CYBERSECURITY

QA Consultants

AUTOMOTIVE CYBERSECURITY

Toni Jardini,
Director, Emerging Technology, QA Consultants

With over 15 years of QA Software and test automation experience, Toni is a senior test automation architect and technical program leader for QAC's EmTech solutions. With a Masters degree in Computer Science, Toni leads a PhD engineer research team. This team is dedicated to developing QA innovations and new technologies such as automotive and robotic domains that involve artificial intelligence, machine learning, and non-deterministic testing.

qaconsultants.com

Why automotive cybersecurity is important

Connected Autonomous Vehicles (CAVs) share a high volume of data and specific information by accessing a digital infrastructure that includes public internet access. With different devices, vehicles can connect and share data from on-board sensors and road infrastructure. This sharing of data, inclusive of personal data, ends up making vehicles more vulnerable to cyber attacks.

Negative implications include property and vehicle damage, poor brand reputation, and a deficit in market value for OEMs. Automotive cybersecurity is crucial as it protects those involved from impending cyber attacks. Just as connected autonomous vehicles have evolved, so has the threat of cyber attacks.

EXECUTIVE SUMMARY

Ensuring the safety and security of self-driving or Connected Autonomous Vehicles (CAVs) is essential because a vehicle malfunction can lead to injury, occupant death, or harm to others outside of the vehicle. Manufacturers must establish vehicles that are both safe and secure.

To ensure that a given system is protected against unauthorized and malicious actions, proper strategies, practices, and techniques need to be in place to mitigate security risks associated with cyber-attacks. Having a proper defense mechanism available to address security vulnerabilities that defines best practices will ensure safe and secure CAVs.

QA Consultants, in collaboration with Ontario Tech University, has conducted extensive research on state-of-the-art CAV cybersecurity and consolidated automotive security vulnerabilities challenges.

As a result of this research, QA Consultants has invested in developing an advanced automated cybersecurity test framework to detect and find solutions to existing cybersecurity vulnerabilities in CAVs.

QA Consultants

CYBERSECURITY

WHAT IS CYBERSECURITY

Cybersecurity can be defined as a mechanism of which block access to information in the digital environment against unauthorized people, with or without malicious intent.

The Information Systems Audit and Control Association (ISACA) defines cybersecurity as an area that seeks to guarantee the right to security and privacy for users in the digital environment including maintaining full and correct functioning networks, devices, and information that can be accessed and shared by interconnected computer systems.

AUTOMOTIVE CYBERSECURITY

According to David Morris et al., the definition of the term "cybersecurity" does not change when it comes to automotive systems. Cybersecurity for CAVs is related to the protection of its electronic systems, communication networks, algorithms, software, hardware, and data.

There are several types of cyber attacks frequently performed to automotive vehicles, which can be classified according to their types and entry points.

> *"Automotive cybersecurity guards against malicious attacks, unauthorized access, and any unwanted manipulation."*
>
> **David Morris et. all**

We consider entry points across six levels from 0 to 5 as follows:

Level 0

This level involves interactions between sensors and drivers. Some example potential entry points are communication interfaces, debug interfaces, memory chips, etc. Also, the physical equipment making up the car itself such as the car doors, windows, trunk, and so on are within the scope of level 0.

Level 1

This level looks at controls such as drive control, process control, safety controls, etc. Some examples of potential entry points include door control, light control, climate control, Anti-lock Braking System (ABS), and Emergency Brake Assist (EBA). There are several types of cyber attacks which can be classified according to their types and entry points.

Level 2

This level looks at interfaces between components such as the infotainment system and its subcomponents. Additionally, the infotainment system could use a third-party application such as Apple CarPlay and Android Auto, which provides direct access to the CAN bus. Since the CAN bus allows microcontrollers and devices to communicate with each other, it is vulnerable to attacks.

Level 3

This level assesses applications on both mobile and infotainment system interfaces. Some potential entry points are peripherals and connected devices such as rear seat entertainment.

Level 4

This level focuses on technologies that leverage communication channels such as those found in wireless entry points. At risk entry points include onboard WiFi within the car, GPS, LiDAR, RADAR, and other network communication.

Level 5

In this level, attacks and entry points fall under the cloak and dagger methodology. For example, mismatched permission issues to access certain features on Android, iOS and other devices.

