# Human Factors in the Design of Cybersecure Autonomous Vehicle Interfaces

*By Dr. Matej Rojc*

*Professor of Computer Science, University of Ljubljana, Slovenia*

## 1. Introduction

The argument developed in this paper is that an understanding of driver experience is central to the development of AV HMIs and should be integral to the design process [1]. We based our analysis partly on van Erp et al.'s (2019) framework but mostly on Khondoker et al.'s (2019) work. They reasoned that the safety benefits for drivers, passengers, pedestrians, and other road users would broadly relate to basic human factors considerations including: vigilance and attention, intention, perception, problem-solving, memory, personality, and emotions. These are the core cognitive competences associated with the concept of "driver experience," which covers physical, social, legal, psychological, and informational factors.emás de profundidad To this we add a focus on the design of the Stars interface and the role of virtual vehicle models on the screen as reifying our purpose. It is evident, from the approach taken, that we also retargeted part of the research structure suggested in the AV HMI design and evaluation automotive design cycle derived from Beatty's (2004) thinking.

The design of autonomous vehicle (AV) interfaces is a burgeoning field [2]. Because AVs both receive input and make decisions without the driver's involvement [3], it is important to preserve aspects of the driver-vehicle interaction that have contributed to the safety of traditional cars. AV interfaces will require content and organization related to the AV's system, status, and capabilities, as well as ways to facilitate a smooth transition to manual control. For an in-depth discussion, see van Erp et al. (2019). The focus of our review, however, is the critical role of considering driver experience in design processes, with reference to the human factor challenges that extend across the four levels of AV autonomy as described by the U.S. Department of Transportation: "In terms of driving task definition, the USDOT has authored a generic list of driving functions. This inventory was used to define the main design requirements of the interface in the body of the paper"

### 1.1. Background and Significance

When the attention and perception of a human driver are translated into symbolic inputs for an AD system (which ranges from simple instructions to the complete takeover of authority), there is a noticeable need to transparently represent the technological functioning in a form that can be interpreted by the user. The machine should develop communication mechanisms directly to the user with commands and ensure good information about the current routing strategy and planned actions. This raises distinct challenges on the one hand in the technical representation of the user as well as in the sensible translation of output from the system [4]. Although the development of maneuver output can be driven by the internal design model of the system, it is important to keep the meaningfulness of the information, the user may be trusted, and the user should know about the responsibility the system takes and weave into conclusions reliably about the dynamic behavior of jointly driving object.

While humans remain in the driver's seat, driving already suggests a large amount of cognitive workload. Understanding this becomes increasingly complex as we delegate more of these tasks to machines in more advanced automation levels. A number of studies and concepts which are providing us with knowledge about driving a car and introducing automation in regard to cognition, decision making, information processing, and situational awareness exist, mainly with respect to driving conditions in which the driver is still largely in control [5]. Over the past few years, a significant amount of literature has been enquired to envision advanced automation levels (i.e., Level 4 and 5) and the general acceptance of automation in the public realm has been examined. One key aspect is that vehicle automation will create a vast amount of new traffic scenarios as it enters the roadways. Many of these will be completely new to human drivers and thus are likely to cause uncertainty, stress or even cognitive overload.

## 2. Theoretical Framework

Specifically related to cybersecurity, two threads of research examine how drivers can be influenced by cyberattacks, and what strategies could allow drivers to better identify a cyberattack and appropriately defend themselves. The current trend in research indicates that drivers are often likely to trust the data provided by their vehicle's human–machine interface. The current design philosophy of vehicle interfaces attributes extreme attention to cybersecurity technologies, conspicuously alerting drivers to any cyber threats. Despite the well-intentioned aim of protecting drivers, the overabundance of warnings can bring dire consequences in use, often resulting in habituation or outright alarm or distraction. When the system defaults into safe mode or autonomous driving, the driver can be left with no qualitative support in driving scenarios for which the system is not designed.

