International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 12 Issue: 03 | Mar 2025 www.irjet.net p-ISSN: 2395-0072

A Comprehensive TARA Approach to In-vehicle network Security in Software-Defined Vehicles

Rutuja Rajole,

[1] *Senior Design Engineer, Tata Technologies Ltd*

Abstract - *The increasing dependency on Software-Defined Vehicles (SDVs) has led to various security vulnerabilities within in-vehicle networks, which can impact the driver safety, personal information, and driver's assets. In the beginning era of security methods used are no longer able to address the rapidly changing threat possibilities. The purpose of this project is to implement a complete TARA analysis approach which is uniquely designed for the security needs of SDVs. My project strategy involves a multi-layered threat analysis framework. These will help us to identify, evaluate, and reduce potential security threats effectively. Considering the TARA method, we are targeting to reduce security risks, boost our ability to detect threats, and make the overall safety of software defined vehicles better.*

Key Words*: *TARA, SDV, IVN, cybersecurity, attack, asset

1. INTRODUCTION

Threat Analysis and Risk Assessment is necessary method which is used to upgrade the cybersecurity within Software-Defined Vehicles. In the era of zonal architectures & domain architectures vehicles are becoming more self-analyzed, connected and automated, they are exposed to an increasing number of cyber-attacks that could risk safety, functionality, and user privacy. TARA analysis is playing a crucial role in identifying and evaluating the cyber-attack. TARA allows industrialist to develop and implement complete and robust solutions. TARA is in line with industry standards that is ISO/SAE 21434 which is the cybersecurity standard, which provides a robust framework for analyzing cybersecurity risks across the vehicle's lifecycle and architecture. The process involves many stages that are identifying assets, setting up attack scenarios, examining risks, evaluating impacts, and measuring risks. By thoroughly investigating potential cyber-attack and their impact on vehicle architectures and driver's safety, TARA framework allows organizations to prioritize risks severity and make robust decisions on the necessary security measures.

2. OBJECTIVES:

1. The identification of Essential features and functionalities in SDV. The above task has been successfully completed, by focusing on the some particular crucial ECU functionalities that will go through TARA analysis based on their value to the vehicle safety and operation.

2. The complete analysis of the architecture design requirements for the SDV world. There are main two task sub division.

   a. The Study of architecture: In this complete study of the architecture, it has both the elements like hardware and software components to create an adaptable system. It covers various layers like the hardware components (i.e. CPUs, sensors, ECUs) and the other big component Software framework that supports vehicle functionalities.

   b. Checking of Cyber-attack vulnerabilities: In this we are more focuses on the major potential pathways where the cyber threats could exploit weakness inside the architecture thus it leads to a major disaster, which includes the vulnerabilities in communication interfaces, and software update process, here comes major one centralized control units.

3. Evaluate the existing cybersecurity vulnerabilities and threats specific to the SDV. Applying effectively cybersecurity measures to address identified risks. Then analyzing how well these cybersecurity solutions improve the resilience of SDV against the potential threats.

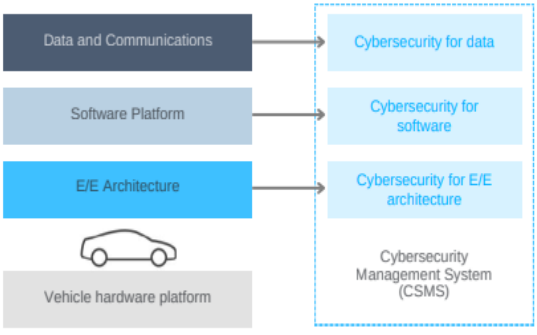

Fig: E/E Architecture in line with TARA

A thorough and flexible framework for controlling cybersecurity threats in software-defined vehicles is offered by the TARA technique. Manufacturers and developers can enhance security posture, proactively resolve vulnerabilities,

and guarantee the dependability and safety of SDVs by implementing TARA. This strategy not only contributes to the protection of vital automotive systems but also fosters user trust by showcasing a dedication to strong cybersecurity procedures.

