*Human Interaction and Emerging Technologies (IHIET-AI)*, Vol. 201, 2026, 497–506
https://doi.org/10.54941/ahfe1007203

# Human-Centric Impacts of Cyberattacks on Autonomous Vehicle User Interactions: A Simulation-Based Study

**Shahzad Alam[1], Giedre Sabaliauskaite[2], Hesamaldin Jadidbonab[1], and Jeremy Bryans[1]**

[1]Centre for Future Transport and Cities, Coventry University, Coventry, CV1 5FB, UK
[2]Mykolas Romeris University, LT-08303 Vilnius, Lithuania

## ABSTRACT

Connected and Autonomous Vehicles (CAVs) are rapidly advancing toward SAE Levels 4 and 5, fundamentally reshaping human–vehicle interaction. As these systems become increasingly automated and connected, cybersecurity incidents introduce risks that extend beyond technical failure, affecting user trust, perceived safety, and acceptance. This study investigates how passengers respond when cyberattacks occur during an autonomous ride-hailing service. A driving simulator study was conducted with 50 participants, replicating a robo-taxi experience along a 5-mile urban route. Participants experienced three scenarios: a control scenario, a passive attack scenario and an active attack scenario. Following each scenario, participants evaluated their trust in the system, perceived safety, perception of risk, privacy assurance, and service intention. The results demonstrate statistically significant differences across the three scenarios. Passive attacks were associated with reduced trust and increased uncertainty, whereas active attacks produced stronger negative responses, including higher perception of risk and lower perceived safety. Participants also expressed concern about the reliability of the automated vehicle and their personal safety when abnormal behaviour occurred. Overall, the findings underscore that cyberattacks meaningfully influence how passengers evaluate the safety, reliability, and future adoption of autonomous mobility services. These results highlight the importance of integrating human-centric impact evaluation within cybersecurity risk assessment framework and the design of secure and trustworthy autonomous transport systems.

**Keywords:** Connected and Autonomous Vehicles (CAVs), Human–vehicle interaction, Cybersecurity, Human-centric factors, ISO/SAE 21434

## INTRODUCTION

Connected and Autonomous Vehicles (CAVs) are rapidly integrating into society, transitioning from conceptualization to global commercial phenomena that offer significant societal benefits, including reduced human error, optimized traffic flow, and enhanced mobility (Almusawi et al., 2024) (Park and Han, 2023). The automotive sector is progressing toward higher levels of automation, with SAE Level 4–5 vehicles capable of performing the full dynamic driving task within defined operational design domains (SAE, 2016). As automation increases (Figure 1), driving responsibility shifts from

Received December 31, 2025; Revised January 14, 2026; Accepted January 24, 2026; Available online April 1, 2026

the human driver to the vehicle system, fundamentally transforming human–vehicle interaction (Sun et al., 2018). Users transition from active drivers to passengers or supervisors who rely on automated decision-making and continuous connectivity.

This transition makes the acceptance and adoption of autonomous vehicles dependent on human-centric factors such as trust, perceived safety, perceived risk, privacy assurance, and intention to use (Park and Han, 2023) (Sitinjak et al., 2024) (Cao et al., 2021). In literature, there are several human-centric constructs which are particularly vital for widespread adoption of autonomous vehicles. Trust captures users' willingness to rely on automated systems under uncertainty and is essential for appropriate reliance when users no longer exercise direct control over vehicle behaviour (Holthausen, 2020) (Carsten and Martens, 2019). Perceived risk reflects subjective judgments about the likelihood and severity of potential negative outcomes and is typically negatively associated with trust (Payre et al., 2022) (Stuck et al., 2022). Perceived safety is a related but distinct construct, referring to users' subjective sense of how safe they feel when using the system, which may diverge from objective crash statistics (Cao et al., 2021) (Montoro et al., 2019) (Prasetio and Nurliyana, 2023). According to Cao et al., perceived safety is two-dimensional construct. Cognitive safety refers to rational evaluations of risk, controllability, and predictability and an Emotional safety refers to, capturing affective states such as feeling calm, reassured, or anxious when interacting with the vehicle (Cao et al., 2021). These two components have demonstrated unique causes and consequences, highlighting the necessity of measuring both when evaluating user response to incidents. Privacy assurance represent users' confidence that the system can protect personal data and prevent misuse, which is increasingly salient in connected services that process sensitive location, identity, and behavioural information (Prasetio and Nurliyana, 2023) (Cao et al., 2021). Service intention (Intention of use) represents the final behavioural outcome of these psychological evaluations reflecting willingness to use driverless ride-hailing services again in the future or recommend it to others. A high level of perceived safety and trust, alongside low risk and privacy concerns, are associated with a greater intention to purchase, use, or recommend the service (Cao et al., 2021).

