Journal of Highway and Transportation Research and Development (English Edition)
Open Access | Editor-in-Chief: Wanheng Li, Daming Lin | ISSN 2095-6215

J. highw. transp. res. dev.

https://doi.org/10.26599/HTRD.2026.9480118

Article Type: Review

Functionality resilience in connected autonomous vehicles: a perspective to enhanced road vehicle safety

Yukun Fang [1,2,*], Rui Teixeira [3], Gongda Hu [4], Haigen Min [5], and Xiangmo Zhao [5,6]

[1] *State Key Laboratory of Digital Intelligent Technology for Unmanned Coal Mining, Anhui University of Science and Technology, Huainan, 232001, China.*

[2] *School of New Energy and Intelligent Connected Vehicles, Anhui University of Science and Technology, Hefei, 231131, China.*

[3] *Department of Civil, Structural and Environmental Engineering, Trinity College Dublin, Dublin, D02 PN40, Ireland.*

[4] *Anhui Province Key Laboratory of Simulation Calculation and Design for Electronic Information System, Hefei Normal University, Hefei, 230601, China.*

[5] *School of Information Engineering, Chang'an University, Xi'an, 710064, China.*

[6] *Xi'an University of Architecture and Technology, Xi'an, 710055, China.*

*Email: fangyukun@aust.edu.cn

**Corresponding author: Yukun Fang, fangyukun@aust.edu.cn

Received：28, 8, 2026；Revised: 10, 9, 2026；Accepted：16, 10, 2026

Just Accepted

Abstract: Widespread deployment of connected autonomous vehicles (CAVs) is hampered by road-vehicle safety concerns rooted in the intrinsic complexity of CAV systems and in the unpredictability of operational environments, spanning functional safety (FUSA), the safety of the intended functionality (SOTIF), and cybersecurity. To confront these complexity-driven challenges in a unified manner, this paper re-examines road-vehicle safety through a functionality-centered resilience lens. The classical risk triplet (events A, consequences C, uncertainties U) is recast as a resilience triplet (A, F, U), in which F denotes the set of system functionalities to be preserved under adversity. This re-framing moves the focus from after-the-fact consequence angle toward the real-time safeguarding of critical functions throughout an adverse event. Building on this view, the interrelation between resilience and road-vehicle safety is elaborated across FUSA, SOTIF, and cybersecurity, and recent advances in CAV resilience within each domain are systematically surveyed. The conceptual demarcation between resilience and related notions such as robustness, recovery, and fault-tolerance are then clarified, showing that a functionality-centered stance absorbs these attributes as complementary phases of one unified objective. The paper closes with an open-issue discussion and future research avenues toward engineering resilient CAV systems.

Keywords: Connected autonomous vehicles; resilience; road vehicle safety; functionality; adverse events; uncertainties

Just Accepted

1 Introduction

The Connected autonomous vehicles (CAVs) are widely regarded as a transformative force for transportation, with expected benefits that include higher traffic efficiency, reduced congestion, lower crash rates, improved energy economy, and greater sustainability of mobility systems [1–3]. At the same time, realizing these benefits in practice is impeded by persistent road-vehicle safety concerns, notably the difficulty of guaranteeing reliable perception and decision-making in complex real-world settings, the unpredictability of vulnerable road users and other traffic participants, and the susceptibility of mission-critical on-board systems to cyber-attacks. These technological, regulatory, and social-acceptance barriers slow the broad roll-out of CAV technology. In this paper, road-vehicle safety is interpreted as the condition in which road vehicles in use do not impose unreasonable hazards of harm on people or property [4]. This umbrella notion groups together functional safety (FUSA), the safety of the intended functionality (SOTIF), and cybersecurity. FUSA, as defined in ISO 26262, addresses the elimination of unacceptable hazards that stem from malfunctioning electrical and electronic (E/E) systems [5], and is concerned with faults, failures, and design shortcomings of components. SOTIF, as defined in ISO 21448, complements FUSA by targeting hazards that arise from limitations of the intended functionality itself or from reasonably foreseeable misuse [6], thereby highlighting the residual risk that remains even when no fault is present. Cybersecurity, as defined in ISO 21434, gathers the safeguards that protect information, communication networks, and on-board data from internal and external threats [7]. CAVs routinely operate in environments that are simultaneously complex internally and variable externally, and these complexities give rise to road-vehicle safety risks that manifest along three principal strands [8, 9]. First, a CAV is itself an assembly of tightly coupled components, modules, and subsystems, whose scale and

interconnections generate intrinsic complexity. Second, the driving environment is highly dynamic, with unanticipated events and uncertainties that create external complexity. Third, the intricate interactions among modules and with the surroundings generate combinatorial event patterns whose outcomes can easily outrun the system's response capacity, producing interaction complexity. As emphasized by Dekker et al. [10], safety risks in complex systems almost always originate from the unexpected coupling of many events, namely the complexity of the system, that of its environment, and that of the countless interactions between them, which calls for holistic mitigation rather than piecemeal fixes.

The resilience of a system, in the present literature, denotes its capacity both to absorb the impact of adverse events and to recover its expected operating state within a bounded time [11], so that safety is regarded as the combined result of resistance to adverse events and adaptation to environmental change. Operating against highly dynamic, highly complex, and highly uncertain surroundings, CAVs inevitably encounter internal functional limitations and failures as well as external disturbances during their mission. Embedding resilience into CAVs offers an integrated way of coping with both internal and external complexity and of containing the potential damage caused by road-vehicle safety risks. A representative example is the failure of a communication link inside a vehicle platoon. Current fragmented remedies, such as re-weighting the communication graph based on isolated indicators like inter-vehicle distance or acceleration [12, 13], address only the immediate symptom of the hazard. By contrast, a resilience-oriented treatment spans every phase of the disruption, including anticipation (e.g., monitoring link stability through predictive analytics), adaptive response (e.g., dynamically rebalancing communication while preserving platoon stability), and recovery validation (e.g., confirming the restoration of nominal performance) [14]. Such a full-event-phase view of adversity handling is, however, still rare in CAV research.

A growing body of literature implicitly addresses pieces of the resilience problem, ranging from vulnerability analysis (e.g., modelling failure likelihood or isolating faults) to robustness enhancement (e.g., fault-tolerance mechanisms that limit failure impact), yet these efforts remain fragmented and lack a unifying conceptualization of resilience. To close this gap, the present paper formalizes CAV resilience research across the FUSA, SOTIF, and cybersecurity domains by proposing a unified, risk-grounded, functionality-centered framework that builds upon the conceptual work of Logan et al. [15]. The paper first reviews the connotation of resilience in a CAV context. It then introduces a formal definition of resilience as a triplet (A, F, U), in which the resilience of a system, conditioned on given events A, is described by the functionalities F to be preserved and the associated uncertainties U. This definition is then interpreted from the perspective of road-vehicle safety, spanning the three strands FUSA, SOTIF, and cybersecurity. After that, recent progress on CAV resilience is examined systematically within each strand, with attention to how published strategies address specific adverse events (A), maintain critical functionalities (F), and cope with the relevant uncertainties (U). Two open issues are then discussed in depth, namely the differences and similarities between resilience and its close concepts, i.e., robustness, recovery, and fault-tolerance, and the practical challenges that SOTIF risks pose to resilience enhancement.

The principal contributions of this study are summarized as follows:

Just Accepted

1) Formalized definition of resilience derived from the concept of risk, in the form of a triplet consisting of events A, functionalities F, and associated uncertainties U.

2) Elaboration of the nexus between resilience and road vehicle safety, i.e., clarifying the connotations of resilience in terms of the three strands of road vehicle safety.

3) Structured review and critical assessment of recent CAV resilience literature within each domain, identifying cross-cutting gaps and opportunities for integration.

4) An in-depth discussion on resilience and similar concepts, *e.g.*, robustness, recovery, and fault-tolerance, and the potential benefits of using the former as an integration of these, as well as the challenges posed by SOTIF risks for resilience enhancement.

The remainder of the paper is organized as follows. Section 2 lays out the problem statement, introducing the connotation of CAV resilience, the functionality-centered definition of resilience, and the interrelation between resilience and road-vehicle safety. Section 3 provides a structured review of recent advances in CAV resilience, with the aim of operationalizing the proposed framework. Section 4 then discusses two major open issues surrounding CAV resilience. Section 5 concludes the paper and outlines promising research directions.

2 Problem statement

In this section, connotation of resilience in literature is first discussed given a CAV background, where key terms (adversity, functionality) and traits (resistance, recovery) are remarked. In terms of this, a formal risk-based definition of resilience is established, i.e., resilience being framed as a triplet (A, F, U), which represents that resilience, related to given events A, is the functionalities F and associated uncertainties U of a system. Further, based on this definition, the nexus between resilience and road vehicle safety is elaborated across FUSA, SOTIF, and cybersecurity domains.

2.1 Is there resilience in CAVs?

The concept of resilience has appeared in many disciplines, and its definition varies considerably from one field to another, and readers interested in the broader cross-disciplinary discussion are referred to Martinez-Pastor [16]. In essence, resilience is treated here as an intrinsic property of a system that allows it to (i) withstand external disturbances and other adverse influences and (ii) return to its expected operating state within a bounded time once the disturbance has passed. Resilience is closely related to, but distinct from, the related properties of reliability, robustness, adaptability, and recoverability, which are contrasted in Table 1. Compared with reliability and robustness, resilience explicitly incorporates a recovery capability, while compared with adaptability and recoverability, it additionally captures the capacity to resist adverse events rather than only to react to them.

Although these related notions occasionally surface in CAV research and engineering practice, the literature still lacks a widely accepted, unified definition of resilience, and the use of resilience in the CAV context is itself an emerging concept. Even so, the overview provided in Table 1 makes it clear that the constituent ideas of resilience are routinely examined within CAV systems, so that a resilience perspective is both timely and pertinent for the CAV domain.

Just Accepted

Table 1 Concepts of resilience, reliability, robustness, adaptability, and recoverability.

Concepts	Meaning
Resilience	The capacity of a system to withstand external disturbances and other adverse influences, and to return to its expected operating state within a bounded time horizon after the disturbance has passed.
Reliability	The capacity of a system to deliver its intended functions over a specified time horizon under given conditions [17–19], which addresses the failure probability following a particular adverse event.
Robustness	The capacity of a system to absorb stresses, pressures, perturbations, unpredictable changes, or variations in its operating environment without losing functionality [17], which addresses the maintenance of its initial state both during and after a specific adverse event [18].
Adaptability	The capacity of a system to adapt its state so as to deliver its intended functions in a new operating environment.
Recoverability	The capacity to bring a system back to its expected operating state [17].

It should be acknowledged that the definition of resilience is intrinsically application-dependent and reflects the characteristics of the system under consideration. Eigner et al. [20] treat the resilience of information systems as the capacity to reduce the impact of disruptive events by (a) anticipating and preparing for such events, (b) withstanding them when they occur, and (c) restoring the affected functionality within a specified time window. In the cyber-physical systems (CPS) literature, resilience is commonly cast as the ability to withstand and recover from attacks, with a particular emphasis on security [21, 22]. Berger et al. [11] characterize resilience as the property of preserving the dependability and security of a system that is subject to change, with explicit reference to the Internet of Things (IoT). Prorok et al. [23], working on multi-robot systems, argue that resilience is the capacity to overcome adversity by exploiting system-wide complementarity, diversity, and redundancy in order to preserve functionality or to minimize the time intervals during which functionality is compromised. In the transportation literature, resilience is typically described as the capacity to maintain the basic functions and structure of a system through resistance, mitigation, and absorption under extreme conditions, and to return to the original equilibrium, or to a new stable equilibrium, within an acceptable time and cost [24–26]. CAV systems can be viewed as an instance, or a combination, of the systems mentioned above, and across these explanatory definitions two recurring keywords and two recurring traits can be identified, i.e.,

key word 1: adversity

key word 2: functionality

key trait 1: the ability to withstand the negative impact in adversity

key trait 2: the ability to recover to the expected status after the adverse event

The first keyword, *adversity*, refers to adverse internal or external operating conditions (e.g., component faults, severe weather) or to challenging operational scenarios (e.g., tunnel driving for GNSS-based localization). A CAV may be exposed to numerous adverse events, and it is regarded as resilient when it overcomes the negative impact of such stressors and continues to deliver, or even to optimize, its intended functionality. Prorok et al. [23] describe two principal dimensions that delineate a stressor, namely whether it is stochastic or out-of-distribution, and whether it is targeted. Stochastic stressors are pervasive but tractable through established knowledge, as in the case of measurement noise, which can be characterized from prior knowledge in the relevant field. Out-of-distribution stressors, by contrast, are disturbances that the system has not been prepared for, such as those caused by unknown faults. Targeted stressors

Just Accepted

usually affect particular subsystems or functions and can be goal-oriented, with adversarial attacks against specific sensors or algorithms being representative examples. Broadly speaking, adversity acts as the trigger that may cause significant functionality degradation if no corresponding measure is taken to enable the system to adapt to the changing environment.

The second keyword, *functionality*, quantifies the performance of a designated function for a given system (e.g., the localization accuracy of a positioning module). In general, system functionality encompasses the specific tasks, operations, or activities that the system is designed to carry out and reflects the system's ability to deliver its intended functions against stated requirements, as expressed by the system's observable features and behaviors. In the resilience discourse, Davis [27] defines functionality as the condition in which a system continues to operate properly and to provide a regular and reliable service at, or as close as possible to, the level delivered prior to the adverse event. Realizing the required functionality of a CAV requires not only the full implementation of the necessary functions within each subsystem but also the coordination, cooperation, and collaboration of all the subsystems and agents involved [23].

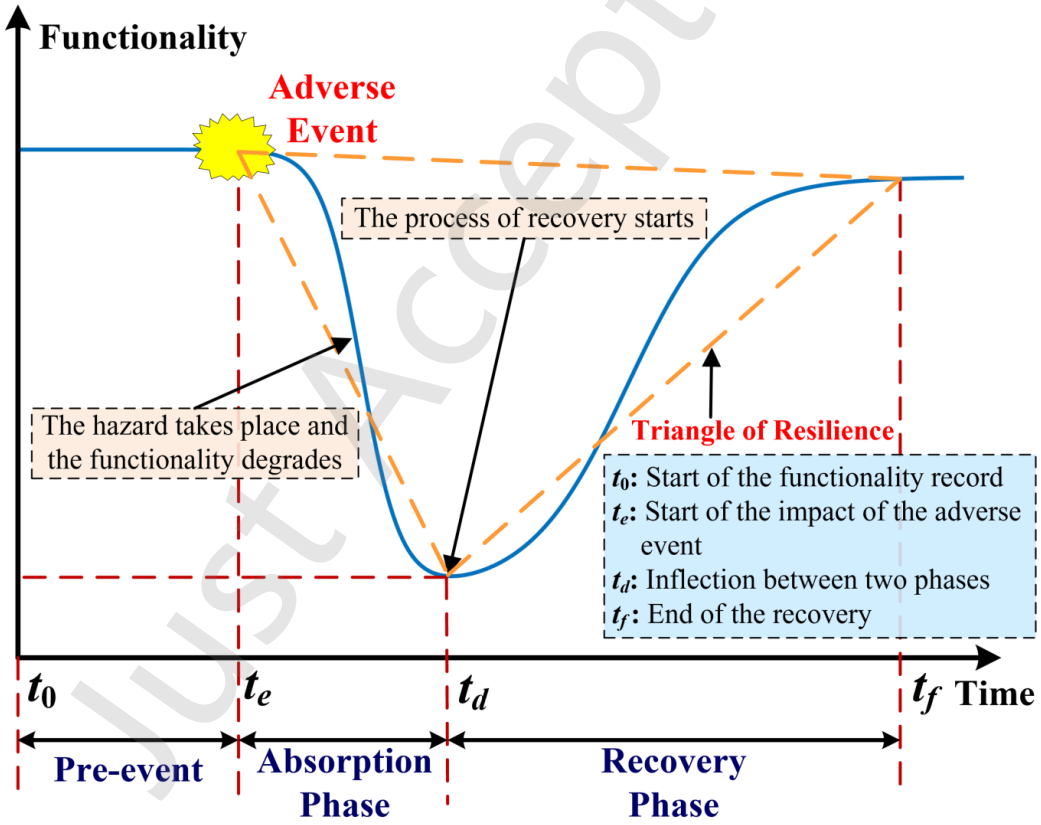


Fig. 1 A typical performance curve of a system under a disruption, given a specific adverse event, which forms the triangle of resilience characterized by its absorption and recovery phases.

