ASME Open Journal of Engineering
Online journal at:
https://asmedigitalcollection.asme.org/openengineering

Reliability-Driven Design Principles for Modern Automotive Systems: A System-Level Assessment

Luca Piancastelli
Department of Industrial Engineering (DIN),
University of Bologna Alma Mater Studiorum,
Bologna 40136, Italy
e-mail: luca.piancastelli@unibo.it

Irene Giusti[1]
Department of Industrial Engineering (DIN),
University of Bologna Alma Mater Studiorum,
Bologna 40136, Italy
e-mail: irene.giusti4@unibo.it

Marella De Santis
Department of Industrial Engineering (DIN),
University of Bologna Alma Mater Studiorum,
Bologna 40136, Italy
e-mail: marella.desantis2@unibo.it

Modern vehicle architectures increasingly rely on distributed electronic control units, advanced driver-assistance systems, and infotainment-driven design, creating unprecedented system-level interdependence. While these innovations improve comfort, connectivity, and nominal safety, their impact on long-term reliability and fleet-scale risk remains underexplored in current validation practices. This article presents a system-level, reliability-oriented reassessment of automotive design. Rather than focusing on subsystem optimization, it reframes safety as a lifecycle reliability challenge that extends beyond hardware and software correctness. A quantitative framework is proposed to evaluate reliability at national, continental, and global fleet scales, demonstrating that even very low failure probabilities become significant when deployed across large fleets. The study combines reliability modeling, fleet exposure estimation, and a comparison of automotive functional safety standards (ISO 26262 and ISO 21448) with aeronautical and railway certification practices. Results reveal gaps in failure budgeting, architectural segregation, and enforceable lifecycle reliability assurance. Based on these findings, a reliability-driven design framework is outlined, emphasizing architectural simplification, isolation of safety-critical domains, verified redundancy, and modular separation of nonessential systems. The framework aims to guide automotive innovation that balances advanced functionality with transparent, verifiable, and durable system reliability. [DOI: 10.1115/1.4071582]

Keywords: safety, vehicle design, reliability, ECUs, infotainment

1 Introduction

Over the past three decades, automotive engineering has undergone a profound transformation driven by rapid advances in electronics, software, and regulatory frameworks. Vehicles that were once dominated by mechanical systems and clearly delimited functional subsystems have evolved into highly interconnected cyber-physical platforms, integrating dozens of electronic control units (ECUs), complex communication networks, advanced driver-assistance systems (ADAS), and infotainment architectures comparable in complexity to consumer electronic devices [1,2]. While these developments have delivered significant gains in comfort, connectivity, emissions control, and nominal safety performance, they have also introduced new challenges for vehicle reliability, human–machine interaction, and lifecycle management.

A defining characteristic of this transformation is the progressive shift toward distributed electronic architectures and feature-driven development. Design priorities are increasingly shaped by regulatory compliance, marketing differentiation, and user-facing functionalities, leading to the accumulation of software-mediated subsystems and tightly coupled control logic. As interdependence between electronic and software-driven components grows, localized failures—whether hardware-related, software-induced, or communication-based—can propagate across functional domains, affecting vehicle behavior in ways that are more complex and less predictable than in traditional mechanical designs [3–5]. Recent work highlights that touchscreen-heavy human–machine interfaces (HMIs) and the proliferation of infotainment can significantly increase driver distraction, even in otherwise well-engineered vehicles [5].

Regulatory escalation has reinforced this trend. Safety and emission standards, while motivated by legitimate public-interest objectives, are often implemented through the mandatory addition of electronic subsystems rather than holistic architectural optimization. Consequently, contemporary vehicles frequently achieve compliance by layering sensing, computation, and control, rather than by simplifying underlying system interactions. Although these measures have demonstrable benefits—such as improved emission performance and the potential for advanced safety features—they can also increase development costs, vehicle mass, and system complexity, with potential implications for long-term operational reliability [6].

Human–machine interaction has become a critical dimension of automotive safety. Modern interfaces increasingly rely on touchscreen controls and multifunction displays, which can centralize multiple functions but require visual attention, potentially increasing eyes-off-road time [5,7,8]. In contrast, physical buttons and dedicated switches provide tactile feedback, enabling rapid,

[1]Corresponding author.

Manuscript received February 9, 2026; final manuscript received March 30, 2026; published online April 16, 2026. Assoc. Editor: John Hunter Mack.

muscle-memory-based operation for safety-critical functions. Evaluating these trade-offs is essential to ensure that interface design supports safe operation over the full vehicle lifecycle.

Despite extensive research on automotive safety, existing approaches are predominantly focused on component-level validation, software correctness, and compliance with standards such as ISO 26262 and ISO 21448. While these methodologies are necessary, they do not explicitly address how failure probabilities scale across large vehicle fleets, nor do they systematically link architectural design choices—such as ECU distribution, functional coupling, or interface design—to long-term operational reliability. Furthermore, cross-sector insights from domains such as aeronautics and railway systems, where lifecycle reliability and quantitative failure targets are central design drivers, remain only partially integrated into automotive engineering practice.

Against this backdrop, the present work adopts a reliability-oriented, system-level perspective to examine how electronic proliferation, supply-chain fragmentation, and regulatory-driven feature accretion influence overall vehicle safety and operational dependability. Rather than focusing on incremental improvements to individual subsystems, the study analyzes architectural choices and subsystem integration strategies that directly affect failure propagation, maintainability, and fleet-scale risk [3,9].

Contributions of This Work. This article provides several original contributions aimed at bridging the gap between component-level validation and lifecycle reliability assessment in modern automotive systems.

First, a fleet-scale reliability framework is introduced, explicitly linking component- and subsystem-level failure probabilities to large-scale operational risk across millions of vehicles. This approach enables quantitative assessment of rare events that may be negligible at the individual vehicle level but become significant when evaluated at the fleet scale.

Second, the article presents a structured cross-sector comparison between automotive safety standards (ISO 26262 and ISO 21448) and certification approaches adopted in aeronautical and railway systems. This comparison highlights key differences in reliability targets, architectural segregation, maintenance enforcement, and lifecycle assurance practices, providing a broader engineering context for evaluating automotive design choices.

Third, the study develops a set of reliability-oriented architectural guidelines based on quantitative considerations of ECU proliferation, system complexity, and fault propagation mechanisms. These guidelines emphasize architectural simplification, functional isolation of safety-critical domains, and the use of centralized or domain-oriented control strategies with explicit reliability targets.

Fourth, historical vehicle design philosophies are analyzed alongside contemporary architectures to demonstrate that alternative, lower-complexity design trajectories remain technically feasible. These examples are not used descriptively, but as analytical references to support the evaluation of architectural trade-offs and their impact on reliability and maintainability.

Together, these contributions distinguish the present work from existing literature by providing a unified framework that connects system architecture, human–machine interaction, and lifecycle reliability within a single, quantitatively grounded perspective.

Building on this framework, the remainder of the article evaluates the implications of electronic complexity on reliability, compares alternative architectural strategies, and proposes design recommendations that balance advanced functionality with robustness, transparency of failure modes, and long-term operational safety.

2 Outsourcing Dynamics in the European Automotive Supply Chain

A major European multinational initially emerged to support domestic automotive production by providing standardized components across multiple manufacturers, enabling economies of scale and higher production volumes. This approach allowed smaller and medium-sized companies to access high-quality components without extensive internal development and testing capabilities.

Over time, strategic priorities evolved toward maximizing profit margins and global competitiveness, leading to extensive relocation of production to lower-cost countries, primarily in East Asia. While these moves improved short-term cost efficiency, they also increased dependency on international supply chains, particularly for electronic and safety-critical components. Concurrently, the company contributed to shaping European regulatory frameworks, promoting mandatory integration of features such as anti-lock braking system (ABS), electronic stability program (ESP), and Advanced Driver-Assistance Systems (ADAS) [3,10]. Although these systems provide measurable safety benefits under standardized testing and controlled conditions, their compulsory adoption adds to system complexity, production costs, and maintenance requirements, creating additional technical and financial challenges for manufacturers.

The intensification of environmental regulations, culminating in Euro 6+ emission standards, further increased development and integration complexity [4,11]. While such regulations have incentivized innovation in sensing, control, and energy management technologies, they have also affected the cost competitiveness of European automakers relative to Asian manufacturers, who often achieve equivalent system functionality with lower overhead [12].

Modern vehicle architectures illustrate a related engineering challenge. Distributed electronic designs, comprising multiple ECUs interconnected via high-speed controller area network (CAN) or optical buses, support modularity and flexible feature deployment. However, these architectures can increase integration effort, potential points of failure, and validation complexity, particularly for safety-critical subsystems such as steering-intervention ADAS. In contrast, consolidated multitasking ECUs can provide equivalent functionality while simplifying integration and enhancing reliability [13]. Effective lifecycle verification, including real-world testing, is essential to ensure that safety-critical functions meet operational reliability targets beyond nominal Hardware/Software (HW/SW) compliance [9].

In summary, the evolution of the European automotive supply chain from a supportive industrial ecosystem to a profit-driven, outsourced network has introduced both opportunities and challenges. While cost efficiencies and access to advanced components have increased, technological dependency and system complexity have grown, reinforcing the importance of modular, reliability-focused design strategies and robust validation processes to maintain safe and predictable operation of modern vehicle systems.

2.1 China's Role in Automotive Electronics and Production. While not all automotive electronics are produced in China, the country has become a global leader in the manufacture and export of numerous automotive components, including complex electronic systems [14]. Multinational automotive companies increasingly leverage Chinese manufacturing to benefit from lower production costs, efficient assembly, and high-volume output. China is also expanding rapidly in electric vehicle (EV) production, battery systems, and associated electronic controls, supported by targeted policy instruments [15].

Chinese companies such as Contemporary Amperex Technology Co. (CATL) have become major global suppliers of automotive batteries and battery management systems, critical elements of vehicle electronic architectures [16]. The concentration of component production, including integrated ADAS modules and control electronics, emphasizes the need for supply-chain reliability, modular design approaches, and rigorous validation processes [17]. From a systems engineering perspective, these dynamics influence global vehicle design decisions, affecting integration strategies, real-world testing requirements, and lifecycle management of safety-critical electronic subsystems.