It is evident from the literature that CAVs are susceptible to cyber-attacks and these vulnerabilities stem from three main trends (Abreu et al., 2025). The increasing complexity of vehicle software systems; the expanded connectivity resulting from integration into the Internet of Things (IoT) environment; and the increased value of embedded personal and sensitive data (e.g., location history, journey routes) (Khan et al., 2020). In response to escalating cybersecurity risks, automotive cybersecurity standard ISO/SAE 21434 (ISO, 2020) provides a structured framework for automotive cybersecurity risk management in which risk is typically defined as a function of attack likelihood and impact, and impact is primarily characterised in terms of Safety, Privacy, Operational, and Financial consequences. However, while technical vulnerabilities and system-level impacts are well documented, the subsequent impact of cybersecurity incidents on human-centric factors remains an open question.

Existing research in automated driving and human–machine interaction has examined trust calibration, perceived safety, and risk perception in relation to automation behaviour and interface design (Wintersberger et al., 2020). Yet, there is limited empirical studies on how cybersecurity incidents influence these human-centric factors during autonomous ride-hailing, and how such effects should be reflected in cybersecurity risk assessment.

This study addresses this gap through driving-simulator research that replicates a fully autonomous ride-hailing service. Participants experienced a baseline control scenario and two cyberattack scenarios, a passive attack and an active attack. Following each scenario, participants evaluated their trust in the system, perceived safety, perceived risk, privacy assurance, and intention to use the service. The study provides quantitative evidence that cybersecurity incidents exert statistically significant adverse effects on these human-centric factors.

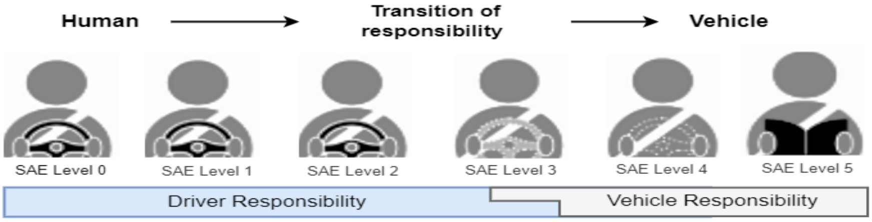

**Figure 1**: Transition of driving responsibility across SAE automation levels. The diagram illustrates the progressive shift in control authority from the human driver to the vehicle system as automation increases from SAE Level 0 to Level 5 (SAE, 2016).

## Method, Material and Experimental Procedure

The sample consisted of 50 participants ($N$ = 50), including 34 males (68%) and 16 females (32%). Participants were recruited via university mailing lists, online postings, and social media within the local academic and urban community and were screened for prior exposure to ride hailing services and basic familiarity with CAV concepts. Most participants were aged 21–30 years (62%, $n$ = 31), followed by 31–40 years (30%, $n$ = 15) and 41–60 years (8%, $n$ = 4). Regarding education, 56% ($n$ = 28) reported a master's degree and 24% ($n$ = 12) a doctoral degree, while 18% ($n$ = 9) held a bachelor's degree and 2% ($n$ = 1) reported a high school qualification. Driving experience varied, with 58% ($n$ = 29) reporting <5 years, 24% ($n$ = 12) reporting 5–10 years, and 18% ($n$ = 9) reporting >10 years. All participants held a valid driving licence and reported no history of simulator sickness or discomfort in virtual environments. Ethical approval was obtained from the Coventry University ethics committee, all participants provided informed consent, and all responses were anonymised.