The two key traits identified above capture how a system reacts to adversity, with the level of specific functionalities serving as the natural metric. A representative performance curve that traces the functionality of a system in response to an adverse event is sketched in Fig. 1. It exhibits two distinct phases after the event, namely the absorption phase and the recovery phase. The triangular shape of the curve is the origin of the term triangle of resilience, and its form characterizes the response to a given pair of adversity and functionality. The first trait concerns how a system reacts in the absorption phase, where a resilient system is expected to withstand the

Just Accepted

negative impact of the adversity, to resist or accommodate the perturbation, and to preserve functionality so as to avoid downtime. The second trait concerns the recovery phase, where a resilient system should restore, return to, or recover at least its nominal performance after the perturbation [16, 28], with explicit attention to mitigating the negative impact through functionality optimization. Taken together, the two traits describe the capacity of a system to maintain and optimize specific functions when faced with adversity and the associated uncertainties.

Even though the two traits of withstanding and recovering are widely accepted, the prevailing definitions of resilience in the CAV literature suffer from two persistent shortcomings. First, they are typically domain-specific and qualitative, treating resilience as a desirable property without offering a common basis for measurement or for cross-system comparison. Second, they tend to merge the absorption and recovery phases into a single notion of "ability", obscuring the distinct mechanisms required for resistance versus for restoration. The functionality-centered framework presented in the next section addresses both shortcomings by grounding resilience in the formal structure of risk and by explicitly separating the two temporal phases of the system response.

2.2 Functionality-centered definition of resilience derived from risk

Although some disagreement remains [29], it is broadly accepted that the concept of resilience is intrinsically related to risk [30], or at the very least should be informed by it [15]. In general, risk can be regarded as the combination of the severity and the likelihood of an undesired outcome [31]. Risk expresses the possibility that an activity will produce unwanted consequences [32]. Formally, risk can be described as a triplet composed of events A, consequences C, and the associated uncertainties U, as formulated in Eq. (1).

$$Risk = \left(A, C, U \right) \tag{1}$$

It means that risk, related to given events A, is the consequences C and associated uncertainties U. Here, the consequences C can be understood as the impacts that are considered given events A and the associated uncertainties U [15, 33]. It is quantified and is inherently related to safety, where a safe system can be understood as a system where risk is acceptably low [34] or free from unacceptable losses.

As remarked previously, resilience is often described as an ability or a set of abilities to achieve desired functionality in a specific environment given specific events, usually adverse. Higher resilience of a system indicates that the system is more suited to maintain and recover the desired functionality in adversity, hence, reducing negative consequences. As such, the measures that attempt to enhance system resilience can also influence the consequences C. Hence, Logan *et al.* [15] argue that resilience should leverage the concept of risk instead of defining it as an ability or a set of abilities:

The [un]resilience of a system equals the risk of [not] attaining the desired functionality, over a specific time window, following an event.

This statement can be challenging to understand since the concept of risk is usually related to undesirable, unwanted, negative consequences [31, 32, 35]. Nevertheless, the consequences of

Just Accepted

an activity, as defined by Logan *et al.* here, can be either positive or negative, as addressed in another paper related to this issue [35]. The purpose of Logan *et al*. is to demonstrate the tight correlation of these two concepts, and the authors then gave a corollary to clarify the connections between risk and resilience, consistent with the definition of *safety as acceptable risk* [15]:

A system is considered resilient when the risk of failing to achieve the desired functionality is judged to be acceptably low.

While Logan et al. [15] established the foundational link between resilience and risk, their formulation remains at the conceptual level. It defines resilience as a type of risk but does not specify how that risk should be tracked or managed in practice. Risk highlights the *consequences* of being unable to deal with adverse events, while resilience focuses on specific *functionalities* to handle adverse events [36]. Therefore, if resilience of CAV is considered, functionalities F should be adopted instead of consequences C in Eq. (1) in the formalization of the concept of resilience, i.e.,

$$Resilience = \left(A, F, U \right) \tag{2}$$

In this context, resilience, relates to given adverse events A, is the functionalities F and associated uncertainties U of a system. By substituting the abstract notion of "consequences" C with the measurable construct of "functionalities" F, the framework anchors resilience in observable performance indicators that can be monitored continuously over time. Consequences are typically binary and observable only after an event concludes. Functionalities are time-varying signals that reflect the system's state throughout the event. Furthermore, the explicit retention of the adverse event A and the uncertainty U alongside the time-varying functionality F provides a structure that enables phase-aware analysis. While the framework itself does not prescribe how to segment the temporal response, it naturally accommodates the examination of how F evolves under A and U, including the distinct stages of degradation and restoration that are empirically observed in resilient systems. This temporal perspective is essential for diagnosing the root cause of insufficient resilience and for guiding targeted design improvements.

It should be noted that not all system functionalities are directly safety-relevant. In this work, F specifically denotes those core functions whose degradation or loss could lead to unacceptable road vehicle safety risks in the sense of FUSA, SOTIF, or cybersecurity. Therefore, as long as the uncertain functionality behavior in adversity does not generate unacceptably low road safety risks, then that system is resilient. In this formulation, the dip in functionality during adversity may elevate risk exposure. However, a resilient system maintains risk at an acceptable level through one of two mechanisms: either the functional degradation is small, or the degradation is larger but recovery is sufficiently rapid that cumulative risk remains bounded. The (A, F, U) framework captures this dynamic by treating functionality F as a real-time proxy for risk: monitoring F over time enables proactive assessment of whether the system remains within acceptable risk boundaries. The framework prompts the question: *can the system maintain or recover F quickly enough to keep risk acceptably low?* This functionality-centered perspective shifts the focus from static failure analysis toward dynamic risk containment, uniting fragmented

Just Accepted

concepts such as robustness and recovery under a common objective: preserving essential functionalities across all phases of an adverse event.

The formalization of resilience as (A, F, U) raises a natural question: *how can this framework be operationalized in practice?* While the framework itself is conceptual, it provides a structured lens through which quantitative evaluation can be developed. Specifically, the functionality F can be associated with one or more observable performance indicators that reflect the degree to which the intended function is achieved over time. The temporal profile of such an indicator, often represented as a performance measure, typically exhibits a phase of degradation (absorption) followed by a phase of restoration (recovery), shown in 错误!未找到引用源。. From this profile, various quantitative metrics, e.g., cumulative functional deficit, recovery duration, can be defined according to the application context [37, 38]. Regarding the uncertainty dimension U, both measurement and modeling approaches have been extensively studied in the literature. The choice of appropriate techniques depends on the nature of the adverse event A and the available knowledge about the system. A detailed treatment of these methods is beyond the scope of this conceptual paper, and interested readers are directed to recent surveys and foundational texts in this area [39-44].

To compare resilience across different systems or design alternatives, the (A, F, U) framework suggests a structured comparison along three dimensions: (i) the severity of functional degradation under the same adverse event A (reflecting resistance), (ii) the speed and completeness of recovery, and (iii) the sensitivity of F to irreducible uncertainties U. A system is considered more resilient if it exhibits smaller functional degradation, faster recovery, and lower sensitivity to uncertainty, given the same A. For systems with multiple critical functionalities, aggregation can be performed via weighted combinations that reflect the relative safety criticality of each function, or via multi-objective analysis when functionalities compete. The specific aggregation approach is application-dependent and should be guided by safety requirements and operational context.

2.3 Nexus between resilience and road vehicle safety

Road-vehicle safety, in this paper, refers to the condition in which road vehicles in use do not impose unreasonable risks of injury or damage on people or property [4]. CAVs operate in complex and dynamic environments in which FUSA, SOTIF, and cybersecurity risks are deeply intertwined, and the motivation for developing the functionality-centered resilience framework (A, F, U) within road-vehicle safety research is precisely to address the inherent complexity and the interconnected risks of CAVs in a holistic way. In this subsection, the nexus between the proposed framework and road-vehicle safety is elucidated by aligning the framework with the three strands of road-vehicle safety, namely FUSA, SOTIF, and cybersecurity.

The events A in a CAV setting denotes the situations or stressors that a system may encounter. They are variously labelled in the literature as disturbances, perturbations, interferences, errors, anomalies, faults, threats, or trigger conditions, among others. Within FUSA, the focus is on preventing or mitigating the impact of hazards produced by the malfunctioning of electrical and electronic (E/E) systems, where the underlying stressors include hardware/software faults, component ageing, and similar phenomena. Within SOTIF, attention

Just Accepted

shifts to hazards that originate from functional insufficiencies of the intended functionality. These insufficiencies are linked to many aspects and triggering factors, with representative stressors including adverse weather, poor road conditions, and scenarios that exceed the response capacity of a system. Cybersecurity, in turn, addresses the protection of information, networks, and data against internal and external threats, with stressors that range across diverse cyber-attacks and adversarial attacks. Bagchi et al. [45] summarize three common forms of adverse events for autonomous systems: 1) faults or failures of hardware or software, including bugs, ageing, misconfigurations, component faults, and system-level failures, 2) unexpected inputs, where the system has to interact with the physical environment and humans and therefore may receive unpredictable data, and 3) maliciously induced failures or security attacks originating from outside the system. In the road-vehicle safety context, these three forms align naturally with the FUSA, SOTIF, and cybersecurity strands. Specifically, CAV resilience concerns adversity caused by faults and failures in FUSA, unexpected scenarios triggered by activating conditions and the associated performance limitations in SOTIF, and attacks launched against on-board or external assets in cybersecurity.

The consequences C, or the functionalities F, are inherently system- and context-specific. As an illustration, a positioning system may fail to localize a vehicle inside a tunnel where GNSS signals are unavailable. Because the intended functionality, namely the continuous and accurate delivery of position information, is not preserved, such a positioning system is regarded as less resilient and carries elevated risk in this scenario. The proposed functionality-centered framework treats the functionality F as the direct proxy for road-vehicle safety, since the level of risk is fundamentally governed by whether the core functionalities of the system remain within an acceptable range under adversity and since any degradation of functionality translates directly into elevated safety risk. The precise definition of the desired functionality differs across the three road-vehicle safety domains. In broad terms, FUSA and SOTIF emphasize the full realization of the foundational functions of a CAV, including perception, localization, planning, decision-making, control, and intra- and inter-vehicle communication. Within FUSA, F refers to the correct execution of the functions of the electrical and electronic systems. Within SOTIF, F extends beyond the component level to the holistic performance of the vehicle in complex scenarios, such as the maintenance of adequate situational awareness under adverse weather. Within cybersecurity, F relates to the confidentiality, integrity, and availability of data and communication channels, for instance ensuring that V2X messages cannot be spoofed and that in-vehicle network traffic remains uncompromised. Despite these domain-specific definitions, the underlying resilience principle remains uniform: to sustain the required level of F under the corresponding adverse events A and the associated uncertainties U.

Uncertainty is a central concept for both risk and resilience. The formal definition of risk given above can be understood as adding the uncertainty dimension U to the events A and the consequences C [46]. More directly, ISO defines risk as the effect of uncertainty on objectives [47]. It is the uncertainty surrounding the events A and the consequences C that gives rise to the risk of the system failing to attain the desired functionality over a specific time window following the event. Resilience can be understood analogously, by adding the uncertainty dimension U to the events A and the functionalities F. It is the uncertainty on A and F that shapes the resilience of

Just Accepted

a system. Across the three domains (FUSA, SOTIF, cybersecurity), uncertainties U aggravate risk by (1) increasing the unpredictability of events (the A component of the triplet), (2) obscuring the pathways of consequences (the C component), and (3) complicating the assurance of functionality (the F component of the triplet). Resilience is therefore achieved by trimming epistemic uncertainty through domain-specific hardening while tolerating irreducible aleatory uncertainty by means of safety margins. Specifically, FUSA concentrates on mitigating risks from systematic or random hardware/software failures, and uncertainty in this domain stems from stochastic faults/failures and from gaps in diagnostic coverage (e.g., latent faults that escape detection because of unanticipated inter-component interactions). The uncertainty U in FUSA therefore centers on the unpredictability of fault occurrence and of diagnostic efficacy, and is typically bounded by redundancy. SOTIF addresses hazards from non-faulty performance limitations, and key uncertainties arise from the dynamic and complex environment, from algorithmic opacity (limited generalizability and explainability), and from unexplored operational scenarios. The uncertainty U in SOTIF reflects the inadequacy of intended functionalities and the gaps in scenario coverage, and is addressed by iterative validation through simulated edge cases and the operational design domain (ODD).

Overall, the (A, F, U) framework is well-aligned with the three strands of road vehicle safety, summarized in Table 2. The proposed functionality-centered resilience framework provides a unified, risk-based approach to resilience that spans all three safety domains, reflected primarily in the following aspects:

1) **Integrating diverse domains of road vehicle safety**: It bridges FUSA (component faults), SOTIF (functional insufficiencies due to triggers), and cybersecurity (malicious attacks) under a common structure, where A captures various types of adverse events, F serves as the universal functionality metric, and U acknowledges the epistemic and aleatory uncertainties in each domain.

2) **Enabling dynamic risk containment**: Instead of static failure analysis, the framework treats functionality (F) as a real-time proxy for risk. Fluctuations in F directly reflect risk levels, allowing proactive measures (e.g., redundancy activation, adaptive algorithms) to maintain functionality within an acceptably low-risk envelope.

3) **Unifying fragmented concepts**: It consolidates traditionally siloed attributes, e.g., robustness, recovery, fault-tolerance, adaptability, and among other (see discussion in Section 4.1), under the overarching goal of *functionality preservation*, providing a common benchmark for evaluating resilience strategies across CAV subsystems.

To summarize, the functionality-centered resilience framework transforms road vehicle safety research from separate hazard-mitigation efforts into a holistic, functionality-driven pursuit of resilience, essential for achieving safety and trustworthy CAV deployment in real-world environments. In the next section, related works of resilience will be reviewed in terms of FUSA, SOTIF, and cybersecurity, respectively, to showcase how resilience strategies are structured to address specific adverse events (A), the maintaining functionalities (F), and the managing of respective uncertainties (U).

Just Accepted

Table 2 Alignment of the (*A*, *F*, *U*) framework with FUSA, SOTIF, and cybersecurity.

