"*Right Now, It's the Wild West*": Qualitative Insights into the Security, Privacy, and Safety of Teleoperated Connected and Autonomous Vehicles (CAVs)

Yichen Luo*, Victor Olaiya*, Sidi Lu, Adwait Nadkarni
William & Mary
{*yluo11, voolaiya, sidi, apnadkarni*}*@wm.edu*

***Abstract*—Commercial connected and autonomous vehicles (CAVs) are limited to specific routes or areas. When CAVs enter unfamiliar environments or experience system failures, they may stop autonomous driving, a process known as disengagement. Disengagement generally triggers "teleoperation", i.e., where a human operator remotely controls the CAV to guide the driving. However, there is very little knowledge about the teleoperation landscape and the security and privacy challenges therein. To bridge this gap, this paper presents the first qualitative, interview-based study (n = 16) involving experts engaged in the development and deployment of CAVs and teleoperation technologies. Our qualitative analysis yields 17 key findings ($\mathcal{F}_1$ – $\mathcal{F}_{17}$) that reveal critical flaws in teleoperation due to the lack of operational frameworks and regulations. We distill our findings into four themes that highlight the security and privacy challenges in teleoperation, propose actionable access control enhancements to address them, and motivate key areas for regulatory intervention.**

1. Introduction

Despite the rapid advancements of connected and autonomous vehicles (**CAVs**), full autonomy remains elusive due to ongoing technical challenges and unpredictable conditions [1]. In unfamiliar settings, a CAV's autonomous mode may deactivate if an autonomous technology failure is detected or safe operation cannot be ensured, a process known as CAV **disengagement** [2], [3]. Disengagement is not uncommon in practice, e.g., in 2023 alone, six major CAV companies reported approximately 6,570 disengagements in California [4].

To solve these problems, companies, such as Google Waymo [5], General Motors (GM) [6], Toyota [7], Uber [8], Aptiv [9], Motional [10], Drive.AI [11], Aurora [12], Zoox [13], offer **teleoperation** solutions, which *engage the assistance of a remote human teleoperator in scenarios that CAVs cannot manage independently* [14], [15], [16], [17], [18], [19], [20], [21], [22], [23], as illustrated in Figure 1. A recent example is Baidu's driverless robotaxi program, which includes nearly 500 autonomous taxis, covering 35% of the city's roads and handling 55% of ride-hailing services [24]. Teleoperation supports these vehicles when needed, with one operator supervising up to three taxis. The resulting traffic data and interventions are also useful for improving the autonomous driving systems [2].

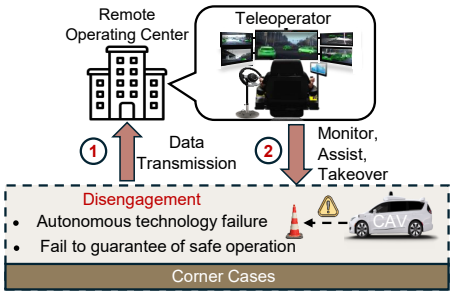


Figure 1: An overview of the teleoperation framework, which integrates CAV and the remote operation center.

While teleoperation in CAVs has its benefits, it also carries significant security, privacy, and safety risks. Particularly, teleoperated vehicles operate in open, public, environments. Any malfunction, misuse (e.g., by a malicious teleoperator), or compromise (e.g., via a compromised communication channel) may be exploited to endanger pedestrians, passengers, and surrounding traffic. Regulators have begun to recognize these risks: Germany recently prohibited teleoperators from exercising *full remote control*, while still allowing discrete commands [25], [26]. By contrast, California, despite substantial CAV adoption [27], mandates teleoperation for field testing new CAVs [28] without addressing the associated risks or specifying restrictions. This fragmented and ad-hoc regulatory response is a symptom of a ***critical knowledge gap***: despite its growing usage in CAVs and elevated risk, there remains a very limited understanding of the teleoperation landscape, including *the design and capabilities of teleoperation systems, and the security, privacy, and safety challenges they face*.

Contributions. To address this gap, this paper presents a qualitative, interview-based, study with 16 expert practitioners from industry and academia who have extensive experience in designing (10/16), deploying (13/16), testing (10/16), and real-world operation (5/16) of CAV teleoperation systems. We explore expert perspectives on why teleoperation is required, the functions and capabilities of the teleoperator, the security, safety, and privacy threats and risks in teleoperated CAVs, and the role of regulations in safeguarding against the risks.

*. These authors contributed equally to this work.

Most participants have over a decade of relevant experience spanning domains including vehicle security, control systems, edge computing, and privacy-preserving CAV systems, with some exceeding *thirty years* in experience.

Moreover, our experts from industry hold senior and influential roles in the automotive sector, including those of Founder/CEO, Associate Vice President, senior engineer, and R&D staff, while those from academia possess significant research expertise focused on CAVs and teleoperation. Together, our 16 experts provide perspectives grounded in practice across commercial, academic, and regulatory contexts. Our interviews and analysis are guided by the following ***key research questions (RQs)***:

RQ$_1$: *What challenges lead to autonomous-mode disengagement in CAVs, and what mitigation strategies are currently employed*? Teleoperation is typically activated when a CAV disengages; hence, understanding disengagement is fundamental to security, privacy, and safety analysis of teleoperated CAVs. We seek to understand the main causes of disengagement and any other mitigation strategies, in order to establish a baseline for where, when, and why teleoperation must intervene.

RQ$_2$: *What are domain experts' expectations regarding the functions and capabilities of teleoperators*? We seek to understand how experts perceive access control in this domain, i.e., which controls are essential, which sensor feeds should be restricted, and under what conditions remote intervention is appropriate. Capturing expert expectations will help identify the capabilities teleoperators should possess, uncover the human-level threat surface that we must address, and highlight areas where standardization and regulation are urgently needed.

RQ$_3$: *How do domain experts characterize the security threats in teleoperated CAVs*? Teleoperation broadens the already complex CAV attack surface and increases vulnerabilities by introducing continuous connectivity, remote control channels, and additional human actors. Yet these security risks remain unevenly recognized and poorly managed. We seek to capture expert perspectives on diverse challenges, including wireless interception, insider threats, and physical and procedural weaknesses in teleoperation, and understand where and why current ad hoc practices fall short.

RQ$_4$: *How do domain experts view the overall privacy challenges of teleoperated CAVs*? Teleoperation expands both the scope of data exposure and the number of entities involved, introducing privacy challenges that exceed those traditionally associated with CAVs. We seek to understand expert perspectives on privacy concerns in teleoperation, considering all the sensors available in teleoperated CAVs, to obtain insights that guide safeguards, consent mechanisms, and policy interventions to enable privacy-preserving teleoperation in real-world contexts.

RQ$_5$: *What role do regulations play in safeguarding security, privacy, and safety in the CAV and teleoperation ecosystem*? Regulation serves as the final safeguard when technical and organizational controls prove insufficient. We seek to understand the regulations governing teleoperation, i.e., if clear, binding, regulations, exist, and how they affect system design and industry norms.

2. Background

This section provides an overview of teleoperation, and describes the three roles of the teleoperator. When a CAV encounters a blocked path, it triggers disengagement and sends a request to a teleoperator [29]. The teleoperator establishes communication with the vehicle and reviews onboard camera feeds to determine whether the obstacle is passable. If the vehicle can proceed, the operator may reroute, adjust the trajectory, or directly maneuver the CAV, after which autonomy resumes. If the obstacle persists, the teleoperator notifies passengers and coordinates with authorities to clear the blockage. Teleoperators fulfill three primary roles [26]:

1. Remote monitoring: Teleoperators oversee CAVs in real time using data from sensors like cameras, LiDAR, and Radar. This data, securely transmitted to a remote center, allows teleoperators to monitor traffic patterns and stay updated on road closures, construction, or obstacles, ensuring effective oversight and decision-making.

2. Remote assistance: Teleoperators assist in ambiguous scenarios. When a CAV encounters unfamiliar conditions, it enters a Minimum Risk Condition (MRC) state [30]; the teleoperator then assesses the environment and determines whether continued operation is safe. Beyond this safety decision, teleoperators may issue high-level commands, answer passenger questions, plan routes, flag road closures, treat low-traffic regions as inaccessible rather than optimal routes, and share relevant updates with other CAVs [31]. Companies including GM's OnStar Crisis Assist, Zoox, AnyConnect, and Sensible4 already provide 24/7 remote support [19].

3. Remote takeover: The operator may remotely take over the dynamic driving task for a period of time [32]. Companies like Zoox and Einride implement remote takeover in specific scenarios or locations, with practices ranging from EasyMile's low-speed shuttles (<25 mph) to Designated Driver's high-speed demonstrations [29].

3. Methodology

This section outlines the interview protocol and guide. In addition, we discuss the qualitative data analysis and limitations of our work. Using a semi-structured interview [33], we gathered insights from stakeholders in the automotive industry, including engineers and researchers responsible for designing and implementing critical components in CAVs. The study was shaped by the combined industry and academic expertise of both the CAV/teleoperation and systems security teams, grounding the interview design, coding, and analysis in teleoperation's practical realities while yielding findings and implications relevant to the security community.

3.1. Interview Protocol

We developed questions regarding our ***RQs*** for our pilot interviews. In addition, we reviewed prior work in teleoperation [26] and vehicle security [34], [35], [36] to identify critical security areas. This section describes the pilot, recruitment, interview process, and ethical considerations.

1. Interview Pilot: We conducted pilot interviews with three participants, i.e., one expert in CAVs and two graduate students with usable security research experience. We incorporated their feedback, refined our questions, and added more clarification, where necessary. Based on our semi-structured interview approach, we designed open questions that transition to more focused questions to explore specific topics in-depth as necessary, following standard practices.

2. Participants Recruitment: We recruited 16 participants both directly and through snowball sampling via our professional networks. This approach suits CAV teleoperation, an emerging domain with a small, specialized community of industry and academic experts who focus on critical components of teleoperation systems (e.g., end-to-end communication, simulation frameworks and testbeds, remote assistance, ECUs). Eligibility required extensive past or ongoing experience with teleoperation and/or CAV areas central to our study, particularly security. We initially assessed expertise using institutional webpages, CVs, and LinkedIn, then verified and characterized each participant's expertise at the start of each interview.

All participants are based in North America and bring substantial domain expertise, averaging over 13 years of automotive-industry experience. Recruitment was guided by thematic saturation [37]. We systematically tracked the emergence of new codes and themes after each interview. We conducted interviews until no new themes or codes emerged; specifically, the final three interviews did not yield new codes, which we interpreted as strong evidence that thematic saturation had been reached. We compensated participants with a $50 gift card.

3. Ethical Considerations: Our study was approved by our Institutional Review Board (IRB). We audio-recorded all interviews, used a locally-hosted transcription service, and deleted audio recordings after their transcription. Participants accepted a consent form before participating in our study. At the beginning of each interview, a summary of the consent form was reexamined and participants were further encouraged to ask any questions or express any unaddressed concerns. We also emphasized that participants had the right to skip questions or terminate the interview at any time. Participants were informed that all information collected during the interview would be anonymized, and all private information willingly shared would be de-identified, e.g., if a participant mentioned a company name, we use <company-name> in its place in this paper. We discuss further ethical considerations in detail in the Appendix.