The study was conducted using a high-fidelity driving simulator powered by XPI simulation software. The simulator comprised a full-body vehicle cockpit with a 220° panoramic, three-channel HD visual display (5760 × 1080 px, 60 Hz) and stereo audio output (2 × 20 W speakers). (Figure 2). Participants were seated in the front passenger position to replicate a passenger role in an autonomous ride hailing service. The virtual environment consisted of 3D replica of Coventry, and each scenarios followed a predefined urban route of approximately 5 miles. Passenger -vehicle interaction was provided via a 17-inch touchscreen tablet mounted on the centre console, serving as the primary HMI for authentication, ride initiation, trip monitoring, notifications, and an SOS function (Figure 2). The interface was implemented in Python and integrated with the simulator via a Hardware-in-the-Loop SDK, ensuring real-time synchronisation between user input, tablet events, and simulated vehicle behaviour.

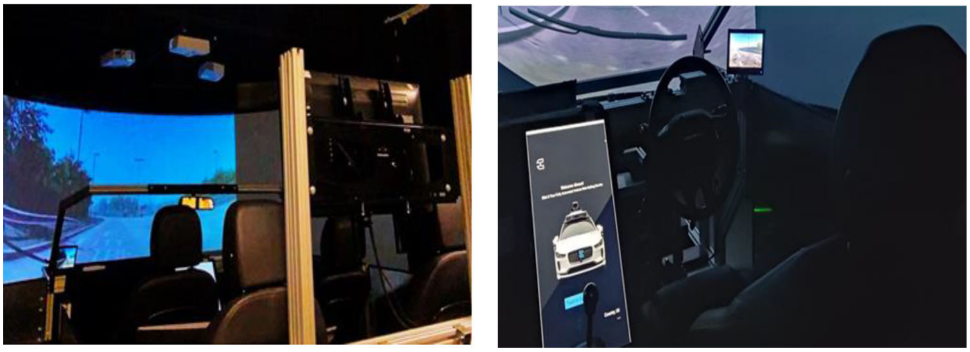

**Figure 2**: Experimental setup and human–machine interface. (left) Driving simulator setup view. (right) In-vehicle tablet interface used by participants to authenticate, initiate rides, monitor trip progress, and interact with the autonomous vehicle during the simulation.

A within-subjects design was used, in which each participant experienced three scenarios: Control (normal ride), Passive Attack (unauthorised route change), and Active Attack (ransomware lockout on the tablet). In the passive scenario, implemented as an unauthorised route change without explicit notification. In the active scenario, the tablet display froze and was replaced with a ransomware-style message demanding payment to resume the trip, following method described in (Wolf and Lambert, 2017) (Payre et al., 2022). The order of scenarios was counterbalanced across participants to control for order effects. Each scenario lasted approximately 10–12 minutes on the same 5-mile route. Participants were first briefed on the autonomous ride-hailing context and given a short familiarisation period with the simulator and tablet interface. After each ride, participants completed a post-scenario questionnaire during a 5-minute break. To reduce anticipation effects, key events were triggered either early or late during ride, and the full session lasted approximately 60–65 minutes including breaks and briefing/debriefing.

## Measures

After each scenario (Control, Passive Attack, Active Attack), participants completed a post-scenario questionnaire capturing five human-centric constructs, all rated on 5-point Likert scales (1 = Strongly Disagree, 5 = Strongly Agree) and adapted from validated scales in automated driving and human factors research.

