Analyse the Vulnerabilities, Threats, and Risks of APA System

Mohamad Ibrahim, Department of Science and Engineering, University of Wolverhampton, UK
Nader Safa, Department of Science and Engineering, University of Wolverhampton, UK

Abstract

Advanced Driver Assistance Systems (ADAS) have gained widespread adoption in the automotive industry in recent years, with the Automatic Parking Assist (APA) system being a prominent example. While these systems offer numerous benefits, they introduce novel vulnerabilities, threats, and risks that require attention. Vulnerabilities in the APA system may emerge as a result of its intricate design and employment of various communication protocols, which adversaries could exploit to gain unauthorized system access and undermine vehicle safety. Threats to the APA system may arise from diverse origins, including malicious actors, software defects, and system malfunctions, and may lead to different types of attacks that compromise the system's integrity and availability. The associated risks with the APA system can be considerable, with potential implications for the well-being and confidentiality of the vehicle's occupants and other road users. Therefore, it is crucial to systematically identify, assess, and manage these risks by deploying appropriate controls.

Introduction

Smart vehicles, also known as autonomous vehicles, have been the subject of extensive research and development for many years. As technology advances, researchers and engineers are working to create vehicles that can handle complex real-world conditions and make quick decisions. A major challenge in the development of smart vehicles is the need for a variety of sensors, systems, and other technologies that enable them to sense their environment. In addition, algorithms and other software that allow smart vehicles to navigate and interact with their environment are also necessary. Many companies and research institutions have made significant progress in this field. Tesla and other companies have also made significant advancements in autonomous vehicle technology. However, several challenges still need to be addressed before smart vehicles can be widely used, including the need for reliable sensing and decision-making systems and addressing concerns about security and safety, including the risk of cyber-attacks targeting sensors, algorithms, systems, networks, and other assets.

There are various domains within smart vehicles, such as the Telematics Domain, Chassis Domain, Infotainment Domain, Powertrain Domain, Body Domain, and Sensor Domain, among others. Each of these domains includes multiple systems that make the vehicle intelligent and functional. There are over 47 systems in smart vehicles, including cruise control, automatic braking, park assist, autopilot, adaptive front lighting, active vibration control, and navigation systems, among others. These systems are vulnerable to various security risks and attacks, which can compromise the privacy and security of personal data as outlined in the General Data Protection Regulation (GDPR). This regulation emphasizes the importance of protecting personal data by processing it. This includes process to avoid unauthorized processing, as well as unintentional loss, deletion, or loss of personal data.

This research will focus on the APA system, also known as the parking assistance system. The APA system is an intelligent system that helps drivers park their vehicles quickly and safely. It consists of various components such as ultrasonic sensors,

cameras, control system, Global Positioning System (GPS), radar, and other technologies that guide the driver in detecting parking spaces. However, there are some challenges related to risks, threats, vulnerabilities, and the mitigation process associated with this system.

Smart vehicles

Key elements of smart vehicles.

According to Rathore et al. [6], there are three key elements in smart vehicles, as shown in Figure 1. These elements are automotive control systems, Vehicle-to-everything (V2X) communication, and autonomous driving systems. Each of these elements contains several systems and components**.**

Automotive Driving Systems

The main unit is the Electronic Control Unit (ECU) which controls the state of the automatic transmission and the sensors inside the vehicles. An in-vehicle network links the ECUs and allows them to exchange data. This network consists of various types of communication technologies, including Control Are Network (CAN), Local Interconnect Network (LIN), digital bus, FlexRay, and radio frequency (as listed in Table 1). The CAN protocol is a data communication standard developed by ISO and is designated as ISO 11,898 [3]. It is commonly used as the primary network for communication among various systems within a vehicle [3].

Table 1: Vehicle Interconnection

Network	CAN	LIN	Domestics digital bus	FlexRay
Rate	1Mb/s	19Mb/s	11Mb/s	20Mb/s
Topology	Linear, Star and Ring	Linear	Ring	Linear, Star and Ring

Autonomous driving systems

The system is composed of various components, including a LIDAR sensor, camera, ultrasonic sensor, radar, and GPS. The LIDAR sensor uses a laser wavelength to detect objects and calculate distances. The camera is used to read road signs, monitor obstacles, and track pedestrians. GPS uses satellite signals to determine the vehicle's location. Radar measures the distance, angle, and velocity of targets to understand the vehicle's environment [6].