2.2 Impact of Outsourcing on Vehicle Reliability. The reliance on Chinese and other non-European suppliers for safety-critical

electronics introduces additional reliability risks. Variability in manufacturing quality, differences in certification standards, and extended logistics chains can affect component consistency and traceability. Delays in shipment or component shortages may force manufacturers to integrate substitute parts, sometimes without comprehensive validation under EU operating conditions. Moreover, over-the-air (OTA) software updates, calibration differences, or variations in embedded firmware between production batches can propagate faults across vehicle fleets. These factors collectively increase the likelihood of integration errors, unexpected failure modes, and long-term reliability issues, particularly in high-volume deployments. Therefore, the outsourcing of electronic components necessitates more stringent quality control, rigorous end-of-line testing, and enhanced system-level validation to ensure fleet-scale reliability and safe operation of complex cyber-physical systems.

Overall, the European and global automotive industries face the dual challenge of leveraging cost-effective international production while maintaining robust, verifiable reliability standards for increasingly complex electronic and safety-critical systems.

3 Infotainment Issues and Reliability Considerations

Modern vehicles increasingly blur the distinction between the automobile as a transportation system and the infotainment subsystem, which provides nondriving-related services such as media playback, app integration, and online connectivity. Empirical studies and human factors research have shown that the operation of infotainment systems during driving can divert driver attention, increasing reaction time and the likelihood of safety-critical events [7,8]. However, these systems also offer clear benefits, including enhanced user satisfaction, integrated navigation, and real-time information that can support safer driving when designed and used appropriately.

Market trends have amplified the emphasis on infotainment features, often prioritizing accessory richness over core vehicle reliability. These systems are typically composed of multiple interconnected modules communicating via high-speed CAN or optical buses, increasing installation, integration, and maintenance costs. Each additional module introduces potential points of failure, and system interdependencies can propagate faults, potentially affecting critical vehicle functions if strict isolation is not enforced.

A reliability-oriented design philosophy therefore recommends explicit separation of the infotainment subsystem from core vehicle control domains. In practice, this can be achieved using a domain-oriented architecture where high-integrity ECUs manage safety-critical functions such as steering, braking, and propulsion, while infotainment operates on dedicated hardware with well-defined communication interfaces. For example, the infotainment ECU can be connected to the body or auxiliary systems through an isolated gateway, preventing software faults, bus congestion, or crashes in the infotainment system from propagating to safety-critical controllers.

Real-world examples reinforce this approach. Premium original equipment manufacturer (OEM) vehicles and modern EV platforms employ isolated infotainment domains, often including dedicated processing units, memory, and power supply lines. Such architectures enable over-the-air updates or third-party app integration without compromising vehicle reliability. Modular interfaces, standardized slots, and detachable infotainment packages allow upgrades or replacements independent of critical systems, facilitating maintenance, reducing downtime, and minimizing the risk of introducing faults into safety-relevant subsystems.

Furthermore, the rapid obsolescence of infotainment hardware and software—typically two or more years old by the time the vehicle reaches production—underscores the need for modular, reliability-focused design. Empirical validation through scenario simulations, fault-injection testing, and in-vehicle operational trials ensures that infotainment remains functionally and safety compliant without affecting vehicle reliability [7,8].

Overall, by adopting physically and logically segregated infotainment domains, manufacturers can deliver rich user experiences while maintaining system-level reliability. This approach supports fault containment, simplifies lifecycle management, and ensures that critical vehicle functions remain operational under all foreseeable conditions.

4 Emission Challenges and Industrial Strategies

In the 1970s, automotive manufacturers recognized that vehicles capable of extremely long service lifetimes could reduce annual replacement demand, potentially impacting sales volumes. Understanding these trade-offs is essential for reliability-driven vehicle design, as industrial strategies directly influence the likelihood of failures over the operational lifecycle and affect maintenance and replacement planning. Two divergent industrial strategies emerged to address this challenge, each with implications for long-term fleet reliability assessment.

The first strategy emphasized high durability and reliability through frequent, strictly scheduled maintenance at authorized workshops using original spare parts. This approach, adopted mainly by premium European manufacturers, provided long-lasting vehicles capable of exceeding one million kilometers with minimal failures, maintaining high residual value [1]. High initial costs were justified by extended service life and consistent performance, demonstrating a clear alignment between engineering design, rigorous maintenance, and reliability over the vehicle lifecycle. From a fleet-scale perspective, this approach reduces the probability of rare but severe failure events and simplifies lifecycle reliability modeling.

The second strategy focused on low-cost, shorter-lifespan vehicles, designed to last approximately 250,000 km, with optimal reliability limited to the first 150,000 km. This approach, reinforced by successive waves of increasingly stringent emission standards, encouraged faster vehicle replacement [18]. While commercially successful and supported by fuel suppliers, this strategy increased maintenance complexity, raised production costs, and introduced a dependency on regulatory-driven upgrades. For fleet reliability analysis, vehicles following this strategy present higher cumulative risk exposure, as low-probability failures in individual vehicles can scale significantly across large fleets, emphasizing the need for robust verification and conservative reliability budgeting.

Over time, both strategies revealed trade-offs in cost-effectiveness, service complexity, and system reliability [19]. Asian manufacturers, benefiting from large-scale production, outsourcing, and efficient regulatory adaptation, gained a competitive advantage, highlighting the importance of integrated system design, component standardization, and lifecycle engineering [20]. An explicit understanding of these industrial strategies is therefore critical when developing reliability-driven design principles, as they determine how fleet-scale exposure, maintenance policies, and system complexity interact to affect long-term vehicle performance and safety.

4.1 Emission Constraints and Engine Efficiency.

The implementation of stringent emission regulations has led to measurable improvements in internal combustion engine performance, but it has also increased development complexity and overall cost. From a systems engineering perspective, achieving targeted fuel consumption and emission levels requires integrated design of the engine, control strategies, and after-treatment systems, alongside thorough validation under realistic operating conditions [11].

Theoretical calculations suggest that significant improvements in fuel efficiency are possible with optimized engine and transmission designs. For example, increasing thermal efficiency from 32% to 60% could theoretically reduce fuel consumption from 3.8 L/100 km to approximately 2.0 L/100 km at a constant speed of 90 km/h.

However, these estimates are based on simplified steady-state assumptions and are intended primarily to illustrate the potential impact of improved thermal efficiency on fuel consumption.

In real-world vehicle operation, fuel consumption is influenced by a wide range of factors that are not captured by the simplified constant speed model used here. These include variable engine load during acceleration and deceleration, urban stop-and-go traffic, road gradients, aerodynamic disturbances, ambient temperature, rolling resistance variations, and driver behavior. Standardized driving cycles such as the Worldwide Harmonized Light Vehicles Test Procedure (WALTP) attempt to represent some of these effects, but even these controlled tests cannot fully reproduce the diversity of real-world operating conditions.

Consequently, the values presented in this section should be interpreted as idealized reference calculations rather than precise predictions of real-world fuel consumption. In practice, the achievable improvements depend on vehicle mass, aerodynamic characteristics, transmission design, driving conditions, and environmental factors. Empirical validation through experimental testing and long-term fleet data is therefore required to quantify the actual benefits under practical operating conditions [6,21].

4.1.1 Theoretical Fuel Economy Improvement With a 60% Efficient Diesel Engine on a Modern Car. The transition from Euro 2 to Euro 6+ vehicles has been accompanied by significant changes in diesel engine design, primarily to comply with increasingly stringent emissions regulations. Empirical studies indicate that thermal efficiency in contemporary diesel engines decreases from approximately 45% in Euro 2 vehicles to around 32% in Euro 6+ vehicles, largely due to additional after-treatment devices and exhaust gas recirculation systems [22–24]. Modern diesel cars equipped with advanced fuel injection, turbocharging, and emission controls typically consume around 3.8 L/100 km at a constant speed of 90 km/h.

The corresponding total vehicle efficiency can be calculated as

$$\eta_{\text{tot,real}} = \eta_m \times \eta_t = 0.32 \times 0.60 = 0.192 \tag{1}$$

where η_m represents the engine thermal efficiency and η_t represents the transmission efficiency. Given a fuel power of 34.3 kW, the useful wheel power output is

$$P_{\text{wheel}} = 34.3 \times 0.192 \approx 6.6\,\text{kW} \tag{2}$$

Considering an advanced engine achieving 60% thermal efficiency while maintaining the same transmission efficiency, the new total efficiency becomes

$$\eta_{\text{tot,new}} = 0.60 \times 0.60 = 0.36 \tag{3}$$

The corresponding fuel power required to achieve the same wheel output is therefore

$$P_{\text{fuel,new}} = \frac{6.6}{0.36} \approx 18.3\,\text{kW} \tag{4}$$

Assuming diesel with an energy content of 10 kW h/L, the volumetric fuel flowrate is

$$\dot{V}_{\text{fuel}} = \frac{18.3}{10} \approx 1.83\,\text{L/h} \tag{5}$$

and the equivalent fuel consumption at 90 km/h becomes

$$C_{\text{new}} = \frac{1.83}{90} \times 100 \approx 2.03\,\text{L/100 km} \tag{6}$$

These calculations demonstrate the theoretical potential of high-efficiency engines under controlled conditions. However, real-world performance is influenced by multiple factors, including vehicle mass, aerodynamic drag, tire rolling resistance, driving cycles, and environmental conditions [24]. For example, incorporating aerodynamic characteristics similar to the Citroën CX, such as reduced frontal area and optimized body shape, could further decrease fuel consumption by lowering drag losses at cruising speeds (Table 1).