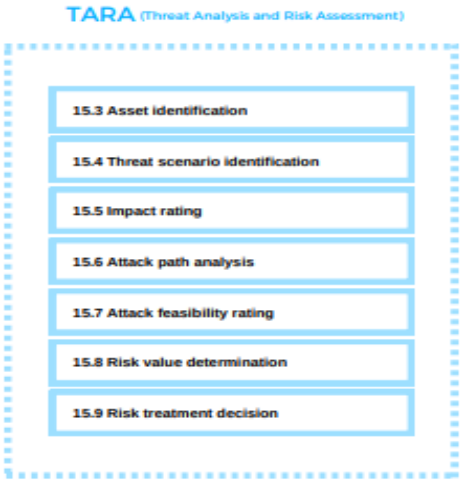

Fig: Overview of TARA

3. Cybersecurity Features:

The CIA model of cybersecurity is

1. **Confidentiality:**
   An organization's attempt to ensure that data is kept private or hidden are referred to as confidentiality. Making sure that individuals without the appropriate authorisation are unable to access assets that are crucial to your company is a crucial part of protecting confidentiality. For instance, in order to diagnose the data, suppliers and vendors should have minimal access to any of your vehicle networks. Confidentiality can be violated in a number of ways. This could entail direct attacks meant to obtain access to systems that the attacker is not authorised to view. An attacker may also try directly to get into a database or application in order to steal or change data.

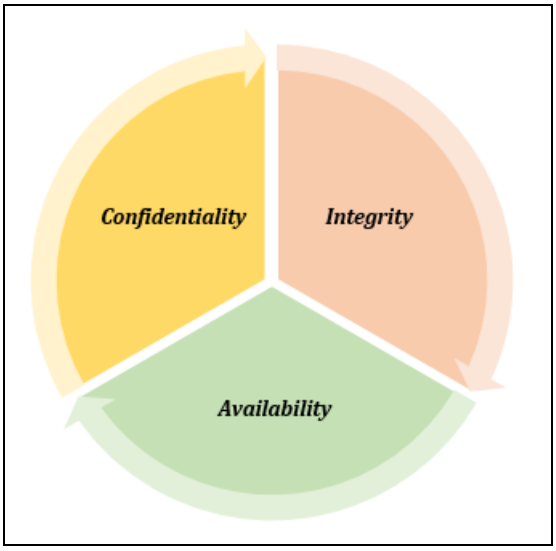

Fig: C.I.A Triad

2. **Integrity:**
   Integrity entails ensuring that your data is reliable and unaltered. Only when your data is genuine, accurate, and trustworthy is its integrity preserved. Integrity is frequently compromised on purpose. For instance, you may have maintained certain information about your car's branding to increase sales, but if it is false, those who are looking into it might conclude that the company is unreliable. An attacker could circumvent an intrusion detection system (IDS), modify file settings to permit unwanted access, or manipulate the system's logs to conceal the attack. Accidental violations of integrity are also possible. Someone might inadvertently type the incorrect code or commit another thoughtless error. You can employ digital certificates, digital signatures, encryption, or hashing to safeguard the integrity of your data.

3. **Availability:**
   Data is frequently worthless unless it is accessible to both the organization's employees and the clients they serve, even if it is kept private and its integrity preserved. This implies that applications, networks, and systems must be operating at the appropriate times and in the appropriate manner. Accessing the data shouldn't take too long, and those who have access to certain information should be able to use it when they need to. Organizations can utilize redundant servers, networks, and applications to guarantee availability.

4. Cybersecurity Threat types:

1. **Spoofing:**
   When a hacker assumes the identity and data of another individual in order to perpetrate fraud, this is known as identity spoofing.

2. **Tampering:**
When information is altered without permission, it is referred to as data tampering.
3. **Repudiation:**
Threats of repudiation occur when a malevolent person conducts a malicious or unlawful action within a system and subsequently denies any involvement in the attack.

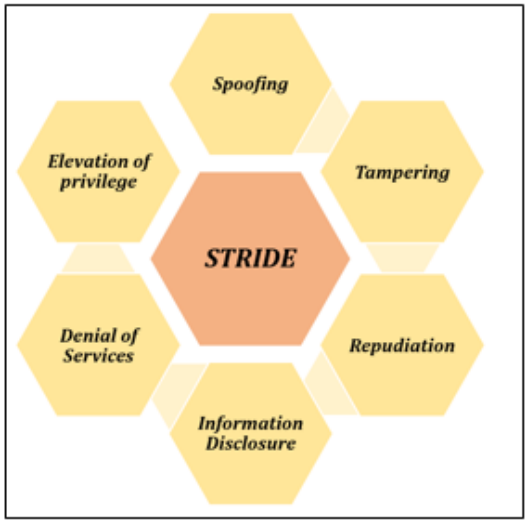

Fig: STRIDE

4. **Information Disclosure:**
Information leaking is another name for information disclosure.
5. **Denial Of Service(DOS):**
Attacks known as denial of service (DoS) prevent a legitimate user from accessing resources that they ought to be able to.
6. **Elevation of Privilege:**
An authorized or unauthorized user in the system can obtain information that they are not permitted to view by elevating their privileges.