4. Interview Process: We used a lead-interviewer approach with one additional shadow interviewer always present during the interview. All interviews were conducted in English language and on Zoom. Participants were provided with a meeting invitation and consent form at least 24 hours in advance. As previously mentioned, at the start of the interview, we briefly reminded the participant of their rights, discussed a summary of the consent form, informed participants that the interview would be recorded and transcribed, and that the recordings would be destroyed after analysis. Additionally, in cases where we asked yes/no style questions, open-ended follow-ups were used to seek further details, explanations, and examples. On average, the duration of each interview was 56 minutes.

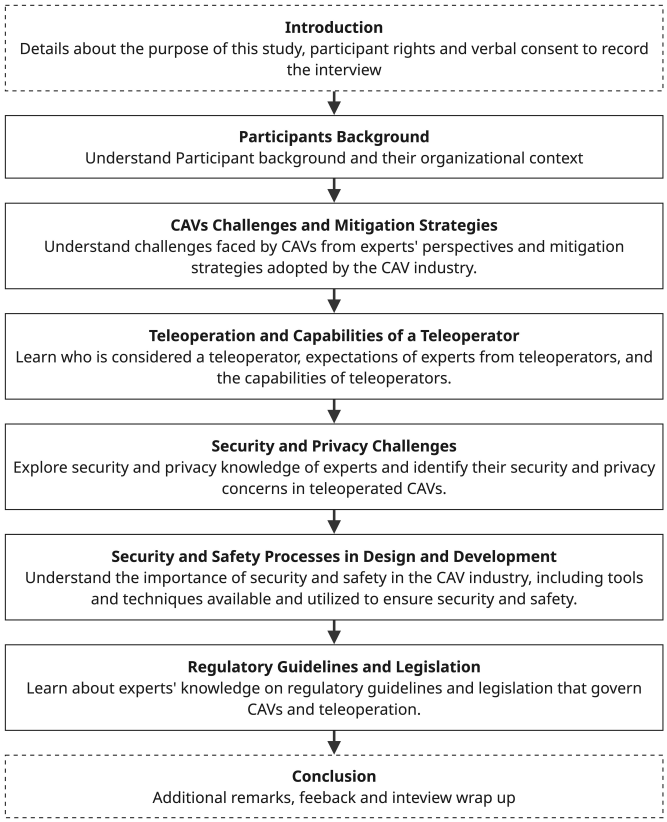


Figure 2: Overview of the interview guide.

3.2. Interview Guide

As previously described, the interview guide was designed via a collaborative effort of all authors, who are domain experts in autonomous vehicles and security. The design of the interview guide was motivated by our research questions, $\mathbf{RQ}_1$ – $\mathbf{RQ}_5$, introduced previously in Section 1. The draft list of questions was iteratively modified and discussed, and in the process, reorganized into relevant topic areas. The pilot interviews led to further refinement to improve clarity. The final interview guide can be found in our online appendix [38]. Figure 2, shows the six topics covered in our interview guide, described as follows:

1. Participant Background: To create a comfortable in-

terview environment, we began with questions about participants' backgrounds, experiences, and organization. We asked about their roles and responsibilities in the automotive industry. This information guided our follow-up questions.

2. CAV Challenges: Next, we presented participants with a common but challenging scenario for a CAV operating in urban environments, where a CAV gets stuck on the road due to construction or traffic cones. We then asked questions about why such scenarios are challenging for CAVs, and how they may be mitigated. Note that at no time did we mention teleoperation, but participants unanimously identified it as a resolution, as we discuss in Section 4.

3. Teleoperation & Capabilities of a Teleoperator: This examines the role of teleoperators and participants' expectations of them. We also asked about the key capabilities of a teleoperator, such as monitoring the CAV, and access to sensors and functions relevant to the security of the CAV and privacy of the passengers.

4. Security & Privacy Challenges: We asked experts about security and privacy challenges and concerns in using teleoperation. Additionally, we asked about the experts' perception of a stronger threat model for teleoperators, where we consider possible insider adversaries.

5. Security & Safety Processes in Design and Development: We asked participants about the importance of security in the design and development process in their respective organizations, infrastructural challenges that may affect teleoperation, and the possible ways to mitigate these challenges. We asked about security and safety testing procedures, tools, and techniques that participants use in their development process. We also asked about unusual and unexpected results participants may have observed while testing. We also discussed CAV data collection, its intended uses, and how such data is protected at rest and in transit.

6. Regulatory Guidelines & Legislation: Finally, we asked the experts about their perspective on the state of regulations that govern CAVs and teleoperation. We asked about the precise regulations and laws they have to comply with, including the certifications and training processes for teleoperators. We also asked about organizational regulations, guidelines, and practices, including security and safety regulations. We concluded by discussing liability, damages, and privacy violations involving teleoperators.

3.3. Transcription, Coding, and Analysis

We used a locally hosted Whisper [39] instance to transcribe the interview recordings, and manually reviewed all transcripts for completeness and accuracy, anonymizing any identifiable information. We then qualitatively analyzed the transcripts using MAXQDA [40]. We adopted an inductive coding approach [41], allowing codes and themes to emerge directly from the data. Two coders with CAV and security expertise first jointly coded one transcript to develop a preliminary codebook through negotiated agreement; accordingly, we did not rely on inter-rater reliability measures [42]. Using this codebook, both coders independently and iteratively coded all transcripts, meeting 2-3 times weekly to discuss new codes, resolve differences, refine the codebook, and discuss emerging themes.

To ensure the reliability of our analysis, we employed a negotiated agreement approach to inter-coder reliability [42], which is well-suited for inductive qualitative studies where codebooks evolve during the analysis process. At the end of this process, both coders jointly revisited all transcripts and the codebook to confirm that all transcripts were accurately and consistently coded. After creating the codebook and identifying initial themes, the coders refined the identified themes through iterative discussions with the broader research team, to avoid any confusion and bias. The codebook can be found in our online appendix [38].

3.4. Limitations

As with any qualitative study, our work is subject to several limitations that we discuss transparently to enable readers to assess the reliability of our findings. We recognize that participant responses may be subject to self-reporting bias, including potential under-reporting or over-reporting. However, these risks are mitigated by the depth and specificity of the examples shared, grounded in substantial professional experience (see Table 1).

Our qualitative findings may not generalize to the entire CAV industry or to regions such as Europe and Asia, since all experts have worked only in North America. However, considering our participants' current roles and years of experience, our study and results can be considered highly reliable. Additionally, many of our participants work for multinational companies with global operations, which broadens the applicability of their perspectives.

Participants had the option to opt in to receive monetary compensation; however, we did not disclose the monetary value to ensure interest-driven participation and prevent participants from consciously or unconsciously calibrating their responses based on the perceived value. After each interview, a $50 Amazon eGift Card was sent by email to participants who opted to receive compensation.

4. Results and Findings

This section presents findings from our thematic analysis of 16 semi-structured interviews. After describing participants' backgrounds, we organize our 17 findings into themes that emerged from our inductive analysis. Each theme is grounded in convergent perspectives from multiple participants. Given the qualitative nature of our analysis, we deliberately refrain from absolute quantitative interpretation of our findings. Rather, we adopt a widely employed convention from prior work [43], [44] where we used proportional descriptors, i.e., few, many, and most are used to characterize the distribution of participant responses, the mapping for which is presented in Fig. 3.

Summary of Participants and Organizations: Our 16 experts span industry (n=9) and academia (n=7), representing

TABLE 1: Overview of the Interview Participants.

ID	Current Role	CAV-specific Area of Expertise	Notable Role Previously Held	Industry experience	Academic experience	Total Experience
P1	Senior Engineer	AD, Software	–	7 years	15 years	15 years
P2	Department Chair	Edge Computing, AD	AV Strategic planning committee	3 years	30 years	30 years
P3	Assistant Professor	Vehicle Health Management	Senior Researcher Global Research and Development	16 years	7 years	23 years
P4	Research Associate	Human Factors in Transportation Safety, Freight Vehicle Safety	Aircraft Engineer	1 year	6 years	7 years
P5	Data Scientist	Connected Vehicle Data Analysis	Research Scientist	5 years	8 years	13 years
P6	Senior Engineer	Autonomous Vehicle	Senior Researcher	6 years	6 years	12 years
P7	Senior Engineer	ADAS Feature Design, ECU Validation, Middleware	AD and Active Safety System Lead Engineer	12 years	8 years	12 years
P8	Assistant Professor	CAV, V2X Communication	–	1 year	9 years	10 years
P9	Assistant Professor	CAV, Internet of Things (IoT), Extended Reality	–	2 years	8 years	10 years
P10	Associate Professor	Vehicle Security, Cybersecurity	Research Scientist	2 years	17 years	17 years
P11	Assistant Professor	Cyber-Physical Systems, Security	–	–	7 years	7 years
P12	Associate Professor	AV, EV, Control Systems	Senior Control Systems Engineer, Vehicle and Propulsion Control	6 years	10 years	16 years
P13	Founder/CEO	AD, Robotics	AV Safety Operator	5 years	6 years	6 years
P14	Technical Delivery Manager	AV, ADAS	–	13 years	–	13 years
P15	Research and Development Staff	Digital Twin, Cybersecurity for CAV	Post-Doctoral Researcher	1.5 years	5 years	6.5 years
P16	Assoc. VP of App Development	Vehicle Software, AV	Sr. Technical Manager	13 years	–	13 years

Abbreviations: AD = Autonomous Driving, AV = Autonomous Vehicle, CAV = Connected and Automated Vehicle, ADAS = Advanced Driver Assistance Systems, ECU = Electronic Control Unit, EV = Electric Vehicle, V2X = Vehicle-to-Everything.

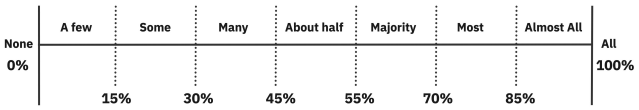


Figure 3: The quantifiers and respective participant percentage ranges used to describe the results and findings.

diverse roles and organizational contexts across the CAV ecosystem, as seen in Table 1. Many have worked across both academia and industry in multiple CAV-relevant roles, particularly in cybersecurity, privacy, and safety-critical system design. For example, **P4** previously worked in aerospace and now focuses on commercial autonomous trucks and heavy vehicles, examining human-factors-driven cybersecurity risks. **P9** has designed edge-computing systems in both a major CAV organization and a research institution, informing secure and scalable teleoperation architectures. **P12** specializes in privacy-preserving CAV systems and formerly worked as a senior control systems engineer in vehicle propulsion control, and **P13** is the founder and CEO of an autonomous vehicle company with prior academic experience. Overall, 14/16 of our participants had direct, extensive research and/or industry experience with CAV teleoperation systems, including 5 with real-world operational experience. These counts are conservative, e.g., **P12** designed and tested teleoperated CAVs, controlling the CAVs with VR and cameras; but we did not count that toward "operating" as we limit that to real-world operation (e.g., **P13**'s role as a "safety driver"). **P10** and **P11** lacked direct teleoperation experience but they were included based on extensive CAV security expertise with real CAV testbeds, which is directly relevant to teleoperation security.