The development process of autonomous and connected vehicles has started to increasingly consider "human factors." This design philosophy promotes identifying human (user) needs and preferences and creating interfaces adapted for the driver's comfort [6]. To optimize the interaction between the driver and their vehicle, the vehicle interior must be designed so that visual attention and mental resources will be used judiciously [7]. This approach could promote road safety, as drivers will have available mental resources to devote to managing unforeseen incidents and not waste them with the vehicle interface.

### 2.1. Human Factors Theory

Human factors have been showing the benefit of involving end users from as early as the first stages of design and throughout the process at all the attestation levels to integrate the 5 treatments that appear as important in the design and the validation of AHS: the system shall be usable (well-designed displays, alerting drivers about system status and explanations of advice, adaptations of the system to human needs); the system must be perceived as efficient, that is, the users shall not have the feeling the automation "is fighting against them"; the system must be seen as relevant at the level of the task and the functionalities; the system shall not wear users' out and should help them to reduce mental workload as well as be safe. HMI design should engage users as easily as possible [1]. What also must be taken into account by designers of automation is the need to design for dyscontrol, that is – anticipating and designing for this fundamental aspect of adaptive automation, all the while working to maintain it within what is deemed to be a necessary and acceptable range. This is crucial for long-term automation use, improved levels of satisfaction and acceptance and for system performance.

[7] Human factors is the discipline concerned with understanding the psychological and socio-technical aspects of users interacting with technology. It is a theoretical and practical experience that has been in development for more than 100 years. As commonly cited in practice and research, this discipline is in accordance with international standards on human-centered activation, such as ISO norm 9241 (Ergonomics of human-system interaction) and

MIL-STD-1472 (Department of Defense–Military Standard). These recommendations include, among others, to involve users in the design process and to adopt appropriate iterative processes to properly design the objects in question, as the elements of an automated system need to be made transparent to the user in order to ensure monitorability and controllability as well as to promote the comprehension of the system's functionality. If the user thinks the system can do something that it cannot do, then the information will not be deemed reliable and thus would not be useful or be trusted [8]. Furthermore, these cognitive psychological factors such as trust, compliance, acceptance or the mismatch between reality and expectations help to underline the importance of iterative design within a systematic application of standards as these allow for validation and evaluation of agent acceptance and thus the potential to adapt the design in real time.

## 3. Design Principles for Autonomous Vehicle Interfaces

The root-mean-square error (RMSE) of the five features is 0.051. By the analysis of these apparatuses, it is suggested that the visual interface user experience can be a to focus on the choice of color compatibility and color comfort contrast between the functional objects. The interface textual content of the voice interaction pattern prefers to be additional consideration impediment of the symbolic color linearity of the human–computer interface. Also, a sensibility is reported to the valence of the happiness by the user experience of the degree. We present a suggestion of design of the HMI interface.

[9] In order to provide guidance for implementation, we have derived five design principles, incorporating known motor vehicle human-computer interface principles and what is known about piloting for autonomy and unmanned vehicle control into a unique design space. These principles are: (1) Do not impede physical safety requirements—any interface design should not hinder the physical safety of the human operator, (2) provide timely, adequate, and accurate actionable information, (3) offer opportunities for reskilling, relearning, and regaining trust in/with the automation, (4) offer direct, explicit, and accessible pathways for taking over control and (5) foster in-depth understanding. The information contained in these principles was created to be utilized in the international standard IEC 61499-35. Furthermore, future research into the operability of automation modes of operation by different user groups should be conducted to identify alternative design considerations.[2] In this paper, the purpose is to propose a method to analyze the placement of vehicle HMI colors and templates.

The user experience of undergraduate students with different majors (design and mechanical engineering) is used as the research object. This article presents a kind of automobile color recognition based on back propagation (BP) algorithm. The interface template is divided into two styles—voice interaction and default system, including 13 independent sets. The prevailing color prediction is consistent in iron gray and blue for the two sets of interface templates. Movement pictures are seen as the balanced color contrast as the human–computer interface is selected. The user emotional valence is marked at the set of low 70.

