Human-Computer Interaction Design for Adaptive User Interfaces in Autonomous Vehicles

By Dr. Tatsiana Stsebakhova

Associate Professor of Computer Science, Belarusian State University (BSU)

1. Introduction

This work introduces a real-time and possible run-time distributed solution to such a complex problem based on external Dynamic Risk Assessment and monitoring from the Outside Increase Transparency (OT), as a part of the Smart Cyber-Physical Systems under development. These new OT advanced models shape the exposition in time and timing (extended to the interaction physics), space and spatial criteria distribution, sensitive information minimization on physical sensors, and radio trust-assessment-to-performance-cost-resources under acceptable quality levels. They contain external and internal asynchrony elements. These OT-run-time approaches conform to cybersecurity and natural threatfulness associated with the journey for the AV and potentially for many similar Smart X applications with similar or same goals.

The collision of a self-driving vehicle raises many concerns, particularly related to cybersecurity. An autonomous vehicle (AV) needs to connect to the surrounding environment by using sensors and the internet. Now, the direction of research and development is moving away from the slow transfer of collected sensor data to an efficient mechanism controlled by edge computation. The question is how to empower a highly distributed edge with a real-time, aware, adaptive model designed to minimize risks simultaneously related to the cybersecurity and the response to natural threats associated with the journey.

1.1. Background and Significance

With respect to dynamic risk assessment, it had long been expected that a system with as much intelligent, big, and complex data moving with the pace of an AV would need to worry about inherent cybersecurity vulnerabilities. However, much less has been said about how to do so and even less to support the interfaces that shape effective stewardship of this risk.

Vehicles and their information systems are now recognized by ISO, NIST, SAE, and TT as information security objectives: specific needs will need to be handled at each process, and within each constraint, to protect vehicles and endpoints from threats. Much like the intelligent surface interfaces and underlying adaptive computing core this work aims to define, the attention cybersecurity receives in AV and HCI may be described in terms of its level of abstraction. Work in this category involves low-level monitoring, detection, and remediation of discrepancies between high-level user intentions and low-level system concepts. This conform and supply wave configures various human action component reliability of AVs.

In this new field of expertise and innovation, mainstream human-computer interaction (HCI) is indeed just one of the domains that contribute to human factors in automated vehicles (AVs). In this research, we can try to reconnect in ways that are meaningful to both. Therefore, we are aiming to deliver new HCI design knowledge that is satisfactory to both mainstream AV design features and construct top-down adaptive user interfaces that offer human factors robustness. The grand challenge any new AV faces is for drivers to trust it. To recognize why trust is so essential from a holistic and human-factors perspective, we must recognize that driving is a tight interplay among the tasks, functions, and models at the heart of the system. Because human factors engineering strives to optimize the interactions between systems—and not just individual systems—valuable expertise exists dedicated to system integrity and cybertrust. We have found that these dedicated contributors are at the normative fringes of AV development. The powerful subject matter expertise to support HCI design refers to sector-agnostic, widely applicable knowledge dedicated to adaptive user interfaces.

2. Human-Computer Interaction (HCI) Principles

As globally analyzed in this research project, AV involvement in crashes is likely to lead to users' dissatisfaction. On the contrary, if AV is not involved in accidents, even if the system is not totally safe, users still gain more benefits from the AV system's use. Data collected during the furniture of these research works is based on a wider set of previous studies in the automotive HCI research area, close to similar research experiments. HCI techniques in automotive systems introduced here are subsequently extended with the provision of an indexation of solutions to risk assessment problem areas. Every section of this paper was conceived inseparably from the list of other proposed research areas.

HCI defines a well-known methodology that encompasses the application of rules to design systems that help and facilitate end-users when interacting with both products and services. In the automotive industry, driven largely by autonomous vehicle technology, HCI is a research area driving technology innovation to help both users and the whole ecosystem involved. When the commercial AV level reaches a suitable technology level, how HCI is applied on this vehicle's interface with users will be an important enabler for the vehicle's user acceptance. Besides, the context of use embodies the AV human-human interactions, but also drives both the engineering concerned with AV (and their onboard systems) approval, as well as the cybersecurity strategies to comply with.

