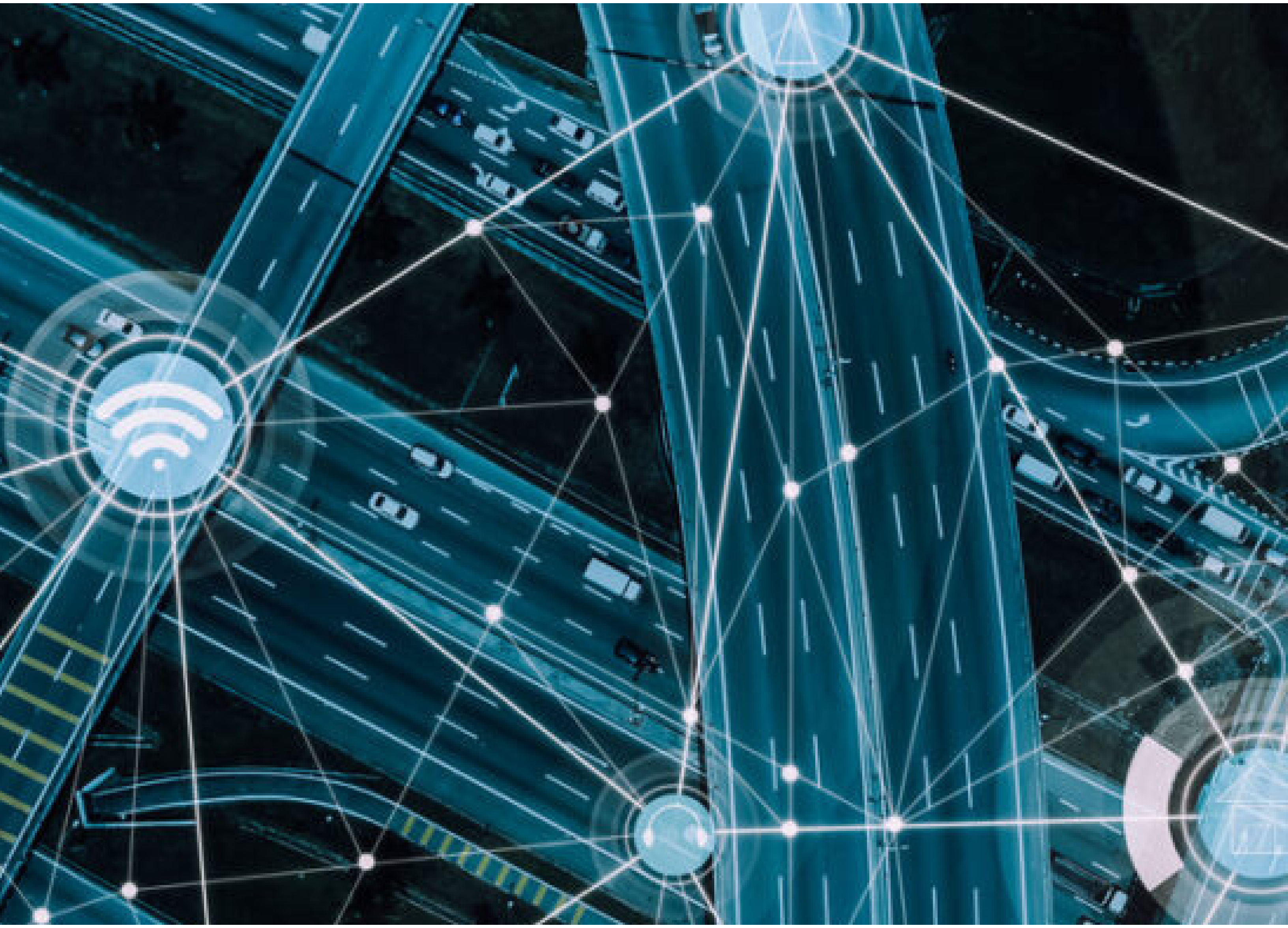
QA Consultants

October, 2022



Privacy and Cybersecurity Challenges in Vehicle Teleoperation and Mitigation Approaches

APMA
LEAD. REACH. CONNECT.

Supported by APMA V2X Cybersecurity Committee

Contents:

Introduction

Vehicle teleoperation uses the advances in vehicular autonomy—while also taking the advantage of human vigilance.

In recent years, significant progress has been made in developing Autonomous Vehicles (AVs). Many companies, including Google Waymo, General Motors, Argo AI, and Baidu, are testing SAE Level-4 vehicles on public roads in predefined geographical areas under a specific set of conditions with human assistance.

Nevertheless, debuting SAE Level 5 fully autonomous vehicles on public roads has not reached prime time due to the technical and regulatory challenges [1]. One of the reasons is that AVs rely on Machine Learning (ML) algorithms to perceive the environment and make safety-critical driving decisions. While non-deterministic ML algorithms' performance is more accurate in detecting hazardous scenarios known as "edge cases" than rule-based systems, 100% accuracy has yet to be achieved. Often, to prevent accidents and provide a safe maneuver, a human operator is required in the vehicle when autonomous vehicles encounter an "edge case". Requiring a human operator to be physically in the vehicle reduces the cost saving benefits of an autonomous vehicle.

A possible interim solution to capture the advantages of autonomous vehicles without having a safety driver behind the wheels is Teleoperated Driving (ToD). In ToD, a remote operator (RO) takes control of the vehicle when necessary and handoffs control to the vehicle when required. Sometimes RO only assists the AV to make the right decision. Hence, in ToD a human driver is always controlling the vehicle from a regulatory perspective.

Remote controlling a vehicle on the public road is difficult. ToD requires a highly reliable data-dependent system where the vehicles generate and share large volumes of data with teleoperation control centers and other stakeholders. This data dependency widens the attack surface and the likelihood of physical and cyber-attacks. The implications of cybersecurity weakness of ToD directly impact the safety of passengers, pedestrians, other vehicles, related infrastructures as well as personal privacy. In addition, ToD needs to address many technical challenges, including, but not limited to, latency, deterioration or loss of connection, reduced situation awareness, and human frailty. Therefore, safely implementing and managing ToD in society is non-trivial, presenting many challenges to public safety.