Table 1 Fuel economy comparison: Citroën CX 2500 D versus modern diesel car

	CX 2.5 D	CX 2.5 D (60%)	Modern diesel	Modern diesel (60%)
η_m	0.30	0.60	0.32	0.60
η_t	0.60	0.60	0.60	0.60
η_{tot}	0.18	0.36	0.192	0.36
P_{wheel} (kW)	9.0	9.0	6.6	6.6
P_{fuel} (kW)	50.0	25.0	34.3	18.3
Consumption (L/100 km)	5.55	2.78	3.8	2.03
Fuel economy (km/L)	18	36	26.3	49.3

Beyond immediate energy savings, higher thermal efficiency also has implications for long-term vehicle reliability. Reduced fuel consumption generally lowers thermal and mechanical stress on engine components, including pistons, bearings, and turbochargers, which can extend service intervals and reduce failure probabilities. By comparing historical vehicles, such as the Citroën CX 2500 D, with modern diesel engines and hypothetical 60% efficient variants, fleet operators can estimate the reduction in cumulative wear and associated maintenance requirements over millions of kilometers. This framework enables quantitative assessments of the lifecycle reliability and fleet exposure to rare failures, linking improvements in fuel economy directly to vehicle durability and system dependability.

Furthermore, such calculations support a reliability-driven design philosophy, where efficiency gains are considered in conjunction with safety-critical systems and operational stress. For instance, lower fuel power requirements can reduce thermal loading on transmission components and electronic control units, enhancing overall vehicle robustness. The integration of quantitative efficiency benchmarks into vehicle design provides a measurable and reproducible metric for manufacturers and regulators to evaluate both environmental and reliability benefits [23].

5 Evolution of Cost Structure in City Cars: 1980s Versus 2020s

Table 2 presents an estimated comparative cost breakdown, expressed in constant 2024 euros, between a typical city car produced in the 1980s and a current-generation city car from the 2020s. All numerical values are based on the authors' own interpretative estimates, derived from historical industry data, inflation adjustments, and comparative teardown analyses of representative

Table 2 Estimated cost breakdown for city cars (1980s versus 2020s, EUR 2024)

Cost category	1980s	2020s
Raw materials (steel, plastics, glass)	2200	3000
Powertrain (engine, gearbox, exhaust)	1200	2200
Electronics and sensors	100	4800
Interior and trim	400	1000
Chassis and suspension	500	850
Manufacturing labor	350	700
Regulatory compliance (safety, emissions)	50	1000
Infotainment and connectivity	0	600
R&D amortization	100	800
Logistics and distribution	100	400
Dealer margin and marketing	1000	650
Total production + overhead cost	6000	16,000

vehicles within the same segment [25,26]. These estimates should be regarded as indicative and not as empirically verified production costs.

The 1980s model shows a total production and overhead cost of approximately 6000 EUR (2024 value), dominated by raw materials and mechanical components. Electronics and sensors accounted for only a minor share, around 100 EUR, reflecting the minimal integration of electronic subsystems at the time. Dealer margins and marketing costs (around 1000 EUR) were relatively high, consistent with the traditional sales and distribution structures of that era.

In contrast, a modern city car from the 2020s exhibits a total estimated cost of approximately 16,000 EUR. The most pronounced increase is observed in the *electronics and sensors* category, which now includes hybrid control units, ADAS sensors, and digital instrumentation, representing roughly 4800 EUR per vehicle. This reflects a substantial increase compared to the 1980s and highlights the growing importance of embedded controllers, software development, and semiconductor supply chains in contemporary automotive design.

These observations indicate a structural transformation in vehicle cost allocation: modern city cars dedicate a larger portion of the total cost to electronic, digital, and compliance-related systems, while traditional mechanical and labor costs have proportionally decreased. From an engineering and control perspective, this shift underscores the increasing complexity of vehicle systems, the critical role of electronics and software in performance and safety, and the necessity for integrated design, testing, and validation strategies to ensure reliability and cost-effectiveness in contemporary vehicles.

5.1 Impact of Increased Electronic Content on Fleet Reliability. The substantial increase in electronics and sensor content has direct implications for long-term fleet reliability. While individual vehicle reliability may still meet component-level standards, the aggregation of low-probability electronic failures across millions of vehicles can significantly affect fleet-level operational exposure. For example, a rare failure in a battery management system, ADAS sensor, or infotainment ECU may be inconsequential in a single vehicle but could result in dozens or hundreds of service interruptions across a large fleet.

Higher electronic complexity also increases interdependencies among subsystems, which can propagate faults and complicate maintenance. Failures in a sensor or ECU can lead to secondary effects in propulsion, braking, or stability control systems if proper modular isolation is not implemented. Consequently, fleet operators must consider not only component reliability but also system integration and redundancy strategies, such as dual sensors, independent control pathways, and modular software updates, to mitigate risks at scale.

By comparing historical 1980s city cars, which had minimal electronics, with modern vehicles, we can quantify how the growth of electronic content correlates with potential fleet exposure. Vehicles with higher sensor density and advanced electronics require more rigorous testing, validation, and maintenance to maintain reliability over their operational lifetime. This emphasizes the need for reliability-driven design principles, even when cost pressures incentivize complex electronic integration.

5.2 Methodological Notes. All cost figures are expressed in constant 2024 euros and should be interpreted as approximate production-level costs, excluding taxes but including estimated dealer margins. The estimates are based on a combination of three methodological approaches, with inherent limitations acknowledged:

(1) *Historical cost reconstruction:* archival data and manufacturer reports from the 1980s were adjusted to 2024 euros using the long-term consumer price index series and harmonized inflation methodologies provided by OECD and Eurostat [27,28]. The reconstruction is indicative and may not fully capture actual past production practices.
(2) *Comparative teardown benchmarking:* component costs of modern city cars were estimated using publicly available automotive teardown analyses and benchmarking studies on B-segment vehicles produced between 2020 and 2024 [25,26]. These benchmarks provide relative trends rather than absolute values.
(3) *Analytical adjustment:* additional corrections were applied to account for changes in materials, regulatory requirements (safety and emissions), and the increasing integration of digital and hybrid subsystems [6]. This step relies on modeling assumptions and expert judgment.

These calculations are intended as an analytical comparison of structural trends rather than precise financial statements. While they provide useful insights into shifts from mechanical to electronic content and the associated design implications, they now explicitly link cost and electronic integration to potential fleet-level reliability risks, demonstrating the practical relevance of these comparisons for lifecycle-oriented, reliability-driven vehicle design. Further data collection and verification would strengthen the conclusions and enhance their applicability to current industrial practice.

6 The Loss of Design Know-How

The increasing emphasis on marketing vehicles through accessory features has progressively shifted design priorities away from the automobile as a reliability-driven transportation system. Consumers are often influenced more by the quantity of electronic subsystems and auxiliary features—such as electric seats, retractable handles, touchscreens, and infotainment modules—than by core vehicle attributes such as reliability, robustness, and lifecycle performance [1,2]. From a systems engineering perspective, this trend results in increased electronic and software complexity, which directly translates into a higher number of potential failure modes, more intricate interdependencies, and greater challenges in verification and validation.

Historically, high-performance vehicles such as the Ferrari 308 GTS driven by Gilles Villeneuve were designed with minimal nonessential equipment. The cockpit featured only critical instruments and controls, including a tachometer, speedometer, fuel and oil gauges, pedals, and the gear lever, all arranged to maximize driver focus and operational safety. Figure 1 illustrates this compact, driver-centric layout, engineered to enhance control, ergonomics, and rapid response under high-speed driving conditions. From a reliability standpoint, this minimalistic approach

Fig. 1 Cockpit of the Ferrari 308 GTS driven by Gilles Villeneuve, illustrating a historically minimalistic and reliability-focused design

reduced both system complexity and the likelihood of component or interface failures, while also minimizing driver distraction and improving response predictability under critical conditions.

Quantitatively, the Ferrari 308 GTS contained only two ECUs and fewer than 10 electrical subsystems, with electronics accounting for less than 5% of total vehicle cost. In contrast, a modern high-performance vehicle may contain 50–100 ECUs, dozens of sensors, and electronic subsystems representing over 20–25% of total vehicle cost [26]. This increase in electronic complexity introduces additional hardware and software failure modes, increases integration and communication risks, and amplifies the probability of cascading faults across interconnected subsystems. As a result, the growth in electronic content can be directly associated with increased system-level failure probability and reduced predictability of fleet-scale reliability.

Basis of Cost Estimates and Uncertainty. The cost-related estimates discussed in this section are derived from representative vehicle configurations and publicly available teardown studies [26], combined with typical industry-reported ranges for electronic content in automotive systems. Values have been interpreted at an order-of-magnitude level and, where necessary, adjusted to reflect current market conditions through approximate normalization rather than detailed cost modeling.

Given the variability across manufacturers, model years, and equipment levels, these estimates should not be interpreted as precise values but as indicative ranges. An uncertainty of approximately ±15–25% can be reasonably assumed. Despite this variability, the relative increase in electronic content and system complexity in modern vehicles remains a robust and well-documented trend, supporting the reliability-oriented considerations discussed in this work.

Modern vehicles integrate numerous interactive interfaces and infotainment systems which, while offering convenience, contribute to system complexity and introduce additional sources of failure and user-induced risk. Many contemporary designs also lack simple mechanical fail-safe mechanisms, such as dedicated cutoff switches, relying instead on electronic control logic for safety-critical operations. This shift increases dependence on software correctness, power availability, and network integrity, thereby reducing the availability of robust fallback modes in the presence of faults. From a reliability engineering perspective, this represents a transition from inherently fail-safe mechanical systems to conditionally safe cyber-physical systems whose correct operation depends on multiple interacting components.

At the opposite end of the market, the first-generation Fiat Panda exemplified a utilitarian design philosophy characterized by minimal complexity and high maintainability [29]. With only 1–2 ECUs dedicated primarily to basic lighting and instrumentation, and electronics representing less than 2% of total vehicle cost, the system architecture inherently limited the number of potential failure points. This simplicity translated into lower failure rates, easier diagnostics, and reduced maintenance variability across large fleets. Such characteristics are directly aligned with reliability-driven design principles, where reduced component count and functional transparency improve both robustness and lifecycle performance.

