Proceedings of the Design Society, Volume 5: ICED25
https://doi.org/10.1017/pds.2025.10292

Resilience-By-Design: Standard-based definition of Resilience and identification of action fields for the systems design of mobility system

Isaac Mpidi Bita[1,✉], **Aschot Hovemann**[1] and **Roman Dumitrescu**[2]

[1] *Digital Engineering, Fraunhofer Institute for Mechatronic Systems Design IEM, Paderborn, Germany,*
[2] *Computer Science, Heinz-Nixdorf-Institute, University of Paderborn, Paderborn, Germany*

✉ isaac.mpidi.bita@iem.fraunhofer.de

ABSTRACT: The increasing complexity and connectivity of the mobility system and modern automotive systems, particularly connected autonomous vehicles, demand a paradigm shift toward resilience-by-design to address disruptions in dynamic environments. Unlike established safety and cybersecurity engineering in automotive, resilience engineering has yet to be systematically integrated into development processes. This paper defines resilience using a standard-based definition method, emphasizing disruption tolerance, adaptability, and recoverability. We identify action fields to advance the topic and propose a resilience-by-design framework extending safety and cybersecurity perspectives. Resilience-by-design offers strategies and methods to design robust, adaptive systems, ensuring reliability and availability of automotive systems, functions, and components in operation.

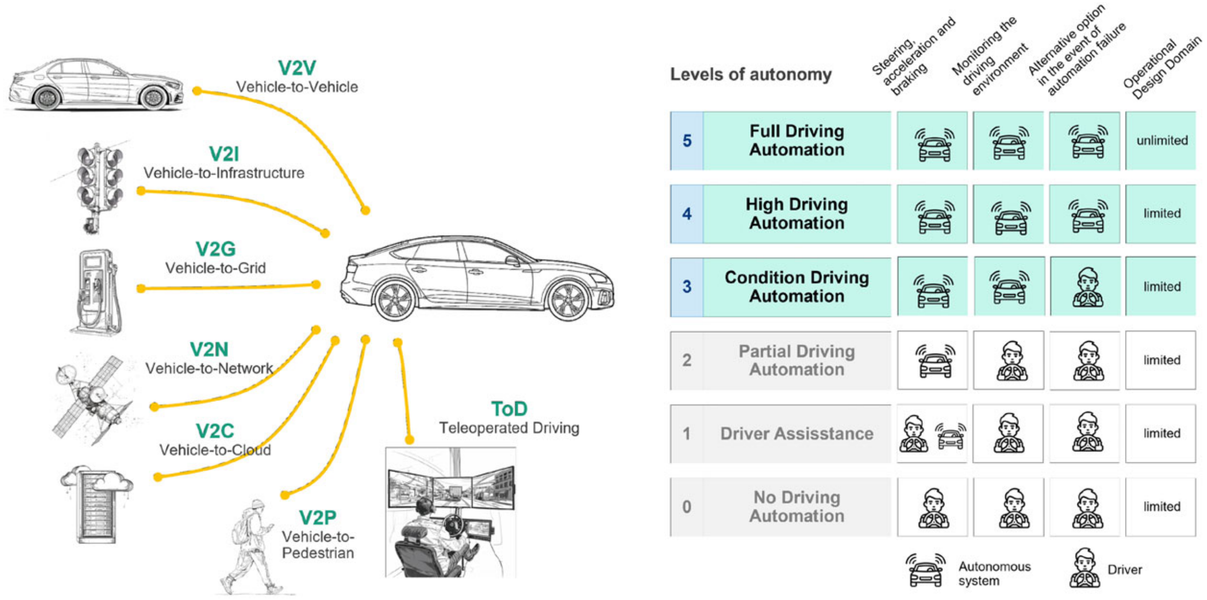
KEYWORDS: Resilience-by-Design, Automotive Systems Engineering, Systems Engineering (SE), Design to X,, Risk Management

1. Introduction

The mobility system has evolved into a complex structure, often described in systems engineering as a system-of-systems (SoS). In such systems, subsystems like connected vehicles or traffic lights operate independently yet are highly interdependent due to intensive networking (Walden et al., 2015). As illustrated in Figure 1, elements of the SoS such as vehicles, pedestrians, cloud services, and infrastructure continuously exchange data, which is processed to trigger actions. This information flow is critical for enabling advanced driver assistance systems and complex driving functions, particularly in autonomous driving. Distributed driving functions, where tasks are decentrally executed across multiple systems, leverage shared data to deliver precise and reliable outcomes—for example, in intersection management systems (Bach et al., 2017). The SAE's levels of vehicle automation highlight that increasing autonomy shifts greater decision-making responsibility to the vehicle, requiring it to analyze dynamic traffic environments independently and make informed decisions accordingly. SAE Standard (2021)

1.1. Challenges

In recent years, many vehicles have been equipped with Level 2 and early Level 3 driving functions. This trend is expected to grow (Buchholz, 2024). Ensuring the reliability and availability of distributed driving functions is crucial, particularly regarding interoperability within the mobility system (SoS). The complexity of the SoS increases due to the interdependencies, not only leading to technical failures but also introducing new cybersecurity threats. For example, Miller and Valasek demonstrated how software vulnerabilities in connected vehicles can be exploited to take control of the vehicle (Valasek and



Levels of autonomy		Steering, acceleration and braking	Monitoring the driving environment	Alternative option in the event of automation failure	Operational Design Domain
5	Full Driving Automation	🚗	🚗	🚗	unlimited
4	High Driving Automation	🚗	🚗	🚗	limited
3	Condition Driving Automation	🚗	🚗	👤	limited
2	Partial Driving Automation	🚗	👤	👤	limited
1	Driver Assisstance	👤 🚗	👤	👤	limited
0	No Driving Automation	👤	👤	👤	limited

Figure 1. Complexity in the modern mobility system based on SAE Standard (2021)