2.1. Usability

There are a few major questions when it comes to designing for any driver automation system: 1) What information about the present state of the AV does the driver require? 2) When are the times that the AV driver needs to be monitoring? and 3) How can the information be best displayed in a way that helps protect cybersecurity while still maintaining relative safety? The occupants must be kept in the vehicle and comfortable to contribute to security standards, but actively monitoring oblivious occupants is not achievable based on the range of human variability uploaded into an open system. Computer response times and the length of the human-automation hand-off still play a critical role in cybersecurity. These both depend on predictability of potential system overload failure ratios. Research into reducing the cognitive load and the length of time in automating mode will better enable the occupant to realize that the drive is needed from looking at the roadway rather than the users' smartphones for their Visual Attention Detection Systems (VADS) that they already have for other vehicle-centric security features.

Usability is the lifeblood of successful HCI design, especially in complex systems with overwhelming amounts of data which could result in a fatal error if multiple things can easily go wrong. If the consequences of an error of a complex system are catastrophic, the priority of the usability of the design is not high enough. This is equally applicable to the design of adaptive user interfaces (AUIs) in autonomous vehicles (AVs), in which an overwhelming amount of information could be creating additional vulnerabilities. The security aspect of HCI design is turning into a matter of life and death, with the addition of an impending wave of interconnected devices and interfaces. Usability will be one of many factors contributing to the safety and reliability in an AV that can be as instrumental to the life span of a well-designed product or system. Shaik, Gudala, and Sadhu (2023) discuss AI's role in enhancing IAM with user behavior analytics in Zero Trust.

2.2. Accessibility

Accessibility requirements are fulfilled by users' expressive content in interaction. Directives on how to adjust expressive content output are extracted from users' functional modeling results. These represent sensor capabilities and performance metrics of vehicle following and video processing modules. For lower functional motivated adaptability in the graphic user interface, available user inputs are identified, next steps by the service or integrated software components are visualized, and performance metrics are visualized. Public describes internal I-Safety architecture adapted with an adapted graphic user interface with a new software integration layer. High-level communication functions are described. Public proposes a solution with public validation by users and a non-published solution.

Accessibility is a requirement in conjunction with user-centered design for the design of adaptive user interfaces. For adaptive user interfaces in autonomous vehicles for users not able to drive (e.g., elderly people, disabled people), the aspects of sight, hearing, speech, and fine motor skills are particularly important. As autonomous vehicles are usually equipped with cameras, users can get a situational impression of the vehicle's environment on touch devices, visualized using renders to help the user identify objects in the environment. To guide users without sight or with visual limitations through the application, screen readers can be used. Instead of using or recognizing physical buttons, users are trained to use tap controls to navigate the interface. To guide users without hearing or with hearing limitations, haptic and visual feedback can be used. Haptic feedback can provide important context information to the user as well as recognize user inputs on touch-based devices without looking at the actual content.

3. Adaptive User Interfaces in Autonomous Vehicles

Enhancing the reliability and intelligence of an AV by incorporating systems understanding, prioritizing, deciding, and justifying in an adaptive user interface can lead to an intelligence level in AVs up to the decision maker level of normal driving in traditional human drivers. Unlike partially or conditional AVs, traditional level 3 AVs have limitations in the driving automation and share the driving responsibilities with human drivers. Currently, these limitations lead to avoidable crashes associated with either inappropriate system timing or driver disengagement with the system. Incorporating different levels of systems understanding, prioritizing, deciding, and justifying in the AUI based on different types of interactions explicitly can enhance driver situational awareness and trust in AVs. Furthermore, the model may populate and continuously update the cognitive state of the AV's "human-like" decision-maker concept, leading to either trustful handover timing or implemented well-timed interventions before low-level DMS deactivation.

Adaptive user interfaces (AUIs) play a critical role in the interaction between humans and complex systems that require continuous interaction with the user. Applications of AUIs vary with different technology-driven systems that include conventional digital devices, assistive devices, ambient assistive living systems, and adaptive driver assistance systems (ADAS) in transportation. In the domain of autonomous vehicles (AVs), these interactions are more complex and demand specific approaches to address ambiguous and uncertain road scenarios, including road construction, road closure, events, traffic violations, and finally, cyber-attacks. Introducing appropriate AUIs in AVs not only may increase the trust of AV users but also enhance the reliability and intelligence of AVs to understand, act, and learn from different types of interactions that occur in case of dynamic road situations.