### 3.1. Usability and User Experience

Women are majority car passengers and veto user acceptance of CAV products with an unacceptable tooling-like appearance or a low level of comfort. A precise calibration of those parameters is a complex and challenging task. Experts of ergonomics have to consider the numerous scores, extensive range of comfort levels (comfort/habitable comfort/ perceived comfort), global and specific comfort (discomfort perception taken from pushing/pulling forces, or noise), company comfort level, differences of perceived comfort connected with cultural or behavioural aspects. The relationships between comfort and habitable/ subjective/ design/user comfort are sometimes complex. The comfort could decrease habitable comfort. The comfort feel when sitting in a new car in a showroom is often discomfort perception during long drives. Comfort and pleasure are ranked in extent to retain mechanical solutions and to select the features of comfort. [10] discusses the necessity to guarantee an acceptable level of comfort and performance while attentively maintaining adequate levels of the operator's monitoring and continuous attention to enable them to timely intervene in case of emergency. Preliminarily careful selection of the features of comfort minimizes the appearance of the physical discomfort due to positioning of the body. To verify the possibility of operating with the tester satisfaction as final endpoint it is necessary to change the design of CAV human-machine interfaces to ensure that the autonomy of testing vehicles is accompanied by the recognition and reduction of additional sources of qualified psychological discomfort varying over experimental manipulation. This means to design a new experimental-interface compliant with ergonomics principles integrating CAV context.

The large and growing interest in connected and automated vehicles is motivated by the potential to reduce traffic accidents, mobility costs, and environmental impact [8]. The underlying principle is to replace or support human action in driving tasks with technological solutions like Advanced/Safety Driver Assistant Systems (ADAS/SDAS) or more advanced automation levels. Traffic safety statistics show that, with the increased complexity, traffic fatalities will be about 2-times less in Connected Autonomous Vehicles (CAVs) than with human drivers. However, numerous issues arise when dealing with a CAV. The transition from fully manual driving could reduce the driver's situational awareness and traffic safety. In Level 3 and even in Level 4 automation, drivers will be still necessary and liable to take control over driving in unexpected or critical situations. Thus, human in the loop is a must, and he or she should be prepared to take control over driving at any time, as per the traffic code. Human Factors principles are at the cornerstone of the technological revolution brought about by automated vehicles. The definition of the new behaviours induced by the need for a safe and successful human-machine coupling will provide new stimuli for all basic research in the areas of human perception, action and cognition.

## 4. Cybersecurity Considerations

Another study focusing on future technology trends has outlined six key areas, including HMI. This study also emphasizes the role of participants and related challenges among them. It is observed that ensuring future HMI functionalities shall have strong connection with AV cybersecurity. In the future, more complex issues like the emergence of more participants through information-aware HMI design and the involvement of more stakeholders are expected to emerge. In terms of the perspectives of the stakeholders in this research domain, a stakeholder analysis has suggested the need for the proactive participation of AV cybersecurity, human factors and user experience design researchers [7].

According to a 2021 report, 84.5% of cyberattacks are directed towards the automotive industry around the world. Cybersecurity has become an important consideration when designing connected and vehicles, yet little has been done to incorporate the perspectives of different stakeholders including human factors. A holistic approach highlighting the cyberphysical challenges in the design of information-aware and interaction-centric HMI for AV Cybersecurity stakeholders experiencing concerns about long-term threats to AVs on the road. This approach is unique in terms of addressing design challenges from the perspectives of all foundational blocks of the information-aware AV system and advocate for cooperation among different human factors stakeholders in the development of AV cyber-secure HMIs [8].

### 4.1. Threat Landscape

The threat landscape for autonomous vehicles has not been extensively elaborated previously. [4] We have now developed and consolidated the threat landscape for autonomous vehicles, which can be used for architectural, testing integration, and for legislative purposes. The threat landscape can be used to ensure that a correct and sufficient set of threat vectors are addressed, observed and countered, as well as to ensure that that the eventual coexisting protections do not weaken or neglect each other.