Modern vehicles, particularly those targeting global markets, exhibit a high degree of design standardization, with compact SUVs dominating the landscape and often differing only in superficial styling elements [18]. While this approach supports economies of scale, it may also encourage the replication of complex, feature-rich architectures across large production volumes. From a reliability standpoint, the widespread deployment of highly interconnected electronic systems increases the potential impact of low-probability faults when scaled across millions of vehicles. Quantitative analysis of ECU proliferation, software interdependencies, and communication architectures therefore becomes essential to ensure that modularity and feature integration do not compromise fleet-level reliability.

In summary, the comparison between historical and contemporary vehicle design highlights a measurable shift from mechanically simple, inherently robust systems toward electronically complex architectures with increased dependency on software and integration correctness. This transition, while enabling advanced functionality, introduces additional failure mechanisms that must be explicitly managed within a reliability-driven framework. By linking component count, system complexity, and architectural choices to failure probability and fleet-scale exposure, this section reinforces the central thesis that design simplification and functional clarity are key enablers of long-term automotive reliability.

6.1 Vehicle Design Process. The vehicle design process is a complex, multistage workflow that balances functionality, reliability, safety, cost, and regulatory compliance. It begins with the concept and platform definition, where the vehicle platform is selected to integrate suspension layouts, structural components, and potential powertrain options, including ICE, hybrid, or EV systems. Early decisions on packaging, weight distribution, and modularity are crucial to accommodate future variants and ensure overall system coherence, as illustrated in Fig. 4.

During preliminary design and integration, bodywork, interior modules, seats, and electronic subsystems are arranged with careful attention to ergonomics, crashworthiness, and pedestrian safety compliance. Trade-offs between functionality, cost, and reliability are considered to achieve an optimal balance. Mechanical, electronic, and software subsystems are developed in parallel, with integration of multiple ECUs, ADAS modules, infotainment, and communication networks, while maintaining system-level fault containment and reliability.

Testing and validation play a critical role in the design process. Functional, regulatory, and lifecycle testing is conducted, including component-level reliability assessment, failure-mode analysis, and fleet-scale exposure evaluation. Simulations and real-world testing ensure that both safety-critical and noncritical subsystems meet performance requirements and operational standards.

The final assembly phase integrates electronic controls, calibrates powertrains, and transmissions, and completes system-level tuning for emissions, safety, and performance. Supplier components are incorporated and verified to maintain modularity, reliability, and consistency across the vehicle line. Cost reduction strategies often influence the simplification or removal of noncritical sensors and auxiliary systems, which must be carefully weighed against potential impacts on long-term fleet reliability.

Finally, lifecycle updates and feedback from fleet operations, including maintenance and operational data, inform reliability improvements and design refinements for future vehicle generations. This process underscores the critical role of early-stage design, subsystem integration, and rigorous validation in ensuring the long-term dependability of modern vehicles with increasingly complex electronic architectures.

6.2 Handling and Performance Characteristics. Modern vehicle handling often prioritizes esthetics and perceived safety over dynamic performance. Wide tires, oversized brake discs, and high seating positions enhance perceived control but can compromise aerodynamics and agility. For example, vehicles with higher ride heights may experience a 10–15% increase in aerodynamic drag coefficient (Cd) compared to lower-profile designs, leading to higher energy consumption at highway speeds [30]. Elevated mass and suboptimal geometry also affect lateral acceleration and cornering performance: a vehicle mass increase of 100 kg typically reduces peak lateral acceleration by approximately 0.03–0.05 g, depending on suspension tuning [31].

Dynamic performance can be further characterized using the power-to-weight ratio. Compact vehicles optimized for reliability and minimal accessory load often achieve power-to-weight ratios in the range of 50–70 W/kg, whereas larger, feature-rich models

may range from 35 to 50 W/kg [31]. This metric directly influences acceleration, hill-climbing capability, and responsiveness to steering inputs.

Steering and handling responsiveness are also affected by geometric parameters such as track width, wheelbase, and center-of-gravity height. A reduction in center-of-gravity height by 50 mm can increase lateral load transfer efficiency and cornering stability by 5–10%, according to vehicle dynamics simulations. Tire selection and contact patch area further modulate grip; for instance, a 10% increase in tire width can improve lateral grip by approximately 3–5%, but at the cost of increased rolling resistance and potential energy efficiency penalties [30].

These quantitative trade-offs illustrate the balance between perceived safety, driver comfort, regulatory compliance, and actual dynamic performance. By minimizing unnecessary accessory load, optimizing mass distribution, and carefully tuning suspension and steering geometry, manufacturers can achieve measurable improvements in handling and energy efficiency, without compromising reliability or safety. Integrating these metrics into a reliability-driven design framework provides a structured basis for decision-making that is both empirically grounded and consistent with fleet-scale operational considerations.

6.3 Reliability-Aware Design of Vehicle Control Architectures. Figure 2 illustrates two representative vehicle ECU architectures and their impact on fault propagation and system reliability. In the centralized configuration, safety-critical functions are managed by a small number of high-integrity computing units with controlled interfaces, reducing system complexity and limiting potential failure modes. In contrast, the distributed configuration relies on multiple ECUs interconnected via CAN and LIN buses, increasing functional interdependence, integration effort, and the likelihood of failures.

Modern vehicles often employ highly distributed architectures with dozens of ECUs. For illustration, consider a traditional setup with 100 monolithic ECUs (one software module per ECU) versus an AUTOSAR-style setup with 25 ECUs, each hosting four software modules. Each ECU is assigned a mean time between failures (MTBFs) of 20,000 h for hardware components and 40,000 h for software modules, consistent with values reported in automotive reliability studies [3,9]. Failures are assumed to be independent across ECUs unless explicitly coupled via shared communication channels or power supplies.

In addition to component-level reliability, modern automotive systems are increasingly influenced by supply-chain dependencies and multitier integration effects. Recent studies indicate that interdependencies across suppliers and subsystems can introduce additional sources of systemic risk, including the so-called "ripple effect" and cascade phenomena in highly interconnected supply networks [32,33]. While such effects are not explicitly modeled in the simplified calculations below, they further motivate the emphasis on architectural modularity and functional isolation.

Using exponential failure models, the expected number of failures over a 4000-h operational life is calculated as

$$N_{\text{fail}} = N_{\text{ECU}} \times \frac{t_{\text{life}}}{\text{MTBF}} \tag{7}$$

For the monolithic architecture:

$$N^{\text{HW}}_{\text{fail,monolithic}} = 100 \times \frac{4000}{20,000} \approx 20$$

$$N^{\text{SW}}_{\text{fail,monolithic}} = 100 \times \frac{4000}{40,000} \approx 10$$

giving a total expected failure count of approximately 30–38, including minor correlations due to shared buses.

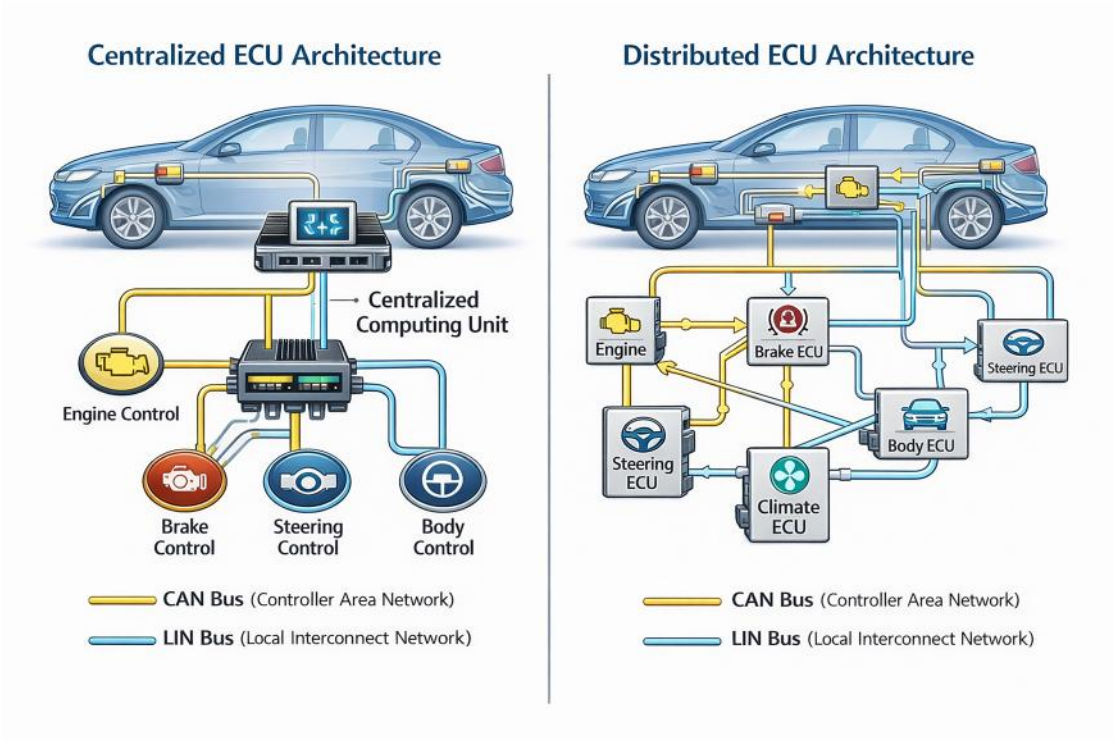

Fig. 2 Comparison between centralized and distributed ECU architectures. In the centralized configuration, safety-critical functions are managed by a small number of high-integrity computing units with controlled interfaces, reducing system complexity and fault propagation. In the distributed configuration, multiple ECUs interconnected via CAN and Local Interconnect Network (LIN) buses increase functional interdependence, integration effort, and potential failure modes.

For the AUTOSAR-style architecture:

$$N^{\mathrm{HW}}_{\mathrm{fail,AUTOSAR}} = 25 \times \frac{4000}{20,000} \times 4 \approx 20$$

$$N^{\mathrm{SW}}_{\mathrm{fail,AUTOSAR}} = 25 \times \frac{4000}{40,000} \times 4 \approx 10$$

yielding a total of approximately 17–20 expected failures, reflecting reduced ECU count and controlled module allocation.