This white paper aims to raise awareness about the potential risks associated with vehicle teleoperation. First, we inform the reader about the challenges and opportunities of vehicle teleoperation. Afterward, we explore the data privacy and cybersecurity challenges and provide recommendations to mitigate these challenges.

Vehicle Teleoperation: In a Nutshell

The history of teleoperation goes back to the 1870s, with inventors working on remotely operated weapons. Since then, a variety of teleoperated services have emerged.

In AV teleoperation, the remote operators (ROs) or the teleoperators act as the safe backup for AVs. ROs are trained drivers who monitor and manage vehicles simultaneously depending on teleoperation services and speak with passengers in an emergency.

For safe driving, an RO needs to understand the car's surroundings. Therefore, data is collected from in-vehicle sensors, such as camera, lidar, radar, and outer components, including vehicles and infrastructure, then transmitted to the teleoperation center through a stable and reliable cellular network. After analyzing the data and real-time video, RO assists the vehicle or takes control of the vehicle. The feedback of the RO is sent back to the vehicle for execution.

Use Cases of ToD

Vehicle teleoperation acts as a catalyst to smooth the transition from human driving to self-driving vehicles.

Based on the level of control the RO has on the vehicle, the AV teleoperation services can be divided into three categories :

- **Remote management of AVs.** In this mode of operation, the RO monitors the AV fleet and assists AVs when AVs move or deviate from a prescribed path.
- **Remote assistance to AVs.** The RO does not remotely drive the vehicle in this mode of operation. The driver only provides information and guides AVs to continue safe navigation when encountering edge cases. Also, the RO may offer services to passengers in the vehicles if a passenger wants to speak with a RO. For example, Google Waymo has a team of humans remotely monitoring the cars and assists the vehicle by providing information [2].

- **Remote control of AVs.** In this mode of operation, RO directly control the vehicles for a substantial amount of time by performing all aspects of driving, including steering, acceleration, and braking. Recently, Vay Taxi in Germany has launched this type of affordable door-to-door transportation [3]. In this type of service, the passenger can order a car, which arrives within a few minutes operated by the RO and then the passenger drives the car to the destination. Upon reaching the destination, the passenger leaves the car without parking it, and the RO regains control of the vehicle and takes it to the hub.

Technological Considerations in ToD

Safest ToD is not possible without leveraging the vehicle's autonomous features.

The automotive industries need to address several technical requirements for enabling safe ToD including:

- **Reliable and ultra-low latency communication.** Teleoperation relies on cellular networks to transfer information between the vehicle and RO. Broad coverage, high data throughput, and ultra-low latency are the most apparent telecommunication requirements for successful teleoperation. Since the vehicle can be in motion most of the time, good network coverage is essential for a stable connection. The unstable connection causes frame loss in video streaming. If connectivity isn't stable, video streaming will be interrupted, and the RO will have to wait for the video to render, which is simply unacceptable. For good coverage, teleoperation requires connecting to multiple network operators simultaneously.

- **Perception module design.** The self-driving system fails when the scenarios are unrecognizable, or multiple conflicting rules are derived. Calling human assistance at the right time depends on the design of an efficient perception module design. To this end, the self-driving car compares the perceived 3D map with the cached 3D map of the road, traffic signs/lights, and surrounding buildings. If the perception module detects road blockage or road signs that were not cached, it tries to understand the situation and transfers the control to a remote human operator if it fails. Designing the critical safety system to identify and transfer control to the human operator is not easy.

- **Human-machine interface design.** ROs control the vehicle using a workstation with a specific human-machine interface (HMI) from the teleoperation control center. The performance of the RO depends on situation awareness. Therefore, one of the main concerns in designing the workstation is increasing the RO's situation awareness. A most common or straightforward approach to developing a teleoperation HMI is using several displays to display the transmitted sensor data and various control options to the RO. However, representing so much data to RO may confuse the decision-making process. Therefore, minimizing the number of visual stimuli on HMI display while ensuring operation safety is challenging. The head-mounted display (HMD) is another option for the RO to visualize the video. The HMD allowed for more visibility around the vehicle, and the RO feels safer than with the regular monitor. However, a recent study shows that using a head-mounted display is insufficient to improve RO's performance [4]. A combined approach with virtual reality and augmented sensor data [5] could help to make ToD safer.

- **Nearly real-time processing.** As the vehicle is controlled remotely, the vehicle's sensors, cameras, and systems must provide sufficient data to enable safe teleoperation. The processing time for sensor data and video compression algorithms, or actuation delay, needs to be kept short as possible to reduce latency. It is also required to pay attention in designing network infrastructures and communication protocols to reduce the overall latency. Selecting a suitable teleoperation center is crucial to avoid any safety issues.

- **Required advanced safety features.** The teleoperated vehicle should be equipped with advanced safety features that react automatically in emergencies. For example, the vehicle's safety features can break or take an evasive maneuver in a sudden signal loss.

Challenges in ToD

Teleoperators face numerous challenges, including, but not limited to, signal latency, signal loss, managing AV capabilities, situation awareness.

- **Signal loss**. Teleoperated driving depends on the information exchange between the vehicle and the remote driver. A stable network connection must be maintained during teleoperation. If connectivity is not stable, data communication will be interrupted, which poses a significant risk if the vehicle requires remote assistance at that particular moment.

- **Signal Latency.** Large latency is one of the biggest challenges in safe teleoperation. Latency in the network leads to a lag in the RO's visualization and results in unstable real-time control of the remote vehicle. Though ultra-low latency and ultra-reliable 5G (1 millisecond) [6] could be sufficient to mitigate this problem, the deployment of 5G is far from widespread.

