A Survey on Threat Analysis and Risk Assessment of Connected Autonomous Vehicles

Abstract- The attack surface of automobiles is rising due to current development trends in the automotive industry toward more connected and autonomous driving, which raises the possibility of security attacks. People could have a better driving experience due to the rapid evolution of interconnected automobiles. On the other hand, communicating to the outside network may increase the number of accidents caused by cybersecurity vulnerabilities. As a result, manufacturers are focusing more on cybersecurity and investing more resources to develop cybersecurity protection measures. Threat analysis and risk assessment (TARA) is a cost-effective way to assure the defensive system impact and save money initially in the vehicle development process. It assesses the threat posed by vehicle systems and determines the hierarchical defenses and mitigations necessary to counteract the threat. The goal of this review is to provide an overview of threat analysis and risk assessment in the automobile industry. Existing approaches have been compared and examined. Some frequently used tools were employed to TARA and their performance when compared. Finally, future TARA development directions in the automotive industry and a few open security issues are discussed.

1. INTRODUCTION

The automobile industry is witnessing a major revolution toward connected and autonomous driving. As a result, the number of sensor nodes, actuators, control units, and communication systems installed in vehicles has increased. Wireless interfaces, such as wireless local area network (WLAN) or Bluetooth, which are used to transfer information between the surroundings and the vehicle, have now become extensively used, transforming vehicles from closed to open systems. As a result, vehicle communication became more sophisticated, increasing the attack surface for cybersecurity threats in which attackers may now get access to the complete vehicle and manipulate its operations from the outside.

The automobile system has become way more complicated in recent years as vehicles have become more intelligent and interconnected. Increasing the number of connections to the external network of cars and software-based operations might increase the possibility of vehicles being hijacked by hackers, criminals, and even terrorists. The intelligent and connected automobile is vulnerable to a variety of cyberattacks that might compromise privacy, safety, and even national security. Automotive manufacturers focus strongly on improving their products' cybersecurity defense. There have been several security solutions offered to provide automobile cybersecurity defense[1].

The current security solutions are mostly passive and provide a single layer of protection for a specific security threat, therefore the cybersecurity problem will not be fixed instantly[2]. TARA techniques can assist in detecting possible threats in the early stages of development and give support for theoretical integrity of selecting mitigation measures by identifying and evaluating potential cybersecurity threats and risks. However, in the automotive area, there is a lack of a study of TARA methodologies and tools, as well as how to employ appropriate mitigation strategies that minimize the vulnerabilities in principle[3].

The purpose of this study is to perform a systematic evaluation of current research in the automotive area that focuses on TARA. The current study explores existing TARA techniques in the automotive field and extracts the features of the suggested methods.

TARA's most common tools are also explained. In addition, the mapping link between vulnerabilities and associated mitigation methods is investigated in this study.

The remaining of the paper is arranged as follows: The technique for conducting a systematic literature review is described in Section 2. (SLR). An overview of the various attacks that are possible in autonomous vehicles is discussed in section 3. Threat analysis and risk assessment methodologies are discussed in Section 4. Threat analysis and risk assessment tools are analyzed and compared in Section 5. Before summarizing our study with a conclusion in Section 7, we explore the future directions of threat analysis and risk assessment advances in Section 6.

1. LITERATURE REVIEW

2.1. Research Question Definition. The primary goal of this article is to provide an overview of recent research on numerous cyberattacks that autonomous vehicles could be vulnerable to, as well as the most up-to-date TARA approaches in the automotive industry. The following questions were therefore formulated, and this stage represents the core of the article...

RQ1. What are the various attacks that are possible in connected autonomous vehicles?

RQ2. What threat analysis and risk assessment procedures are performed to examine the vehicle's cybersecurity status??

RQ3.What tools could be used to analyze threats and determine risks??

RQ1 identifies the numerous types of threats that might occur in connected autonomous cars. RQ2 will look into how threat analysis and risk assessment are done in the automobile industry. RQ3's goal is to figure out what tools may be used to analyze threats and estimate risks.

2.2. Search Process. The preceding is a step-by-step procedure for doing this literature review's comprehensive search...