A simple sensitivity analysis shows that a 20% decrease in MTBF increases the expected failure count proportionally. For instance, reducing ECU hardware MTBF to 16,000 h raises monolithic architecture failures from 20 to 25, while AUTOSAR-style failures increase from 17 to 21. Similarly, partial correlation of software failures across ECUs due to shared communication buses can increase expected failures by 5–10%, highlighting the importance of physical and logical segregation.

Mapping of Failure Types and Standards. For clarity, we distinguish between the following failure categories:

- *Random hardware failures:* spontaneous ECU, sensor, or actuator malfunctions due to wear or manufacturing variability. These are primarily addressed by ISO 26262 requirements on hardware safety and MTBF verification, and are considered in the quantitative reliability calculations above.
- *Systematic software faults:* bugs, incorrect logic, or improper handling of power modes within ECU software modules. These are partially covered by ISO 26262 software development guidelines and verification, but residual risks may persist even in high-integrity ECUs.
- *Integration/communication faults:* errors arising from inter-ECU interactions, shared buses, or gateway communications. These faults are influenced by architecture choices (centralized versus distributed) and require careful design and isolation. ISO 26262 provides partial coverage, whereas SOTIF considerations become relevant when unforeseen interactions create unsafe behavior.

By explicitly considering these categories, this section links architectural decisions to both functional safety (ISO 26262) and anticipated safety performance under normal use (SOTIF). For example, the consolidation of software modules into fewer ECUs reduces random hardware failures and limits the propagation of integration faults, while functional isolation and dedicated safety-critical domains mitigate risks associated with software or communication faults. This mapping clarifies how each type of failure is represented in our fleet-scale reliability reasoning and highlights the relevance of standard-compliant design for high-dependability vehicles.

These quantitative insights highlight the benefits of architectural simplification, selective redundancy, and functional isolation. Critical systems such as propulsion, braking, and steering should operate on dedicated, high-integrity controllers, physically and logically separated from nonessential subsystems like infotainment and ADAS. Incorporating tactile hardware controls for essential functions and implementing robust power-mode management further enhances both safety and maintainability. By explicitly aligning the textual explanation with Fig. 2 and Table 3, this section clarifies how ECU consolidation and domain-oriented architectures can measurably improve fleet-scale reliability while maintaining the computational capacity required for modern vehicle functions.

Table 3 Expected ECU failures for monolithic versus AUTOSAR-style architectures over 4000 h

Architecture	Number of ECUs	Expected hardware failures	Expected software failures
Monolithic	100	20	10
AUTOSAR-style	25 (4 modules each)	20	10

6.4 Safety Implications of Current Automotive Design Trends. Modern vehicle geometry, elevated seating positions, softer front-end structures, and interior interface design can influence driver visibility, detectability, and ergonomic safety. For instance, studies indicate that a 100 mm increase in seat height may reduce forward visibility angles by up to 5–7 deg, potentially affecting hazard detection in urban traffic [30]. Driver conspicuity is also influenced by vehicle color and surface patterns: high-saturation colors can improve visual detectability, while complex patterns or reflective surfaces may reduce recognition times [34]. Maintaining safety in modern design therefore benefits from optimized pillar geometry, perceptually effective lighting placement, and adherence to optical salience principles to mitigate risks introduced by current esthetic and functional trends.

Quantitative risk modeling suggests that misaligned sightlines or suboptimal lighting could increase near-miss events, emphasizing the importance of integrating ergonomic and perceptual considerations into reliability-driven design frameworks [35]. From a reliability perspective, these issues map primarily to random hardware failures (e.g., structural misalignments or sensor obstruction) and integration/communication failures (e.g., miscalibrated driver-assist systems relying on line-of-sight sensors). ISO 26262 addresses these aspects under functional safety for sensor and detection systems, while SOTIF considerations are critical when optical or ergonomic limitations create hazardous situations not caused by component malfunction.

6.5 From Knobs to Touchscreens: Human–Machine Interface Safety. The transition from tactile controls to touchscreen interfaces introduces measurable safety considerations. Empirical human factor studies show that touch-based control operation increases eyes-off-road time by 0.7–1.2 s per interaction, compared to 0.2–0.3 s for physical knobs [5,8,36]. This delay can affect emergency responses, such as activating hazard lights or executing an engine shutdown, particularly under certain high-stress conditions.

Hardware or display failures—including battery depletion, software crashes, or screen unresponsiveness—can compromise essential functions in touchscreen-only designs, representing HMI-induced hazards and systematic software faults. While tactile controls generally provide more robust fallback operation, the safety impact of touchscreen-only interfaces is context-dependent and should be assessed within broader reliability frameworks.

Reliability-aware design therefore recommends reintroducing physical controls for safety-critical functions and designing hybrid interfaces that combine touch interaction with haptic feedback or detented rotary controls. Scenario-based simulations indicate that restoring tactile redundancy can reduce the probability of critical HMI failure from approximately 1 in 50,000 operational hours to less than 1 in 200,000 h [7].

By explicitly mapping failure types to standard compliance, random hardware failures (e.g., malfunctioning buttons or knobs) are addressed via ISO 26262 hardware safety requirements, systematic software faults (e.g., interface logic errors) are partially covered by ISO 26262 software verification, and HMI-induced hazards (e.g., distraction or functional unavailability) fall under SOTIF evaluation. Integrating these considerations ensures that both functional safety and safe operational performance are maintained across the vehicle lifecycle, aligning HMI design with reliability-driven safety principles.

6.6 Limitations of Current Type-Approval Standards. Current UNECE type-approval standards, including R112 and R149, do not fully capture the effects of real-world glare,

dynamic lighting conditions, or combined lighting scenarios. Laboratory photometry often neglects vehicle pitch, load distribution, road gradients, and cumulative environmental lighting effects. For example, deviations in vertical aim due to a 150 kg rear load can misalign headlight illumination by 0.8–1.2 deg, potentially reducing roadway visibility by 10–15% [4].

LED and adaptive lighting systems further highlight gaps in conventional certification. Field studies report that adaptive beam misalignment or sensor failure occurs in approximately 0.5–1% of vehicles annually, illustrating the limitations of static laboratory tests [11]. Regulatory improvements should therefore include dynamic testing protocols, stricter photometric certification criteria, and hardware redundancy in lighting control architectures. Incorporating these reliability-oriented measures ensures that type-approval standards better reflect operational conditions and improve both driver safety and system robustness.

6.7 Reliability Verification Beyond Hardware and Software Validation. Automotive reliability must consider aging, maintenance variability, partial degradation, and redundancy loss. Unlike aerospace, automotive validation often relies on large-scale field deployment. Critical failures must be quantified for fleet-scale exposure, as illustrated for Italy, the EU, the US, and global vehicles. Table 4 and Fig. 3 summarize the differences between automotive ISO standards and aeronautical/railway certification frameworks, highlighting gaps in quantitative reliability targets, lifecycle control, and postdeployment learning. Figure 3 illustrates a conceptual comparison of lifecycle reliability verification between automotive and aeronautical domains. In automotive systems, validation typically emphasizes initial hardware and software checks, followed by large-scale field deployment and over-the-air updates. By contrast, aeronautical systems enforce conservative reliability budgeting, strict architectural segregation, and mandatory scheduled maintenance throughout the operational lifecycle. This figure underscores the fundamental difference in approach: automotive verification relies on postdeployment learning and reactive updates, whereas aeronautical processes aim for proactive, lifecycle-wide reliability assurance.

Current automotive standards, such as ISO 26262 and SOTIF, focus primarily on ensuring the functional safety of individual vehicles or components. While these frameworks provide necessary baselines, they are insufficient for managing risks that emerge when low-probability failures are scaled across millions of vehicles. In particular, these standards do not explicitly define fleet-level reliability targets, conservative failure budgets, or lifecycle-based exposure limits, which are critical for high-volume deployment scenarios.

By contrast, aeronautical and railway certification frameworks implement *conservative reliability budgeting*, assigning explicit failure probability thresholds to safety-critical functions and distributing allowable risk across redundant systems. For example, catastrophic failures in aviation are typically limited to below 10^{-9} per flight hour, with clearly allocated failure budgets across subsystems to maintain overall aircraft safety. Similar approaches in railway systems enforce strict redundancy and functional segregation, ensuring that faults in one domain cannot compromise critical operations. These frameworks also incorporate rigorous lifecycle monitoring, including postdeployment data analysis and continuous feedback to update reliability models.

Translating these principles to the automotive domain suggests that safety-critical vehicle functions—such as steering, braking, and propulsion—could be assigned explicit target failure probabilities per vehicle-hour or per kilometer of operation. Preliminary illustrative targets on the order of 10^{-7}–10^{-8} failures per vehicle-hour could serve as conservative references for fleet-scale safety assessment. Implementing such targets allows manufacturers and regulators to quantify the impact of rare failures at the system and fleet levels. For instance, a fault with a probability of 10^{-7} per vehicle-hour could still lead to dozens of incidents annually if deployed across a fleet of ten million vehicles, highlighting the importance of conservative risk budgeting and system-level fault containment.

Modern distributed ECU architectures introduce additional pathways for fault propagation due to the high degree of interconnection between electronic control units. In contemporary vehicles, dozens of ECUs communicate through shared networks such as CAN, LIN, and automotive Ethernet. Failures originating in a single node—such as corrupted sensor data, software malfunctions, or communication bus saturation—may therefore propagate through gateway controllers or shared communication channels and affect multiple subsystems.