4.1. Necessity, and Operational Challenges

Experts highlighted several real-world scenarios that CAVs face, such as construction zones, detours, dense pedestrian traffic, and narrow roads. This unpredictability of road conditions cannot be mitigated in the near term, as there is very little training data for such scenarios. In such scenarios, CAVs may ***disengage***, i.e., abruptly stop and deactivate the autonomous mode if safe operation cannot be ensured. Experts noted that there is **no reliable way to prevent disengagement**, i.e., *"no matter how good of your driving algorithms, you're still going to be in a situation you can't really...don't really know how to handle"* (**P2**).

More importantly, experts overwhelmingly emphasized the importance of *human intervention* to recover the CAV in such challenging scenarios. Particularly, majority of experts stated that these challenging edge cases can be addressed using *remote* human intervention, or ***teleoperation***. A quote from **P13** highlights the critical role of teleoperation in ensuring safe CAV operation:

> *"...**It's a basic function** for all the autonomous vehicles or robotics. And I think even without this function, the robots shouldn't be on the road."* — P13

P4 explained that remote operators could either guide CAVs by suggesting potential paths or take direct control via ***remote driving***. This approach, according to **P4**, is gaining traction within both government and industry, and **P4** cited an example of a company that operates a large-scale remote driving hub, stating:*"<company-name>, ...*

they have a whole driving, remote driving hub with like a hundred remote driving station with a human that actually can provide direct <remote> driving control...".

Similarly, **P13** states that teleoperators can also be thought of as ***supervisors***, and having such remote supervision takeover CAVs is a common practice:

> *"<company-name> are doing robotics delivery, like delivery food with small robots. But from our experience, we have seen that a lot of takeovers happen on that robot. For example, if a robot runs into a construction area...your little robot will trip in that zone. And the many supervisors behind the robot will just take over..remotely control the robot."* — P13

P7 supports this view, adding that teleoperation can help manage unpredictable situations, since present CAVs are neither trusted nor trustworthy. They argue that human drivers or remote operators remain the benchmark due to their adaptability to unexpected conditions. These discussions bring us to the first key finding:

Finding 1 ($\mathcal{F}_1$) – All experts note that CAVs face persistent challenges in real-world adaptability, and while improved data and training help, they are not sufficient on their own. Thus, majority of experts widely agree that **teleoperation is a necessary and practical function** that enables remote human intervention in uncertain scenarios, and has been widely adopted by the industry.

4.2. The Teleoperation Attack Surface

Having established that experts view teleoperation as a practical fallback for CAV edge cases, we next examine the security and safety challenges experts identified when remote operators are integrated into the process of recovering a CAV from situations it cannot resolve autonomously.

4.2.1. Vulnerable Communication. Our participants emphasized that wireless communication exposes CAV data and operator commands to confidentiality, integrity, and availability risks, particularly in the context of Man-in-the-middle (MiTM) attacks. For example, **P15**, **P1**, and **P16** discussed how attackers could intercept or alter commands to/from vehicles with disastrous consequences, e.g., manipulating a "go straight at 2 mph" instruction into a "go straight at 50 mph". Beyond active manipulation, experts identified eavesdropping as a threat despite authentication, i.e., as **P15** explains: *"...the content itself is being authenticated, but has been eavesdropped. So, if we know...there's a person in this car that we want to do bad things [to], we get this information and wait at the next intersection...until the teleoperated vehicle arrives...and the attacker can launch..."*

4.2.2. Threats from Software and Sensors. The teleoperation pipeline relies on sensor data and perception modules to enable remote operators to interpret the vehicle's surroundings, in addition to software modules in the CAV to remotely control it. Experts raised concerns regarding the vulnerability of vehicle software and perception systems. **P2** highlighted risks stemming from vulnerable supply chains, noting that vehicle software is often developed in countries with regulatory frameworks different from those of the country of use. This mismatch can introduce backdoors, granting unauthorized administrative access to foreign governments. For example, **P2** referred to recent U.S. government proposals to ban software from China and Russia [45], [46]. At the firmware layer, **P10** warned of malicious code injection into ECU firmware, stressing the need for attestation and secure recovery protocols. **P10** and **P11** further emphasized that perception-layer attacks such as LiDAR spoofing can corrupt the vehicle-provided data, which is especially consequential because remote operators rely on sensor and perception outputs to understand the road situation. As **P11** pointed out, even a well-intentioned teleoperator can make unsafe decisions when the underlying sensor data is misleading.

> *"...since the operator relies on those sensors on the autonomous vehicle to drive on the roads...if the sensors are compromised and the sensory data is not correct, then the operator, even <if> the operator is benign...cannot drive safely..."* — P11

Finding 2 ($\mathcal{F}_2$) – The teleoperation system pipeline **presents a broad attack surface**, as it consists of untrusted sensors, perception modules, and software. Many experts emphasize the susceptibility to backdoors due to untrusted supply chains, malicious code injection, or attacks on sensors and perception modules.

To counter these threats, participants stressed the importance of robust perception model training and anomaly detection. For example, downstream modules should flag abnormal inputs and enable fallback actions (e.g., halting or rerouting), allowing the system to *"mitigate the attack and remain [in] normal operation"* (**P15**).

4.2.3. OTA Updates and Physical Security Oversights. Participants described how unlike an onboard driver, a remote operator must assess the vehicle through software-generated evidence, including perception, localization, actuator/drive-by-wire status, and recovery reports. If compromised over-the-air (OTA) updates or physical tampering corrupts this evidence chain, the operator may authorize movement, recovery, or return-to-autonomy based on misleading vehicle-reported state.

This concern appeared in **P7**'s example of inconsistent update protections. To preempt security risks from OTA updates, their company *blocks all means for remote software updates*. However, this contrasts with their lax approach to physical security, as nothing prevents an adversary from installing a malicious update with physical access and a tool:

> *"I'm sure there are some open loops in our existing software...so when we ship the vehicles the communication the is pretty <much> blocked,...unless you have a physical tool to connect with the controller with the vehicle..."* — P7

Similarly, **P4** highlighted that emphasis is often placed on cybersecurity while ***ignoring physical security***, i.e.,*"The thief can actually just go into the facility and then plug in a flash drive and your whole database and everything is compromised..."*(**P4**). The lack of physical security and access control is exemplified by the **P4**'s experience with semi-autonomous truck fleets, where companies often have ***a single key for their entire fleet*** to lower operational costs.

Finding 3 ($\mathcal{F}_3$) **–** While the CAV industry is sensitive to malicious OTA updates, to the point of disabling them, there is **less awareness of the physical attack surface**. A few experts recount companies with one key to unlock all vehicles for ease of operation, and firmware that can be easily updated by an adversary with physical access.

Finally, experts noted how teleoperation exposes traditionally offline components to attacks. **P4** discussed how *Electronic Logging Devices (ELDs)* used in the trucking industry to log driving hours are not traditionally designed for connectivity or remote access. However, in teleoperated CAVs, they are connected to an onboard cellular device, expanding their attack surface. Similarly, **P15** discussed how the CAN protocol was not designed with security in mind, but is now the focal point of attacks [47], [48].

Finding 4 ($\mathcal{F}_4$) **–** Connectivity is an unavoidable for teleoperation, which expands the attack surface of CAV **components like ELDs that were traditionally isolated from the network**, but are now remotely accessible.

4.2.4. Security Gaps in Design & Implementation. Experts emphasized that CAV security immaturity becomes a teleoperation concern because the industry remains heavily focused on functionality, safety, and market penetration. As **P4** states: *"... we don't have a lot of security things related and now it's all just about how to make sure we can drive this thing safely..."*. **P9**, who conducted research in a top-10 automotive company, stated that while they recognize the adverse impact of vulnerable modules, they never considered security at the design stage due to their lack of expertise.

For security testing on CAVs, participants such as **P15**, who evaluates and design testing libraries for CAVs from most of the large automotive manufacturing companies, admits that some companies often consider security more than others, and even these companies do not have a concrete idea of what they should test for when they evaluate their vehicles. Similarly, participants such as **P4** described detailed workflows for designing teleoperated CAVs. While individual workflow stages emphasize performance and safety, we observe that they rarely incorporate systematic security evaluation.

This lack of systematic security testing is not only the result of oversight, but also stems from varying organizational priorities and the limited availability of suitable tools for vehicle-specific security evaluation. For instance, as **P15** states, *"I know some car manufacturers, say <company-name>, <company-name>, they are very responsive and they take cybersecurity into consideration a lot...some companies, they want to, you know, push their market, push their product to the market as fast as possible"*. Other participants like **P10** described their experience of having to rely on existing tools built on techniques such as static analysis, dynamic analysis, and symbolic execution, which do not necessarily apply in the CAV context As **P10** states: *"...for general software, you can use those tools to help something, but some still need to customize for the vehicle scenario too...but we don't have too much to write this...vehicle research is still something new..."*.

Finding 5 ($\mathcal{F}_5$) **–** Some experts state that the CAV industry is highly focused on safety, functionality, and increasing market penetration, but shows **few security considerations during design or testing**, with some exceptions. The lack of security testing stems from the absence of vehicle-specific security-focused tools, since experts often have to adapt tools from other domains or design vehicle-specific testing libraries from scratch.

4.3. Access Control, Trust, and the Teleoperator Threat Model

When asked about their expectations of teleoperators, most experts emphasized requirements driven by passenger safety, such as ensuring that teleoperators hold the necessary licenses, permits, and training, pass extensive background checks, understand CAV regulations, and maintain constant situational awareness. However, none of the experts immediately discussed security or privacy.

This trend changed when we asked about the ***capabilities*** that a teleoperator must possess, i.e., the amount of information and controls they should have access to. We saw several patterns emerging at the intersection of teleoperation and established security and privacy approaches.

4.3.1. Defining access through least privilege. When asked if a teleoperator should have access to functions and components in a CAV besides those needed to drive, most experts stated that a teleoperator's responsibility is helping in navigating challenging scenarios with access to only the necessary driving controls. That is, as **P11** aptly states: *"...I believe the reasonable way is to allow the operator have access to only the functions that (are) related to driving and control and also perception."*.

We observe that this need for ***least privilege*** in teleoperation stems from privacy concerns. Particularly, experts emphasized that teleoperators should only have access to the external sensors, and not the sensors inside the vehicles such as the camera and microphone. As **P7** states: *"... they shouldn't have any access to that information because that to me becomes a privacy concern...data that's coming from outside to the vehicle like all the sensor data they should have access to that..."*.

4.3.2. The need for context-aware exceptions to least privilege. Participants also discussed granting a teleoperator

additional access during emergency situations, beyond what their notion of least privilege permits. However, there were differing views on how such access should be authorized, and who should authorize it. For instance, **P1** and **P7** expressed the need for ***explicit requests from passengers*** to grant a teleoperator access to privacy sensitive sensors that go beyond those typically needed for driving. Some others expressed reservations with this approach, citing that passengers may not always be available or able to make the necessary requests, e.g., *"... in an accident and the passenger needs to evacuate as fast as possible or the passenger is having issue, say, unconscious..."* (**P15**).

Alternatively, **P6** and **P12** suggested using *a predefined discretionary access control (DAC) policy* managed by the teleoperator's supervisor, which would exempt passengers from being a dependency in the decision process.