Issue	Adverse events (*A*)	Functionalities (*F*)	Uncertainties (*U*)	Nexus
FUSA	faults or failures of hardware/software components	core functions of electronic and software systems	unpredictability in fault occurrence, propagation, and diagnostic coverage, etc.	The framework directly supports FUSA by focusing on maintaining and recovering core functionalities despite component faults, through strategies like fault diagnosis, fault-tolerance, and prognostic health management
SOTIF	trigger conditions (e.g., adverse weather, complex scenarios) that cause functional insufficiencies	both basic and holistic system functions (e.g., situational awareness, decision-making)	environmental variability, algorithmic limitations, and unanticipated interactions, etc.	The framework addresses SOTIF by emphasizing functionality preservation under uncertain triggers, enabling resilience through scenario analysis, performance boundary identification, and adaptive responses.
Cybersecurity	cyber threats (e.g., spoofing, DoS attacks, data injection)	security-related functions like confidentiality, integrity, and availability of data and systems	threat mutability, attack unpredictability, and systemic vulnerabilities, etc.	The framework enhances cyber resilience by prioritizing the maintenance of security functionalities under adversarial conditions, using encryption, intrusion detection, and adaptive countermeasures.

3 Structured review and critical assessment of CAV resilience from a road-vehicle safety perspective

Building upon the formalized risk-based resilience framework (*A*, *F*, *U*) and its nexus with road vehicle safety through FUSA, SOTIF, and cybersecurity, recent advances in CAV resilience research are structurally investigated. This section critically examines how resilience strategies manifest across these three critical safety domains, structured according to the triplet dimensions. Concrete implementations of resilience mechanisms are explored, highlighting desired functionalities (*F*), addressed stressors (*A*), and associated uncertainties (*U*), to assess both the progress made and the significant opportunities that remain for enhancing system-wide resilience in CAVs. This structured review serves to operationalize the theoretical framework while identifying gaps for future research.

3.1 CAV Resilience given FUSA Background

As already noted in Section 2.3, FUSA is concerned with the absence of unreasonable risks that result from malfunctions of E/E systems. In this setting, the desired functionality F is defined as the correct operation of the electronic and software components, and resilience is aimed at preserving these functionalities in the presence of component faults or failures. Fault diagnosis, fault-tolerance measures, and prognostic health management (PHM) constitute the most widely deployed countermeasures against the negative impact of faults and failures in electronic and software components. The meanings of fault diagnosis, fault-tolerance, and PHM are summarized in Table 3. From the discussion of fault diagnosis, fault-tolerance, and PHM, the following points can be drawn.

Just Accepted

1) Fault diagnosis emphasizes the detection and analysis of the characteristics of the adverse factors to provide required information for subsequent measures (e.g., active fault-tolerance measures, PHM measures).

2) Fault-tolerance is another important facet of system resilience. Passive fault-tolerance is akin to robustness in that it emphasizes resisting the adverse effects of known faults or disturbances and maintaining basic functionality. Active fault-tolerance, in contrast, improves the adaptability of a system in the presence of faults/failures by exploiting the information provided by the fault diagnosis module, so that functionality can be progressively recovered after faults/failures have occurred through active reconfiguration of the system.

3) PHM can be regarded as the integration of preventive measures for functionality maintaining, which emphasizes improving the functionality of the system itself to avoid possible hazards.

Table 3 Illustration of fault diagnosis, fault-tolerance, and PHM [9].

Concept	Illustration
Fault diagnosis	· The activity of identifying which faults or failures occur and in which components or subsystems, comprising three core tasks: fault detection, fault isolation, and fault identification, with the goal of supplying actionable information about the faults or failures [48]. · Fault detection: monitoring the status of the relevant systems and detecting any malfunctions or faults that appear in them. · Fault isolation: locating the faulty components or subsystems, or the faulty variables in the monitored process [49]. · Fault identification: determining the type, severity, and/or root causes of the faults [49].
Fault-tolerance	· The capacity of a system to keep operating despite the presence of faults [50], where the system can automatically compensate for the impact of faulty components while preserving the intended functionality at the desired level of overall performance [51]. · Passive fault-tolerance: design-time measures aimed at robustness enhancement, where the system is pre-engineered to withstand predefined faults. · Active fault-tolerance: runtime measures that adapt the parameters and structure of the system, select appropriate strategies, and schedule available resources to compensate for the impact of an occurred fault, based on the fault/failure information supplied by the fault diagnosis module.
Prognostic health management (PHM)	· A holistic approach to managing the health and maintenance of components, equipment, and systems throughout their lifecycle, in order to: 1) detect equipment and process anomalies, 2) diagnose degradation states and faults, 3) predict the future health state of the system, estimate its remaining useful life (RUL), and anticipate potential failures, and 4) take proactive measures to prevent or mitigate the negative impact of functional degradation [52, 53].

Related works on fault diagnosis, fault-tolerant control, and PHM for CAVs have been surveyed in an earlier paper [9], and the concept of fault-tolerant control is here extended to a more general notion of fault-tolerance. Given that fault-tolerance is tightly coupled with resilience in the face of faults under the FUSA background, the remainder of this subsection briefly discusses fault-tolerance in CAV applications. In abstract terms, a CAV can be modelled as a feedback control system that gathers the status information of the ego-vehicle and the situational information of the surrounding environment and then adjusts the system states through decision-making algorithms on the basis of the available information, as illustrated in Fig. 2. In this context, faults can originate from data sources, actuators, and the object/process in operation [54]:

· Faults originate from data sources: the data gathered have substantial errors and cannot represent the real status of the object/process being observed.

Just Accepted

- Faults originate from actuators: the actuators failed to adjust the states of the object/process in operation as expected.
- Faults originate from the object/process in operation: the dynamic input/output properties of a system change owing to this kind of fault.

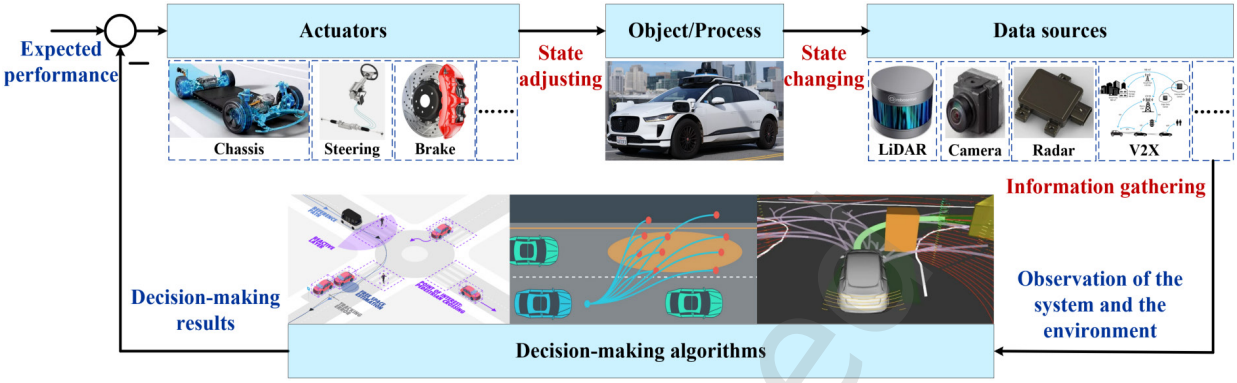


Fig. 2 A simplified CAV system architecture from a feedback control perspective.

Designing fault-tolerance strategies in operation demands domain-specific expertise in the mechanical structure and the electrical and electronic (E/E) architecture of the vehicle, and most fault-tolerance research on CAVs therefore concentrates on these two aspects. Redundancy is one of the cornerstones of fault-tolerance, alongside diversity and independence. For faults that originate in data sources such as on-board sensors and V2X links, the priority is to safeguard data quality through redundancy. Common remedies include multi-source data fusion [55–59] and system-state prediction (e.g., leveraging redundancy supplied by vehicle kinematic/dynamic models and similar sources) [60–62]. For faults that originate in actuators, the priority is to compensate for the degraded or faulty actuation through redundancy [63–67].

The above illustration on fault diagnosis, PHM, and fault-tolerance is insightful and instructive for the resilience research of CAVs in the face of component faults/failures, and these techniques are deployed for CAV resilience enhancement given the FUSA background, shown in Table 4. Most of these works focused on the functionality resilience of specific subsystems against faults or failures [68-72], and some works further extend the resilience research to the case of cooperative driving of a group of CAVs, primarily tackling with the negative effects caused by communication failures [14, 73]. Most of the works highlight the strategy design for resilience enhancement against faults or failures, but only some of them clearly define the concept of resilience [14, 69, 71, 72]. Connotations of resilience in several works are ambiguous and reminiscent of robustness or fault-tolerance [68, 70, 73]. These works emphasized the functionality enhancement of specific systems in response to faults or failures, but few of them studied the characteristics of specific adverse events and involved uncertainties. Thus, pinpointing the concept of resilience should be the primary work in future studies for system resilience in CAV applications given the FUSA background, and paying attention to the characteristics of specific adverse events (e.g., faults, failures, errors, etc.) and involved uncertainties will facilitate the strategy design for resilience enhancement and mitigate FUSA risks.

Just Accepted

Table 4 Some recent advances in resilience given FUSA background for CAV applications.

Work	Desired functionality (*F*)	Stressors (*A*)	Uncertainties involved (*U*)
Monteuuis [68]	fundamental perception ability of a CAV	perception failures, threats against the perception system	uncertainty in perception data, vehicle operating environment, and various threats
Moosavi *et al.* [69]	required functionality of multiple sensors for autonomous driving	sensor failures	uncertainty in sensor measurement, sensor health uncertainty
Leach *et al.* [70]	secure operation of the software	faults, software errors, system failures, cyberattacks, or environmental changes	uncertainty of the embedded systems and failure scenarios
Wan *et al.* [71]	required functionality of an autonomous system	faults, random errors	uncertainty of various faults and errors, and their propagation process
Krecht *et al.* [72]	required functionality of a CAV like perception, localization, planning, decision-making, control, etc.	component or system-level failures, factors that can cause physical damage or malfunctions in electronic and mechanical components	uncertainty of failure scenarios
Fang *et al.* [14]	platoon oscillation dampening and string stability	intermittent link failures	uncertainty of the status of the V2X links
Liu *et al.* [73]	formation keeping, individual vehicle stability, and string stability for autonomous vehicle platoons	heterogeneity of vehicles, communication failures	uncertainty in the heterogeneous vehicle parameters, communication failures, and measurement noise

Critical Assessment. The works reviewed above demonstrate that resilience strategies in the FUSA domain are relatively mature, with fault diagnosis, fault-tolerance, and PHM being well-established methodologies. However, several limitations persist. First, **maturity and scalability**: While fault-tolerance for individual subsystems is well-studied, holistic resilience at the vehicle level, i.e., integrating multiple fault sources across perception, planning, and control, remains underexplored. For instance, Monteuuis [68] proposes a perception resilience framework but limits evaluation to specific failure modes. Krecht et al. [72] discuss military UGV resilience conceptually but do not provide scalable algorithms. The computational overhead of real-time fault diagnosis and reconfiguration also poses scalability challenges for deployment on resource-constrained automotive platforms. Second, **validation rigor**: The majority of studies rely on simulation-based validation, and real-world testing under injected faults is rare due to safety and cost constraints. Leach et al. [57] is a notable exception, reporting practical experience with a trusted and resilient AV framework, though the evaluation is qualitative. Third, **treatment of uncertainty**: Most works assume known fault models and treat uncertainty as bounded disturbances or Gaussian noise without empirical validation of these assumptions. Fourth, **phase coverage**: The reviewed works predominantly address the absorption phase (robustness against faults) but seldom evaluate recovery dynamics, i.e., how quickly and completely functionality is restored after fault occurrence. Only Fang et al. [14] explicitly considers recovery validation. This leaves an important gap in understanding full-event-phase resilience.

3.2 CAV resilience from SOTIF perspective

As already mentioned in Section 2.3, SOTIF targets hazards arising from functional insufficiencies of the intended functionality, as well as from reasonably foreseeable misuse. Here, functional insufficiency denotes the incomplete specification or insufficient implementation of the intended functionality, where the resulting risk is unreasonable [6]. SOTIF can be viewed as a complement, or extension, of FUSA, and it is particularly relevant in autonomous-driving applications, where it addresses the safety of the vehicle behavior under normal operation and

Just Accepted

under reasonably foreseeable misuse, rather than only under explicit failures or malfunctions [74]. The SOTIF concept conveys the expectation that a system should perform as intended under diverse conditions and use cases, including hazards caused by design deficiencies or by performance limitations. This in turn requires the system to handle complex scenarios, to fuse information from multiple sources correctly, and to respond to unexpected events in a way that avoids potential hazards [75]. Consequently, under the SOTIF lens the desired functionality is defined not only at the level of individual modules or subsystems but also at the level of the holistic system, and resilience here emphasizes the preservation of the holistic functionality in the face of the factors and events encountered during operation, such as unfavorable weather and complex driving scenarios. According to Wang et al. [76], SOTIF concerns can be decomposed into two essential aspects, namely trigger conditions and performance limitations. Trigger conditions denote specific scenarios or events that can activate latent functional insufficiencies of a system, including environmental factors, user behavior, system performance limits, and other elements that may push the system into hazardous behavior. Performance limitations refer to the inherent boundaries or constraints of a system's capabilities that may prevent it from functioning as intended under certain conditions. Risks in the SOTIF background derive from the uncertainty of the trigger conditions and the uncertainty of performance limitations in specific scenarios or certain conditions, leading to the uncertainty of the consequences. Antona-Makoshi *et al.* [77] directly define trigger conditions as the events that cause risks. System resilience in the context of SOTIF is the complement to the mentioned risks of the system not achieving desired functionality, during a specific time, following specific threats. Therefore, studies on resilience given SOTIF background should highlight the analysis of trigger conditions and performance limitations in specific scenarios or certain conditions. Analysis of trigger conditions facilitates to understand under what circumstances a system may fail, for instance, adverse weather conditions, sensor contamination, electromagnetic interference, and other factors that degrade the performance or lead to improper actions by the system, and taking corresponding measures to operate safely as intended. Performance limitations are tightly related to scenarios and arise due to various triggers, and Kinalzyk [78] regarded trigger conditions as causes for performance limitations and functional insufficiencies. Some of these triggers are illustrated in Table 5.

Functional insufficiencies vary across CAV systems, so that trigger conditions are inherently system-dependent. Fig. 3 illustrates the chain through which a trigger condition can eventually lead to an accident, in which the concept of hazard plays a central role. Within ISO 21448, hazard denotes a potential source of harm caused by hazardous behavior at the vehicle level [6]. Zhu et al. [81] describe hazardous behavior under ISO 21448 as an external, observable, and unintended vehicle behavior, and hazardous event as an incident in which a hazardous behavior of the ego vehicle, combined with specific scenario conditions, brings a hazard into reality. This chain highlights the pivotal role of trigger conditions in SOTIF studies, with existing solutions for trigger-condition identification grouped by Zhu et al. [81] into knowledge-driven, data-driven, and combined approaches. Knowledge-driven approaches draw on the expertise and experience of domain specialists [82], and representative methods include hazard analysis and risk assessment (HARA) [83, 84] and system-theoretic process analysis (STPA) [85]. Data-driven approaches rely on data collected from the real world [86, 87] and require diverse naturalistic driving data sets covering accidents and near-miss incidents.