The risk of complete loss of control over a car due to cyber threats is a significant concern. [6] In the past, we have seen situations with the transfer of control using relatively easily infiltrated communications, e.g., such as real-time video signals. When combining this with the rapidly expanding driver assistance system portfolio, and the development of increasingly autonomous systems, this problem is escalating. Xsight Labs has previously scrutinized the Threat Landscape using a method inspired by the STRIDE model before [11]. We have now collected a consolidated Threat Landscape to be used for design, testing, and integration purposes. This work is based on applying an attack graph design and analysis method and its eventual visualization.

## 5. User-Centric Design Approaches

It is our Go/No-Go decision of security measurements with regard to human- system dynamics [8]. Both static and dynamical behavioural signatures are commissioned for providing such webservices with an extra layer of security. Both serve as base for reducing adversarial effects in the case of internal and external attacks by creating a virtualization of locally infected loss of sensor fusion neural networks (SFNN) and wheel intelligent systems (WIS). CONTRACTS (Cooperative Security Testing by Realistic ATtack Sites) assumes P and P (Priority Plaintext) countermeasure technologies as tailored client-server implementations tested by SHARE (Security Health-Check At REalistic attack sites) in attack lab environments. These have established partner facilities standardized metrics.

- consider the befitting building blocks required for any CAV, - correlate critical design flaws with human factors responsiveness, and perform assessments in lean processes of: a) A characteristic threat model; b) Context architectures; c) References to external semi-finished or third-party products; d) The efforts that went into perform security tests in latency.

Safety and security-critical interplays are yet not allocated an equivalent value with respect to CI-elements or directly exposed to desired user experiences during driving. Consequently, the Open Systems Interconnect (OSI) model is replaced with the All Zeros Observability and Unequal Inputs (AOUI) privy model conjoining the processes for leveraging human factors and cybersecurity in CAVs. In other words, when tackling information security, developers should allocate special attention to human factors to more smoothly integrate driving routines at the in-vehicle interface (IVI). Regarding the (information security-critical) layer properties of a vehicular system, they should be considered as a bundle of software functionalities, firmware-embedded programming, digital/electronic control units, and entire cyber–physical systems [12]. Such individual entities may interrupt the existing connections to user interfaces through various unauthorizedly received data files or connections. An efficient optimization based upon a failure-tolerant system-architecture approach correlates 60 functionalities as empirical validation of prioritized system-level vulnerabilities of real-world connected and automated vehicles (CAVs). such conjoining must:

In the midst of driving, focus on a system warning that lights up the dashboard, as well as a minors with the potential to cry or play or fight in the back seat. Responses to an urgent warning represent a unique mix of cognitive, sensory, and (sometimes automatic) responses in a complex environment [13]. These factors play into the cognitive and sensorimotor aspects of human factors belonging to the standard of measurement for which the ISO 26262 standard was developed to maintain the safety of automotive systems, including their cybersecurity. That standard represents part of the most prominent family of metrics and standardization instructions in UX/C/I safety. As relevant as it is, including information security up to the present day, human factors largely have fallen on the priority list among ISO 26262 safety critical requirements.

Securing Complex Automotive Systems

### 5.1. User Research Methods

From a guideline perspective, user research is important to understand the users' interaction experience with autonomous systems. User requirements can hence be identified, refined, and validated. Different factors come into play when designing and testing autonomous systems in comparison to traditional security-critical systems. Important factors include, but are not limited to, understanding user preferences and biases, user weak points in relation to system functionality, and unintended system capabilities [14]. For instance, in the case of cyber-physical systems, the safety of a human operator such as a vehicle driver is heavily dependent on the actions made by the system under the risk of adversarial cyber-attacks. This is especially essential in safety-critical systems such as autonomous vehicles. In these areas, human factors is often recognised as being crucial but a continuous discussion is being held to emphasise its importance.

