International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 3.392| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 8, Issue 2, March-April 2021 ||

Methods for Threat and Risk Assessment and Mitigation to Improve Security in the Automotive Sector

Pankit Arora[1*], Sachin Bharadwaj[2]

Sr. Risk Modeling/Analytics Analyst, Mr. Cooper, USA[1]

Assistant Manager (GRC), EXL Service Pvt Ltd. India[2]

ABSTRACT: Increased interconnection between application utilities and car wireless connections may increase the likelihood of cybercrime, attackers, and, in some situations, terrorists using automobiles. Additionally, as automated driving technology advances, the autonomy of the vehicle system increases, increasing the destructiveness of vehicle breaches. In addition to domestic security, the same multifaceted and varied problems that intelligent and integrated cars should face could jeopardise privacy and physical safety. Several nations have previously proposed stricter laws and regulations for vehicle safety in response to the aforementioned incidents. Automobile manufacturers make a great emphasis on enhancing the confidentiality of their automobiles. This study expands on a thorough examination of risk as well as vulnerability assessment techniques for the automotive industry with the goal of enhancing security mechanisms.

KEYWORDS: Risk assessment, Threat analysis, TARA approach, Automotive domain.

I. INTRODUCTION

A variety of safety solutions have been offered to provide automotive security precautions. Regrettably, this same security vulnerability could well be addressed quickly since present safety precautions largely provide passive or unique protection for a particular safety risk. TARA techniques may aid in locating possible dangers during an early point in the process and offer theoretical justification for choosing strategies to mitigate by detecting potential prospective security risks and vulnerabilities. Furthermore, there is limited information available on TARA strategies and tools in the automobile industry, nor is there a discussion regarding how to theoretically apply effective countermeasures to counteract the associated dangers. The purpose of this investigation is to undertake a comprehensive investigation of recent TARA-related findings in the automobile industry. The current research examines the TARA techniques already employed in the automobile industry and draws out the qualities of the suggested ways. Additionally, standard TARA technologies were presented.

1.1. Threat Analysis and Risk Assessment Methods (TARA)

TARA is currently in the beginning stages of development in the manufacturing of smart as well as linked automobiles. The cyber-physical systems of such smart as well as interconnected vehicles can lower the overall vulnerability of perceived attacks to a satisfactory limit at a minimal cost using vulnerability assessments as well as risk analysis [1-6]. The security of cars might then be raised. The methodology of risk examination and risk assessments is depicted in Figure 1. TARA primarily entails three steps:

1. Vulnerability assessment is responsible for spotting certain possible dangers concerning specific automobile infrastructures.
2. Risk assessment is capable of categorizing and analyzing the vulnerabilities that have been found, as well as determining the hazards that go along with them.
3. Risk assessment sorts risks per their level of risk and determines whether the risk posed by a certain danger is reasonable and whether risk-reduction actions are required.

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 3.392| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 8, Issue 2, March-April 2021 ||

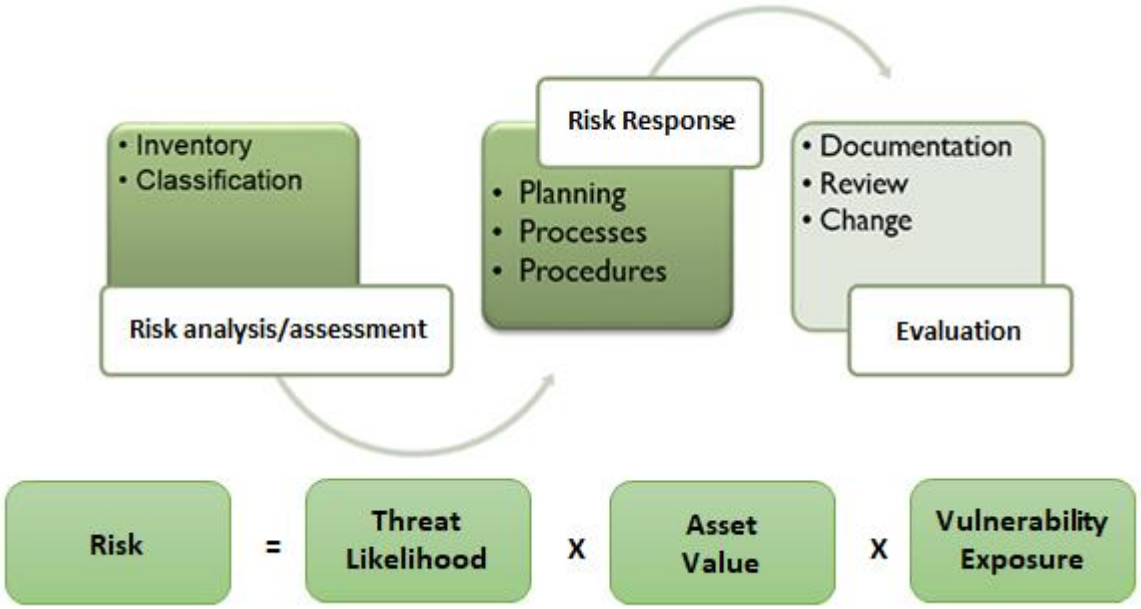

Figure 1. Threat analysis and risk assessment procedure

Formula-based approaches as well as prototype techniques seem to be the two divisions of TARA methodologies. Techniques for risk evaluation and risk assessment of such systems that primarily use statistics, textual, or equations are known as formula-based approaches. Asset-based techniques, vulnerabilities and threats approaches, and attacker-based techniques are indeed the three categories into which formula-based methodologies are separated following the various issues they address. Model-based approaches, a form of vulnerability analytical technique, model and analyze the risks and dangers to the network using various systems, such as flow diagrams, charts, and tree modeling techniques. Model-based approaches can be classified as either graph-based or tree-based, depending on the varied issues they address.

