Connected and automated vehicle cyber security for your organization

CANADIAN CENTRE FOR CYBER SECURITY

OCTOBER 2022 | ITSAP.00.142

While fully automated vehicles may be commonplace in the future, there are many partially automated vehicles and even more connected vehicles on the road today. Drivers have the potential to transform travel by connecting their vehicles to wireless networks and using their devices to produce and provide real-time information. While offering many convenient features, connected vehicles, and in some cases automated vehicles, can pose risks to sensitive information. You should consider the risks associated with these vehicles and understand how to mitigate them.

Levels Of Driving Automation

Level 0
No Automation

The vehicle has no autonomy and the human driver performs all driving tasks.

Level 1
Driver Assistance

The vehicle assists the driver with steering **or** acceleration and deceleration under **specific conditions**. The human driver performs all other driving tasks and monitors the driving environment **at all times**.

Level 2
Partial Automation

The vehicle assists the driver with steering as well as acceleration and deceleration under specific conditions. The human driver performs all other tasks and monitors the driving environment **at all times**.

Level 3
Conditional Automation

The vehicle can perform all aspects of driving under **specific conditions**. The human driver must be **alert and ready** to take control of the vehicle at all times.

Level 4
High Automation

The vehicle can perform all aspects of driving under **specific conditions** and can respond safely without human action to all situations. The human driver has the option to control the vehicle.

Level 5
Full Automation

The vehicle can perform all dynamic driving functions under **all conditions**. The human driver has the option to control the vehicle.

What are connected and automated vehicles?

Connected vehicles use different technologies, such as cellular networks, to assist drivers. This connection enables a wide variety of features, such as navigation guidance, to communicate with the surrounding driving environment. These features can connect to mobile and Internet of Things (IoT) devices to leverage apps and services, as well as to other vehicles. Some examples of connected vehicle capabilities include:

- **Bluetooth and Wi-Fi:** Passengers can listen to music, make phone calls, or send voice texts through system applications or a smartphone connection. Some vehicles allow the downloading of software updates over wi-fi networks.
- **GPS/location services:** Location tracking, roadside assistance, and emergency services contribute to the safety and security of a connected vehicle. While travelling, your location data makes it possible to receive information about directions, accommodations, restaurants, and many other things.

Vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) technologies may be available in the near future and provide drivers even further information about upcoming hazards and road infrastructure.

There are varying levels of automated vehicles, ranging from partially automated, which allows for some driver assistance features, to fully automated, which does not require human intervention to operate. However, connected and automated vehicles (levels 3 to 5) are not currently available for public purchase in Canada. The testing of such vehicles is now underway by researchers and developers to promote their safety.

Automated vehicles use different technologies to assess driving environments and perform specific tasks (e.g. steering, braking, acceleration, and deceleration) such as computers, software, and artificial intelligence (AI). Automated vehicles leverage a variety of sensors to perform their functions:

- **Vehicle system performance sensors** are used for optimizing the performance of an automated vehicle on the road and include steering and braking sensors. Environmental sensors, such as outside temperature and rain sensors, adjust vehicle performance due to weather and environmental conditions.
- **Passenger safety sensors** include occupancy sensor, external cameras, collision impact sensors and internal cameras that track eye and head movements of the driver for alertness.
- **Ranging and positioning sensors** include GPS-based positioning sensors as well as ranging technologies that determine the distance to objects in the environment by measuring the reflections of radio waves (RADAR), laser light (LiDAR) or sound waves (ultrasonic parking sensors).

Automated technologies have many benefits, such as driver assistance systems that may reduce road incidents and anticipate dangerous situations and provide convenient transportation for individuals with limited mobility.

Communications Security Establishment | Centre de la sécurité des télécommunications

Canada

Connected and automated vehicle cyber security for your organization

CANADIAN CENTRE FOR CYBER SECURITY

OCTOBER 2022 | ITSAP.00.142

How can my organization mitigate the risks?

Your personal and organizational information is at risk when using the features of connected or automated vehicles. Vulnerabilities can include devices connected to your vehicle, connections over Wi-Fi and Bluetooth, and applications or software installed on your vehicle or device. These vulnerabilities represent channels that threat actors may use to hack into your device or vehicle.

- **Exploiting software vulnerabilities and Wi-Fi:** Connected and automated vehicles are vulnerable to cyber attacks on embedded software and mobile or Wi-Fi networks. Threat actors target infotainment systems, firmware, or third-party applications and leverage them to perform various attacks. For example, **distributed denial of service (DDoS) attacks** can disrupt a vehicle's communications by overwhelming it with data and effectively shutting down its functions.
- **Spoofing and jamming:** Threat actors can manipulate several types of sensors to create inaccurate data that an automated vehicle will think is real. They can use an electronic device to send signals that create false obstacles (e.g. cars, walls, or pedestrians) or send false signals to the GPS receiver and cause it to direct the driver in the wrong direction or make the vehicle think that the car is somewhere else. Signal jamming interferes with a vehicle's communications and ensures it does not receive anything at all, such as the signals between a keyless fob and a vehicle, to steal it.

Organizations can mitigate the risks to connected and automated vehicles by better protecting device and fleet data. Some mitigation strategies include:

- **Maintain vigilance when operating an automated vehicle:** Drivers must be prepared to override automated systems if they anticipate an unsafe condition developing. All requirements for driver monitoring and attention under the levels of driving automation should be complied with. It might be necessary to report suspicious activity or anomalies to the vehicle manufacturer or relevant authorities.
- **Conduct vulnerability assessments:** Your organization should seek to detect, monitor, and analyze threats to its connected and automated vehicle fleets. Regular audits and a vulnerability management plan help to secure assets against flaws in programming and a changing threat environment.
- **Prioritize security:** Ensure firmware and software upgrades are up to date for your vehicles and connected devices through your vehicle manufacturer. Implement authentication and access control methods to define which employees are permitted to access and use connected or autonomous vehicles. Where possible, encrypt the data collected by vehicles to protect your organization and your clients. Separate your connected or automated vehicles from networks that hold sensitive information or systems network to minimize damage in the event of a cyber attack.
- **Turn off Bluetooth and secure your personal information:** Turning off the Bluetooth visibility on both your vehicle and connected device is an important step to take in ensuring that only trusted devices are connected. You may also want to disable automatic connection features, and have the vehicle prompt the driver or passenger to allow or deny access to contacts or other data on mobile devices before connecting where possible. When selling or trading in your car, take steps to remove your personal information. Cancelling subscriptions, logging out of mobile applications, and removing contacts and navigational information are all ways to prepare for transferring the ownership of your connected or automated vehicle.

Learn more

Visit the Canadian Centre for Cyber Security website (**cyber.gc.ca**) to learn more about cyber security and our services.

You can find our catalogue of publications, including:

- Artificial Intelligence (ITSAP.00.040)
- Using Bluetooth Technology (ITSAP.00.011)
- Internet of Things Security for Small and Medium Organizations (ITSAP.00.012)
- How updates secure your device (ITSAP.10.096)
- Cyber security hygiene best practices for your organization (ITSAP.10.102)
- Protecting your organization against denial of service attacks (ITSAP.80.100)

Communications Security Establishment | Centre de la sécurité des télécommunications

Canada