Neither of these extremes is tenable, as they either sacrifice the safe operation of a CAV by relying on a potentially incapacitated passenger or put full control in the hands of a supervisor, who may become overprivileged and grant access when unnecessary. Thus, in practice, it appears that an approach that considers the nature of the situation, i.e., the context in which the access is being requested, would be practical when granting exceptions to the least privilege policy. A quote from **P2** highlights this possible direction for access control in teleoperated CAVs, i.e., as **P2** states, *"... sometimes you don't want the door to be opened right when you're sitting there but when sometimes its flooding...you better open the open the door immediately otherwise you will be dead...***it's really scenario driven***..."* That is, from our interviews, we observe a clear need for ***context-aware access control*** in order to grant teleoperators access beyond the least privilege needed to drive the vehicle.

Finding 6 ($\mathcal{F}_6$) **–** Majority of experts state that access to security and privacy sensitive sensors by teleoperators must be restricted using a least privilege policy, i.e., by granting access to only the set of sensors necessary for driving. However, experts differ on how exceptions to such a policy must be handled, i.e., via the passenger's consent, or by bypassing the passenger and consulting an administrator. Some experts note the *need for context-aware exceptions* to least privilege in this domain.

4.3.3. Proactive monitoring, and involuntary takeover. When experts are asked whether teleoperators should have the capability to continuously monitor CAVs, some advocated for proactive monitoring, while some expressed concerns. **P4** described an existing experimental framework being used in tests for monitoring autonomous semi-trucks, which consists of a control center where *"...there are like a thousand displays...and they are actively monitoring all the trucks that the company has..."* (**P4**). Some other participants, particularly **P1**, **P12**, and **P13**, expressed privacy concerns regarding continuous monitoring, e.g., as **P12** states: *"...I don't like people watching me all the time...because when I call an autonomous vehicle I don't want someone to know my real-time location."*.

Another issue raised by experts as a complement to the continuous monitoring was the ***involuntary takeover*** of the CAV by the teleoperator, i.e., where an operator would gain remote control of a vehicle whenever they see fit. Most participants were not in favor of such an approach, with **P4** highlighting that even in their experimental framework, the semi-truck has to send an alert for the teleoperator to assume control. Alternately, some experts were in favor of involuntary takeovers, and stated that teleoperators should be able to intervene if the passenger's safety is at risk (**P4**, **P5**) or if CAV is in a complex situation not identified by driving algorithm (**P4**, **P7**). For instance, **P7** stressed the need for such interventions to *avoid* impending failures,

> *"...you can somehow know from the surroundings of the vehicle and the vehicle's capability that vehicle will definitely struggle to make a decision here, so you are proactively intervening before something has happened."* — P7

These discussions further highlight the important role that context-aware access control plays in teleoperation, as it may also help in deciding when disengagement and monitoring is appropriate.

Finding 7 ($\mathcal{F}_7$) **–** Some experts note that real-time monitoring of CAVs as well as their proactive takeover by teleoperators may help prevent failures. However, such strong interventions also raise equally significant privacy and security concerns.

4.3.4. Lack of standards/frameworks for access control, licensing, or even general operation. Despite differing views on appropriate operational bounds, experts consistently noted the ***absence of any operational standards for teleoperation*** that spans functional requirements, access control, and teleoperator training and licensing.

For instance, **P12** pointed out that each company has its own approach toward interfaces, controls, and remote driving. From his experience as a safety operator in an autonomous shuttle service, **P13** described the minimal training and organization-specific standards, i.e.,*"...before I became the formal testing operator on the mini shuttle...I got trained...like,* ***two days training*** *of driving that vehicle..."* (**P13**) However, since such training/certification is ad-hoc it is challenging to enforce or expect bare minimum operational or security standards from the industry in general. Thus, as **P4** aptly states, the state of the teleoperation industry is like *the wild west*:

> *"... They are all privately owned training facility like <company-name>, <company-name>, <company-name>, all of them, they have their own training people, and they are their own training program...because the equipment is not even standardized right now the policy is not standardized...,* ***nothing is standardized in this area right now it's the wild west****..."* — P4

Finding 8 ($\mathcal{F}_8$) – Many experts describe a **severe lack of standardization** in the fragmented teleoperation industry, be it in terms of operator training, certifications, operational requirements, or security/privacy constraints.

4.3.5. The threat of malicious teleoperators. While all participants consider it important to authenticate teleoperators so as to prevent hostile takeover, their perspectives differ on *an insider adversary*, i.e., a malicious teleoperator, who would, for instance, forcefully disengage and control a CAV to cause damage or spy on passengers. **P2** discussed the ease with which either unskilled but benign or malicious teleoperators can cause harm with CAVs, particularly in public spaces or against pedestrians. This is possible largely due to the ***reduced personal risk teleoperators face*** when operating vehicles remotely. Some experts, such as **P12**, are not concerned about such a scenario at all, not because they think it's unlikely, but because they view it as an unavoidable risk, i.e., as **P12** states: *"... I wouldn't worry about it at all, because the same thing can happen with (the driver) can be in a bad mood or something, right?"*.

Others, such as **P10**, **P3**, and **P16**, expressed that the insider adversary is a hard, but *non-technical*, problem, which can be addressed with proper training and vetting. As **P3** states: *"... I think that's more, more on a training issue, right? If you're providing this kind of service...So you probably have to guarantee that the operators that you hire or you provide is well, means well..."*. This quote from **P16** summarizes the sentiment among experts:

> *"...the certification, the vetting, the screening of the driver, would be critical as well...because you are putting your trust into someone else that is remotely operating the vehicle, there would have to be those checks and balances in place to make sure that they're not putting a bad actor behind the wheel..."* — P16

Experts noted that a malicious teleoperator is a strong threat model, and there may not be significant research on it purely because of this, i.e., as **P15** states, *"Unfortunately, I do not see much work targeting this because one thing is the people fear that this might be too strong assumption."*

Finding 9 ($\mathcal{F}_9$) – About half of the experts perceive the threat model of a **malicious teleoperator** as a hard problem. They see it as an **unavoidable risk**, but one that could be mitigated through standardized training and vetting processes.

4.3.6. Trust, safety, and contextual decision-making. Experts highlight both technical and non-technical factors that may compromise safety of the passengers in a teleoperated CAV. **P4** and **P5** identified the unreliable communication infrastructure and latency as a major concern. Lag can be particularly dangerous, as **P4** states: *"...it's very dangerous if you're driving over 35 or at a higher speed and there's a lag and you saw you're, you're making a left turn, but the vehicle is two seconds behind"*. Experts believe that teleoperators may overcorrect to account for latency, which makes things worse. Similarly, **P6** described how blindspots, combined with the lack of a reliable communication infrastructure, can result in serious harm when teleoperating CAVs in dense pedestrian environments.

Given that the effectiveness of a teleoperator can be limited by their own skill, as well as factors such as communications latency, several experts raised an important question: *who do we trust more; the teleoperator, or the autonomous driving system?* As the teleoperation model allows the operator to take over in the case the CAV disengages, one might reflexively say that we trust the teleoperator more. However, experts discussed several nuances that motivate a more balanced outlook that considers the scenarios in which the system should lean on teleoperation, or the CAV. For example, **P1** states that when the CAV is driving at 60 mph in a 30 mph zone, the teleoperator should be alerted and possibly intervene, i.e.,*"...the speed limit i know 30 and the vehicle is going 60 miles per hour that should be a distress call..."* (**P1**). In contrast, experts also posit scenarios in which the driving algorithm should override the teleoperator's controls, such as when dealing with blind spots and inclement weather that may inhibit the teleoperator's perception and performance. Particularly, **P2** also believes that the CAV should be designed to adhere to certain invariants regardless of the teleoperator's instructions.

Finding 10 ($\mathcal{F}_{10}$) – Many experts pose a pertinent question for secure and safe teleoperation: *who to trust more, the teleoperator or the CAV?* As safety and security risks are contextual, many experts support the teleoperator in some contexts, but also support overriding the teleoperator to adhere to safety invariants.

4.4. Privacy Implications Unique to Teleoperation

In real-world teleoperation, CAV sensors (e.g., cameras, LiDAR, radar, and GPS) may inadvertently capture sensitive personal information, such as conversations, facial expressions, and geolocation, often without explicit user consent. In large-scale deployments, the centralized nature of data management further increases the risk of privacy violations. This section examines expert perspectives on the risks of data exposure and misuse in teleoperated CAV.

4.4.1. Privacy Risks from Interior and Exterior Monitoring. Teleoperated vehicle systems raise significant privacy concerns due to internal and external sensory monitoring, e.g., internal microphones and cameras that enable functional interactions such as teleoperator-passenger communication. While essential for system operation, these sensors inherently capture sensitive data: real-time transmission of passengers' video/audio feeds may expose verbal content, facial expressions, and other biometric cues without explicit consent. As **P3** states: *"If someone is monitoring where your vehicles are or what you're seeing, what you're*

hearing...They probably don't want people to know where they are or what they're talking about." This captures the dual discomfort with both geolocation tracking and audio-visual surveillance.

These privacy concerns are complicated by the fact that the same channels that introduce privacy risk may also support important teleoperation or driving functions (See Section 5.2). For example, a remote operator may need to communicate with an on-site traffic controller through an in-cabin audio channel to resolve ambiguous road conditions, or explain the situation to passengers when the vehicle unexpectedly disengages. These functions may expose sensitive information from passengers, traffic controllers, law enforcement, and other nearby road users.

To address these privacy concerns, for interior sensor data privacy protection, **P6** proposes mitigation strategies such as applying real-time face-blurring to passenger video feeds. **P6** continues to advocate for explicit consent mechanisms, suggesting that companies *"send [a] consent [request] through the email... before they drive"* and then respect the passenger's decision, i.e.,*"If the passenger... refuse[s] to agree, I believe the company should not record the conversations, the camera, images, video."* (**P6**). While experts raised privacy concerns regarding interior sensor access in teleoperated CAVs, there is tension between passengers' functional needs and privacy, where prioritizing one may come at the expense of the other [26].

Finding 11 ($\mathcal{F}_{11}$) **–** Almost All experts discuss significant **privacy concerns unique to teleoperation**, as they emerge from the teleoperator's ability to access sensors **inside** the vehicle, including camera and microphone feeds. This deviates from existing perspectives on the privacy concerns in CAVs, which generally focus on the privacy of bystanders/pedestrians recorded by the exterior sensors.

4.4.2. Protection Mechanisms Across the Data Pipeline. To mitigate some of these risks, encryption and proprietary encoding formats are employed during transmission, as noted by **P1**: *"you have some encoding...a special format of the data...you can only use your parser to parse the data,"* Some systems apply fine-grained transformations to avoid transmitting raw data, only reversing the obfuscation locally. As **P12** highlights, this approach prevents attacks, but may reduce situational awareness, reflecting a trade-off between data protection and operational transparency.

In addition, data protection extends beyond transmission to include secure storage on edge servers or in the cloud. As **P16** explained, *"all the data was encrypted at rest,"* and stored in client-specific shards to avoid cross-contamination. Specifically, *"each customer had their own shard of data."* Together, encryption during transmission and at rest, along with logical separation, form a robust defense for protecting vehicle data throughout its lifecycle.