Miller, 2015). Addressing such risks in the systems design phase is a key focus of cybersecurity engineering. Autonomous vehicles face challenges beyond technical faults, such as poor decision-making in unpredictable traffic situations. A well-known example is a Tesla accident where assistance systems failed to detect a crossing semi-trailer due to system boundary mismanagement, inadequate sensors, and insufficient driver task handover (Schnieder and Hosse, 2020). Such issues are addressed through Safety of the Intended Functionality (SOTIF) during the systems design phase. Engineering automated driving functions also requires compliance with international regulations like UNECE R155 or Germany’s national type approval (Kraftfahrt-Bundesamt, 2022). Meeting these regulations involves detailed functional descriptions, operational domain definitions, and analyses for functional safety and security to address hazard, misuse, and threat scenarios. OEMs must develop assurance concepts to support the argumentation (Kraftfahrt-Bundesamt, 2022). This should take a holistic view of a system in terms of all types of disruptive events. This perspective is not only safety-centric or security-centric but adopts a holistic view to ensure the availability and reliability not only of the implemented driving functionality but also of the vehicle and its internal systems and subsystems. One of the technical terms that is often associated with this issue in the literature is resilience. Resilience encompasses the ability to maintain functionality and recover from disruptions. A clear understanding of resilience is essential for addressing the complex challenges of automated driving systems.

1.2. Research Questions

Resilience is a concept used in various fields, typically defined as the ability to withstand environmental risks or to overcome stress or adversity (Rutter, 2006). According to this definition, a resilient system should be able to deal with different stresses or adversities. This paper analyses the concept of resilience in the context of the automotive industry. This analysis aims to define it in the automotive context and to distinguish it from the essential concepts and principles of classical cybersecurity and safety engineering in the automotive sector. We also include research questions that can be addressed in the context of automotive resilience. The increasing networking and automation of modern vehicles require new approaches and concepts, such as Resilience-By-Design. In this context, this paper poses two central research questions:

1. How can resilience be defined in the automotive context and distinguished from related concepts such as automotive safety and cybersecurity engineering?
2. Which central action fields can be identified for the development of resilient automotive systems, especially in the context of resilience-by-design?

The first research question is addressed in Chapters 2 and 3. The aim is to derive a standard-based definition of resilience that can be applied to connected and autonomous vehicles and serve as a basis for further research on resilience in the automotive context. The second research question is discussed in Chapter 4. In this section, the identified fields of action are explained, which can enable the consideration of resilience in the design phase of resilient automotive systems.

2. Concept of Resilience

In this section, the concept of resilience is explained and defined for automotive systems. First, the term and the broader context are defined. The resilience graph is then explained. Subsequently, the properties of resilient systems are presented. Finally, we introduce the terms resilience-by-design, resilience in operation, and resilience engineering in the automotive context.

2.1. Standard-based definition of Resilience in automotive context

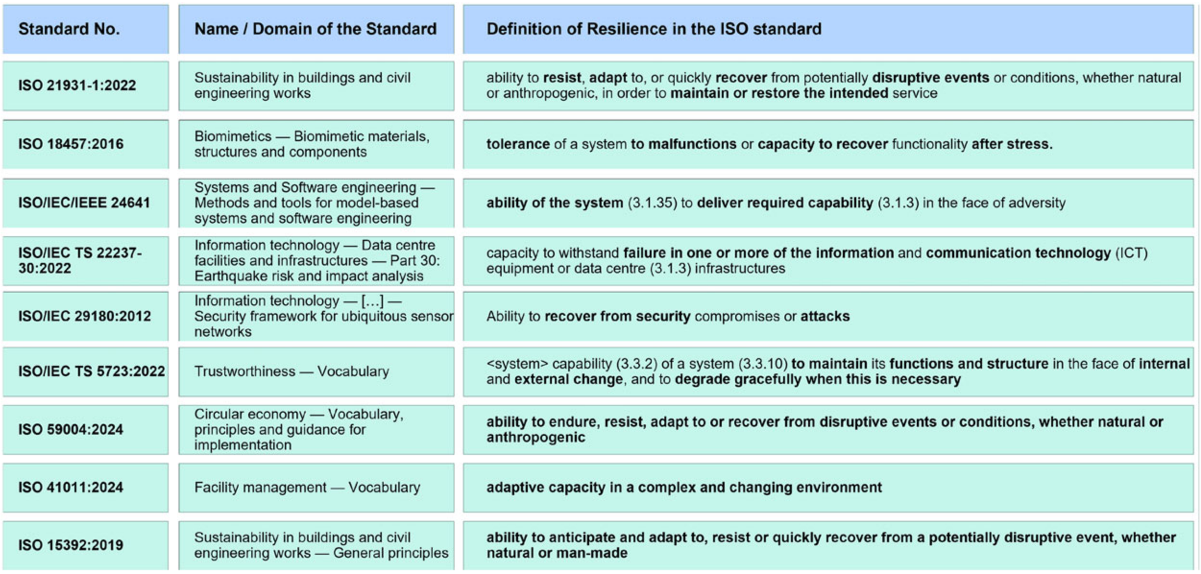
The concept of resilience is applied across many fields. In the automotive sector, however, it is often implicitly addressed within safety and cybersecurity engineering rather than treated as a distinct discipline. This paper aims to define resilience explicitly in the automotive context, separate from safety and cybersecurity. While safety and cybersecurity are well-supported by standards such as ISO 26262, ISO 21448, and ISO/SAE 21434, resilience lacks a dedicated framework, making a clear distinction essential. To establish a definition, various standard-based definitions of resilience were analyzed. Using the ISO Online Browsing Platform (OBP), 70 entries for “resilience” were identified, from which nine relevant definitions were selected, as illustrated in Figure 2. Key terms and concepts from these definitions were extracted and classified to ensure applicability to automotive systems. Several common aspects emerged: First, resistance — the system’s ability to withstand internal faults or external disruptions (ISO/IEC TS 5723:2022). Second, degradation — the system’s controlled transition to a limited operational state during a disruption. Third, recovery — the ability to restore functionality after degradation. Additionally, ISO/IEC 29180:2012 emphasizes resilience in the context of cybersecurity, highlighting potential cyber-attacks. ISO/IEC TS 22237-30:2022 addresses resilience regarding communication faults, and ISO 18457:2016 stresses tolerance to malfunctions and faulty information. From these aspects, the following definition is proposed:

> *“Resilience describes the ability of a system to maintain its intended functionality and availability despite unexpected disruptive events.”*

Disruptive events include cyber-attacks, environmental changes, internal failures, communication issues, and erroneous data. This clear definition enables resilience to be addressed independently within the automotive sector, supporting the development of specific methods and systematic approaches for resilient system design.