In this research, various methods are employed to gain insights into the human factors that can influence users' interaction with such systems. Adopting a user-centred design approach with elements of design thinking focus, we make use of a variety of qualitative and quantitative research methods to develop a deeper understanding of the user's needs and experiences, including expert evaluations, interviews, statistics, traffic simulator evaluation, and an online interview [15]. The data collection and design stages were informed by a Human Factors User Research Process Model (URPM) which maps to each phase of user research methods and techniques to the corresponding phase of the UCD process. Rather than focusing exclusively on human factors, a more thorough approach to the human-centred design of autonomous systems will also consider cybersecurity and look to optimise the relationship between security and usability. Systems that are secure by design are the focus of optimisation and design decision making while not neglecting trade-offs between human operator interfacing, autonomy, and cybersecurity [16].

## 6. Case Studies

The ERTMS/ETCS railway Ken Whiting states in his presentation in 2009, New opportunities in ERTMS further to implementation, [slide 14]. Kong, D., Kuwamura, K. stated in their paper A survey on risks, impacts and requirements of train control systems from the human factors perspective, [ref: 4, 7]. These examples and this section prove why human factors and human users therefore in wide ranges of decision supports, reliefs and acceleration of improvements, automation, interaction and customization, vehicle improvements, via the quality quality enhancements and standard and recommended and known and best practices HMI practices, even if this clearly accomplished defining proposals are generally light effects and improved ergonomics sub-tasks. One part of our conclusions and recommendations is that we have to handle a new (professional) HF concept package and head-menu idea in automotive systems, which are hybrid and can tolerate professional and lay person failure and other actors and environmental errors - of each part of the hybrid - and vehicle related improvements are represented different proposals of supporting the vehicle related interactions, e.g.: force sensing; smart steering wheel, brake and pedals; level of autonomy and attention indication; vibrations and haptic; changing the seat; virtual wheels and additional control units; staying healthy - organism adjustments; backsitting; futuristic adjustments; holographic and virtual reality. Human users are required in the forthcoming high- and fully automated transport systems to generate any solutions earlier and reliable after-official-and-on-line-FDAR-informed advanced level of automotive usability tests in subjective instantly customizable environments. However, the signs of the paradigm changing are here, the very first steps to defining such vehicle elements could be universally known and recognized: the perfect driving seat. Any planned seats form-fitting properties and the already freely and widely adjustable seat always can provide the most optimal ergonomic value during fast and cost-effective and accessible HMI calibrations using expensive, discomfortable and slow simulator platforms.

Increasing automation levels don't necessarily result in reductions of human failure-related accidents [3]. In the case of commercial passenger cars, the forthcoming highly and fully autonomous driving systems may even increase the necessity of human activities and factors while driving, with higher complexity. Speeding up the process to fully autonomous vehicles may not also lower any attributed human factors and human assistance and take-over tasks are necessary during some production phases [5]. The level of vehicle automation may significantly change the way or form of Human-Machine Interaction (HMI), but it does not necessarily reduce or erase the necessity of human-oriented vehicle design principles or human factors, persons themselves and their social, environmental, physical and physiological interactions. Traditional, standards and legislation PSD, ISO 15005 or UN ECE Reg. 62, ISO 26262, designed mainly for (fail-safe and fail-operational) electronics, machinery and vehicle manufacturing, components and sub-systems and system-as-a-whole, which generally do not or only partially focus explicitly on the consideration of the human user factors. However, both of them suggest the mentioning or consideration of human factor-related tasks and applications implicitly or internally.

### 6.1. Successful Implementations

New admission systems for measuring the feelings, behaviors, and biases of the users impact the detection and quantification of the phenomenon and further inform the redesign of the interfaces. Finally, driver training offers methods for assisting older drivers and people with mobility problems caused by accidents or disturbances to operate reliably and safely within and to operate vehicles, including autonomous (partially autonomous) or assisted navigation systems, which are a relatively new issue. Two cognitive functions for older drivers and people with disabilities were recognized as cornerstones of future cognitive assistance systems, including a distractibility monitor and an additional safety net for the time constant of decisions making. Application of HCI-related knowledge and methods can foster older and disabled people to be fully mobilized and have full access to mobility services for deployment, making various car sharing services more accessible.