- **Automation bias.** Remote drivers may be susceptible to the automation bias. It could happen when the vehicle fails to detect a problem, and the RO does not notice it because he did not appropriately monitor the environment due to his overreliance on vehicles' autonomy.

- **Situation Awareness.** Another challenge in ToD is reduced situation awareness or weak feelings of telepresence. Due to the low field of view of cameras, delays over network transmission, and the lack of sensory information, such as sounds and vibrations, it is hard for a RO to develop a similar level of situation awareness as a driver seated in the vehicle.

- In addition, fatigue, distraction, or mistakes of RO also influence RO's performance in teleoperation.

5

6

Opportunities in ToD

ToD is an interim solution to realize the benefits of automated vehicles within existing regulatory frameworks.

ToD has been gaining momentum in several countries. ToD is providing several social and economic opportunities, including but not limited to:

- **Teleoperated driving accelerates AV deployment.** Where regulations allow, Teleoperation can replace the need for having a safety driver behind the wheels during AV's testing on the public road**.**
- **Employment opportunities.** Teleoperated driving could bring significant labor benefits. The RO can work from the same place every day and receive a predictable income. In addition, he/she does not need to bear the costs and uncertainty of owning and maintaining a vehicle.
- **New job creations**. Teleoperated driving may help reduce the driver shortage problem in the supply chain and logistic industry. Furthermore, it enables gender-balanced employment opportunity.
- **Transit in a pandemic.** Since RO and rider are located separate from the vehicle, the health and safety for both the passengers and drivers is protected from COVID related infection.
- **Reduced costs.** Owning a car can be expensive. The owner needs to pay insurance, parking, and maintenance costs. In teleoperated vehicle rental services, an individual can enjoy driving without possessing the vehicle.
- **Improved accessibility for underserved populations.** Mobility is essential for a rich, productive, and healthy life. In society, older people, impaired, adolescents, and indigents face mobility challenges. ToD may provide more efficient transportation that helps these people overcome the obstacles of limited mobility and get access to the associated social and economic benefits.

AV Regulation Status and ToD

The regulation of AV's faces unique legal challenges. At this time, twenty-nine states and Washington D.C have enacted legislation, and eleven states have issued executive orders regarding the testing and operation of self-driving vehicles. However, there must be a human in the loop during the testing of an AV on a public road.

As ToD services continue to be adopted, several countries have added teleoperation to their AV regulation, including Canada, the US, Finland, the Netherlands, and England [7]. In the recent release of Transport Canada's Guidelines for Testing Automated Driving Systems in Canada Version 2.0 [8], which replaced the previous 2018 guidelines for testing highly automated vehicles in Canada [9], Transport Canada emphasizes the safe management of remote driving. In its assessment, there is a lack of evidence the safety-related risks of remote driving can be adequately managed. Therefore, Transport Canada does not currently support the safe conduct of remote driving use cases. In 2018, California included teleoperation as part of its regulation for driverless vehicles. Many states like Arizona, Michigan, Ohio, Texas, and recently Florida have legislated that an AV must have a teleoperation system for supervising the autonomous vehicle. Recently, Germany has also included teleoperation under the category "Technical Supervision" in the German AV rules [10].

Data Privacy in ToD

Teleoperation can support several forms of vehicle provision, like car-rental or ride-hailing/sharing, logistic fleet, and more. Today's connected vehicle collects massive data (approximately 25GB [11]) per hour. Since teleoperated vehicles take pictures of the vehicles' surroundings during operation, they typically gather more data than a usual connected shared vehicle. Some of this data is collected automatically without consumers' acknowledgments. Sometimes data is collected to enable certain features chosen by consumers.

The data collected by the teleoperated vehicle may contain sensitive personal information. Therefore, the services that collect and use data of the teleoperated vehicle should strictly consider privacy policies; otherwise, sharing this data may pose risks to privacy and security.

Common Types of Collected Data

A general overview of the types of data collected by a connected vehicle, with or without consumers' acknowledgment:

- **Telematics information.** Telematics devices collect data from vehicles' onboard modem and diagnostics (ODB-II) and send data to the cloud using wireless networks. Telematics data include location, speed, vehicle diagnostics, braking, acceleration, fuel consumption, and idling time. Navigation software also may collect the vehicle's location and travel history to route to the destination.
- **Event data recorders.** Today, around 90% of vehicles are equipped with event data recorders (EDRs). EDRs record a vehicle's operation before and after a crash, including speed, acceleration, and brake position, seat belt usage, and whether the airbags deployed or not.

- **Vehicles' surroundings information.** Onboard sensors and cameras collect information about vehicles' surroundings to detect road, weather conditions, lane markings, obstacles, surrounding traffic, and more. Key technologies such as assisted braking, blind-spot detection, lane-departure warnings, rear-parking detection, and vehicle teleoperation depend on this data.
- **In-cabin information.** Microphones, cameras, and other devices inside the vehicles may record information about vehicle occupants. Sensors are integrated in-vehicle parts that collect airbag and seatbelt status, engine temperature, and current location. This information is then transmitted back to the automaker or third parties.
- **User recognition.** Modern vehicles also employ sensors to collect biometric information such as voice, fingerprint, facial patterns to identify the individual behind the wheels and adjust the systems accordingly.

Who Has Access to What Data?

- Automakers have access to a wide range of vehicle data, customers' and remote drivers' accounts information, remote drivers' behavior data (e.g., speed, seat belt use, braking habits), vehicle location data, and data from customers' smartphones due to connecting with the infotainment systems.
- Rental car and car-sharing services have access to vehicles' location data, travel data (e.g., current location, destination, speed, route, date, and time), vehicle health data, driver behavioral data, and customers' accounts information.
- Teleoperation service providers access the vehicle data, video feeds surrounding the vehicles and in-vehicle environments, remote drivers' behavior data with additional information about the customers and remote drivers' identities and accounts.
- Ridesharing and other mobile applications gain access to the customers' smart devices and gather additional personal information directly from users, devices, or social networking sites.
- Insurance companies could access remote drivers' behavior and vehicle location data via telemetric devices to assess risk and determine the insurance premium of a particular remote driver.
- Aftermarket telematics service providers have access to the vehicle, remote driver's behavior, and location data.
- Government agencies and foreign government bodies may have access to real-time telematics and location data through data-sharing arrangements with OEMs and mobility service provides.
- Insurance companies could access remote drivers' behavior and vehicle location data via telemetric devices to assess risk and determine the insurance premium of a particular remote driver.