Just Accepted

Table 5 Some triggers that may lead to performance limitations, given SOTIF background [76, 79-81]

Trigger	Illustration
Sensor limitations	The range, accuracy, or resolution of sensors may not be sufficient to detect or interpret the environment correctly in all situations.
V2X limitations	Limitations on V2X ability can lead to a lack of situation awareness and trigger potential hazards.
Data quality and integrity	Poor data quality or integrity issues can be a trigger condition for SOTIF concerns for those applications that rely on high-quality data.
Dataset bias	Bias in the data used for training and validation can cause the system to perform suboptimally in real-world scenarios.
Actuator capabilities	The physical components that execute actions, such as motors or brakes, may have limitations in their speed, force, or precision.
Algorithmic constraints	The algorithms used for processing sensor data and making decisions may have limitations in their logic or capability to handle complex or unexpected scenarios.
Computational source limitations	The system may lack the necessary computational resources to process information quickly enough to respond to dynamic situations.
Hardware and software reliability	The system may have bugs or defects that affect its performance, or hardware may fail or degrade over time.
System integration	The way different components of the system work together may introduce limitations, such as delays in data transmission or integration deficiencies.
Human-machine interface	Limitations in how information is communicated to the user or how user inputs are interpreted can affect system performance.
Environmental conditions	The system may not perform expectedly under adverse environmental conditions, like extreme temperatures, bad illumination, adverse weather conditions, and among others.
Road conditions	The state of the roads, including wet, icy, or uneven surfaces, can impact the stability and control of CAVs, potentially leading to safety incidents.
Complex traffic scenarios	High-density traffic, merging lanes, or construction zones can present complex situations that challenge the decision-making capabilities of the CAV system.
Unexpected behaviors of other traffic participants	The behaviors of other road users or objects that are not in line with expected patterns can trigger SOTIF issues if the system does not respond appropriately.
Ethical and legal constraints	The system may be designed to follow certain ethical principles or legal regulations that constrain its actions or responses.

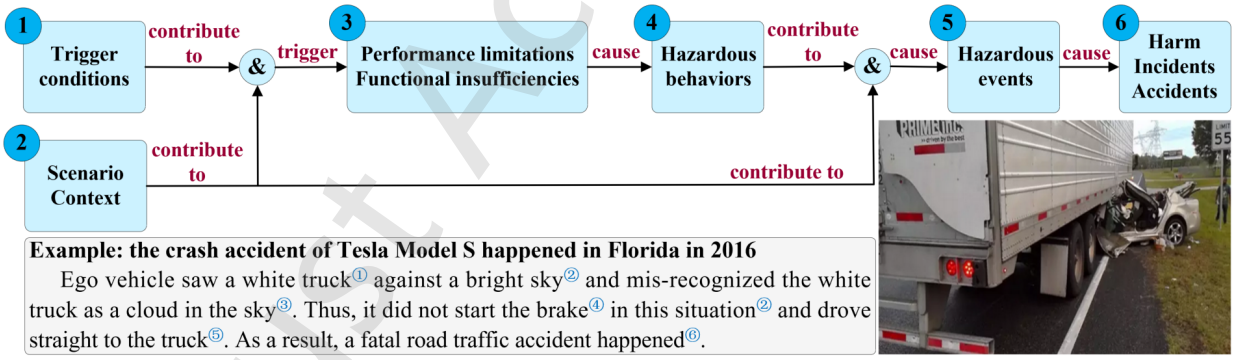


Fig. 3. Demonstration of the chain from trigger conditions to accidents given SOTIF background.

The above investigation on the common triggers that can result in performance limitations in CAV applications and the demonstration of the chain from trigger conditions to accidents inspire resilience research from the SOTIF perspective. Recent advances in literature that involve CAV resilience given the SOTIF background, listed in Table 6, further verified the key roles that trigger conditions play in resilience enhancement (see the third column). Functionality of specific systems [88-91] and situation awareness of the operating conditions [92-96] are two fundamental focuses for SOTIF risk mitigation and resilience enhancement, no matter for an individual intelligent vehicles or for a group of CAVs of cooperative driving [97-100]. There also exists the problem of ambiguity for the concept of resilience in several works [88-90, 97, 98]. It should be noted that SOTIF risks tightly depend on trigger conditions, i.e., specific scenarios or events that can activate the potential functional insufficiencies of a system, while it is the unanticipated interaction of a multitude of events that results in the unexpected behaviors or results [10], leading that there involve numerous adverse events and various types of uncertainties given

Just Accepted

SOTIF background. Therefore, research on resilience in the context of SOTIF can be quite challenging since some adverse events can be unknown and unpredictable, leading that the potential SOTIF risks are difficult to capture and the involved uncertainties are hard to describe (see discussion in Section 4.2).

Table 6 Related works on resilience given SOTIF background for CAV applications.

Work	Desired functionality (*F*)	Stressors (*A*)	Uncertainties involved (*U*)
Grimm *et al.* [88]	required functionality of the software or hardware of an autonomous vehicle	malfunctions of software or hardware, intentional manipulations	uncertainty of the hardware, network, and vehicle dynamics integrated in the software
Ängskog *et al.* [89]	required functionality of vehicular electronic systems and that of various sensors, controllers, and actuators	intentional electromagnetic interference	uncertainty in training data and the impact of the intentional electromagnetic interference
Lin *et al.* [90]	path tracking performance	operational and environmental changes, e.g., obstacles	model disturbance, state and control actions uncertainty
Hajdu *et al.* [91]	required functionality of the software or hardware	adverse factors in a military environment	UGV modelling complexity, uncertainty of the military environment
Yu *et al.* [92]	required functionality for autonomous driving	unusual weather conditions, abnormal vehicle behavior, abnormal road conditions	uncertainty of weather conditions, vehicle behavior, and road conditions
Rojas *et al.* [93]	lateral path tracking with acceptable tracking error	operational changes, like the increase of the vehicle speed	controller performance variation with speed
Rojas *et al.* [94]	lane-keeping	lane line occlusion, operational changes, e.g., the change of the vehicle speed	uncertainty of sensors, driving environment, vehicle states, road curvature, and driver response
Patil *et al.* [95]	lane detection performance	hazardous conditions like lane line occlusion, sensor failure, and environmental obstructions	uncertainty of sensor limitations and environmental conditions
Fang *et al.* [96]	required functionality of specific subsystems	environmental changes, adverse environmental factors	uncertainty of the driving scenarios
Caiazzo *et al.* [97]	individual vehicle stability and string stability for autonomous vehicle platoons	multiple input delays, uncertainties of the communication	uncertainty of the V2X links
Ge *et al.* [98]	individual vehicle stability and string stability for autonomous vehicle platoons	various uncertainties, such as unknown engine time lags, external disturbances, measurement noises, actuator anomalies, and unknown leader status	unknown engine time lags, external disturbances, measurement noises, actuator anomalies, and unknown leader status
Pirani *et al.* [99]	operational stability of a vehicle in a platoon	communication disturbance or anomalies	uncertainty of the ad-hoc network and vehicle model
Khan *et al.* [100]	platoon string stability	sustained communication delays and external disturbances	uncertainty in the communication delays and unknown disturbances

Critical Assessment. Resilience research in the SOTIF domain is less mature than in FUSA, reflecting the inherent difficulty of characterizing trigger conditions and performance limitations. Key observations from the reviewed literature include: **Maturity and scalability**: Knowledge-driven approaches (e.g., HARA, STPA) are systematic but labor-intensive and may miss unknown triggers. Data-driven approaches can uncover hidden scenarios from naturalistic driving data but require vast, diverse datasets that are expensive to acquire and annotate. The scalability of SOTIF resilience strategies to the long tail of rare but critical scenarios remains an open challenge. **Validation rigor**: Validation is predominantly simulation-based, with a growing emphasis on scenario-based testing. However, the fidelity of simulated sensor models and environmental conditions often limits the transferability of results to real-world operation. Exceptions include Rojas et al. [93, 94] and Patil et al. [95], the former demonstrate real-vehicle tests of resilience assessment for lateral path tracking and lane-keeping, and the latter report real-vehicle tests for lane detection under hazardous conditions. However, these tests cover only a limited set of pre-defined scenarios and are not easily generalized. **Treatment of uncertainty**: Epistemic uncertainty is central to SOTIF, yet few works quantify it explicitly. Most studies

Just Accepted

identify trigger conditions but do not estimate the confidence or bounds of system performance under those conditions. Exceptions include Peng et al. [79], who propose an online SOTIF entropy metric, but such quantification is not yet mainstream. The epistemic uncertainty inherent in trigger conditions and system limitations is acknowledged but not formally characterized. **Phase coverage**: Similar to FUSA, SOTIF studies emphasize the identification and mitigation of triggering events but rarely assess recovery behavior. The temporal dynamics of how a system returns to safe operation after a SOTIF-related degradation are largely neglected.

3.3 CAV resilience under cybersecurity considerations

Cybersecurity denotes the practice of safeguarding networks, devices, programs, and data against various cyber threats, with the explicit goal of ensuring the confidentiality (protection of data against unauthorized access and disclosure), integrity (preservation of the accuracy and completeness of data), and availability (assured access of authorized users to the required resources) of information and systems in the face of threats [101]. In the cybersecurity context, the desired functionality is therefore expressed in terms of these three properties, and resilience here amounts to maintaining the confidentiality, integrity, and availability of information and systems to a satisfactory extent under cyber threats and to recovering, or even strengthening, these properties once an adverse event has occurred. According to Eq. (1), the cyber risks arise from the uncertainty surrounding the threats, the system itself, and the various interactions among these factors, leading to uncertainty in the final consequences when faced with diverse cyber threats. From the resilience perspective, cybersecurity resilience is the complement to the risk of the system failing to achieve the desired functionality, over a specific time window, following a given threat. Numerous works have examined cyber threats against CAV applications [8, 9, 102–123]. Several commonly observed attack surfaces (the specific attack points through which adversaries attempt to compromise vehicle security) and attack types are summarized in Table 7 and Table 8, respectively, drawing on recent CAV cybersecurity surveys. Han et al. [114] systematically enumerate the principal security threats as false data, information theft, privilege escalation, blocked communication, and time delay. Qurashi et al. [121] categorize resilience techniques in the cybersecurity context into method-based and model-based approaches. The former focus on enhancing cybersecurity mechanisms and the latter on strengthening the system's resilience through modelling and analysis. Niroumand et al. [116] proposed a generalized attack function π, formulated as

$$(y_m, h_m, k_m, c_m, x_m, z_m, u_m, r_m, t_m) \triangleq \pi(y, h, k, c, x, z, u, r, t) \tag{3}$$

in which the authors show that cyber-attacks can alter the system output y, the controller behavior h, the decision-making result k, the communication channel c, the system states x, the sensory information (observation) z, the control signal u, the reference signal r, and the time t, with superscript "m" denoting the modified counterparts. For example, the false data injection attack (a member of the data-falsification family) targeting the state x can be expressed by Eq. (4), using Eq. (3) as the basis:

$$\pi_x(x,t) = x(t) + \varepsilon_x(t) \tag{4}$$

where $\varepsilon_x(t)$ represents the false data injected into the system states. Similarly, spoofing attack function π_z can be formulated by Eq.(5) in terms of Eq.(3):

Just Accepted

$$\pi_z(z,t) = z(t) + \varepsilon_z(t) \tag{5}$$

where $\varepsilon_z(t)$ represents the false data injected into the observations provided by the sensors.

Table 7 Several attack surfaces in CAV applications.

Attack surfaces	**Illustration**
Sensors	Exteroceptive sensors like cameras, LiDAR, radar, and ultrasonic sensors used for environmental perception, and proprioceptive sensors like localization sensors (e.g., GNSS receiver), inertial sensors, wheel speed sensors employed for system status monitoring, are vulnerable to attacks that can affect the vehicle's ability of situation awareness and state assessment.
Actuators	Components like throttle control, steering, and braking systems can be compromised to manipulate the vehicle's physical behavior.
In-vehicle networks	In-vehicle networks such as the Controller Area Network (CAN), which connect various Electronic Control Units (ECUs), can be attacked, leading to compromised control, physical damage, breaches of data integrity, service disruption, privacy violations, and similar consequences.
Telematics units	These units, which link vehicles to cellular networks and the Internet, can be compromised through Bluetooth, Wi-Fi, or cellular connections, allowing attackers to penetrate the vehicle's internal network.
V2X networks	V2X communication systems can be targeted to disrupt the exchange of information and control commands.
Edge computing and cloud infrastructures	Since CAVs rely on edge and cloud computing for processing and data storage, these infrastructures can be targeted for cyber-attacks and further impair the cybersecurity of CAVs.
Machine learning models	The machine learning algorithms in CAVs can be targeted with adversarial attacks that aim to deceive the AI systems into making incorrect decisions.
On-board diagnostics (OBD) port	The OBD port is a common physical access point that can be exploited to intercept data, inject malicious data frames, or even modify the software embedded in the vehicle's ECUs.
Firmware	Over-the-Air (OTA) firmware updates can be exposed to attacks involving the interception, modification, or injection of malicious firmware.

Table 8 Several attack types in CAV applications.

Attack types		**Meaning**
Sensor attacks	Spoofing attacks	Injecting false data into sensor observations to manipulate the vehicle's perception of its environment.
	Jamming attacks	Overwhelming sensors with noise or interference, impairing their ability to detect objects or receive signals.
	Blinding attacks	Temporarily or permanently disabling sensors, particularly cameras, with intense light sources.
In-vehicle network attacks	CAN bus attacks	Dropping data packets to disrupt network communications.
	ECU compromise	Compromising Electronic Control Units through various means, including physical access or network vulnerabilities.
External communication network attacks	Man-in-the-middle (MitM) attacks	Intercepting and altering communication between vehicle components or external entities.
	Denial of service (DoS) attacks	Disrupting the availability of communication services by overwhelming the network with traffic.
	Sybil attacks	Creating multiple fake identities to manipulate consensus or reputation systems.
	Impersonation attacks	Masquerading as legitimate entities within the network to inject false information or commands.
	Blackhole attacks	Dropping data packets to disrupt network communications.
Firmware and software attacks	Firmware manipulation	Altering or replacing firmware during OTA updates in order to introduce malicious functionality.
	Malicious code injection	Injecting malware or viruses into the vehicle's software to gain control or disrupt operations.
Physical access attacks	OBD port attacks	Exploiting the OBD port for unauthorized access to vehicle systems.
	Hardware tampering	Physically altering or manipulating hardware components to cause malfunctions or introduce vulnerabilities.
Machine learning and AI attacks	Adversarial attacks	Using specially crafted inputs to deceive machine learning models, leading to incorrect decision-making.
	Data poisoning	Corrupting the training data of AI systems to affect their behavior or performance.
Side-channel attacks		Exploiting information leaked through side channels, such as power consumption or electromagnetic emissions, in order to infer cryptographic keys or other sensitive data.
Replay attacks		Recording and retransmitting valid data packets to deceive the system.
Data falsification		Altering or injecting false data into the vehicle's systems to cause misbehavior.
Timing attacks		Exploiting the timing of cryptographic operations or system responses in order to extract sensitive information or to manipulate system behavior.

Just Accepted

The summary of the characteristics for attack surfaces and attack types adds prior knowledge on the commonly seen cyber threats in CAV applications, decreasing the epistemic uncertainty of potential adverse events (corresponding to the events A defined in the triplet by Eq. (1) and Eq. (2) in the context of cybersecurity, so that countermeasures can be pertinently designed and employed to deal with these cyber threats and enhance system resilience. Some countermeasures are concluded based on the surveys or reviews on cybersecurity in CAV applications [8, 9, 102-120], shown in Table 9.

