously pose an even greater threat, as they can propagate across connected vehicles in a manner akin to a worm-like cyberattack, spreading from a single point of entry to compromise an entire network (Trullols-Cruces et al., 2015). These issues have been compounded by similar security breaches through compromised vehicle partner applications, which allow further unauthorised control over various vehicle functions, such as engine ignition and headlight operation (Curry, 2023; Colombo, 2022). These vulnerabilities have been substantiated by a body of research, which points to an overarching risk of remote control over a vehicle's secondary functions, leading to direct threats to the safe operation of connected and autonomous vehicles (Jayaratne et al., 2025).

Beyond individual vehicles, cyber threats extend to mobility services and urban transportation systems, further amplifying systemic risks. Ride-hailing platforms have been targeted through compromised applications, leading to service disruptions, fraudulent ride allocations, and artificial congestion (Gordon, 2022). Further underscoring the urgency of the issue, Upstream's 2024 Global Automotive Cybersecurity Report estimates that 95 % of automotive cyberattacks are executed remotely (Upstream Security, 2024).

Collectively, these incidents highlight the urgent necessity for enhanced cybersecurity frameworks to address the expanding attack surfaces within connected transport networks. As road transportation systems become increasingly reliant on digital infrastructure, the demand for proactive, multi-layered defence strategies is paramount to safeguarding against operational disruptions, protecting road users, and ensuring the long-term resilience of intelligent transport ecosystems.

1.2. Limitations of current cybersecurity approaches

The increasing complexity of software stacks in modern and future vehicles underscores the critical need for secure and resilient vehicle and connected road transport infrastructure. To address these concerns, the automotive industry has increasingly adopted secure-by-design principles, guided by ISO/SAE 21434: Road Vehicles – Cybersecurity Engineering, which operationalises cybersecurity lifecycle activities (SAE, 2010). This standard mandates the implementation of Threat Analysis and Risk Assessment (TARA) for connected vehicles, focusing on the identification of threats, vulnerabilities, and associated risks. UN-ECE R155 establishes the regulatory Cybersecurity Management System (CSMS) for type approval, with ISO/SAE 21434 serving as the principal technical means by which industry demonstrates compliance (UNITED NATIONS, 2021). In practice, ISO/SAE 21434 also interfaces with ISO 26262: Road Vehicles – Functional Safety, particularly for severity terminology and safety-of-the-intended-function considerations (Organisation, 2018). Despite this strong ecosystem, the current approach is limited in scope to the vehicular level and fails to consider potential impacts beyond the vehicle itself, despite these systems operating within shared spaces where malfunctions can lead to severe operational, safety, privacy and financial consequences. Furthermore, the effectiveness of these frameworks heavily relies on the expertise of assessors, which may result in inconsistent or unreliable outputs.

1.3. Research gap and contributions of this study

There is thus a pressing need to account for the systemic impacts of vehicular cyber threats and to develop a framework that systematically evaluates damage scenarios arising from automotive cyber incidents. Such a framework would enable stakeholders to make informed decisions about mitigating risks and addressing vulnerabilities. This study aims to address this gap by integrating a systematic simulation-based framework within the ISO/SAE 21434 TARA process to quantitatively evaluate both operational and safety impacts of cyber threats. The main contributions of this study are:

1. Expansion of the TARA process: This study extends the existing the TARA methodology by incorporating systemic impact assessments, explicitly addressing cascading effects that extend beyond individual vehicles.
2. Quantitative evaluation through simulation: A simulation-driven framework is developed to provide data-driven insights into cyber risks, enabling structured, quantitative assessments of operational and safety impacts.

Table 1
Glossary covering key terms used in this study.

Acronym	Description
AIS	Abbreviated Injury Scale
CACC	Cooperative Adaptive Cruise Control
CAN	Controller Area Network
CAV	Connected and Automated Vehicle
CDS	Crashworthiness Data System
COR	Coefficient of Restitution
CV	Connected Vehicle
ECU	Electronic Control Unit
FR	Flow Ratio
ISO/SAE 21434	Standard for Road vehicles - Cybersecurity engineering
LOS	Level of Service
MAIS	Maximum Abbreviated Injury Scale
NASS	National Automotive Sampling System
NHTSA	National Highway Traffic Safety Administration
PR	Penetration Ratio
RSU	Roadside Unit
SR	Speed Ratio
TARA	Threat Analysis and Risk Assessment
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-Everything
VSL	Variable Speed Limit

1.4. Paper structure

The remainder of this paper is organised as follows. Section 2 provides background information and reviews related work. Section 3 outlines the overall methodology of the proposed frameworks. Section 4 details the operational impact assessment framework, while Section 5 describes the safety impact assessment framework. Section 6 presents three case studies to demonstrate the application of the proposed frameworks. Finally, Section 8 concludes the paper by summarising the contributions and suggesting directions for future research. The key technical terms used in this paper are defined in the Glossary Table 1.

2. Related work

2.1. Automotive cybersecurity risk assessment frameworks

Cybersecurity risk assessment frameworks play a crucial role in safeguarding connected vehicles from evolving cyber threats. Various methodologies have been developed to evaluate risks within cyber-physical systems, integrating both safety and security aspects. Frameworks such as Goal Tree Success Tree – Master Logic Diagram (GTST-MLD) (Di Maio et al., 2019), S-CUBE SCADA (Supervisory Control and Data Acquisition) Safety and Security modelling)) (Kriaa et al., 2015), and Boolean Driven Markov Processes (Pièrre-Cambacédès and Bouissou, 2010) provide structured approaches for assessing risks in industrial and critical infrastructure systems. These frameworks rely on techniques such as hierarchical logic models, domain-specific languages, and graph-based representations to analyse vulnerabilities. While these methods are robust for general cyber-physical systems, they lack specificity in addressing the unique challenges of the automotive domain.

In the context of connected vehicles, the ISO/SAE 21434: Road Vehicles – Cybersecurity Engineering standard is the foundational framework for automotive cybersecurity risk management. Aligned with UN Regulation No. 155, ISO/SAE 21434 provides a structured approach for identifying, assessing, and mitigating cybersecurity risks throughout the lifecycle of vehicular components (Manuel, 2022). At its core is the TARA methodology, which evaluates risks based on asset identification, threat scenarios, impact analysis, attack feasibility, and risk value determination. TARA's adaptability makes it well-suited for evolving automotive technologies, yet its primary focus remains on in-vehicle systems and perimeter components, with limited attention to systemic risks across broader transport networks.

The impact assessment framework within TARA evaluates the potential consequences of cyber threats across four key categories: safety, operational, financial, and privacy impacts. Each damage scenario is assigned a severity rating, ranging from negligible to severe, based on its potential implications. However, the reliance on qualitative assessments and assessor expertise introduces subjectivity, making it challenging to address network-wide risks.

Beyond ISO 21434 TARA other popular automotive risk assessment frameworks can largely be classified as formula and model based methods (Luo et al., 2021). Formula-based methods (e.g., EVITA (E-safety Vehicle Intrusion Protected Applications), HEAVENS (HEAling Vulnerabilities to ENhance Software Security and Safe), SAHARA (Security-Aware Hazard Analysis and Risk Assessment), SARA, CVSS (Common Vulnerability Scoring System)-based adaptations) score impacts and feasibility at the vehicle/function level with varying granularity (Lautenbach and Mafijul Islam, 2016; Macher et al., 2015; Monteuuis et al., 2018; EVITA, 2009). Model-based approaches (STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege), PASTA (Process for Attack Simulation and Threat Analysis), attack graphs/ Boolean logic Driven Markov Processes (BDMP)) improve coverage and automation (graph-centric tooling such as attack-path prioritisation), and Bayesian formulations have been explored for attacker modelling and risk aggregation (Saulaiman et al., 2025; Wang et al., 2023). While valuable for identifying and ranking threats, these lines of work do not quantify the transport-network-level outcomes that follow from a successful manipulation.

Recent work in the domain continues to refine threat modelling and TARA for CVs. Benyahya et. al introduced TARA 2.0 which extends traditional TARA with focus on privacy centric modelling for vehicles with higher autonomy incorporating SAE automation levels as a metric influencing attack likelihood and expert objectivity (Benyahya et al., 2025). However its scope remains risk identification/feasibility at the component level rather than on systemic impact assessment. Other studies include the application of STRIDE analyses for in-vehicle infotainment stacks combining SAHARA/ DREAD (Damage, Reproducibility, Exploitability, Affected users, and Discoverability) scoring to identify component level threat catalogues (Das et al., 2024), ISO 21434/ ISO 24089 application to Autonomous Emergency Braking (AEB) systems to identify risk ratings and mitigations (Della Monica et al., 2025) both with no focus on impacts beyond the perimeter of the vehicle. Finally, ISO/SAE 21434 assessments of Automatic Collision Notification (ACN) architectures illustrate the community's reliance on 21434/TARA for architectural security evaluation (Boi et al., 2023) Taken together, these studies strengthen the standardised risk-assessment pipeline but remain item-centred and expert-dependent.

To address these limitations, this study proposes a simulation-based framework that complements TARA by providing quantitative metrics to support impact assessments. By simulating cascading cyber-induced disruptions, the proposed methodology enhances TARA's ability to evaluate systemic risks, offering a more comprehensive and data-driven approach to cybersecurity risk assessment for connected vehicles.

2.2. Impact assessment metrics

Most research related to impact assessment of connected vehicles within the scope of transport networks focuses on the efficiency and safety benefits introduced by connectivity and automation. A review of previous studies reveals that the majority of impact assessments evaluate their influence on traffic efficiency and safety, with some also considering environmental effects, such as energy consumption and emissions (Sadid and Antoniou, 2023). For efficiency assessments, common metrics include traffic flow parameters (e.g., flow rate and density), average travel time, string stability, and average velocity (Rahman et al., 2021; Tympakianaki et al., 2022; Song et al., 2023). Some studies have specifically examined the impact of cyberattacks on CV operations. One such study evaluated CVs operating in an exclusive traffic environment—i.e., without mixed traffic conditions—using a Cooperative Adaptive Cruise Control (CACC) model. The attack scenario involved communication-based spoofing, where adversaries manipulated vehicle speed and position information to assess the impact of falsified data. The study measured the impact in terms of collision risk, using a surrogate measure, and speed variations to determine how cyber disruptions influence network safety and stability (Dong et al., 2020).

Similarly, for safety impact evaluations, some studies have used surrogate safety measures (SSMs) to quantify potential conflicting situations and assess the impact of CV penetration rates on traffic safety. The most frequently used metrics for safety assessment in the literature include time-to-collision (TTC), post-encroachment time (PET), and the number of conflicts, often based on TTC and PET thresholds (Karbasi and O'Hern, 2022; Miqdady et al., 2023; Rahman et al., 2021). Speed is recognised as a key contributor in crash likelihood and severity (Jurewicz et al., 2016; Elvik, 2013). In a popular study in 2005, speed-fatality probability relationships (Wramborg's curves) were proposed for vehicle-pedestrian/cyclist and vehicle-vehicle collisions (Wramborg, 2005). These relationships indicate a 10 % fatality probability in vehicle-vehicle collisions at 70 km/h (front-end) and 50 km/h (side), and in vehicle-pedestrian/cyclist collisions at just 30 km/h, mirroring values presented in Vision Zero (Tingvall and Haworth, 1999). In a later study, it was argued that delta-V (Δv) as a measure for the severity of vehicular

conflicts overcomes significant shortcomings in common metrics such as maximum speed, post-encroachment time, deceleration rate, and surrogate safety measures like time-to-collision (Shelby, 2011). It is well established that delta-V is closely related to injury severity in vehicular crashes (Joksch, 1993; Shelby, 2011).

There have been numerous studies that link Δv with injury severity and probability of fatality since it became evident that Δv is a strong predictor of crash severity. One of the earliest efforts to link Δv with injury severity was in a study by Carlson, who rated the injury severity using the Abbreviated Injury Scale (AIS) (Carlson, 1979). Research on vehicle-to-vehicle collisions by the National Highway Traffic Safety Administration (NHTSA) has been pivotal, particularly studies by Bahouth and Schulman (2012), Bahouth et al. (2014). These studies have established detailed delta-v versus severe injury probability relationships for various collision types using extensive crash data from the NASS/CDS (National Automotive Sampling System/ Crashworthiness Data System) and Crash Injury Research and Engineering Network (CIREN) databases in the USA.

3. Methodology

3.1. Scope

This study enhances the existing TARA process, as defined by ISO/SAE 21434, by integrating a systematic simulation-based framework for quantitatively evaluating operational and safety impacts stemming from cyber threat-induced events.