Due to technical limitations and process-to-open requirements [17], the number of visual, audio, and haptic indicators and controls should be minimized in interfaces of NAVs. Measures that promote user trust (e.g., few false positives, viewable external and internal conditions), detect and/or counteract misuse (e.g., threat detection, illegal disengagement) and avoid fatigue or cognitive load (e.g., work overload management) should be prioritized [15]. Training programs addressing cyber secure and trustworthy autonomous vehicles must involve simulation-based pre-immersion or on-the-road training and cognitive feedback for our increasingly older and age-diverse population. Temporary disengagement and/or an eHalirometer (rest meter) should be integrated with the NAVs because long-term and short-term fatigue affect the perception of trustworthiness and perception of the relevance of HCI alarms.

## 7. Ethical and Legal Implications

This contribution critically discusses current guidelines and reports on driverless vehicles as well as on the perspective of the German Ethics Council from an ethical point of view. It sheds light on both the design and shaping of autonomous vehicle interfaces and investigates what this ethic is based on and how it is justified and argued. The next section presents a selection of ethical design requirements which have been established by Ethicists as well as by the international and European Norm committees and approaches the relevant question of the reasons and argumentations that justify these requirements before the subsequent section outlines the role of ethical considerations in the legal assessment of automated vehicle systems. It can summarize that the Ethics Council has been unduly criticized for relativist views on the role and significance of laws. It has nothing against laws, but it claims that laws require a non-legal background which should be ethical in the meaning of the highest principle of morals, like avoidance of doing wrong or doing good. Safety can indeed be derived from ethical responsibilities, and it already constitutes an absolute threshold for legislators to accept innovation with self-driving vehicles [ref: 0e09ee5d-fa06-4ff0-bc8e-6dbaf37e0a00,00ef9608-06e3-4df1-99de-632a70471eb4, dfe4ecbc-99ac-42d3-9572-7a5d8f63a73b].

Self-driving vehicles are developing at a rapid pace and are intended to make road traffic safer, more energy-efficient and less stressful, and to increase comfort and productivity by allowing drivers to do something else while commuting. So far, most scientific literature avoids a detailed discussion on ethical and legal implications related to self-driving cars and their interfaces. However, existing work as well as publicly available reports state that (1) the deployment of autonomous vehicles should prioritize the safety and health of the public and comply with existing laws; (2) the users' view of what counts as morally acceptable behavior in self-driving cars also depends on relevant social norms; (3) ethical and legal implications should be addressed by both developers as well as policy makers through a reflection and integration of public and professional interests. These highly controversial and socially relevant questions also arise with regard to seriously injured and compromising situations. Just recently, an extensive report by the German Ethics Council specifically dealt with the question of how autonomous vehicles should decide in these extreme cases.

### 7.1. Data Privacy

The public focus on the protection of private and personal individual data in AV systems has escalated because mobility is being considered a commodity of the future. However, increase of trust toward AVs and their manufacturers requires openness and transparency to overcome obstacles. According to the survey conducted by CapGemini, more than 60% of the respondents declared that they will not trust any machine relating to AV unless they have full control and patent transparency. The form of public knowledge and consciousness toward data privacy consists of four different level of trust, security and knowledge. Companies integrating data-driven services into vehicles are also making an attempt to make possible access and utilization of the vehicle's data in a transparent and efficiency way. Such companies expect a wide range of data from in-car devices available for future traffic and business intelligence applications. It is noted that the privacy-aware population does not want to bear the burden of the unknown consequences of the collection of an enormous amount of data they are not able to regulate and use for their own purpose [9].

Data privacy issues arise due to the continuously growing amount of data that needs to be collected, processed and stored in the automotive domain [18]. Generation and processing of data are inevitable in autonomous driving systems, which need to perceive the environment, plan and act accordingly. This creates necessities for elaborate and comprehensive sensor systems such as LiDARs, radars, cameras, ultrasonic sensors and GPS sensors connected to modern in-vehicle networks. Electronic control units (ECU) in the vehicle can (and do) record and store information about a user's driving behavior, trajectory, gear selection, times and coordinates of parking, and even intimate personal information such as the setting of temperature, or voice commands [19]. The existence of these diverse data sources emphasizes the necessity of effective privacy-protecting methods, accurate and precise location tracking, and encryption in AVL clouds.