2.2.1. Database Selection.

Digital libraries selected for this survey include the following:
(i)IEEE Xplore Digital Library (https://ieeexplore.ieee. org/)
(ii) Springer (https://link.springer.com/) (
iii) Leddy Library(https://leddy.uwindsor.ca/)

2.2.2. Search Terms. The search phrase used to identify relevant papers in selected databases was given in the study's subsequent steps. To search the necessary databases, we specify the following Boolean string.: (risk OR vulnerability in autonomous vehicles OR security threats) AND (risk analysis OR cyber risk assessment OR evaluate threats) AND (security) AND (connected autonomous vehicle OR automotive industry).

2.3. Selection Criteria. The purpose of this paper's research is to determine whether or not screening-related research activity should be defined to eliminate ambiguity in the screening process. As a result, the following criteria for inclusion were considered:
(i) Papers must focus on automotive security challenges
(ii) Papers must be peer-reviewed, and the following criteria must be met for a paper to be excluded:
(i) Papers are not written in English;
(ii) Papers are not available in full text; and
(iii) Papers are duplicates of previous research.

3. OVERVIEW OF SECURITY ATTACKS IN CONNECTED AND AUTONOMOUS VEHICLES

Existing cyber-attacks are classified as in-vehicle network attacks, vehicle-to-everything network (V2X) attacks, and additional attacks in the context of CAVs[4]. For the execution of these cyber-attacks, we first determine the vehicle's attack surfaces. The total of distinct attack points on a system's attack surface is the number of ways an adversary might try to inject or extract data from the system to compromise the vehicle's security. Remote sensor intrusions, for example, can be carried out via a hacked radar, which is called an attack surface[5].

3.1 In-Vehicle Network Attacks

Remote sensor attacks, GPS spoofing attacks, location trailing attacks, proximity vulnerabilities, controller area network (CAN) and society of automotive engineers buses vulnerabilities, software flashing attacks on electronic control units (ECUs)[6], and integrated business services attacks are all examples of in-vehicle network attacks.

3.1.2 Remote Sensor Attacks

One of the main issues in the environment of CAVs is that numerous electrical components, such as ultrasonic radar, lidar, camera, and other sensors, are connected via an in-vehicle network. In terms of range, detecting capabilities, and reliability, each type of sensor has its own set of advantages and disadvantages. Furthermore, existing wireless access technologies can be used by other organizations to connect to sensors[7].

3.1.2 GPS Spoofing Attacks

Global Positioning System, which provides geolocation and trilateration, is frequently used by CAVs. Many important operations rely on it, including pseudonym certificates, fundamental safety messages, and message timestamps. For CAVs, accuracy and truthfulness are essential. The attacker manipulates the received GPS signal arbitrarily in the attacked region in GPS spoofing assaults[8]. It gives recipients false information. Furthermore, the opponent broadcasts a fraudulent GPS signal with a higher signal strength than the real GPS signal.

3.1.3 Location Trailing Attacks

The attacker can collect private information from drivers by finding and following their automobiles in location tracing attacks[9]. The enemy can use location information to uncover car habits and activities, as well as collect the driver's profile and connect it to personal privacy in the real world.

3.1.4 Close Proximity Vulnerabilities

Short-range communication systems reveal risks close. These flaws might have occurred by chance. Bluetooth, tire pressure monitoring systems (TPMS), and keyless entry and ignition systems can all be used to carry out these tasks[10].

Bluetooth:

A possible memory attack has been identified in the Bluetooth control code, allowing code from any linked Bluetooth device to be executed. The engine control units of a vehicle may be attacked by a hacked device that has been linked with it. The driver, on the other hand, is completely unaware of the attack. Furthermore, cryptography algorithms have built numerous safe Bluetooth protocols.

Tire Pressure Monitoring System (TPMS):

Standard modulation schemes and simple protocols are typically used in TPMS communications. TPMS communications can be reverse-engineered since they don't rely on cryptographic techniques. Furthermore, TPMS malfunctions may be caused by spoofing and battery depletion assaults.