As illustrated in Fig. 1, the proposed framework fits within the TARA process by providing quantitative input through the simulation of the damage scenario and feeding the impact evaluations into the overall risk assessment methodology. This integration enables stakeholders to adopt an evidence-based approach in assessing the broader consequences of automotive cyber incidents.

The framework extends the conventional TARA methodology, which primarily focuses on vehicle-level risk assessment, by incorporating systemic impacts across the connected transport network. This addresses a critical gap in current cybersecurity evaluations, where the cascading effects of cyber threats on broader transportation systems remain underexplored. By integrating operational and safety impact assessments into TARA, this approach provides a holistic risk perspective, enabling more resilient cybersecurity strategies for connected vehicle ecosystems. This integrated framework lays the foundation for informed decision-making, enabling stakeholders to enhance the resilience and security of connected transport systems through structured, data-driven risk evaluation.

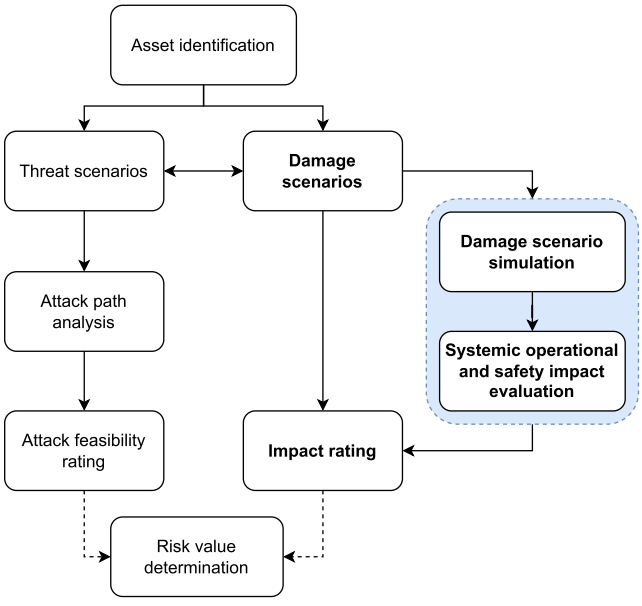

Fig. 1. Integration of the proposed operational and safety impact assessment framework within the TARA process, illustrating its role in simulating damage scenarios and evaluating their impacts to support systemic risk analysis.

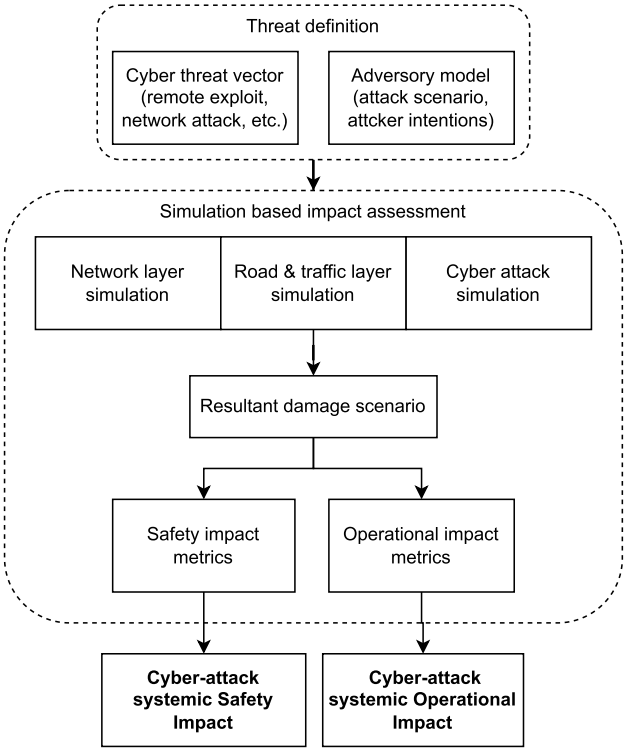

Fig. 2. Framework for simulation-based impact assessment of cyber threats in connected vehicles, integrating network, road traffic, and cyber-attack simulations to evaluate systemic operational and safety impacts.

3.2. Overview of the methodological framework

Fig. 2 illustrates the integration of the simulation-based impact assessment framework within the broader TARA framework. The proposed framework consists of three key stages: threat definition, simulation-based impact assessment, and impact evaluation and rating.

The threat definition stage involves identifying potential cyber threat vectors alongside an adversary model that characterizes attacker intentions, capabilities, and attack scenarios. This step ensures a structured understanding of the attack landscape and enables the identification of plausible threat scenarios that could compromise vehicle and transport system security.

Once these threats are defined, they are analysed through simulation-based impact assessment, which employs a multi-layered simulation model (see Section 3.3). This model consists of three key components: the network communications layer, which represents vehicle-to-everything (V2X) communications; the road and traffic layer, which simulates road infrastructure and vehicle interactions within the transport network; and the cyber attack simulation, which manipulates parameters within both the network and road traffic layers to replicate the execution and propagation of a cyber threat.

The final stage, impact evaluation and rating, quantifies the resultant damage scenario by assessing both safety and operational consequences. The incident safety vector (I_S) is introduced as a structured metric for rating safety impact, incorporating factors such as injury severity and the number of collisions. Similarly, the systemic operational impact is captured through the operational impact vector (I_O), which evaluates

parameters such as travel speed and traffic flow. By integrating I_S and I_O, the framework enhances conventional risk assessment methodologies, providing stakeholders with a data-driven foundation for decision-making in automotive cybersecurity.

3.3. Simulation framework

The road and traffic layer in this study is simulated using the microscopic traffic simulator SUMO, offering a robust platform for modelling detailed vehicular dynamics (Lopez et al., 2018). To effectively incorporate V2X communications where necessary, the VEINS simulation framework is employed, following the approach outlined in our earlier work (Jayaratne et al., 2024). VEINS leverages OMNeT++ for advanced network modelling and uses TraCI for seamless bi-directional coupling with SUMO (Sommer et al., 2019), thereby enabling realistic integration of V2V and V2I interactions. This integration enables a cohesive simulation of both the physical and communication layers, providing a comprehensive representation of transportation networks. The current study builds upon this foundation; the focus here shifts toward the transport impacts of cyber-threat scenarios, where SUMO is utilised independently to simulate traffic dynamics.

Within SUMO, the default car-following model 'Krauss' (Krauß, 1998) and the lane-changing model 'LC2013' govern longitudinal and lateral vehicle movements, respectively. These models, together with secondary modelling parameters, create an adaptable and precise simulation environment. For scenarios requiring high-fidelity communication modelling, VEINS emulates wireless vehicular communications to capture the interactions within an integrated transportation system. In cases where communication simulation is not critical, the VEINS framework is bypassed, and custom scripts are used to simulate the influence of the communication layer. This flexible approach allows the framework to adapt to a variety of operational conditions, facilitating the analysis of cyber-threat impacts on transportation systems.

4. Systemic operational impact assessment

To address the diverse nature of cyber threats in transportation systems and the varying requirements of operational impact assessment, we propose a model that is both adaptable and scalable. This flexibility allows for the evaluation of operational impacts at a granular level, such as individual lanes or intersections, as well as at a macroscopic scale, including entire motorways or urban transport networks. The systemic operational impact of a cyber incident is modelled as a function of key factors influencing the severity and extent of the disruption (Eq. (1)).

$$I_O = f\left(I_C, I_D, I_{TC}, I_{NR} | A, T\right) \tag{1}$$

Here I_C represents the direct outcome of the cyber attack, such as a vehicle being disabled, involuntary acceleration, or unintended activation of signal lights. I_D quantifies the duration over which this direct outcome persists and continue to disrupt normal operations. For instance, if a vehicle is immobilised due to the attack, I_D would reflect the time taken to restore functionality, remove the vehicle, or otherwise mitigate its disruptive effect on traffic flow. I_{TC} represents the prevailing traffic conditions of the transportation network during the time of the attack. I_{NR} reflects the network's resilience, considering both the criticality of the affected segment and the system's capacity to reroute traffic during disruptions. Finally, A and T define the spatial and temporal areas of the assessment, specifying the geographic scope and the time frame over which the impact is evaluated, respectively.

While Eq. (1) encapsulates the key factors influencing systemic operational impact, translating these factors into measurable outcomes requires a structured assessment process. Fig. 3 outlines the operational impact assessment framework, which provides a scalable methodology for quantifying impact across different spatial and temporal scales.

The framework begins by comparing the cyber incident-induced damage scenario with an incident-free baseline scenario. This comparison, based on simulation data, enables the identification of impacts

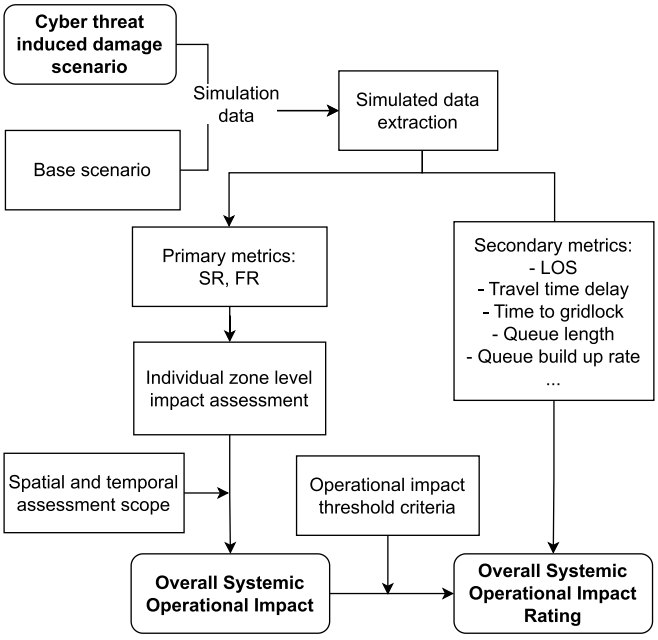

Fig. 3. Simulation-based systemic operational impact assessment framework.

attributable specifically to the cyber incident. Primary performance metrics—Speed Ratio (SR) and Flow Ratio (FR)—are used to quantify this impact (see Sections 4.1 and 4.4). Secondary metrics, such as Level of Service (LOS), Mean Travel Time Loss ($MTTL$), Total Vehicle Delay (TVD), queue length, time to gridlock, and queue build-up rate, may also be incorporated to provide additional context and insight.

The spatial and temporal assessment areas are defined based on the scope of analysis (see Section 4.2), allowing the framework to capture both localised impacts and widespread disruptions. Within the defined assessment area, SR and FR are computed for each zone and subsequently aggregated to produce overall metrics representing the systemic operational impact. These aggregate values are then mapped to predefined impact thresholds, resulting in a categorical rating that reflects the severity and extent of the impact. Details on the threshold definitions are provided in Section 4.4.

The high-level model described in Eq. (1) is practically applied in this framework, supporting a nuanced understanding of the systemic operational impact of cyber threats, for informed decision-making and resilience planning.

4.1. Operational impact metric definitions

The impact of a cyberattack on road transportation networks can be evaluated at varying scales, from individual lanes and intersections to entire roadways, motorways, sections of a city, or even city-wide networks. Speed and flow are fundamental traffic flow metrics that are universally applicable across all scenarios, regardless of the scale or infrastructure being evaluated. The performance measures SR and FR evaluate the system's mobility and throughput under attack scenarios compared to baseline conditions.

SR evaluates the operational impact of a cyberattack-induced incident on mean travel speed (Eq. (2)).

$$SR = \frac{v_{\text{att}}}{v_{\text{base}}} \tag{2}$$

Where v_{att} is the mean travel speed during the attack scenario, and v_{base} is the mean travel speed during the baseline scenario. SR provides a measure of mobility, highlighting the extent to which the incident disrupts the expected travel speed. A lower SR indicates a greater impact on mobility.

Table 2
Operational metrics at a glance. SR and FR are baseline-normalised ratios.

Metric	Interpretation
SR	1: no impact; < 1: slower than baseline
FR	1: no impact; < 1: reduced throughput
LOS	[$A \Leftrightarrow F$]; A best, F worst

The FR assesses the impact on the system's vehicular throughput and is expressed as given in Eq. (3).

$$FR = \frac{q_{\text{att}}}{q_{\text{base}}} \tag{3}$$

Where q_{att} is the vehicular flow during the attack scenario, and q_{base} is the vehicular flow during the baseline scenario. FR reflects the system's ability to maintain throughput under cyberattack-induced disruptions. A lower FR signifies a more significant reduction in vehicular flow. By construction, both SR and FR are normalised ratios to the scenario's baseline; values are reported only where the corresponding baseline denominator is non-zero.