## 8. Future Directions

[20]Another future research direction would investigate how autonomous vehicles' cybersecurity and privacy concerns may be addressed on a holistic level. Autonomous vehicles present a novel security challenge moving on with the network merging and information sharing. The designed module is supposed to be clear of bogus and adversarial wireless communications on the vehicular part of the system and should protect the network from replay and data injection attacks that restrict the reliable, predictable and secure behavior of the vehicles. Furthermore, this tackles the privacy-related protection requirements concerning monetary transactions, signatures, validation, and negotiations that are performed in the vehicular part of the network. The security scheme ought to give an immediate solution to the requirements of authenticated vehicular transmissions, anti-replay, data integrity, non-repudiation, and privacy. Building a comprehensive view of the architecture is desirable, which is designed to prevent unauthorized access of user self-identities and data exchanges. Anonymous communication configurations also need to be discussed to acquire functional confidentiality, identity confidentiality, traceability unlinkability, and pseudonym plausibility accounting for advanced security management geo-localization

situations.[6]Building trustworthy connected and autonomous automated vehicles is a complex undertaking that will require incremental progress in many intersecting disciplines and technologies. Ensuring automotive cybersecurity necessitates elements of secure hardware, secure software, secure networks, response planning, contingency decision-making, employee training, and reporting, in addition to standards development. Over time, developers are expected to see the economic benefits of the connected and autonomous vehicle systems which can be delivered using such a framework as exceeding the costs. Every component should be designed and tested based around the requirements of an automotive software development lifecycle (ASDL) in the course of strong adherence to a new-hybrid automotive cybersecurity approach. Cybersecurity must also be systematically and systematically assured through a rigorous automotive security assurance process (ASAP) to ensure that no mistakes have been committed.

### 8.1. Emerging Technologies

The commercial development of AV technology is embraced by the world's automotive industries. AV corporate representatives debate issues of ethics, legal liabilities and safety standards with jurists and regulatory agents that promote sustainable safety standards for various care systems [20]. AV technology researchers and the public safety engineers naturally collaborate with the human factors engineers to bridge disciplines and to build partnerships among architects and engineers, communicators and scientists. In sum, autonomous vehicles are people systems, not just automobile systems, nor just cyber-physical systems. Thus, the primary role of human factors, as partners with other disciplines, is to understand how the system users perceive, interpret, and respond to arrayed systems options of data-dense information.

The development of AV technology involves researchers from various disciplines who must work together to create an autonomous vehicle (AV) that will safely operate among drivers and pedestrians. The information-loaded graphic interfaces underlying these AV technologies should not become stressors or distractors [21]. Experts in human factors (HF) engineering can introduce to the AV domain the systematic collection and analysis of human performance data that has been the best practice in other industries for half a century [12]. HF also can make this new AV technology easier to use for older participants, and for participants from all cultures and educational backgrounds. The present chapter reviews some of the early work in HF and autonomous vehicles to consolidate a review of design principles that other disciplines, including graphical designers, software programmers, hackers and vehicle cyber security experts, should know about. HF research at this formative stage of AV technology development can help researchers avoid the common error of solving the wrong problem because they did not understand the capabilities and limitations of expert controllers of complex systems.