Key Fob and Keyless Entry:

There are two methods for entering the vehicle: key fob entry and keyless automobile entry. When the driver tries to lock his car with a variety of devices, such as garage door openers and house light controllers/dimmers, the opponent may block the signals from the key fob. The signals of the key fob will be jammed in entire regions of car parks or streets once these devices are buried in bushes and operated for lengthy periods.

3.2 Vehicle to Everything Network Attacks

A vehicle-to-everything network allows data to be exchanged between a connected car, other vehicles, and CAV infrastructure. This form of communication is used by the adversary to disclose network access points. WiFi, Bluetooth, and the worldwide system for mobile communication protocols are used to create communication channels between a vehicle and external devices, such as smartphones. Once the cars are linked via communication channels, they become subject to network assaults, which are discussed below.

3.2.1 DoS Attacks

DoS attacks occur when an attacker uses interference signals to block the whole communication channel. On the network nodes, the attacker inserts useless messages or causes problems. As a result, legitimate users are unable to access network services. Correct communications are unable to reach their intended recipients. DoS attacks can cause a delay in the receiver's response and interfere with it. In the context of CAVs, a slight delay might compromise the vehicle's driving safety.An accident can be caused or avoided in a fraction of a second.

Impersonation Attacks:
Every vehicle has a unique identification number that may be used to identify it and the communications it sends. Impersonation assaults are carried out by assuming a different or fictitious identity. Node impersonation attacks and Sybil attacks are the two types of impersonation attacks. Furthermore, the Sybil opponent is capable of transmitting bogus communications, propagating changed received messages, and dropping vital messages, among other things.

Replay Attacks:
The adversary records and retransmits early legitimate packets at a later period in replay attacks [39]. It frequently happens at the network or transport layer. It has the potential to confound authorities, mislead the whole traffic, and even jeopardize transportation safety.

Routing Attacks:
Routing attacks make use of routing protocols' flaws and vulnerabilities. The attacker might disrupt the usual routing process or discard passing packets in these attacks. Blackhole attacks, grey hole attacks, and wormhole assaults are examples of routing attacks. A single hacked node or a group of collaborating nodes can launch a black hole assault. The attacker selectively drops packets during grey hole assaults. Furthermore, it can transition from proper actions to behaviors that are carried out as if by a black hole. Grey hole assaults are difficult to identify due to their occasional correct behavior. There are at least two cooperate nodes in wormhole assaults, which can establish a private high-speed tunnel.

Attacks on Data Falsification:
One of the most important requirements of vehicular communication for ensuring road safety and preventing accidents is honesty. The adversary can provide or broadcast fake information and safety alarms in data falsification attacks. The bogus message might be created through message tampering, suppression, fabrication, or change.

Eavesdropping Assaults:
Eavesdropping attacks are carried out by listening in on wireless communications. Stealth attacks are another name for these types of assaults. In these assaults, the adversary secretly analyses network traffic as well as the present positions and activities of the specific target. The enemy can then collect CAVs' private information.

Password and Key Assaults:
Password and key attacks are extremely difficult to carry out. They frequently necessitate the use of specialized gear and software. For financial reasons, these assaults are conceivable to carry out. The technique is tested with different parameters until it can be hacked in a password and key assaults. Finally, the key or password may be broken. Dictionary attacks, rainbow table assaults, and brute force attacks are the three types of attacks that can be used. The adversary utilizes a list of words to repeatedly crack the password in dictionary assaults. Dictionary assaults are identical to the other two types of attacks.

3.3 Other Attacks

Infrastructure assaults, minor attacks, and attacks on machine learning systems are among the other types of attacks.

Infrastructure Attacks:
CAVs will almost certainly necessitate the creation of new transportation infrastructure. Furthermore, car makers must deal with the associated infrastructure and autonomous vehicle interoperability difficulties. Existing entities in the infrastructure of CAVs include roadside units, onboard units, cloud servers, intelligent traffic lights and signals, traffic cameras, and traffic control centers, among others.

Slight Attacks:
The conveyed data has arbitrarily deviated from the actual ones in these attacks. Furthermore, variances do not surpass the limit. A security method will be engaged if the difference between predicted and measured behaviors reaches a predefined level. The

planned security mechanism may be rendered worthless in this situation.