V2X communication systems

V2X technology is used to facilitate network communication between a vehicle and external terminals. Smart vehicles utilize several types of communication, such as Dedicated Short-Range Communications (DSRC), Infotainment, traffic safety and Cellular V2X. DSRC, based on the IEEE 802.11p wireless standard, is used for short-range communication, while Cellular V2X is used for long-range communication [1].

<INSERT FIG.1>

Figure 1: Key elements of smart vehicles

APA System

Some vehicles are equipped with an APA system, which helps the driver park the vehicle by automatically controlling the steering, acceleration, and braking. This system utilizes sensors, such as ultrasonic sensors or cameras, to detect the location and movement of objects around the vehicle. When the driver activates the automatic parking assist feature and shifts the car into reverse, the system takes over and guides the vehicle into a parking spot. Some systems can even parallel park the vehicle automatically [5]. The purpose of automatic parking

assist systems is to make parking easier and more convenient, particularly in tight spaces. The functionality of the automatic systems is illustrated in Figure 2.
The GPS locates empty spaces to park based on the vehicle's location, the ultrasonic sensor detects obstacles, the camera measures the parking space's dimensions precisely and keeps track of the vehicle's surroundings., and the radar detects other vehicles and measures the distance and angle. Based on the information received from all these components, the automatic parking assist controller makes decisions and begins to control and brake the vehicle in order to park safely and accurately [5].
<INSERT FIG.2>
Figure 2: APA operation

APA Body Diagram

Kuang, Zhang and Wang [5] indicate that the automatic parking system is comprised of five control systems: the ultrasonic system, the image processing system, the vehicle speed control system, the power steering control system, and the vehicle control system. All work together to facilitate the automatic parking process in a smart vehicle. These systems communicate with each other through the CAN communication protocol, and the vehicle control system coordinates their cooperation to control the actuators of the vehicle and park it safely and efficiently.
<INSERT FIG.3>
Figure 3: APA System Diagram
Each control system in a smart vehicle includes several components that assist with the vehicle's functionality. For example, the GPS determines the vehicle's location and searches for a parking space, while the long and low-range ultrasonic sensor gathers information about obstacles. At the same time, the radar system measures the distance, angle, and velocity of the vehicle and helps to detect other vehicles, pedestrians, and obstacles, also assists the vehicle to navigate and avoid collisions. This information is then sent to the APA system for analysis and to initiate actions to control the vehicle. During the parking process, the In Vehicle Head Unit (IHU) checks for human interaction, and the EPS and ESC systems provide movement information. The Transmission Control Unit (TCU) provides information about the vehicle's gear, and the Inertial Measurement Unit (IMU) provides information about the body posture of the vehicle.

APA Assets

Asset Identification

Smart vehicles have various assets that are used to enable them to function effectively. These assets can include both physical components, such as sensors and cameras and software applications, such as operating systems. These assets allow the vehicle to gather data about its environment, a process that data to make decisions about how to navigate and interact with the environment and communicate with other vehicles and infrastructure. They may also be used to power the vehicle, provide safety features, and enable drivers and passengers to interact with the vehicle. In summary, these assets are essential for enabling the vehicle to perform tasks such as autonomous driving, navigation, and communication. The APA system, which is part of the smart vehicle system, uses a range of components, including sensors, cameras, radar, GPS, control systems, and connectivity systems, to function.
<INSERT FIG.4>
Figure 4: APA Assets

Asset Classification

Assets in the APA system refer to the resources, systems, and data that are critical to the operation and success of the system. These assets can include hardware, such as

sensors and control systems, software, networks, data, and people. There are various ways to classify assets in the APA system, depending on the needs and priorities of the system. Some common methods of classification include:

1. Criticality: This can include assets that are essential for the operation of the system, such as sensors, control systems, and other hardware and software components.
2. Sensitivity: This can include assets that contain highly sensitive data, such as images captured by cameras or vehicle location data, as well as assets that provide access to sensitive systems, such as the control system.
3. Vulnerability: This can include assets that are more vulnerable to attack, such as systems that are connected to the internet or have weak passwords, as well as assets that are less vulnerable, such as air-gapped systems or systems with strong security controls in place.

