Deep Science Publishing
https://doi.org/10.70593/978-93-49307-21-6_11

DeepScience
Open Access Books

Chapter 11: Addressing cybersecurity, data governance, and ethical concerns in automotive digital transformation

11.1. Introduction

The automotive industry is undergoing a profound transformation due to advancing digitalisation and new mobility models alongside the changing expectations of vehicle users. Automotive OEMs are increasingly adopting new digital technologies, including over-the-air software updates, embedded electronics, connected vehicles, and mobility services to implement the above digitalisation technologies. This transformation is expected to create significant new opportunities and threats. It is projected that by 2030, the vehicle park in Europe and the USA will slightly decline from 2020 levels, but the global automotive industry profit pool will significantly grow. The total profit pool is expected to rise from 307 billion US Dollars in 2020 to 650 billion US Dollars in 2030. The main driver behind this profit growth is the transition from individual car ownership to car sharing, ride pooling, and similar services. By 2025, around 20 million new cars shipped globally every year will be based on a completely different vehicle architecture allowing to build a broad variety of car types on it, in order to improve efficiency and lower costs. Furthermore, by 2025, all new cars worldwide will be shipped connected. Cars will no longer be isolated electronic devices but will be vehicles in a new mobility ecosystem. In this scenario, the V2X (Vehicle-to-X) paradigm will be a crucial enabler. Vehicles will be able to communicate among each other, with the infrastructure, and with pedestrians, allowing a more efficient and safer travel experience. This will allow the smart city application: optimising traffic management, in order to improve traffic flow and avoid critical congestion. Recently, there is a growing expectation that the automotive industry would have a breakthrough in autonomous driving applications with Level 5 automation. Current Advanced Driver Assistance Systems (ADASs) are being expanded by adding more sensors and more complex algorithms to achieve fully

autonomous (driverless) cars. Unfortunately, they remain largely unreliable and dangerously flawed for wider income. In the last decade, the electronic complexity of current top-end vehicles has dramatically increased to about 200 million lines of code and up to 200 Electronic Control Units (ECUs) used to control them, allowing for a seamless experience to users, bringing more comfort items, helping customer mobility experience, and improving energy efficiency. As a consequence, vehicles are becoming complex software-based IT systems. The increasing software complexity, as on other critical infrastructures, raises concerns on the safety and security associated with its development and deployment. Major automotive OEMs converging with IT companies are racing to develop new advancing vehicle applications relying on ever changing and potentially unreliable components and platforms. These new applications tend to open the automotive delivery chain to third parties, including component vendors and service providers with unprecedented concerns about maintaining the appropriate quality assurance and protection. In this context, as safety is paramount to automotive production, the 2019 decision by the United Nations Economic Commission for Europe (UN/ECE) to provide for the creation of a cyber security regulation has raised a world-wide debate on how to guarantee the cyber security assurance of new vehicles and the safety of advanced vehicle applications still necessarily relying on the exchange and sharing of third-party data.

Fig 11.1: The Ethics of Digital Transformation

11.1.1. Background and Significance

People are increasingly opting for mobility services instead of car ownership. The transition in developed countries has just begun but is set to accelerate rapidly. Market players will have to realign their strategies along the new automotive value chain, which is expected to change significantly over the next five years. New players with unequaled competences will enter the market. All mobility service providers will have to contend

with new entrants and drivers, as well as the moves made by traditional players. One important aspect is the aspect of ride-sharing. Instead of owning and operating their own vehicles, new alternatives are emerging based on sharing mobility services and vehicle usage. These offerings will reduce the volume of car ownership and, potentially, car sales per provider, although the future disruption is uncertain. In many industries, scale, consumer preference aggregation, and bundling are shifting power into the hands of a few firms, creating oligopolies.

The analysis proceeds as follows: First, the impact of ride-sharing on the business model of traditional players is assessed. To specify the opportunities and risks for an OEM, separate ridesharing impacts on vehicle manufacturers, suppliers, and the market for pre-owned vehicles are considered. Further consequences, such as newly emerging market positions, the emerging hierarchy of the reshaped automotive ecosystem, and policy responses, are also introduced. Impact variation across regions considering structural must-have properties is outlined in a way that informs and supports an OEM's decision-making processes. Finally, by posing two questions relating to missing research approaches in the literature, the relevance of a systems-architecture approach is sketched. Economies of scale have the potential to create a threat, a shift in power through consolidation in supply markets is more likely but cannot be reliably inferred, and the vehicle ownership question has to be freshly posed and addressed.