Table 9 Several countermeasures for guaranteeing cybersecurity in CAV applications.

Countermeasures	**Illustration**
Encryption and cryptographic techniques	Using symmetric and asymmetric encryption methods to secure data transmission and storage, preventing unauthorised access, and safeguarding data integrity.
Intrusion detection	Deploying signature-based and anomaly-based detection systems in order to identify and respond to malicious activities by comparing traffic against known attack signatures or detecting anomalous behavior.
Multi-factor authentication	Implementing multi-factor authentication mechanisms to add layers of security, making it more difficult for attackers to gain unauthorised access.
Secure communication protocols	Developing and using secure communication protocols for in-vehicle networks.
Secure OTA	Ensuring secure OTA updates for firmware and software with integrity checks, authentication, and encryption to prevent firmware tampering and control override attacks.
Role-based access control (RBAC)	Applying RBAC to limit access to sensitive vehicle systems, ensuring only authorized entities can perform critical operations.
Physical security measures	Enhancing the physical security of components like OBD ports to prevent unauthorized physical access and tampering.
Network Segmentation and Isolation	Segmenting vehicle networks to limit the spread of attacks and isolating critical systems from less critical ones.
Security audits and penetration testing	Regularly conducting security audits and penetration tests to identify vulnerabilities and test the effectiveness of defence mechanisms.
Formal verification methods	Employing formal verification methods to mathematically prove the correctness of security mechanisms and identify potential vulnerabilities during the design phase.
Threat profiling	Creating real-time threat profiles in order to enable deeper analysis and provide greater transparency for dealing with uncertain system behaviors and common security problems.
Standards and regulations	Developing and adhering to industry standards and regulations for automotive cybersecurity, such as ISO/SAE 21434.

The attack surfaces, attack types, and countermeasures surveyed above provide informative and insightful viewpoints of the resilience studies, given the background of cybersecurity in CAV applications. Items listed in Table 10 are several recent advances of CAV cyber resilience in literature, involving the functionality of basic CAV systems [124-126], functionality of the communication network [127, 128], the resilient strategies of maintaining cooperative driving against the threat of cyber-attacks [129-134], and cyber resilience of CAVs in traffic and transportation backgrounds [135-138]. Some works consider to establish the dimensions to describe and evaluate resilience in the background of cybersecurity. For example, in [139], a method for evaluating the cybersecurity risks associated with CAVs was proposed, where the method incorporated cyber resilience into the risk assessment process by introducing criteria including probability (of adverse events), impact (of adverse events), exposure (of the system in threats) and recovery. Some scholars also studied the trust model to enhance resilience against cyberattacks, which involves the analysis of critical nodes or links, like the works conducted by Wang *et al.* [140] and Ahmad *et al.* [141]. Most of the works above illustrate the strategies to enhance cyber resilience but fail to clearly define the concept of resilience in specific applications. Besides, the word “resilience” (or “resilient”, “resiliency”, etc.) is often misused with “robustness”, “resistance”, “recovery”, “fault-tolerance”, and among others. In regard to adverse

Just Accepted

events in the context of cybersecurity, most of the works above analyzed the types and characteristics of attacks in detail and proposed corresponding strategies in response to the adversity. Nevertheless, studies on the involved uncertainties should be further and structurally investigated to provide insights for cyber resilience enhancement.

Table 10 Some recent advances in cyber resilience in CAV applications.

Work	**Desired functionality (*F*)**	**Stressors (*A*)**	**Uncertainties involved (*U*)**
Wang *et al*. [124]	tracking a desired path	intermittent DoS attacks	uncertainty of vehicle models, DoS attacks, and vehicle operations
Qurashi *et al*. [125]	safety operation and required functionality of a CAV like perception, localization, planning, decision-making, control, etc.	cyber-attacks	uncertainty of data availability and quality, attacks, and environmental factors
Ayrault *et al*. [126]	quality of service of the embedded systems	cyber-attacks	uncertainty of input parameters and various types of attacks
Li *et al*. [129]	individual vehicle stability and string stability for autonomous vehicle platoons	actuator attacks	uncertainty of actuator attacks, communication delay, and system disturbance
Caiazzo *et al*. [130]	individual vehicle stability and string stability for autonomous vehicle platoons, safe inter-vehicle spacing, and speed synchronization	DoS attacks and communication delays	uncertainty of communication delay and DoS attacks
Ge *et al*. [131]	individual vehicle stability and string stability for autonomous vehicle platoons, collision avoidance	intermittent DoS attacks	uncertainty of the vehicle states, measurement noise, and status of the leader
Safi *et al*. [132]	consensus on longitudinal position and velocity	malicious agents in a network of vehicles	uncertainty of malicious vehicle behavior, network topology, and communication delays
Khoshnevisan and Liu [133]	consensus on velocity/acceleration and maintaining safe inter-vehicle distances for heterogeneous platoons	deception attacks and external disturbances	unknown vehicle nonlinearities, uncertainty of the deception attacks and disturbance
Wei *et al.* [134]	individual vehicle stability and string stability for autonomous vehicle platoons, safe inter-vehicle spacing	FDI attacks	uncertainty of the FDI attacks and human behaviors
Mahbub *et al*. [127]	reliable in-vehicle communication	spoofing, replay, and side-channel attacks	uncertainty of various attacks and the coupling of different components and subsystems
Yue *et al*. [128]	individual vehicle stability and string stability for autonomous vehicle platoons, quality of service of the communication	DoS and deception attacks	uncertainty of attacks, external disturbance, communication delay, and vehicle dynamics
Wang *et al*. [135]	to maintain safe following distances and restore traffic flow stability	cyber-attacks	uncertainty of the car-following model, cyberattack types, and sensor data
Al Mallah *et al*. [136]	optimizing the signal timings at intersections to reduce delays, minimize congestion, and improve traffic flow efficiency, and being responsive to traffic demands	coordinated sybil attack	uncertainty of the status of traffic flow and threat model
Boddupalli *et al*. [137]	traffic safety and efficiency	cyber-attacks	uncertainty of data collection and processing process, and adversarial attacks
Zou *et al*. [138]	vehicle level: basic functions like perception, localization, planning, control, etc. traffic-system-level: proper traffic conditions and accident avoidance	cyber-attacks	uncertainty of attack forms and system status
Park & Park [139]	secure OTA and collision avoidance	cyber-attacks	uncertainty of real-world scenarios, various attacks, and human factors
Wang *et al*. [140]	security and reliability of the IoV networks	cyber-attacks	uncertainty of the trust model and data collection process
Ahmad *et al*. [141]	collision avoidance, congestion mitigation	adversarial attacks and uncooperative behavior of other vehicles	uncertainty of the trust model and the behavior of adversarial agents

Just Accepted

Critical Assessment. Cyber resilience for CAVs has attracted substantial research attention, resulting in a rich body of countermeasures. Nevertheless, the reviewed literature reveals several critical gaps. **Maturity and scalability**: While cryptographic and intrusion detection techniques are relatively mature, their real-time performance on automotive-grade hardware with limited computational budget remains a concern. Moving target defense and adaptive countermeasures show promise but are still at early stages of maturity. **Validation rigor**: Many proposed cyber resilience strategies are validated only in simulation or on small-scale testbeds, and full vehicle-level validation under realistic attack scenarios is scarce. The effectiveness of defenses against adaptive adversaries that evolve their attack strategies is rarely evaluated. **Treatment of uncertainty**: Uncertainty in cybersecurity is predominantly epistemic, stemming from unknown attack vectors and adversary behaviors. Most works model attacks as deterministic or bounded disturbances, with limited attention to probabilistic threat modeling or uncertainty quantification. Trust-based approaches [140, 141] partially address this by incorporating belief degrees, but systematic uncertainty management remains underexplored. **Phase coverage**: Cyber resilience research often focuses on attack detection and prevention, with comparatively less emphasis on recovery and post-attack system restoration. The speed and completeness of recovery after a successful intrusion are critical metrics that deserve more attention.

FUSA, SOTIF, and cybersecurity issues can be interrelated and some works studied system resilience across FUSA, SOTIF, and cybersecurity. To instantiate, Kahlert *et al.*, [142] comprehensively reviewed resilience in spatial environmental perception systems for fully automated driving. It defined resilience as the system's ability to dependably generate an accurate model of the vehicle's surroundings despite internal disturbances (e.g., hardware/software failures) and external disturbances (e.g., adverse weather, sensor interference). The work systematically analyzed the strengths and weaknesses of core sensor technologies, explores sensor fusion strategies to mitigate individual sensor limitations, and examines fault-tolerant E/E architectures incorporating redundancy topologies and safety standards (ISO 26262, ISO 21448, ISO 21434). Based on this analysis, the authors proposed a holistic framework for resilient spatial perception, integrating robust sensing, data processing, architectural design, and countermeasures against disturbances. The authors finally concluded by highlighting key research challenges, including managing increasing sensor complexity, ensuring cybersecurity, and enabling reliable operation in all conditions.

The structured review and critical assessment across FUSA, SOTIF, and cybersecurity highlights several cross-cutting research gaps. First, recovery-phase resilience remains underexplored in all three domains, since most existing works focus on resisting or absorbing adversity but provide limited insight into the restoration dynamics that follow. Second, uncertainty quantification is still rudimentary: uncertainty is acknowledged but rarely leveraged for resilience enhancement. Third, validation practice is heavily skewed towards simulation, with scarce real-world testing under fault injection, rare SOTIF scenarios, or live cyberattacks. Fourth, there is a notable lack of cross-domain integration, as resilience strategies developed for FUSA, SOTIF, and cybersecurity are rarely examined for their interactions or combined effects. The (*A*,

Just Accepted

F, *U*) framework proposed in this paper is designed to address these gaps by providing a unified language and evaluation structure that spans domains and phases.

To summarize, this section has reviewed resilience strategies across FUSA, SOTIF, and cybersecurity through the lens of the risk-based, functionality-centered triplet (*A*, *F*, *U*), highlighting empirical implementations, knowledge gaps, and domain-specific challenges. FUSA resilience centers on the preservation of core functionalities (*F*) against component faults and failures (*A*) through fault diagnosis, fault-tolerance, and prognostic health management, with redundancy as the main measures for resilience enhancement, and the principal uncertainties (*U*) concern the unpredictability of fault propagation and gaps in diagnostic coverage. SOTIF resilience addresses functional insufficiencies triggered by environmental or operational stressors (*A*) through trigger-condition analysis and performance-boundary identification, and epistemic uncertainties (*U*) rooted in black-box algorithms and incomplete scenario coverage remain major obstacles to maintaining the holistic system functionality (*F*). Cybersecurity resilience preserves the confidentiality, integrity, and availability of information (*F*) against attacks (*A*) by means of encryption and intrusion detection, with threat mutability as the principal uncertainty (*U*).

4 Discussion

4.1 Functionality resilience: beyond robustness, recovery, and fault-tolerance

In literature, the word "resilience" (or "resilient", "resiliency", etc.) is increasingly used but connotations of resilience in many situations are ambiguous and reminiscent of the concepts like "robustness", "resistance", "recovery", "adaptability", "fault-tolerance", and among others. In fact, all these concepts depict how a system responds to events (usually adverse or negative). Review of the concept of resilience in Section 2, showed that it involves the characteristics of *withstanding the negative impact in adversity* and *recovering to the expected status after the adverse event*. The former is reminiscent of robustness or resistance, and the latter is reminiscent of recovery or adaptability. In addition, the trait of responding to adverse events is reminiscent of fault-tolerance. Therefore, the terminology "resilience" is often interchangeably used with these mentioned terms in many works to describe the characteristics of a system responding to (adverse or negative) events. However, the concept of resilience should be beyond robustness, recovery, and/or fault-tolerance and this interchangeable use has not benefited CAV deployment.

Robustness describes the ability of a system to withstand or overcome adverse conditions without structural changes, so that the system retains its initial state both during and after a specific adverse event [18]. It also concerns the sensitivity of the system output to parametric changes or bounded disturbances [23]. Robustness is typically achieved by over-provisioning, redundancy, and predictive models that account for known uncertainties and antagonistic conditions, and is concerned with the maintenance of functionality in the presence of adverse events [23]. By contrast, when faced with adverse events, resilience calls for system-wide transformation through reconfiguration, adaptation, or growth in order to preserve functionality or to minimize the time during which functionality is compromised, and therefore requires more

Just Accepted

flexible and adaptive responses [23], opening new opportunities for resilience to complement robustness.

Recovery refers to the restoration of a system to its expected state [17], namely the return to a previous state or the transition to another steady state after an event has occurred. Recovery is one of the traits of resilience (or one of the phases through which a resilient system responds to adversity). Adaptability refers to the capacity of an agent to adjust itself in order to perform its intended functions in a new environment. In the CAV context, adaptability is the ability of a system to modify its functioning and structures in order to cope effectively with the complexities of real-world traffic scenarios, including the variety of traffic conditions, the highly dynamic driving environment, and the uncertainties surrounding the behavior of different traffic participants. In contrast to resilience, both recovery and adaptability neglect the absorption phase of the adversity response.

Fault-tolerance denotes the ability of a system to continue its operation regardless of faults [50]. Works that use "resilience" and "fault-tolerance" interchangeably implicitly assume that faults are the only source of adversity. However, as already noted in Section 3, the forms of adverse events span at least 1) hardware/software faults or failures, 2) unexpected inputs, and 3) maliciously induced failures or security attacks [45]. Faults and failures constitute only one class of source of negative system impact. In CAV applications, apart from maliciously induced failures or attacks, most road-vehicle safety risks do not originate from component or system faults/failures but from the unanticipated interaction of several events [10] that trigger potential functional insufficiencies of a system. According to the California Department of Motor Vehicles, more than 90% of the takeovers during real-world CAV testing stemmed from SOTIF issues, while takeovers owing to FUSA issues accounted for only 0.28% [143]. Although both resilience and fault-tolerance emphasize the response to adverse events, a resilient system should tolerate a far broader range of adversity than faults alone, namely what may be termed adversity-tolerance, with particular attention to the uncertainty of trigger conditions that activate functional insufficiency and lead to SOTIF risks.

Resilience integrates all these aspects in a unified form. If taken in a unified form under functionalities, it allows to better understand how these interact such that strategies to enhance resilience are more comprehensively designed. For example, a system may be robust and experience a small loss of functionality when adversity impacts, but it can be less resilient than another that experiences higher loss of functionality but that recover it very fast, if it has a slow recovery of that functionality. This remarks that comprehensively looking in an integrated form to all these aspects related to withstanding and recovering from adversity can lead to better outcomes for the system resilience enhancement, and further, dynamic risk containment to guarantee road vehicle safety. A critical distinction elevating resilience above related concepts lies in its intrinsic reliance on functionality (F) as its primary metric. Unlike robustness (which emphasizes structural integrity), recovery (focused on restoration timelines), or fault-tolerance (concerned with operation continuity), resilience quantifies system performance through the *sustained delivery of intended functionalities* under adversity. This functionality-centered perspective offers three key advantages:

Just Accepted

1) Full-event phase view: Functionality explicitly captures both the *absorption* (magnitude of performance dip) and *recovery* (rate and completeness of rebound) phases inherent in resilience. Robustness only addresses the absorption dip, while recovery focuses solely on the rebound. Functionality integrates both, providing a complete picture of system response.