TYPES OF CYBER ATTACKS

Common types of cyber attacks can be categorized into physical, sensor, software, and network attack.

PHYSICAL ATTACKS

These include leveraging physical devices to attack the vehicle. Some examples are listed as follow:

Hardware Modification

Hardware hacking and modification happens when the physical infrastructure of a computer is attacked. Hardware hacking may also be the result of replacing, removing, or replicating components of hardware systems within a car.

Node Replication

Node replication means duplicating the physical hardware itself. This occurs when an attacker harms the functionality of a network or communication device by injecting a clone, or replica, into the environment. This type of attack may be done via a network where a car is considered a node.

Physical Damage

Physical damage deals with both the destruction of vehicle components and the vehicle itself. This potential attack can cause physical damage to a vehicle, damaging headlights, locks, and related components that may be responsible for the power windows in a vehicle.

Side Channels

Side channels are based on information gained from the implementation of a computer system to directly access the vehicle in service. A vehicle may be sold to a third party (such as registered dealer), so data may be wiped or left on components of the car, which could serve as potential information disclosure vulnerabilities, privacy, and sensitive user data.

TYPES OF CYBER ATTACKS

Common types of cyber attacks can be categorized into physical, sensor, software, and network attack.

SENSOR ATTACKS

The definition of “sensor” is not limited to sensor components such as oil, or oxygen sensors, but any components of connected vehicles which intake data. Some examples sensor attacks are listed as follow:

CAN bus

The controller area network (CAN bus) allows microcontrollers and devices to communicate with each other within the vehicle. Attacks on these devices may include signal injection, physical disruption to the device, spoofing, etc.

LIDAR

Light detection and ranging (LiDAR) sensors emit light pulses and measure the time light takes to return after bouncing off surfaces. Typical uses for LiDAR in a vehicle include collision avoidance, adaptive cruise control, and object recognition. Typical attacks on these systems look at fooling the LiDAR data algorithms by providing misinformation, spoofing, and a denial-of-service (DoS). The DoS is a type of cyber attack which tries to interrupt the device's normal functionality.

Radar

Typically, radar attacks fall under sensor jamming, denial of service, spoofing, and interference. Attacks under these categories may create similar situations to attacks that are found within LiDAR.

USBs

Potential inputs that could increase the area of attack include USBs, SDs, external drives, mobile device chargers.

CDs

CDs are traditionally used for playing music, but it is possible to embed code in music files that when a CD is played, the corrupt codes are transmitted to the CAN bus which allows the cyber attacker to access the vehicle and execute commands on ECUs.

TYPES OF CYBER ATTACKS

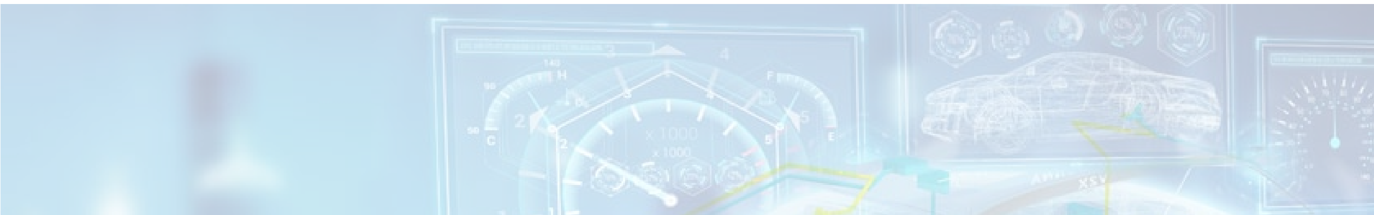
Common types of cyber attacks can be categorized into physical, sensor, software, and network attack.

SOFTWARE ATTACKS

Software attacks are programs written deliberately to damage or use the system in an unauthorized way. Some examples of such attacks are:

Infotainment Systems

Infotainments typically run operating systems such as those seen with Android, Integrity real-time operating system (RTOS), Linux, QNX, and Windows Embedded Automotive. Potential areas of attacks are ransomware, crypto mining, keylogging, and rootkits, etc.



Firmware

Firmware is a software that provides low-level control for a device's specific hardware. These types of attacks include the vulnerabilities that exist in the firmware itself. Attacks may be a result of updates which include hiding malicious software. Attacks can be done over the air or within the system itself by connecting to an external device.