Machine Learning System Attacks:
Machine learning systems can be utilized for several security-sensitive activities in the context of CAVs, such as security monitoring and vulnerability identification. Machine learning systems, on the other hand, have limitations and can be exploited throughout the data gathering, training, and prediction stages.

In data poisoning attacks, the attacker might alter the original training data or substitute harmful data, affecting the machine learning algorithm's judgment. The adversary can change the training algorithm and leak the user's private information via attacks on the learning algorithm and its libraries without compromising the accuracy and generalization of the machine learning model.

4. THREAT DETECTION AND RISK ASSESSMENT METHODOLOGIES

TARA is mostly in the early stages of development for intelligent and connected automobiles. The risk value of prospective threats may be decreased to an acceptable level at a cheap cost by threat modeling and risk assessment of the intelligent and connected vehicle cyber-physical system.

TARA is broken down into three sections:
(i) Threat analysis: able to spot some possible threats threats in the automobile industry
(ii) Risk assessment: the ability to analyze and categorize risks. Threats are detected, and the accompanying risks are assessed.
(iii) Risk analysis: categorizing threats by risk level and assessing whether the risk associated with a certain danger is acceptable or whether mitigation actions are required

TARA approaches are separated into two types in this section: formula-based methods and model-based methods. Formula-based approaches are those that use tables, texts, or formulae to analyze and assess a system's hazard and risk. Asset-based techniques, vulnerability-based methods, and attacker-based methods are the three categories of formula-based approaches based on their respective concerns.

Model-based approaches are a sort of threat analysis method that employs a range of models, such as data flow diagrams, graphs, and tree models, to model and analyze the system's hazards and risks. According to their varied concerns, model-based approaches are separated into two types: graph-based methods and tree-based methods.

According to their varied concerns, model-based approaches are separated into two types: graph-based methods and tree-based methods. Model-based approaches use multiple models to do threat assessments on the system, making them more objective. The precision and reliability of quantitative analysis outputs are improved.

3.1. Model-Based Methods

3.1.1 Graph-Based Methods.

Graph-based methods use nodes and directional edges to link them. Graph-based approaches may represent each node module's direct mathematical quantitative link, making quantitative threat analysis of the system easier.

STRIDE:
Spoofing (S), tampering (T), repudiation (R), information disclosure (I), denial of service (D), and elevation of privilege (E) are all part of the STRIDE concept (E). The STRIDE approach is extensively utilized in the IT sector, and it is useful in identifying and analyzing dangers in the system, lowering the chance of the system being attacked. The STRIDE approach is progressively being implemented in different sectors due to its remarkable result.

3.1.2 PASTA method

In addition to the STRIDE approach, PASTA (Process for Attack Simulation and Threat Analysis) was established as a seven-stage threat analysis method. Data flow diagrams are used by PASTA at the application decomposition layer. The (i.eLinkability, identifiability, nonrepudiation, detectability, data disclosure, unawareness, and noncompliance) technique uses a six-step analysis to offer data security and privacy protection for the system. It analyzes and detects various dangers using data flow diagram iterative model parts. The VAST approach (visual, agile, and simple threat) may be expanded and used to analyze large-scale threat models.

3.1.3 Markov chain

The Markov chain technique has the benefit of including the time dimension in the threat analysis of the system. This technique assumes that the present state of the system determines the system's upcoming state, resulting in a dynamic threat analysis of the system. It expands the dimension of the overall threat analysis as a dynamic approach by defining the assault processes and simulating the related defense measures.

3.1.4 Graph Transformation System

The GTS technique (graph transformation system) is a formal way of altering the system structure graph according to particular principles. The full graph transformation system may be represented as a tuple (G, R), with G denoting the graph and R denoting a set of transformation rules. The GTS approach includes three transformation rules that are used to represent service activity, regular hardware component behavior, and attack activities. GTS can simply and rapidly convert between the overall design and the module architecture with the use of transformation rules, which is highly useful for OEMs in the creation of large-scale projects.