However, according to ISO 21434, an international standard for cybersecurity in road vehicles, assets should be classified based on their importance to the operation and safety of the vehicle, as well as the impact that their loss or compromise would have on the vehicle and its occupants. This standard guides how to prioritize and protect assets in smart vehicles to minimize the risk of cyber threats.
According to Figure 5, the assets in the APA system will be classified based on the ISO 21434 standard. Assets classified as high level have a high impact on the safety and operation of vehicle such as the control system, while assets classified as medium level have a lesser impact on the safety and function of vehicle such as data storage. Assets classified as low-level have the least impact on the safety and operation of vehicle such as GPS.
<INSERT FIG.5>
Figure 5: APA Assets Classification level

Vulnerabilities and Threats

Vulnerabilities

It is important to recognize that all systems in smart vehicles have vulnerabilities. APA, like any vehicle system, are vulnerable to cyber-attacks and other types of threats that could disrupt its operation or compromise sensitive data as in figure 6. Some potential vulnerabilities are mentioned in table 2.
<INSERT FIG6>
Figure 6: APA Vulnerabilities cause
Table 2: APA Vulnerabilities cause

Vulnerabilities Causes	Vulnerabilities Details	Asset Affected
Damage or loss of Assets	• Leakage of sensitive data • Unencrypted data	• Communication System • Data storage System • Sensor system. • Software System
Software Failure and Malfunctions	• Software bugs • Design Flaws • Hardware failure • Human Error • Firmware update	• All assets
Accidental damage	• Errors in storing data • Untrained person • Poor data protection	• All assets

	• Design Flaws	
Network outage	• Cyber attack • Unsecured networks • Interference • Interception • Physical access	• Communication System • Sensor • CAN • ECU
Entry Points	• Insider threats • Protocol flaws • Interference • Firmware update	• All assets
Nefarious and abuse activity	• Unauthorized access • Remote activity • Interference • Manipulation in hardware and software • Unauthorized installation software	• All assets
Eavesdropping/ Interception/Hijacking	• Interfering radiation • Unsecured signals	• Data storage • Sensor • Control System • Communication System

Threats and potential attacks

Smart vehicles, also known as connected or autonomous vehicles, are vulnerable to a variety of threats that can compromise their safety, security, and privacy. These threats can come from a variety of sources, including hackers, malicious software, and physical attacks. As mentioned, the APA system is a type of smart vehicle technology, and therefore it is also susceptible to various attacks that may be specifically targeted at it or that it may be exposed to due to vulnerabilities in other smart vehicle systems. As in figure 7, these threats to the APA system can be classified into six categories: control system, communication, autonomous system components, infotainment system, data storage system and physical. Each category contains several specific threats that may differ from one another.

<INSERT FIG.7>

Figure 7: Threats Classification on APA system

Risks, Mitigations and Challenges

Risk Analysis Process

ISO 21434 is a standard that provides guidelines for the security of road vehicles and their systems, including the risk assessment process. The standard covers a wide range of threats and vulnerabilities, including cyber threats, physical threats, and supply chain threats [2] .

The risk analysis process is outlined in ISO 21434 [4] as in figure 8.

<INSERT FIG.8>

Figure 8: Risk Analysis Process

ISO 21434 is intended to be used in conjunction with other relevant standards and guidelines, such as ISO/IEC 27001 and NIST SP 800-53.

Risk Assessment

Threats to smart vehicles should be ranked according to their risk level, which is determined by the likelihood or the probability of the threat appearing and the impact it would have on the system. The likelihood of a threat occurring is based on whether

there is sufficient knowledge available for attackers to carry out the attack. The impact of a threat refers to the severity of the consequences if the threat were to occur. The risk level is determined by multiplying the numerical values for likelihood and impact. This allows organizations to prioritize their efforts in addressing the most significant threats and vulnerabilities. Table 3 is used to determine the risk level of different threats to a smart vehicle based on the motivation of the attacker and the impact of the threats.