4.4.3. Risks from Third-party Data Annotation. Collected sensor data enables real-time perception and control during teleoperation while serving as a foundation for continual learning. The teleoperator relies on raw sensor inputs and insights that are derived from the sensor inputs in real time. Particularly, the teleoperator benefits from ***perception modules*** that adapt to region-specific driving patterns and dynamic environmental conditions. That is, as **P7** states,

> *"... if you only give them raw data and ask them to do all the processing mentally, you are not taking full advantage of the system. What the perception module does, like sensor fusion...Providing both gives the operator more information than either."* — P7

To support model training, autonomous systems generally rely on annotated datasets. The industry often depends on a small number of annotation service providers, with Scale AI [49] being one of the most prominent. While such platforms help companies reduce the cost of maintaining in-house annotation teams, this reliance on third-party services raises significant privacy concerns.

Finding 12 ($\mathcal{F}_{12}$) **–** Teleoperators rely on insights obtained from sensor data in order to issue appropriate commands to CAVs. These insights come from machine learning models that rely on real-world sensor data to enhance model robustness. In such cases, **data annotation is often outsourced** to providers such as Scale AI, which raises privacy concerns.

4.5. Regulatory Gaps and the Need for CAV-Specific Standards

Despite the rapid increase in teleoperated CAVs, the regulations governing their security, safety and data practices remain fragmented and underdeveloped. In the absence of cohesive federal standards, individual states impose inconsistent requirements, industry bodies grapple with the regulatory gaps, and smaller companies operate with minimal security oversights. This section describes expert perspectives on the regulatory landscape and the need for CAV-specific standards in teleoperated systems.

4.5.1. Inadequate regulation and lack of cohesion among regulators. To understand the regulatory landscape, we asked participants about regulatory guidelines that govern the CAV industry, or regulations they have to follow when designing CAV systems. However, they had no knowledge of such regulations. When discussing one of the key areas i.e., data collection, **P5** stated that: *"... if we [are] working on something, we, there's no, like a paper listed, like a, a regulations you need to follow one by one..."*, while highlighting that they often rely on ***"common sense"***, when handling personal identifiable information:

> *"... some of the common sense when we're dealing with the data, we need to understand that we cannot, you know, expose to the people outside, outside of our team..."* — P5

Similarly, **P16** pointed out that while working in a team responsible for ***collecting telematics data from personal vehicles***, which is sold back to various OEMs, there were **no regulations** that restricted them on what to collect and how to collect it, although there were quality standards.

Most regulations surrounding CAVs and teleoperation are postulated and enforced by individual states in the US. For example, **P4** highlighted that Indiana does not allow autonomous trucks to drive without a human driver on board. Similarly, in May 2025 Colorado introduced and passed bill HB25-1122 that bans commercial motor vehicles (trucks) with automated driving systems from operating without a person on board with a commercial driver's license (CDL) who can intervene and monitor the vehicle [50]. Other states might follow similar regulatory trends and may require teleoperation for CAVs in the future.

Finding 13 ($\mathcal{F}_{13}$) – Some experts note a **lack of regulations addressing data collection and handling** from teleoperated CAVs, often leaving them to rely on "common sense". This regulatory gap may be exploited by CAV companies for profit.

4.5.2. Enforcing safety invariants and limiting teleoperators control. In the event a malicious teleoperator does get control of a CAV, **P2** highlights that *regulations may aid in limiting the impact* of such a compromise. For example, **P2** claimed that USDOT does not allow CAVs to be remotely operated for more than 30 seconds. While this is consistent with NHTSA's AV STEP proposal [51] which permits teleoperation only for *briefly* moving a vehicle, we found no evidence of USDOT-specific "30 seconds" time limit for teleoperation. However, regulatory frameworks such as NHTSA AV STEP, consistent with **P2**'s claim, ensure that remote control is available for emergencies but is severely time-limited to reduce damage.

Interestingly, **P13** mentioned that a CAV company in China is developing technology known as ***"Active Security"***, which allows the CAV to detect road boundaries, and stop if a malicious or benign remote operator tries to drive the CAV off the road, i.e., a safety invariant to prevent harm.

Finding 14 ($\mathcal{F}_{14}$) – Some experts note that **regulations may limit the damage** caused by a malicious teleoperator by mandating restrictions on the duration and driving speed of full remote control. However, safety-driven approaches like ***"Active Security"***, which enforce safety invariants that override the teleoperator, may prevent harm entirely in such scenarios.

4.5.3. Unreported insider incidents and industry accountability. P15 notes that such attacks by malicious teleoperators may have occurred in industry; however, they are unlikely to ever be reported due to the negative impact on industry, such as robo-taxi services. This phenomena may not be limited to attacks due to malicious teleoperators, but may extend to all attacks, i.e., as **P4** states: *"... some companies will pay it and a lot of times the companies, when they actually get hacked and they were asked for ransom, they don't even report it because it's a bad history."*

Finding 15 ($\mathcal{F}_{15}$) – A few experts note that attacks by insider adversaries like malicious teleoperators may have occurred in the CAV industry. They suggest that misaligned incentives may discourage companies from reporting such incidents due to the potential negative impact on their business.

4.5.4. Security Posture Disparities Across Company Sizes. Experts who work for top-20 automotive companies believe that they have large security teams and resources sufficient to tackle any security challenge, i.e., as **P4** states, *"... especially in the security area, the big companies, they have the money, they have the resource to prevent all of this happening...they have the biggest lock...the small companies, the original companies, they are very vulnerable..."*. **P13**, who is the CEO of a smaller automotive company, substantiates **P4**'s assertion, admitting how they ***do not have protected communication channels for communicating with their teleoperated vehicles***.

Finding 16 ($\mathcal{F}_{16}$) – Some domain experts affirm that larger automotive companies often have dedicated security teams and resources to combat security threats that might arise. However, smaller automotive manufacturers may struggle when confronted with such threats and often maintain a weaker security posture.

4.5.5. The Role of Industry Standards Bodies. Another important gap in regulations is how various states handle the interaction between law enforcement and CAVs. From a law enforcement perspective, it remains unclear on how to stop and interface with a CAV vehicle that may have broken traffic rules. **P4** highlighted that the Commercial Vehicle Safety Alliance (CVSA) [52] has developed an inspection program for commercial vehicles (trucks) equipped with self driving technology known as the enhanced Commercial Motor Vehicle (CMV) Inspection Program [53], under which vehicles undergo stringent security and safety inspections, and earn a pass that is conveyed to law enforcement as well. As **P4** states: *"... they check everything before the truck even go and then they they put some kind of electronic identifier ..."*. Similarly, **P7** highlighted the Motor Industry Software Reliability Association (MISRA) [54] guidelines developed for secure and safe software for embedded systems, used to automate their organization's security and quality testing for CAV software. This exemplifies how, in the absence of regulation, industry bodies have stepped in to fulfill the need for regulation and standardization in the CAV space.

4.5.6. Toward New, CAV-focused regulations. Some participants advocated for specific security and privacy regulations for teleoperated CAVs. Particularly, **P13** suggested that the notion of *active security*, described earlier, where

the CAV adheres to certain invariants even if it has to override the teleoperator, should be a minimum regulatory requirement, as it affords protection against malicious or incapable teleoperators. Similarly, **P10** highlights that the CAV landscape is more complicated than Internet of Things (IoT) and mobile device platforms, and notes the need for CAV-specific security regulations or guidelines that addressed the sensors, actuators, teleoperator behavior, and robustness of the driving algorithm against attacks and failure. Finally, participants also motivated the need for CAV-specific data protection regulations, particularly considering sensors inside the vehicle that expose privacy concerns unique to teleoperation. In a similar vein, **P7** suggested that passengers' identities should be protected from the teleoperator through a regulation requiring double blind teleoperation.

Finding 17 ($\mathcal{F}_{17}$) – Many experts express **strong support for CAV-specific security and privacy regulations**, due to the unique challenges posed by teleoperated CAVs. Particularly, experts highlight the need for regulations mandating security and safety invariants that override the teleoperator, govern the use of data from interior sensors, and enforce a double-blind teleoperation.

5. Discussion

This interview-based qualitative study examines the need for teleoperation in CAV systems and its related security, privacy, safety, and regulatory challenges. We synthesize the 17 findings ($\mathcal{F}_1$–$\mathcal{F}_{17}$) from our analysis into the following key *discussion themes* that identify the challenges unique to teleoperation, and outline actionable directions for researchers, practitioners, and policymakers in both security and teleoperation.

5.1. Teleoperation vs. General CAV Challenges

It is important to note some findings represent challenges unique to teleoperation and others reflect broader CAV challenges. The insider threat of a malicious teleoperator ($\mathcal{F}_9$) is entirely new: unlike a compromised software module, the teleoperator is a human actor with judgment and intent, making this adversary model fundamentally different from conventional CAV threats. The privacy risks from interior sensor access ($\mathcal{F}_{11}$) are also teleoperation-specific: while standalone CAVs collect data from exterior sensors (raising bystander privacy concerns), teleoperation requires access to in-cabin sensors that can compromise passenger privacy. Finally, the need for context-aware access control that dynamically adjusts teleoperator privileges ($\mathcal{F}_6$, $\mathcal{F}_7$) is a challenge without a direct equivalent in non-teleoperated CAVs. In Section 5.3, we discuss a critical teleoperation-specific challenge, i.e., the confused deputy scenario, where a well-intentioned teleoperator makes unsafe decisions.

Some security challenges identified by experts, such as sensor spoofing, vulnerable supply chain ($\mathcal{F}_2$), malicious OTA updates ($\mathcal{F}_3$), and the general lack of security prioritization in the industry ($\mathcal{F}_5$), are not specific to teleoperation. However, teleoperation *amplifies* these risks in critical. For instance, sensor attacks on a standalone CAV may cause the vehicle to stop safely; in a teleoperated context, the same attack corrupts the teleoperator's situational awareness, potentially leading to actively unsafe remote commands.

5.2. Practical Access Control for Teleoperation

Addressing the functional gaps, security challenges, and privacy issues discussed in Section 4 would be a significant feat; however, that would only fix the system-level issues in the teleoperation pipeline. For truly secure, safe, and privacy-preserving teleoperation, we must also address issues associated with a key participant in the teleoperation pipeline: *the teleoperator*.

Experts consider the teleoperator as *untrusted*, as they overwhelmingly recommend granting the teleoperator access to only the minimal sensors and driving controls necessary, i.e., a least privilege policy ($\mathcal{F}_6$). However, experts also support exceptions to least privilege in emergency situations, or support features such as real-time monitoring and full driving takeovers, which help the teleoperator proactively detect and prevent failures before the CAV disengages ($\mathcal{F}_6$, $\mathcal{F}_7$). These concerns reflect a broader CAV access control challenge that teleoperation *amplifies* by introducing a remote human operator whose required privileges may vary with the driving context. Notably, in 2023 Tesla employees were found to have accessed and shared interior and exterior camera footage without explicit passenger consent [55], [56]. While the interior cabin camera's main function is to determine driver inattentiveness and provide audible alerts [57], as highlighted in Section 4.4, addressing the teleoperator-specific privacy risks may impact the functional needs of passengers. Thus, we observe that these access control challenges naturally motivate the design of ***context-aware access control*** [58], [59], [60], [61] for this domain, where the specific driving scenario, and precise, context-sensitive access control policies, would determine the operator's capabilities.