11.2. Overview of Automotive Digital Transformation

The automotive industry is experiencing a transformation that was unthinkable just a few years ago. Each of today's movies featuring automated cars are based on technologies that automotive manufacturers are developing and that could be operational in a few years. Cars are rapidly turning into complex cyber-physical systems fulfilling an ever-increasing demand for a plethora of services related to safety and entertainment, meaning a dramatic transformation of engines continues with the dissolution of the distinct boundaries that historically separated the different components of the vehicles. Within this transformation, the role of automotive manufacturers in the automotive stack is changing too. Industry manufacturers developed three main components on which they built their models: transportation systems composed of vehicles; infrastructure to allow the vehicle to safely operate; sustainable business models based on the ownership of the first two. Then, the traditional "safety first" approach and the corresponding meticulously designed processes have led to providing extremely safe cars. New players —depending on interactions of a unique kind— changed the rules of the game forcing automotive manufacturers to go back to square one in less than 6 years, possibly forever; so far, they could focus on the vehicle's design leaving business models to evolve on their historical own, likely, with SDPs could give up ownership altogether.

Vehicles will be digitally orchestrated in a manner similar to smartphones, exposing manufacturers' models to new rounds of congruences and divergences. Another wave of similar pressures will arise from the oncoming advent of connected vehicles, unleashing new cybersecurity issues that could be possibly a bitter pills to swallow by some in the automotive industry, which could be faced with the sudden attendance of national/international hackers with an unimaginable level of professionalism or groups of disappearing hooded men, leaving behind broken and “unbreakable” bricks. Most importantly, and similar to smartphones and despite the lighthouses on the way, such a rapid transformation in businesses, ecosystems, sociocultural norms, etc. defines a big deal of uncertainty that is common to all industries, likely.

This chapter focuses on the automotive context. The automotive industry has relatively lagged behind other major sectors in the application of software-based advancements. A growing variety of automotive digital technologies - including vehicle connectivity, electrification, driver assistance systems (ADAS), and autonomous driving - are driving digital transformation across the automotive industry. However, digital transformation is inherently linked with an increasing dependency on software, connectivity, and data analysis. As a consequence, intact data governance, cybersecurity, and ethical issues are becoming increasingly important. What is needed is to develop frameworks for understanding the industry’s current state-of-the-art technologies and for identifying the management implications concerning the business model, data governance, cybersecurity, and ethical concerns.

11.2.1. Research design

While some qualitative research methods exist, they only cover certain aspects of the IoT ecosystem but have limitations themselves. Other researchers have proposed relevant conceptual cooperation frameworks but failed to empirically validate them. Therefore, there is little practical knowledge of growing explicit cooperation, including the complexities and challenges. Thus, grounded theory and its variation of strengths and challenges are useful as a research method as it excels in the exploratory study of emerging areas in this field. This method can be employed as a one-case study.

To identify, document, and explain the current state of actionable knowledge on cooperative result-oriented solutions and their implementation addressing legitimate privacy and ethical concerns regarding the IoT-based innovations, using and interviewing the stakeholders’ representatives in a European automotive consortium that is developing an IoT-based platform for improving the road safety of vehicle travel. The implementation would include the ecosystem setup, cooperation entities and roles, product frames, and result types, and would also address the complexities and challenges of their implementation. Thus, it would contribute with trustworthy cooperation,

technical solutions, and operationalized governance concepts for coining cooperation, advancing automobile cybersecurity readiness and awareness, and increasing passenger trust toward connected vehicles.

The chosen qualitative research design is kicked off by defining the design proposition, key concepts, the application context, and a number of targeted stakeholders for selection, recruitment, and interviewing. To facilitate a critical and elaborated expert process on the methods to be applied for this exploratory study, a pre-study plan is designed including generation of questions sets for a kick-off agenda to discuss the steps and a tips list to facilitate a systematized analysis of the recorded interviews. The data collection would start by interviewing individuals and later providing a cohort structured interview for the first round evaluations. A machine-readable open-ended questionnaire is proposed for interviews to obtain descriptive data on the implementation steps.