Integrated & Third-Party Applications

Software attacks do not necessarily affect the vehicle itself but rather provide additional access to areas unlocked typically through the infotainment system. Attacks are usually done through rogue (using computer malware to trick users), malicious, and compromised applications.

TYPES OF CYBER ATTACKS

Common types of cyber attacks can be categorized into physical, sensor, software, and network attack.

NETWORK ATTACKS

Network attacks could be implemented through Wireless (Bluetooth, WiFi and Remote Keyless Entry) or In-Vehicle Network (FlexRay, CAN, LIN and Ethernet) communications.

Controller Area Network (CAN)

CAN is often targeted by malicious agents. One of the most common attacks include replacing an authorized ECU program with an unauthorized and malicious program and connecting to the CAN bus using an unauthorized device. A malicious invasion may cause a DoS attack and create messages with ID 0, which are of the highest priority, then in turn causes the CAN bus to become unusable.

Local Interconnect Network (LIN)

LIN is used to facilitate the intercommunication of the ECU, used to control lights, engines, air conditioning, steering wheels, seats, and doors. After CAN, LIN is the network most subject to exploitation by malicious agents. Among the threats to LIN, the most frequent and common are Message Spoofing (criminals send messages with inaccurate information, so that vehicle communications are stopped), Response Collision (take advantage of the error-handling mechanism of the LIN), and Header Collision attacks (an attacker sends a fake header to collide with a legitimate header).

FlexRay

FlexRay is an automotive network protocol used to help govern on-board systems. This network is exposed to standard attacks such as spoofing, where an attacker can create and inject requests. Additionally, FlexRay runs the risk of possible DoS attacks.

Ethernet

Ethernet has a variety of attack vectors, from unused ports, MAC spoofing, and bandwidth abuse, to the more sophisticated, such as TCP hijacking, etc.

TYPES OF CYBER ATTACKS

Common types of cyber attacks can be categorized into physical, sensor, software, and network attack.

NETWORK ATTACKS (CONT.)

Network attacks could be implemented through Wireless (Bluetooth, WiFi and Remote Keyless Entry) or In-Vehicle Network (FlexRay, CAN, LIN, and Ethernet) communications.

Bluetooth

Bluetooth networks provide a capability for cyber attackers to intercept data and images passed between both car and mobile phone. Bluetooth network attack examples include BlueBorne and Carwhisperer. BlueBorne is an attack vector by which hackers can leverage Bluetooth connections to penetrate and take complete control over targeted devices. Carwhisperer is a hacking technique that can be used by attackers to hack a handsfree Bluetooth in-car system and connect it to a Linux system.

WiFi

Compared to Bluetooth, WiFi is a more stable and secure protocol when considering vehicle connectivity. However, it comes with its own areas of attack vulnerabilities. For example, such attacks include "Man-in-the-middle attack" (or Attack hijack) and "Wi-Fi spoofing". In the Man-in-the-middle attack, attacker intercepts communications between two parties. WiFi spoofing is deployed via an open network or public free WiFi networks where the user who joined the WiFi network will be asked to login to a spoofed page.

Remote Keyless Entry

Remote Keyless Entry has two communication types. In passive keyless entry and start (PKES), the communication relies on bidirectional challenge-response schemes which provide the potential for replay attacks. In remote keyless entry (RKE), the communication relies on unidirectional data transmission from the remote control embedded within the key. Both communication types create potential for side-channel attacks.

THE AUTOMOTIVE CYBER ATTACKS IMPLICATIONS

Attacks within CAVs have a broad range, stemming from direct and physical attacks to the car, which may impact both the driver and the data.

"Loss of data, privacy, asset, service, trust and even life."

When evaluating attack surfaces and entry points each attack level increases in complexity. Below are seven areas of implications.

Loss of Data

may occur when an attacker gains entry via a successful attack on the vehicle physically or remotely. Data implication loss may affect the reputation of the protocol, OEM, and the underlying technology.

Loss of Privacy

may occur when an attacker gains entry via a successful attack on the vehicle physically or remotely. Data implication loss may affect the reputation of the protocol, OEM, and the underlying technology.

Loss of Asset

may take place at the physical level, where a break occurs, or in a virtual level such as loss in information and currency (sensor does not properly send currency to a remote device).

Loss of Service

may include loss of access to a vehicle. It can also mean loss of service to core functionalities of that vehicle including malfunctioning blinker or brake.