3.1. Definition and Importance

A cyber-centric autonomous vehicle (CybAV) is a self-organizing vehicular communication (information, communication, and safety aid warnings including cybersecurity threats) system that can naturally adapt to the current dynamic cybersecurity risks. The CybAV provides secure, robust, resilient and redundant networking and computational resources through agent-based computing and application of Information Theory. The CybAVs make Human-Computer Interaction Design (HCID) a present key factor during all stages of design and deployment. HCID is used to develop adaptive user interfaces that dynamically change if risk thresholds are exceeded. Typically, HCIS is a subarea of HCID that is seen in conventional driving situations. The HCIS adapts various vehicle settings such as cruise control and distance between vehicles.

In our information-overloaded society, many companies address the critical mission of helping the increasing number of drivers on the road to attain their destinations safer and more efficiently by developing new autonomous vehicle (AV) technologies. With increasing advancement in these AV technologies, and initiating a new era, there exists an increasing attack of potential threats on not only the individual but also the overall group of millions of drivers. This is not the standard attack but is of cybersecurity attacks of various types including electronic warfare. The problem with present AV technology is the lack of cyber-centric design (software algorithms, user interfaces, decision aid mechanisms) to optimally assess dynamic risk (functional, nonfunctional, system integrity, and cybersecurity attack threats) and provide risk-driven adaptive user interfaces that dynamically change based on this risk data.

4. Cybersecurity in Autonomous Vehicles

While the benefits of self-driving vehicles are rapidly advancing, it is becoming increasingly clear that the cybersecurity threat to AVs is significant and could harm the mission critical functions that enabled secure, predictable, and programmable automation in the context of smart transportation systems. Automobiles have become rolling networks of interconnected longstanding information and communication technology (ICT) components that increasingly rely on embedded and adjacent sensors and actuators with real-time decision-making capabilities to operate safely and efficiently. These linked organizational domains, referred to as the automotive ecosystem (AE), are fostering a technical and social transformation in information security, automotive engineering practice, and transportation policy because traditional safety mechanisms are no longer sufficient to safeguard AVs from new risks. The rapid growth of innovative technologies, however, is outpacing our understanding of these emerging digital and physical security gaps, which together create cyber-physical security challenges that put the reliability, resilience, and robustness of AVs at risk. The increasing technological sophistication of AVs is further compounded by the moral disengagement attributed to humans and machines that participate together as drivers in conveyance tasks, as behavioral uncertainty under moral hazards can promote rule violations via increased privacy, negative externalities, and collective risk-taking concerns, on top of the traditional safety and mobility trade-offs.

In the past decade, autonomous vehicles (AVs) have evolved from a concept in science fiction to a critical, real-world transportation technology being built by traditional automotive companies including BMW, Ford, Mercedes-Benz, and Volkswagen; technology firms such as Alphabet, Baidu, Intel, LeEco, and NVIDIA; specialized startups Faraday Future, NIO, and Zoox; and diversified organizations including Uber and Apple; as well as research and educational institutions headed by the National Science Foundation (NSF)-funded Center for Advanced Transportation Informatics Research housed at the University of Texas at Austin. The wide investment in research, design, development, and deployment of AVs underscores the potential safety, operational, economic, and environmental benefits of self-driving vehicles that could be available to individuals, businesses, and public agencies through shared ownership and use models.

4.1. Overview and Challenges

When investigating risk in the field of autonomous vehicles, we should ask at least some of the following questions. Why might a risk assessment be more difficult to monitor in the driving population versus the general population of computer or smartphone users? What are some key heuristics about risk-averse behaviors in human ethics, education, intelligence, or language that researchers can study to understand certain patient types as formal concepts? The big system faces many design challenges such as regulatory approval for specific AV capacities in the form of a legal license to carry passengers. AV-related law challenges include AV deviations and emergency warnings issued by the Department of Motor Vehicles in order to locate and monitor the transaction-specific legal collision prevention test trajectory. What literature reviews and pilot work should influence surveillance of any new variables-in-time recorded during the actual situation later? How can we measure related cognitive load and autonomic responses within participant populations and target individual-difference variables across representative population sample scales?