2) Risk-aligned quantification: As defined by the triplet (*A*, *F*, *U*), functionality *F* is inherently linked to risk. The level of maintained/recovered functionality directly determines whether the system operates within an "acceptably low-risk envelope" (Section 2.2 & 2.3). A small dip or rapid recovery in F translates to contained risk, making *F* a direct proxy for safety outcomes.

3) Unified benchmark for diverse strategies: Functionality provides a common, measurable benchmark to evaluate *any* resilience-enhancing strategy, whether it aims to improve robustness (minimizing F dip), accelerate recovery (speeding *F* rebound), enhance adaptability (enabling new F optimization), or ensure fault-tolerance (sustaining core *F*). This enables comparative assessment of disparate techniques under a unified resilience goal.

4.2 Challenges of SOTIF Risks for Resilience Enhancement

Having delineated resilience as an integrative concept surpassing fragmented approaches like robustness, recovery, and fault-tolerance, particularly through its functionality-centered view, one of the most pressing challenges for resilience implementation is required further addressed: SOTIF risks. Unlike FUSA or cybersecurity, there are no explicit "adverse events" in SOTIF, and inherent uncertainty in trigger conditions and system limitations presents unique complexity. This section will dissect uncertainties underpinning SOTIF-driven adversity, illustrating how functional insufficiencies arise from environmental, algorithmic, and interaction complexities. This analysis reveals why SOTIF demands a paradigm shift toward resilience-by-design and resilience-by-response, fundamentally tied to functionality assurance under uncertainty.

As already noted in Section 2.2, resilience is the complement to the risk of the system failing to achieve the desired functionality, over a specific time window, following an event. Functionality was highlighted as an avenue for replacing consequences *C*, providing a foundation for resilience in the CAV field. The challenge posed by SOTIF risks to resilience enhancement stems from the highly intricate uncertainty surrounding events *A* in the SOTIF context: in practice the system may believe it has preserved its functionality, yet the residual risks in the SOTIF background arise from the uncertainty of the trigger conditions and from the uncertainty of the performance limitations activated by those trigger conditions in specific scenarios. Analyzing the uncertainty of trigger conditions is therefore far from trivial. Several triggers that may lead to functional insufficiency are listed in Table 5 in Section 3.2. Roughly speaking, the uncertainty of trigger conditions stems from (but is not limited to) the following sources.

1) inherent limitations or constraints of a system (or its subsystems). Limitations or constraints of a system (or its subsystems) can be a relative concept in relation to the tasks that a system is required to conduct and the complexity of the operational environment. All systems have limitations or constraints, and the difficulty lies in what adversities the limitations or constraints do affect the system and lead to SOTIF risks, i.e., how sufficient of specific functionalities is sufficient? To accommodate to all situations is extremely challenging and the

Just Accepted

key is to know the performance boundaries of a system in specific scenarios (that translate in functionalities) so that the probability of limitations or constraints triggering functional insufficiency is sufficiently or acceptably low.

2) driving environments and other traffic participants. The complexity of the driving environment generates a number of trigger conditions that activates functional insufficiency, including but not limited to weather conditions, illumination, road conditions, various traffic scenarios, among other. Besides, the behaviors of diverse traffic participants can be unanticipated. Owing to the highly dynamic nature of the driving scenarios, how these environmental factors and participants interact with each other is quite uncertain and such interactions will generate countless events that exceed the response ability of the system and leads to SOTIF risks. As such, functionalities should be known for their operational boundaries.

3) algorithms/models and data (with particular attention to black-box models such as deep neural networks). Model uncertainty may originate from incomplete requirement analysis, insufficient or biased training data, improper model design, and inadequate training, all of which leave gaps and ambiguities in the understanding of the system status diagnosis and the situation awareness of the driving environment [76]. Data uncertainty concerns the quality of the data used to train and to operate an algorithm. Inaccurate labelling of training data, noisy sensor data, and variations in real-world conditions not anticipated during model training all contribute to data uncertainty, which in turn produces incorrect and unstable perceptions and decision-making [76]. In addition, the widespread use of artificial intelligence (AI) algorithms, particularly deep learning models, in CAV applications means that the black-box behavior exhibited by many machine-learning models makes it difficult to follow the underlying reasoning and decision-making processes. This opacity creates challenges for the analysis of critical safety requirements and for model validation, as well as for comprehending the logic underlying decisions [76], thereby contributing to the uncertainty of the results and undermining the confidence that one can place in the outputs of AI algorithms.

4) the way in which all of the above factors interact. As pointed out by Dekker et al. [10], safety risks, and even accidents, primarily arise from the unanticipated interaction of a multitude of events, and a consequence (such as an incident or an accident) is an emergent behavior that cannot be reduced to a description of independent factors. It is the outcome of complex interactions and relationships among the involved factors and the environment in which they operate [15, 35].

SOTIF research can be partitioned into three key phases: the development phase, the verification and validation (V&V) phase, and the operation phase. For resilience enhancement under the SOTIF background, the first two phases correspond to resilience-by-design while the operation phase corresponds to resilience-by-response. Wang et al. [76] summarize several measures to mitigate SOTIF risks across these phases, which provide useful guidance for resilience enhancement in the SOTIF context. In the development phase, key measures include hazard analysis and risk assessment (HARA) using safety-analysis tools such as fault tree analysis (FTA), failure mode and effects analysis (FMEA), hazard and operability analysis (HAZOP), and system-theoretic process analysis (STPA) to identify and assess potential hazards and risks, together with the development of explainable AI algorithms and the reduction of

Just Accepted

uncertainty at every stage of the pipeline, including requirement analysis, data acquisition and processing, and model design and training. In the V&V phase, techniques of verification, falsification, and testing can be deployed to ensure that components satisfy the functional requirements and that the residual risk is acceptable. In the operation phase, runtime monitors for system-status diagnosis and situational awareness of the surroundings should be employed, with strategies such as anomaly detection and uncertainty quantification.

In summary, enhancing resilience against SOTIF risks requires confronting multifaceted uncertainties: 1) the stochastic interplay of system limitations, environmental dynamics, and unpredictable traffic participants, 2) the black-box opacity of AI-driven perception and decision-making, and 3) risks arising from unanticipated interactions within complex scenarios. Crucially, resilience here hinges on the quantification and bounding of the functionality (F) under adversarial trigger conditions (A), while explicitly modelling the uncertainty (U). As depicted in Fig. 3 in Section 3.2, resilience must proactively break the trigger-to-accident sequence by anchoring safety to the sustained delivery of functionality throughout the adversity lifecycle. Across the three SOTIF phases, namely the development phase, the V&V phase, and the operation phase, functionality-centered resilience should be embedded into SOTIF management, shifting the focus from isolated tactics aimed at guaranteeing specific system properties (robustness, recovery, fault-tolerance, and so on) towards holistic risk containment. Moreover, functionality-centered resilience, with uncertainty treated explicitly, establishes a direct relationship with the issues that produce SOTIF shortcomings. Resilience with respect to SOTIF can use functionality as a matter of belief regarding the uncertainty attached to the functionality, in a manner highly compatible with a risk-based approach in which beliefs play a central role. Empirically, this means that the resilience of the system under adversity can be ensured by combining the targeted functionality with the contextual uncertainty surrounding it.

5 Conclusion

The safe large-scale deployment of CAVs remains critically impeded by unresolved road vehicle safety challenges. This paper has argued that functionality-centered resilience, formalized through a risk-based triplet (A, F, U) encapsulating adverse events, functionalities, and associated uncertainties, offers a unified lens for addressing these challenges across the domains of FUSA, SOTIF, and cybersecurity. Innovative works are threefold:

1) Formalizing resilience: The functionality-centered resilience framework is established, explicitly linking it to risk through the (A, F, U) framework. The framework shifts the emphasis from avoiding negative consequences to sustaining critical functionalities under adversity, thereby enabling a more proactive and phase-aware approach to risk management.

2) Bridging resilience and road vehicle safety: How resilience manifests across the three strands of road vehicle safety are demonstrated, i.e., mitigating risks via the measures of fault diagnosis, fault-tolerance, and prognostic health management given FUSA background, addressing functional insufficiencies triggered by environmental/operational uncertainties in SOTIF context, and ensuring functionality preservation against malicious threats for cybersecurity.

Just Accepted

3) Unifying fragmented concepts: Resilience is positioned as an integration of several isolated attributes (robustness, recovery, adaptability, fault-tolerance, among other), emphasizing that functionality (F) serves as the universal metric for evaluating system response across all adversity phases (i.e., absorption and recovery).

The structured review of recent advances has shown that while resilience strategies exist in each safety domain, they are often developed in isolation and lack a common basis for quantification and comparison. The critical assessment further reveals that resilience in the recovery-phase, uncertainty quantification, and cross-domain integration remain underexplored. For future works, the benefit of an integrated studying of resilience following the triplet (A, F, U) in different CAV applications remains to be further exploited. Application specific studies may further unlock the potential of this rationale. Efforts should prioritize quantifying resilience using the (A, F, U) framework to enable cross-domain benchmarking. Besides, how to validate resilience in real-world edge cases, particularly for SOTIF-driven scenarios, is worth exploring. By adopting functionality-centered resilience as a unified design philosophy, i.e., sustaining functionality within an acceptably low-risk envelope, the path toward safer CAV systems can be accelerated.

Just Accepted

Funding

This research is supported in part by Scientific Research Foundation for High-level Talents of Anhui University of Science and Technology (2025yjrc0012), China Postdoctoral Science Foundation – Anhui Joint Support Program (2026T009AH), Open project supported by Hubei Provincial Key Laboratory of Automotive Power Train and Electronic Control (ZDK12026B02), and Open project supported by Anhui Provincial Key Laboratory of Traffic Information and Safety (JTX202604).

Declaration of competing interest

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

Author contribution statement

Yukun Fang: Conceptualization, Methodology, Formal analysis, Investigation, Writing – original draft, review & editing. Rui Teixeira: Conceptualization, Methodology, Formal analysis, Writing – review & editing. Gongda Hu: Writing – review & editing. Haigen Min: Conceptualization, Supervision. Xiangmo Zhao: Conceptualization, Supervision.

Data availability statement

Data sharing is not applicable to this article as no new data were created or analyzed in this study.

Use of AI statement

During the preparation of this work the author(s) used DeepSeek to improve the readability and language of the manuscript. After using this tool, the authors reviewed and edited the content as needed and take full responsibility for the content of the publication

References

[1] A. Eskandarian, C.X. Wu, C.Y. Sun, Research Advances and Challenges of Autonomous and Connected Ground Vehicles, IEEE T Intell Transp, 22 (2021) 683-711.

[2] M. Taiebat, A.L. Brown, H.R. Safford, S. Qu, M. Xu, A Review on Energy, Environmental, and Sustainability Implications of Connected and Automated Vehicles, Environ Sci Technol, 52 (2018) 11449-11465.

[3] Z.H. Yao, Y. Wang, B. Liu, B. Zhao, Y.S. Jiang, Fuel consumption and transportation emissions evaluation of mixed traffic flow with connected automated vehicles and human-driven vehicles on expressway, Energy, 230 (2021).

[4] P. Koopman, M. Wagner, Autonomous Vehicle Safety: An Interdisciplinary Challenge, IEEE Intel Transp Sy, 9 (2017) 90-96.

[5] Technical Committee ISO/TC 22, Road Vehicles- Functional Safety ISO 26262: 2018, in, International Organization for Standardization, Switzerland, 2018.

[6] Technical Committee ISO/TC 22, Road Vehicles- Safety of the Intended Functionality: ISO 21448: 2022, in, International Organization for Standardization, Switzerland, 2022.

[7] Technical Committee ISO/TC 22, Road Vehicles- Cybersecurity Engineering: ISO 21434: 2021, in, International Organization for Standardization, Switzerland, 2021.

[8] Y.K. Fang, H.G. Min, X. Wu, W.Q. Wang, X.M. Zhao, B. Martinez-Pastor, R. Teixeira, Anomaly diagnosis of connected autonomous vehicles: A survey, Inform Fusion, 105 (2024).

[9] X.M. Zhao, Y.K. Fang, H.G. Min, X. Wu, W.Q. Wang, R. Teixeira, Potential sources of sensor data anomalies for autonomous vehicles: An overview from road vehicle safety perspective, Expert Syst Appl, 236 (2024).

[10] S. Dekker, P. Cilliers, J.H. Hofmeyr, The complexity of failure: Implications of complexity theory for safety investigations, Safety Sci, 49 (2011) 939-945.

[11] C. Berger, P. Eichhammer, H.P. Reiser, J. Domaschka, F.J. Hauck, G. Habiger, A Survey on Resilience in the IoT: Taxonomy, Classification, and Discussion of Resilience Mechanisms, ACM Comput Surv, 54 (2021).

[12] R.K. Liu, Y.L. Ren, H.Y. Yu, Z.H. Li, H. Jiang, Connected and automated vehicle platoon maintenance under communication failures, Veh Commun, 35 (2022).

[13] E. Abolfarzli, B. Besselink, T. Charalambous, On Time Headway Selection in Platoons Under the MPF Topology in the Presence of Communication Delays, IEEE T Intell Transp, 23 (2022) 8881-8894.

[14] Y. Fang, H. Min, X. Wu, X. Zhao, X. Wang, G. Li, R. Teixeira, Resilience-Oriented Oscillation Dampening for Connected Autonomous Vehicle Platoons, IEEE Transactions on Vehicular Technology, 73 (2024) 16024-16040.

Just Accepted

[15] T.M. Logan, T. Aven, S.D. Guikema, R. Flage, Risk science offers an integrated approach to resilience, Nat Sustain, 5 (2022) 741-748.

[16] B. Martinez-Pastor, Resilience of traffic networks to extreme weather events: analysis and assessment, in, Trinity College Dublin, 2017.

[17] F. Barber, M.A. Salido, Robustness, stability, recoverability, and reliability in constraint satisfaction problems, Knowl Inf Syst, 44 (2015) 719-734.

[18] Y.M. Zhou, J.W. Wang, H. Yang, Resilience of Transportation Systems: Concepts and Comprehensive Review, IEEE T Intell Transp, 20 (2019) 4262-4276.

[19] S. Zheng, K. Pan, Y. Chen, J. Liu, E. Zio, Causality-enhanced system reliability and safety analysis: An overview, Reliab Eng Syst Safe, 270 (2026) 112109.

[20] O. Eigner, S. Eresheim, P. Kieseberg, L.D. Klausner, M. Pirker, T. Priebe, S. Tjoa, F. Marulli, F. Mercaldo, Towards Resilient Artificial Intelligence: Survey and Research Issues, in: Proceedings of the 2021 IEEE International Conference on Cyber Security and Resilience (IEEE CSR), 2021, pp. 536-542.

[21] F.O. Olowononi, D.B. Rawat, C. Liu, Resilient Machine Learning for Networked Cyber Physical Systems: A Survey for Machine Learning Security to Securing Machine Learning for CPS, IEEE Commun Surv Tut, 23 (2021) 524-552.

[22] P. Shi, B. Yan, A Survey on Intelligent Control for Multiagent Systems, IEEE T Syst Man Cy-S, 51 (2021) 161-175.

[23] A. Prorok, M. Malencia, L. Carlone, G.S. Sukhatme, B.M. Sadler, V. Kumar, Beyond robustness: A taxonomy of approaches towards resilient multi-robot systems, arXiv preprint arXiv: 2109.12343, (2021).