5. TARA Analysis of EV powertrain architecture:

1. Detailed Analysis of Architecture Requirements for SDVs
There is main two task sub division.

a. Study of In-Vehicle Architecture: Study of the SDV architecture which involves zonal, domain architectures and which involves HPCs, focusing on its hardware, software, and connectivity layers to understand how various ECUs interact to each other and supporting various vehicle functionalities, application and SDV features.

b. The Cyber-Attack Risks Identification involves performing the Analysis of the In-vehicle architectures which involves zonal/domain controller architectures to discover possible paths that attackers can attack or manipulate, such as CAN/Ethernet communication interfaces, OBD connectors, software updates, and centralized ECUs like domain controllers or HPCs.

2. Based on the criticality prioritization of the vehicle functions and applications: Have to identify and focus on an important vehicle functionalities which are essential for the safety, operation and especially for the user experience, privacy. These functions, such as ADAS, V2X communication, infotainment systems, and powertrain control, are selected for TARA analysis based on their importance and possible impact if harmed.

3. Threat Analysis and Risk Assessment analysis of selected functionalities which will be based on driver's safety and privacy, vehicle important operation, SDV features and powertrain operations, Perform a robust TARA analysis on the selected functionalities by identifying associated assets, evaluating possible threats and risks, and assessing the impact of successful attacks. Evaluating risks by combining possibility and severity, then propose reduction strategies such as encryption algorithms, secure updates, or redundancy to enhance the overall cybersecurity of SDVs

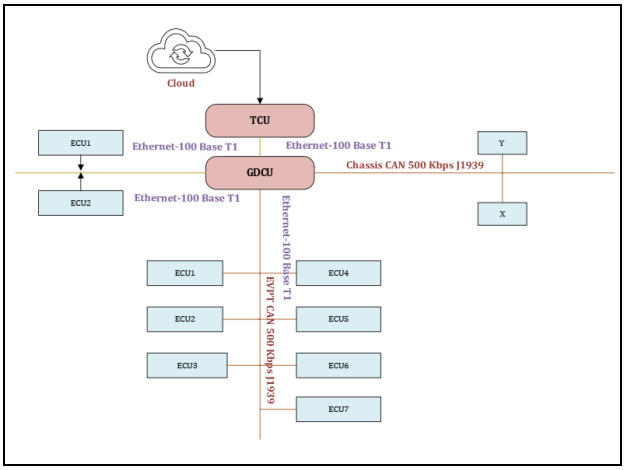

Fig: Sample Vehicle architecture

6. Analysis of Threat Scenario:

a) EV Domain Controller Area Network

Threat Scenario:

1. Potential threat scenarios for an Electric Vehicle (EV) Domain Controller Area Network (CAN bus) considering the cybersecurity properties of confidentiality and asset type spoofing

Confidentiality Breach:

- Scenario: An attacker obtains unauthorized access to the EV Powertrain CAN bus network and interchange confidential data transmitted between different ECUs within the EV's powertrain domain.

- This data could include:
  - Information about battery voltage, current, temperature and state of charge.
  - Details about motor speed, torque and derate info, regeneration info.
  - Signals sent from the brake pedals, accelerator pedals and steering wheel to control acceleration, braking and steering.
  - The data from vehicle control unit such as fuel economy, various fault status, Telltale status etc.
- Impact: Disclosure of this confidential data could have several negative impacts:
  - Compromised battery data could lead to inaccurate estimates of the vehicle's remaining driving range, causing inconvenience to the driver.
  - Tampering with motor controller data could potentially affect vehicle performance or even lead to safety hazards and also safety of the driver.
  - Interchanged control commands could be used by attackers to understand how the vehicle operates and potentially develop opportunities for future attacks.
  - Tampering of fault data can lead to driver's life if any fault telltale will not blink.