Perceived safety assessed using a 6-item scale adapted from prior work (Cao et al., 2021) on safety perception in automated vehicles: items capture perceived safety during ride, including comfort with driverless operation and confidence in the AV's ability to anticipate hazards and respond appropriately. Trust in the automated system measured using the items adapted from Situational Trust Scale–Automated Driving (STS-AD) (Holthausen, 2020), capturing confidence in system safety and appropriateness of system behaviour, negatively worded items were reverse-coded prior to aggregation. Perception of risk was assessed using a 3-item scale adopted from prior work (Payre et al., 2022) applied in automated-driving malfunction/cyber context. Capturing perceived likelihood and severity of negative outcomes when using the automated driving system in the given scenario Privacy assurance assessed with four items scale reflecting confidence that the system's security mechanisms can protect personal data and prevent misuse, particularly in relation to ride, location, and identity data (Cao et al., 2021). Service intention (intention to use) measured using 3-item scale adapted from (Cao et al., 2021), capturing willingness to use, continue using, and recommend a driverless ride-hailing service.

For each construct and scenario, item responses were aggregated (mean score) to produce five dependent variables per participant, enabling within-subject comparisons across the three scenarios.

## RESULTS

Table 2 presents the descriptive statistics (Mean and Standard Deviation) for all dependent variables across the three scenarios: Control (C), Passive Attack (P), and Active Attack (A) and Figure 3 illustrates the corresponding mean trends. The Control condition established a baseline of normal user perception, while both cybersecurity scenarios elicited significant adverse changes in perception.

Perceived Safety showed the most pronounced decline, decreasing from the Control scenario ($M_C$ = 3.78, $SD$ = 0.53) to the Passive attack ($M_P$ = 2.64, $SD$ = 0.80) and reaching its lowest point in the Active attack ($M_A$ = 2.29, $SD$ = 0.97). Consistent downward trends were observed for Trust ($M_C$ = 3.42, $SD$ = 0.48, $M_P$ = 2.79, $SD$ = 0.55, $M_A$ = 2.62, $SD$ = 0.62) and Service Intention ($M_C$ = 2.98, $SD$ = 0.69, $M_P$ = 2.21, $SD$ = 0.76, $M_A$= 1.92, $SD$ = 0.86) indicating that exposure to cyber incidents reduced both confidence in the automated system and willingness to use the service. In contrast, Perception of Risk increased significantly under exposure to cyber incidents, rising from the Control scenario ($M_C$ = 2.57, $SD$ = 0.83) to Passive ($M_P$ = 3.50, $SD$ = 0.85) and Active ($M_A$ = 3.71, $SD$ = 1.09). Privacy concern also decreased ($M_c$ = 3.52, $SD$ = 0.38, $M_P$ = 2.88, $SD$ = 0.56, $M_A$ = 2.34, $SD$ = 0.65), indicating reduced confidence in data protection when cyber incidents occurred.

**Table 1:** Descriptive statistics (mean and standard deviation) for human-centric dependent variables across the three scenarios: Control (C), Passive Attack (P), and Active Attack (A).

| Dependent Variable | Count *(N)* | Control *M(SD)* | Passive Attack *M(SD)* | Active Attack *M (SD)* |
|---|---|---|---|---|
| Perceived safety | 50 | 3.78 (0.53) | 2.64 (0.80) | 2.29 (0.97) |
| Trust | 50 | 3.42 (0.48) | 2.79 (0.55) | 2.62 (0.62) |
| Privacy assurance | 50 | 3.52 (0.38) | 2.88 (0.56) | 2.34(0.65) |
| Perceived risk | 50 | 2.57 (0.83) | 3.50 (0.85) | 3.71 (1.09) |
| Service intention | 50 | 2.98 (0.69) | 2.21 (0.76) | 1.92(0.86) |