Teleoperated Vehicles' Data Uses

Both public and private sectors can benefit from the generated and collected data of teleoperated vehicles as follows:

- **Development of fully autonomous vehicles.** The interaction between the vehicle and the remote driver in various scenarios is collected from teleoperated vehicles. This collected data provide helpful information to improve the AV software qualities and capabilities. Since the performance of ML relies on the availability of large amounts of training data, some autonomous vehicle companies, including Waymo, Argo, and Aptiv, have been releasing their data sets publicly for use by other researchers [12].
- **Transportation system management.** Teleoperated vehicles data provide real-time information about the movement of the vehicles, traffic congestion, and weather conditions. These data can enhance safety and efficiency in traffic flow management in the transportation sector. This data also can be used for policy development and better transportation law enforcement.
- **Automakers use vehicle data for many purposes.** OEM and parts manufacturers have access to a wide range of vehicle data, including vehicle health data, driver behavior data, vehicle location data, and all data passing through telematics and infotainment systems. They may use these data for various purposes, such as monitoring vehicle health, performing remote diagnostics for preventative maintenance, and offering over-the-air software updates, thereby reducing recall and warranty costs.
- **Shared mobility services.** Shared mobility services rely on vehicles' data for booking, billing, and efficiently managing vehicle fleets. This data help mobility service providers to identify gaps and opportunities in meeting users' needs.

- **Auto insurers.** Insurance companies could use driver behavioral information (e.g., how fast the individual drives, the driving speed, how aggressively the brakes are applied, etc.) and geolocation data (e.g., the individual's location, the route, and the destination) to determine the insurance rates of an individual.
- **Public safety and law enforcement.** Sharing vehicles' data with emergency response data platform can significantly reduce response times. Telemetry data, GPS location data can be used by first responders when an accident occurs to get first responder on scene faster.

Privacy Implications of Teleoperated Vehicle Data

Data privacy risks are not unique to teleoperated vehicles but may be exacerbated due to the streaming of video data and involving more stakeholders in the ecosystem.

In addition to vehicle data, ToD may collect various types of personal and non-personal data about the vehicle's passengers and drivers, including passengers' in-vehicle activities, passengers' trip history, vehicle locations, biometric and health data, remote driver's behavior data, and passengers' private communications, contacts, web browsing data, and infotainment preferences [13]. Furthermore, it collects the data of the people in the vehicle's surrounding environment without their acknowledgment while running on the public roads. This data may reveal a lot of information about the individual, such as a person's lifestyle, religious and political association, personal preferences, and more, which may cause risks to personal privacy.

Since various organizations have access to different types of data generated by teleoperated vehicles, governance clarity is required around the data ownership, privacy and data monetization [13].

Many Canadians are legitimately wary about the privacy risks associated with vehicle data. Over 80% of Canadians surveyed were concerned about the privacy risks of this technology and believed that consumers should have exclusive rights over control and access to their data [14].

Hence, protecting the personal information of drivers and passengers is an important concern in ToD. Since teleoperated vehicles may travel from one country to another, data interoperability and privacy between states and mobile network operators also create new challenges.

Data Privacy Legislation and Regulations

In Canada, the Personal Information Protection and Electronic Documents Act (PIPEDA) regulates how private-sector organizations handle personal information [15]. However, PIPEDA does not deal with data protection rules that apply directly to connected autonomous shared vehicles. In 2019, Canada developed a best practice code on data handling of connected autonomous vehicles (CAV), namely "A Privacy Code Practice for the Connected Car" [16], outlining the best practices for data handling in the CAV sector. Unlike PIPEDA, this code is opposed to endorsing legal compliance; it guides collecting and sharing data practices in the CAV sector.

Several US states have enacted legislation around data privacy issues related to EDR (event data recorder). Under these laws, vehicle owners' consent is required to download EDR data without exceptional situations [17]. In 2020, the California Consumer Privacy Act (CCPA) provided privacy rights to consumers to know about the personal information a business collects about them and opt-out of sharing their data [18]. In the EU, the General Data Protection Regulation (GDPR) protects personal data [19]. However, it does not provide any specific data protection rules that apply directly to connected shared vehicles. In 2017, the French data protection authority (Commission Nationale de l'informatique et des libertés) developed a reference framework for collecting and sharing personal data by connected vehicles, incorporating GDPR and French data protection law [20].

Cybersecurity of ToD

It has been noted that connected non-autonomous vehicles have over 69 attack points those attackers can exploit [21]. This number increases further in the case of autonomous vehicles. Since, ToD takes advantage of the vehicle's autonomy while maintaining the vehicle-to-human communication over a wireless link to control the vehicle, it may inherit all the threats associated with autonomous vehicles with several unique threats depending on the teleoperation mode. Furthermore, the consequences of hacking teleoperated vehicles used in mobility services may be much more severe than with conventional connected vehicles. ToD opens more doors for ransomware attacks by ordinary criminals and sophisticated attacks to critical infrastructure by aggressive nation-states.