SR evaluates mobility by measuring the extent to which vehicular speeds are maintained under incident conditions, directly reflecting the road users' experience of movement efficiency. This metric primarily captures the perspective of road users by highlighting how a cyberattack-induced disruption impacts their ability to traverse the network efficiently. In contrast, FR serves as a proxy for accessibility by assessing the system's ability to accommodate traffic and sustain throughput. By reflecting the performance and capacity of the network under incident conditions, FR aligns with the concerns of service providers, such as road authorities, who focus on maintaining the operational integrity and accessibility of the transportation system.

While SR and FR form the primary metrics for evaluating operational impact, additional secondary metrics can provide deeper insights, depending on the specific scale and type of facility being studied. At the scale of individual lane or intersection, metrics such as queue length, intersection delay, and stop frequency are relevant for understanding localised impacts. For roadways or motorways, metrics such as LOS, lane density, volume-to-capacity (V/C) ratio offer insights into how efficiently the system operates under stress. At a city-wide scale, metrics such as time to gridlock and time to recovery help quantify the broader systemic impact of a cyber incident. Table 2 summarises the key operational impact metrics and its interpretation.

Illustrative example. If the baseline mean speed is 100 km/h and the attack mean speed is 70 km/h, then $SR = 0.70$, indicating reduced mobility relative to baseline. If the baseline flow is 1800 veh/h and the attack flow is 1500 veh/h, then $FR = 0.83$, indicating reduced throughput on the sampled road section.

4.2. Assessment scope: spatial and temporal definitions

The scope of the operational impact assessment is defined in terms of '*Spatial assessment region* (A)' and '*Temporal assessment window* (T)'. These represent the geographical extent and the duration, respectively, over which the operational impacts are evaluated. The spatial assessment region comprises all the spatial zones included in the analysis, representing the total area of analysis. The assessment time window encompasses the total duration over which operational metrics are monitored; this could include the incident onset, disruption phase, and system recovery. Together, these form the scope within which operational impacts are measured.

4.2.1. Spatial assessment region (A)

The assessment region is composed of discrete spatial zones. A spatial zone (a_i) is defined as a geographically homogeneous segment within the transportation network, characterised by consistent traffic operational conditions, road geometry, or functional classification. This segmentation enables the independent assessment of operational impacts within each zone, facilitating a detailed analysis of disruptions across specific sections of the network.

The assessment region is defined as the total of all spatial zones (a_i) considered within the operational impact evaluation. Formally, this is expressed as:

$$A = \sum_{i=1}^{N_a} a_i \tag{4}$$

where each zone a_i represents a geographically homogeneous segment, and N_a is the total number of zones.

This formulation allows the assessment region to be flexibly defined based on the required level of analysis, accommodating both broad network-level evaluations and detailed, localised assessments. This ensures its applicability across a wide range of transportation network configurations and disruption scenarios.

4.2.2. Temporal assessment window (T)

The temporal assessment window (T) is defined as the total duration over which operational impact metrics are evaluated, composed of discrete time intervals (Δt_j). Formally, the total assessed duration is expressed as:

$$T = \sum_{j=1}^{N_t} \Delta t_j \tag{5}$$

where Δt_j is the duration of the jth time interval, and N_t is the total number of intervals within the assessment period.

The temporal boundary can be adapted based on the nature of the incident or the specific objectives of the assessment. For example, a fixed time limit approach involves using a predefined duration to evaluate the impact. Alternatively, the assessment can extend until the end of the incident, capturing the period during which the incident actively influences traffic flow or speed. A further approach is to continue the evaluation until traffic stabilises, encompassing the time required for conditions to return to a steady state.

Both the spatial and temporal assessment scopes are designed to be flexible, allowing adjustments that reflect the specific characteristics of the incident under consideration. For the spatial assessment, segmenting the network into discrete zones based on the locations where primary metrics are evaluated ensures a systematic and granular analysis. Similarly, the temporal assessment window allows for adaptability to different time scales, enabling the capture of both short-term disruptions and longer-term recovery processes.

4.3. Overall systemic operational impact

The operational impact is defined using SR and FR metrics calculated for each individual spatio-temporal zone. For a given spatial zone (a_i) and time step (Δt_j), SR and FR are defined as shown in Eqs. (6) and (7):

$$SR_{i,j} = \frac{(v_{att})_{i,j}}{(v_{base})_{i,j}} \tag{6}$$

$$FR_{i,j} = \frac{(q_{att})_{i,j}}{(q_{base})_{i,j}} \tag{7}$$

Where $v_{\text{att}}(i,j)$ and $v_{\text{base}}(i,j)$ denote the mean travel speeds in attack and baseline scenarios, respectively, while $q_{\text{att}}(i,j)$ and $q_{\text{base}}(i,j)$ represent the corresponding vehicular flows for zone i at time step j.

To evaluate the systemic operational impact across the network, spatial weighting factors (ω_i) reflecting the operational significance of each spatial zone (e.g., arterials vs. minor roads) are introduced. The

Table 3
Operational impact threshold definitions for Speed ratio (SR) and Flow ratio (FR) metrics.

Operational impact rating	Description	Metric threshold
Negligible	Minimal operational impact relative to baseline conditions. The system operates near its baseline performance, with negligible reductions in speed and flow.	$0.75 \leq SR \leq 1.00$ $0.75 \leq FR \leq 1.00$
Moderate	Noticeable but manageable impact relative to baseline conditions. Speed and flow show moderate reductions, resulting in some delays or reduced efficiency.	$0.50 \leq SR < 0.75$ $0.50 \leq FR < 0.75$
Major	Significant operational disruption compared to baseline conditions. Speed and flow experience substantial reductions, leading to severe delays, reduced capacity, and a marked decrease in system efficiency.	$0.25 \leq SR < 0.50$ $0.25 \leq FR < 0.50$
Severe	Critical operational breakdown relative to baseline conditions. Speed and flow are drastically reduced. The system operates under highly degraded conditions, far from its baseline performance.	$SR < 0.25$ $FR < 0.25$

weighted aggregation of SR and FR metrics over all spatial zones (N_a) and time intervals (N_t) is expressed as:

$$SR_{AT,\omega} = \frac{\sum_{i=1}^{N_a} \sum_{j=1}^{N_t} \omega_i \cdot SR_{i,j}}{N_t \cdot \sum_{i=1}^{N_a} \omega_i} \tag{8}$$

$$FR_{AT,\omega} = \frac{\sum_{i=1}^{N_a} \sum_{j=1}^{N_t} \omega_i \cdot FR_{i,j}}{N_t \cdot \sum_{i=1}^{N_a} \omega_i} \tag{9}$$

The systemic operational impact is formalised as a vector of key performance metrics, evaluated over a defined spatial assessment region and temporal assessment window (Eq. (10)). This structure supports scalability, allowing the same formulation to be applied at various levels of analysis—from individual zones and time steps to corridor-wide or network-level assessments.

$$[I_O]_{AT,\omega} = \left[SR_{AT,\omega};\ FR_{AT,\omega};\ S_{AT,\omega}\right] \tag{10}$$

The metrics $SR_{AT,\omega}$ and $FR_{AT,\omega}$ reflect relative changes in speed and flow due to the cyber-induced incident. Complementary metrics, such as LOS, offer additional context regarding absolute operational impact is represented by $S_{AT,\omega}$. This formulation allows results to be consistently interpreted across varying temporal and spatial scales, enabling tailored yet comparable impact assessments.

4.4. Impact metric threshold criteria

Table 3 establishes the operational impact rating criteria, delineating threshold values for varying degrees of transport network disruption caused by the cyber threat. The impact rating follows a four-tier classification aligned with the ISO 21434 TARA framework. Each classification represents a quantifiable deviation from baseline operational performance, ranging from negligible impact (*Negligible*) to severe network degradation (*Severe*). These criteria offer a structured methodology for evaluating operational degradation and assessing the network's capacity for recovery following a cyberthreat-induced incident.

The threshold boundaries are adapted from the Speed Performance Index developed by He et al., and are used to define operational thresholds for SR and FR that represent deviations from baseline performance under cyber-induced disruptions (He et al., 2016). The thresholds applied in this study follow a uniform segmentation: values below 0.25 indicate a *Severe* impact, reflecting substantial degradation in vehicular mobility, while values approaching 1.00 correspond to a *Negligible* impact, signifying near-baseline functionality. This segmentation provides a practical approach in the absence of context-specific thresholds. These definitions are not intended to be prescriptive, but rather serve as a configurable template for classifying operational impact. They may be refined or calibrated to reflect specific operational contexts, stakeholder priorities, or domain-specific considerations.

5. Systemic safety impact assessment

5.1. Scope

This subsection outlines the methodology for assessing the safety impact of vehicular collision scenarios in the context of cyber-threat-induced events. The framework, illustrated in Fig. 4, provides a structured approach to evaluate such damage scenarios. Fig. 4 depicts the process flow of the safety impact assessment, starting from a simulated damage scenario of a vehicular collision, through to the calculation of pre- and post-collision speeds, the determination of Delta-V (Section 5.2), and finally the assignment of a vehicular safety impact rating and incident safety vector (Section 5.5).

The damage scenario is simulated to obtain the necessary data for the safety impact assessment. This process involves modelling vehicular collisions and extracting the pre-collision speeds of the involved vehicles from the simulation. These pre-collision speeds are used to calculate the delta-v (Δv) metric, which measures the change in velocity due to the collision.

5.2. Post collision speed and delta-V

Speed is recognised as a key contributor in crash likelihood and severity (Jurewicz et al., 2016; Elvik, 2013). In vehicular collisions, delta-V is a widely accepted measure for the severity of vehicular conflicts, as it overcomes significant shortcomings in common metrics such as maximum speed, post-encroachment time, deceleration rate, and surrogate safety measures like time-to-collision (Shelby, 2011). It is well established that delta-V is closely related to injury severity in vehicular crashes (Joksch, 1993; Shelby, 2011).

To accurately calculate delta-V, both pre-collision and post-collision speeds of the vehicles involved are required. Pre-collision speeds are extracted from the simulated damage scenario, which provides the initial conditions for the collision. The change in velocity (delta-V) between the pre-collision and post-collision trajectories of a vehicle is calculated using the following fundamental equation (Eq. (11)).

$$\Delta\vec{v} = \vec{v}_{after} - \vec{v}_{before} \tag{11}$$

We derive the fundamental equation for the change in velocity (Δv) as follows. Consider a vehicle, with mass m_1, travelling at an initial velocity v_1 and approaching another vehicle, which has a mass m_2 and an initial velocity v_2. The velocities of both vehicles post-collision are represented as $\tilde{v}_1$, $\tilde{v}_2$ (see Fig. 5). The change in velocity (Δv) for each vehicle is determined by the difference between their respective pre-collision and post-collision velocities, as detailed in Eq. (12).

$$\begin{aligned} \Delta v_1 &= \tilde{v}_1 - v_1 \\ \Delta v_2 &= \tilde{v}_2 - v_2 \end{aligned} \tag{12}$$

Vehicular collisions exhibit a somewhat elastic effect where they rebound from each other. The elasticity of collisions is represented through the coefficient of restitution (COR), with zero (COR = 0) for perfectly inelastic collisions and one (COR = 1) for perfectly elastic collisions. Research suggests that while vehicular collisions exhibit elastic behaviour, the COR is typically between 0.1-0.3, with lower values at higher collision speeds (Neades and Smith, 2011; Rose et al., 2006). For simplicity, we assume that the collisions are inelastic, as done by previous studies (Jurewicz et al., 2016; Shelby, 2011; Tolouei et al., 2012). This assumption simplifies the complex dynamics of the collision and logically follows the movement of vehicles during the initial impulse of the crash. Hence, applying conservation of momentum equations, we

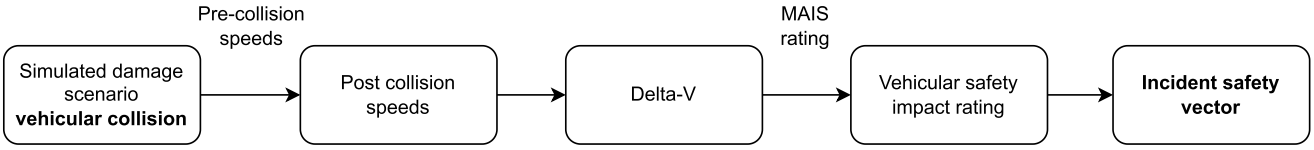

Fig. 4. Safety impact assessment framework. The framework evaluates the severity of vehicular collisions using pre- and post-collision speeds, Delta-V, and Maximum Abbreviated Injury Scale (MAIS) ratings to determine the Incident safety vector.