Loss of Trust

In cases where interactions with a third-party system occur, both the third party and the end-user may lose trust in the respective party due to a potential attack.

Loss of Life

In almost all attacks, there is potential that upon entry, an attacker could directly affect the life of one or many Individuals. Typically, these attacks require interaction with levels 0 and 1.

HOW TO PROTECT AGAINST CYBER ATTACKS?

Cybersecurity defense mechanisms in CAVs pertain to preventing an exploitative situation. The defense mechanisms can be grouped by the phase in which they are used as authentication and encryption, malware and intrusion detection, and software vulnerability analysis.

Authentication and Encryption

Authentication and encryption are both critical components for any communication channels to be secured. Authentication mechanisms involve identity verification. A common example is entering a username and password when you log in to an application. Encryption mechanisms provide a means to securely communicate over a channel and assist in preventing unauthorized access.

A simple example of an encryption algorithm would be changing all Ns to a 3, or all Zs to a 1. In doing that, the data will look meaningless. While there is no perfect solution, some potential authentication and encryption solutions are listed below.

CAVs impose their unique requirements and limitations that restrict the ability to implement the existing authentication and encryption mechanisms used in other industries

Utilizing a decentralized method to provide a lightweight authentication mechanism for vehicles.

Utilizing a symmetric key encryption mechanism which use the ad-hoc networks and group keys to securely exchange keys at regular intervals.

A Peer-to-Peer Anonymous Authentication (PPAA) is another solution that is available to protect from spoofing. This method leverages asymmetric encryption to represent all client and server connections.

HOW TO PROTECT AGAINST CYBER ATTACKS?

Malware and Intrusion Detection

Although authentication and encryption systems deter attacks, they cannot be the only defense mechanism to securely protect any system.

Detection of attacks is another critical layer of defense to protect vehicular networks from attacks.

Detection of attacks can be categorized into two categories; intrusion detection, which focuses on the network aspect, and malware detection, which is associated with executable code and file systems.

Some potential detection methods include:

- Utilizing **intrusion detection system** that utilizes signature-based detection
- Utilizing **machine learning algorithms** to help classify the traffic and attacks
- **Scanning file systems** for new executable code that may be malicious

Software Vulnerability Analysis

Software vulnerability analysis is a technique that attempts to identify vulnerabilities in the code prior to its use. It is usually divided into three groups of static, dynamic, and combination analysis.

In static analysis, the code does not need to be executed to perform verification checks. It can leverage various techniques to detect vulnerabilities, including lexical and data flow analysis.

Whereas in dynamic analysis, the code is required to be executed to determine errors. Fuzzing (fuzz testing) is a common technique used for dynamic analysis where invalid, unexpected, or random data are used as inputs to a computer program. Combination analysis involves both static and dynamic analysis.

INDUSTRIAL CYBERSECURITY SOLUTIONS

Extensive research has been conducted into cybersecurity issues with CAVs and several companies have developed their solutions for certain aspects of the problem. The current offerings by different organizations in the industry can be grouped in three different categories:

Cybersecurity Solutions for CAVs

Many companies already offer and develop cybersecurity solutions for connected and autonomous vehicles. These solutions can address a specific aspect of security or provide an overall framework for a vehicle to abide. One example is a specific solution for secure digital mobile keys. This solution enables vehicle owners to replace traditional car keys and fobs with a secure digital key on their mobile. A successful case study using this solution has been demonstrated with the car manufacturer Hyundai. Securely executing code in vehicles has also been proven as a successful option.

Cybersecurity Testing Services for CAVs

Aside from the development of cybersecurity solutions, many vendors have begun to offer cybersecurity testing services for CAVs. As with any technology, when developing a solution, it is important to consider the security of the system early on. As such, many of these companies offer their expert knowledge to identify vulnerabilities on the design, code, execution environment, and more. These organizations have dedicated teams that are well-versed in CAV concepts, security best practices, and leverage this skill to provide consultation services. One such example is a solution created through adedicated practice for Connected Vehicle Cybersecurity services where inputs on design, specification, and implementation flaws utilizing dynamic analysis, static analysis, unit testing, and other techniques are provided.