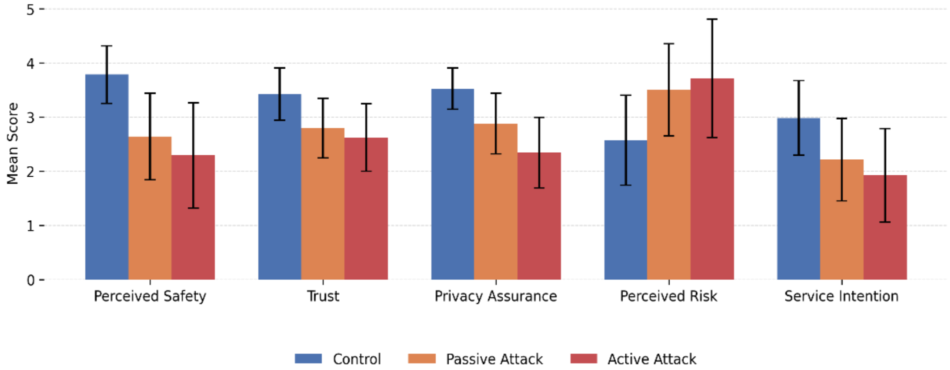

**Figure 3:** Comparison of mean scores (± SD) for human-centric factors across control, passive attack, and active attack scenarios.The results show a degradation in perceived safety, trust, privacy assurance, and service intention under cybersecurity attacks, alongside an increase in perceived risk.

To test whether these differences were statistically reliable, repeated-measures ANOVAs were conducted for each dependent variable (Table 2). The analyses revealed significant main effect of condition for all measures: Perceived Safety, $F$ (2,98) = 62.79, $p$ < .001; Privacy concern, $F$ (2,98) = 69.54, $p$ < .001, Trust, $F$ (2,98) = 31.74, $p$ < .001, Perception of Risk, $F$ (2,98) = 33.35, $p$ < .001 and Service Intention, $F$ (2,98) = 44.50, $p$ < .001. Overall, these results indicate that exposure to cybersecurity incidents had a statistically significant impact on users' safety perceptions, trust, risk perception, privacy confidence, and intention to use autonomous ride-hailing services.

**Table 2:** Results of repeated-measures ANOVA for the effect of scenario (Control, Passive Attack, Active Attack) on human-centric dependent variables.

| Dependent Variable | *F* Value | *P* Value |
|---|---|---|
| Perceived safety | *F* (2, 98) = 62.78 | *P* < .001 |
| Trust | *F* (2, 98) = 60.53 | *P* < .001 |
| Privacy concerns | *F* (2, 98) = 31.74 | *P* < .001 |
| Perceived risk | *F* (2, 98) = 33.35 | *P* < .001 |
| Service intention | *F* (2, 98) = 44.50 | *P* < .001 |

Given the significant main effects, Bonferroni-corrected pairwise comparisons were performed to examine differences between specific scenario pairs. For Perceived Safety, all comparisons were statistically significant: Control vs. Passive Attack: A significant drop occurred ($\Delta M$ = 1.14, $p$ < .001), Control vs. Active Attack: A larger significant drop occurred ($\Delta M$ = 1.49, $p$ < .001), Passive vs. Active Attack: A small but significant drop was noted ($\Delta M$ = 0.35, $p$ < .05) indicating a graded decline in perceived safety with increasing attack severity. For Trust and Perceived Risk, significant differences were found between the Control scenario and both attack scenarios (p < .001), but no significant difference was found between the Passive and Active attacks scenarios ($p$ > .05). This pattern suggests that the occurrence of any cybersecurity incident was sufficient to degrade trust and elevate perceived risk to a comparable level. In contrast, for Privacy assurance and Service Intention, significant differences were found across all three scenarios ($p$ < .05), indicating that active attack led to progressively lower confidence in data protection and reduced willingness to use the autonomous ride-hailing service as compared to passive attack.

## DISCUSSION

This driving simulator research explored the effects of cybersecurity incidents on key human-centric factors during an SAE Level 4–5 autonomous ride-hailing service. Overall, the results showed that both passive and active attack scenarios reduced trust, perceived safety, privacy assurance and service intention, while increasing perception of risk relative to the control scenario. These results were congruent with previous work identifying cyber threats as critical factor affecting negatively the adoption of autonomous vehicles (Payre et al., 2022) (Prasetio and Nurliyana, 2023) (Khan et al., 2020) (Seetharaman et al., 2021).