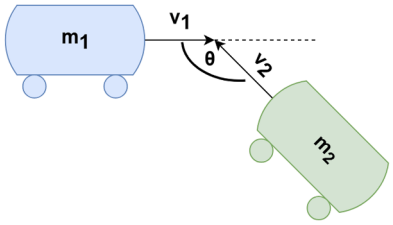

Fig. 5. Illustration of velocity change (ΔV) in a vehicular collision, showing initial velocities (v_1, v_2), impact angle (θ) and vehicle masses (m_1, m_2).

get Δv (Δv_1 and Δv_2 for the vehicles with mass m_1 and m_2 respectively) as in Eq. (13), where θ is the angle between the pre-collision velocity vectors of the two vehicles: $\theta = 0$ corresponds to a rear-end collision, and $\theta = \pi$ corresponds to a head-on collision.

$$\Delta v_1 = \frac{m_2}{m_1 + m_2}\sqrt{v_1^2 + v_2^2 - 2 \cdot v_1 \cdot v_2 \cdot \cos\theta}$$
$$\Delta v_2 = \frac{m_1}{m_1 + m_2}\sqrt{v_1^2 + v_2^2 - 2 \cdot v_1 \cdot v_2 \cdot \cos\theta} \quad (13)$$

It is noted that the assumption of inelastic collisions leads to a slight overestimation of Δv side-impact scenarios (Jurewicz et al., 2016). While such cases are not explicitly modelled within the current framework, this renders the derived risk estimates conservative.

5.3. MAIS rating

The Maximum Abbreviated Injury Scale (MAIS) is a globally recognised trauma severity index widely applied in vehicle collision injury assessment (Wang, 2022). It represents the highest Abbreviated Injury Scale (AIS) score sustained by a patient with multiple injuries. This study adopts the 2005 revision of the AIS, updated in 2008 (referred to as MAIS(05/08)), which remains a standard in injury severity analysis. To quantify the relationship between collision severity and injury outcomes, we utilise data from the NASS/CDS covering the years 2010 to 2015. In this dataset, the key severity metric, delta-V, is estimated using the WinSMASH crash reconstruction tool (Wang, 2022).

The AIS categorises injuries on a scale from 1 (minor) to 6 (maximum). MAIS corresponds to the most severe injury a person sustains in an accident. The report presents curves that estimate the likelihood of different MAIS level injuries as a function of delta-V, using logistic regression to model these probabilities. Due to sample size limitations for severe injuries, non-fatal MAIS 5 and MAIS 6 categories are combined, with fatalities designated as MAIS 6 and above. MAIS 3+ is widely considered the serious injury threshold and includes fatalities.

For a given delta-v value, near-side impacts (driver's side) are the most severe for occupants due to minimal protection from the vehicle body. Far-side impacts are less severe, benefiting from the empty crush zone to the left of the driver. Frontal impacts follow, where the engine compartment provides some protection, though the steering wheel poses a risk. Rear-end impacts are the least severe, thanks to the extensive and usually empty crush space behind the driver.

Fig. 6 depicts the MAIS+ curves for frontal and rear end crashes against Delta-V. The probability models are given in Appendix A. For example, given a delta-v value of 40 mph, the probabilistic MAIS+ values would be as given in Fig. 7 for frontal and rear-end crashes.

5.4. Safety impact rating mapping

The next step is to map the correlated delta-V to MAIS probabilities to a safety impact rating. For this, we take the direction from ISO 26262-3 (Road vehicles – Functional safety – Part 3: Concept phase), which provides a mapping from MAIS to safety ratings. However, the empirical equations developed and presented in the previous subsection are not sensitive enough to distinguish between S0 and S1 severity ratings. To address this, we turn to the literature for threshold delta-V speeds that can distinguish between S0 and S1. The remaining thresholds are based on the empirical method discussed in the previous section.

Table 4 presents a mapping between different scales used to rate the severity of impacts in vehicle collisions. The 'Impact rating/severity class' provides a general description ranging from 'Negligible' to 'Severe'. It is mapped against the ISO/SAE 21434: 2021 standard, which offers a structured classification of injury potential from no injuries (S0) to fatal injuries (S3). These classifications are compared to the MAIS rating, which quantifies injury severity from 0 (no injury) to 6 (maximum, untreatable injuries). This mapping serves as a reference for assessing vehicle impact severity across different standards and methodologies.

Table 5 provides the delta-V thresholds corresponding to each severity class, distinguishing between front-end and rear-end impacts. These thresholds serve as an operational output of the proposed framework, enabling users to estimate injury severity classes directly from known delta-V values. Threshold values for classes S2 and S3 are adapted from the NHTSA MAIS study, while the threshold for S1 is derived from prior literature (Khastgir et al., 2017; Sini and Violante, 2020). This classification scheme allows for risk categorisation in post-collision analysis where delta-V data are available.

5.5. Incident safety vector

The incident safety vector (I_S) is introduced to present a structured representation of the safety impact of a collision event by reporting the number of affected parties across each severity level. Severity is classified in accordance with the ISO/SAE 21434 safety impact rating. Each involved party in a crash is assigned a severity level based on the observed or estimated injury outcome. The overall safety impact of an incident is expressed as a severity distribution vector, structured as given in Eq. (14):

$$I_S = [S_3;\ S_2;\ S_1;\ S_0] \quad (14)$$

This representation captures both the extent and distribution of injury severity in a compact and scalable format, supporting both high-level comparisons and detailed risk evaluations. For an example, consider a two-vehicle collision where Vehicle 1 sustains moderate injuries (S1) and Vehicle 2 sustains major injuries (S2). The incident safety vector will be as shown in Eq. (15):

$$I_S = [S_3 : 0;\ S_2 : 1;\ S_1 : 1;\ S_0 : 0] \quad (15)$$

6. Scenarios

This section presents three illustrative scenarios used to demonstrate the proposed impact assessment frameworks. Scenario I involves a cyberthreat-induced cascading collision event on a multi-lane road and is evaluated using the safety impact assessment framework. Scenario II

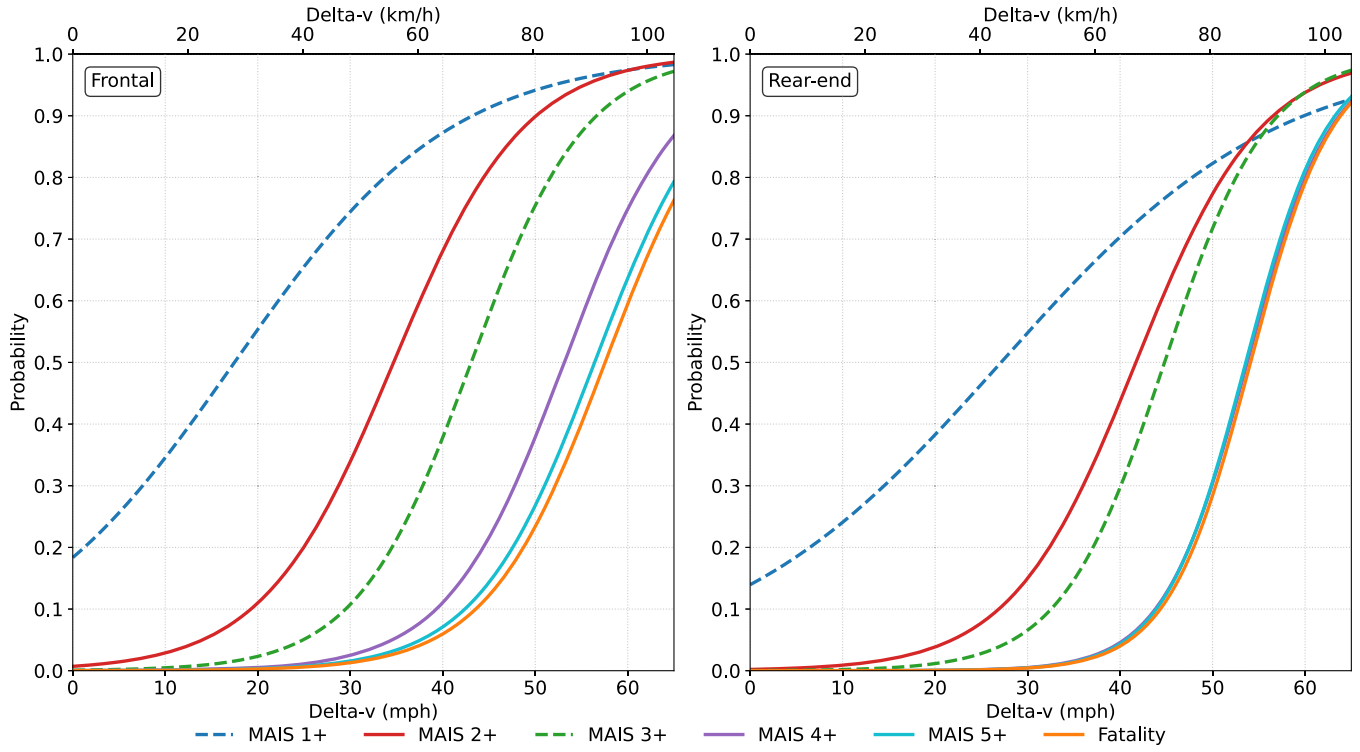

Fig. 6. MAIS+(05/08) injury probability curves for frontal (left) and rear-end (right) collisions as a function of delta-V. Adapted from Gennarelli and Wodzin (2008), Wang (2022).

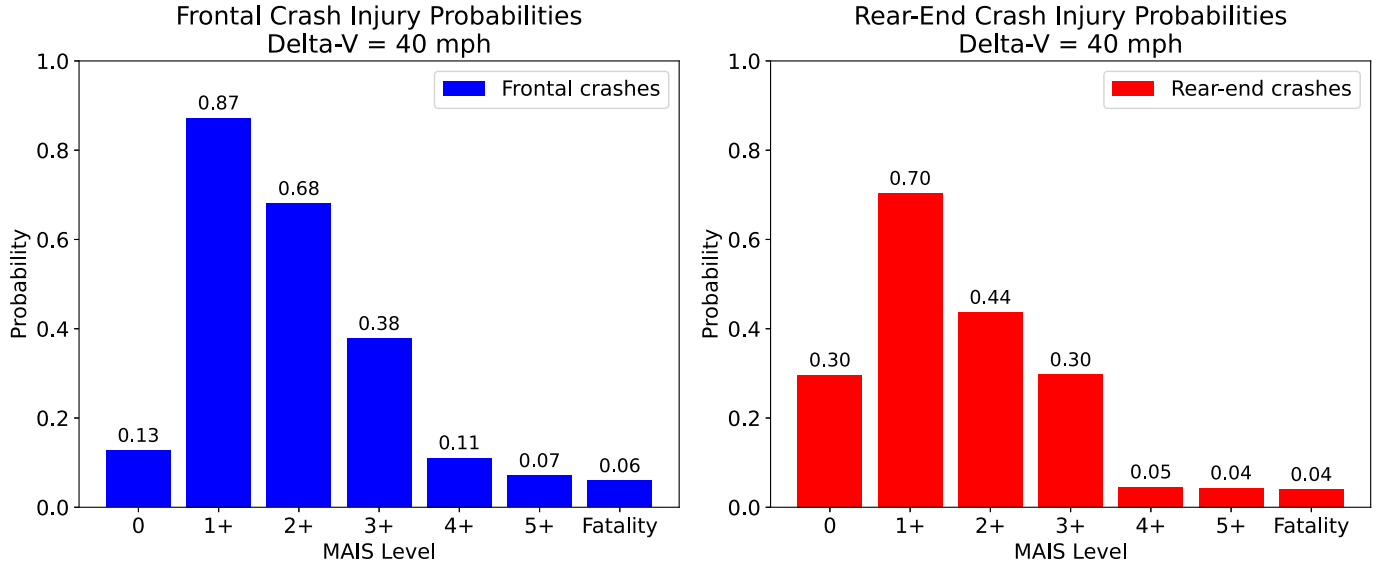

Fig. 7. Injury probability distribution at Delta-V of 40 mph for frontal and rear-end vehicle collisions. Severity levels follow the maximum abbreviated injury scale, where 0 = no injury, 1+ = MAIS 1 or higher, 2+ = MAIS 2 or higher, etc.

Table 4
Impact rating and severity classifications for safety impact assessment.

Impact rating / severity class	ISO/SAE 21434: 2021	MAIS threshold values
0: Negligible	S0: No injuries	< (0.1 MAIS1+)
1: Moderate	S1: Light and moderate injuries	> (0.1 MAIS1+)
2: Major	S2: Severe and life-threatening injuries (survival probable)	> (0.1 MAIS3+)
3: Severe	S3: Life-threatening injuries (survival uncertain), fatal injuries	> (0.1 MAIS5+)

Table 5
Severity class thresholds based on delta-V for front-end and rear-end collisions.