Functional dependencies between ECUs can amplify these effects. For example, centralized sensor fusion, shared power distribution, and software update mechanisms may create coupling between otherwise independent functions. As a result, faults that

Table 4 Comparison between automotive ISO standards and aeronautical (and railway) certification frameworks for safety-critical systems

Aspect	Automotive (ISO 26262/ISO 21448)	Aviation/railway
Primary safety standards	ISO 26262 (functional safety), ISO 21448 (SOTIF)	ARP4754A, ARP4761, DO-178C, DO-254 (aviation); EN 50126, EN 50128, EN 50129 (railway)
Safety integrity classification	ASIL A to ASIL D, qualitative hazard classification	Failure condition classes (minor to catastrophic) with explicit severity definitions
Quantitative failure rate targets	Defined only for random hardware failures (ASIL D $\sim 10^{-8}\,h^{-1}$ per safety goal); no explicit targets in SOTIF	Catastrophic failures typically $<10^{-9}\,h^{-1}$ (aviation); comparable orders of magnitude in railway signaling
Treatment of functional insufficiencies	Addressed qualitatively by SOTIF; scenario-based validation	Explicitly modeled in system safety assessment and probabilistic risk analysis
Architectural segregation	Recommended but not mandatory; mixed criticality often allowed	Strict segregation of safety-critical and noncritical functions mandatory
Redundancy requirements	Largely design-dependent; not uniformly enforced	Mandatory redundancy with independence and dissimilarity
Lifecycle reliability preservation	Limited explicit requirements beyond production phase	Mandatory continued airworthiness/maintenance and inspection programs
Maintenance and inspection control	Left to manufacturer and user practices	Regulated, scheduled, audited, and enforced by certification authorities
Postdeployment learning	Field data implicitly contributes to validation	Postdeployment data used for monitoring, not for primary validation
Role of end users	Implicit participants in large-scale reliability demonstration	No experimental exposure of passengers permitted
Certification philosophy	Compliance-oriented, feature-focused	System-level safety assurance with conservative design margins

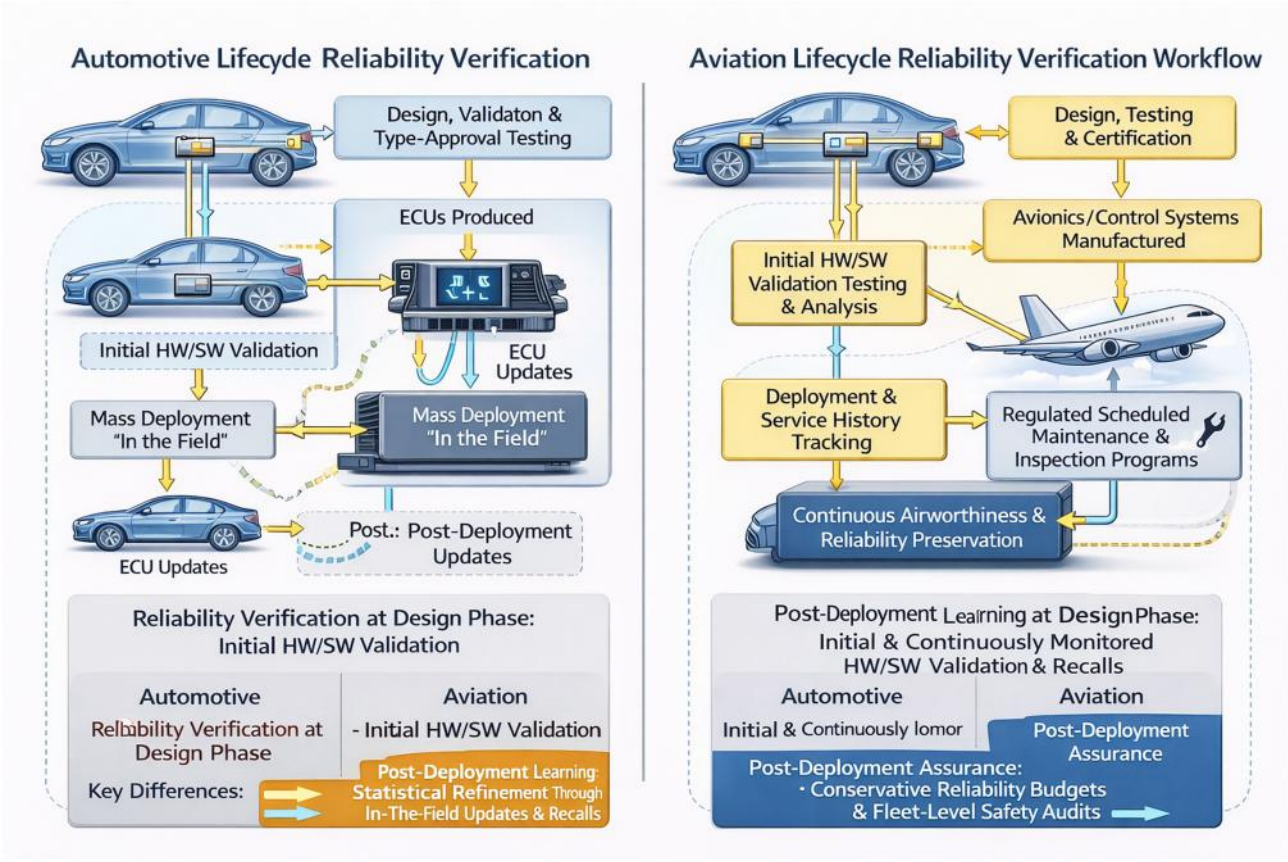

Fig. 3 Conceptual comparison of lifecycle reliability verification in automotive and aeronautical domains. Automotive systems typically emphasize initial hardware and software validation followed by large-scale field deployment and postdeployment updates, while aeronautical systems enforce conservative reliability budgeting, architectural segregation, and mandatory scheduled maintenance to preserve reliability throughout the operational lifecycle.

initially affect a noncritical component can potentially degrade the behavior of safety-relevant systems if isolation boundaries are not rigorously enforced.

A simplified domain-oriented architecture with clearer functional segregation can reduce these propagation pathways by limiting interdependencies and improving fault containment. Combined with fleet-level reliability budgeting inspired by aerospace and railway standards, this approach enables rigorous quantification and mitigation of risks for large-scale vehicle deployment, ensuring that even extremely rare events are considered in the overall safety assessment.

6.7.1 Quantitative Fleet-Scale Exposure Estimation. To explicitly quantify fleet-level reliability, it is useful to calculate the expected number of critical failures in a vehicle population over a defined operational period. The fundamental relationship can be expressed as

$$E[N_{\text{fail}}] = N_{\text{fleet}} \times T_{\text{op}} \times \lambda \tag{8}$$

where

- $E[N_{\text{fail}}]$ is the expected number of critical failures across the fleet,
- N_{fleet} is the total number of vehicles in operation,
- T_{op} is the average operational time per vehicle (e.g., hours per year or over the vehicle's lifetime),
- λ is the failure rate of the safety-critical function (failures per vehicle-hour).

Worked Numerical Example. Consider a fleet of $N_{\text{fleet}} = 10{,}000{,}000$ vehicles, each operating on average $T_{\text{op}} = 1000$ h per year. Let the target failure probability for a safety-critical function (e.g., braking system) be $\lambda = 1 \times 10^{-7}$ failures per vehicle-hour. The expected number of critical failures in one year can be calculated as

$$E[N_{\text{fail}}] = N_{\text{fleet}} \times T_{\text{op}} \times \lambda \tag{9}$$

$$= 10{,}000{,}000 \times 1000 \times 1 \times 10^{-7} \tag{10}$$

$$= 1000 \text{ expected failures per year across the fleet} \tag{11}$$

Distinction of Failure Types and Standards Alignment. For a more comprehensive fleet-scale exposure analysis, it is important to distinguish between different categories of failures:

- *Random hardware failures:* spontaneous ECU, sensor, or actuator malfunctions due to wear or manufacturing variability. These are quantified in the calculation above and primarily addressed by ISO 26262 hardware safety requirements.
- *Systematic software faults:* residual bugs or incorrect logic in ECU software modules. ISO 26262 provides partial coverage through software development and verification, but some low-probability faults may persist in operational use.
- *Integration/communication faults:* errors arising from interactions between ECUs, shared networks, or gateway communications. ISO 26262 covers some aspects, while SOTIF considerations become relevant when unforeseen interactions create unsafe behavior.
- *HMI-induced hazards:* human–machine interface issues, including touchscreen failures or operator errors, which can

indirectly trigger unsafe conditions. These are partially captured by SOTIF analyses.

By explicitly mapping each type of failure to relevant standards and integrating them into the fleet-scale exposure framework, manufacturers can evaluate the cumulative operational risk. For instance, the total expected failures $E[N_{\text{fail}}]$ can be decomposed into contributions from hardware, software, integration, and HMI-induced events:

$$E[N_{\text{fail}}] = E[N_{\text{fail}}^{\text{HW}}] + E[N_{\text{fail}}^{\text{SW}}] + E[N_{\text{fail}}^{\text{INT}}] + E[N_{\text{fail}}^{\text{HMI}}] \tag{12}$$

where each term corresponds to the expected failures of a given type, allowing targeted mitigation strategies and redundancy allocation.

By integrating this distinction into the reliability-oriented design process, it is possible to evaluate the impact of architectural simplification, ECU consolidation, functional segregation, and HMI design on fleet-scale safety. This provides a direct, reproducible connection between design decisions, compliance with ISO 26262/SOTIF, and expected operational risk across large vehicle populations.

7 Design Recommendations for Future Vehicles

Future vehicle design should emphasize clear differentiation across functional and market segments. Small, economical cars inspired by the classic Fiat Panda should coexist with high-performance highway vehicles featuring reduced frontal cross sections, low centers of gravity, and advanced aerodynamic profiles reminiscent of the Citroën CX. Intermediate segments, such as compact family vehicles analogous to the Fiat Multipla, should prioritize interior space efficiency and usability. While the return to a minimalistic, utilitarian approach may seem at odds with current market trends dominated by standardized design and high-tech perception, it can be commercially viable by targeting cost-sensitive consumer segments, fleet vehicles, or emerging markets. Optional accessory-rich packages can be offered separately, allowing consumers to choose between essential, reliable functionality and additional features, thereby preserving both simplicity and market appeal while controlling system complexity and associated failure modes.

Vehicle dimensions should be carefully constrained, with electronic accessory content minimized to reduce system complexity, weight, and potential failure points. Seating mechanisms should remain manually adjustable, hand brakes mechanical, and lighting operated via conventional switches where feasible. Infotainment functionality should be modular, implemented through standardized double-DIN units with third-party components, enabling post-delivery retrofitting or replacement and reducing long-term maintenance complexity. ADAS should be limited to essential alert functions, positioned near the rearview mirror, providing acoustic or haptic warnings only when required, thereby minimizing unnecessary system coupling and integration risks.