3.1.5 STPA-Sec

When using STPA-Sec for security and safety analysis, Schmittner et al. presented enhancements and found many limitations of STPA-Sec. STPA-Sec generates a list of system-level situations that potentially result in losses. The STPA-Sec method's threat analysis process can be broken down into four steps: the first is to establish basic system engineering; the second is to build a high-level control structure model; the third is to identify unsafe or risky control actions, and the fourth is to develop security requirements and constraint causal scenarios.

3.1.6 Tree-Based Methods

The attack tree model, which can express the assault encountered by the system and indicate the attack path, is an example of a tree-based technique that can represent the affinity between nodes and define the hierarchical relationship between nodes.

The top event is used to describe the attack target, and the nodes below the attack target represent all possible events that can cause the attack target to occur. The logical relationship between these events can be connected through "OR" and "AND" gates.

Attack tree analysis may be done top-down, which means identifying the final attack target first and then assessing all alternative attack pathways based on that target. It may also be done from the bottom up, first assessing the potential attack surface and then analyzing the potential vulnerabilities based on this method.

How to create a fair and impartial assessment of various TARA approaches is another issue that researchers are worried about. Distinct assessment methods have different scenarios and settings under which they might be used. It is vital to provide a platform for the assessment process so that various TARA approaches may be fairly assessed.

3.2 Formula-Based Methods

3.2.1. Asset-Based Methods.

The most common type of TARA method in the automotive domain is the asset-based approach. This series of methods first identifies the final target asset under attack and then exhausts the attack paths and attack methods that can pose a threat to this target asset using relevant experience and the minds of security experts so that advance prevention can be carried out. Figure 1. Explains the workflow of the TARA method in asset-based methods.

Asset-based techniques concentrate on different types of assets in the system. Because a vehicle is fundamentally a cyber-physical system, the ultimate objective of automotive cybersecurity is to safeguard the system against the attack and allow it to function properly. As a result, asset-based threat analysis and risk assessment techniques are ideal for the automobile industry.

3.2.2 Octave method

The OCTAVE approach has become one of the most widely used TARA methods worldwide. The

OCTAVE methodology separates the assessment into three parts, each of which examines and discusses management and technological concerns so that the organization's personnel can fully own the organization's information security needs.

The OCTAVE technique is defined as a method of assessment that considers assets, threats, and vulnerabilities. It enables managers to decide on the OCTAVE approach, which is defined by a combination of asset, threat, and vulnerability evaluations, based on the assessment findings.

Managers can also utilize the assessment results to prioritize risks that need to be addressed.

3.2.3 Evita Method

The EVITA approach is an asset-based threat analysis technique that provides a cost-effective security architecture that may provide complete security across various development phases for vehicle networks, such as design, verification, and prototype. The EVITA technique examines the amount of risk posed by an attack on each asset in the system before determining the severity of the assault. The possibility of an assault and the degree of the damage produced by the attack determine the risk. Threats are risk-rated and threat priority is decided based on these factors.

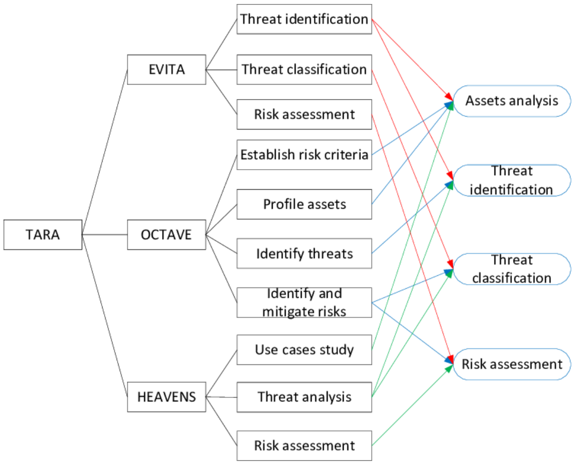


Figure 1. Work flow of Asset based methods in TARA

3.2.4 HEAVENS Method

During threat analysis, a mix of security goals and level of effect helps analyze the possible business impact of a threat on key stakeholders.