Severity Class		S0	S1	S2	S3
Delta-V Thresholds (km/h)	Front End	$\Delta V < 21$	$21 \leq \Delta V < 47$	$47 \leq \Delta V < 68$	$\Delta V \geq 68$
	Rear End	$\Delta V < 21$	$21 \leq \Delta V < 52$	$52 \leq \Delta V < 71$	$\Delta V \geq 71$

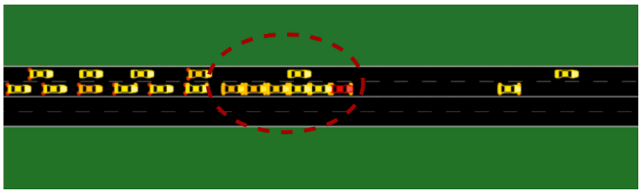

Fig. 8. Simulation of a cyber-induced sudden deceleration event leading to a multi-vehicle collision on a motorway, illustrating the propagation of secondary crashes due to traffic disruption.

examines a similar cyber threat, using real-world traffic and location data from the UK M25 motorway. Here, the operational impact assessment framework is applied. Scenario III explores a prospective attack leveraging compromised Roadside Units (RSUs) in a connected vehicle environment, also assessed using the operational impact framework.

6.1. Scenario I: telematics - cascading braking attack

This scenario examines the potential consequences of a cyberattack targeting the telematics unit of a connected vehicle, a critical asset responsible for vehicle-to-cloud communication. The telematics unit can be compromised through its cellular interface, which serves as a gateway for remote diagnostics, firmware updates, and fleet management functions. Once breached, this vulnerability allows an attacker to manipulate the vehicle's electronic control architecture, leading to systemic safety and operational risks across the transport network. This scenario highlights how a single compromised asset in a connected vehicle ecosystem can propagate threats, ultimately disrupting road safety and traffic efficiency (see Fig. 8).

Threat-vector mapping. This scenario represents a telematics/ECU compromise via the cellular path; in simulation we issue an emergency brake command to a single CV, while all other vehicles operate nominally.

The feasibility of such an attack has been demonstrated in real-world experiments. In 2015, Miller and Valasek remotely exploited a 2014 Jeep Cherokee by targeting its Uconnect telematics system over a cellular network (Common Vulnerabilities and Exposures, CVE-2015-5611; rated 8.3 "High" on the Common Vulnerability Scoring System, CVSS), enabling them to manipulate critical functions such as braking, acceleration, and steering (Miller and Valasek, 2015; Database, 2015; NVD, 2007).

Following the ISO/SAE 21434 framework, the telematics unit is identified as a high-value asset due to its integral role in vehicle connectivity. In this scenario, a threat vector is introduced where the cellular interface is exploited, granting unauthorised access to the gateway electronic control unit (ECU). This access allows the attacker to inject malicious control signals, leading to unintended acceleration or deceleration.

6.1.1. Scenario I: configuration

The attack scenario is modelled on a 70 mph motorway with flow rate of 1800 veh/h/l simulating a high traffic condition. The compromised vehicle induced to a rapid deceleration by activating emergency braking causing a cascading rear-end collision event. The simulation results, depicted in Fig. 9, show the speed profiles of the involved vehicles, illustrating the rapid deceleration of the attacked vehicle followed by sequential braking and collisions of surrounding vehicles. The cascading

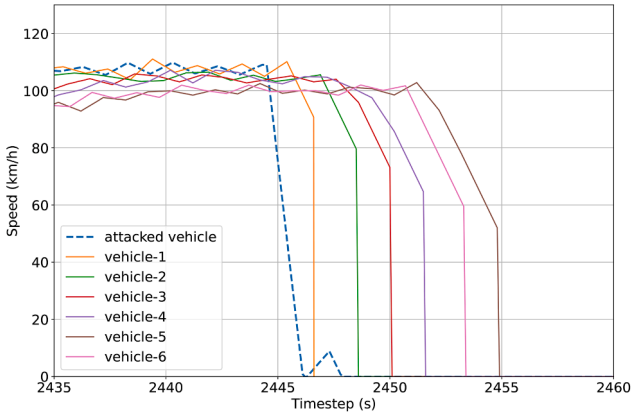

Fig. 9. Speed profiles of vehicles affected, illustrating the propagation of braking events leading to a multi-lane blockage.

nature of these collisions highlights the potential for multi-vehicle incidents in real-world traffic scenarios due to a cybersecurity compromise.

6.1.2. Scenario I: impact assessment results

The safety impact of the collision sequence was assessed using the safety impact assessment framework, which classifies collision severity and estimates injury risk probabilities. The quantitative results presented in Table 6 demonstrate that the attacked vehicle experienced a Delta-V of -92 km/h, with a probability of fatality of 0.66, classifying it under the S3 (Severe) safety impact rating. Additionally, the first impacted vehicle (vehicle 1) also exhibited a severe frontal collision with a Delta-V of 92 km/h, leading to a high fatality probability of 0.48. The subsequent vehicles in the chain collision exhibit progressively lower Delta-V values, resulting in lower severity classifications (S2: Major and S1: Moderate). The distribution of safety impact ratings across all affected vehicles in this scenario is summarised by the incident safety vector, Eq. (16):

$$I_S = [S_3 : 2;\ S_2 : 4;\ S_1 : 1;\ S_0 : 0] \tag{16}$$

Here, two vehicles are classified under S3 (Severe), four under S2 (Major), one under S1 (Moderate), and none under S0 (Negligible).

6.2. Scenario II: telematics - remote disabling attack

This scenario investigates a cyberattack similar to that in Scenario 1, in which multiple vehicles are disabled remotely; this time within a real-world motorway setting. Traffic data were sourced from WebTRIS (National Highways Traffic Data) (England, 2025), providing baseline flow rates reflective of actual operating conditions. Fig. 10 presents a geospatial overview of the modelled M25 segment between Junctions 27 and 28.

Threat-vector mapping. This stands in for a coordinated telematics immobiliser attack; we implement it by immobilising 1-3 CVs, pinned to their lanes, to emulate the loss of lane capacity and create a merge bottleneck.

6.2.1. Scenario II: configuration

The simulated section is a four-lane per direction, 70 mph segment of the M25 motorway. The analysis focuses on the weekday afternoon peak period (15:30–16:30), during which the recorded total

Table 6
Scenario I: Safety impact assessment data table.

Vehicle ID	Pre-collision speed (km/h)	Collision type	Delta-V (km/h)	Probability of Fatality	Safety impact rating
attacked vehicle	0	Rear end	-92	0.66	S3: Severe
vehicle 1	92	Frontal	92	0.48	S3: Severe
vehicle 2	79	Frontal	79	0.21	S2: Major
vehicle 3	74	Frontal	74	0.14	S2: Major
vehicle 4	64	Frontal	64	0.06	S2: Major
vehicle 5	60	Frontal	60	0.04	S2: Major
vehicle 6	51	Frontal	51	0.02	S1: Moderate

Table 7
Summary of operational impact across three attack cases in Scenario II. Each case reflects a different number of effective blocked lanes over a 3 km motorway segment during a 1 h window. Qualitative severity levels are mapped based on metric thresholds defined in the framework.

Case	Effective no. of blocked lanes	Operational impact vector string
Case 1	1	$[I_O]_{A=3km,T=1h;\omega=1} = [SR = 0.97(Negligible); FR = 1.00(Negligible); LOS_{C\to D}]$
Case 2	2	$[I_O]_{A=3km,T=1h;\omega=1} = [SR = 0.67(Moderate); FR = 0.94(Negligible); LOS_{C\to F}]$
Case 3	3	$[I_O]_{A=3km,T=1h;\omega=1} = [SR = 0.44(Major); FR = 0.59(Moderate); LOS_{C\to F}]$

Fig. 10. Simulation of a cyber-induced vehicle disabling attack on a section of the M25 motorway, illustrating the resulting congestion and disruption to traffic flow.

flow was 7167 veh/h. The cyberattack is modelled at the 3 km mark along the direction of travel from Junction 27 to Junction 28. To evaluate the operational impacts, three simulation configurations are considered, corresponding to the blockage of one, two, and three motorway lanes.

6.2.2. Scenario II: impact assessment results

The spatial assessment region comprises the 3 km upstream segment leading to the incident location, and the temporal assessment window is defined as 3600 s. The spatial zones (a_i) are taken as 100m, Δt_j as 300 s and ω as 1 since the spatial zones are homogeneous. The primary operational metrics, SR and FR, are computed for each configuration. To capture service quality degradation, the LOS is evaluated for both baseline and attack scenarios based on the US HCM methodology for urban freeways using density thresholds (Board, 2016).

The resultant operational impact vector strings for each case are summarised in Table 7. Fig. 11 illustrates the SR, FR, and LOS heatmaps for Case 2, demonstrating the spatial and temporal degradation in network performance.

The results indicate negligible to major impacts on vehicle speeds and negligible to moderate impacts on flow across the three configurations. In Cases 1 and 2, the motorway's high capacity and multi-lane geometry allow traffic to recover and reroute effectively, resulting in limited operational disruption. In contrast, Case 3 exhibits significant performance degradation, with the SR falling to 0.44 and LOS deteriorating from baseline LOS C to LOS F. These outcomes reflect the network's reduced ability to absorb disruptions under severe lane loss conditions.

6.3. Scenario III: RSU spoofing attack

This scenario simulates a futuristic cyber-physical attack in which a compromised Roadside Unit (RSU) disseminates deceptive messages to Connected and Automated Vehicles (CAVs) operating on a motorway segment equipped with Variable Speed Limit (VSL) control (see Fig. 12). RSUs are anticipated to play a critical role in V2I communication, serving as trusted broadcasters of traffic information to nearby vehicles (RSU Standardization Working Group, 2022). However, due to this trust relationship, a compromised RSU presents a significant attack vector (Abhishek et al., 2022; Dibaei et al., 2020a). Services such as In-Vehicle Signage (IVS) and speed advisories, which transmit digital updates and hazard alerts directly to vehicles, enhance driving safety but simultaneously introduce substantial cyber-physical risks (Autotalks, 2021).

The attack is modelled across four sequential 30 min phases. In Phases 1 to 3, the compromised RSU progressively reduces the broadcasted VSL from 70 mph to 50 mph, then to 40 mph, and finally to 30 mph. These spoofed advisories target CAVs exclusively, inducing unnecessary deceleration. In Phase 4, the RSU broadcasts phantom lane closure messages affecting the left lane, beginning at the midpoint of its service region. This causes CAVs to execute unilateral lane changes, concentrating flow into the right lane and further compounding congestion. Human-driven vehicles (HDVs) remain unaffected, operating under standard conditions.

Within the ISO 21434 TARA framework, this constitutes a downstream damage scenario, emerging from a successful cyberattack on a critical asset vulnerability; specifically, the V2I data communication channel. The scenario illustrates how spoofed infrastructure-originated messages, if not adequately filtered or validated by in-vehicle systems, can propagate through the functional communication chain (from the navigation ECU to vehicle actuators), leading to broader systemic traffic disruptions.

Threat-vector mapping. This represents RSU credential misuse/misconfiguration; the manipulated variables are the time-varying VSL profile and a lane-closure flag applied to CAVs, under an assumed 100 % CAV compliance; HDVs remain unaffected.

6.3.1. Scenario III: configuration

The simulated environment consists of a two-lane per direction, 70 mph motorway segment of total length 5 km. This includes a 1 km feeder section, 2 km upstream section, a 1 km incident section (corresponding to the compromised RSU broadcast range), and a 1 km downstream section. Three configurations of CAV penetration rate (PR) are evaluated: 20 %, 40 %, and 60 %. The traffic flow rate is fixed at

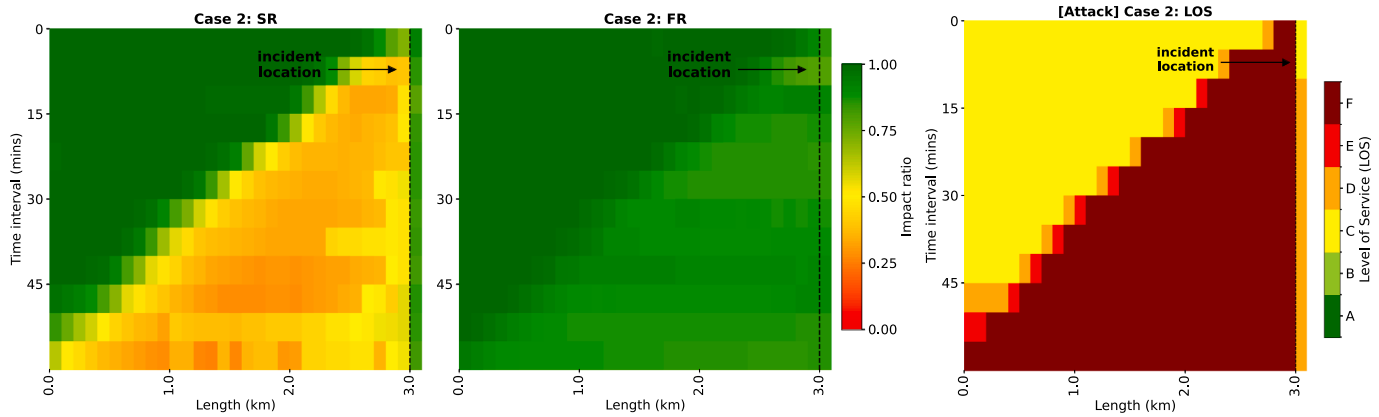

Fig. 11. Heatmaps of SR, FR and LOS of Case 2, Scenario II, illustrating the spatial and temporal degradation in traffic flow due to a cyber-induced disruption.