2.2. Resilience Graph

The resilience graph is commonly used alongside the concept of resilience to represent a system’s ability to withstand and recover from disruptions, as illustrated in Figure 3 (Cho et al., 2019; Madni and Jackson, 2009; Wang et al., 2024; Phillips et al., 2020). It visualizes system capacity or performance over time, providing insights into system availability and reliability. The graph is structured into four key phases: Detection, Degradation, Mitigation, and Recovery. Initially, the system operates at its baseline capability, defined during the design phase based on stakeholder requirements and system objectives. When a disruptive event occurs—such as a cyber-attack—the system should detect it promptly. The time between the event’s occurrence and its detection is referred to as detection time. Detection triggers the degradation phase, marked by a decline in system capability. The robustness of the system is reflected here: robust systems experience minimal performance loss and can sustain essential functionality despite disruptions. Following degradation, the mitigation phase begins. Here, the system implements measures to contain and reduce the impact of the disruption. The time taken to execute these measures is known as mitigation time. The purpose is to halt further performance decline and prepare for recovery. In the recovery phase, the system seeks to restore its original capability. Three recovery outcomes are possible: the system may not regain its initial capability, may fully restore to its pre-disruption state, or may even enhance its capability—e.g., through learning mechanisms that improve future responses. How can the resilience graph be leveraged as a quantitative framework to benchmark and compare resilience across different automotive architectures and scenarios?



Standard No.	Name / Domain of the Standard	Definition of Resilience in the ISO standard
ISO 21931-1:2022	Sustainability in buildings and civil engineering works	ability to **resist**, **adapt** to, or quickly **recover** from potentially **disruptive events** or conditions, whether natural or anthropogenic, in order to **maintain or restore the intended** service
ISO 18457:2016	Biomimetics — Biomimetic materials, structures and components	**tolerance** of a system **to malfunctions** or **capacity to recover** functionality **after stress.**
ISO/IEC/IEEE 24641	Systems and Software engineering — Methods and tools for model-based systems and software engineering	**ability of the system** (3.1.35) to **deliver required capability** (3.1.3) in the face of adversity
ISO/IEC TS 22237-30:2022	Information technology — Data centre facilities and infrastructures — Part 30: Earthquake risk and impact analysis	capacity to withstand **failure in one or more of the information** and **communication technology** (ICT) equipment or data centre (3.1.3) infrastructures
ISO/IEC 29180:2012	Information technology — [...] — Security framework for ubiquitous sensor networks	Ability to **recover from security** compromises or **attacks**
ISO/IEC TS 5723:2022	Trustworthiness — Vocabulary	<system> capability (3.3.2) of a system (3.3.10) **to maintain** its **functions and structure** in the face of **internal** and **external change**, and to **degrade gracefully when this is necessary**
ISO 59004:2024	Circular economy — Vocabulary, principles and guidance for implementation	**ability to endure, resist, adapt to or recover from disruptive events or conditions, whether natural or anthropogenic**
ISO 41011:2024	Facility management — Vocabulary	**adaptive capacity in a complex and changing environment**
ISO 15392:2019	Sustainability in buildings and civil engineering works — General principles	**ability to anticipate and adapt to, resist or quickly recover from a potentially disruptive event, whether natural or man-made**