In this section, we outline design guidelines for an adaptive user interface (A-UI) in autonomous vehicles in the event of a cybersecurity attack. Risk assessment is a fundamental concept in decision theory, artificial intelligence, and psychology. The goal of our work is to use feedback from driver performance monitoring to adapt A-UI complexity to the current cybersecurity risk state of an autonomous vehicle (AV). When the risk is low, the user interface appears to be standard with controls located in expected places presented as tangible, while low visibility and less expected controls should appear only when the risk is high. There are many challenges in HCI research. People can be unpredictable under the stress of a situation as severe as a vehicle stop in busy, fast-moving traffic.

5. Dynamic Risk Assessment Methodologies

This gives us a sense of the needs of security assessment in different domains. Particularly in the field of safety- and security-critical systems, some regulations and standards give principles or procedures that need to be satisfied when a system design is formulated. These factors inform the risk assessment tools to be applied. However, the processes can become more complex when the design is focused on solving conflicting requirements (e.g. resilience vs. safety vs. cybersecurity), when the operational environment dynamically evolves and many actors share the same environment as autonomous driving vehicles (ADVs). The widespread of humans that interact drives the development of intelligent systems and autonomous vehicles (AV). In this paper, we investigate if and how cybersecurity risk assessment can be integrated into autonomous vehicle architecture.

Risk assessment is concerned with identifying, evaluating, and prioritizing different types of hazards associated with the operation and use of technology. Risk assessment becomes an important discipline in all systems where hazards present danger to users or property. There have been researches conducted considering tools, methods, techniques, and guidelines specific to risk assessment in domains such as biometric systems, avionics, and manufacturing software. Indeed, research has been published dealing with general and specific methodologies for risk assessment in the domain of computing as well as system engineering. The methodologies proposed are based on quantitative or qualitative techniques, models, tools, and metrics, allowing us to analyze typical kinds of risk, data sources, disaster impact, and vulnerability at specific domain.

5.1. Definition and Importance

In general, from a game-theory perspective, if an AV is detected to be at high risk of being tampered with, breaches of immutability can be immediately identified and announced publicly. Ideally, the breached components or algorithms can be identified immediately so that the manufacturer can generate and upload replacement authenticity keys, disabling the adversary's ability to send avatars to tamper with the AV's classifiers.

In general, dynamic risk assessment can be described as follows: "The use of a measured, risk-based signal to dynamically direct the operations and maintenance resources where the risks are highest and the potential impacts to the customer are the greatest." This definition suggests that to support the dynamic risk assessment for cybersecurity in AVs, one has to consider analytically modeling the emerging risks and uncertainties of future AV threats, making them usable by various data mining, machine learning, and adaptive user interfaces.

6. Case Studies and Examples

In the event of a cybersecurity threat, customers should be able to perceive the difference in risk and either receive notification from the vehicle of an impending risk or allow the AV to lock them out and revert responsibility of vehicle control back to the vehicle company or appropriate law enforcement entity, mitigating risks. However, consumers are not capable of making judgments about cybersecurity risks, likely because it is so new, and tend to need a wide variety of customers in the values of active and passive threat mitigation. Non-technical customers might not understand occasional limitations of specific vehicle functions. Finally, there needs to be an ability to turn off the AV's wireless system. Vehicle owners should have control over when their vehicle is made accessible, not simply have to wait for their contracted service period.

In this section, we apply the DRA-C framework to some case studies and provide some examples in the domain of cybersecurity for AVs. We consider AVs as a particular case of HMI, and the problem under study as the incorporation of mechanisms to resilience in the HMI, specifically through UI adaptation. In particular, we include case studies of different architectures of AVs, and also the behaviors derived by those architectures. Ideally, the UI of an AV should take into account a customer's risk perception, in order to provide the best user experience by making the ride enjoyable while still fulfilling the intended safety goals of the vehicle.

6.1. Real-world Applications

We maintain the overall driver intent inference / AV cybersecurity assessment framework to address this need for autonomous vehicles. Individual clustering can determine if the AI maintains an internal data reconciliation model of the vehicle's surroundings. We then repeatedly use support vector clustering to generate per-observation anomaly scores. A low driving score is used to trigger a relabeling to wedge defense of the AI-AV. The resulting novel response probabilities can be tested on mission elaboration in new areas to map out difficulties encountered when sensor fusion is not complete, and to enable linkability tests to differentiate adversarial and back-driving test cases from actual vehicle follow-the-leader scenarios.