11.3. The Role of Cybersecurity in Automotive Systems

Automobile manufacturers need to rethink their product and service approach. Simply designing, manufacturing, and distributing vehicles is no longer sufficient. In the automotive sector, there is a need for stricter safety, security, and environmental and ethical requirements. The automotive industry is facing significant changes driven by emerging technologies, with the rapid development of new electric vehicles (EVs), autonomous cars, car-to-X (cX) communication, automotive cyber-physical systems (CPS), vehicle cloud computing, big data, the Internet of Things (IoT), and AI. These new vehicles will adopt several connected cooperative applications such as safety, automated driving (AD), and over-the-air (OTA) software updates for the improvement of user experience and safety. However, cybersecurity attacks on automotive systems are one of the most significant and concerning aspects that need to be addressed.

Like other industries, automotive cybersecurity is a challenge with growing sophistication against user privacy and data protection. Evolving smart-CPS constitutes the next generation of automotive systems and services. Thus, new cybersecurity controls are warranted to guarantee the resilience of smart-CPS to misuse. For the vehicular domain, with its critical implications for safety and privacy, there is an urgent need for automotive system design frameworks and assessment methodologies for accountability and finance compliance. As a promising solution, cybersecurity by design raises the need for prior evaluation of the vulnerability of system architecture and design. The aim is to disentangle CPS hierarchies and demonstrate how a transdisciplinary systems engineering model allows addressing vehicle cybersecurity risk and compliance at the architecture level. Finally, a recent case study is exploited to show the effectiveness of this approach in a real industry context.

Over the past few years, software attacks on vehicles have been doubling every year, affecting over 300 million vehicles worldwide. Vehicle connectivity increases manufacturers' targets for hackers and cybercriminals targeting sensitive information and critical systems. Recently, state of the art updates have been employed by several vehicle manufacturers, which enhance the security and capabilities of the vehicle post-deployment. Taking Over-The-Air updates to the next level, cybersecurity firmware update SOTA aims at improving the vehicle's resistance to discovered cybersecurity vulnerabilities. Post-deployment vehicle firmware updates are crucial for manufacturing devices and platforms deployed remotely and continuously. The automotive industry has been slowing in adopting firmware over-the-air update systems compared to industries dealing with online-connected IoT devices. Yet, it still poses one of the biggest cyberattack surfaces with potentially life-threatening implications.

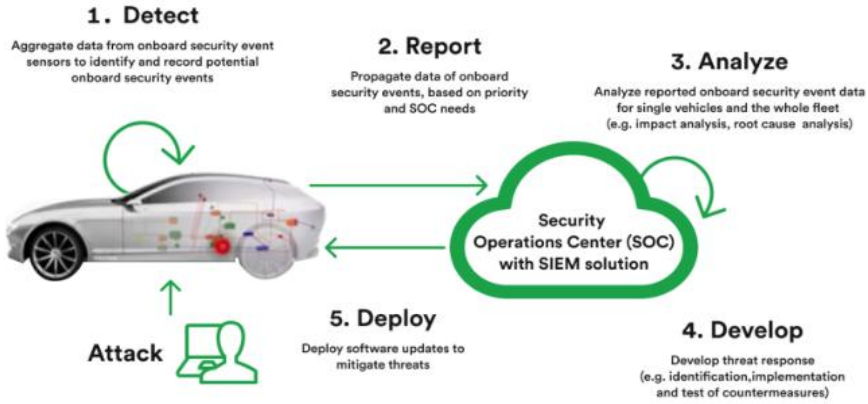

Fig 11.2: Cybersecurity in Automotive

11.3.1. Threat Landscape Analysis

The automotive industry is undergoing a digital transformation to improve performance, create revenues and increase competitive advantage. This transformation entails several challenges in cybersecurity, data governance and ethical issues. The challenges require a multi-dimensional analysis of the threat landscape for the whole automotive ecosystem. Vehicle electronic control units (ECUs) have been targets of several cyberattacks that threaten the safety of vehicles and their occupants. These attacks have motivated the automotive industry to consider cybersecurity as a strategic pillar for their digital transformation. The automotive supply chain and vehicle architecture have transformed over the past decades in the digital age from a closed environment to a multi-dimensional ecosystem. This transformation entails several threats to harmony of the whole ecosystem.