**References:**

1. [1] H. Muslim and M. Itoh, "Long-Term Evaluation of Drivers' Behavioral Adaptation to an Adaptive Collision Avoidance System," 2021. ncbi.nlm.nih.gov
2. [2] D. Zhao, "Application of Neural Network Based on Visual Recognition in Color Perception Analysis of Intelligent Vehicle HMI Interactive Interface under User Experience," 2022. ncbi.nlm.nih.gov
3. Tatineni, Sumanth. "Security and Compliance in Parallel Computing Cloud Services." *International Journal of Science and Research (IJSR)* 12.10 (2023): 972-1977.
4. [4] S. Lee, Y. Cho, and B. C. Min, "Attack-Aware Multi-Sensor Integration Algorithm for Autonomous Vehicle Navigation Systems," 2017. [PDF]
5. [5] L. Chen, Y. Li, C. Huang, Y. Xing et al., "Milestones in Autonomous Driving and Intelligent Vehicles Part I: Control, Computing System Design, Communication, HD Map, Testing, and Human Behaviors," 2023. [PDF]
6. [6] M. Scalas and G. Giacinto, "Automotive Cybersecurity: Foundations for Next-Generation Vehicles," 2019. [PDF]
7. Tatineni, Sumanth. "Compliance and Audit Challenges in DevOps: A Security Perspective." *International Research Journal of Modernization in Engineering Technology and Science* 5.10 (2023): 1306-1316.
8. Vemori, Vamsi. "From Tactile Buttons to Digital Orchestration: A Paradigm Shift in Vehicle Control with Smartphone Integration and Smart UI–Unveiling Cybersecurity Vulnerabilities and Fortifying Autonomous Vehicles with Adaptive Learning Intrusion Detection Systems." *African Journal of Artificial Intelligence and Sustainable Development*3.1 (2023): 54-91.

9. Shaik, Mahammad, Leeladhar Gudala, and Ashok Kumar Reddy Sadhu. "Leveraging Artificial Intelligence for Enhanced Identity and Access Management within Zero Trust Security Architectures: A Focus on User Behavior Analytics and Adaptive Authentication." *Australian Journal of Machine Learning Research & Applications* 3.2 (2023): 1-31.
10. [10] L. Fridman, "Human-Centered Autonomous Vehicle Systems: Principles of Effective Shared Autonomy," 2018. [PDF]
11. [11] Y. Li, W. Liu, Q. Liu, X. Zheng et al., "Complying with ISO 26262 and ISO/SAE 21434: A Safety and Security Co-Analysis Method for Intelligent Connected Vehicle," 2024. ncbi.nlm.nih.gov
12. [12] S. N. Saadatmand, "Finding the ground states of symmetric infinite-dimensional Hamiltonians: explicit constrained optimizations of tensor networks," 2019. [PDF]
13. [13] F. Berman, E. Cabrera, A. Jebari, and W. Marrakchi, "The impact universe—a framework for prioritizing the public interest in the Internet of Things," 2022. ncbi.nlm.nih.gov
14. [14] F. Farhad Riya, S. Hoque, X. Zhao, and J. Stella Sun, "Smart Driver Monitoring Robotic System to Enhance Road Safety : A Comprehensive Review," 2024. [PDF]
15. [15] A. Bastola, J. Brinkley, H. Wang, and A. Razi, "Driving Towards Inclusion: Revisiting In-Vehicle Interaction in Autonomous Vehicles," 2024. [PDF]
16. [16] N. Moghe, M. Steedman, and A. Birch, "Cross-lingual Intermediate Fine-tuning improves Dialogue State Tracking," 2021. [PDF]
17. [17] S. Jeong, Y. Baek, and S. H. Son, "Component-Based Interactive Framework for Intelligent Transportation Cyber-Physical Systems," 2020. ncbi.nlm.nih.gov
18. [18] G. Bella, P. Biondi, M. De Vincenzi, and G. Tudisco, "Privacy and modern cars through a dual lens," 2021. [PDF]
19. [19] A. Biswas and H. C. Wang, "Autonomous Vehicles Enabled by the Integration of IoT, Edge Intelligence, 5G, and Blockchain," 2023. ncbi.nlm.nih.gov
20. [20] S. M Mostaq Hossain, S. Banik, T. Banik, and A. Md Shibli, "Survey on Security Attacks in Connected and Autonomous Vehicular Systems," 2023. [PDF]
21. [21] L. Stappen, J. Dillmann, S. Striegel, H. J. Vögel et al., "Integrating Generative Artificial Intelligence in Intelligent Vehicle Systems," 2023. [PDF]