[24] T. Ji, Y.H. Yao, Y. Dou, S.J. Deng, S.J. Yu, Y.Q. Zhu, H.J. Liao, The Impact of Climate Change on Urban Transportation Resilience to Compound Extreme Events, Sustainability-Basel, 14 (2022).

[25] M. Taghizadeh, M. Mahsuli, Probabilistic modeling of the risk and resilience of transportation systems for community resilience analysis, Reliab Eng Syst Safe, 271 (2026) 112073.

[26] R. Azargoshasbi, M.A. Esfeh, L. Kattan, Urban road network resilience assessment framework: Integrating spatiotemporal analysis with the resilience triangle and temporal performance indicators, Reliab Eng Syst Safe, 266 (2026) 111742.

[27] C.A. Davis, Understanding Functionality and Operability for Infrastructure System Resilience, Nat Hazards Rev, 22 (2021).

[28] X. Wang, H. Du, Y. Dang, X. Pan, Resilience evaluation and recovery strategy optimization for unmanned system-of-systems considering relay communication, Reliab Eng Syst Safe, 274 (2026) 112444.

[29] I. Linkov, B.D. Trump, J. Keisler, Risk and resilience must be independently managed, Nature, 555 (2018).

[30] L. Pinciroli, S.A. Hosseini, M. Chen, M.V.C. Mesa, T.M. Coscia, J.-P. Futalef, S. Marchetti, L. Miqueles, S.T. Menza, E. Zio, Risk assessment for modern industry, Reliab Eng Syst Safe, 269 (2026) 112126.

[31] N. Leveson, Safety III: A systems approach to safety and resilience, MIT Eng. Syst. Lab, 16 (2020).

[32] T. Aven, A risk science perspective on the discussion concerning Safety I, Safety II and Safety III, Reliab Eng Syst Safe, 217 (2022).

Just Accepted

[33] T. Vairo, S. Guarino, A. Benvenuto, B. Fabiano, R. Setola, Emergent risks in complex systems: A Bayesian perspective on uncertainty and prediction, Reliab Eng Syst Safe, 270 (2026) 112129.

[34] I. Glette-Iversen, R. Flage, T. Aven, Extending and improving current frameworks for risk management and decision-making: A new approach for incorporating dynamic aspects of risk and uncertainty, Safety Sci, 168 (2023) 106317.

[35] K. Anna, T.M. Logan, Resilience: Lessons to be learned from safety and acceptable risk, J Saf Sci Resil, 2 (2021) 253-257.

[36] M. Yang, H. Sun, S.Y. Geng, On the quantitative resilience assessment of complex engineered systems, Process Saf Environ, 174 (2023) 941-950.

[37] H. Sun, M. Yang, H. Wang, An integrated approach to quantitative resilience assessment in process systems, Reliab Eng Syst Safe, 243 (2024) 109878.

[38] P.C. Haritha, M.V.L.R. Anjaneyulu, Comparison of topological functionality-based resilience metrics using link criticality, Reliab Eng Syst Safe, 243 (2024) 109881.

[39] W. He, Z. Jiang, T. Xiao, Z. Xu, Y. Li, A Survey on Uncertainty Quantification Methods for Deep Learning, ACM Comput Surv, 58 (2026) 1-35.

[40] T. Chakraborti, C.R.S. Banerji, A. Marandon, V. Hellon, R. Mitra, B. Lehmann, L. Bräuninger, S. McGough, C. Turkay, A.F. Frangi, G. Bianconi, W. Li, O. Rackham, D. Parashar, C. Harbron, B. MacArthur, Personalized uncertainty quantification in artificial intelligence, Nature Machine Intelligence, 7 (2025) 522-530.

[41] W. Shao, J. Xu, Z. Cao, H. Wang, J. Li, From Prediction to Planning: Comprehensive Uncertainty Management in Autonomous Driving, IEEE T Intell Transp, 26 (2025) 16466-16480.

[42] K. Yang, X. Tang, J. Li, H. Wang, G. Zhong, J. Chen, D. Cao, Uncertainties in Onboard Algorithms for Autonomous Vehicles: Challenges, Mitigation, and Perspectives, IEEE T Intell Transp, 24 (2023) 8963-8987.

[43] K. Wang, C. Shen, X. Li, J. Lu, Uncertainty Quantification for Safe and Reliable Autonomous Vehicles: A Review of Methods and Applications, IEEE T Intell Transp, 26 (2025) 2880-2896.

[44] J. Mandouri, A.F. Taha, H. Baroud, C. Philip, P. Johnson, S. Mahadevan, Uncertainty quantification and reliability assessment for intermodal freight transportation, Reliab Eng Syst Safe, 268 (2026) 111996.

[45] S. Bagchi, V. Aggarwal, S. Chaterji, F. Douglis, A. El Gamal, J.W. Han, B.J. Henz, H. Hoffmann, S. Jana, M. Kulkarni, F.X. Lin, K. Marais, P. Mittal, S.S. Mou, X.K. Qiu, G. Scutari, Vision Paper: Grand Challenges in Resilience: Autonomous System Resilience through Design and Runtime Measures, IEEE Open J Comp Soc, 1 (2020) 155-172.

[46] T. Aven, Risk assessment and risk management: Review of recent advances on their foundation, Eur J Oper Res, 253 (2016) 1-13.

[47] Technical Committee ISO/TC 22, Risk management—Guidelines: ISO 31000: 2018, in, International Organization for Standardization, Switzerland, 2018.

[48] J. Feng, F. Qi, F. Zhu, J. Zhang, P. Gao, Y. Zhu, Uncertainty-informed cascaded diagnosis of compound faults in electromechanical systems via a physics-informed hypergraph framework, Reliab Eng Syst Safe, 272 (2026) 112685.

Just Accepted

[49] Z.W. Gao, C. Cecati, S.X. Ding, A Survey of Fault Diagnosis and Fault-Tolerant Techniques-Part I: Fault Diagnosis With Model-Based and Signal-Based Approaches, IEEE T Ind Electron, 62 (2015) 3757-3767.

[50] A.A. Amin, K.M. Hasan, A review of Fault Tolerant Control Systems: Advancements and applications, Measurement, 143 (2019) 58-68.

[51] X. Yu, J. Jiang, A survey of fault-tolerant controllers based on safety-related issues, Annu Rev Control, 39 (2015) 46-57.

[52] E. Zio, Prognostics and Health Management (PHM): Where are we and where do we (need to) go in theory and practice, Reliab Eng Syst Safe, 218 (2022).

[53] Y. Hu, X.W. Miao, Y. Si, E.S. Pan, E. Zio, Prognostics and health management: A review from the perspectives of design, development and decision, Reliab Eng Syst Safe, 217 (2022).

[54] A. Abbaspour, S. Mokhtari, A. Sargolzaei, K.K. Yen, A Survey on Active Fault-Tolerant Control Systems, Electronics-Switz, 9 (2020).

[55] T.Y. Tseng, D.J. Huang, J.Y. Lin, P.J. Chang, C.W. Lin, C.L. Liu, Consensus-Based Fault-Tolerant Platooning for Connected and Autonomous Vehicles, IEEE Int Veh Sym, (2023).

[56] H.H. Pan, W.C. Sun, Q.M. Sun, H.J. Gao, Deep Learning Based Data Fusion for Sensor Fault Diagnosis and Tolerance in Autonomous Vehicles, Chin J Mech Eng-En, 34 (2021).

[57] X.Q. Hu, Y. He, D.S. Xu, A Fault-Tolerant Integrated Navigation Method for Intelligent Vehicles, Arab J Sci Eng, 47 (2022) 15015-15025.

[58] W.P. Wang, B.J. Han, Y.Z. Guo, X. Luo, M.M. Yuan, Fault-Tolerant Platoon Control of Autonomous Vehicles Based on Event-Triggered Control Strategy, IEEE Access, 8 (2020) 25122-25134.

[59] J. Almeida, J. Rufino, M. Alam, J. Ferreira, A Survey on Fault Tolerance Techniques for Wireless Vehicular Networks, Electronics-Switz, 8 (2019).

[60] P.P. Zhu, S.T. Jin, X.H. Bu, Z.S. Hou, Distributed Data-Driven Event-Triggered Fault-Tolerant Control for a Connected Heterogeneous Vehicle Platoon With Sensor Faults, IEEE T Intell Transp, 25 (2024) 5498-5509.

[61] Q.Y. Liu, J.W. Zhang, W.Q. Zhong, Z.H. Li, X.G. Ban, S. Li, L. Li, Fault-Tolerant cooperative driving at highway on-ramps considering communication failure, Transport Res C-Emer, 153 (2023).

[62] M. Saraoglu, F. Hart, A. Morozov, K. Janschek, Fault-tolerant path planning in networked vehicle systems in presence of communication failures, IFAC-PapersOnLine, 51 (2018) 82-87.

[63] S. Hasan, S. Girs, E. Uhlemann, Characterization of Transient Communication Outages Into States to Enable Autonomous Fault Tolerance in Vehicle Platooning, IEEE Open J Intel Tr, 4 (2023) 101-129.

[64] L. Wang, H. Qin, P. Hang, C. Chen, M. Hu, Y. Bian, Cyber-Physical-Level Safe Control of Intelligent and Connected Vehicles With Unreliable Communication and Actuator Faults, IEEE T Intell Vehicl, (2024).

[65] C.W. Pan, Y. Chen, Y.Z. Liu, I. Ali, W. He, Distributed Finite-Time Fault-Tolerant Control for Heterogeneous Vehicular Platoon With Saturation, IEEE T Intell Transp, 23 (2022) 21259-21273.

[66] T. Jo, I. Park, J. Lee, J. Yoon, J. Lee, H. Kim, A Fault Diagnosis and Fault-tolerant Anti-lock Brake System Control for Actuator Stuck Failures in Braking System in Autonomous Vehicles, IEEE Transactions on Transportation Electrification, (2024).

Just Accepted

[67] T. Stolte, M. Loba, M. Nee, L.R. Wu, M. Maurer, Toward Fault-Tolerant Vehicle Motion Control for Over-Actuated Automated Vehicles: A Non-Linear Model Predictive Approach, IEEE Access, 11 (2023) 10499-10519.

[68] J.-P. Monteuuis, Resilience by design & failures forecasting for a connected autonomous vehicle, in, Institut Polytechnique de Paris, 2020.

[69] S. Moosavi, A. Weaver, S. Gopalswamy, Sensor-Health Aware Resilient Fusion With Application to Multi-Vehicle Tracking Using Infrastructure Sensors and Edge Compute, IEEE T Intell Transp, 25 (2024) 16059-16071.

[70] K. Leach, C.S. Timperley, K. Angstadt, N.T. Anh, J. Hiser, A. Paulos, P. Pal, P. Hurley, C. Thomas, J.W. Davidson, S. Forrest, C. Le Goues, W. Weimer, START: A Framework for Trusted and Resilient Autonomous Vehicles (Practical Experience Report), in: 2022 IEEE 33rd International Symposium on Software Reliability Engineering (ISSRE 2022), 2022, pp. 73-84.

[71] Z.S. Wan, K. Swaminathan, P.Y. Chen, N. Chandramoorthy, A. Raychowdhury, Analyzing and Improving Resilience and Robustness of Autonomous Systems (Invited Paper), in: 2022 IEEE/ACM International Conference on Computer Aided Design, ICCAD, 2022.

[72] R. Krecht, A. Suta, A. Tóth, A. Ballagi, Towards the resilience quantification of (military) unmanned ground vehicles, Clean Eng Technol, 14 (2023).

[73] D. Liu, S. Mair, K. Yang, S. Baldi, P. Frasca, M. Althoff, Resilience in Platoons of Cooperative Heterogeneous Vehicles: Self-Organization Strategies and Provably-Correct Design, IEEE T Intell Vehicl, 9 (2024) 2262-2275.

[74] J. Pimentel, Automated Vehicles: Safety of the Intended Functionality (SOTIF), in: Safety of the Intended Functionality, SAE, 2020, pp. i-xliv.

[75] M. Götze, M. Witt, N. Willer, F. Raisch, Safety in use and automated driving in consideration of the new ISO 21448, ATZ worldwide, 125 (2023) 38-43.

[76] H. Wang, W.B. Shao, C. Sun, K. Yang, D.P. Cao, J. Li, A Survey on an Emerging Safety Challenge for Autonomous Vehicles: Safety of the Intended Functionality, Engineering-Prc, 33 (2024) 17-34.

[77] J. Antona-Makoshi, N. Uchida, K. Yamazaki, K. Ozawa, E. Kitahara, S. Taniguchi, Development of a safety assurance process for autonomous vehicles in Japan, in: 26th International Technical Conference on the Enhanced Safety of Vehicles (ESV): Technology: Enabling a Safer TomorrowNational Highway Traffic Safety Administration, 2019.

[78] D. Kinalzyk, SOTIF process and methods in combination with functional safety, in: Systems, Software and Services Process Improvement: 28th European Conference, EuroSPI Springer, 2021, pp. 612-623.

[79] L. Peng, B.Q. Li, W.H. Yu, K. Yang, W.B. Shao, H. Wang, SOTIF Entropy: Online SOTIF Risk Quantification and Mitigation for Autonomous Driving, IEEE T Intell Transp, 25 (2024) 1530-1546.

[80] X. Xia, Y. Wang, L. Liu, Q. Wang, R. Zhai, R. Zhao, Research on Typical SOTIF Trigger Conditions of Autonomous Vehicle Perception Layer, in: 2022 4th International Symposium on Smart and Healthy Cities (ISHC), IEEE, 2022, pp. 186-189.

[81] Z.J. Zhu, R. Philipp, C. Hungar, F. Howar, Systematization and Identification of Triggering Conditions: A Preliminary Step for Efficient Testing of Autonomous Vehicles, in: 2022 IEEE Intelligent Vehicles Symposium (IV), 2022, pp. 798-805.

Just Accepted

[82] V.J. Expósito Jiménez, H. Martin, C. Schwarzl, G. Macher, E. Brenner, Triggering conditions analysis and use case for validation of ADAS/ADS functions, in: International Conference on Computer Safety, Reliability, and Security, Springer, 2022, pp. 11-22.

[83] A. Huang, X. Xing, T. Zhou, J. Chen, A safety analysis and verification framework for autonomous vehicles based on the identification of triggering events, SAE Technical Paper, (2021).

[84] H. Martin, B. Winkler, S. Grubmüller, D. Watzenig, Identification of performance limitations of sensing technologies for automated driving, in: 2019 IEEE International Conference on Connected Vehicles and Expo (ICCVE), IEEE, 2019, pp. 1-6.

[85] B. Kramer, C. Neurohr, M. Büker, E. Böde, M. Fränzle, W. Damm, Identification and quantification of hazardous scenarios for automated driving, in: International symposium on model-based safety and assessment, Springer, 2020, pp. 163-178.

[86] A. Adee, R. Gansch, P. Liggesmeyer, C. Glaeser, F. Drews, Discovery of perception performance limiting triggering conditions in automated driving, in: 2021 5th International Conference on System Reliability and Safety (ICSRS), IEEE, 2021, pp. 248-257.

[87] F. Favarò, S. Eurich, N. Nader, Autonomous vehicles' disengagements: Trends, triggers, and regulatory limitations, Accident Analysis Prevention, 110 (2018) 136-148.

[88] D. Grimm, M. Schindewolf, E. Sax, Fleet in the Loop: An Open Source approach for design and test of resilient vehicle architectures, in: 2023 IEEE 15th International Symposium on Autonomous Decentralized System, ISADS, 2023, pp. 67-74.