Model-based methods analyze the system's vulnerabilities using several approaches, making them highly realistic. The findings from the quantitative analysis are more accurate and therefore are also more reproducible. The complexity of these strategies makes them increasingly challenging to comprehend and apply. The classification of TARA approaches will be covered in the next sections.

II. FORMULA-BASED METHODS

2.1. Asset-Based Methods

The most popular TARA strategy inside the automobile industry seems to be the asset-based methodology. To carry out advanced protection, this sequence of approaches initially determines the ultimate target resource that is currently being attacked. It next exhausts all future attack routes and attack vectors that could endanger this target resource. Such an approach is additionally referred to as a top-down approach. OCTAVE was made available in 1999 by CERT/CC. Among the most popular TARA techniques in use, today is the OCTAVE technique.

For the employees of the organization to fully own business's network security requirements, the OCTAVE technique separates the evaluation into three stages. During these stages, managerial concerns and technology factors are evaluated as well as debated. As a technique of evaluation that incorporates resources, risks, as well as exposures, the OCTAVE methodology is described. It enables the management to utilize the assessment results to choose the OCTAVE technique that combines resource, risk, as well as vulnerability evaluations. Additionally, companies can leverage the assessment's findings to order the threats that need to be resolved. It moreover takes into account how well the cloud provider is utilized and how well it contributes to the achievement of organizational goals. Figure 2 depicts the stages in the OCTAVE approach for risk analysis.

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 3.392| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 8, Issue 2, March-April 2021 ||

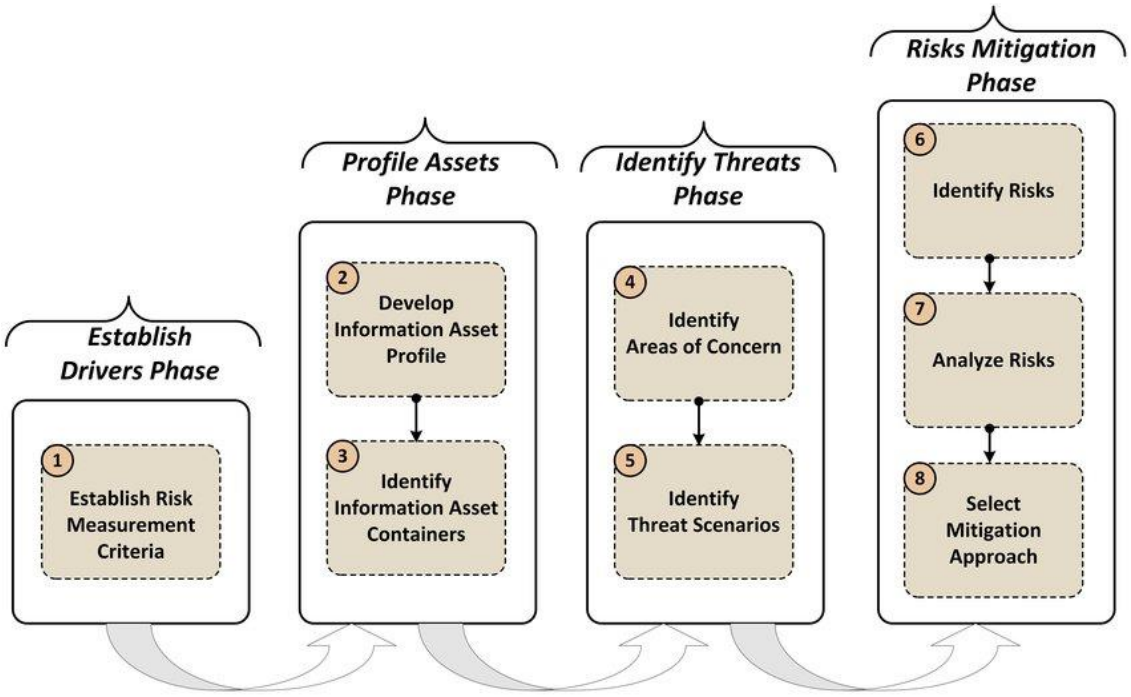

Figure 2. Sages in OCTAVE Methodology

The interconnected technological configurations underlying the computing environment are combined with OCTAVE. Additionally, it enables a reproducible, flexible approach that can be altered to meet the requirements of other businesses. A technique for asset-based vulnerability assessments is the EVITA approach. This approach offers an economical cybersecurity strategy that may offer thorough safety during several phases of evolution, including architecture, validation, or prototyping for vehicular communications. Every resource in the network is subject to a threat evaluation using the EVITA approach, after which the degree of danger posed by the assault is determined. The possibility of an assault as well as the extent of the damage it would certainly occur determine risks. Those are used to risk-rate risks as well as assign them a risk level. Significant risks could be evaluated using the EVITA risk assessment approach. To narrow down the assessment to the risks with the greatest risk levels, the detected potential threats could be graded based on the danger level they pose.

Assets and defense goals can be quickly and effortlessly identified by non-security professionals using the SGM Method. Ten reference terms were generated from this, including admission, disconnection, delay, removal, pause, deny, trigger, inclusion, reset, and manipulations. A customizable authentication protocol that is controllable as well as adaptive throughout the equipment's entire lifecycle is offered, and the policy-based authentication process may be modified to meet the security goals of the particular use scenario. OEMs can avoid depending mostly on security guarantees of outside providers by enforcing safety requirements through rules. Deployment tactics could guarantee that hardware performs as the OEM had anticipated. The OEM could provide security specification updates if the safety specifications of such equipment change after manufacturing, for instance, if a significant vulnerability has been discovered. Whereas other asset-based approaches could analyze threats numerically, the vulnerability scanning methodologies mentioned earlier concentrate on the subjective examination of levels of exposure.