5.3. Malicious Teleoperators, Confused Deputies

A context-aware access control system would prevent a teleoperator from exceeding their privileges, but it cannot address the teleoperation-specific risk that a ***malicious operator*** may intentionally misuse legitimate vehicle control privileges to damage the CAV or its surroundings (e.g., drive into a protest [62], or purposefully crash a plane [63]). While experts find this threat model believable, they see it as a hard problem, and more importantly, a non-technical problem that can be addressed with training and vetting ($\mathcal{F}_9$). That said, some experts also proposed a practical solution for this harder adversary model: *safety invariants*, which are currently being explored in the CAV industry in China in the form of "active security" (stated by **P13**, $\mathcal{F}_{14}$). Safety invariants derived using domain knowledge and the analysis

of prior CAV incidents, in conjunction with common-sense restrictions on the duration of takeover, provide a promising and actionable solution to the challenging threat model of a malicious teleoperator.

In addition to intentionally malicious teleoperators, teleoperation introduces a subtler threat in which a well-intentioned operator can be manipulated into exercising legitimate vehicle control authority on behalf of an attacker, consistent with the authority-misuse structure of the ***confused deputy*** problem. That is, by manipulating the environmental state, an attacker can induce a benign teleoperator to perform privileged actions that the attacker could not perform directly. For example, an attacker could stage a roadblock to trigger CAV disengagement and teleoperation, then impersonate a police officer and request access to the vehicle. Although the attacker lacks the authority to unlock the CAV, the attacker can manipulate the teleoperator's observations and induce the operator to exercise that authority, potentially enabling vehicle theft. In this case, the teleoperator is a *confused deputy*, effectively reversing the role of teleoperation from a safety fallback into a source of risk. This highlights the need for mechanisms that either ensure teleoperators are presented with faithful context or constrain their actions when contextual integrity cannot be guaranteed, such as the "active security" approach ($\mathcal{F}_{14}$) discussed previously.

5.4. CAV-specific Regulations for Safe, Secure and Privacy-Preserving Teleoperation

A common sentiment among experts was that the CAV domain is highly unregulated, and according to one participant, analogous to the wild west, with no standards, norms, or uniformity across companies. That is, experts note that every aspect of the design of a teleoperation system, including testing and operator training, is company-specific, and there are no industry-wide standards for the same ($\mathcal{F}_{13}$). With practices such as collecting telematics data from personal vehicles and selling it to OEMs without restrictions ($\mathcal{F}_{13}$), experts also note the absence of privacy regulations to handle the intricate privacy challenges of this space ($\mathcal{F}_{14}$).

These observations motivate dedicated CAV-specific security and privacy regulations ($\mathcal{F}_{17}$), which will offer two key benefits. First, regulations and industry standards will motivate organizations to incorporate security/privacy considerations early in the design process, instead of employing an ad-hoc approach. Second, consumers data will also be protected from exploitation by third parties that annotate sensor data ($\mathcal{F}_{12}$). CAV-specific regulations will codify broadly-accepted security and safety invariants, the expectations from teleoperators, their acceptable abilities, and constraints, which will ensure their adoption by CAV companies and translate into consumer safety gains. In addition to safety invariants, such regulations and standards will also incorporate a formal reporting process that is currently lacking ($\mathcal{F}_{10}$), similar to GDPR-style disclosure requirements [64], [65], that facilitates collective threat awareness and supports more timely incident response [66].

To summarize, reining in this wild west through targeted standards and regulations will promote the development of secure and privacy-preserving teleoperation-based CAV systems, and enable improved security, safety, and privacy guarantees for consumers.

6. Related Works

While prior studies have explored teleoperation in the context of CAV adoption [26], [67], our work is the first qualitative investigation focused specifically on the security, privacy, and safety of teleoperated CAVs, grounded in insights from domain experts (n=16). In this section, we review closely related works in three key areas: user studies on privacy perceptions of CAVs, sensor attacks on CAVs, and the proposed countermeasures to these challenges.

1. User Studies on Privacy Perceptions of CAVs: Prior work has used user studies to examine data collection and privacy concerns in CAVs [68], [69], [70], [71], [72]. For example, Bloom *et al.* [68] found that over 50% of 302 surveyed pedestrians preferred to opt out of identifiable data collection due to concerns about tracking and identification. Krontiris *et al.* [69] emphasized the importance of consumer privacy rights for building trust and acceptance, while Reig *et al.* [70] reported that trust is closely tied to brand reputation and public awareness of CAV technology. Cai *et al.* [71], [72] further showed that passengers are generally unwilling to trade safety and security for privacy, though they may sacrifice convenience. Jing *et al.* [36] confirmed what experts claimed in our study as they uncovered new attack surfaces in the CAV pipeline, including private data leakage through charging pile and apps. Our study complements these studies by providing expert perspectives on consumer privacy in teleoperated CAVs.

2. Sensor Attacks on CAV: Most work in CAV security focused on sensor attacks [73], [74], [75], [76], [77], [78]. For example, Eykholt *et al.* [78] demonstrated a physical disappearing attack by adding adversarial stickers to stop signs, causing neural networks to miss detections. Cao *et al.* [74] showed that attackers can effectively mislead LiDAR-based object detection by altering model inputs rather than compromising the sensor. They later extended this to multi-sensor fusion systems using adversarial 3D objects in the physical world [75]. While these efforts reveal that CAV perception pipelines are vulnerable to adversarial manipulation, much less is known about how security concerns are interpreted and managed in teleoperation contexts. Our findings, grounded in the experience and perspectives of experts, underscore the urgent need for the CAV industry to treat security as a priority ($\mathcal{F}_4$, $\mathcal{F}_6$, $\mathcal{F}_8$, $\mathcal{F}_{11}$, $\mathcal{F}_{12}$), given the numerous attack surfaces that apply to teleoperation, i.e., perception models, hardware sensors, communication channels, *etc.* ($\mathcal{F}_5$, $\mathcal{F}_7$). In addition, the lack of rigorous testing in the CAV industry emphasizes the need for CAV-specific security tools, methodologies, and regulations that

address these diverse and evolving vulnerabilities ($\mathcal{F}_{16}$, $\mathcal{F}_{17}$). Similarly, both internal (e.g., CAN, LIN, FlexRay) and external communications (to the teleoperator) in the CAV present a broad attack surface [79], [80], [81]. As discussed in this paper, communication and data integrity remain essential for safety and privacy, in teleoperation scenarios where remote commands directly influence vehicle behavior.

3. Proposed Countermeasures for Privacy Challenges and CAV Sensor Attacks: To address privacy risks in CAVs, prior work has explored anonymization and differential privacy [82]. However, these mechanisms primarily protect stored or shared data and do not address real-time privacy risks in teleoperated CAVs ($\mathcal{F}_{14}$, $\mathcal{F}_{15}$), where remote operators access raw sensor feeds ($\mathcal{F}_2$, $\mathcal{F}_3$). For sensor attacks in CAVs, while cryptographic techniques offer security guarantees [83], their computational overhead makes them impractical for many embedded ECUs. Lightweight alternatives like gateway-based isolation have been proposed to enforce access boundaries and restrict attacker mobility within the vehicle network [84]. In addition, traditional security mechanisms like access control [85] and encryption [86] have recently been adapted to CAV contexts, e.g., Zhang *et al.* [87] proposed AC4AV, a real-time access control framework for live and archived in-vehicle data. However, such frameworks do not incorporate the contextual exceptions highlighted by our experts and therefore may lack practical applicability. As discussed in Section 5, our findings motivate revisiting prior context-aware access control frameworks [58], [59], [60], [61] in teleoperated CAV settings to achieve practical security gains.

7. Conclusion

This paper presents a qualitative study based on 16 in-depth interviews with experts involved in the development and deployment of CAV and teleoperation. Through thematic analysis of the interview transcripts, we identify 17 key findings ($\mathcal{F}_1$–$\mathcal{F}_{17}$) that reveal critical challenges for the security, privacy, and safety of teleoperated CAVs, many of which can be attributed to the absence of industry-wide standards, or targeted regulations. Our analysis uncovers several unique aspects of security and privacy under teleoperation, including the neglected physical attack surface, inadvertent network exposure of traditionally isolated CAV components for remote operation, and the unique privacy constraints arising from a focus on sensors inside the vehicle. Our findings motivate context-aware access control that limits teleoperator privileges while preserving emergency access, together with security and safety invariants that constrain malicious or unsafe actions. Finally, we describe actionable regulatory interventions to complement these measures and promote their adoption in the CAV industry.

Acknowledgments

The authors would like to thank the shepherd, and the anonymous reviewers for their constructive feedback on the paper. This work was supported in part by COVA Commonwealth Cyber Initiative (CCI) under Supply Chain Cybersecurity and HC-2Q26-032 grants, and by the National Science Foundation (NSF) under grants CNS-2237012 and CNS-2348151. Any opinions, findings, and conclusions expressed herein are the authors' and do not reflect those of the sponsors.

Ethical Considerations

As discussed in Section 3.1, this interview-based study was reviewed and approved by our IRB. We have followed standard best practices toward limiting harm throughout the study, as discussed in the rest of this section.

1. Stakeholders: We identify three primary stakeholder groups potentially affected by this work. First, the interview participants who contributed professional perspectives on teleoperation practices. Their main risk is reputational or professional harm if their views were traceable to them or their employers. We mitigated this through informed consent, removal of all identifying details, and anonymized, aggregate reporting. Second, the companies and engineering organizations responsible for developing and operating teleoperated CAV systems. Because our analysis reflects on current deployment practices, it may shape perceptions among customers, regulators, and the public. To avoid unintended negative impact, we do not name organizations or deployments, and we explicitly avoid system-level evaluation. Instead, our focus is on cross-cutting security and usability challenges observable across the ecosystem. Third, CAV passengers and other road users, whose physical safety depends on reliable human-in-the-loop control when autonomous functions encounter uncertainty or failure. Our study aims to improve teleoperation safety and accountability by documenting real-world practice and identifying points of operational risk, rather than exposing information that could facilitate misuse.

2. Potential Harm Mitigation: This research did not involve experimentation with deployed vehicles, modification of operational systems, or interaction with live teleoperation environments. Instead, all findings are derived from semi-structured interviews conducted under informed consent, with participants free to skip questions or withdraw at any time. We intentionally avoided soliciting sensitive operational details, proprietary engineering information, or security-critical procedures. All transcripts were securely stored with restricted access limited to the research team, and were anonymized prior to analysis. In reporting our findings, we present only aggregated insights about security, safety, and usability practices rather than implementation-level details. This approach ensures that our results inform safer system design while minimizing the risk of adversarial exploitation and preventing reputational harm to individual participants or their organizations.