Figure 2. Different definition of resilience

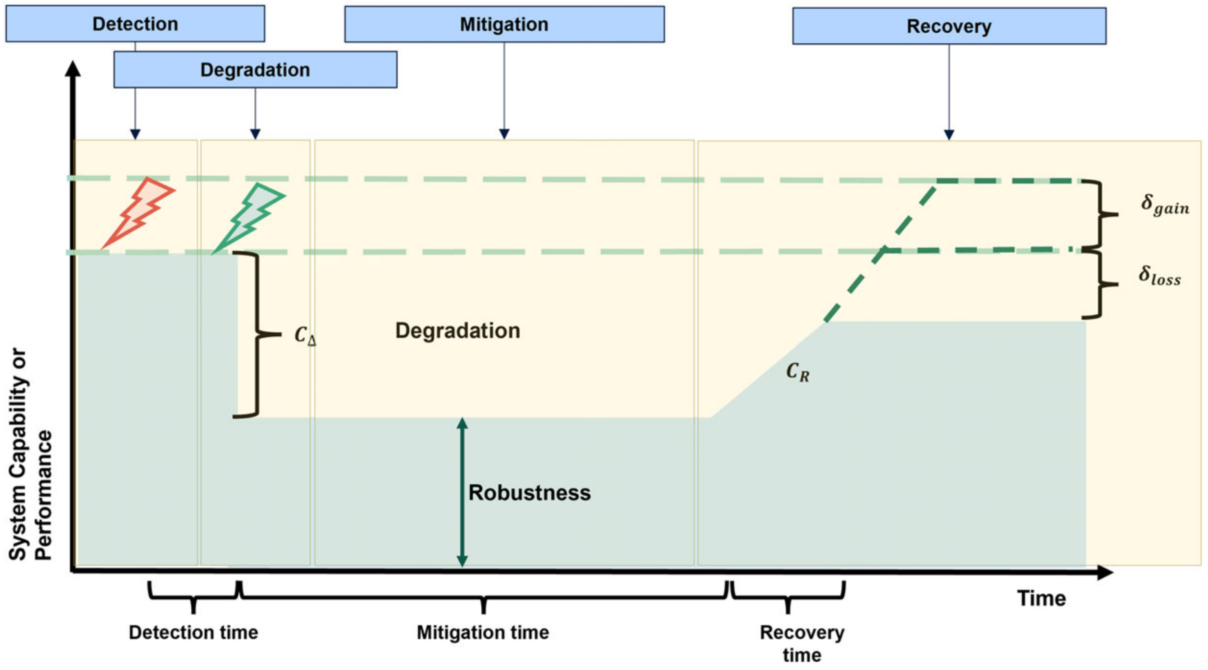


Figure 3. Resilience Graph

2.3. Resilience properties of an automotive system

Based on the definition of resilience and the resilience graph, the following properties can be determined: disruption tolerance, detection, adaptability, and recoverability. Since not all scenarios and situations can be tested during the testing phase of the system, additional disruptions may occur during the operational phase. Therefore, a resilient system must be disruption-tolerant. Disruption tolerance complements classical fault tolerance properties, considering a broader spectrum that goes beyond ordinary errors. While fault tolerance usually aims at specific, previously identified errors, disruption tolerance is designed for more comprehensive scenarios that are not fully predictable. Detection is the property of a resilient system to identify disruptions early on. Another property of a resilient system is adaptability, which enables the system to dynamically respond to disruptions by executing appropriate degradation and mitigation measures. Recoverability is the most important property of resilient systems, allowing the system to return to its normal state quickly and effectively after a disruption. It can be concluded that a resilient system is characterized by its ability to tolerate disruptions, detect them early, respond flexibly with suitable measures, and recover quickly.

2.4. Resilience-by-Design, Resilience in Operation and Resilience Engineering

This section explains the concepts of Resilience-By-Design, Resilience in Operation, and Resilience Engineering. With so-called X-By-Design, different aspects (X) can be systematically considered and integrated already in the systems design phase, such as through Safety-by-Design or Security-by-Design (Molina et al., 2017; Madni and Jackson, 2009). Khaloopour et al. (2024) has conducted an extensive systematic literature analysis on the topic of resilience with a focus on 6G networks. Based on this, we can generalize and state that Resilience-By-Design describes the systematic integration of resilience properties already in the early phase. The aim is to ensure that systems can cope with disruptions in operation. The focus is on system analysis, such as identifying potential sources of disruption and vulnerabilities, conducting impact analyses, and implementing and integrating appropriate mechanisms during the systems design phase. Resilience in Operation, or operational resilience, refers to the phase of system operation after development. Essuman et al. (2020) deals with operational resilience on the basis of a conceptual and empirical analysis. Phillips et al. (2020), on the other hand, establishes metrics for measuring operational resilience for critical infrastructure. From these contributions, it can be concluded that Resilience in Operation applies these mechanisms during system operation to maintain availability and reliability under changing conditions, using continuous monitoring to detect and respond to disruptions. Resilience Engineering is the application of a systematic and quantifiable approach to the development and maintenance of systems to ensure resilience in operation. It ensures that resilience requirements are considered throughout the entire lifecycle, from requirements analysis to maintenance. Resilience Engineering considers the entire system lifecycle and combines the concepts of Resilience-By-Design and Resilience in Operation.

3. Differentiation of resilience engineering from safety engineering and cybersecurity engineering in automotive

In this chapter, safety and cybersecurity engineering are distinguished from resilience engineering in the automotive sector to provide a better initial understanding of the scope and importance of the field.

3.1. Automotive Systems Engineering

Systems engineering is an interdisciplinary approach to the development of complex systems (Walden et al., 2015). In the automotive sector, this is referred to as Automotive Systems Engineering (ASE). It focuses on the development and optimisation of the whole vehicle and its internal systems, components, and functions. ASE integrates different disciplines such as mechatronics, driving dynamics, functional safety, and cybersecurity in order to meet the requirements of the stakeholders. ASE follows a systematic approach, illustrated in Figure 4, often based on the V-model (VDI 2206, 2004; Winner et al., 2018).

3.2. Automotive Safety Engineering

Automotive safety engineering is primarily covered by two main standards: functional safety with ISO 26262 and safety of the intended functionality with ISO 21448. ISO 26262 focuses on protecting road users from failures in electrical and electronic components, requiring Hazard Analysis and Risk Assessment (HARA) during design to address component malfunctions. ISO 21448 extends this

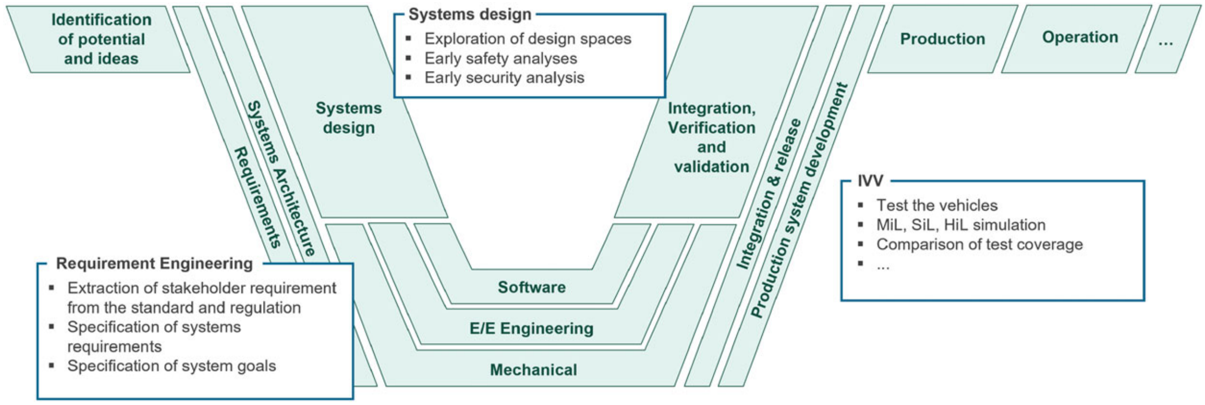

Identification of potential and ideas
Systems design
Exploration of design spaces
Early safety analyses
Early security analysis
Production
Operation
...
Systems Architecture
Requirements
Systems design
Integration, Verification and validation
Integration & release
Production system development
IVV
Test the vehicles
MiL, SiL, HiL simulation
Comparison of test coverage
...
Requirement Engineering
Extraction of stakeholder requirement from the standard and regulation
Specification of systems requirements
Specification of system goals
Software
E/E Engineering
Mechanical