Depending on the likelihood of an assault happening and the effect an assault would have on the network, TVRA can determine the risk degree of a framework. TVRA may produce a numerical assessment of network asset risk as well as a comprehensive list of safety precautions to reduce management complexity. The US2 utilizes a straightforward statistical methodology to assess security risks and dangers simultaneously and successfully determine what is needed for security and protection.

2.2. Vulnerability-Based Methods

The vulnerability-based approaches are bottom-up TARA methodologies, similar to asset-based procedures. They examine whatever other, more serious flaws as well as breakdowns the discovered flaw in the system might lead to after starting with this. CVSS is indeed an established industry norm used to assess the significance as well as the severity of a required response. The fundamental goal underlying CVSS would be to aid in the development of a

standard to assess vulnerability seriousness, allowing for comparison of vulnerability magnitude as well as prioritization of remediation.

Depending on test findings on a number of variables known as indicators, CVSS ratings are generated. Three distinct sorts of ratings are available throughout the CVSS: basic, temporal, as well as environment metrics. By extending the safety qualities based on FMEA, FMVEA transforms into a co-analysis technique for ensuring safety and security. Risk categories are applied to examine whether safety features collapse, while its modes of failure could analyze whether elements' quality parameters collapse. The recurrence of risk patterns could be estimated by recognizing risk components, and indeed the likelihood that a risk pattern will happen depends on the potential attackers and vulnerability.

The CHASSIS modeling approach divides the entire procedure into two parts that specify the objectives for usability, security, as well as protection. For such incorporation of security and protection criteria, the first phase primarily establishes the performance requirements. The second phase is where the implementation of safety and protection standards takes place. This stage will depend on the collective knowledge of industry specialists in cybersecurity to suggest certain potential abuse circumstances as a crucial foundation for the comprehensive research findings. This means that the CHASSIS assessment methodology incorporates several arbitrary aspects.

Six criteria are used to assess the two methodologies, FMVEA and CHASSIS: level of abstraction, the accurateness of repeated analysis, reuse of assessment artifacts, the context of assessment, appropriateness for a risk level, and flexibility to the dynamic environment through an automotive FOTA application scenario. Additionally, a technique is suggested in NIST SP 800-30, Risk Management Guide for Information Technology Systems, for carrying out a risk evaluation in nine successive stages.

2.3. Attacker-Based Methods

A risk modeling approach that examines intruders would be the attacker-based methodology. It performs vulnerability assessment including threat assessment on the system by taking into account the amount of expertise, possible attacks, attacking goals, and availability of materials for future attacks. Throughout this manner, the risk could be represented as well as examined starting with the attack's underlying reason. SARA is indeed an extra security vulnerability assessment methodology for automobiles with autonomous vehicle systems that take into account security specialist perspectives, emerging threat categories, network intrusions, resource mappings, including descriptions of assault trees. Additionally, SARA introduces a brand-new parameter that takes the predictability of the operator or automated car technology into account when calculating the risk rating. By providing an abstract explanation of the fundamentals of automobile safety modeling, SAM (Security Abstraction Model) tightly integrates safety practices with model-based requirement engineering. The purpose of the risk agents' risk management approach, which is carried out in 6 phases, would be to identify the interconnected car's essential vulnerability. TAL (threat Agent Library), MOL (Methods and Objectives Library), and CEL (Common Exposure Library) make up the Threat Agent Risk Assessment approach. Threat Agent Risk Assessment could create a collection of possible assaults as well as score them in terms of how likely they are to materialize. Unfortunately, the risk agent risk assessment approach is relatively new, therefore aside from the negligible information made available by Intel Security, there must be essentially no accompanying material.

2.4. Graph-Based Methods

The terminals as well as unidirectional connections link the graph-based approaches together. The statistical risk evaluation of the system is made easier by the use of graph-based approaches that might represent the direct mathematical statistical interaction of every component module. Spoofing (S), tampering (T), repudiation (R), information disclosure (I), denial of service (D), and elevation of privilege (E) make up the STRIDE model. The STRIDE approach has been extensively utilized in the IT sector and also has demonstrated the ability to recognize as well as assess issues that may arise, significantly lowering the likelihood that the network would be hacked. The STRIDE approach is progressively being implemented in different sectors because of its outstanding results.

The SAE J3061 rules explicitly advocate the STRIDE approach for vehicle data protection. In complement to the STRIDE approach, PASTA is a seven-stage risk analytical technique (i.e., Process for Attack Simulation and Threat Analysis). The data flow diagrams are used by PASTA only at the software decomposition layer. Through a six-step examination, the LINDDUN technique protects the platform's data confidentiality and privacy. Incremental development components based on information flow diagrams are used to analyze and find various risks. The VAST methodology could be expanded to include massive risk model evaluation.

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 3.392| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 8, Issue 2, March-April 2021 ||

2.5. Tree-Based Methods

The affiliation among components and their organizational relationships could both be represented and described using tree-based approaches. The attack tree paradigm that can explain the threat the system is encountering and demonstrate the offensive route, is among the most characteristic of this type of approach. A vulnerability assessment technique called attack tree analysis makes use of a tree's architecture. Figure 3 depicts the attack tree's basic structure.

The attacking destination is represented by the event of interest, while all other occurrences that may just lead to the assault targets occurring are represented by the networks beneath the attacked target. Through the OR and AND gates, the logical connection between such occurrences can be made. Attack tree analysis may be carried out top-down, which involves selecting the assault destination initially and then examining all potential attack routes in light of that destination. This could alternatively be done from the bottom up, which helps in analyzing future attack surfaces before examining security vulnerabilities in light of those surfaces.