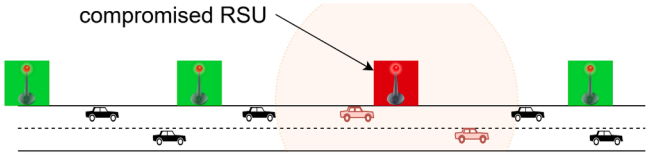

Fig. 12. Attack scenario showing compromised RSU affecting motorway traffic.

Table 8
Operational impact across three cases in scenario III - Incident region within RSU broadcast range.

CAV PR	Operational impact vector string
20 %	$[I_O]_{A=1km,T=2h;\omega=1} = [SR = 0.69(Moderate); FR = 1.00(Negligible); LOS_{C\to D}]$
40 %	$[I_O]_{A=1km,T=2h;\omega=1} = [SR = 0.61(Moderate); FR = 0.99(Negligible); LOS_{C\to E}]$
60 %	$[I_O]_{A=1km,T=2h;\omega=1} = [SR = 0.58(Moderate); FR = 0.93(Negligible); LOS_{C\to E}]$

Table 9
Operational impact across three cases in scenario III - Incident region and upstream region.

CAV PR	Operational impact vector string
20 %	$[I_O]_{A=3km,T=2h;\omega=1} = [SR = 0.89(Negligible); FR = 1.00(Negligible); LOS_{C\to C}]$
40 %	$[I_O]_{A=3km,T=2h;\omega=1} = [SR = 0.86(Negligible); FR = 0.98(Negligible); LOS_{C\to D}]$
60 %	$[I_O]_{A=3km,T=2h;\omega=1} = [SR = 0.79(Negligible); FR = 0.96(Negligible); LOS_{C\to E}]$

1250 veh/h/l, representing a typical medium-flow condition with a baseline LOS of C. CAVs are modelled using the CACC car-following model (Xiao et al., 2017).

6.3.2. Scenario III: impact assessment results

The spatial assessment region is defined as 1 km for the incident area and 3 km for the combined incident and upstream region. Spatial zones (a_i) are set to 100 m intervals, with a temporal resolution $\Delta t_j = 300$ s. The resultant operational impact vectors for each case are summarised in Tables 8 and 9. Fig. 13 presents heatmaps for the SR, FR, and LOS for the 60 % PR case, capturing the spatial-temporal propagation of the disruption.

The results show that the incident region experiences more severe degradation than the upstream region, as expected due to its proximity to the compromised RSU. Additionally, the impact intensifies with higher CAV penetration rates, both in severity and in the spatial extent of upstream propagation. This scenario illustrates a critical cybersecurity vulnerability in future connected vehicle ecosystems. While current vehicle fleets are not fully reliant on RSUs, the increasing deployment of V2X-enabled CAVs may expose systems to such attacks, especially where infrastructure-based advisories are prioritised over onboard decision-making.

Table 10
Operational impact across three demand traffic flow values in scenario III at 60 % CAV PR- Incident region.

Demand flow	Operational impact vector string
500 veh/h/l	$[I_O]_{A=1km,T=2h;\omega=1} = [SR = 0.64(Moderate); FR = 1.00(Negligible); LOS_{A\to B}]$
1250 veh/h/l	$[I_O]_{A=1km,T=2h;\omega=1} = [SR = 0.58(Moderate); FR = 0.93(Negligible); LOS_{C\to E}]$
2000 veh/h/l	$[I_O]_{A=1km,T=2h;\omega=1} = [SR = 0.52(Moderate); FR = 0.86(Negligible); LOS_{E\to F}]$

6.4. Sensitivity analysis

To evaluate the sensitivity of the primary operational metrics (SR, FR) and LOS to traffic demand levels, additional experiments were conducted with demand flows of 500, 1250, and 2000 veh/h/l. These correspond to increasing traffic densities with baseline LOS values of A, C, and E, respectively, while all other parameters were held constant. Table 10 summarises the results, showing the progressive degradation of SR, FR, and LOS with higher demand.

7. Discussion

The systemic impact assessment framework proposed in this study is agnostic to the cyber kill-chain; it consumes manipulated operational variables (e.g., commanded deceleration, VSL profile) and returns systemic impact metrics. This decoupling helps keep TARA updates tractable as new vectors emerge. Other vectors (e.g., V2V spoofing/jamming, GPS spoofing) would enter the framework via equivalent manipulated variables (e.g., stochastic emergency-brake probability; spatial/time bias); their full exploration is left to future work.

7.1. Comparative positioning to ISO/SAE 21434 TARA

Our framework complements the ISO/SAE 21434 process by sitting downstream of threat identification and feasibility analysis. Given a defined damage scenario, it returns quantitative, baseline-normalised operational metrics (SR, FR, LOS) and Δv-derived safety classes from a systemic perspective. The mapping from these outputs to an organisation's severity labels is an external layer, so assessors can consume our results without altering existing workflows (see Fig. 1).

For Scenario I we report the incident safety vector I_S (Eq. (16)). For Scenarios II–III we report the operational impact vectors $[I_O]_{A,T,\omega}$ (SR/FR with LOS) relative to baseline. The framework thus extends the impact rating step from item-level judgement to system-level measurement, without altering21434's likelihood/feasibility workflow.

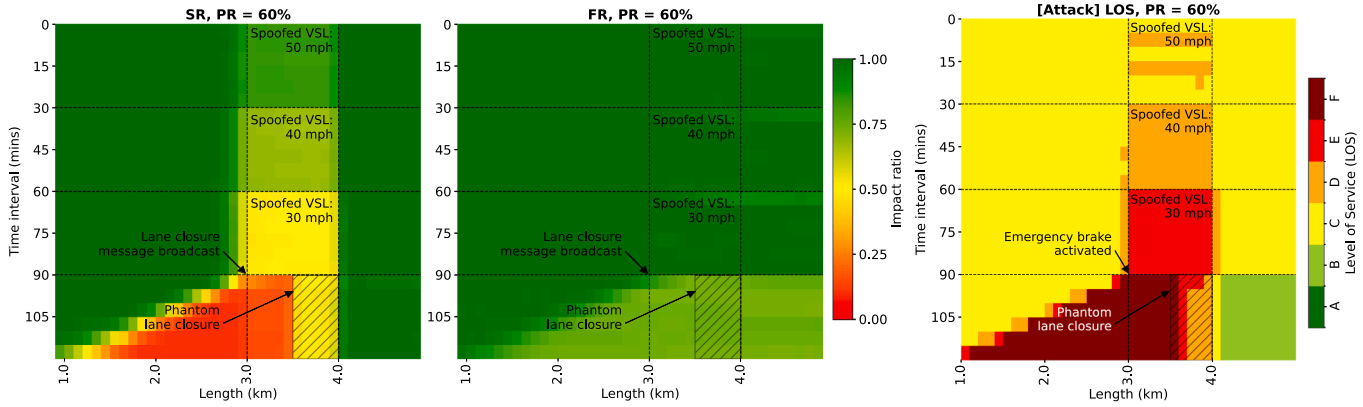

Fig. 13. Heatmaps of SR, FR, and LOS for Scenario 3 (PR = 60 %), illustrating spatial and temporal degradation in traffic flow due to a cyber-induced disruption.

Table 11
Simulation runtime summary. Runtimes are wall-clock times on Intel Xeon W-2125, SUMO (GUI off).

Scenario / Config	Network (km)	Demand (veh/h/l)	Assessment window T (s)	Simulated duration‡ (per run) (s)	Runtime per seed† (median [IQR]) (min)
I	5.5 (2 lanes)	1800	–	3600	**20.6 [19.3–20.9]**
II: Case 1					**37.6 [35.9 - 38.6]**
II: Case 2	13.0 (4 lanes)	1792	3600	600 + 3600	**49.1 [47.9 - 49.9]**
II: Case 3					**58.5 [58.1 - 58.7]**
III: PR 20 %					**22.8 [22.0 - 23.4]**
III: PR 40 %	5.0 (2 lanes)	1250	7200	600 + 7200	**37.7 [36.5 - 38.4]**
III: PR 60 %					**49.2 [47.7 - 50.1]**

‡ Simulated duration per run = warm-up + assessment window T; warm-up populates demand.
† Per seed = baseline run + attack run (combined wall time).

7.2. Simulation runtimes and scalability

Table 11 presents per-seed runtimes with sequential execution of the scenarios on a dedicated workstation (Intel® Xeon® W-2125 @ 4.00 GHz, 32 GB RAM, Ubuntu 24.04). The simulation step length for all experiments was 0.1 s. The experiments were executed sequentially across seeds, and the runtimes reflect network size, simulated duration, and scenario complexity. The current experiments imposed a light computational load, indicating that larger networks can be accommodated within the same framework using SUMO without fundamental changes to the workflow.

7.3. Validation

The framework quantifies potential systemic impacts conditional on a successful cyber attack to support existing TARA processes. Accordingly, the framework is validated at three levels. (i) At the framework level, primary operational metrics (SR, FR) are defined as ratios normalised to each scenario's baseline, and supplementary metric LOS is interpreted based on standard HCM guidelines. This anchors the outputs to accepted operational constructs independent of any singular network. For safety impact assessment, Δv is mapped to safety severity classes using published empirical relationships and ISO 26262 classifications. (ii) At the implementation level, the SUMO microsimulator is widely used in transport research and is established for reproducing key traffic phenomena; our setup follows standard practice (simulation step size, car-following and lane-change models). (iii) At the instantiation level (Scenario II), baseline flows/speeds are reproduced within the observed WebTRIS ranges for the assessment period. This anchors the baseline reference state to site conditions before we report relative degradation via SR/FR and LOS.

Given the limited availability of ground-truth cyber-incident impact data, the framework is designed to be readily calibratable when such data are available. With field or test-bed data, standard parameters can be tuned: (a) *traffic/network*: demand levels, route splits, road geometry, control plans; (b) *microscopic behaviour*: car-following/lane-change parameters and CAV compliance; (c) *attack/disruption*: onset timing, clearance duration, RSU scope.

7.4. Limitations

The following limitations are noted within the current work:
Compliance variability: In the present study, message compliance is treated implicitly and, for CAVs, effectively deterministic within the spoofed-zone logic. In practice, compliance may vary across drivers, OEM designs, and context (message salience, enforcement image, trust in the source).
Risk perception and avoidance: Vehicles' adaptation to perceived risk through manoeuvres such as earlier braking, longer headways, and conservative lane changes and CAVs risk-aware fall-back modes are not explicitly modelled.
Delta-v calculation: For post-impact kinematics we adopt a plastic-impact approximation (COR, $e = 0$) along the line of impact to keep the safety pipeline simple and reproducible. In the one-dimensional normal component, the change in velocity scales as $\Delta v(e) = (1 + e)\,\Delta v|_{e=0}$. This assumption is conservative at motorway-relevant speeds, where restitution values tend to be very small, but it may underestimate Δv for lower-speed impacts where partial rebound occurs. The framework can be adjusted by scaling with $(1 + e)$ if site-specific restitution values are available.

8. Conclusions and future work

This study presents a systematic framework for assessing the systemic impacts of cyber threats on connected vehicles. By integrating operational and safety impact assessments, the proposed methodology

offers a structured and quantifiable approach to evaluating the impacts of cyber incidents. Through the use of simulation-based assessment, we demonstrate how impacts can significantly affect mobility and safety. The findings highlight the importance of accounting for systemic risks beyond individual vehicle vulnerabilities, extending traditional risk assessment approaches like ISO/SAE 21434 to incorporate broader transport network implications.