The simulation results demonstrated participants perceptions were significantly influenced by the presence and severity of cybersecurity attacks during the autonomous ride-hailing experience. The sharp decline in Perceived Safety and Trust (($p$ < .001) for control vs. attack scenarios) highlights a critical vulnerability in autonomous ride hailing service adoption. When the AV system's behaviour deviated from the expected normal operation (i.e., in the attack scenarios), participants confidence eroded rapidly. The fact that the Active Attack caused significantly lower safety perceptions than the Passive Attack. Participants felt less confident in the vehicle's ability to operate safely and uncomfortable during the ride. This suggests that conspicuous, explicit system failures trigger a more severe psychological disruption than silent anomalies. Conversely, for Trust there was no significant difference between the Passive and Active attacks. This implies once trust is violated even slightly, further severity does not significantly erode that trust further in the short term. Participants also reported Perception of risk significantly higher under attack exposure, indicating that cybersecurity incidents translated into higher perceived likelihood or severity of negative outcomes during the ride, even in a controlled simulator context. In parallel, privacy assurance decreased substantially, reflecting reduced confidence in the system's ability to protect personal information and heightened concern regarding potential unauthorised access, exposure, or misuse of passenger data under compromised scenarios. Service intention also decreased significantly in both attack scenarios, indicating a lower willingness to use autonomous ride-hailing in the future following cyber incident exposure. This finding was aligned with number of studies identifying cyber threats as critical factors affecting negatively human-centric factors in autonomous vehicles (Seetharaman et al., 2021) (Cao et al., 2021) . Importantly, the present study extends this evidence to an autonomous ride-hailing context.

These findings are particularly relevant in the context of increasing vehicle automation, where human–vehicle interaction has transitioned from direct control to reliance on automated decision-making. This transition fundamentally redefines user interaction with autonomous systems and elevates the importance of trust, perceived safety, and perceived risk as key determinants of acceptance of autonomous mobility services. As autonomy and connectivity increase, the consequences of cybersecurity incidents extend beyond functional degradation to directly influence user perceptions. The results of this simulation-based study showed that cybersecurity incidents had significant adverse effects on key human-centric factors, underscoring their importance within cybersecurity risk assessment for SAE Level 4–5 vehicles. Given that risk is conventionally defined as a function of attack likelihood and impact, and that ISO/SAE 21434 primarily characterizes impact in terms of Safety (physical), Privacy, Operational, and Financial consequences, these findings support integrating human-centric impact analysis alongside these established impact categories. Incorporating human-centric impacts into cybersecurity risk frameworks is therefore essential to support the safe and trustworthy integration of CAVs into society.

This study has certain limitations. First, the outcomes were captured using self-reported measures within a driving simulator, which may not fully reflect the complexity and consequences of real-world autonomous vehicle operation. Second, the participant sample was skewed toward younger and highly educated individuals, which limit generalisability to broader user populations. Third, the analysis was limited to two representative cyberattack types. Future work will extend this investigation by considering additional attack vectors and mitigation strategies, and by incorporating behavioural and physiological measures to complement subjective self-reports.

## CONCLUSION

This study investigated the effects of cybersecurity incidents on human-centric factors in an SAE Level 4–5 autonomous ride-hailing context using a driving-simulator experiment. A control scenario was compared with two cyber incident scenarios: a passive attack (route manipulation) and an active attack (ransomware-style attack). The results demonstrated that both incidents significantly reduced perceived safety, trust, privacy confidence, and intention to use, while increasing perceived risk, relative to control scenario. Overall, the findings indicate that cybersecurity incidents undermine the human-centric factors required for user reliance on highly automated mobility services. These findings are important for an automotive cybersecurity risk assessment, the results show that the impact of cyber incidents extends beyond the conventional impact categories (safety, privacy, operational, and financial). Cybersecurity risk assessment for SAE Level 4–5 CAVs where users rely heavily on vehicle automated decision making and continuous connectivity, should incorporate human-centric impact alongside established impact categories to enable a holistic approach to risk management, and support the safe and trustworthy integration of CAVs into society.