Figure 4. Automotive Systems Engineering based on VDI 2206 (2004); Winner et al. (2018); Tekaat et al. (2019); Kharatyan et al. (2022)

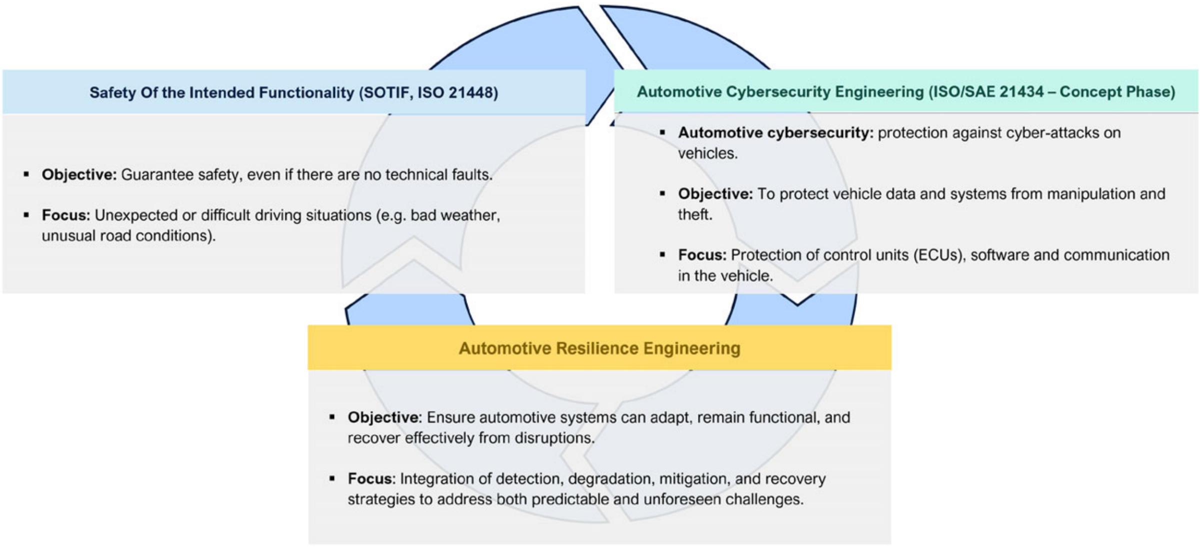
approach and considers behaviour that can occur without direct system failure. ISO 21448 examines possible system behaviour that can occur even in unknown scenarios. Such scenarios arise, for example, when the system enters an unsafe state while still performing its intended function (ISO 21448, 2022). In the case of the Tesla accident, the system failed to recognize a crossing tractor-trailer because the radar sensors were looking through the trailer and the camera did not interpret the white surface of the trailer as an obstacle. The system was unable to recognize the limits of its functionality, making the accident unavoidable (Schnieder and Hosse, 2020).

3.3. Automotive Cybersecurity Engineering

Automotive cybersecurity engineering is addressed in ISO/SAE 21434. The standard specifies engineering requirements for cybersecurity risk management that focus exclusively on the ego-vehicle and internal vehicle components. External systems, such as backend servers or cloud services, are not comprehensively considered (ISO/SAE 21434, 2021). Charlie Miller and Chris Valasek demonstrated how a vulnerability in a vehicle's infotainment system could be exploited to remotely control critical driving functions such as braking and steering (Valasek and Miller, 2015). This attack impressively showed that connected vehicles without adequate cybersecurity measures are exposed to significant risks that not only compromise the system's functionality but also threaten the safety of occupants and other road users.

3.4. Automotive Resilience Engineering

While safety and cybersecurity engineering have established standards and approaches, there is currently no specific standard for resilience engineering in the automotive sector. Resilience engineering, however, builds on the results of HARA and TARA but goes beyond the defence and prevention of hazards and threats. Resilience engineering focuses on the ability of a system to adapt to disruptions, remain functional, and recover after a disruption (Rosenstatter et al., 2020). A resilient system combines strategies for detection, degradation, mitigation, and recovery. This perspective enables the system to respond to both known and combined or unforeseen disruptions. In the case of the Tesla accident, the system should have been able to recognize the changing operating conditions or operating range and take appropriate action. In the Jeep hack example, the system should have been able to detect the disruption caused by the attack, isolate the infotainment system until the security vulnerability is closed or the attack is mitigated, and then reactivate the infotainment system (Valasek and Miller, 2015). These are possible actions that a resilient system could take. These optimal actions should be defined as part of the resilience assurance process. Figure 5 shows the difference between cybersecurity, safety, and resilience in the automotive industry. The focus of each discipline is highlighted here.



Safety Of the Intended Functionality (SOTIF, ISO 21448)

- Objective: Guarantee safety, even if there are no technical faults.
- Focus: Unexpected or difficult driving situations (e.g. bad weather, unusual road conditions).

Automotive Cybersecurity Engineering (ISO/SAE 21434 – Concept Phase)

- Automotive cybersecurity: protection against cyber-attacks on vehicles.
- Objective: To protect vehicle data and systems from manipulation and theft.
- Focus: Protection of control units (ECUs), software and communication in the vehicle.

Automotive Resilience Engineering

- Objective: Ensure automotive systems can adapt, remain functional, and recover effectively from disruptions.
- Focus: Integration of detection, degradation, mitigation, and recovery strategies to address both predictable and unforeseen challenges.