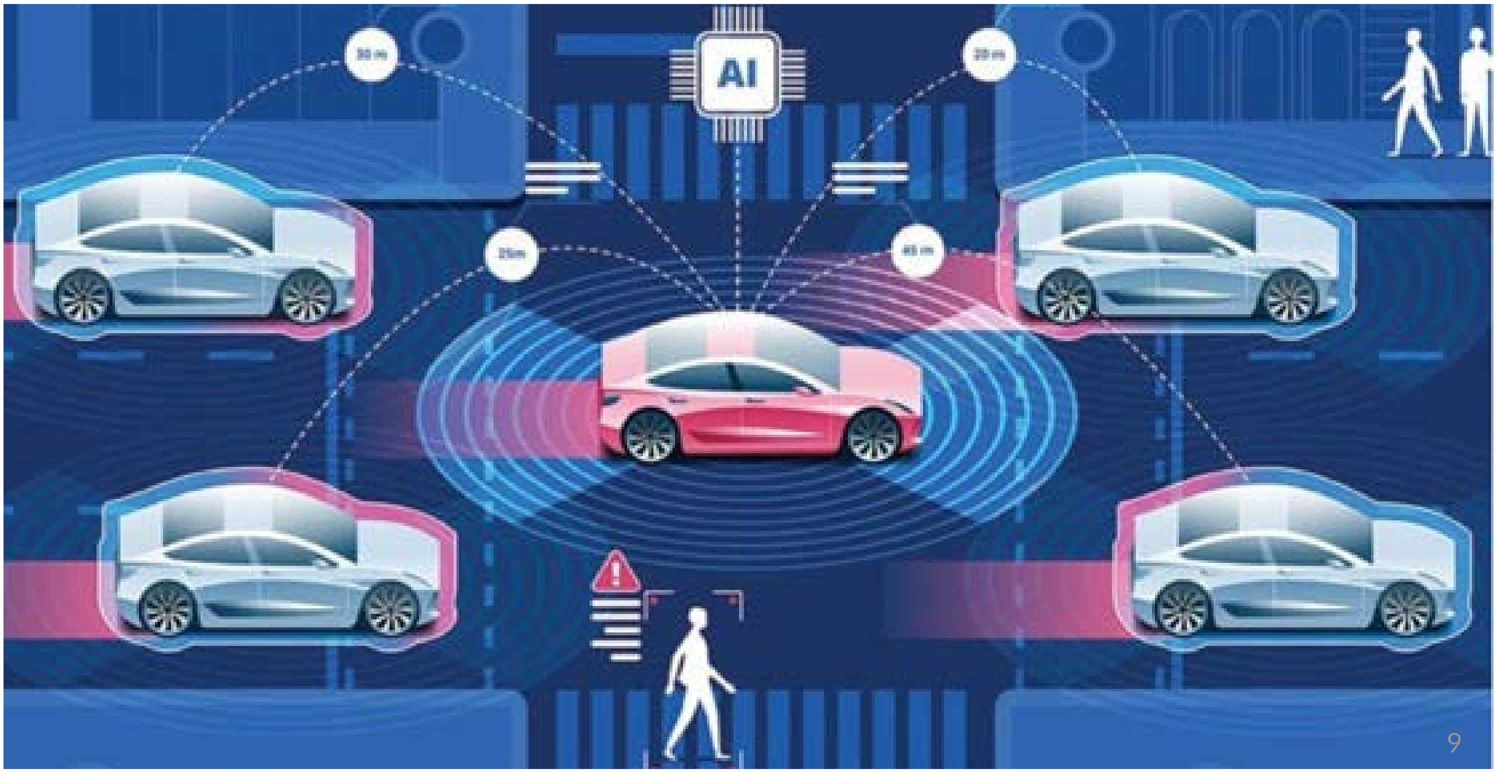
Before discussing the unique security challenges of teleoperated vehicles, we focus on the associated risks of autonomous vehicles.

Design of Autonomous Vehicles

When analyzing the security of a system and identifying the associated threats, it is essential to understand the system's underlying architecture. AV observes and perceives the surrounding environment, makes decisions to reach the desired location safely, and takes actions based on these decisions to control the vehicle. Three main types of data processing modules are involved in autonomous vehicles [22] such as:

- **Perception module.** AV depends on the perception module that collects information from onboard sensors and extracts the relevant information from them to understand the scene. This includes detection and tracking and positioning over time of vehicles, pedestrians, and objects, recognition of traffic, and element of interest for the driving.
- **Planning module**. This module calculates the trajectory that the vehicle will undertake to reach the destination. It takes appropriate decisions for the vehicle's movement after analyzing the data received from the perception unit, inter-vehicle communication, and the control unit's feedback.
- **Control module**. This module is responsible for implementing the decision taken by the planning module through a large number of Electronic Control Units (ECUs).

The functionalities of these data processing modules are dependent on intra-vehicle and inter-vehicle communications. The increased levels of communications make the autonomous vehicle more vulnerable to security attacks.



Vulnerabilities of Having V2X and Physical Connections

AVs sense the surroundings using a variety of onboard sensors, including cameras, lidar, and radar. The Lidar data is integrated with digital images that enable the vehicle to precisely understand its position on the road. Also, radar is used to detect nearby objects and their proximity.

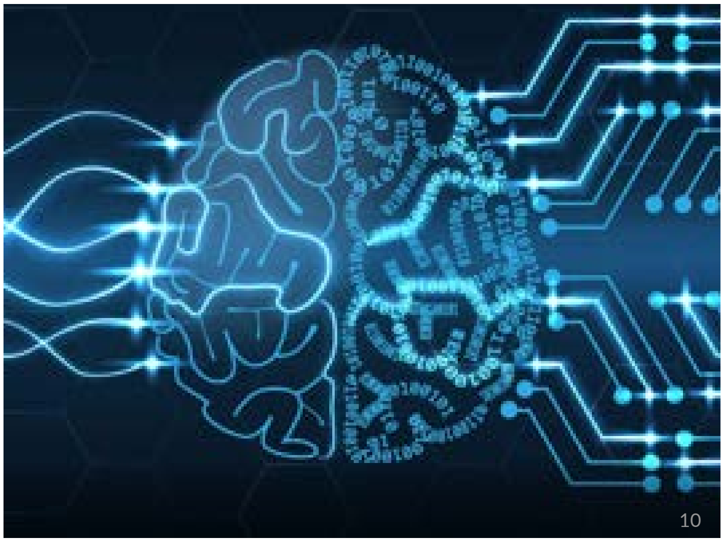
In addition, AVs require managing continuous communication with other vehicles on the road (V2V), roadside infrastructure (V2I), and cloud services to upgrade the software and store data. This connectivity opens access to various sophisticated and highly damaging attacks. For example, an attacker could send false GPS signals or fake V2X safety messages through spoofing attacks to mislead the vehicle and disrupt the traffic flows [23]. Moreover, an attacker might attempt a denial-of-service (DoS) attack and prevent the vehicle from receiving critical messages from other vehicles and roadside units. Various cybersecurity attacks can exploit V2X communication, including, but not limited to, DoS attacks, distributed denial-of-service (DDoS) attacks, man-in-the-middle (MitM) attacks, phishing, injection attacks, jamming, eavesdropping attack, and malware attacks.