Table 3: Risk Assessment

<table>
<tr><th>Motivation</th><th>Difficulty</th><th>Likelihood</th><th colspan="3">Impact</th></tr>
<tr><td rowspan="2">High</td><td>None</td><td rowspan="3">Likely</td><td>High</td><td>Medium</td><td>Low</td></tr>
<tr><td>Solvable</td><td colspan="2" rowspan="2">Critical</td><td rowspan="4">Minor</td></tr>
<tr><td rowspan="2">Moderate</td><td>None</td></tr>
<tr><td>Solvable</td><td>Possible</td><td>Major</td></tr>
<tr><td>Low</td><td>Any</td><td rowspan="2">Unlikely</td><td colspan="2">Minor</td></tr>
<tr><td>Any</td><td>Strong</td></tr>
</table>

Table 4 shows the assessment risk of the threats based on the threats classification in figure 8.

The Risk assessment of the threats.

Table 2: The Risk assessment of the threats

Threats	Motivation	Difficulty	Likelihood	Impact	Risk
DDOS attack	High	Solvable	Possible	High	Critical
Malicious CAN message	High	Solvable	Unlikely	High	Major
Bus-off attacks	Moderate	Strong	Unlikely	Medium	Major
Masquerading attacks	Moderate	Solvable	Possible	High	Major
Injection attacks	Moderate	Strong	Unlikely	Medium	Major
Eavesdropping attacks	High	Solvable	Possible	Medium	Major
Replay attacks	Moderate	Solvable	Unlikely	Medium	Major
Movement Tracking	High	Solvable	Unlikely	Low	Minor
Spoofing Attack	High	Solvable	Possible	Medium	Major
Brute Force	Moderate	Strong	Possible	High	Major
Jamming Attack	Moderate	Strong	Possible	Medium	Major
Interference Attack	Moderate	Solvable	Likely	Medium	Minor
Blind Spot Exploitation	High	Solvable	Possible	High	Critical
Cloaking Attack	Moderate	Any	Unlikely	Medium	Major
Cache Attack	Moderate	Solvable	Possible	High	Major
Tampering	Moderate	Strong	Unlikely	Medium	Major
Movement Tracking	High	Solvable	Unlikely	Low	Minor
Acoustic Cancellation	Moderate	Any	Possible	Medium	Major
Man in the Middle	Moderate	Solvable	Possible	Medium	Major
Acoustic Cancellation	Moderate	Any	Possible	Medium	Major
Auto-control attacks	Moderate	Any	Likely	Medium	Critical
Remote code execution	High	Solvable	Possible	High	Major

Risk management and mitigation

After identifying the risks of an APA system through a risk analysis process, the next step is to implement risk treatment strategies. The "4 Ts" of risk management, which includes treatment, transfer, terminate, and tolerate, can be used to manage these risks. Treatment involves implementing controls to mitigate or eliminate the identified risk. Transfer involves transferring the risk to another party, such as through insurance or other risk-sharing arrangements. Terminate involves by removing or retiring the activity or asset that is causing the risk. Tolerate involves accepting the risk and taking no further action to mitigate or eliminate it. For critical and major risks, the treatment

strategy involves implementing controls to mitigate the risk. For minor risks, the terminate or tolerate strategies may be used based on the impact of the risk.
Moreover, applying some security standards to ensure that the APA system is protected against threats and vulnerabilities. These standards are ISO/SAE 21434, ISO 27001, ISO 26262, ISO 15408 and SAE J3061.
According to Kuang, Zhang and Wang [5], some mitigation approaches are used as shown in table 5. For example, Kuang, Zhang and Wang [5] have used intrusion detection to protect CAN against some attacks.