3. Decision: Teleoperation is increasingly used as a fallback when commercial CAVs disengage from autonomous driving. Yet we still know very little about the security, safety, and usability risks that arise when humans remotely control vehicles in dynamic driving environments. Our study helps address this gap by revealing weaknesses and friction points in current teleoperation practice, many of which stem from the lack of mature operational frameworks and clear regulatory guidance. Building on these findings, we identify key security and privacy challenges in human–machine coordination and propose actionable improvements to access control and organizational processes, while also motivating future regulatory attention. We carefully weighed the public benefits of advancing transparency, safety, and security in teleoperated CAV systems against the possibility of unintended harm. Given the safeguards incorporated into our study design, data handling, and reporting practices, we conclude that disseminating these results offers a clear net positive to both the research community and the broader public.

Open Science

We are committed to complying with the open science policy to promote transparency and reproducibility of research and science. For confidentiality reasons, we do not release the transcripts of our study. Artifacts are available in the Online Appendix [38], which includes the following:

1. The semi-structured interview questions.

2. The codebook developed during our qualitative analysis. This codebook contains primary and secondary-level codings, as well as a description and an example for each code.

References

[1] E. Yurtsever, J. Lambert, A. Carballo, and K. Takeda, "A survey of autonomous driving: Common practices and emerging technologies," *IEEE access*, vol. 8, pp. 58 443–58 469, 2020.

[2] Z. Xu, Z. Jiang, G. Wang, R. Wang, T. Li, J. Liu, Y. Zhang, and P. Liu, "When the automated driving system fails: Dynamics of public responses to automated vehicles," *Transportation research part C: emerging technologies*, vol. 129, p. 103271, 2021.

[3] C. Cui, Y. Ma, X. Cao, W. Ye, Y. Zhou, K. Liang, J. Chen, J. Lu, Z. Yang, K.-D. Liao *et al.*, "A survey on multimodal large language models for autonomous driving," in *Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision*, 2024, pp. 958–979.

[4] The Last Driver License Holder, "2023 disengagement report from california (online)," https://thelastdriverlicenseholder.com/2024/02/03/2023-disengagement-reports-from-california/, accessed: 2024-03-03.

[5] A. Hawkins, "Waymo's driverless car: ghost-riding in the back seat of a robot taxi," *The Verge*, 2019.

[6] J. L. LaReau, "How General Motors is leading the race for self-driving cars," 2018.

[7] CB Insights Research Briefs, "Remote control: Companies researching teleoperation for autonomous vehicles," https://www.cbinsights.com/research/autonomous-vehicle-teleoperation-patents/, 2017, accessed: 2026-05-31.

[8] A. Sarmiento, "Smooth teleoperator: The rise of the remote controller," https://venturebeat.com/2020/08/17/smooth-teleoperator-the-rise-of-the-remote-controller/, 2022, accessed: 2026-05-31.

[9] Aptiv, "Aptiv and Hyundai Motor Group to form autonomous driving joint venture," https://www.aptiv.com/en/newsroom/article/aptiv-and-hyundai-motor-group-to-form-autonomous-driving-joint-venture, 2019.

[10] Ottopia, "Motional selects Ottopia to enable teleoperation of its mass robotaxi fleets," https://www.prnewswire.com/news-releases/motional-selects-ottopia-to-enable-teleoperation-of-its-mass-robotaxi-fleets-301343097.html, 2021, accessed: 2026-05-31.

[11] Ottopia Ltd, "Drive.ai launches robot car pilot in Texas with a focus on humans," https://spectrum.ieee.org/driveai-launches-dallas-robot-car-pilot-with-a-focus-on-humans, 2018.

[12] A. Ohnsman, "Amazon-backed Aurora readies an air-traffic control system for self-driving cars," https://www.forbes.com/sites/alanohnsman/2019/12/16/amazon-backed-aurora-readies-air-traffic-control-system-for-self-driving-cars/?sh=111bb6c01a16, 2019, accessed: 2026-05-31.

[13] M. Herger, "How teleguidance helps Zoox vehicles to navigate difficult traffic scenarios," https://thelastdriverlicenseholder.com/2020/11/12/how-teleguidance-helps-zoox-vehicles-to-navigate-difficult-traffic-scenarios/, 2020, accessed: 2026-05-31.

[14] D. Bogdoll, S. Orf, L. Töttel, and J. M. Zöllner, "Taxonomy and survey on remote human input systems for driving automation systems," in *Future of Information and Communication Conference*. Springer, 2022, pp. 94–108.

[15] C. Kettwich, A. Schrank, H. Avsar, and M. Oehl, "A helping human hand: relevant scenarios for the remote operation of highly automated vehicles in public transport," *Applied Sciences*, vol. 12, no. 9, p. 4350, 2022.

[16] N. Goodall, "Non-technological challenges for the remote operation of automated vehicles," *Transportation research part A: policy and practice*, vol. 142, pp. 14–26, 2020.

[17] R. C. Hampshire, S. Bao, W. S. Lasecki, A. Daw, and J. Pender, "Beyond safety drivers: Applying air traffic control principles to support the deployment of driverless vehicles," *PLoS one*, vol. 15, no. 5, p. e0232837, 2020.

[18] S. Gnatzig, F. Chucholowski, T. Tang, and M. Lienkamp, "A system design for teleoperated road vehicles," in *International Conference on Informatics in Control, Automation and Robotics*, vol. 2. SciTePress, 2013, pp. 231–238.

[19] C. Mutzenich, S. Durant, S. Helman, and P. Dalton, "Updating our understanding of situation awareness in relation to remote operators of autonomous vehicles," *Cognitive research: principles and implications*, vol. 6, pp. 1–17, 2021.

[20] D. Majstorović, S. Hoffmann, F. Pfab, A. Schimpe, M.-M. Wolf, and F. Diermeyer, "Driving from a distance," in *2022 IEEE international conference on systems, man, and cybernetics (SMC)*. IEEE, 2022, pp. 1290–1296.

[21] Y. Trabelsi, O. Shabat, J. Lanir, O. Maksimov, and S. Kraus, "Advice provision in teleoperation of autonomous vehicles," in *Proceedings of the 28th International Conference on Intelligent User Interfaces*, 2023, pp. 750–761.

[22] F. Tener and J. Lanir, "Driving from a distance: challenges and guidelines for autonomous vehicle teleoperation interfaces," in *Proceedings of the 2022 CHI conference on human factors in computing systems*, 2022, pp. 1–13.

[23] G. Sharma and R. Rajamani, "Teleoperation enhancement for autonomous vehicles using estimation based predictive display," *IEEE Transactions on Intelligent Vehicles*, 2024.

[24] Z. Yiyi, "Baidu's robotaxis orders surge, paving way for large-scale autonomous ride-hailing services (online)," https://www.globaltimes.cn/page/202407/1315784.shtml, accessed: 2024-07-10.

[25] A. Rosenzweig, "Regulators know teleoperation is key for self-driving vehicles to succeed," 2021.

[26] S. Lu, R. Zhong, and W. Shi, "Teleoperation technologies for enhancing connected and autonomous vehicles," in *2022 IEEE 19th International Conference on Mobile Ad Hoc and Smart Systems (MASS)*. IEEE, 2022, pp. 435–443.

[27] California Department of Motor Vehicles. (2026) Autonomous vehicles testing with a driver. Accessed: 2026-01-10. [Online]. Available: https://www.cpuc.ca.gov/regulatory-services/licensing/transportation-licensing-and-analysis-branch/autonomous-vehicle-programs

[28] C. S. Legislature, "AB 1777: Autonomous vehicles." Available: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202320240AB1777, January 2026, accessed: Jan. 10, 2026.

[29] M. Cummings, S. Li, D. Seth, M. Seong *et al.*, "Concepts of operations for autonomous vehicle dispatch operations," Collaborative Sciences Center for Road Safety, Tech. Rep., 2021.

[30] M. Gyllenhammar, M. Brännström, R. Johansson, F. Sandblom, S. Ursing, and F. Warg, "Minimal risk condition for safety assurance of automated driving systems," in *CARS: 6th International Workshop on Critical Automotive Applications: Robustness & Safety*, 2021.

[31] A. Daw, R. C. Hampshire, and J. Pender, "Beyond safety drivers: staffing a teleoperations system for autonomous vehicles," *arXiv preprint arXiv:1907.12650*, 2019.

[32] O. Carsten, "Human factors challenges of remote support and control a position paper from HF-IRADS," *Proc. Working Party Automated/Autonomous Connected Vehicles*, pp. 1–9, 2020.

[33] W. C. Adams, "Conducting semi-structured interviews," *Handbook of practical program evaluation*, pp. 492–505, 2015.

[34] C. Miller and C. Valasek, "A survey of remote automotive attack surfaces," *black hat USA*, vol. 2014, no. 2014, p. 94, 2014.

[35] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno, "Comprehensive experimental analyses of automotive attack surfaces," in *20th USENIX security symposium (USENIX Security 11)*, 2011.

[36] P. Jing, Z. Cai, Y. Cao, L. Yu, Y. Du, W. Zhang, C. Qian, X. Luo, S. Nie, and S. Wu, "Revisiting automotive attack surfaces: A practitioners' perspective," in *2024 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2024, pp. 2348–2365.

[37] P. I. Fusch Ph D and L. R. Ness, "Are we there yet? data saturation in qualitative research," 2015.

[38] A. Authors, "Online appendix," 2026, accessed: 2026-05-30. [Online]. Available: https://anonymous.4open.science/r/teleoperated cavs-3223/

[39] OpenAI, "Introducing whisper," 2022, accessed: 2025-05-29. [Online]. Available: https://openai.com/index/whisper/

[40] D. Cohen and B. Crabtree, "Qualitative research guidelines project," http://www.qualres.org/, 2006.

[41] V. Braun and V. Clarke, "Thematic analysis: A practical guide," 2021.

[42] N. McDonald, S. Schoenebeck, and A. Forte, "Reliability and inter-rater reliability in qualitative research: Norms and guidelines for CSCW and HCI practice," *Proceedings of the ACM on Human-Computer Interaction*, vol. 3, no. CSCW, pp. 1–23, 2019.

[43] S. Klivan, S. Höltervennhoff, R. Panskus, K. Marky, and S. Fahl, "Everyone for themselves? a qualitative study about individual security setups of open source software contributors," in *2024 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2024, pp. 1065–1082.

[44] P. Emami-Naeini, H. Dixon, Y. Agarwal, and L. F. Cranor, "Exploring how privacy and security factor into iot device purchase behavior," in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 2019, pp. 1–12.

[45] Ravie Lakshmanan. (2025) U.s. proposes ban on connected vehicles using chinese and russian tech. Accessed: 2025-05-29. [Online]. Available: https://thehackernews.com/2024/09/us-proposes-ban-on-connected-vehicles.html

[46] Larry Avila. (2025) Us finalizes ban on connected vehicle tech from china, russia. Accessed: 2025-05-29. [Online]. Available: https://www.automotivedive.com/news/federal-ruling-bans-sale-connected-vehicle-tech-china-russia/737325/

[47] M. Bozdal, M. Samie, and I. Jennions, "A survey on can bus protocol: Attacks, challenges, and potential solutions," in *2018 International Conference on Computing, Electronics & Communications Engineering (iCCECE)*. IEEE, 2018, pp. 201–205.