Furthermore, attackers could access autonomous vehicles through physical connections such as a USB interface or the vehicle's onboard diagnostics port. A malware-harboring vehicle at dealerships or auto mechanics for service could inadvertently spread the malware to other vehicles.

Vulnerabilities of AI Software Components

AV is highly dependent on AI software for making high stake decisions. Successful cyberattacks against AI software stakes may confuse the AV to ask the assistance of remote drivers that directly impact the safety of passengers, pedestrians, vehicles, and infrastructure. Therefore, it is essential to investigate potential vulnerabilities due to the usage of AI.

An AI system may fail due to the adversarial attacks on the algorithms and data, or the inherent design flaws of the system [24]. AV employs deep learning algorithms to classify the camera-captured traffic sign image and then control the vehicle according to the classification results. Evasion and poisoning attacks are the two most distinguishable adversarial attacks on the DNN model. Evasion attack manipulates what is fed into the DNN model to produce a system output that seems typical for a human but is wrong in that the image now shows something differently classified by DNN. In a digital domain, an attacker takes an image and changes some pixels to convince the DNN model that the image now shows something different.


10

On the other hand, poisoning attacks have the potential to corrupt the training so that the resulting system malfunctions in a way desired by the attacker. The research exploring vulnerabilities in machine learning algorithms has gained much attention in the last decade.

Several examples of physical malicious attacks on AI components of semi-autonomous cars were reported in recent years. One notable instance of physical aggression is Deceiving Autonomous vehicles with Toxic Signs (DARTS) [25]. The authors created a pipeline for upscaling adversarial perturbation to a printable size and used the real-size printed signs to deceive autonomous vehicles' traffic sign recognition systems. Another example is misleading a Tesla car by slightly elongating the middle line in "3" to read 85 mph instead of 35mph [26].

Classical Cyberattacks Against ToD Systems

Any classical cyberattacks against teleoperation components: control station, in-vehicle software module, and the communication channel may lead to catastrophic consequences. A malicious attacker can attempt a denial of service (DoS) attack that blocks all communications between the vehicle and the control station. Also, an attacker can gain unauthorized access to the vehicle controls through the injection of fake control messages to cause the vehicle to crash and damage humans or infrastructures. Other scenarios include an attacker injecting fake video messages to the teleoperator to interrupt the teleoperation or an attacker may access sensitive information on the vehicle and passenger, compromising confidentiality.

AI-powered Cyberattacks Against ToD systems

Today, AV teleoperation is still in a nascent stage and dependent on the remote human operator to overcome difficult driving situations. It is expected that cloud-based automated teleoperated driving will evolve in the future. The automated teleoperator, an AI-based software agent in the cloud, will collaborate with the self-driving intelligence on the vehicle and RO and take more control from the RO [27]. Although it may reduce the cost and drawbacks of human teleoperators, such an approach opens more doors for the attacker. It may make digital adversarial attacks feasible against the cloud-based automated teleoperator. Moreover, applying advanced AI techniques to launch deep fake attacks for altering the road sign or cloning the voice of the passengers in the vehicle is not impossible.

Attack Scenarios Related with ToD

Considerable research effort should be taken to identify the vulnerabilities of ToD. Some of the potential attack vectors include:

- **Gaining remote access to computers in the teleoperation center.** The attacker can access the computer in the control station via outdated software installed on the computer. In this type of attack, the attacker runs malicious code in a teleoperation computer to control all the vehicles served by this computer. Examples: an attacker may trick the teleoperator into installing the malware in any of the computers in the control center, and then, this malware spreads across the network.
- **Attacker gains physical access to the vehicle network.** An attacker may gain physical access to the vehicle network during car maintenance and install a malicious piece of software in the vehicle computer. Then this malicious software is used to apply small perturbations to the captured images that result in misclassification in object detection.
- **Gaining physical access to computers in the teleoperation center**. The attacker may gain physical access to a teleoperation computer and use the computer to control a vehicle. Examples include unauthorized entry into the teleoperation control system and the employment of an attacker as a driver. Controls against this attack include improving the physical security of the vehicles.
- **Attacker gains remote access to the vehicle network**. An attacker may remotely exploit the vulnerability of the vehicle head unit (HU) and get access to the vehicle's internal network. Controls against this attack include improving the physical security of the vehicles.
- **Attacks targeting communication channels**. Communication channels' security should be paramount in AV teleoperation, as the communication channels transmit critical information between the vehicle and the remote driver. The main types of cyberattacks on communication channels are DoS attacks, blocking all communications between the vehicle and the control station. An adversary may modify or drop transmitted video signals, sensor readings, control command sent by RO, and messages coming from road infrastructures or other vehicles.
- **Attacks on vehicle's camera**. In AV teleoperation, cameras are necessary so that the vehicular system and the remote driver can understand the vehicles' surroundings. The blinding and auto control attack disables the functionality of the vehicle's camera sensors. Moreover, malicious hackers may manipulate the camera-captured data. Recently, a group of researchers in Argus Cybersecurity hacked the automotive ethernet-graded camera [28]. They stopped the live-streaming of camera-captured data and injected their pre-recorded video stream by compromising the camera's command and control port.
- **Sensor jamming, spoofing, and blinding/saturation.** There is a possibility that sensors may be blinded or jammed. Using this method, the attacker can corrupt the AI model of the vehicle, feed the algorithm with incorrect information, or intentionally provide scarce information. Therefore, the vehicle gets confused and can not ask for human assistance when required.
- **Information disclosure.** Since the teleoperated vehicle collects sensitive and personal data and shares this data with various stakeholders, an adversary may be motivated to gain access to this confidential data and cause a data breach.