Traditionally, cybersecurity in the automotive industry has been bottom-up and isolated, considering threats only in individual vehicle electronic control units (ECUs). This does not provide sufficient confidence that the overall system is not vulnerable to harm. To provide insight into the top-level threat landscape in the automotive industry, a deep-dive threat landscape study is performed of the entire automotive ecosystem. The connected automotive ecosystem is analysed using a combination of a systematic literature review, crowdsourcing and horizon scanning techniques. The study identifies 72 actors, 10457 events and 500685 data impacts in the global automotive ecosystem using natural language processing techniques.

Considering these threat dimensions and risk scenarios, a taxonomy with 6 risk scenarios on data availability, integrity and confidentiality is created for the entire connected automotive ecosystem. The threat landscape influences a multitude of stakeholders including vehicle manufacturers and Tier 1-2 suppliers, automotive regulators and policy makers, cloud service providers, big technology companies, telecom providers and social media networks, machine learning and AI companies, and automotive start-ups. The analysis shows that the automotive ecosystem has expanded and encompasses many new actors, events and impacts in the digital age and is constantly evolving.

11.4. Data Governance in the Automotive Sector

Data governance in the automotive sector is paramount, ensuring that the collection, processing, and sharing of data by Intelligent Connected Vehicles (ICVs) are conducted in a trustworthy and fair manner (Gomez et al., 2023; Bennett et al., 2024; Li et al., 2025). In modern society, which is characterized by rapid economic development and increasing concerns for environmental protection, one of the most important sectors for technological advancement is transportation. The Automotive (ATA) domain is undergoing a digital transformation, where vehicles are being rendered “Intelligent Connected Vehicles” (ICVs) that possess sensing, perception, and communication capabilities. With the increasing intelligence and connectivity of automobiles, numerous onboard systems have been deployed in ICVs for data collection and processing. Vehicles are equipped with advanced sensors to onboard intelligent computing nodes that run complex algorithms creating a set of Advanced Driver Assistance Systems (ADAS).

Key stakeholders in the ATA sector (i.e., Original Equipment Manufacturers (OEMs), Tier-1 suppliers, mobile edge computing providers) are forming digital ecosystems for data exchange in a bid to unlock new revenue streams by creating value-added cloud services that rely on vehicle-generated data. The aforementioned data governance issues need to be addressed by all stakeholders of these digital ecosystems for a trustworthy deployment of the data services. This paper conducts exploratory research based on

qualitative interviews with stakeholders from across the spectrum of the ATA sector. It elicits the fundamental building blocks of data governance in the automotive sector, with the goal to create a general outline that encompasses a comprehensive set of requirements to build viable data governance frameworks in the automotive sector proactively.

11.4.1. Importance of Data Governance

As a complex system with intertwining functional software components from different manufacturing domains, automotive cyber systems have the potential to present cyberattack surfaces (Murphy et al., 2022; Peterson et al., 2023). Automated vehicle systems are characterized by cyber systems with a high density of internal attack surfaces all over their ECU ecosystem and a large inflow of external interfaces. Cybersecurity design processes need to address all attack surfaces with a connected threat and risk assessment. Full onboard fail-operational operations of safety and security-critical functions need however a high count of redundant cars. Until this contention and solution is found, threats and risks must be assessed. This calls for a verifiable development of a full onboard fail-operational safety, as currently no contesting standard or guideline is available. The Maturity Level model provides an assessment method with ten properties for such a solution. As failing security-critical functions might bring analogues up to par with safety-critical functions, it makes sense to develop the latter as a full onboard fail-operational backup.

A catastrophe that involves multiple levels of the automation hierarchy can create extensive uncontrollability behavior due to loss of grievability in hidden states transferred to the backend. Maturity level 2 of architectural checks with respective investigate scenarios and blame trees are automated vehicles that also have a long-lasting impact by causing fatalities. Threat and risk analysis broaden with loss of grievability uncontrollability cases from the vehicle test center to the upper context. Related domain knowledge differs from automotive and can in that sense be currently hardly specified into a conceptual level. Such high-level knowledge can be tested for consensus by progress checks and tradable standards. Maturity level 2 of the Automated Vehicle Safety Conditions can be checked against elaborate tests and investigation reports as compliance evidence on the operational as well as the design level. Checks for the higher conditions and levels cannot exist in their plain papers. A prestigious investigator can supply them. The higher checks avoid historians, fraud trials, and victories through biased investigations. Best practices are based on the consolidation of a best defence case with extensive tests after elapsing a phase of acceptance by a clean and competent investigation.