As a result, HEAVENS is an excellent tool for assessing the information security threats posed by automobile electronic and electrical systems. Simultaneously, the HEAVENS technique provides a complete threat analysis and risk assessment procedure, which considerably decreases the method's complexity of use and boosts its practicality, which is also a necessity for its widespread application. Figure 2 explains the workflow of HEAVENS method

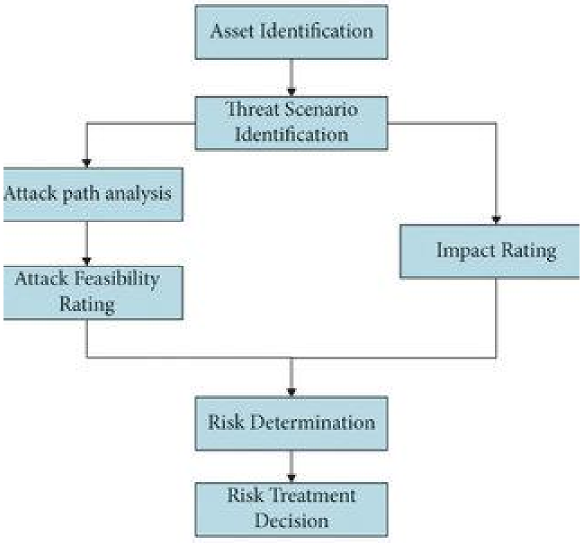


Figure2. Workflow of HEAVENS method

3.2.5 Binary Risk Analysis

In just a few minutes, the BRA approach may be utilized for rapid risk talks to explore specific issues. Despite this, the hazards are only categorized as high, medium, or low. Furthermore, a conservative analytical trend leads to only high-risk threats being classified as threats. Furthermore, no organized danger scenario assessment is provided, and the threat classification that results is too primitive for idea development phases. Figure 3. Portrays the workflow of Binary Risk Analysis Mapping

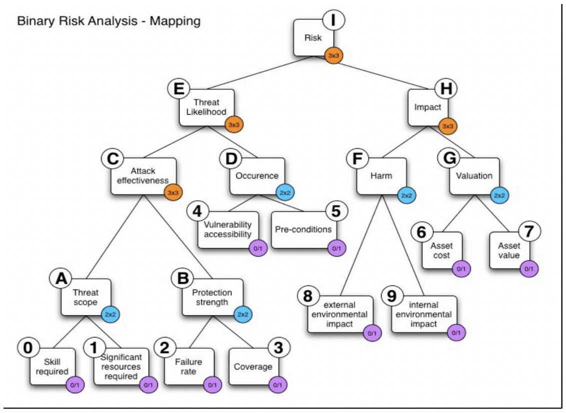
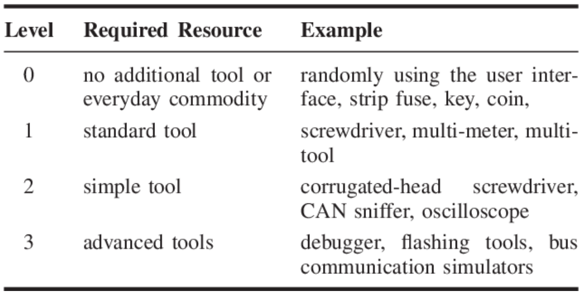


Figure 3. Binary Risk Analysis Mapping

3.2.6 SAHARA Method

SAHARA allows for the estimation of the likelihood of security concerns occurring and their effects on safety objectives. Because the fundamental categorization corresponds to the ASIL classification, it is ideal for use in integrated security and safety engineering procedures. A software vulnerability analysis approach determines if known software code should be avoided to avoid possible vulnerabilities.



Level	Required Resource	Example
0	no additional tool or everyday commodity	randomly using the user interface, strip fuse, key, coin,
1	standard tool	screwdriver, multi-meter, multi-tool
2	simple tool	corrugated-head screwdriver, CAN sniffer, oscilloscope
3	advanced tools	debugger, flashing tools, bus communication simulators

Figure 4. SAHARA method

3.3 Vulnerability Methods

The vulnerability-based techniques are "bottom-up" TARA approaches, similar to the asset-based methods. They start with a vulnerability or weakness discovered in a system and then examine what additional bigger vulnerabilities or failures the vulnerability may create.