Figure 5. Differentiation of resilience engineering from safety engineering (SOTIF) and cybersecurity engineering in automotive

3.5. Integration of resilience engineering in the development process

Integrating resilience engineering into the development process requires that it be considered in the early stages of systems engineering, as illustrated in Figure 6. The system architecture serves as the input for domain-specific analyses. Following HARA and TARA, the respective domain-specific safety and cybersecurity concepts are developed. The domain-specific system goals, scenarios, and measures must be linked to the components and functions of the system architecture (Kharatyan et al., 2022). These results can then be extended to identify and analyse disruptions and to add further resilience mechanisms. For example, adaptive strategies can be implemented that allow a vehicle to respond flexibly to failures of individual sensors or components before a damage scenario or threat scenario occurs. At the same time, decisions must be documented in the form of comprehensive assurance concepts to demonstrate the resilience of a system. Resilience engineering thus extends the established approaches of safety and cybersecurity engineering by prioritising comprehensive robustness to ensure the reliability, availability, and robustness of connected automated vehicles even in complex and unpredictable scenarios. To achieve this, some research questions remain open: How can the integration of resilience engineering create a comprehensive framework for dealing with disruptions? What tools and methodologies are needed to effectively integrate resilience engineering into model-based systems engineering processes for autonomous vehicles?

4. Assurance Concept in Automotive

To obtain vehicle approval, automobile manufacturers must comply with certain regulations. These regulations can be either regional, such as the AFGBV in Germany, or international, such as UNECE R155. Germany's type approval, for example, specifies the conditions under which autonomous vehicles can be approved and operated on public roads. To obtain approval for a new vehicle in Germany, the following documents must be submitted with the application: (1) a functional description of the vehicle with autonomous driving functions, (2) a safety concept for functional safety, (3) a cybersecurity concept for information technology, and (4) evidence that environmental conditions, which may occur in the specified operating range of the vehicle but cannot be represented in tests, can be safely controlled (Kraftfahrt-Bundesamt, 2022). Using model-based systems engineering (MBSE), systems can be described in detail from different perspectives of architecture and behaviour. This description is necessary for creating the required evidence. ISO 26262 contributes to the development of the safety concept for functional safety based on a HARA. On the other hand, ISO/SAE 21434 provides guidelines for developing the cybersecurity concept for information technology through a TARA. In the context of SOTIF, the aim is to identify and address increasingly uncertain and unknown risks. However, some risks remain uncertain and unknown. For approval, it must still be demonstrated that the autonomous vehicle can also operate safely in non-demonstrable tests within the specified operating range. SOTIF helps to identify unknown scenarios, so that the proportion of unknown scenarios becomes smaller. However, this cannot cover the entire spectrum. For this purpose, a resilience concept has to be investigated and

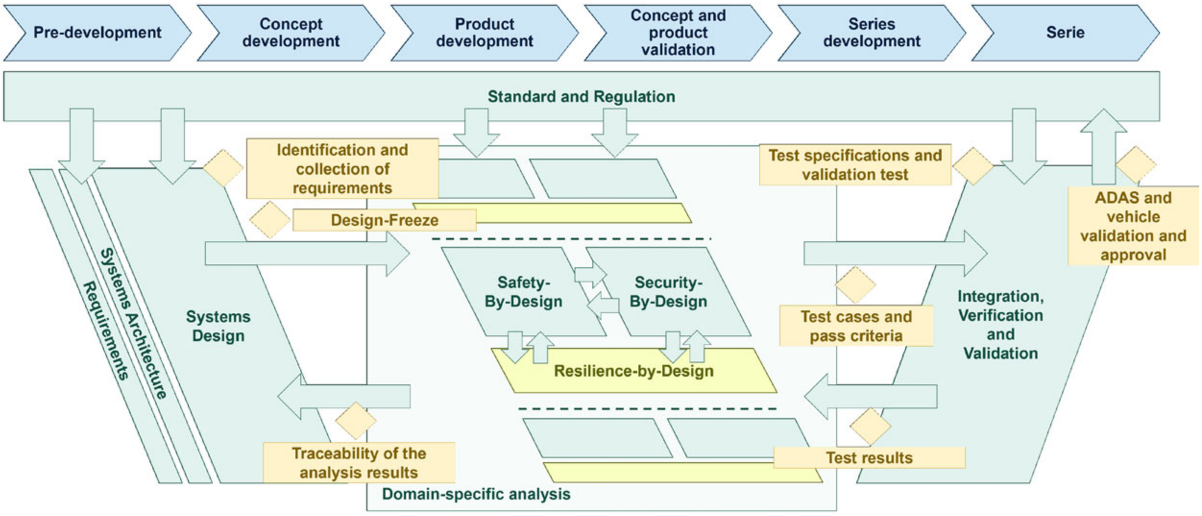

Pre-development
Concept development
Product development
Concept and product validation
Series development
Serie
Standard and Regulation
Identification and collection of requirements
Design-Freeze
Test specifications and validation test
ADAS and vehicle validation and approval
Requirements
Systems Architecture
Systems Design
Safety-By-Design
Security-By-Design
Resilience-by-Design
Test cases and pass criteria
Integration, Verification and Validation
Traceability of the analysis results
Test results
Domain-specific analysis

Figure 6. Integration of Resilience-by-Design in the development Process based on Tekaat et al. (2019); Kharatyan et al. (2022)

developed. Figure 7 shows the general steps of the assurance process. This is divided into four essential steps: (1) identification, (2) risk assessment, (3) concept, and (4) implementation. HARA for safety and TARA for security also follow this scheme. For resilience, however, the approach needs to be clearly defined, and the content of the resilience concept needs to be established. How can resilience assurance processes be developed to provide verifiable evidence of system resilience across the lifecycle of connected and autonomous vehicles?