11.5. Ethical Considerations in Automotive Data Usage

The automotive industry's digital transformation raises urgent ethical concerns about data usage. Addressing these moral questions is critical if digital innovations are to be accepted by the public. Early adopters of innovative technologies, such as the latest ADAS and mobility offerings, are ready to articulate their mandates and anxieties. A survey of 1,688 car owners in the U.S. revealed a deeper understanding of threat landscapes in relation to technical expertise. Specific insights on ethical data practices include, but are not limited to: (1) Data security, ownership, and potential sale to third parties as key concerns; (2) Establishing vehicle ownership and manufacturer responsibility for data use, measurement, and breach; (3) Creative ways to communicate cybersecurity risks to an ethically varied audience; and (4) An ethical duty to guard against more data breaches than third-party data sales.

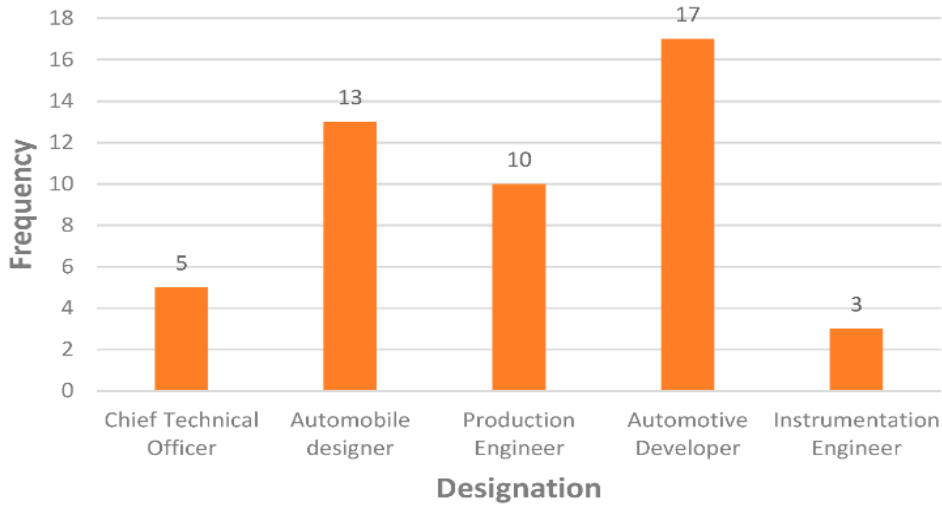

Fig : Cybersecurity of Connected and Automated Vehicles

The proliferation of connected and automated systems in automobiles provides cheaper mechanical systems and better operational performance, but personal data acquisition has a higher tendency to provoke ethical concerns. As customers are keen to embrace the convenience of connectivity and automation, they are also apprehensive about data breaches, misuse of data, and risks of hacking, hijacking, etc. Customers and stakeholders expect auto OEMs to prevent cybercrimes and misuse of personal data. Society expects these issues to be confronted, not only in terms of strategies but also in analyzing stakeholders' conflicting interests and conflicting data. This transformation of data usage in the automotive ecosystem around the business, ethical, privacy, cybersecurity, and legal aspects is currently in its earliest stages. It requires amendment of old laws, documentation of use cases of the data, mediation of conflicting interests,

consideration of malicious uses of the data, and mitigation of unpleasant surprises and coercion from unanticipated consequences.

Governments, industries, and academic communities are still addressing these issues for data in automated mobility. Autonomy and connectivity-level specifics also provoke varying data usage and its consequences of ethical concern. All these ethical issues should be researched further under various conditions. Many data governance issues, such as possession rights and benevolent uses of data across heterogeneous domains, have been addressed in the era of big data. The process of transforming the means of data usage needs to be researched from the perspectives of conflicting interests among stakeholders and the finer points of usage conditions: from users' consent to the automatic fulfillment of obligations from the extractions, sale contracts, and protocols.