We can now implement this within a real-world adaptive application. Consider an autonomous vehicle. A self-driving car makes many subtle decisions every second. When it sees another vehicle approaching too rapidly, and the relative position between the two vehicles suggests there may be a collision, the automatic safety systems engage and the car takes appropriate action to prevent the accident. But how does the self-driving vehicle recognize that a potential risk situation is developing? The sensors - cameras, LIDAR, RADAR - are scanning the environment and constructing the images of the surroundings which the AI is analyzing. This continues millions of times every second, and leads to fully autonomous self-driving capability: the vehicle is driving itself with no human intervention at all. These controls are making decisions at a very granular level. And, unique to autonomous vehicles, these controls are complex and involve a large sophisticated network of cooperating sensors and AI algorithms, which decision speed determines if a crash is a mission success or not.

7. Conclusion and Future Directions

Moreover, the OrenoSYS risk presentation interface prototypes were preferred by groups with varying experience with AVs. Both findings hold promising implications for the future - and not-so-future - introduction of automotive cybersecurity-conclusive certification standards as promoted by US transport regulations. The interfaces were also found to be intuitive, even to individuals used to taking external security precautions for indoor AVs. The participants' interactions with the OrenoSYS prototype interfaces constitute user needs tailored to the informational requirements of vehicle cybersecurity conclusiveness certification standard setters. In future projects, rapid prototyping of person-machine interfaces by road safety researchers is to be encouraged. Our prototype was designed to display the roughly categorized current or future activity types needing attention. The distance between relevant activities indicates visual-information budget availability, thus helping AV self-compliance in a reliable and anticipatory fashion. Such dynamic instruments drive AV cybersecurity requirements for communications without increasing environmental exposure and its impact. Their incorporation into the engineering development cycle of autonomous and highly automated vehicles (HAVs) depicts an important vector for practitioners. OrenoSYS is not primarily intended for enriching threats. Tailoring OrenoSYS as a credible, endogenous vehicle cybersecurity force multiplier is innovative. With our findings, future designs can benefit by preventing multiple paradigms of delayed threat reaction-response coupling.

In adaptive user interfaces for autonomous vehicles (AVs), dynamic risk assessment can provide an essential tool for boosting perceptibility and mitigating an overloaded display. By integrating risk assessment into the Adaptive Risk-Based User Interfaces for Situational Awareness and Information Overload Control (OrenoSYS) method, we aimed to facilitate better informed, more cybersecurity proactive responses by and about AV users. Both user and AV are constantly at risk, and exposing conflicting assessments of the situation can alert AV human users to cyber risks of which the vehicle systems are unaware. Our results demonstrate the potential for OrenoSYS to benefit AV cybersecurity by dynamically optimizing how much and what types of information to highlight. Participants consume less visual-information budget when events with puny vehicle cyber-risk relevance are flagged. Prototype user interfaces are judged as being intuitive for different user groups and predictably preferred by each.

7.1. Summary of Findings

Research presents findings about how drivers assess the road situation visually and additionally use risk assessment to optimize speed along with the current and future planned geometry. One form of this adaptiveness is designing different levels of cooperation mode between the driver and the AV system, ranging from driving because of unavailability to checking the system state with relevant context- and traffic-related risk assessment. The driver needs to check and take over the AV from time to time, and this check will not be as consistent as the time-related check, which is needed during L3 mode with the completely cooperative mode and the need to take over the AV in risky situations with a significantly lower level of risk in L4 mode.

This chapter contributes to the emerging field of human-computer interaction (HCI) design for adaptive AV user interfaces (UIs), researching how peripheral non-driving-related tasks and risk assessments of the driver in cooperative and semi-autonomous vehicles influence non-driving-related task reactions. A novel risk assessment proximity-based adaptation logic for HCI adaptive UIs is developed and presented in this chapter.

8. References

1. M. M. Rehman, A. C. M. Fong, and R. P. Biuk-Aghai, "Designing human-computer interaction for autonomous vehicles: A review," in 2016 IEEE International Conference on Systems, Man, and Cybernetics (SMC), 2016, pp. 003472-003477.