Threats Mitigation Approach

Table 3: System Mitigation Approach

Threats	Risk	Mitigation Approach
DDOS attack	Critical	Intrusion Detection and Artificial intelligence
Malicious CAN message	Major	Software-based firewall and Message integrity checks
Bus-off attacks	Major	Intrusion Detection
Masquerading attacks	Major	Message Authentication and Network Segmentation
Injection attacks	Major	Web Application Firewall
Eavesdropping attacks	Major	Secure communication protocols
Replay attacks	Major	Encryption
Movement Tracking	Minor	Data minimization
Spoofing Attack	Major	Secure communication protocol and Encryption
Brute Force	Major	Two-factor authentication
Jamming Attack	Major	Frequency hopping
Interference Attack	Minor	Frequency hopping and directional antennas
Blind Spot Exploitation	Critical	Implement a warning system and multiple sensors
Cloaking Attack	Major	Intrusion Detection and Artificial intelligence
Cache Attack	Major	Encryption
Tampering	Major	Encryption and regularly software updating
Movement Tracking	Minor	Data minimization
Acoustic Cancellation	Major	Use of soundproofing materials and Active noise cancellation
Man in the Middle	Major	Encrypted communication protocols and digital certificates
Acoustic Cancellation	Major	Use of soundproofing materials and Active noise cancellation
Auto-control attacks	Critical	Secure communication protocols and Access controls
Remote code execution	Major	Secure coding standards

Challenges

Smart vehicles are vulnerable to a variety of threats that could have significant impacts on their operation and safety. These threats may include physical attacks that manipulate the vehicle or its components, as well as cyber-attacks that exploit vulnerabilities in the vehicle's systems or communication channels. Some of these attacks may have a high risk of causing damage to the vehicle or other assets, leading to potential accidents or other safety issues. In addition to these risks, there are also privacy concerns, as attackers may be able to acquire access to private information stored in a smart vehicle by exploiting vulnerabilities in APA systems or other components. Data leaks can occur due to a variety of factors, including abuse of authorized access, security vulnerabilities, social engineering, and software flaws. To mitigate these risks, it is important to follow best practices for security and privacy in the design, development, and data of smart vehicles [7].
It is important for companies operating smart vehicles to be mindful of GDPR requirements and ensure that they are complying with these requirements when

collecting and processing personal data. Failing to do so can result in significant fines and other penalties. In addition to GDPR, other standards should be applied ISO/IEC 27001, ISO/IEC 29100, NIST Cybersecurity Framework and ISO 21434.
Therefore, Safa et al. [7] classified the privacy protection approaches into two main categories as in table 6.
Table 6: Privacy protection approaches

Data-oriented approaches	**Process-oriented approaches**
Data Minimization	Privacy by Design
Data Anonymization	Privacy Requirement Engineering
Differential Privacy	Testing and Verification
Encryption	Transparency
Secret Sharing	Consent and Control
Pseudonymous Digital Credentials	Auditing and Accountability
Private Information Retrieval	Privacy Architectures
Zero-Knowledge Proofs	

Conclusion and Future Work

In conclusion, APA systems in smart vehicles are vulnerable to a range of threats and vulnerabilities that can result in various risks. These threats and vulnerabilities include injection attacks, eavesdropping, replay attacks, tampering, spoofing, man-in-the-middle attacks, brute force attacks, jamming, and blind spot exploitation, among others. These threats and vulnerabilities can result in risks such as damage to the vehicle or other assets, potential accidents or other safety issues, and privacy violations. To mitigate these risks, APA systems need to be designed and developed with security in mind, and appropriate controls to be put in place to identify and mitigate potential threats and vulnerabilities. This may include the implementation of security standards such as ISO/SAE 21434, ISO 27001, ISO 26262, and ISO 15408, as well as the application of risk management strategies such as the "4 Ts" (treatment, transfer, terminate, and tolerate). Moreover, apply mitigation standards such as blockchain, Hashing, Intrusion Detection, and others.
For future work, it is important to regularly assess and evaluate the risks associated with the APA system to identify and address any vulnerabilities or potential threats therefore attack three can be applied.