Vulnerability-based methodologies can identify system vulnerabilities and examine the dangers and risks that the vulnerability may pose to the system. When these technologies are paired with a large vulnerability database, a more thorough vulnerability scan of the system may be performed. This technique allows for the analysis of each vulnerability that might cause system failure damage using a database of vulnerabilities with a large number of vulnerabilities. It can successfully prevent the vulnerability from compromising the system's security.

3.3.1 Common Vulnerability Scoring System

The CVSS (Common Vulnerability Scoring System) is an open industry standard for determining the urgency and relevance of response. The major goal of CVSS is to help develop a standard for quantifying the severity of vulnerabilities so that they can be compared and the priority of addressing them can be decided. CVSS scores are determined by the outcomes of measurements on a set of dimensions known as metrics.

3.3.2 CHASSIS Method

The CHASSIS procedure as a whole

To identify functionality, safety, and security requirements, the analytical approach is separated into two parts. ‚e initial step

primarily outlines the functional requirements that will be followed by the addition of safety and security criteria. The introduction of the second stage is the major focus. The standards for safety and security This phase will be dependent on the bringing together relevant security experts in the field to brainstorm as a crucial consideration to suggest some probable misuse situations

The outcomes of the entire analysis will be based on this. As a result, there are several

In the approach of analysis, there are too many subjective aspects.

3.3.3 Analytical Network Process

For joint evaluation, the ANP (Analytical Network Process) matrix technique may simply and efficiently address the dependencies and conflicts between qualities. It aids in the development of sound design judgments, reducing the number of design iterations. The hierarchical fault and threat propagation structures are described in the matrix, and the interaction between them is taken into account, resulting in a network structure.

3.3.4 VeRA Method

VeRA (Vehicles Risk Analysis) employs a streamlined analysis procedure and fewer components, resulting in a significant reduction in analysis time without compromising accuracy. Furthermore, using VeRA, a simple and effective mathematical model is developed to evaluate risk value by taking into account attack likelihood, severity, and human control, reducing the time-consuming procedure of looking up tables used in earlier systems.

5. THREAT ANALYSIS AND RISK ASSESSMENT TOOLS

5.1 MTMT:

The Microsoft Threat Modeling Tool 2016 (MTMT) is a threat modeling and analysis tool based on the STRIDE approach that can assist users in identifying possible risks early in the system design process. To explain the communication between different components of the system, the user needs first to create a data flow diagram (DFD). MTMT identifies and analyses the DFD automatically. Finally, it will offer a list of the system's probable dangers.

MTMT may also generate reports that users can see at any time to record the findings of threat modeling and analysis. Although MTMT can correctly and fully represent the system's possible threats, it cannot relate the threats to the asset losses produced by the assault, nor can it give a complete system perspective for threat analysis and risk management.

5.2 GROOVE:

GROOVE is a tool that transforms a generic graph using simply labeled graphs and single push-out (SPO) transformation rules. GROOVE may apply transformation rules to a graph in a recursive manner. GROOVE can simulate the vehicle's network architecture. It may construct the matching state space, which is the attack graph, based on the model's initial state and the preset conversion process. If a state in the attack graph has weaknesses, that state might be considered the root of the attack tree. The equivalent attack tree may be determined by checking the other state in the attack tree.

5.3 Practical Threat Analysis:

PTA (Practical Threat Analysis) is a tool that may be used in a variety of situations. used to model threats and calculate risk automatically, the outcome of the evaluation must first define some factors, including system assets, threats, exploited vulnerabilities, mitigation methods, attack kinds, and so on. In a PTA project, attack entrance points. The danger model Information is maintained in a dynamic database to allow for dynamic changes in model parameters. By continuing to do so. It is possible to ensure that the model's parameters are revised. The process of risk assessment and security management can be complicated. done out consistently and efficiently.