Asset Type Spoofing:

- Scenario: A harmful device mimics the identity of an authorized domain controller ECU on the CAN bus. After successfully gains the access of ECU, attacker then inject inaccurate data on the CAN bus or alter existing CAN data. Let's consider two possibilities:
  - A Hacker might mimic a battery sensor and send fake data indicating a good health of battery even if it's defective. This can delay required maintenance of battery unit and also display wrong information of battery parameters.
  - An unauthorized person might mimic a control unit like the motor controller/ vehicle control unit and send inaccurate commands. This can potentially affect vehicle handling or even lead to safety risks.
- Impact: Asset type spoofing can have serious consequences:
  - Degraded Performance: Fake data from a spoofed sensor could lead to the vehicle entering limp home mode or experiencing unexpected behaviour.
  - Safety Hazards: Spoofed control commands could trick the vehicle into performing unsafe actions, which will impact the driver's safety.
  - Reduced System Reliability: The presence of a spoofed device can disturb the communication on the CAN bus, hampering the overall reliability of the vehicle's systems.

Impact Rating for Confidentiality Breach and Asset Type Spoofing on EV CAN Bus

Let's breakdown the potential impact of confidentiality breaches and asset type spoofing on an EV Powertrain network into different categories

Safety:

- Severity: High
- Description: Tampering with confidential CAN communication data between ECUs or mimicking authorized ECUs can lead to the safety-critical activities such as unexpected braking, loss of steering control, or complete system failures. These scenarios can cause a high risk of accidents and injuries.

Finance:

- Severity: Medium
- Description: While financial losses might not be immediate, a security breach could lead to:
  i. Costly repairs: Incorrect data from spoofed sensors might resulting of unnecessary repairs or replacements of components.
  ii. Warranty claims: Malfunctions caused by attacks might not be covered under warranty, because of which financial issues may occur to driver/vehicle owner.
  iii. Recall campaigns: In severe cases, It will impact manufacturer financially s well if vehicle to be returned or any particular ECU to be replaced by manufacturer under some claims.

Operational:

- Severity: High
- Description: Confidentiality breaches and spoofing can disturb the operational capabilities of the EV:
  i. Reduced driving range: Inaccurate range estimation due to due to inaccurate battery data can lead to inconvenience and disturb planned journeys and it will be harmful in case of any emergency.
  ii. Limited functionality: The vehicle goes into limp home mode due to malfunctioning caused by spoofed sensors on the Vehicle CAN network.
  iii. Increased downtime: Understanding of issues and then diagnose them will take some time which will cause vehicle unavailability

Privacy:

- Severity: High
- Description: The privacy impact depends on the specific data altered/tampered:
  i. Limited privacy impact: Interchanged data might only include non-personal information like battery voltage or motor speed.

ii. Moderate privacy impact: In some cases, interchanged data might reveal the driver's location or driving habits, which will eventually hampers driver's privacy.

5. CONCLUSIONS

The creation and upkeep of SDVs that incorporate the TARA methodology promote a more secure and robust automotive ecosystem. It contributes to the protection of vehicle networks and raises public confidence in the security and dependability of cutting-edge automotive systems.

REFERENCES

[1] Teri Lenard; Anastasija Collen; Niels Alexander Nijdam; Meriem Benyahya. A Systematic Review of Threat Analysis and Risk Assessment Methodologies for Connected and Automated Vehicles ARES 2023, August 29–September 01, 2023, Benevento, Italy

[2] Jherrod Thomas. HATARA: A Novel Approach by Fusion of HARA and TARA for System Safety and Security Analysis, February, 2024

[3] Loskin, Ilona. TARA+AD: Threat Analysis and Risk Assessment for Automated Driving – Cybersecurity of Road Vehicles, 2023

[4] Meriem Benyahya, Anastasija Collen, Sotiria Kechagia, and Niels Alexander Nij- dam. 2022. Automated city shuttles: Mapping the key challenges in cybersecurity, privacy and standards to future developments. Computers & Security 122 (11 2022), 102904

[5] ISO/SAE 21434:2021Road vehicles — Cybersecurity engineering

[6] Taxonomy and Definitions for Terms Related to Driving Automation Systems for OnRoad Motor Vehicles J3016_202104

- https://www.fortinet.com/resources/cyberglossary/cia-triad