Recommendation for Mitigating the Cybersecurity Risks

Both WP.29 Cybersecurity and cybersecurity management system (CSMS) regulation; and ISO/SAE 21434 Road Vehicles - Cybersecurity Engineering standard aim to secure the vehicle throughout its life cycle. The WP.29 CSMS regulation provides a comprehensive list of threats and corresponding mitigation techniques to help automakers and automotive suppliers understand and assess the risks associated with connected vehicles. Since day by day, the attackers have been developing sophisticated attack techniques, the list of threats mentioned in WP.29 CSMS is not complete. Therefore, rigorous threat analysis, risk assessment, and mitigation techniques for new invented threats are required to ensure public safety. The mitigation approaches include, but are not limited to,

- **Ensuring robust communication between vehicle and remote operator.** The communication between vehicle and teleoperation control center should be strongly protected, using proper encryption and authentication to prevent different types of attacks such as DoS, the Man in the Middle, information spoofing, etc. Moreover, multiple trusted entities like session servers can be introduced between vehicle and teleoperation control centers [29] to ensure secure data transfer. The session server can perform a list of tasks, including registering vehicles and ROs, handling vehicle remote control requests, selecting a suitable teleoperator for each request, and initiating an encrypted peer-to-peer connection between vehicles and ROs.
- **Systematic security validation and testing.** The performance of the AI model is data-dependent. The manufacturer or software developer updates the AI model with new trained data. Hence, systematic security validation and testing are required throughout the vehicle's life cycle to combat newly developed cyber-attacks and security vulnerabilities created by updating the vehicles' AI models [30].
- **Managing risks in the supply chain for an extended period.** Today's cyber-attacks have been more targeted to supply chain communities than direct attacks on OEMs. The supply chain of the connected autonomous vehicle is long and complex, and further extended by adding teleoperation features in vehicles.

The responsibility of securing this automotive ecosystem lies upon stakeholders, including OEMs, all levels of suppliers, subcontractors, and third-party vendors, those who provide software, firmware, and hardware components.

- **Privacy by design to address data privacy.** Since ToD constantly broadcast data and video streaming regarding vehicle speed, location, and surrounding environment, raising potential privacy and data protection concerns. Automotive industries need to adhere to the privacy by design (PbD) approach in V2X communication to proactively ensure the privacy of passengers, vehicle owners, and operators. In Canada, the office of the privacy commissioner of Canada has recommended the "Privacy code of connected vehicle" for data handling practices in the CAV sector. Canadian companies ESCRYP [31] and Blackberry Certicom have incorporated PbD principles in their Security Credential Management System (SCMS) services to secure V2X communication. In Europe, the GDPR incorporates the principles of PbD. In Germany, federal and state data protection authorities have instructed auto manufacturers to observe the principles of PbD in developing new vehicles and services [32]. The US Federal Trade Commission has also recommended data-collecting organizations adopt the PbD framework [33].
- **Require preparedness and incident response capabilities.** Due to the increased connectivity of the vehicle with infrastructures and stakeholders, it is impossible to predict future attacks. Therefore, it is prudent to have a precise and established cybersecurity incident handling and response plan to handle incidents effectively.

Acknowledgements

Colin Dhillon
Chief Technical Officer,
APMA

Peter Watkins
Chief Operating Officer,
QA Consultants

The Automotive Parts Manufacturers' Association (APMA) of Canada CTO and QA Consultants COO would like to thank the V2X cybersecurity committee members for their continuing efforts to provide global representation and leadership on automotive cybersecurity, privacy and safety issues. The work you have all accomplished is having a positive impact on the overall auto ecosystem.

Dr. Ahasanun Nessa
Senior Applied Scientist,
QA Consultants

We would like to acknowledge Dr. Ahasanun Nessa, Senior Applied Scientist at QA Consultants, for leading the development of this white paper.

APMA V2X cybersecurity committee

Peter Watkins -- Chief Operating Officer, QA Consultants and Chair of APMA V2X cybersecurity committee
Colin Dhillon -- Chief Technical Officer, APMA, Canada
Spencer Reuben-- Senior Manager, Emtech at QA Consultants
Ahasanun Nessa --Senior Applied Scientist, QA Consultants
Ken Schultz --General Manager, ESCRYPT (the security division of Bosch) Canada
Dr. Khalil El-Khatib -- Professor and Associate Dean (Networking and IT Security) at Ontario Tech University
John Esvelt -- Chief Risk Officer (CRO) at Dentons, Canada
Dr. Ikjot Saini -- Assistant Professor & Co-Director at SHIELD Automotive Cybersecurity Centre of Excellence at the University of Windsor
Marc Kneppers -- The chief Security Architect at TELUS
Jazz Singh --Jazz Singh--AVP/Sr. Director & Product Leader, Global Identity, Fraud & Compliance Products at Equifax, Canada
Martin Totev -- Vice President of AUTOCRYPT North America Ltd

QA Consultants

QA Consultants is North America's largest independent software quality engineering services firm. Through quality engineering, QA Consultants reduce risk and improves time to market, keeps applications secure with dedicated application security capabilities, and reduces costs while enabling applications to scale. For almost 30 years, QA Consultants has successfully delivered 12,000+ mission-critical projects in the private, public and not-for-profit sectors. The company is proud of its vision to assist clients in achieving flawless technology outcomes.