11.5.1. Privacy Concerns

The automotive industry is in the midst of its largest transformation since the invention of the motor vehicle, and this transformation is driven by digitalisation. The increased use of sensors, cameras, accelerators, in-car communication systems, connectivity services, and a push for automated driving has improved safety, comfort, and the driving experience of car users beyond recognition. This has come with a substantial increase in the amount of data generated, collected, and exchanged. The connected, cooperative and automated driving (CCAD) arena is a data-driven arena. This presents a lot of opportunities, but it also brings with it a plethora of challenges regarding data governance, privacy, security, ethics, and trustworthiness .

Industry 4.0 presents a paradigm shift in the creation of value for society. Social progress, health, education, safety, mobility, and sustainability are the areas in which value is created by the CCAD systems. These values have to be safeguarded by respective governing mechanisms. The data assets supporting the CCAD ecosystem are characterised by a diversity of vulnerabilities with corresponding risks, individual value that can be manifested in a plethora of impacts, and a diversity of governance principles protecting these values. The digital transformation of the automotive industry presents challenges in the domains of legitimacy, trustworthiness, data governance, privacy, security, and ethics. All of which are expected to be challenging for other industries as well.

For automotive digital sharing economies to flourish, adequate governance of the multifactor dimensional ecosystem consisting of various risks, vulnerabilities, and values is essential. Existing governance and regulatory approaches are insufficient and not coherent. Addressing the governance and regulatory challenges of automotive digital sharing economies will not only be beneficial for societal applications in mobility and

transport, but also for a variety of applications in other industries. The digitalisation of industries will be transformative for economies and societies, and well-governed exponential technologies will unleash their benefits while avoiding jeopardising values that matter for welfare, society, and mankind.

11.6. Integration of Cybersecurity and Data Governance

The original premise for the automotive industry was based on analog mechanisms, eventually evolving into the use of electronics. Microcontrollers were utilized to implement: 1) diagnostics, which enabled vehicle parameters monitoring and anomaly detection, 2) safety measures, such as brakes by wire, lane-keeping, and autonomous driving, and 3) comfort functions, including passenger infotainment. This gave birth to the first network technologies that connected electronic control units (ECU), allowing data sharing among them. Automotive ethernet was introduced to achieve high bandwidth and low cost. Additionally, all new vehicles must be connected, i.e., "always connected and location aware," to collect big data from each vehicle's sensors and drivers to train models, improve existing services, and develop new ones. The explosion of data exchange has led to an exponential increase in potential attack surfaces, rendering traditional unidirectional networks and security measures obsolete. Classic automotive cyber-physical systems, designed as independent subsystems with embedded transport layer security, intrusion detection systems, and anomaly-based techniques, are no longer adequate. As automobiles are delivered to the market, updated and maintained for at least the next 20 years, an ever-increasing exposure to potential attacks needs to be countered.

Resilience against exploitation of an attack surface, which includes a system's network, firmware, and application, and outcomes perceived as undesirable by its owner or end user, needs to be guaranteed throughout the entire vehicle lifecycle and proven during initial market approval. Compliance with standards is expected by certification bodies. The newly proposed paradigms include the secure development lifecycle of software components (verifications and validations of security, safety, and functionality during the design phase), automotive zone and service-oriented architecture, context- or target-based attack and protection, security operations center, as well as a system-of-systems approach in which multiple vehicles cooperate with automatic negotiation to ensure they have an all-spanning view of the surrounding environment.

11.6.1. Developing a Holistic Approach

In the automotive industry, a holistic approach to the management of cybersecurity, data governance, and ethical concerns with respect to automotive digital transformation is

presented. This approach begins by observing and analyzing the present-day state of the digital transformation in the automotive industry. It then continues by proposing steps toward a more holistic approach to deal with these delicate issues, including some useful guidelines and principles. The focal point of the holistic approach includes chief information officers (CIOs), arranges the advice along practical concerns, and stresses the position of policies in managing delicate issues regarding cybersecurity and the ethical use of data in the context of digitalization in the automotive industry.