[89] P. Ängskog, P. Näsman, L.G. Mattsson, Resilience to Intentional Electromagnetic Interference Is Required for Connected Autonomous Vehicles, IEEE T Electromagn C, 61 (2019) 1552-1559.

[90] Q. Lin, S. Mitsch, A. Platzer, J.M. Dolan, Safe and Resilient Practical Waypoint-Following for Autonomous Vehicles, IEEE Contr Syst Lett, 6 (2022) 1574-1579.

[91] A. Hajdu, R. Krecht, A. Suta, Á. Tóth, F. Friedler, The Resilience Barriers of Automated Ground Vehicles from Military Perspectives, Chemical Engineering Transactions, 94 (2022) 1195-1200.

[92] W. Yu, J. Li, L.-M. Peng, X. Xiong, K. Yang, H. Wang, SOTIF risk mitigation based on unified ODD monitoring for autonomous vehicles, Journal of Intelligent Connected Vehicles, 5 (2022) 157-166.

[93] J.F. Rojas, N. Brown, J. Rupp, T. Bradley, Z.D. Asher, Performance Evaluation of an Autonomous Vehicle Using Resilience Engineering, SAE Technical Paper, (2022).

[94] J.F. Rojas, P. Patil, A.M. Masterson, T. Bradley, A.R. Ekti, Z.D. Asher, Automated Vehicle Lane Centering System Requirements Informed by Resilience Engineering and a Solution Using Infrastructure-Based Sensors, IEEE Access, (2024) 1-1.

[95] P. Patil, J.F. Rojas, P. Kadav, S. Sharma, A. Masterson, R. Wang, A. Ekti, L. DaHan, N. Brown, Z. Asher, Assessing Resilience in Lane Detection Methods: Infrastructure-Based Sensors and Traditional Approaches for Autonomous Vehicles, SAE Technical Paper, (2024).

[96] Y. Fang, R. Teixeira, H. Min, X. Lei, S. Chen, X. Zhao, A Safety Enhancing Framework for Autonomous Vehicles with a Resilience Rationale, in: 2023 7th International Conference on Transportation Information and Safety (ICTIS), IEEE, 2023, pp. 1699-1705.

[97] B. Caiazzo, F. Di Rosa, D.G. Lui, A. Petrillo, S. Santini, Distributed Resilient Control for autonomous connected vehicles platoon over uncertain V2X communication links, in: 2023 IEEE 26th International Conference on Intelligent Transportation Systems, ITSC, 2023, pp. 5241-5246.

Just Accepted

[98] X.H. Ge, Q.L. Han, J. Wang, X.M. Zhang, Scalable and Resilient Platooning Control of Cooperative Automated Vehicles, IEEE Transactions on Vehicular Technology, 71 (2022) 3595-3608.

[99] M. Pirani, S. Baldi, K.H. Johansson, Impact of Network Topology on the Resilience of Vehicle Platoons, IEEE T Intell Transp, 23 (2022) 15166-15177.

[100] A. Khan, M.A. Javeed, W. Ul Hassan, A.U.K. Niazi, S. Ahmed, Y.B. Zhong, S. Riaz, Stability analysis and resilient communication in connected vehicle platooning: Addressing input communication delays and disruptions through Lyapunov analysis and event-triggered control, Alex Eng J, 116 (2025) 342-350.

[101] D. Herrmann, H. Pridöhl, Basic concepts and models of cybersecurity, in: The ethics of cybersecurity, 2020, pp. 11-44.

[102] A. Al-Sabaawi, K. Al-Dulaimi, E. Foo, M. Alazab, Addressing malware attacks on connected and autonomous vehicles: recent techniques and challenges, Malware Analysis Using Artificial Intelligence Deep Learning, (2021) 97-119.

[103] B.R. Mudhivarthi, P. Thakur, G. Singh, Aspects of Cyber Security in Autonomous and Connected Vehicles, Appl Sci-Basel, 13 (2023).

[104] M. Dibaei, X. Zheng, K. Jiang, R. Abbas, S.G. Liu, Y.X. Zhang, Y. Xiang, S. Yu, Attacks and defences on intelligent connected vehicles: a survey, Digit Commun Netw, 6 (2020) 399-421.

[105] C. Gao, G. Wang, W.S. Shi, Z.M. Wang, Y.P. Chen, Autonomous Driving Security: State of the Art and Challenges, IEEE Internet Things, 9 (2022) 7572-7595.

[106] G. Bendiab, A. Hameurlaine, G. Germanos, N. Kolokotronis, S. Shiaeles, Autonomous Vehicles Security: Challenges and Solutions Using Blockchain and Artificial Intelligence, IEEE T Intell Transp, 24 (2023) 3614-3637.

[107] A. Botta, S. Rotbei, S. Zinno, G. Ventre, Cyber security of robots: A comprehensive survey, Intelligent Systems with Applications, (2023) 200237.

[108] P. Sharma, J. Gillanders, Cybersecurity and Forensics in Connected Autonomous Vehicles: A Review of the State-of-the-Art, IEEE Access, 10 (2022) 108979-108996.

[109] K. Kim, J.S. Kim, S. Jeong, J.H. Park, H.K. Kim, Cybersecurity for autonomous vehicles: Review of attacks and defense, Comput Secur, 103 (2021).

[110] A. Abdo, H.L. Chen, X.P. Zhao, G.Y. Wu, Y.H. Feng, Cybersecurity on Connected and Automated Transportation Systems: A Survey, IEEE T Intell Vehicl, 9 (2024) 1382-1401.

[111] Y. Deng, T.H. Zhang, G.N. Lou, X. Zheng, J. Jin, Q.L. Han, Deep Learning-Based Autonomous Driving Systems: A Survey of Attacks and Defenses, IEEE T Ind Inform, 17 (2021) 7897-7912.

[112] A. Nanda, D. Puthal, J.J.P.C. Rodrigues, S.A. Kozlov, Internet of Autonomous Vehicles Communications Security: Overview, Issues, and Directions, IEEE Wirel Commun, 26 (2019) 60-65.

[113] S. Gupta, C. Maple, R. Passerone, An Investigation of Cyber-Attacks and Security Mechanisms for Connected and Autonomous Vehicles, IEEE Access, 11 (2023) 90641-90669.

[114] J.P. Han, Z.Y. Ju, X.G. Chen, M.Z. Yang, H. Zhang, R.X. Huai, Secure Operations of Connected and Autonomous Vehicles, IEEE T Intell Vehicl, 8 (2023) 4484-4497.

[115] A. Qayyum, M. Usama, J. Qadir, A. Al-Fuqaha, Securing Connected & Autonomous Vehicles: Challenges Posed by Adversarial Machine Learning and the Way Forward, IEEE Commun Surv Tut, 22 (2020) 998-1026.

Just Accepted

[116] F.J. Niroumand, P.A. Bonab, A. Sargolzaei, Security of Connected and Autonomous Vehicles: A Review of Attacks and Mitigation Strategies, in: SoutheastCon, 2024, pp. 1197-1204.

[117] Z.Y. Ju, H. Zhang, X. Li, X.G. Chen, J.P. Han, M.Z. Yang, A Survey on Attack Detection and Resilience for Connected and Automated Vehicles: From Vehicle Dynamics and Control Perspective, IEEE T Intell Vehicl, 7 (2022) 815-837.

[118] X.Q. Sun, F.R. Yu, P. Zhang, A Survey on Cyber-Security of Connected and Autonomous Vehicles (CAVs), IEEE T Intell Transp, 23 (2022) 6240-6259.

[119] M. Pham, K.Q. Xiong, A survey on security attacks and defense techniques for connected and autonomous vehicles, Comput Secur, 109 (2021).

[120] T. Limbasiya, K.Z. Teng, S. Chattopadhyay, J.Y. Zhou, A systematic survey of attack detection and prevention in Connected and Autonomous Vehicles, Veh Commun, 37 (2022).

[121] J.M. Qurashi, K. Jambi, F. Alsolami, F.E. Eassa, M. Khemakhem, A. Basuhail, Resilient Countermeasures Against Cyber-Attacks on Self-Driving Car Architecture, IEEE T Intell Transp, 24 (2023) 11514-11543.

[122] R. Guo, M. Vallati, S. Parkinson, J. Ma, Cyberattack impacts and mitigation tradeoff in CAV-based fixed-route and demand-responsive transit systems, Reliab Eng Syst Safe, 274 (2026) 112352.

[123] S.M. Alhidaifi, M.R. Asghar, I.S. Ansari, Cyber resilience quantification: A probabilistic estimation model for IT infrastructure, Reliab Eng Syst Safe, 265 (2026) 111473.

[124] Y.L. Wang, N. Bian, L. Zhang, Y.J. Huang, H. Chen, Resilient path-following control of autonomous vehicles subject to intermittent denial-of-service attacks, Iet Intell Transp Sy, 15 (2021) 1508-1521.

[125] J.M. Qurashi, K. Jambi, F.E. Eassa, M. Khemakhem, F. Alsolami, A.A. Basuhail, Toward Attack Modeling Technique Addressing Resilience in Self-Driving Car, IEEE Access, 11 (2023) 2652-2673.

[126] M. Ayrault, U. Kühne, É. Borde, Finding Optimal Moving Target Defense Strategies: A Resilience Booster for Connected Cars, Information, 13 (2022).

[127] K. Mahbub, M. Patwary, A. Nehme, Towards an Integrated In-Vehicle Isolation and Resilience Framework for Connected Autonomous Vehicles, in: The Ninth International Conference on Advances in Vehicular Systems, Technologies and Applications, Porto, Portugal, 2020, pp. 15-19.

[128] W. Yue, X.J. Guo, H.X. Shen, Internet of connected vehicles against cyber-attacks based on resilient adaptive event trigger mechanism control, T I Meas Control, 46 (2024) 223-236.

[129] K. Li, Y. Wang, H. Chen, J. Gao, A Resilient Control Strategy in Connected Vehicles under Actuator Attacks, in: 2023 7th CAA International Conference on Vehicular Control and Intelligence (CVCI), 2023, pp. 1-8.

[130] B. Caiazzo, D.G. Lui, A. Mungiello, A. Petrillo, S. Santini, On the resilience of Autonomous Connected Vehicles Platoon Under DoS Attacks: a predictor-based sampled data control, in: 2023 IEEE 26th International Conference on Intelligent Transportation Systems, Itsc, 2023, pp. 4907-4912.

[131] X.H. Ge, Q.L. Han, Q. Wu, X.M. Zhang, Resilient and Safe Platooning Control of Connected Automated Vehicles Against Intermittent Denial-of-Service Attacks, IEEE-Caa J Automatic, 10 (2023) 1234-1251.

[132] M. Safi, S.M. Dibaji, M. Pirani, Resilient coordinated movement of connected autonomous vehicles, Eur J Control, 64 (2022).

Just Accepted

[133] L. Khoshnevisan, X. Liu, A Secure Adaptive Resilient Neural Network-Based Control of Heterogeneous Connected Automated Vehicles Subject to Cyber Attacks, IEEE Transactions on Vehicular Technology, (2025) 1-11.

[134] H.L. Wei, Y.R. Zhang, C. Lv, B.B. Hu, Y. Shi, Human-Assisted Resilient Coordination for Automated Platoon With False Data Injection Attack, IEEE Transactions on Vehicular Technology, 73 (2024) 19389-19399.

[135] T. Wang, M.T. Tu, H. Lyu, Y. Li, O. Orfila, G.J. Zou, D. Gruyer, Impact Evaluation of Cyberattacks on Connected and Automated Vehicles in Mixed Traffic Flow and Its Resilient and Robust Control Strategy, Sensors-Basel, 23 (2023).

[136] R. Al Mallah, T. Halabi, B. Farooq, Resilience-by-design in Adaptive Multi-agent Traffic Control Systems, ACM T Priv Secur, 26 (2023).

[137] S. Boddupalli, A.S. Rao, S. Ray, Resilient Cooperative Adaptive Cruise Control for Autonomous Vehicles Using Machine Learning, IEEE T Intell Transp, 23 (2022) 15655-15672.

[138] B. Zou, P. Choobchian, J. Rozenberg, Cyber resilience of autonomous mobility systems: cyber-attacks and resilience-enhancing strategies, J Transp Secur, 14 (2021) 137-155.

[139] S. Park, H. Park, PIER: cyber-resilient risk assessment model for connected and autonomous vehicles, Wirel Netw, 30 (2024) 4591-4605.

[140] Y.X. Wang, H. Zen, M.F.M. Sabri, X. Wang, L.C. Kho, Towards Strengthening the Resilience of IoV Networks-A Trust Management Perspective, Future Internet, 14 (2022).

[141] H.M.S. Ahmad, E. Sabouni, W. Xiao, C.G. Cassandras, W. Li, Trust-Aware Resilient Control and Coordination of Connected and Automated Vehicles, in: 2023 IEEE 26th International Conference on Intelligent Transportation Systems, ITSC, 2023, pp. 4309-4314.

[142] M. Kahlert, H. Peitzmeier, D. Evans, K. Talits, F. Kortmann, C. Tebruegge, Resilience of Spatial Environment Perception Toward Fully Automated Driving: A Review, IEEE Sensors Journal, 24 (2024) 21801-21812.

[143] Department of Motor Vehicles of State of California, Autonomous Vehicles Testing with a Driver, 2024. Available online: https://www.dmv.ca.gov/portal/vehicle-industry-services/autonomous-vehicles/testing-autonomous-vehicles-with-a-driver/.

Just Accepted

Author biography



Yukun Fang received the Ph.D. degree in Traffic Information Engineering and Control from Chang'an University, China, in 2024. He is currently a Lecturer with the School of New Energy and Intelligent Connected Vehicles, Anhui University of Science and Technology. His research interests include anomaly detection and diagnosis for connected autonomous vehicles (CAVs), CAV resilience, and CAV cooperative control.



Rui Teixeira received his Ph.D. from Trinity College Dublin in 2019. He is currently an Assistant Professor in the Department of Civil, Structural and Environmental Engineering at Trinity College Dublin. His research focuses on the risk and resilience of systems, aiming to enable safe and reliable civil engineering systems by improving decision-making processes, leveraging digitization in risk and resilience with real-time system identification, and performing probabilistic evaluations of systems and their uncertain behavior.



Gongda Hu received the Ph.D. degree in Electronic Science and Technology from University of Science and Technology of China in 2025. He is currently a Lecturer with the School of Electronic Information and Integrated Circuits, Hefei Normal University, and a member of Anhui Province Key Laboratory of Simulation Calculation and Design for Electronic Information System. His research interests include planar electromagnetic structure optimization and advanced AI-based electromagnetic applications.



Haigen Min received the Ph.D. degree in Traffic Information Engineering and Control from Chang'an University, China, in 2018. He is currently a Professor with the School of Information Engineering, Chang'an University. His research interests include high-precision localization, environment perception, and cooperative control for connected and autonomous vehicles and its fault detection and diagnosis.



Xiangmo Zhao received the Ph.D. degree from Chang'an University, China, in 2005. He is currently a Professor with the School of Information Engineering, Chang'an University, and the President of Xi'an Technological University. He is a Vice President of the Joint Laboratory for Connected vehicles, Ministry of Education and China Mobile, and is also a Leader of the National Key Subjects-Traffic Information Engineering and Control, Chang'an University. His research interests include connected vehicles, automated vehicles, intelligent transportation systems, and computer science.

Just Accepted