[48] F. Amato, L. Coppolino, F. Mercaldo, F. Moscato, R. Nardone, and A. Santone, "Can-bus attack detection with deep learning," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 8, pp. 5081–5090, 2021.

[49] Scale AI. (2025) Power with your data. Accessed: 2025-06-05. [Online]. Available: https://scale.com/

[50] H. B. 25-1122, "Automated Driving System Commercial Motor Vehicle," Available: https://leg.colorado.gov/sites/default/files/documents/2025A/bills/2025a_1122_enr.pdf, May 2025, accessed: May. 29, 2025.

[51] U.S. National Highway Traffic Safety Administration, "Ads-equipped vehicle safety, transparency, and evaluation program," https://www.nhtsa.gov/sites/nhtsa.gov/files/2024-12/nprm-av-step-2024-web.pdf, 2024, accessed: 2026-10-01.

[52] CVSA. (2025) Cvsa. Accessed: 2025-06-05. [Online]. Available: https://cvsa.org/

[53] CMV. (2022) Cvsa announces new enhanced cmv inspection program for autonomous truck motor carriers. Accessed: 2025-06-05. [Online]. Available: https://cvsa.org/news/new-enhanced-cmv-inspection-program/

[54] MISRA. (2025) Misra. Accessed: 2025-06-05. [Online]. Available: https://misra.org.uk/

[55] "Yeh v. tesla, inc., no. 3:23-cv-01704," https://www.classaction.org/media/yeh-v-tesla-inc.pdf, 2023, accessed: Oct. 5, 2026.

[56] Reuter, "Tesla workers shared sensitive images recorded by customer cars," https://www.reuters.com/technology/tesla-workers-shared-sensitive-images-recorded-by-customer-cars-2023-04-06/, 2023, accessed: Oct. 5, 2026.

[57] Tesla Inc, "Cabin camera," https://www.tesla.com/ownersmanual/model3/en_us/GUID-EDAD116F-3C73-40FA-A861-68112FF7961F.html, 2023, accessed: Oct. 5, 2026.

[58] Y. J. Jia, Q. A. Chen, S. Wang, A. Rahmati, E. Fernandes, Z. M. Mao, A. Prakash, and S. Unviersity, "Contexlot: Towards providing contextual integrity to appified iot platforms." in *ndss*, vol. 2, no. 2. San Diego, 2017, pp. 2–2.

[59] P. Wijesekera, A. Baokar, A. Hosseini, S. Egelman, D. Wagner, and K. Beznosov, "Android permissions remystified: A field study on contextual integrity," in *24th USENIX Security Symposium (USENIX Security 15)*, 2015, pp. 499–514.

[60] F. Roesner, T. Kohno, A. Moshchuk, B. Parno, H. J. Wang, and C. Cowan, "User-driven access control: Rethinking permission granting in modern operating systems," in *2012 IEEE Symposium on Security and Privacy*. IEEE, 2012, pp. 224–238.

[61] A. Rahmati and H. V. Madhyastha, "Context-specific access control: Conforming permissions with user expectations," in *Proceedings of the 5th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices*, 2015, pp. 75–80.

[62] U. D. of Justice Archives, "Ohio man sentenced to life in prison for federal hate crimes related to august 2017 car attack at rally in charlottesville, virginia," https://www.justice.gov/archives/opa/pr/ohio-man-sentenced-life-prison-federal-hate-crimes-related-august-2017-car-attack-rally, 2022, accessed: 2025-06-05.

[63] A. News, "Chinese plane crash that killed 132 caused by intentional act: Us officials," 2022, accessed: 2025-06-05. [Online]. Available: https://abcnews.go.com/International/chinese-plane-crash-killed-132-caused-intentional-act/story?id=84782873

[64] F. Z. Borgesius, H. Asghari, N. Bangma, and J.-H. Hoepman, "The gdpr's rules on data breaches: Analysing their rationales and effects," *SCRIPTed*, vol. 20, p. 352, 2023.

[65] F. Nahai, "General data protection regulation (gdpr) and data breaches: What you should know," pp. 238–240, 2019.

[66] S. Romanosky, A. Acquisti, and R. Sharp, "Data breaches and identity theft: When is mandatory disclosure optimal?" TPRC, 2010.

[67] L. Zhao, M. Nybacka, M. Aramrattana, M. Rothhämel, A. Habibovic, L. Drugge, and F. Jiang, "Remote driving of road vehicles: A survey of driving feedback, latency, support control, and real applications," *IEEE Transactions on Intelligent Vehicles*, pp. 1–22, 2024.

[68] C. Bloom, J. Tan, J. Ramjohn, and L. Bauer, "Self-driving cars and data collection: Privacy perceptions of networked autonomous vehicles," in *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. Santa Clara, CA: USENIX Association, Jul. 2017, pp. 357–375. [Online]. Available: https://www.usenix.org/conference/soups2017/technical-sessions/presentation/bloom

[69] I. Krontiris, K. Grammenou, K. Terzidou, M. Zacharopoulou, M. Tsikintikou, F. Baladima, C. Sakellari, and K. Kaouras, "Autonomous vehicles: Data protection and ethical considerations," ser. CSCS '20. New York, NY, USA: Association for Computing Machinery, 2020. [Online]. Available: https://doi.org/10.1145/3385958.3430481

[70] S. Reig, S. Norman, C. G. Morales, S. Das, A. Steinfeld, and J. Forlizzi, "A field study of pedestrians and autonomous vehicles," in *Proceedings of the 10th International Conference on Automotive User Interfaces and Interactive Vehicular Applications*, ser. AutomotiveUI '18. New York, NY, USA: Association for Computing Machinery, 2018, p. 198–209. [Online]. Available: https://doi.org/10.1145/3239060.3239064

[71] Z. Cai and A. Xiong, "Effects of knowledge and experience on privacy decision-making in connected autonomous vehicle scenarios," in *Proceedings of the Workshop on Usable Security (USEC'22)*, 2022, pp. 1–18.

[72] ——, "Understand users' privacy perception and decision of V2X communication in connected autonomous vehicles," in *32nd USENIX Security Symposium (USENIX Security 23)*. Anaheim, CA: USENIX Association, Aug. 2023, pp. 2975–2992. [Online]. Available: https://www.usenix.org/conference/usenixsecurity23/presentation/cai-zekun

[73] J. Sun, Y. Cao, Q. A. Chen, and Z. M. Mao, "Towards robust LiDAR-based perception in autonomous driving: General black-box adversarial sensor attack and countermeasures," in *29th USENIX Security Symposium (USENIX Security 20)*. USENIX Association, Aug. 2020, pp. 877–894. [Online]. Available: https://www.usenix.org/conference/usenixsecurity20/presentation/sun

[74] Y. Cao, C. Xiao, B. Cyr, Y. Zhou, W. Park, S. Rampazzi, Q. A. Chen, K. Fu, and Z. M. Mao, "Adversarial sensor attack on lidar-based perception in autonomous driving," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '19. New York, NY, USA: Association for Computing Machinery, 2019, p. 2267–2281. [Online]. Available: https://doi.org/10.1145/3319535.3339815

[75] Y. Cao, N. Wang, C. Xiao, D. Yang, J. Fang, R. Yang, Q. A. Chen, M. Liu, and B. Li, "Invisible for both camera and lidar: Security of multi-sensor fusion based perception in autonomous driving under physical-world attacks," in *2021 IEEE Symposium on Security and Privacy (SP)*, 2021, pp. 176–194.

[76] C. Yan, W. Xu, and J. Liu, "Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle," vol. 24, no. 8, 2016, p. 109.

[77] K. Eykholt, I. Evtimov, E. Fernandes, B. Li, A. Rahmati, C. Xiao, A. Prakash, T. Kohno, and D. Song, "Robust physical-world attacks on deep learning visual classification," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2018, pp. 1625–1634.

[78] D. Song, K. Eykholt, I. Evtimov, E. Fernandes, B. Li, A. Rahmati, F. Tramèr, A. Prakash, and T. Kohno, "Physical adversarial examples for object detectors," in *12th USENIX Workshop on Offensive Technologies (WOOT 18)*. Baltimore, MD: USENIX Association, Aug. 2018. [Online]. Available: https://www.usenix.org/conference/woot18/presentation/eykholt

[79] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, "Experimental security analysis of a modern automobile," in *2010 IEEE Symposium on Security and Privacy*, 2010, pp. 447–462.

[80] J. M. Ernst and A. J. Michaels, "Lin bus security analysis," in *IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society*, 2018, pp. 2085–2090.

[81] D. K. Nilsson, U. E. Larson, F. Picasso, and E. Jonsson, "A first simulation of attacks in the automotive network communications protocol flexray," in *Proceedings of the International Workshop on Computational Intelligence in Security for Information Systems CISIS'08*, E. Corchado, R. Zunino, P. Gastaldo, and Á. Herrero, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 84–91.

[82] F. Martinelli, F. Mercaldo, A. Orlando, V. Nardone, A. Santone, and A. K. Sangaiah, "Human behavior characterization for driving style recognition in vehicle system," *Computers & Electrical Engineering*, vol. 83, p. 102504, 2020. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0045790617329531

[83] D. R. Stinson and M. Paterson, *Cryptography: theory and practice*. CRC press, 2018.

[84] J. H. Kim, S. Seo, N. Hai, B. M. Cheon, Y. S. Lee, and J. W. Jeon, "Gateway framework for in-vehicle networks based on CAN, FlexRay, and ethernet," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 10, pp. 4472–4486, 2015.

[85] R. S. Sandhu and P. Samarati, "Access control: principle and practice," *IEEE Communications Magazine*, vol. 32, no. 9, pp. 40–48, Sep. 1994. [Online]. Available: https://doi.org/10.1109/35.312842

[86] K. Ren, Q. Wang, C. Wang, Z. Qin, and X. Lin, "The security of autonomous driving: Threats, defenses, and future directions," *Proceedings of the IEEE*, vol. 108, no. 2, pp. 357–372, 2020.

[87] Q. Zhang, H. Zhong, J. Cui, L. Ren, and W. Shi, "AC4AV: a flexible and dynamic access control framework for connected and autonomous vehicles," *IEEE Internet of Things Journal*, pp. 1–1, 2020.

Appendix A. Meta Review

The following meta-review was prepared by the program committee for the 2027 IEEE Symposium on Security and Privacy (S&P) as part of the review process as detailed in the call for papers.

A.1. Summary

This paper examines the security, privacy, and safety challenges of teleoperated connected and autonomous vehicles (CAVs) through semi-structured interviews with 16 experts from industry and academia. The paper identifies risks associated with teleoperation and discusses implications for access control, safety, privacy, and regulation.

A.2. Scientific Contributions

- Provides a Valuable Step Forward in an Established Field
- Establishes a New Research Direction

A.3. Reasons for Acceptance

1) The paper provides a valuable step forward in an understudied area. Reviewers found the interview study timely and useful, particularly the findings on remote operator access, teleoperation-specific attack surfaces, access to interior sensors, and the interaction between operator authority and vehicle safety constraints.
2) The paper also helps establish a research direction around security and privacy in CAV teleoperation. While some findings overlap with broader CAV security issues, the paper highlights how teleoperation can introduce or amplify these risks and motivates further work on access control, insider threats, safety mechanisms, privacy, and regulation.