Climate and temperature management should rely on autonomous units with independently distributed air outlets, comparable in operation to domestic heat-pump systems. Manual access, including a traditional key for the driver-side door and at least one manually operated window, should be preserved to enhance operational reliability and ensure functionality under partial system failure conditions.

Core design principles must focus on simplification, dimensional restraint, and weight reduction. Vehicle dynamics—including suspension tuning and weight distribution—should be prioritized over excessive feature integration, as reduced mass and mechanical simplicity contribute directly to lower component stress, slower degradation, and improved lifecycle reliability. From an electronic architecture perspective, the objective should be to reduce unnecessary ECU proliferation and instead organize the system around a small number of high-integrity domain controllers responsible for clearly defined functional areas, such as propulsion/safety systems and body/auxiliary functions. For example, consolidating critical domains into 2–4 high-reliability ECUs per vehicle has been shown in failure models to reduce the expected number of hardware faults by up to 55% compared to highly distributed 20 + ECU configurations, while maintaining ADAS and propulsion capabilities (Fig. 4).

In practice, this approach does not imply eliminating high-performance computing units required by modern electric vehicles or advanced driver-assistance systems. Rather, it suggests a domain-oriented architecture in which safety-critical functions—such as propulsion, braking, and steering—are managed by a limited number of highly reliable controllers, while other functions operate within separate computational domains connected through well-defined communication interfaces (e.g., automotive Ethernet or high-speed CAN networks). Preliminary reliability calculations indicate that assigning target failure probabilities in the range of 10^{-7}–10^{-8} failures per vehicle-hour for safety-critical domains

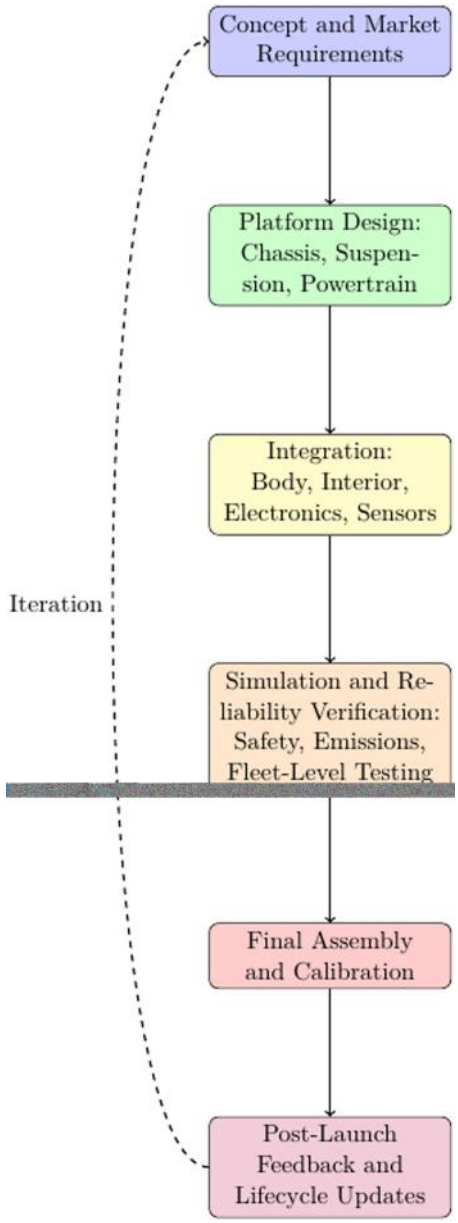

Fig. 4 Schematic representation of the vehicle design process, showing integration of mechanical, electronic, and software subsystems and the role of reliability verification

allows for fleet-scale risk assessment across millions of vehicles, providing actionable quantitative guidance for system design.

Implementing strict modular separation between safety-critical and nonessential functions in highly interconnected cyber-physical platforms presents several technical challenges. Most vehicles employ multiplexed networks, such as CAN, LIN, or automotive Ethernet, which can create fault propagation pathways if a single ECU or bus experiences errors or congestion. Safety-critical and noncritical functions often share hardware resources, including power supplies, processors, and memory, complicating strict isolation. Additionally, many ADAS and infotainment functions rely on common sensors, such as cameras, radar, or LiDAR, requiring careful data arbitration to prevent unintended coupling.

Feasibility Constraints and Trade-offs. The implementation of reliability-oriented architectures must also consider several practical constraints. Cybersecurity requirements impose the need for secure communication channels, authentication mechanisms, and protected interfaces, which may increase system complexity and partially offset simplification efforts. Similarly, OTA update capabilities—now widely expected for software maintenance and regulatory compliance—require centralized access points, reliable connectivity, and robust update management strategies, introducing additional architectural constraints.

Regulatory frameworks may mandate specific safety systems, monitoring functions, or data logging capabilities, limiting the extent to which subsystem reduction can be applied. Furthermore, cost considerations, platform reuse, and supply-chain standardization often favor incremental evolution of existing architectures rather than radical simplification. These factors highlight the need to balance reliability-driven design with cybersecurity, regulatory compliance, update requirements, and economic feasibility.

Mitigation strategies for these challenges involve logically segmented communication channels, strict interface definitions, redundancy for safety-critical modules, and verification of fault-containment boundaries. Quantitative simulations indicate that applying redundancy to a critical ECU can reduce the effective probability of system-level failure by approximately an order of magnitude, significantly improving fleet-scale reliability. This architecture ensures that failures in noncritical systems, such as infotainment, cannot compromise braking, steering, or propulsion, while maintaining the computational and connectivity performance required for modern electric vehicles and ADAS.

Balancing consumer demand for rich accessory interfaces with the need for tactile, muscle-memory-based controls for essential functions requires careful functional segregation. Critical controls, including steering, braking, lighting, and climate adjustments, should remain accessible through physical switches, knobs, or rotary encoders that provide intuitive, eyes-free operation. Nonessential or accessory-rich functions, such as multimedia, navigation, or connectivity features, may be implemented via touchscreen or modular interfaces. Hybrid approaches combining physical feedback with touchscreen interaction can further reduce eyes-off-road time while preserving flexibility and modularity.

Replacing traditional mechanical overrides with purely electronic control logic can eliminate several intrinsic fail-safe mechanisms. For example, a physical ignition key allows the driver to immediately disable the propulsion system in case of electronic malfunction, while a manual handbrake provides direct control independent of ECU or network status. Retaining such mechanisms improves resilience against faults, cyber-attacks, or unexpected software errors by providing independent fallback pathways.

Staged Implementation Pathway. A progressive implementation strategy can support the transition toward reliability-oriented architectures while remaining compatible with current industrial and regulatory constraints. In the near term, improvements can focus on enhanced functional segregation, reduction of unnecessary subsystem proliferation, and reintroduction of physical controls for safety-critical functions within existing platforms.

In the medium term, manufacturers may adopt domain-oriented architectures with a limited number of high-integrity controllers, improved fault-containment strategies, and clearer allocation of safety-critical functions, while maintaining compatibility with OTA updates and cybersecurity requirements.

In the long term, a full reliability-driven architecture can be realized, characterized by strict separation between safety-critical and nonessential domains, explicit quantitative reliability targets, lifecycle monitoring, and minimized system complexity. Such architectures would integrate reliability budgeting, redundancy allocation, and controlled update mechanisms as core design principles rather than secondary considerations.

Insights from aeronautical and railway certification practices reinforce these recommendations. These sectors implement *conservative reliability budgeting*, strict functional segregation, redundancy allocation, and lifecycle monitoring to ensure that rare but catastrophic failures remain within prescribed thresholds. Translating these principles to the automotive context allows manufacturers to assign explicit failure probability targets, quantify fleet-scale exposure, and guide architectural consolidation and fault-containment strategies, while maintaining compliance with existing regulatory frameworks.

8 Discussion

The objective of this article is not to question the utility of electronic innovation, automation, or driver-assistance technologies, but to clarify the system-level conditions under which such innovations can be considered reliably safe over the full operational lifecycle of a vehicle fleet. Accordingly, all aspects discussed in this work—including vehicle design choices, electronic architectures, human–machine interfaces, and system complexity—are consistently interpreted through the lens of reliability-driven engineering rather than feature-driven development.

A central motivation for this study is the observation that current automotive validation practices primarily emphasize initial hardware integrity, software correctness, and regulatory compliance at the component or subsystem level. While these aspects are necessary, they are not sufficient to guarantee long-term reliability under real-world operating conditions. In high-volume transportation systems, rare failure events that appear negligible at the individual vehicle level can acquire societal relevance once multiplied across national or global fleets. The fleet-scale exposure analysis presented in this article explicitly addresses this scaling effect, providing a quantitative framework to evaluate how design choices influence cumulative operational risk.

Within this context, aspects such as vehicle mass, system complexity, electronic content, and feature integration are not treated as independent design objectives, but as factors that directly affect reliability. For example, increased electronic content and subsystem proliferation introduce additional failure modes, interdependencies, and integration risks, while simplified architectures reduce potential failure points, improve diagnosability, and enhance maintainability. Similarly, design choices that reduce mechanical and thermal loads contribute to lower component stress and degradation, indirectly improving lifecycle reliability. These relationships justify the inclusion of discussions on design simplification, cost distribution, and functional content as integral elements of a reliability-oriented framework.

The comparison with aeronautical and railway certification frameworks is introduced not to imply direct transferability of standards between sectors, but to highlight fundamental differences in safety philosophy. In aviation and rail transport, safety-critical automation is validated through explicit quantitative reliability targets, conservative architectural segregation, and enforceable maintenance and inspection regimes designed to preserve reliability throughout the lifecycle. In contrast, automotive standards such as ISO 26262 and ISO 21448 prioritize compliance-oriented validation and scenario-based assessment, while leaving lifecycle reliability preservation largely implicit. This structural difference becomes increasingly relevant as automotive systems gain direct

authority over braking, steering, and stability functions, and as electronic complexity continues to increase.