About the author

Mohamad Ibrahim, Department of Science and Engineering, University of Wolverhampton, UK
Nader Safa, Department of Science and Engineering, University of Wolverhampton, UK

Resources

Algarni, A. and Thayananthan, V. (2022). Autonomous Vehicles: The Cybersecurity Vulnerabilities and Countermeasures for Big Data Communication. Symmetry, [online] 14(12), p.2494. doi:10.3390/sym14122494.

International Organization for Standardization [ISO] (2018) BS ISO 31000:2018 - TC Tracked Changes. Risk management, ISO [Online]. Available at https://bsol-bsigroup-com.ezproxy.wlv.ac.uk/PdfViewer/Viewer?pid=000000000030409468 [Accessed 21 December 2021].

International Organization for Standardization [ISO] (2018) ISO 26262-1:2018 - TC Tracked Changes. Road vehicles. Functional safety, ISO [Online]. Available at https://bsol-bsigroup-com.ezproxy.wlv.ac.uk/PdfViewer/Viewer?pid=000000000030413403 [Accessed 25 December 2021].

International Organization for Standardization [ISO] (2018) BS ISO/IEC 15408-3:2022 - Tracked Changes. Information security, cybersecurity and privacy protection. Evaluation criteria for IT security, ISO [Online]. Available at https://bsol-bsigroup-com.ezproxy.wlv.ac.uk/PdfViewer/Viewer?pid=000000000030462821 [Accessed 15 December 2021].

Kong, H.-K., Hong, M.K. and Kim, T.-S. (2017). Security risk assessment framework for smart car using the attack tree analysis. Journal of Ambient Intelligence and Humanized Computing, [online] 9(3), pp.531–551. doi:10.1007/s12652-016-0442-8.

Laurendeau, C. and Barbeau, M. (2006). Threats to Security in DSRC/WAVE. In: Ad-Hoc, Mobile, and Wireless Networks. [online] pp.266–279. doi:10.1007/11814764_22.

NIST (2020). Security and Privacy Controls for Information Systems and Organizations. Security and Privacy Controlsfor Information Systems and Organizations, [online] 5(5). doi:10.6028/nist.sp.800-53r5.

References

1. Amrita Ghosal and Conti, M. (2020). Security Issues and Challenges in V2X: A Survey. [online] ResearchGate. Available at: https://www.researchgate.net/publication/338405291_Security_Issues_and_Challenges_in_V2X_A_Survey [Accessed 27 Dec. 2022].
2. D.B.Naga Muruga (2018). The Smart Vehicle Concept. [online] ResearchGate. Available at: https://www.researchgate.net/publication/336119769_The_Smart_Vehicle_Concept [Accessed 26 Dec. 2022].
3. International Organization for Standardization [ISO] (2018) ISO/IEC 27001:2017 Information technology. Security techniques. Information security management systems, ISO [Online]. Available at https://bsol-bsigroup com.ezproxy.wlv.ac.uk/PdfViewer/Viewer?pid=000000000030347472 [Accessed 23 December 2022].
4. International Organization for Standardization [ISO] (2021) ISO/SAE 21434:2021 Road vehicles. Cybersecurity engineering, ISO [Online]. Available at https://bsol-bsigroup com.ezproxy.wlv.ac.uk/PdfViewer/Viewer ?pid=000000000030350149 [Accessed 23 December 2021].
5. Kuang, X., Zhang, Y. and Wang, X. (2022). System Design of Automatic Parking Assist Based on ISO26262. Journal of Physics: Conference Series, [online] 2195(1), p.012032. doi:10.1088/1742-6596/2195/1/012032.
6. Rathore, R.S., Hewage, C., Kaiwartya, O. and Lloret, J. (2022). In-Vehicle Communication Cyber Security: Challenges and Solutions. Sensors, 22(17), p.6679. doi:10.3390/s22176679.
7. Safa, N.S., Mitchell, F., Maple, C., Azad, M.A. and Dabbagh, M. (2020). Privacy Enhancing Technologies (PETs) for connected vehicles in smart

cities. Transactions on Emerging Telecommunications Technologies, [online] 33(10). doi:https://doi.org/10.1002/ett.4173.