5.4 OMNeT++:

OMNeT++ is a C++ simulation toolkit and framework that may be used to model vehicle networks. It is open-source, modular, and component-based. OMNeT++ is simple to use and features a high level of simulation granularity. It also can simulate network attacks and do threat assessments. The impact of various forms of assaults on-network data can be reflected by the data recording function.

5.5 SeaMonster:

SeaMonster is a threat model security modeling tool.
It facilitates the creation of attack trees and misoperation models using standard visual symbols, and freshly produced models may be attached to the database to be shared and reused. OWASP, rest Dragon is another tool that creates a threat model diagram using visual symbols. It is compatible with STRIDE, LINDDUN, and CIA (confidentiality, integrity, and availability). It may automatically build possible threats in the model and deliver associated mitigations based on the threat modeling diagram and rule engine given.

Tool	**Function**	**Result**
MTMT	Threat modeling	Threat assessment

	and analysis	reports
GROOVE	Creating an attack graph and modeling the network architecture	Attack graph
Practical Threat Analysis	Modeling threats and estimating risk assessment outcomes	Level of security/threat model parameters/counter measure efficacy analysis
OMNeT++	Simulation and threat analysis of network attacks	Simulation of a network assault and threat analysis results
SeaMonster	Creating attack tree models and a model of misbehavior	Threat models

Table 1 Comparison of TARA tools and its functions

6. FUTURE DEVELOPMENTS

Scholars from both the United States and elsewhere have developed a number of cybersecurity threat analysis frameworks, however the process is extremely subjective and lacks quantitative research. TARA techniques, both formal and quantitative, are a research direction that can successfully handle this challenge. A formal quantitative threat analysis technique employs standardized languages like SysML to explicitly describe the system under test and do threat modeling at the system level.

6.1 TARA Process Based on Data

OEMs may acquire more actual data from consumers' automobiles as contemporary vehicles increasingly communicate data with the cloud. TARA can benefit greatly from a big volume of data. For example, the TARA method, which is based on machine learning techniques, has extremely large data size needs. The accuracy of threat model training can be guaranteed with large-scale data. The data-driven TARA approach is a new research path.

6.2 TARA Methods that Take into Account Trade-Offs

The increased interaction and communication of cyber and automobile systems has created new safety and security problems.Because cyber-attacks might compromise a vehicle's functional safety, it's impossible to improve overall protection levels without including both sides. Furthermore, having too many security defensive measures would not only raise the overall vehicle cost, but it will also have an impact on the user experience. As a result, one essential aspect of TARA approaches is to evaluate the trade-offs of security, safety, vehicle cost, and user pleasure.

7. CONCLUSION

The probable security threats in linked autonomous vehicles are explored in this study, as well as the approaches of Threat Analysis and Risk Assessment in the automotive area, which are studied and contrasted. All of the approaches are categorized so that researchers may quickly and thoroughly grasp the topic of TARA. Additionally, the many ways to evaluate TARA methods in the literature are described. In addition, the future directions of TARA for the automotive area are explored.

References

[1]https://www2.deloitte.com/content/dam/Deloitte/be/Documents/strategy/Securing%20The%20Future%20Of%20Mobility.pdf

[2]https://www.sciencedirect.com/science/article/pii/S2352484721007289

[3]https://www.hindawi.com/journals/scn/2021/1263820/

[4]https://www.researchgate.net/publication/344947562_Cyber-attacks_in_the_next-generation_cars_mitigation_techniques_anticipated_readiness_and_future_directions

[5]https://www.nrel.gov/docs/fy19osti/74247.pdf

[6]https://www.researchgate.net/publication/320056629_Vulnerability_assessment_of_Electronic_Control_Unit_ECU_of_automotive_system_through_OBD-II_port_and_CAN_bus

[7]https://www.sciencedirect.com/topics/engineering/wireless-technology

[8]https://www.researchgate.net/publication/313543601_Survey_on_effective_GPS_spoofing_countermeasures

[9]https://www.sciencedirect.com/science/article/pii/S221420961930261X

[10]https://www.bridgestonetire.ca/learn/maintenance/tire-pressure-monitoring-system-how-tpms-works/