5. Action Fields for Resilience-By-Design

The development of resilient systems is essential for the future of autonomous vehicles, enabling them to make independent decisions in various traffic situations. Systems engineering provides an interdisciplinary approach to developing complex systems in general. A systematic approach is required to embed resilience into the standard development process. An overview of the action fields for integrating resilience-by-design into development is illustrated in Figure 7. It should be noted that the action fields are a hypothesis, based on the observation that there are currently no specific norms or standards addressing resilience in the automotive domain. They are intended as a practical suggestion to fill this gap and give systems engineers guidance on how resilience can be considered in the systems design phase. The **first action field** deals with norm conformity and the development of a holistic systematic approach for designing resilient systems. The goal is to embed resilience systematically into automotive systems and explore interfaces with disciplines like automotive cybersecurity and safety. Action Field 1 ensures that resilience properties are systematically integrated into the development process and that established standards and regulations in the automotive sector are taken into account. The **second action field** focuses on domain-specific analysis regarding resilience. Here, the emphasis is on the early methodological identification of disruptions and their potential impact on other functions, systems, or components. Based on this, a risk assessment can be conducted. It requires new methods to assess risks and to extend the results from HARA and TARA for resilience purposes. The **third action field** addresses the development of a resilience concept, analogous to the safety and security concepts. The resilience concept defines goals, strategies, requirements, and measures to manage disruptions, focusing on traceability to system architecture elements and the results from safety and security analyses. The second part of the third action field addresses the measures of the resilience concept that need to be implemented in the system architecture. Before implementation, decisions for the overall system must be made. Trade-off analyses and evaluation methods must be developed to assess resilience within the created architecture. In the **fourth action field**, tools must be provided to enable the development of resilient systems. These could include model-based methods, modeling language development, or AI-augmented methods and tools. How can resilience-by-design principles be formalized and incorporated into a unified framework for automotive systems design?

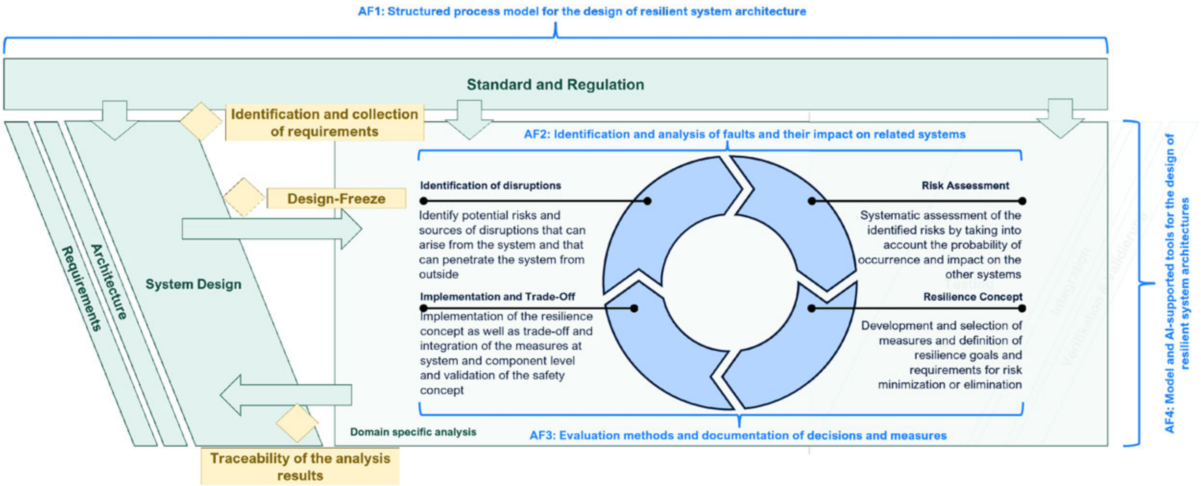

AF1: Structured process model for the design of resilient system architecture
Standard and Regulation
Identification and collection of requirements
Design-Freeze
Requirements
Architecture
System Design
AF2: Identification and analysis of faults and their impact on related systems
Identification of disruptions
Identify potential risks and sources of disruptions that can arise from the system and that can penetrate the system from outside
Risk Assessment
Systematic assessment of the identified risks by taking into account the probability of occurrence and impact on the other systems
Implementation and Trade-Off
Implementation of the resilience concept as well as trade-off and integration of the measures at system and component level and validation of the safety concept
Resilience Concept
Development and selection of measures and definition of resilience goals and requirements for risk minimization or elimination
Domain specific analysis
AF3: Evaluation methods and documentation of decisions and measures
Traceability of the analysis results
AF4: Model and AI-supported tools for the design of resilient system architectures

Figure 7. Action fields for developing a framework for resilient systems design

6. Conclusions and Outlook

This paper present resilience in the automotive sector, highlighting its importance for connected autonomous vehicles. Resilience enables systems to maintain or restore functionality despite disruptions and complements safety (ISO 26262, ISO 21448) and cybersecurity (ISO/SAE 21434) engineering by addressing broader challenges. It emphasizes systems' ability to adapt, mitigate, and recover from disruptions, representing a higher-level perspective built on safety and cybersecurity foundations. The identified action fields provide a framework for systematically embedding resilience in automotive systems design. These fields address research gaps in resilience-by-design, which will grow in importance as vehicles become increasingly connected and autonomous. This development brings new opportunities but also more complex risks that cannot be fully addressed by classical safety and cybersecurity approaches. Developing standards for resilience engineering is essential to harmonize methods and integrate resilience-by-design into existing processes. Advanced model-based engineering methods and tools are key to designing resilient systems and creating a resilience concept. Further research should focus on mechanisms like self-healing, reconfiguration, and adaptive architectures to strengthen resilience at system and component levels. We will focus on addressing these fields step by step with practical methods and tools, making resilience engineering an integral part of automotive development processes. As part of future work, we will evaluate the practicability and conduct a deeper analysis of the proposed approach. This paper defines only the initial direction and conceptual considerations. A detailed case study and empirical validation will follow in subsequent phases. Additionally, since engineering fields like critical infrastructure resilience have already been examined, it is worth analyzing whether concepts from that field can be transferred to the automotive domain. This requires an in-depth comparative analysis, which will also be part of the continued research.