Unfortunately, the conventional attack tree analysis technique necessitates the manual development of several assault possibilities while dealing with the vulnerability assessments of large systems. Many OEMs consider it intolerable that new vulnerabilities would be compromised as well as the higher probability that vehicular technologies will be hacked. A technique for automatically generating attacking forests for automobile networking for malware threats has been developed to address this weakness of attack tree assessment. With the help of a simulation environment, the system may dynamically determine the best assault route seen between the assailant and the resource.

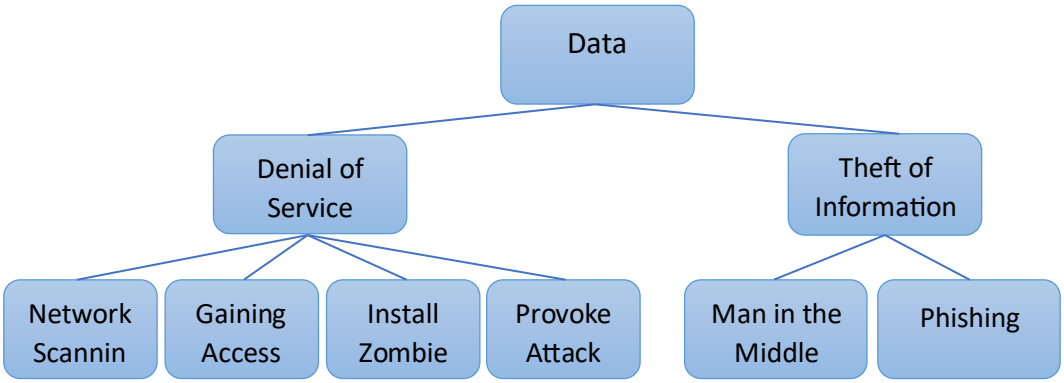

Figure 3. The common construction of the attack tree

This approach could finish a huge platform's risk analysis including vulnerability assessments in a short amount of time even when the worst-case scenario. For OEMs, which frequently have to conduct extensive risk analyses on vehicle systems, this seems to be particularly advantageous. By including probability density functions depending on attack tree analyses, the RISKEE approach makes it possible to quantitatively quantify the risks to safety and protection. The RISKEE technique additionally employs the RISKEE dissemination algorithms to compute risk via both forward and reverse. Additionally, the BDMP technique increases the scope of how risks can be described through the analysis of fault trees and attack tree assessment. However, the beginning stages of risk examination and risk assessments are not appropriate for the BDMP technique.

As demonstrated by the given description, recent exposures revealed many risks in nearly all interrelated components of automobiles: To protect external access to third-party services and equipment through automobiles in their leases, vehicle manufacturers now function as local internet registries and manage a collection of IPs, certificates, including credential monitoring systems. Contemporary automobiles accomplish this by implementing remote access to third-party services through a bridge gateway that runs Linux.

During the End-of-Line (EOL) manufacturing operation, the gateway servers for every automobile are set up with unique original keys as well as credentials. In addition to the gateway infrastructure, automobiles provide a number of alternative mechanisms to handle on-board features, including the specific Vehicle2X routing protocols, WLAN, Bluetooth, and the on-board diagnostics (OBD) interface as well as capabilities.

Contemporary automobiles' assault surfaces are widened by such connection characteristics, rendering them more open coming from external attacks. In this multi-layered assault, flaws in the external connections are taken advantage of to control the car's on-board systems, which finally results in undesired driving. The components of the strategy shown are as follows:

1. Information disclosure: In the initial phase, hackers prepare their attacks employing the same model and manufacturer of automobiles. The OBD platform enables hackers to intercept car network communications and discover some characteristics of such network communications (i.e., parts of the message catalog). Additionally, even the producer of the car's IP address clusters could be located. In the following assault, the targeted car's precise IP address is discovered by listening into the conversation seen between the specific vehicle as well as the manager's cell phone.

2. Privilege elevation: The hacker subsequently uses the Linux gateway's firewall's critical vulnerabilities to get administrator rights, allowing them to enter the car's network infrastructure. At this time, harmful instructions can be transmitted to the interior network environment using the gateways as well as harmful programs can be installed on the gateways.

3. Spoofing: The last stage is attacking that automobile by running a code that was previously established mostly on gateways. This code delivers messages with malicious links although properly constructed automatic steering orders including speed of the vehicle data to the car's local network. The initial assault phase revealed the message structure, which is currently being employed in a so-called spoofed IP address to mimic the actions and communications of other public transportation. In the following case, the steering control unit (SCU) is tricked into accepting steerable instructions from the parking assistance control unit (PACU), while the automobile is moving at a considerable speed to the replicated speed of the vehicle data (i.e., the driver is traveling at a speed compared with fewer from over 5 km/h).

III. ISO 26262 FOR AUTOMOTIVE SAFETY

The worldwide guideline concerning security requirements of electrical and/or telecommunications devices in new vehicles is ISO 26262 "Road vehicles - Functional safety" (ISO, 2011). It adheres to the concept of ISO 31000 and represents a risk-oriented standard (ISO, 2018). This is an application of the risk-based inspection and testing standard IEC 61508, which would apply to all sectors.

The specification defines security procedures to prevent or lessen the impact of breakdowns, whether of a systematic character, by addressing the likelihood of dangerous operating circumstances utilizing subjective HARA techniques. From a procedural standpoint, it incorporates two V phases for hardware and software components, following the automobile's W-shaped lifespan [7-12]. Significant risks are identified as a consequence of HARA, which is carried out at the conceptual phase. A rating mechanism of an operating environment, the degree of controllability, as well as the seriousness of the injury inflicted, is utilized to evaluate the associated threats. The automobile safety integrity level (ASIL) that ranges from A to D which is the most dangerous threshold, is used to assess it. Process improvement practices for technologies having lesser vulnerabilities This specification outlines the fundamental network security principles for the early stages of development. It does not include any rigorous guidelines for handling particular cybersecurity threats, post-production, dismantling stages, or vehicle computer security.