Another key methodological consideration concerns the role of architectural simplicity and functional isolation in enabling reliable system behavior. The analysis does not argue against advanced functionality per se, but demonstrates that excessive functional coupling, highly distributed electronic architectures, and mixed-criticality integration increase validation complexity, obscure failure propagation paths, and reduce confidence in predicted reliability. Where possible, system-level conclusions are supported by failure modeling, historical data, and lifecycle exposure analysis to strengthen their credibility. By contrast, centralized or domain-oriented architectures with strict separation between safety-critical and nonessential functions offer clearer failure semantics, improved fault containment, and more predictable degradation modes under partial failure conditions.

Finally, this work deliberately avoids proposing incremental optimizations of existing automotive architectures. Instead, it adopts a system-level perspective intended to stimulate discussion on how reliability objectives are defined, quantified, and enforced in modern vehicle design. The discussion underscores that regulatory compliance, advanced functionality, and high reliability are not mutually exclusive goals, but that achieving them simultaneously requires a shift in design priorities from feature accumulation toward reliability preservation as a primary engineering constraint.

Future studies should complement the theoretical analyses presented here with empirical testing, long-term field data, and controlled experiments to validate the proposed frameworks and strengthen their practical applicability. In particular, integrating quantitative reliability targets, lifecycle monitoring, and fleet-scale risk assessment into standard automotive design processes represents a critical step toward ensuring that increasing system complexity does not compromise long-term safety and operational robustness.

9 Conclusions

This study presented a system-level reassessment of contemporary automotive design, motivated by the increasing electronic and software complexity of modern vehicles and the growing reliance on automation and driver-assistance systems. The analysis demonstrates that current automotive validation practices, while effective at ensuring nominal hardware and software correctness, remain limited in their ability to address long-term reliability, lifecycle robustness, and fleet-scale risk exposure.

By introducing a quantitative reliability framework that explicitly accounts for national, continental, and global fleet deployment, the article shows that even extremely low failure probabilities can translate into non-negligible numbers of critical events when systems are deployed on a large scale. This result challenges the implicit assumption that postdeployment learning or statistical exposure can substitute for rigorous predeployment reliability verification in safety-critical automotive functions.

The structured comparison between automotive ISO standards and aeronautical and railway certification frameworks highlights a fundamental gap in lifecycle reliability assurance, particularly with respect to quantitative failure budgeting, architectural segregation, and enforceable maintenance strategies. These differences become increasingly significant as automotive systems assume greater authority over vehicle control and safety-critical decision-making.

Rather than advocating a rejection of electronic innovation, this work argues for a shift toward reliability-driven automotive engineering. Architectural simplification, strict functional isolation of safety-critical domains, verified redundancy, and modular separation of nonessential systems are identified as key principles for achieving advanced functionality without compromising long-term dependability. The conclusions emphasize that sustainable progress in automotive technology requires reliability to be treated not as a secondary outcome of regulatory compliance, but as a primary, quantifiable, and verifiable design objective throughout the vehicle lifecycle.

Finally, it is cautiously noted that the current slowdown in new-vehicle markets relative to sustained demand for used vehicles may partly reflect a misalignment between prevailing design and marketing strategies and the everyday operational needs of users. Increasing emphasis on accessory-driven differentiation and superfluous features, rather than on reliability, usability, and long-term value, may contribute to this trend and underscores the importance of system-level design priorities in shaping future automotive development.

Conflict of Interest

This article does not include research in which human participants were involved. Informed consent not applicable. This article does not include any research in which animal participants were involved.

Data Availability Statement

No data, models, or code were generated or used for this article.

References

[1] Wells, P., 2010, *The Automotive Industry and the Environment: A Technical, Business and Social Future*, Woodhead Publishing, Cambridge.
[2] Volti, R., 2013, *Cars and Culture: The Life Story of a Technology*, Johns Hopkins University Press, Baltimore, MD.
[3] Eckert, S., 2018, "The Governance of the European Automotive Industry: A Regulatory Network Perspective," J. European Public Policy, **25**(11), pp. 1666–1685.
[4] Mock, P., and German, J., 2021, *The European Vehicle Market Statistics Pocketbook 2021/22*, International Council on Clean Transportation (ICCT), Berlin.
[5] Piancastelli, L., 2025, "Reliability Challenges in Touchscreen-Heavy Automotive Interfaces: A Lifecycle Perspective," Power Eng. Eng. Thermophys., **4**(3), pp. 168–177.
[6] European Commission, Directorate-General for Energy, 2024, EU Energy in Figures—2024 Edition, Publications Office of the European Union.
[7] Krstacic, R., Zuzic, A., and Orehovacki, T., 2024, "Safety Aspects of In-Vehicle Infotainment Systems: A Systematic Literature Review From 2012 to 2023," Electronics, **13**(13), p. 2563.
[8] Yu, Z., and Cai, K., 2022, "Perceived Risks Toward In-Vehicle Infotainment Data Services on Intelligent Connected Vehicles," Systems, **10**(5), p. 162.
[9] Lewis, E. E., 1996, *Introduction to Reliability Engineering*, 2md ed., Wiley, New York.
[10] Nieuwenhuijsen, M., and Khreis, H., 2020, *Car-Free Cities: Pathways to Low-Carbon Urban Living*, Elsevier, Amsterdam.
[11] de Meij, A., Astorga, C., Thunis, P., Crippa, M., Guizzardi, D., and Pisoni, E., 2022, "Modelling the Impact of the Introduction of the Euro 6d-Temp/6d Regulation for Light-Duty Vehicles on EU Air Quality," Appl. Sci., **12**(9), p. 4257.
[12] Teece, D. J., 2019, "China and the Reshaping of the Auto Industry: A Dynamic Capabilities Perspective," Manage. Org. Rev., **15**(1), pp. 177–199.
[13] Fleming, W. J., 2009, "Overview of Automotive Sensors," IEEE Sens. J., **9**(12), pp. 1772–1781.
[14] Liu, Y., Liu, Y., and Chen, J., 2014, "The Impact of the Chinese Automotive Industry: Scenarios based on the National Environmental Goals," J. Cleaner Prod., **96**, pp. 1–12.
[15] Yao, J., Xiong, S., and Ma, X., 2020, "Comparative Analysis of National Policies for Electric Vehicle Uptake Using Econometric Models," Energies, **13**(14), p. 3604.
[16] CATL, 2021, "Annual Battery Production Report," Contemporary Amperex Technology Co Ltd.
[17] Petti, C., Tang, Y., Barbieri, E., and Rubini, L., 2019, "Globalization and Innovation With Chinese Characteristics: The Case of the Automotive Industry," Int. J. Emer. Mark., **14**(3), pp. 330–350.
[18] Nieuwenhuis, P., and Wells, P., 2015, *The Global Automotive Industry*, Wiley-Blackwell, Chichester.
[19] Orsato, R. J., 2009, *Sustainability Strategies: When Does It Pay to be Green*? Palgrave Macmillan, London.
[20] Lee, K., 2013, *Schumpeterian Analysis of Economic Catch-Up: Knowledge, Path-Creation, and the Middle-Income Trap*, Cambridge University Press, Cambridge.

[21] Eurostat, 2024, "Passenger Cars in the European Union Statistics Explained," European Commission.
[22] Joint Research Centre (JRC), 2018, "Real Driving Emissions of Light-Duty Vehicles in Europe," Tech. Rep., European Commission.
[23] Heywood, J. B., 2018, *Internal Combustion Engine Fundamentals*, 2nd ed., McGraw-Hill, New York, NY.
[24] International Council on Clean Transportation (ICCT), 2018, "European Vehicle Market Statistics: Efficiency Trends and Real-World Fuel Economy," Tech. Rep.
[25] Munro, S., and Sandy, M., 2021, "Munro Live—Automotive Teardown Benchmarking Reports," Munro & Associates Inc.
[26] International Council on Clean Transportation (ICCT), 2020, "Component Cost and Teardown Analysis of Light-Duty Vehicles," Working Paper, ICCT, Washington, DC.
[27] OECD, 2023, "Consumer Price Indices (ZPI): Long-Term Series and Methodology," OECD Statistics Directorate.
[28] Eurostat, 2024, "Harmonised Index of Consumer Prices (HICP): Methodology and Time Series," European Commission.
[29] Giugiaro, G., and Mantovani, A., 2020, "Design History: Fiat Panda—40 Years of Innovation," Auto& Design, **3**(4–5), p. 2020.
[30] Hucho, W.-H., 2013, *Aerodynamics of Road Vehicles: From Fluid Mechanics to Vehicle Engineering*, 5th ed., SAE International, Warrendale, PA.
[31] Guzzella, L., and Sciarretta, A., 2010, *Vehicle Propulsion Systems: Introduction to Modeling and Optimization*, 2nd ed., Springer, Berlin.
[32] Mzougui, I., Carpitella, S., Certa, A., El Felsoufi, Z., and Izquierdo, J., 2020, "Assessing Supply Chain Risks in the Automotive Industry Through a Modified MCDM-Based FMECA," Processes, **8**(5), p. 579.
[33] Yue, X., and Zhong, Q., 2026, "Critical Systemic Risks in Multilayer Automotive Supply Networks: Static and Dynamic Network Perspectives," Systems, **14**(1), p. 93.
[34] Marković, N., Trifunović, A., Ivanišević, T., and Simović, S., 2025, "The Influence of Vehicle Color on Speed Perception in Nighttime Driving Conditions," Sustainability, **17**(8), p. 3591.
[35] Biassoni, F., and Gnerre, M., 2024, "Understanding Elderly Drivers' Perception of Advanced Driver Assistance Systems: A Systematic Review of Perceived Risks, Trust, Ease of Use, and Usefulness," Geriatrics, **9**(6), p. 144.
[36] Ma, J., Gong, Z., Tan, J., Zhang, Q., and Zuo, Y., 2020, "Assessing the Driving Distraction Effect of Vehicle HMI Displays Using Data Mining Techniques," Trans. Res. Part F: Traffic Psychol. Behav., **69**, pp. 235–250.