Contents

[Introduction 2](#_Toc179732397)

[Functional Summary 3](#_Toc179732398)

[Assumptions 5](#_Toc179732399)

[Functional Requirements 6](#_Toc179732400)

# Introduction

The goal of my project is to investigate mileage tampering and create a solution on how it can be prevented or minimised.   
  
The recent increase of complexity within vehicle electronics and systems has led to new opportunities for vehicle exploitation. One of the most popular forms of automotive fraud in the automotive market is odometer tampering also known as mileage fraud. Odometer tampering is the illegal practice of altering the mileage displayed on a vehicle’s odometer which results in the vehicle displaying a lower mileage than the vehicle has actually travelled.   
  
Mileage fraud effects many in the automotive space such as buyers in the second-hand market, vehicle manufactures and vehicle leasing companies. Mileage fraud can be used against vehicle manufacturers who have a warranty in place for their vehicles which includes a maximum mileage limit before the vehicle is out of warranty. This is a very relevant topic as more manufactures begin to sell electric cars that come with a warranty cover on the battery itself, such as Hyundai Ireland who grant warranty on their batteries for 8 years or up to 160,000 kms. Similarly with leased vehicles they will come with an annual mileage limit which typically falls between 8,000 and 15,000 kilometres and mileage fraud can be used to exceed this limit to avoid addiction charges.  
  
To combat the issues of mileage fraud there has been several regulations been put in place at both national and international levels. In the European Union one of the key directive addressing the issue is [EU Directive 2014/45/EU](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0045#:~:text=(25),by%20the%20Commission.). This Directive mandates that Member States are required to conduct periodic vehicle inspections along with recording the odometer readings at the time of the inspection. This solution is not a 100% fix to the problem and includes some gaps

* **Cross Border Sales:** One major problem with this solution is that mileage records are typically only accessible with a single Member State, this meaning once a vehicle is exported to a different state the records for that vehicle are often not transferred.
* **Technological Limitations:** With the current regulation in place it heavily relies on manual inspections which is not a sufficient solution to combat mileage blockers as they are and active device fitted to the vehicle which blocks mileage or blocks a percentage of mileage from being recorded.

The aim for this project is to address the problems with mileage tampering and to develop a solution to include a large amount of vehicle manufactures. I will attempt this by using Vector standards along with using Vector tools to develop my solution along with using Vector CANoe to demonstrate the solution to prevent mileage tampering.

# Functional Summary

What I plan to do to accomplish this project idea includes the following but that may be subject to change:

* **Research Impact of mileage blocker on industry and second-hand market.** 
  + Study how odometer fraud affects the used car market. Research the financial losses, consumer trust issues, and regulatory concerns.
  + Explore legal cases or studies documenting the extent of mileage tampering fraud.
* **Research the estimated usage of mileage blockers.**
  + Research the prevalence of mileage tampering devices (like blockers) across different regions or industries.
  + Explore how often these devices are used and in which types of vehicles e.g. high-value cars, commercial vehicles.
* Understand How Mileage Blockers Work.
  + **Hardware Research**: Investigate how mileage blockers interact with a vehicle’s systems e.g. CAN bus, ECUs.
  + Learn about the software protocols that can interfere with odometer readings.
  + **Vehicle Systems**: CAN bus communication, and ECU architecture.
* Research the software tools what I may need to research and develop this project.
  + Vector tools.
  + Cloud tools.
  + Database tools.
* Development:
  + **Mileage Tracking:** The system will continuously monitor and display accurate odometer readings using data collected from the vehicle’s ECUs.
  + **Tamper Detection:** The system will detect any attempt to modify or block the odometer data. It will log all tampering attempts and store these logs securely.
  + **Secure Data Storage:** Odometer data will be stored both onboard and offboard, ensuring that the mileage data is tamper proof and can be verified at any time.
  + **Data Integrity Verification:** The system will provide mechanisms to verify the authenticity of odometer data. In case of a discrepancy, the offboard stored data will serve as a reference to verify legitimate mileage.
  + **Reporting of Tampering Attempts:** Any tampering or inconsistency in mileage data will trigger alerts and generate logs that can be accessed for reporting.

# Assumptions

* **Vehicle Compatibility:** This project assumes that the vehicle models targeted for testing have standardised communication protocols such as OBD-II and CAN bus, which will allow for easy access to odometer data.
* **Regulatory Compliance:** It is assumed that the system will be designed within the bounds of current automotive regulations regarding data logging and tamper protection.
* **Network Connectivity:** The offboard storage system assumes stable internet connectivity for transmitting odometer data securely.
* **Tamper Detection Mechanisms:** It is assumed that mileage tampering can be detected based on either change in the communication patterns of the vehicle’s ECUs or the failure of the system to log mileage data at regular intervals.
* **Onboard Storage Capacity:** It is assumed that the onboard storage capacity in the vehicle’s hardware is sufficient to store encrypted odometer data locally.

# Functional Requirements

* **Data Management:** 
  + The system shall read odometer data from the vehicle's ECU periodically.
  + The system shall store odometer data onboard in encrypted form to prevent unauthorized modifications.
  + The system shall transmit odometer data to offboard storage after each vehicle shutdown or at regular intervals.
* **Tamper Detection:** 
  + The system shall detect any attempt to manipulate odometer readings or disrupt the communication flow between the ECU and the odometer.
  + The system shall log all tampering attempts in a secure and non-tampering format.
  + The system shall detect any tampering attempts and log such attempts via onboard diagnostics and offboard storage.
* **Data Integrity:**
  + The system shall use encryption and cryptographic signatures to verify the integrity of odometer data stored onboard and offboard.
  + The system shall compare onboard odometer data with offboard stored data to verify its authenticity upon each vehicle startup.
* **Security:**
  + The system shall use industry standard encryption algorithms for storing data.
  + The system shall employ user authentication to access mileage data logs e.g. data is only accessible to main dealers.