3.1. ISO 21434 for Automotive Cyber Security

This forthcoming guideline, which is scheduled to be published, hopes to encourage manufacturing agreement regarding important concerns about cyber security inside the automobile sector. This should replace J3061, practice guidelines, and even more organized suggestions which demonstrate whether seriously the company is taking the issue of guaranteeing vehicle information security. The focus is now on commercial vehicles (such as cars, lorries, and buses) as well as includes information on all of their modules, parts, and interconnections, including programming. Their objective is to make sure that producers or every supply chain stakeholder have organized procedures in place that promote security by design procedure.

Corresponding to ISO 26262, it examines the safety full project development and evolutionary history of an automobile from a management standpoint. The V-model is used, and a diverse range of tasks are taken into account, including TARA inside the development branches, validation and confirmation inside the test division, security management, and event or reaction administration in the operation and maintenance. Ten parts and fifteen sections make up the format's organization. It begins by explaining the following terms: (1) the context; (2) the legal references; (3) the terminology; (4) basic principles; and (5) the management framework (clauses 5-6-7). Next, the concentration is on threat assessment (6/clause 8). It is then followed by three parts that discuss the conception stage (7/clause 9), product design (8/clauses 10-11), and production, operations, and service (9/clauses 12-13-14). The accompanying mechanisms are covered in the last portion (10/clause 15).

The specification does not enforce any TARA methodologies about the risk assessments, however, clause 8 informs of the required stages it should include, in line with ISO 27005. The convenience, as well as the economic efficiency of new automobiles, can indeed be accomplished without such usage of management software. Modern security measures including accident prevention cannot exist without clever software applications, in specific. Though software

applications are always present in automobiles, as automobiles are becoming more connected, safety concerns are growing. Massive remote cyberattacks by knowledgeable hackers are conceivable, especially when using the world wide web and Car2X technologies. The greatest concern is how this kind of attempt will affect security. A most serious situation could occur if the brake, wheels, and perhaps other essential components were disabled, jeopardizing the vehicle's safety of the automobile and perhaps having catastrophic results. It should be noted that historical past, to carry out a distant cyberattack on vehicular systems, the hacker had to physically access the automobile at least occasionally. Violent events had demonstrated that they don't need accessibility [13-20].
Techniques that protect bus communications as well as introduce trustworthy computation to every electronic control unit (ECU) executing technology products are necessary to resist such attacks. Most approaches necessitate no modifications to a distributed operational application or even its design phases, instead modifying the base AUTOSAR-compliant fundamental programming. These may reduce various security problems while also raising the threshold for intruders. Nevertheless, such technologies suffer the same basic management challenges as IT platforms as well as significantly increase the expense of every ECU. Since price per unit is the single most important factor in vehicle manufacture, the implementation expense of trustworthy computing hardware could be prohibitively expensive. Furthermore, since consumers demand fundamental protection, providing a car security solution from malicious hackers could be difficult to explain to such buyers.

Rather than addressing cybersecurity with a one-size-fits-all custom solution, researchers proposed a complete as well as a comprehensive strategy for such protection for safety-critical technologies in automobiles established utilizing ISO 26262. Investigators want to integrate ISO 26262 with globally appropriate security standards. Two widely acknowledged safety regulations are the ISO 27001 benchmark as well as the Common Criteria. This same ISO recognized 23 972 ISO 27001 certificates in 2014, representing a 7% improvement over 2013. In addition, the ISO recorded 275 Common Criteria certifications in 2015, a 15% improvement over 2014. Those figures encompass certificates globally and therefore demonstrate the importance of safety requirements. As a result, such a technique adheres to the cutting-edge security model ISO 27001 to identify risks, execute a safety vulnerability assessment, and explain procedures to particularly handle dangers.

This is compatible with both ISO standards but also allows the system checks of such safety-critical technologies by incorporating sustainable artifacts needed by the safety lifecycle in the security lifecycle. Nonetheless, investigations show that the certificate requirement is still not enforced throughout this approach. It could also be used even without the goal of certifying, to consider cybersecurity throughout the process safety lifespan. Using current information, this technique delivers cost-effective as well as suitable protective measures. It gives a high-level perspective that might determine whether a security flaw is handled in several instances either with inappropriate or consequently expensive procedures. It may offer particular safeguards for the automotive industry, including plausibility checking or perhaps the strengthening of a gateway connecting various buses, which has been proved in the previous to thwart assaults.

IV. SYSTEMATIC RISK ASSESSMENT FRAMEWORK

Automotive security risks must evaluate changes to the security architecture, and information provided throughout the lifespan of the automobile. Vehicle security vulnerabilities can affect human security along with financial losses as well as privacy breaches [21-27].

