Low-Level Design Document for IDS Components in Automotive

|  |  |  |
| --- | --- | --- |
| Version | Date | Description |
| 1.0 | 19/03/2025 | Initial draft |
| 1.1 | 25/03/2025 | Added detailed component design |
| 1.2 | 02/04/2025 | Updated sequence diagrams and references |

# Introduction

The Intrusion Detection System (IDS) in automotive applications plays a crucial role in ensuring the cyber-security of vehicular networks. This document outlines the low-level design of IDS components, including detailed sequence diagrams and references to relevant standards and literature.

# System Overview

The IDS architecture for automotive systems is designed to monitor, detect, and respond to potential security threats within the vehicle's network. The system comprises several components, including sensors, data processors, and response mechanisms.

## Components

* Sensors: These devices capture data from various parts of the vehicle network, including CAN bus traffic, ECU status, and more.
* Data Processors: These units analyze the collected data to identify potential intrusions or anomalies using predefined algorithms and machine learning models.
* Response Mechanisms: Upon detection of a threat, these mechanisms initiate actions such as alerting the driver, logging the event, or taking corrective measures.

# Detailed Component Design

## Sensors

The sensors are strategically placed across the vehicle's network to ensure comprehensive coverage. They are responsible for real-time data collection and forwarding the data to the data processors.

## Data Processors

The data processors are equipped with advanced algorithms for threat detection. They utilize signature-based detection, anomaly-based detection, and machine learning techniques to identify potential threats.

# Sequence Diagrams

Below are the sequence diagrams illustrating the interaction between the IDS components under different scenarios.

## Normal Operation

## Threat Detection and Response

# References

* ISO/SAE 21434: "Road vehicles – Cybersecurity engineering"
* NHTSA Cybersecurity Best Practices for Modern Vehicles
* Relevant articles and research papers on automotive IDS

# Conclusion

This document provides a comprehensive low-level design for the IDS components in automotive systems. The sequence diagrams illustrate the interaction between components during normal operation and threat detection scenarios. By adhering to the standards and best practices referenced, we can ensure a robust and reliable IDS for automotive applications.