The case studies illustrate the applicability of the framework in quantifying the severity of cyber-induced incidents. In the first scenario, a telematics-based attack led to a multi-vehicle collision with severe safety consequences, while the second and third scenarios demonstrated the systemic operational impact of telematics and RSU-based attacks on motorway traffic flow. These results underscore the need for proactive cybersecurity measures that consider not only vehicle-level risks but also network-wide disruptions.

The framework's baseline-normalised operational metrics (SR, FR, LOS) and incident safety vector (I_S) provide decision-ready evidence for road authorities and operators. Beyond TARA integration, the same metrics are relevant to defining autonomous-vehicle Operational Design Domains (ODDs): scenario sweeps across facility types, demand levels, and CAV penetration can delineate operating envelopes under acceptable risk, supporting evidence-based ODD entry/exit criteria and geofencing policies. Thresholds (e.g., SR<0.7 or a ≥2-class LOS drop within a defined (A,T) window) can be used to trigger lane control, diversions, or hard-shoulder use; $[I_O]_{AT,\omega}$ and I_S further inform incident response planning, resource sizing, and post-incident debriefs with reproducible metrics.

The framework outputs translate directly into cyber-resilience practice. For example, scenario sweeps across facility type, demand, and CAV penetration highlight where impacts are most pronounced (e.g., in Scenario III, spoofed VSL advisories drive LOS to F under higher demand), guiding targeted hardening (e.g., RSU authentication and monitoring on links with the largest SR/FR degradation) and resource pre-positioning. Finally, baseline-normalised histories allow like-for-like after-action comparisons across corridors and periods; the resulting thresholds and compliance parameters feed back into connected-infrastructure implementation policies and ODD/geofencing updates.

As connected vehicle technologies continue to evolve, the methodologies developed in this study can serve as a foundation for enhancing cyber resilience in next-generation connected vehicles. By providing a comprehensive and quantifiable approach to evaluating cyber threats in connected vehicle networks, this research contributes to the growing body of knowledge in automotive cybersecurity. It supports policymakers, transport authorities, and industry stakeholders in making informed decisions to enhance the security, safety, and operational resilience of future transportation infrastructures.

In future work, we plan to expand the simulation framework to include a broader range of cyber-attack vectors and transport environments, such as complex urban networks and mixed traffic scenarios involving autonomous, connected, and conventional vehicles. Incorporating attack scenarios that target signalised intersections, V2X-based routing mechanisms, and public transport systems would improve scenario diversity and practical relevance. Finally, a key research direction lies in coupling impact assessment with attack feasibility analysis to enable quantified cyber risk estimation framework for connected vehicle ecosystems.

CRediT authorship contribution statement

Don Nalin Dharshana Jayaratne: Writing – original draft, Visualization, Methodology, Conceptualization; **Qian Lu:** Writing – review & editing, Supervision, Conceptualization; **Abdur Rakib:** Writing – review & editing, Supervision, Conceptualization; **Muhamad Azfar Ramli:** Writing – review & editing, Supervision, Conceptualization; **Rakhi Manohar Mepparambath:** Writing – review & editing, Supervision, Conceptualization; **Siraj Ahmed Shaikh:** Writing – review & editing, Conceptualization; **Hoang Nga Nguyen:** Writing – review & editing, Conceptualization.

Data availability

No data was used for the research described in the article.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

This work was supported by Coventry University, UK and the A*STAR Research Attachment Programme (ARAP), Singapore.

Appendix A. MAIS probability model

Table A.1 gives the MAIS functions.

Table A.1
MAIS levels and probability curves by crash type (Wang, 2022).

MAIS Level	Frontal	Rear End
MAIS 0	$p(D) = 1 - \frac{e^{-1.4930+0.0854\cdot D}}{1+e^{-1.4930+0.0854\cdot D}}$	$p(D) = 1 - \frac{e^{-1.8199+0.0671\cdot D}}{1+e^{-1.8199+0.0671\cdot D}}$
MAIS 1+	$p(D) = \frac{e^{-1.4930+0.0854\cdot D}}{1+e^{-1.4930+0.0854\cdot D}} - \frac{e^{-4.9429+0.1425\cdot D}}{1+e^{-4.9429+0.1425\cdot D}}$	$p(D) = \frac{e^{-1.8199+0.0671\cdot D}}{1+e^{-1.8199+0.0671\cdot D}} - \frac{e^{-6.1818+0.1482\cdot D}}{1+e^{-6.1818+0.1482\cdot D}}$
MAIS 2+	$p(D) = \frac{e^{-4.9429+0.1425\cdot D}}{1+e^{-4.9429+0.1425\cdot D}} - \frac{e^{-6.9774+0.1620\cdot D}}{1+e^{-6.9774+0.1620\cdot D}}$	$p(D) = \frac{e^{-6.1818+0.1482\cdot D}}{1+e^{-6.1818+0.1482\cdot D}} - \frac{e^{-8.0329+0.1793\cdot D}}{1+e^{-8.0329+0.1793\cdot D}}$
MAIS 3+	$p(D) = \frac{e^{-6.9774+0.1620\cdot D}}{1+e^{-6.9774+0.1620\cdot D}} - \frac{e^{-8.4254+0.1586\cdot D}}{1+e^{-8.4254+0.1586\cdot D}}$	$p(D) = \frac{e^{-8.0329+0.1793\cdot D}}{1+e^{-8.0329+0.1793\cdot D}} - \frac{e^{-11.8787+0.2210\cdot D}}{1+e^{-11.8787+0.2210\cdot D}}$
MAIS 4+	$p(D) = \frac{e^{-8.4254+0.1586\cdot D}}{1+e^{-8.4254+0.1586\cdot D}} - \frac{e^{-8.8355+0.1566\cdot D}}{1+e^{-8.8355+0.1566\cdot D}}$	$p(D) = \frac{e^{-11.8787+0.2210\cdot D}}{1+e^{-11.8787+0.2210\cdot D}} - \frac{e^{-12.1944+0.2276\cdot D}}{1+e^{-12.1944+0.2276\cdot D}}$
MAIS 5+	$p(D) = \frac{e^{-8.8355+0.1566\cdot D}}{1+e^{-8.8355+0.1566\cdot D}} - \frac{e^{-9.0422+0.1571\cdot D}}{1+e^{-9.0422+0.1571\cdot D}}$	$p(D) = \frac{e^{-12.1944+0.2276\cdot D}}{1+e^{-12.1944+0.2276\cdot D}} - \frac{e^{-12.1982+0.2255\cdot D}}{1+e^{-12.1982+0.2255\cdot D}}$
Fatality	$p(D) = \frac{e^{-9.0422+0.1571\cdot D}}{1+e^{-9.0422+0.1571\cdot D}}$	$p(D) = \frac{e^{-12.1982+0.2255\cdot D}}{1+e^{-12.1982+0.2255\cdot D}}$

References

Abhishek, N.V., Aman, M.N., Lim, T.J., Sikdar, B., 2022. DRiVe: detecting malicious roadside units in the internet of vehicles with low latency data integrity. IEEE Internet Things J. 9 (5), 3270–3281. https://doi.org/10.1109/JIOT.2021.3097809

Autotalks, 2021. V2X Infrastructure for safety. Technical Report. https://auto-talks.com/wp-content/uploads/2021/07/V2X-Infrastructure-for-Safety-RSU.pdf.

Bahouth, G., Graygo, J., Digges, K., Schulman, C., Baur, P., 2014. Traffic injury prevention the benefits and tradeoffs for varied high-severity injury risk thresholds for advanced automatic crash notification systems https://doi.org/10.1080/15389588.2014.936011

Bahouth, G., Schulman, K.C., 2012. Influence of injury risk thresholds on the performance of an algorithm to predict crashes with serious injuries. In: 56th AAAM Annual Conference Annals of Advances in Automotive Medicine, pp. 223–230.

Benyahya, M., Collen, A., Lenard, T., Nijdam, N.A., 2025. TARA 2.0 for connected and automated vehicles. IEEE Trans. Intell. Transp. Syst.. https://doi.org/10.1109/TITS.2025.3574638

Board, T.R., 2016. Highway capacity manual, sixth edition: a guide for multimodal mobility analysis. Technical Report. https://www.trb.org/Main/Blurbs/175169.aspx.

Boi, B., Gupta, T., Rinhel, M., Jubea, I., Khondoker, R., Esposito, C., Sousa, B.M., 2023. Strengthening automotive cybersecurity: a comparative analysis of ISO/SAE 21434-compliant automatic collision notification (ACN) systems. Vehicles 5 (4), 1760–1802. https://doi.org/10.3390/vehicles5040096

Carlson, W.L., 1979. Crash injury prediction model. Accid. Anal. Prev. 11 (2), 137–153.

Centre for Connected and Autonomous Vehicles, 2020. Innovation is great: connected and automated vehicles. https://assets.publishing.service.gov.uk/media/5f969cd98fa8f543ef5c3195/innovation-is-great-connected-and-automated-vehicles-booklet.pdf.

Chowdhury, A., Karmakar, G., Kamruzzaman, J., Jolfaei, A., Das, R., 2020. Attacks on self-driving cars and their countermeasures: a survey. IEEE Access 8 207308–207342. https://doi.org/10.1109/ACCESS.2020.3037705

Colombo, D., 2022. How I got access to 25+ Tesla's around the world. By accident. and curiosity. | by David Colombo | Medium. https://medium.com/@david_colombo/how-i-got-access-to-25-teslas-around-the-world-by-accident-and-curiosity-8b9ef040a028.

Costantino, G., Matteucci, I., 2022. Reversing Kia motors head unit to discover and exploit software vulnerabilities. J. Comput. Virol Hacking Tech. 19 (1), 33–49. https://doi.org/10.1007/s11416-022-00430-5

Curry, S., 2023. Web hackers vs. the auto industry: critical vulnerabilities in Ferrari, BMW, Rolls Royce, Porsche, and more. https://samcurry.net/web-hackers-vs-the-auto-industry.

Das, P., Asif, M.R.A., Jahan, S., Ahmed, K., Bui, F.M., Khondoker, R., 2024. STRIDE-based cybersecurity threat modeling, risk assessment and treatment of an in-vehicle infotainment system. Vehicles 6 (3), 1140–1163. https://doi.org/10.3390/vehicles6030054

Database, N.V., 2015. NVD - CVE-2015-5611. https://nvd.nist.gov/vuln/detail/CVE-2015-5611#vulnCurrentDescriptionTitle.

Deka, L., Khan, S.M., Chowdhury, M., Ayres, N., 2018. Transportation Cyber-Physical System and its Importance for Future Mobility. Elsevier Inc. https://doi.org/10.1016/B978-0-12-814295-0.00001-0

Della Monica, U., Munjal, K.A., Tamas, M.P., Boi, B., Esposito, C., Khondoker, R., 2025. Threat analysis and risk assessment (TARA) analysis of an autonomous emergency braking (AEB) system. Appl. Sci. 15 (3). https://doi.org/10.3390/app15031400

Di Maio, F., Mascherona, R., Zio, E., 2019. Risk analysis of cyber-physical systems by GTST-MLD. IEEE Syst. J. 14 (1), 1333–1340.

Dibaei, M., Zheng, X., Jiang, K., Abbas, R., Liu, S., Zhang, Y., Xiang, Y., Yu, S., 2020a. Attacks and defences on intelligent connected vehicles: a survey. Digital Commun. Netw. 6 (4), 399–421. https://doi.org/10.1016/j.dcan.2020.04.007

Dong, C., Wang, H., Ni, D., Liu, Y., Chen, Q., 2020. Impact evaluation of cyber-attacks on traffic flow of connected and automated vehicles. https://doi.org/10.1109/ACCESS.2020.2993254

Elvik, R., 2013. A re-parameterisation of the power model of the relationship between the speed of traffic and the number of accidents and accident victims. Accid. Anal. Prev. 50, 854–860. https://doi.org/10.1016/j.aap.2012.07.012

England, H., 2025. National highways - WebTRIS - map view. https://webtris.nationalhighways.co.uk/.

EVITA, 2009. Deliverable 2.3: security requirements for automotive on-board networks based on dark-side scenarios. Technical Report.

Gennarelli, T.A., Wodzin, E., 2008. Abbreviated Injury Scale (AIS) 2005 – Update 2008. Association for the Advancement of Automotive Medicine.

Gordon, A., 2022. Hackers create traffic jam in Moscow by ordering dozens of taxis at once through app. https://www.vice.com/en/article/y3pbgy/hackers-create-traffic-jam-in-moscow-by-ordering-dozens-of-taxis-at-once-through-app.