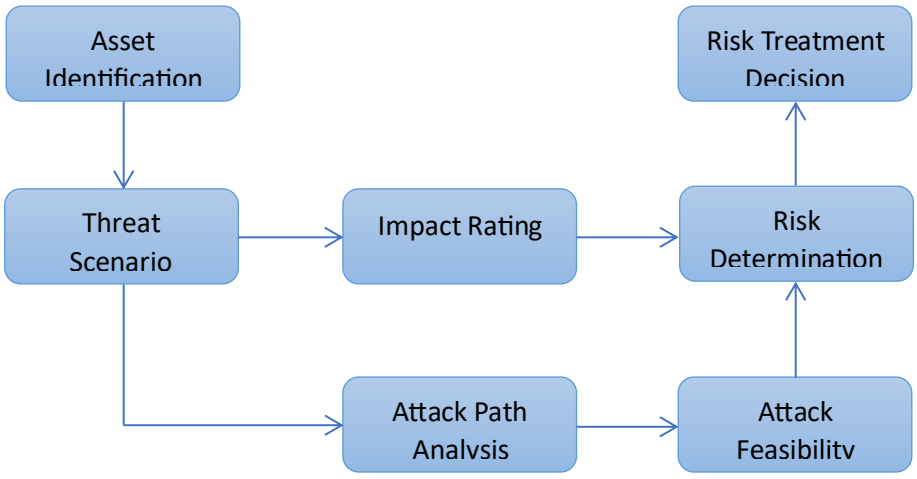

Figure 4. Automotive cybersecurity risk management framework

Additionally, the threat assessment of automobile security is particularly complex due to the broad diversity of security resources as well as possible attacks. This study provides a well-organized methodology as a result. The risk evaluation method as well as structured evaluation techniques make up the platform's two major building parts. The three steps of such a risk management process include identification, risk evaluation, and vulnerability assessments. As illustrated in Figure 4, each entity's evaluation procedures are defined inside the procedure that corresponds to it.

4.1. Identification of Risks

To evaluate if the prospects inside an element are real resources in automobile risk assessment, TOE or even use cases must be established before actual asset identification. The next step is risk assessment, which locates risk situations in an asset's security features. Eight subcategories will be used to classify automotive resources following the ENISA resource classification technique, i.e., sensors and actuators, to evaluate if the candidates in items are real assets, TOE or use cases should indeed be established before asset identification in automotive risk assessment.

Automotive resources can be categorized into eight groups using the ENISA asset taxonomy system. The data flow graph will be created using the asset categories as well as the TOE/use case to define fine-grained resources and define the associated security mechanisms including damaging possibilities. This STRIDE threat classification scheme is used next to identify assets. The SDL vulnerability assessment software is used by the STRIDE framework that determines the impact of hypothetical cyberattacks or the victim's objectives.

4.2. Risk Analysis

The goal of risk analysis is to evaluate each risk instance's effect as well as the viability of every offensive route. Outcome evaluation as well as assault assessment are included. Independent analysis seeks to calculate the extent of harm brought on by resources with breached security features. Assault path analysis, as well as threat capability evaluation, are the two basic components of attack analysis activity.

It is possible to estimate the effects on participants (i.e., safety (S), finance (F), operation (O), and privacy or law (P)) of automobile cyberattacks affecting driver safety, privacy protection, and global defense. The components of the impact evaluation could be measured using pertinent industry best practices like ISO 26262-3:2018 and BSI 100-4. The HEAVENS technique is referenced by the effect evaluation criteria inside this paradigm.

4.3. Transport Layer Security Communication

Into an encrypted connection as well as the EVSE's verification by the EV, Transport Layer Security (TLS) enables secure communications between the two devices. This guarantees the information flow's secrecy as well as security, but in certain circumstances, ISO-15118 sometimes does not call for the usage of TLS. This seems to be especially noticeable in situations with prescribed requirements for trustworthiness. Because in many cases in a shared environment the communications between EV and EVSE must be secure, if the trustworthy system is disrupted, the absence of TLS could constitute a serious safety issue.

4.4. Payment Modes

Regarding individual consumers, the ISO-15118 system permits more straightforward payment choices. Aid for something like the power provided is collected by numerous government entities and fee-based activities. The standard sets out specific payment options, External Identification Means (EIM) and Plug-N-Charge (PnC)., where the person can access power upon supplying the required information.

EIM—alternative transaction mechanism utilizing a physical point of sale (POS) device, such as a payment terminal or radio-frequency identification (RFID) device which communicates with EVSE. With such a sort of payment, the operator or the vehicle's driver physically charges for the fuel, such as at a petrol station. For EVSE operations, this is currently the most widely used form of payment. This approach could use TLS to provide a secured communication line even though it does need certificates. EIM can also integrate applications on mobile phones for permission and payments.

PnC—another substitute for such EIM POS which uses the electrical charge coupler to validate EV identities. PnC automates EV identification as well as authorizes the utilization of the EVSE using certificates. Making use of a public key infrastructure mechanism, the EVSE offers a contractual certification. The owner of the automobile or perhaps the EVSE must put such a certificate in the automobile. If implemented by EVSE, the communications must be encoded as well as communications safeguarded so that only the designated party can decode the information, including secret keys as well as digital certificates.

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 3.392| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 8, Issue 2, March-April 2021 ||

4.5. Threat Analysis

An attacker can use the following techniques to take advantage of the CCS charge platform's weaknesses [28-33]:

Spoofing—Changing an EV or EVSE's apparent identification to obtain charge authority. It might enable the intruder to refuel the car for nothing, without being required to pay or verify the subscriptions. Due to weakened authentication processes, this vulnerability could also harm additional EVSE customers. EIM without TLS/encrypted communications and PnC settings where TLS is still not necessary to run a higher risk of this happening.

Tampering—Accessing these EVSE controls physically may lead to electricity theft, system instabilities, and even the destruction of such EVs' mechanical systems. The current electronics and controls are particularly vulnerable. For instance, when a malicious hacker edits the messages, the local power devices' input power might well be impacted, or even the malicious party could delay or prevent charges. Zero charges might be possible if the meter or pricing data are fabricated. This same EIM POS system could be more susceptible to manipulation over PnC, but also through EVSE mobile software penetration.

Man-in-the-Middle—Installing a fraudulent bridge element that might be exploited to install malware or reroute money with an EVSE and an EV.

Contract Sharing—Concerning PnC implementation, if such an EV holder communicates the electronic agreement credential as well as secret key with certain other EV owners—and those holders can reconfigure their own vehicle's credential both these holders may be capable of charging their automobiles for free in according to the terms of the initial owner's agreement. The owners of the charging stations would suffer a loss of income.

Eavesdropping—Although not adequately secured, confidential material about EV as well as its owner is accessible to eavesdroppers. Any hostile group may utilize such data for commercial gain.