Acknowledgments

This research was funded by the German Federal Ministry of Education and Research (BMBF) in the project ConnRAD, grant number 16KISR029K. The contents of this publication are the sole responsibility of the authors.

References

Bach, Johannes, Otten, Stefan and Sax, Eric (2017). A Taxonomy and Systematic Approach for Automotive System Architectures - From Functional Chains to Functional Networks. In *Proceedings of the 3rd International Conference on Vehicle Technology and Intelligent Transport Systems* (pp. 90–101). SCITEPRESS - Science and Technology Publications.

Buchholz, Katharina (2024). Autonomous Driving: Cars Increasingly Ready for Autonomous Driving. Available at: https://www.statista.com/chart/25754/newly-registered-cars-by-autonomous-driving-level/.

Cho, Jin-Hee, Xu, Shouhuai, Hurley, Patrick M., Mackay, Matthew, Benjamin, Trevor and Beaumont, Mark (2019). STRAM. *ACM Computing Surveys*, 51 (6), 1–47.

Essuman, Dominic, Boso, Nathaniel and Annan, Jonathan (2020). Operational resilience, disruption, and efficiency: Conceptual and empirical analyses. *International journal of production economics*, 229, 107762.

Fayyazi, Saeed, Azad-Farsani, Ehsan and Haghighi, Ali Asghar (2024). Resilience-oriented sectionalizing and tie switches sitting in distribution networks with complex topologies. *Reliability Engineering & System Safety*, 243, 109919.

IEEE (2020). 2020 IEEE Secure Development (SecDev).

International Organization for Standardization (2022). Road vehicles - Safety of the intended functionality (ISO 21448). Available at: https://www.iso.org/standard/77490.html.

International Organization for Standardization (2021). Road vehicles - Cybersecurity Engineering (ISO/SAE 21434). ISO. Available at: https://www.iso.org/standard/70918.html.

Khaloopour, Ladan, Su, Yanpeng, Raskob, Florian, Meuser, Tobias, Bless, Roland, Janzen, Leon, Abedi, Kamyar, Andjelkovic, Marko, Chaari, Hekma, Chakraborty, Pousali, Kreutzer, Michael, Hollick, Matthias, Strufe, Thorsten, Franchi, Norman and Jamali, Vahid (2024). Resilience-by-Design in 6G Networks: Literature Review and Novel Enabling Concepts. *IEEE Access*, 12, 155666–155695.

Kharatyan, Aschot, Günther, Matthias, Anacker, Harald, Japs, Sergej and Dumitrescu, Roman (2022). Security-and Safety-Driven Functional Architecture Development Exemplified by Automotive Systems Engineering. *Procedia CIRP*, 109, 586–591.

Kraftfahrt-Bundesamt (2022). National type approval for motor vehicles with a fully automated driving function. Available at: https://dserver.bundestag.de/brd/2022/0086-22.pdf.

Madni, A. M. and Jackson, S. (2009). Towards a Conceptual Framework for Resilience Engineering. *IEEE Systems Journal*, 3 (2), 181–191.

Molina, Caroline Bianca Santos Tancredi, de Almeida, Jorge Rady, Vismari, Lucio F., Gonzalez, Rodrigo Ignacio R., Naufal, Jamil K. and Camargo, Joao Batista (2017). Assuring Fully Autonomous Vehicles Safety by Design: The Autonomous Vehicle Control (AVC) Module Strategy. In *2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)*, 16–21. IEEE.

Phillips, Tyler, McJunkin, Timothy, Rieger, Craig, Gardner, John and Mehrpouyan, Hoda (2020). An Operational Resilience Metric for Modern Power Distribution Systems. In *2020 IEEE 20th International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, 334–342. IEEE.

Rosenstatter, Thomas, Strandberg, Kim, Jolak, Rodi, Scandariato, Riccardo and Olovsson, Tomas (2020). REMIND: A Framework for the Resilient Design of Automotive Systems. In *2020 IEEE Secure Development (SecDev)* (pp. 81–95). IEEE.

Rutter, Michael (2006). Implications of resilience concepts for scientific understanding. *Annals of the New York Academy of Sciences*, 1094, 1–12.

SAE Standard (2021). Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles. Available at: https://www.sae.org/standards/content/j3016_202104/.

SCITEPRESS - Science and Technology Publications (2017). *Proceedings of the 3rd International Conference on Vehicle Technology and Intelligent Transport Systems*.

Schnieder, Lars and Hosse, René Sebastian (2020). Leitfaden safety of the intended functionality: Verfeinerung der Sicherheit der Sollfunktion auf dem Weg zum autonomen Fahren. Springer Vieweg.

Tekaat, Julian, Kharatyan, Aschot, Anacker, Harald and Dumitrescu, Roman (2019). Potentials for the Integration of Design Thinking along Automotive Systems Engineering Focusing Security and Safety. *Proceedings of the Design Society: International Conference on Engineering Design*, 1 (1), 2883–2892.

Verein Deutscher Ingenieure (2004). Design methodology for mechatronic systems (VDI 2206). *VDI-Richtlinie 2206, VDI-Verlag*, Düsseldorf, Germany.

Valasek, Chris and Miller, Charlie (2015). Remote Exploitation of an Unaltered Passenger Vehicle. Available at: https://ioactive.com/pdfs/IOActive_Remote_Car_Hacking.pdf.

Walden, David D., Roedler, Garry J., Forsberg, Kevin, Hamelin, R. Douglas and Shortell, Thomas M. (2015). Systems engineering handbook: A guide for system life cycle processes and activities. Wiley.

Wang, Feng, Tian, Jin, Shi, Chenli, Ling, Jiamu, Chen, Zian and Xu, Zhengguo (2024). A multi-stage quantitative resilience analysis and optimization framework considering dynamic decisions for urban infrastructure systems. *Reliability Engineering & System Safety*, 243, 109851.

Winner, Hermann, Prokop, Günther and Maurer, Markus (2018). Automotive systems engineering II. Springer.