Environment Simulation for CAVs

One method to test a developed solution or service is to run it through a simulated environment. A few companies have begun to offer environment simulation tools for the development of V2X solutions. Some companies offer their own unique environment simulation tool sets. Those solutions are designed to test individual or multiple Electronic Control Units (ECUs) against a simulated environment and usually consists of many components such as an emulation software for other vehicles and v2x devices, a radio frequency transmitter for producing the communications to the ECU, and GPS signal transmitters to list a few.

INDUSTRIAL CYBERSECURITY SOLUTIONS

Quality is rarely captured by a single idea and its complex nature can make it difficult to describe. In popular culture, phrases like `I'll know it when I see' can be used to define quality. In a professional context like autonomous vehicle manufacturing and development, it is important to consider a more precise definition of quality.

In CAV, a comprehensive and robust cybersecurity approach is necessary to ensure high software quality. Cybersecurity can ensure that software quality requirements related to security, safety and privacy are achieved. Further overlap between cybersecurity and software quality occurs in the methods and techniques employed including testing. As newer capabilities and features of connected vehicles are explored, a proper testing framework is necessary to facilitate for rigorous security review of them before they are released or accepted as solutions. CAV space is complex and has many possible attack vectors, and as such the environment designed for testing must be able to accommodate for these diverse situations. There are various methods to gain access and infiltrate a connected vehicle. There may be inherent vulnerabilities present in the code of a certain solution within the connected vehicles, its interactions with other components, or against the environment. Each of these would need to be addressed and tested for a comprehensive security review. The concept of Secure Software or Systems Development Life Cycle, provides a solid foundation for security testing in connected vehicles. There are many variations of such a lifecycle, including waterfall, iterative, and agile to name a few. When introducing security to the variations however, the concept is to consider security along all phases of the cycle rather than one. This methodology provides the kind of resilience against various attack vectors mentioned earlier. By capturing different vulnerabilities at different phases of the software or systems development this method provides resilience against the various attack vectors previously mentioned.

Biggest cybersecurity challenges in the current and next-generation automobiles

Software Security Testing

This testing should be executed whenever a solution introduces new software or code that will be integrated into the vehicle. Each code segment in a solution is susceptible to a variety of software vulnerabilities.

Simulated Solution Testing

The concept involves leveraging an autonomous vehicle simulator, such as Carla, to integrate the software of a solution into a connected vehicle. This module is primarily relevant when developing a solution that introduces new functionality to a vehicle. In this case a simulated environment offers the ability observe the functionality and impact of the solution with a virtual vehicle. This module proposes leveraging this simulated environment to also test for security vulnerabilities that can be identified within the scope of the simulation.

CHALLENGES AND OPEN ISSUES

"Cybersecurity is one of the most challenging issues for CAVs because they are vulnerable to diverse types of cyber attacks."

The CAN protocol is a widely used standard developed by BOSCH. The CAN differs from many other network technologies in that it is both cost efficiency and flexibility. However, the CAN does not handle encryption and authentication well and has repeatedly been vulnerable to cyber attacks. CAN vulnerability will grow as vehicle autonomy and connectivity increases..

Since vehicles hold large amounts of personal data, which may be accessed via vehicle networks or through devices connected to cars, automotive cybersecurity becomes a challenge in itself. Also, CAVs systems find it very difficult to deal with real-time tracking and analysis of security mechanisms to prevent attacks.

Connected autonomous vehicles have become much more than just a means of transportation. In addition to transportation, they also have entertainment systems,communication, virtual shopping options, and even function as mobile offices. These vehicles cannot merely be seen as valuable physical property, but as an interconnected technology node that communicates with various other objects, shares and processes data on all sides, and arouses the interest of cyber criminals. The more complex technology becomes, with various levels of vehicle communication, the more likely the levels will become a target. The human element cannot be underestimated when it comes to successful cyber attacks. Unknowingly, the average person is vulnerable and enables would be cyber attackers due to their lack of knowledge. When it comes to CAVs, live agent tests can be expensive and dangerous. Using precision simulations that can identify attacks and threats from intruders is attractive but has proved to be a significant challenge due to the costs and complexities involved.

Biggest cybersecurity challenges in the current and next-generation automobiles

Mobility Services

There is a new attack vector for every new service added to the vehicle. In the near future, remote attacks will increase substantially because of ransomware and unauthorized access in mobility services provided by back-end servers, telematics servers, and mobile applications.