Denial of Service (DoS)—EVSE lines of communication are vulnerable to DoS attacks by hostile parties that want to prevent charges or interfere with grid functions, which might lead to something like an unsteady grid.

There are methods to integrate safety and protection which offer a cooperative examination of security and protection including related interdependence. In essence, this refers to the set of practices that promote the development including both secure and reliable platforms. Such a collection of methodologies presents original means of combined security and protection assessments that handle the interrelations throughout the assessment that limit the number of potential repetitions which could be caused by the competing protection and security standards in separate techniques. Although minimizing the number of iterations for coordinating safety and protection is an essential aim, one constraint of such approaches is that they are typically highly sophisticated and therefore would necessitate more effort to conduct, for illustration, two different operations for safety and protection assessment. Additionally, as these techniques involve significant differences in the level of practice for safety and protection procedures employed in businesses, they may be difficult to adopt in reality.

The degree to which techniques from such a category promote protection and reliability, i.e., if they accomplish detecting hazards and flaws at a minimum as well as autonomous procedures, is a widespread issue. The emphasis, for instance, is on damages done by breaches of transparency and availability, whereas anonymity is ignored. Furthermore, the approach's potential to aid investigators in assessing security restrictions deterioration through time is still not explored.

The researchers explain a strategy in which the characteristics connected with the model's safety may be challenging to assess. To overcome that, researchers focus also on the durability of the conclusions that could be made, attempting to identify conclusions that stay viable throughout a large range of values for the most dependent variables. The provided technique, which is centered on MILS infrastructure as well as a contract-based methodology, could be viewed as a promising alternative since it supports designing the network topology, contract-based architectural style assessment, and automated platforms setup, including verification case creation using a pattern. Nevertheless, the technique is quite particular, as well as a lack of experience in this area may lead to inadequate findings, while there is no assistance for managing finer-grained data flows features. Researchers examined standard failure modes and effects analysis (FMEA), which is centered on hardware failures, whereas STPA-Sec is considered system is a computer risk assessment. It calls into doubt the approach's sustainability since it is unclear if lower-level faults or risks were adequate in enabling modeling in systems with complicated relationships and spontaneous behaviors.

Strategies that provide a combined manner of evaluating stability and privacy with security as the ultimate aim, i.e., integrated safety-guided security methods. Because this category of techniques is concentrated on increased safety, the

majority of the methods are appropriately designed owing to conformity to a particular specification, but explored techniques are rather sophisticated as limits have already been taken into account of malfunctions, interconnections, and complicated assaults. Because the major emphasis of such a collection of techniques is protection, one possible drawback is their use in networks wherein non-safety-associated safety problems are equally significant. There is duplicate work in this situation since a portion of the information security would indeed be completed inside the integrated security-informed risk action, but the whole analysis still needs to be conducted independently.

Although this might minimize the number of feasible iterations for coordinating protection and reliability, it would nonetheless result in task redundancy when contrasted with the integrated holistic techniques. Additionally, a number of the ideas are specific and could necessitate additional research before they could be implemented in other fields. For instance, because the method sets criteria utilizing ISO 26262 and the Hazard and Operability Study (HAZOP) methodology in conjunction using Boolean logic Driven Markov Processes (BDMP), a greater standard of complexity and specialist expertise are needed. Given that it is dependent on expertise and knowledge, reuse in the repeated analysis is indeed not relevant because the amount of expertise in various groups may change, thereby impacting outcomes.

This same technique offered is indeed consistent with a railway regulation and, in practice, is based on domain experts. Considering this, the researchers are not quite confident that the technique will be appropriate for many other areas without first being tailored toward individual demands. The investigation is based on FMEA, which evaluates just individual sources of an impact, excluding multi-stage assaults.

V. CONCLUSION

Lacking sophisticated management software, cutting-edge security features such as accident predictions are challenging to implement in vehicles. Moreover, although automobiles have traditionally-featured software applications, the automotive connection has been rising, therefore cybersecurity is growing more important. This paper perceived that massive offsite assaults involving trained hackers are conceivable, especially through the utilization of the internet and Car2X services. Also, the greatest concern in this kind of assault is the disruption of security. This paper identified a few misguided activities like disabling the brakes, wheels, or even other important elements, that would jeopardize a driver's vehicle safety and result in deadly repercussions. Traditional cyberattacks on security technologies necessitated the intruder to obtain accessibility to the automobile at minimum once before launching a distant hack on safety-critical systems. Several assaults demonstrate that accessibility is not required. Finally, a detailed analysis of threat and risk assessment approaches for the automobile area is summarised in this paper.