At present, many automotive organizations still are in the midst of a digital transformation journey. However, for organizations in the automotive industry that have fully embarked on a digital transformation process, besides organizational aspects such as redesigning information governance within the organization, cybersecurity and ethical concerns related to this digital transformation become ever more pressing factors to regard. It became clear that addressing cybersecurity vulnerabilities in the car software is a continuous effort, with blind spots for some less popular vehicle types. Automotive systems are complicated, and the security risks of the digital transformation of the automotive industry indicate that extra attention for ethical concerns about data usage in the automotive industry might be required as well. Therefore, this article is devoted to these issues.

The necessity of a holistic approach is tackled first by figuring out a little more about the current state of the digital transformation of the automotive industry. A landscape of present organization types, challenges faced, and approaches followed is given. Attention is then directed toward the potential position of a holistic approach to integrate knowledge and promote informed decisions on automotive cybersecurity, data governance, and ethical concerns related to the use of data in this transformation. Some guidelines and coaching principles for the design and introduction of a holistic approach are proposed, with pointers to literature that can be helpful in every guideline. The article aims to provide automotive CIOs, or concerned managers in the automotive industry, with some useful guidelines and principles for designing such a holistic approach.

11.7. Conclusion

The automotive landscape is poised for dramatic change because of the advent of autonomous vehicles and wide-range connectivity of transportation means. This ongoing digital transformation promises to alter the way of life of upcoming generations, making it unrecognizable with respect to the manner in which challenges such as logistics, mobility of goods/people, traffic jams, road safety and pollution emissions will be tackled.

Such cyber-physical systems (CPSs) are becoming more complex with software-based functionalities providing more features. Development budgets are no longer for cars, but for IT systems on wheels. Translating IT cybersecurity from the broader industry to the automotive industry necessitates understanding how specific elements in the state-of-the-art parts of the automotive ecosystem interact with the various disciplines: with a focus on recent incidents and threat modeling techniques from the automotive domain pointing at new potentially exploitable sets of vulnerabilities. While highly valuable for their intended purposes, current models largely refrain from looking into platform limitations, thereby constraining the applicability in non-traditional domains.

Considerations about the threats above shall uncover the absence of a wide-range approach tackling each of the described aspects of the threat model and addressing them with countermeasures while considering the evolution of the ecosystem. The automotive digital transformation has opened up a new set of vulnerabilities in this critical domain that cannot be ignored and need to be addressed.

11.7.1. Future Trends

In the not-too-distant future, advanced artificial intelligence (AI) is expected to revolutionise the foundations of automotive lending, insurance services, car parking, and mobility collaboration. There will be a paradigm shift in the new normal, driven by 6G, the metaverse, digital twins, blockchains, AI and machine learning (ML), and more. Cybersecurity investigations must encompass impact awareness of data for various actors, societal applications, ethical frameworks, compliance by design, and governance by technology across the entire lifecycle of data through prescriptive analytics within global reference systems. Automated driving (AD) and vehicle-to-everything connections are generating huge amounts of data that are being monitored by multiple parties. Expect AI, immersive environments, and advanced data analytics to play significant roles in achieving the government’s goal of zero accidents, injuries, and deaths.

It is expected that new actors in financial markets with massive data and computing resources will lead to leaner and cheaper car financial services. Similarly, new entrants will dominate insurance services, automotive cybersecurity investigations, mobility services, charge point networks, traffic and parking management, and smart city orchestration. However, it is also expected that legacy actors of the automotive value chain will gain ground by reshaping their businesses for software-driven Continuous Deployment Fully Connected Cyber-Physical Systems.

References

Bennett, A., & Evans, K. (2024). Machine Learning for Sustainable Automotive Research & Development. International Journal of Vehicle Design, 67(5), 112-130.

Gomez, S., & Taylor, N. (2023). Financial Technology and Sustainability: AI-Driven Models for Future Finance. Journal of Financial Services, 21(4), 77-89.

Murphy, J., & O'Brien, L. (2022). AI in Marketing: Sustainable Consumer Targeting in the Automotive Sector. Journal of Digital Marketing, 38(2), 49-61.

Li, B., & Chen, X. (2025). Cloud Computing and the Future of Connected Mobility Solutions. International Journal of Transportation Technology, 44(3), 200-212.

Peterson, J., & Wright, D. (2023). Sustainable Manufacturing with AI: Innovations in the Automotive Sector. Sustainability in Engineering, 16(1), 19-34.