References:

[1]Ekim Yurtsever et al. , "A survey of autonomous driving: common practices and emerging technologies," *IEEE Access*, 2020

[2] Ira Boudway et al., "Waymo sees human drivers in autonomous cars for the foreseeable future,"January 2020.

[3] Vay Unveils 'TeleDriving' As a New Path to Autonomous Future. [Online]. Available: https://www.businesswire.com/news/home/20210907005952/en/Vay-Unveils-%E2%80%98TeleDriving%E2%80%99-As-a-New-Path-to-Autonomous-Future.

[4] Jean-Michael Georg et al., "Teleoperated Driving, a Key Technology for Automated Driving? Comparison of Actual Test Drives with a Head-Mounted Display and Conventional Monitors," *in Proc. 21st International Conference on Intelligent Transportation System (ITSC)*, 2018.

[5] Hosseini, "Enhancing telepresence during the teleoperation of road vehicles using HMD-based mixed reality," *in Proc. IEEE Intelligent Vehicles Symposium (IV)*, 2016.

[6] "5G technology and networks (speed, use cases, rollout)," [Online]. Available: https://www.thalesgroup.com/en/markets/digital-identity-and-security/mobile/inspired/5G.

[7 Clare Mutzenich et al., "Updating our understanding of situation awareness in relation to remote operators of autonomous vehicles." *Cognitive research: principles and implications journal*, 2021

[8] Transport Canada, "Guidelines for Testing Automated Driving Systems in Canada Version 2.0". Available: https://tc.canada.ca/en/road-transportation/innovative-technologies/connected-automated-vehicles/guidelines-testing-automated-driving-systems-canada

[9] Transport Canada, "Testing highly automated vehicle in Canada", 2018

[10]Germany First to Pass AV Regulations,"Available: https://www.eetasia.com/germany-first-to-pass-av-regulations/.

[11] McKinsey & Company, "What's driving the connected car." [Online]. Available: https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/whats-driving-the-connected-car

[12] Sam Abuelsamid, "Argo AI And Waymo Release Automated Driving Data Sets," 2019. [Online]. Available: https://www.forbes.com/sites/samabuelsamid/2019/06/19/argo-ai-and-waymo-release-automated-driving-data-sets/?sh=63279e8d1d00

[13]Council of Canadian Academies," Choosing Canada's automotive future" Ottawa (ON). The Expert Panel on Connected and Autonomous Vehicles and Shared Mobility, Council of Canadian Academies, March 2021

[14]Canadian Automobile Association, "Special Study on the Regulatory and Technical Issues Related to the Deployment of Connected and Automated Vehicles". Ottawa(ON), 2017

[15]Government of Canada, "Personal Information Protection and Electronic Documents Act." Ottawa (ON), 2000

[16]"A Privacy Code Practice for the Connected Car." [Online]. Available: https://www.priv.gc.ca/en/opc-actions-and-decisions/research/funding-for-privacy-research-and-knowledge-translation/completed-contributions-program-projects/2018-2019/p_201819_09/

[17]Raquel Toral, "Evolving autonomous vehicle technology and the erosion of privacy," University of Miami Business Law Review, 27(1), 2018.

[18] California Consumer Privacy Act (CCPA),[Online]. Available: https://oag.ca.gov/privacy/ccpa

[19]European Commission, "General Data Protection Regulation", Brussels, Belgium: EC 2016

[20] NIL (Commission nationale informatique & libertés (French Data Protection Authority)). 2017. Compliance Package – Connected Vehicles and Personal Data. Paris, France: CNIL.

[21]UN Regulation on uniform provisions concerning the approval of vehicles with regard to cybersecurity and of their cybersecurity management systems, 2020

[22]Mustafa Saed et al., "A Survey of Autonomous Vehicle Technology and Security," i*n Proc. International Conference on Advances in Vehicular Systems, Technologies, and Applications*, Rome, Italy., 2019.

[23]Prateek Kapoor et al.,"Detecting and mitigating spoofing attack against an automotive radar," *in Proc. IEEE Vehicular Technology Conference*, 2018.

[23]Simon Parkinson et al., "Cyber threats facing autonomous and connected vehicles: Future challenges.," *EEE Transactions on Intelligent Transport Systems*, Vols. 18(11), pp. 2898-2915., 2017

[24]Ram Shankar Siva Kumar et al., "Failure Modes in Machine Learning systems," 2019

[25]Chawin Sitawarin et al., " DARTS: Deceiving Autonomous Cars with toxic signs," 2018

[26]Steve Povolny, "Model Hacking ADAS to Pave Safer Roads for Autonomous Vehicles," McAfee Blogs, 2020.

[27] Tao Zhang, "Toward Automated Vehicle Teleoperation: Vision, Opportunities, and Challenges," *IEEE Internet of Things Journal, 2021*

[28]Hacking Automotive Ethernet Cameras," [Online]. Available: https://argus-sec.com/hacking-automotive-ethernet-cameras/.

[29] Stefan Neumeier et al., "A Secure and Privacy-Preserving System Design for Teleoperated Driving," 2021.

[30]European Union Agency for Cybersecurity (ENISA), " Cybersecurity Challenges in the Uptake of Artificial Intelligence in Autonomous Driving," February, 2021

[31] SCMS: Recommended Operation and Governance model report" ETAS Embedded Systems Canada Inc. [Online]. Available: https://tcdocs.ingeniumcanada.org/sites/default/files/2021-07/Security%20Credential%20Management%20System%20%28SCMS%29%20%E2%80%93%20Recommended%20Operating%20and%20Governance%20Model%20report.PDF

[32] Germany: Data protection and security in the automotive sector. [Online]. Available: https://www.dataguidance.com/opinion/germany-data-protection-and-security-automotive

[33]Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change," Washington (DC): FTC. 2012