## REFERENCES

Abreu, R., Branco, F., Reis, M. J. & Serôdio, C. 2025. Cybersecurity in Connected and Autonomous Vehicles: A Systematic Review of Automotive Security. *IEEE Access*.

Almusawi, A., Albdairi, M. & Qadri, S. S. S. M. 2024. Integrating Autonomous Vehicles (AVs) into Urban Traffic: Simulating Driving and Signal Control. *Applied Sciences,* 14, 8851.

Cao, J., Lin, L., Zhang, J., Zhang, L., Wang, Y. & Wang, J. 2021. The development and validation of the perceived safety of intelligent connected vehicles scale. *Accident Analysis & Prevention,* 154, 106092.

Carsten, O. & Martens, M. H. 2019. How can humans understand their automated cars? HMI principles, problems and solutions. *Cognition, Technology & Work,* 21, 3–20.

Holthausen, B. E. 2020. Development and validation of the situational trust scale for automated driving (STS-AD).

ISO, S. 2020. ISO/SAE DIS 21434: Road vehicles—Cybersecurity engineering. *Draft International Standard*.

Khan, S. K., Shiwakoti, N., Stasinopoulos, P. & Chen, Y. 2020. Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions. *Accident Analysis & Prevention,* 148, 105837.

Montoro, L., Useche, S. A., Alonso, F., Lijarcio, I., Bosó-Seguí, P. & Martí-Belda, A. 2019. Perceived safety and attributed value as predictors of the intention to use autonomous vehicles: A national study with Spanish drivers. *Safety Science,* 120, 865–876.

Park, J. & Han, S. 2023. Investigating older consumers' acceptance factors of autonomous vehicles. *Journal of Retailing and Consumer Services,* 72, 103241.

Payre, W., Perellomarch, J., Sabaliauskaite, G., Jadidbonab, H., Shaikh, S., Nguyen, H. & Birrell, S. 2022. Understanding drivers' trust after software malfunctions and cyber intrusions of digital displays in an automated car.

Prasetio, E. A. & Nurliyana, C. 2023. Evaluating perceived safety of autonomous vehicle: The influence of privacy and cybersecurity to cognitive and emotional safety. *IATSS research,* 47, 160–170.

Sae, T. 2016. Definitions for terms related to driving automation systems for on-road motor vehicles. *SAE Standard J,* 3016, 2016.

Seetharaman, A., Patwa, N., Jadhav, V., Saravanan, A. & Sangeeth, D. 2021. Impact of factors influencing cyber threats on autonomous vehicles. *Applied Artificial Intelligence,* 35, 105–132.

Sitinjak, C., Simic, V. & Pamucar, D. 2024. Psychological factors shaping public acceptance of the adoption of autonomous vehicles in Indonesia. *Journal of Transport & Health,* 34, 101726.

Stuck, R. E., Tomlinson, B. J. & Walker, B. N. 2022. The importance of incorporating risk into human-automation trust. *Theoretical Issues in Ergonomics Science,* 23, 500–516.

Sun, X., Chen, H., Shi, J., Guo, W. & Li, J. From hmi to hri: Human-vehicle interaction design for smart cockpit. International conference on human-computer interaction, 2018. Springer, 440–454.

Wintersberger, P., Nicklas, H., Martlbauer, T., Hammer, S. & Riener, A. Explainable automation: Personalized and adaptive UIs to foster trust and understanding of driving automation systems. 12th International Conference on Automotive User Interfaces and Interactive Vehicular Applications, 2020. 252–261.

Wolf, M. & Lambert, R. Hacking trucks-cybersecurity risks and effective cybersecurity protection for heavy duty vehicles. Automotive-Safety & Security 2017-Sicherheit und Zuverlässigkeit für automobile Informationstechnik, 2017. Gesellschaft für Informatik, Bonn, 45–60.