REFERENCES

[1] Boudguiga, A., Boulanger, A., Chiron, P., et al.: Race: Risk analysis for cooperative engines. New Technologies, Mobility and Security (NTMS), 7th International Conference, IEEE. (2015).
[2] CCRA Members.: Common methodology for information technology security evaluation –evaluation methodology. CCMB, version 3.1, revision 4, common criteria (2012).
[3] Cisar, P., Rajnai, Z., Cisar, S.M., et al.: Scoring system as a method of improving IT vulnerability status. Ann. Fac. Eng. Hunedo. 14(3), 207 (2016).
[4] Dominic, D., Chhawri, S., Eustice, R.M., et al.: Risk assessment for cooperative automated driving. Proc. 2nd ACM Workshop Cyber-Phys. Syst. Secur. Priv. 47–58 (2016).
[5] Foster et al. 2015. "Fast and Vulnerable: A Story of Telematic Failures."
[6] Geotab. 2017. “Best Practices for Cybersecurity Management in Telematics.” Geotab Inc., Accessed May 2019.
[7] Greenberg, Andy. 2015a. “Hackers Remotely Kill a Jeep on the Highway—With Me in It.” WIRED, July 21, 2015. https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.
[8] Greenberg, Andy. 2015b. “This Hacker's Tiny Device Unlocks Cars and Opens Garages.” WIRED, August 6, 2015. https://www.wired.com/2015/08/hackers-tiny-device-unlocks-cars-opens-garages/.
[9] Greenberg, Andy. 2016. “Hackers Fool Tesla S’s Autopilot to Hide and Spoof Obstacles.” WIRED, August 4, 2016. https://www.wired.com/2016/08/hackers-fool-tesla-ss-autopilot-hide-spoof-obstacles/.
[10] Hawkins, Andrew. “No, Elon, the Navigate on Autopilot is not ‘full self-driving’.” The Verge, January 30, 2019. https://www.theverge.com/2019/1/30/18204427/tesla-autopilot-elon-musk-full-self-driving-confusion.
[11] Hodge, Cabell and Mark Singer. 2017. Telematics Framework for Federal Agencies: Lessons from the Marine Corps Fleet. Golden, CO: National Renewable Energy Laboratory. NREL/TP-5400-70223, October 2017. https://www.nrel.gov/docs/fy18osti/70223.pdf.
[12] Hunt, Troy. 2016. “Controlling vehicle features of Nissan LEAFs across the globe via vulnerable APIs.” TroyHunt.com, February 24, 2016. https://www.troyhunt.com/controlling-vehicle-features-of-nissan/.

[13] IIHS-HLDI. 2018. "GM front crash prevention systems cut police-reported crashes." Insurance Institute for Highway Safety Highway Loss Data Institute, November 13, 2018. https://www.iihs.org/iihs/news/desktopnews/gm-front-crash-prevention-systems-cut-police-reported-crashes.
[14] Islam, M.M., Lautenbach, A., Sandberg, C., et al.: A risk assessment framework for automotive embedded systems. 2nd ACM International Workshop on Cyber-Physical System Security, AMC. (2016).
[15] Kadhirvelan, S.P., Soderberg-Rivkin, A.: Threat modelling and risk assessment within vehicular systems. Chalmers University of Technology Department of Computer Science and Engineering, Goteborg (2014).
[16] Asuvaran & S. Senthilkumar, "Low delay error correction codes to correct stuck-at defects and soft errors", 2014 International Conference on Advances in Engineering and Technology (ICAET), 02-03 May 2014. doi:10.1109/icaet.2014.7105257.
[17] Li, Xiangxue, Yu, Guannan Sun, and Kefei Chen. 2018. "Connected Vehicles' Security from the Perspective of the In-Vehicle Network." IEEE Network 32 (3): 58–63. https://doi.org/10.1109/MNET.2018.1700319.
[18] Li, Yansong, Qian Luo, Jiajia Liu, Hongzhi Guo, and Nei Kato. 2019. "TSP Security in Intelligent and Connected Vehicles: Challenges and Solutions." IEEE Wireless Communications, 1–7. https://doi.org/10.1109/MWC.2019.1800289.
[19] Macher, G., Sporer, H., Berlach, R., et al.: SAHARA: A securityaware hazard and risk analysis method. Design, Automation & Test in Europe Conference & Exhibition, IEEE. (2015).
[20] Mäkilä, Tommi, Jukka Taimisto, and Miia Vuontisjärvi, 2011. "Fuzzing Bluetooth: Crash-testing bluetooth-enabled devices." Codenomicon Ltd, September 19, 2011.
[21] Mariani, Riccardo. 2018. "An Overview of Autonomous Vehicles Safety." In 2018 IEEE International Reliability Physics Symposium (IRPS), 6A.1-1-6A.1-6 (March 11-15, 2018). https://doi.org/10.1109/IRPS.2018.8353618.
[22] Michael, Craig. 2018. "What Is Telematics?" Geotab Blog, January 8, 2018.
[23] Miller, Charlie and Chris Valasek, 2014. "A Survey of Remote Automotive Attack Surfaces." Illmatics.com. Accessed May 2019. http://illmatics.com/remote%20attack%20surfaces.pdf.
[24] Moalla, R., Labiod, H., Lonc, B., et al.: Risk analysis study of its communication architecture. In Network of the Future (NOF), 3rd International Conference, IEEE. (2012).
[25] Montalbano, Elizabeth, 2019. "Hackers Remotely Steer Tesla Model S Using Autopilot System." https://securityledger.com/2019/04/hackers-remotely-steer-tesla-model-s-using-autopilot-system/.
[26] Monteuuis, J.P., Boudguiga, A., Zhang, J., et al.: SARA: Security Automotive Risk Analysis Method. the 4th ACM Workshop, ACM. (2018).
[27] NIST. 2013. Security and Privacy Controls for Federal Information Systems and Organizations. National Institute of Standards and Technology (NIST) Special Publication 800-53 Rev. 4. April 2013 https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final.
[28] Paukert, Chris. n.d. "Why the 2019 Audi A8 won't get Level 3 partial automation in the U.S." Roadshow by CNET, May 14, 2018.
[29] Ruddle, A., Ward, D., et al.: Security requirements for automotive on-board networks based on dark-side scenarios. EVITA deliverable D2.3, EVITA project (2009).
[30] Scandariato, R., Wuyts, K., Joosen, W.: A descriptive study of Microsoft's threat modeling technique. Requir. Eng. **20**(2), 163–180 (2015).
[31] Schneier, B.: Secrets and lies: digital security in a networked world. Wiley, Hoboken (2000)
[32] Shao, X.B., Jin, Y.Z.: Research on the classification of automobile industry vulnerability based on HEAVENS model. Jiangsu Sci. Technol. Inf. **563**(14), 80–82 (2018).
[33] Wolf, M., Scheibel, M.: A systematic approach to a qualified security risk analysis for vehicular IT systems. Auto. Saf. Secur. 195–210 (2012).