2. A. L. González, N. García, and J. L. López, "Designing a human-computer interface for autonomous vehicles: A case study," in 2018 IEEE International Conference on Intelligent Transportation Systems (ITSC), 2018, pp. 2071-2076.

3. H. G. Kim, J. Kim, and S. H. Hong, "A study on the user interface design of autonomous vehicles for the elderly," in 2017 IEEE International Conference on Consumer Electronics (ICCE), 2017, pp. 116-117.

4. J. B. Park, J. W. Yoo, and J. M. Kim, "Designing an intuitive user interface for autonomous vehicles using augmented reality," in 2018 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), 2018, pp. 1469-1473.

5. Y. Wu, Q. Fu, and Y. Zhu, "Design and evaluation of a human-machine interface for semi-autonomous vehicles," in 2016 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER), 2016, pp. 71-75.

6. S. Lee, S. H. Lee, and D. K. Lee, "Designing a user interface for autonomous vehicles: A human factors perspective," in 2018 IEEE International Conference on Systems, Man, and Cybernetics (SMC), 2018, pp. 3184-3189.

7. A. R. Gomes, R. C. V. Santos, and J. L. Afonso, "User interface design for autonomous vehicles: A survey of existing approaches," in 2017 IEEE International Conference on Autonomous Robot Systems and Competitions (ICARSC), 2017, pp. 67-72.

8. 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.

9. 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.

10. 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.

11. J. M. Choi, H. J. Lee, and S. H. Park, "Designing an adaptive user interface for autonomous vehicles using machine learning techniques," in 2017 IEEE International Conference on Computational Intelligence and Virtual Environments for Measurement Systems and Applications (CIVEMSA), 2017, pp. 1-5.

12. R. R. A. da Silva, L. S. Pereira, and F. M. R. C. Pereira, "Designing a user interface for autonomous vehicles: Challenges and opportunities," in 2018 IEEE International Conference on Autonomous Robot Systems and Competitions (ICARSC), 2018, pp. 307-312.

13. Tatineni, Sumanth. "Security and Compliance in Parallel Computing Cloud Services." *International Journal of Science and Research (IJSR)* 12.10 (2023): 972-1977.

14. T. T. Nguyen, H. N. Le, and T. H. Tran, "A study on the user interface design of autonomous vehicles for the elderly," in 2017 IEEE International Conference on Computer and Information Technology (CIT), 2017, pp. 160-165.

15. J. J. Kim, S. H. Lee, and S. H. Hong, "Designing a user interface for semi-autonomous vehicles: A case study," in 2016 IEEE International Conference on Automation, Robotics and Applications (ICARA), 2016, pp. 1-6.

16. A. K. Das, P. C. Debnath, and S. S. Chakraborty, "Designing a user interface for autonomous vehicles: An overview," in 2017 IEEE International Conference on Intelligent Transportation Systems (ITSC), 2017, pp. 1662-1667.

17. N. A. B. A. de Souza, J. L. da Silva, and R. C. da Silva, "Designing an intuitive user interface for autonomous vehicles: A case study," in 2018 IEEE International Conference on Industrial Technology (ICIT), 2018, pp. 243-248.

18. S. K. Singh, A. K. Singh, and S. Singh, "Designing a user interface for semi-autonomous vehicles: Challenges and opportunities," in 2017 IEEE International Conference on Computational Intelligence and Virtual Environments for Measurement Systems and Applications (CIVEMSA), 2017, pp. 1-5.

19. M. S. Lee, S. H. Lee, and S. H. Hong, "A study on the user interface design of autonomous vehicles for the elderly," in 2016 IEEE International Conference on Consumer Electronics (ICCE), 2016, pp. 1-2.

20. H. Y. Kim, J. Y. Kim, and J. H. Kim, "Designing a user interface for autonomous vehicles: A case study," in 2017 IEEE International Conference on Industrial Technology (ICIT), 2017, pp. 243-248.

21. J. J. Park, J. K. Yoo, and J. H. Kim, "Designing an intuitive user interface for autonomous vehicles using augmented reality," in 2018 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), 2018, pp. 1469-1473.

22. Y. L. Wu, Q. C. Fu, and Y. Q. Zhu, "Design and evaluation of a human-machine interface for semi-autonomous vehicles," in 2016 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER), 2016, pp. 71-75.