Sensor Attacks

Attacks on LIDAR, sensors, and other radar functionality are continuously growing

Smart Mobility

The attack on the network or back-end due to smart mobility is on the rise which can cause a service-wide disruption

Keyless Entry

Keyless entry is becoming a common trend in modern vehicles. Keyless entry cars are vulnerable to many attacks such as relay attacks, jamming attacks, and others. These attacks will cause an increase in theft of valuable property and compromise the safety of the vehicles.

Data Sharing

Vehicle exchange will cause data privacy issues. Car sharing is becoming common in the automotive domain. There, cloud based/in-vehicle services could store personal information and become a vulnerable point of attack. Attacks on LiDAR, sensors, and other radar functionality are continuously growing.

Third-party Apps

The integration of third-party apps is common in vehicles which makes it difficult to guarantee security because of the absence of security by design.

FINAL CONSIDERATIONS

In order to have a secure and safe CAV system, it is required to identify threats and security flaws in the systems. The first and most important step is to detect all entry points and types of attack frequently performed on automotive vehicles. This involves understanding the implications of those cyber attacks and the defense mechanisms to protect the system against cyber attacks. QA Consultants team is committed to mitigating cybersecurity risk in CAVs through expanding its proprietary cybersecurity framework in collaboration with Ontario Tech University and QA Consultants role in leading the cybersecurity initiative for the XIVT Project, for automotive, rail, telecom and industry 4.0 domains being developed by 5 countries, Canada, Sweden, Germany, Turkey and Portugal, in a multi-year international program.

REFERENCES

- Morris, David, Garikayi Madzudzo,and Alexeis Garcia-Perez. "Cybersecurity and the auto industry: the growing challenges presented by connected cars." International journal of automotive technology and management 18.2 (2018): 105-118.
- Majumder, Subhrajit, Akshay Mathur, and Ahmad Y. Javaid. "A Study on Recent Applications of Blockchain Technology in Vehicular Adhoc Network (VANET)." National Cyber Summit. Springer, Cham, 2019.
-Sun, Joey, et al. "A classification of attacks to In-Vehicle Components (IVCs)." Vehicular Communications (2020):100253.
- Jahan, Farha, et al. "Security Modeling of Autonomous Systems: A Survey." ACM Computing Surveys (CSUR) 52.5 (2019): 1-34.
- Automotive cybersecurity solutions for connected car technology. web page: https://www.trustonic.com/industries/automotive/ (last accessed: Jun. 4, 2020).
- Automotive cyber security testing: Connected vehicle: Nettitude.web page:https://www.nettitude.com/us/penetration-testing/connected-vehicle-testing/(last accessed: July 9, 2020).
- Connected vehicles / V2X. web page: https://www.spirent.com/products/connected-vehicles-v2x (last accessed: July 9, 2020).
- V2X test tools. web page: https://www.danlawinc.com/v2xtesttools/ (last accessed: Jun. 4, 2020).
- Dibaei, Mahdi, et al. "An overview of attacks and defences on intelligent connected vehicles." arXiv preprint arXiv:1907.07455 (2019).
- Hayward, Jake, Andrew Tomlinson, and Jeremy Bryans. "Adding Cyberattacks To An Industry-Leading CAN Simulator." 2019 IEEE 19th International Conference on Software Quality, Reliability and Security Companion (QRS-C). IEEE, 2019.
- Morris, David, Garikayi Madzudzo, and Alexeis Garcia-Perez. "Cybersecurity and the auto industry: the growing challenges presented by connected cars." International journal of automotive technology and management 18.2 (2018): 105-118.
- Linkov, Václav, et al. "Human factors in the cybersecurity of autonomous vehicles: trends in current research." Frontiers in psychology 10 (2019): 995.
- Clark, George W., Todd R. Andel, and Michael V. Doran. "Simulation-Based Reduction of Operational and Cybersecurity Risks in Autonomous Vehicles." 2019 IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA). IEEE, 2019.
- Cybersecurity report. web page: https://www.upstream.auto/.
- XIVT Project. web page: https://www.xivt.org/ (last accessed: August 12, 2020).
- Hossam A. Gabbar, Abul Hasan Fahad, and Ahmed M. Othman. Design oftest platform of connected-autonomous vehicles and transportation electrication. In Proc. of the 4th International Conference on Intelligent Computing Communication & Devices (ICCD 2018), pages 1035{1046. SpringerSingapore, 2018.