He, F., Yan, X., Liu, Y., Ma, L., 2016. A traffic congestion assessment method for urban road networks based on speed performance index. Procedia Eng. 137, 425–433. https://doi.org/10.1016/j.proeng.2016.01.277

Jayaratne, D. N.D., Kamtam, S.H., Shaikh, S.A., Ramli, M.A., Lu, Q., Mepparambath, R.M., Nguyen, H.N., Rakib, A., 2024. A simulation framework for automotive cybersecurity risk assessment. Simul. Modell. Pract. Theory 136, 103005. https://doi.org/10.1016/j.simpat.2024.103005

Jayaratne, D. N.D., Lu, Q., Rakib, A., Ramli, M.A., Mepparambath, R.M., Shaikh, S.A., Nguyen, H.N., Kamtam, S.H., 2025. The threat landscape of connected vehicles. In: Jahankhani, H., Issac, B. (Eds.), Cybersecurity and Human Capabilities through Symbiotic Artificial Intelligence. Springer Nature Switzerland, Cham, pp. 227–247. https://doi.org/10.1007/978-3-031-82031-1_13

Ji, X., Cheng, Y., Zhang, Y., Wang, K., Yan, C., Xu, W., Fu, K., 2021. Poltergeist: acoustic adversarial machine learning against cameras and computer vision. In: Proceedings - IEEE Symposium on Security and Privacy 2021-May, 160–175. https://doi.org/10.1109/SP40001.2021.00091

Joksch, H.C., 1993. Velocity change and fatality risk in a crash–a rule of thumb. Accid. Anal. Prev. 25, 103–104. https://doi.org/10.1016/0001-4575(93)90102-3

Joseph, A.D., 2006. Intelligent Transportation Systems. Vol. 5. https://doi.org/10.1109/MPRV.2006.77

Jurewicz, C., Sobhani, A., Woolley, J., Dutschke, J., Corben, B., 2016. Exploration of vehicle impact speed – injury severity relationships for application in safer road design. Transp. Res. Procedia 14, 4247–4256. https://doi.org/10.1016/j.trpro.2016.05.396

Karbasi, A., O'Hern, S., 2022. Investigating the impact of connected and automated vehicles on signalized and unsignalized intersections safety in mixed traffic. Future Transp. 2022 2 (1), 24–40. https://doi.org/10.3390/FUTURETRANSP2010002

Khastgir, S., Birrell, S., Dhadyalla, G., Sivencrona, H., Jennings, P., 2017. Towards increased reliability by objectification of hazard analysis and risk assessment (HARA) of automated automotive systems. Saf. Sci. 99, 166–177. https://doi.org/10.1016/j.ssci.2017.03.024

Krauß, S., 1998. Microscopic modeling of traffic flow: investigation of collision free vehicle dynamics. D L R - Forschungsberichte, 116.

Kriaa, S., Bouissou, M., Laarouchi, Y., 2015. SCADA safety and security joint modeling (S-cube): case study of a dam. In: Proceedings of the 22th Computer & Electronics Security Applications Rendez-vous (C&ESAR'2015) , 55–69.

Kulandaivel, S., Jain, S., Guajardo, J., Sekar, V., 2021. CANNON: reliable and stealthy remote shutdown attacks via unaltered automotive microcontrollers. In: Proceedings - IEEE Symposium on Security and Privacy 2021-May, 195–210. https://doi.org/10.1109/SP40001.2021.00122

Lab, T. S.K., 2021. Mercedes Benz security research report. Technical Report. https://keenlab.tencent.com/en/whitepapers/Mercedes_Benz_Security_Research_Report_Final.pdf.

Lamssaggad, A., Benamar, N., Hafid, A.S., Msahli, M., 2021. A survey on the current security landscape of intelligent transportation systems. IEEE Access 9 9180–9208. https://doi.org/10.1109/ACCESS.2021.3050038

Lautenbach, A., Mafijul Islam, C., 2016. Heavens-healing vulnerabilities to enhance software security and safety Dnr 2012-04625 document title security models project title healing vulnerabilities to enhance software security and safety. Technical Report.

Lopez, P.A., Behrisch, M., Bieker-Walz, L., Erdmann, J., Flotterod, Y.P., Hilbrich, R., Lucken, L., Rummel, J., Wagner, P., Wiebner, E., 2018. Microscopic traffic simulation using SUMO. In: IEEE Conference on Intelligent Transportation Systems, Proceedings, ITSC 2018-Novem, 2575–2582. https://doi.org/10.1109/ITSC.2018.8569938

Luo, F., Jiang, Y., Zhang, Z., Ren, Y., Hou, S., 2021. Threat analysis and risk assessment for connected vehicles: a survey. https://doi.org/10.1155/2021/1263820

Macher, G., Sporer, H., Berlach, R., Armengaud, E., Kreiner, C., 2015. SAHARA: a security-aware hazard and risk analysis method. In: Proceedings -Design, Automation and Test in Europe, DATE 2015-April, 621–624. https://doi.org/10.7873/DATE.2015.0622

Manuel, S., 2022. UN regulation No 155 & how to comply? What you need to know. https://www.cyres-consulting.com/un-regulation-no-155-requirements-what-you-need-to-know/.

Miller, C., Valasek, C., 2015. Remote exploitation of an unaltered passenger vehicle. Technical Report. http://illmatics.com/RemoteCarHacking.pdf.

Miqdady, T., De Ona, R., Casas, J., De Ona, J., 2023. Studying traffic safety during the transition period between manual driving and autonomous driving: a simulation-based approach. IEEE Trans. Intell. Transp. Syst. 24 (6), 6690–6710. https://doi.org/10.1109/TITS.2023.3241970

Monteuuis, J.-P., Boudguiga, A., Zhang, J., Labiod, H., Servel, A., Urien, P., 2018. SARA. In: Proceedings of the 4th ACM Workshop on Cyber-Physical System Security. ACM, New York, NY, USA, pp. 3–14. https://doi.org/10.1145/3198458.3198465

Neades, J., Smith, R., 2011. The determination of vehicle speeds from Delta-V in two vehicle planar collisions. In: Proceedings of the Institution of Mechanical Engineers, Part D: Journal of Automobile Engineering, pp. 43–53.

Nie, S., Liu, L., Du, Y., 2016. Free-Fall: Hacking Tesla from Wireless to Can Bus. Technical Report. https://www.blackhat.com/docs/us-17/thursday/us-17-Nie-Free-Fall-Hacking-Tesla-From-Wireless-To-CAN-Bus-wp.pdf.

NVD, 2007. NVD - CVSS v2.0 calculator. https://nvd.nist.gov/vuln-metrics/cvss/v2-calculator?name=CVE-2015-5611&vector=(AV:A/AC:L/Au:N/C:C/I:C/A:C)&version=2.0&source=NIST.

Organisation, I.S., 2018. ISO 26262-3 Road Vehicles -Functional Safety - Part 3: Concept Phase. Technical Report.

Perallos, A., Hernandez-Jayo, U., Onieva, E., García-Zuazola, I.J., 2013. Intelligent Transport Systems: Technologies and Applications. https://doi.org/10.1002/9781118557495.ch6

Pièrre-Cambacédès, L., Bouissou, M., 2010. Beyond attack trees: dynamic security modeling with Boolean logic driven Markov processes (BDMP). In: 2010 European Dependable Computing Conference, pp. 199–208.

Plappert, C., Zelle, D., Gadacz, H., Rieke, R., Scheuermann, D., Kraus, C., 2021. Attack surface assessment for cybersecurity engineering in the automotive domain. In: 2021 29th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP). IEEE, pp. 266–275. https://ieeexplore.ieee.org/document/9407241/. https://doi.org/10.1109/PDP52278.2021.00050

Rahman, M.H., Abdel-Aty, M., Wu, Y., 2021. A multi-vehicle communication system to assess the safety and mobility of connected and automated vehicles. Transp. Res. Part C Emerging Technol. 124. https://doi.org/10.1016/j.trc.2020.102887

Rose, N.A., Fenton, S.J., Beauchamp, G., 2006. Restitution modeling for crush analysis: theory and validation. SAE Technical Paper. https://doi.org/10.4271/2006-01-0908

RSU Standardization Working Group, 2022. Roadside Unit (RSU) Standard. The United States Department of Transportation (USDOT). SAE Technical Report. https://www.ite.org/pub/?id=9406F15D-F384-B5E3-9653-9AF6E6057471.

Sadid, H., Antoniou, C., 2023. Modelling and simulation of (connected) autonomous vehicles longitudinal driving behavior: a state-of-the-art. IET Intell. Transp. Syst. 17 (6), 1051–1071. https://doi.org/10.1049/ITR2.12337

SAE, 2010. J1711 Surface Vehicle Recommended Practice. Technical Report. http://papers3://publication/uuid/ECB5448C-F3D8-414A-A46E-857726E32846.

Saulaiman, M. N.-E., Kozlovszky, M., Csilling, A., 2025. Graph-based automation of threat analysis and risk assessment for automotive security. Information 16 (6), 449. https://doi.org/10.3390/INFO16060449

Shelby, S.G., 2011. DELTA-V as a measure of traffic conflict severity. In: 3rd International Conference on Road Safety and Simulation, pp. 14–16.

Shladover, S.E., 2018. Connected and automated vehicle systems: introduction and overview. J. Intell. Transp. Syst. Technol. Plann. Oper. 22 (3), 190–200. https://doi.org/10.1080/15472450.2017.1336053

Sini, J., Violante, M., 2020. A simulation-based methodology for aiding advanced driver assistance systems hazard analysis and risk assessment https://doi.org/10.1016/j.microrel.2020.113661

Sommer, C., Eckhoff, D., Brummer, A., Buse, D.S., Hagenauer, F., Joerer, S., Segata, M., 2019. Veins: The Open Source Vehicular Network Simulation Framework. https://doi.org/10.1007/978-3-030-12842-5_6

Song, H., Zhao, F., Zhu, G., Liu, Z., 2023. Impacts of connected and autonomous vehicles with level 2 automation on traffic efficiency and energy consumption. J. Adv. Transp. 2023. https://doi.org/10.1155/2023/6348778

Sun, X., Yu, F.R., Zhang, P., 2021. A survey on cyber-security of connected and autonomous vehicles (CAVs). IEEE Trans. Intell. Transp. Syst. , 1–20. https://doi.org/10.1109/TITS.2021.3085297

Thompson, C., 2022. WARNING: objects in driverless car sensors may be closer than they appear. https://pratt.duke.edu/news/warning-objects-driverless-car-sensors-may-be-closer-they-appear/.

Tingvall, C., Haworth, N., 1999. Vision zero-an ethical approach to safety and mobility. In: 6th ITE International Conference Road Safety & Traffic Enforcement: Beyond 2000.

Tolouei, R., Maher, M., Titheridge, H., 2012. This is a repository copy of Vehicle mass and injury risk in two-car crashes: a novel methodology. https://doi.org/10.1016/j.aap.2012.04.005

Trullols-Cruces, O., Fiore, M., Barcelo-Ordinas, J.M., 2015. Worm epidemics in vehicular networks. IEEE Trans. Mob. Comput. 14 (10), 2173–2187. https://doi.org/10.1109/TMC.2014.2375822

Tympakianaki, A., Nogues, L., Casas, J., Brackstone, M., Oikonomou, M.G., Vlahogianni, E.I., Djukic, T., Yannis, G., 2022. Autonomous vehicles in urban networks: a simulation-based assessment. Transp. Res. Rec. 2676 (10), 540–552. https://doi.org/10.1177/03611981221090507/ASSET/IMAGES/LARGE/10.1177_03611981221090507-FIG11.JPEG

UNITED NATIONS, 2021. UN Regulation No. 155: uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system. Technical Report.

Upstream Security, L., 2024. Upstream's 2024 global automotive cybersecurity report. https://upstream.auto/reports/global-automotive-cybersecurity-report/.

Vellinga, N.E., 2022. Connected and vulnerable: cybersecurity in vehicles. Int. Rev. Law Comput. Technol., 1–20. https://doi.org/10.1080/13600869.2022.2060472

Wang, J.-S., 2022. MAIS(05/08) Injury Probability Curves as Functions of Delta V. Technical Report May. National Highway Traffic Safety Administration.

Wang, Y., Yu, B., Yu, H., Xiao, L., Ji, H., Zhao, Y., 2023. Automotive cybersecurity vulnerability assessment using the common vulnerability scoring system and Bayesian network model. IEEE Syst. J. 17 (2), 2880–2891. https://doi.org/10.1109/JSYST.2022.3230097

Wramborg, P., 2005. A new approach to a safe and sustainable road structure and street design for urban areas. In: Proceedings of the Road Safety on Four Continents Conference. Vol. 13, p. 12p.

Xiao, L., Wang, M., Van Arem, B., 2017. Realistic car-following models for microscopic simulation of adaptive and cooperative adaptive cruise control vehicles. https://doi.org/10.3141/2623-01