CAN DEMONSTRATOR WITH INTRUSION DETECTION SYSTEM

Dipl.-Ing. (FH) Heiko Polster

Prof. Dr. rer. nat. Dirk Labudde

Lernlabor
Cybersicherheit

HOCHSCHULE MITTWEIDA
University of Applied Sciences

Fraunhofer
ACADEMY

offen

Fraunhofer
ACADEMY

DEVELOPMENT OF THE CAN BUS DEMONSTRATOR

Introduction

- This work deals with an environment to reproduce and test attacks on Controller Area Network (CAN) bus systems

- using the Vector CANoe tool and a CAN bus demonstrator

- It describes how a CAN bus demonstrator is structured

- It shows how the demonstrator hardware can be controlled using the Vector CANoe tool

- In addition, an implementation of an Intrusion Detection System (IDS) is shown

- with IDS CAN bus attacks generated in the CANoe tool can be analyzed

- The CAN bus demonstrator offers a useful alternative for performing and analyzing hacking attacks on automotive bus systems

Fraunhofer
ACADEMY

DEVELOPMENT OF THE CAN BUS DEMONSTRATOR

Components

- mechanical basis of the CAN bus demonstrator: Joy-It's Robot Car Kit 4WD

- Design a CAN bus system, which includes:

  - central gateway

  - motor control unit

  - control unit for lighting

  - control unit for other electronic (distance measurement, battery monitoring and horn)

Fraunhofer
ACADEMY
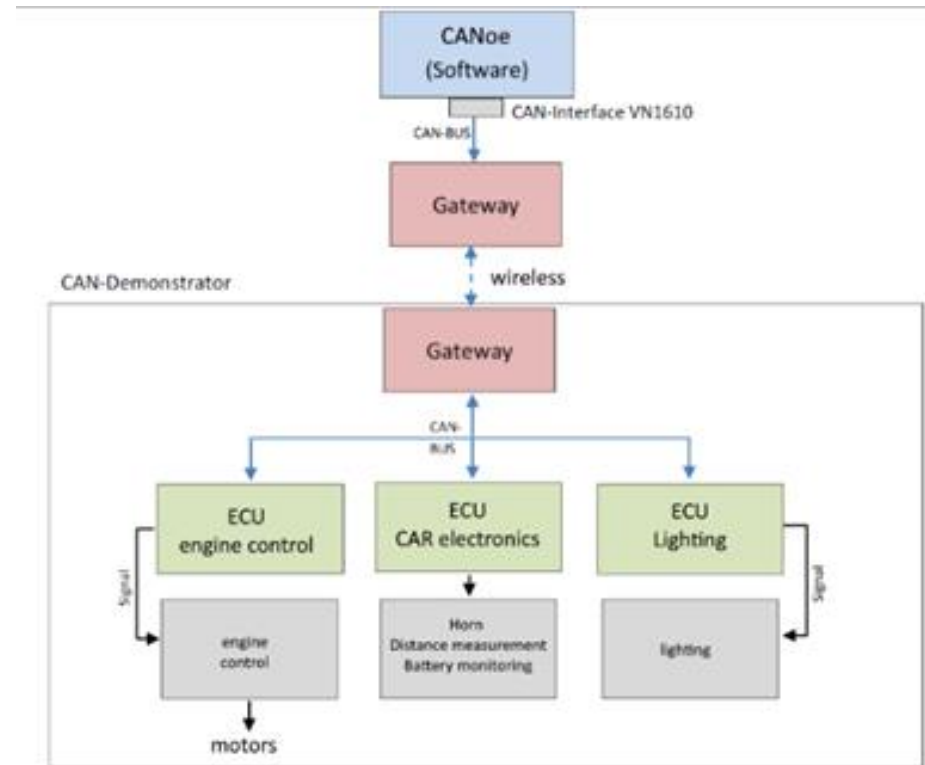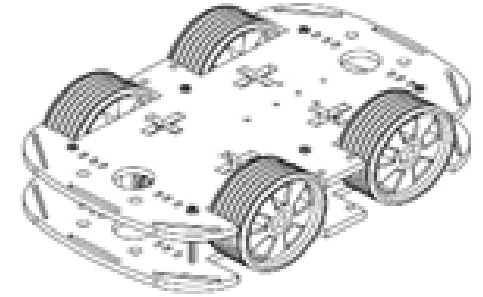
DEVELOPMENT OF THE CAN BUS DEMONSTRATOR

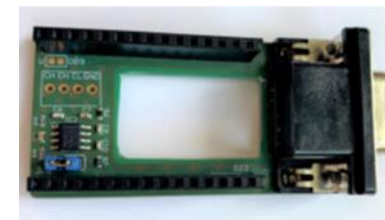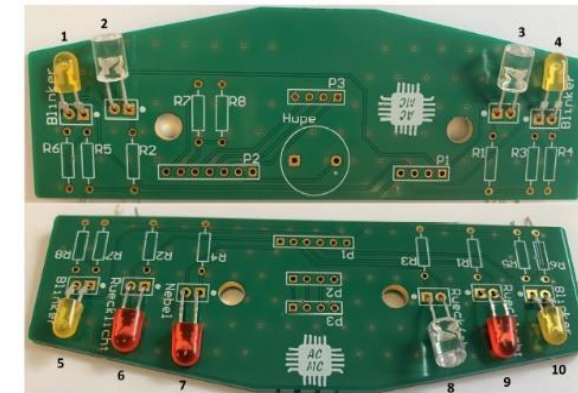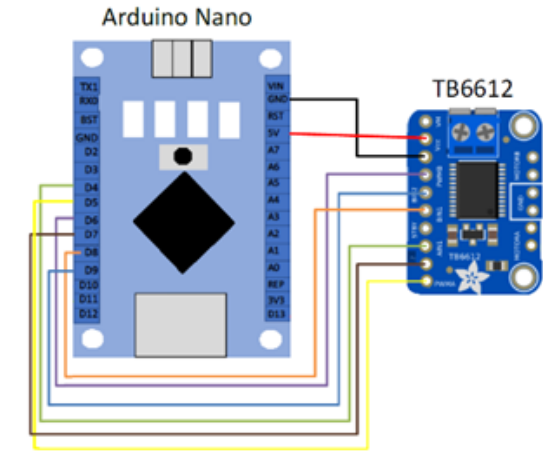## Electronic Control Units (ECU)

- **Motor ECU**
  - Arduino Nano
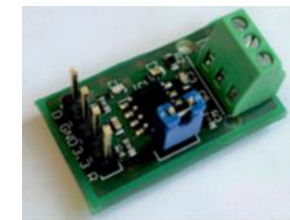 - engine driver TB6612 from Adafruit

- **Car ECU**
  - 10 LEDs
  - Horn → SUMMER AL-60P12
  - Distance measurement → sensors HC-SR04

- **Gateway ECU**
  - NodeMCU-ESP32
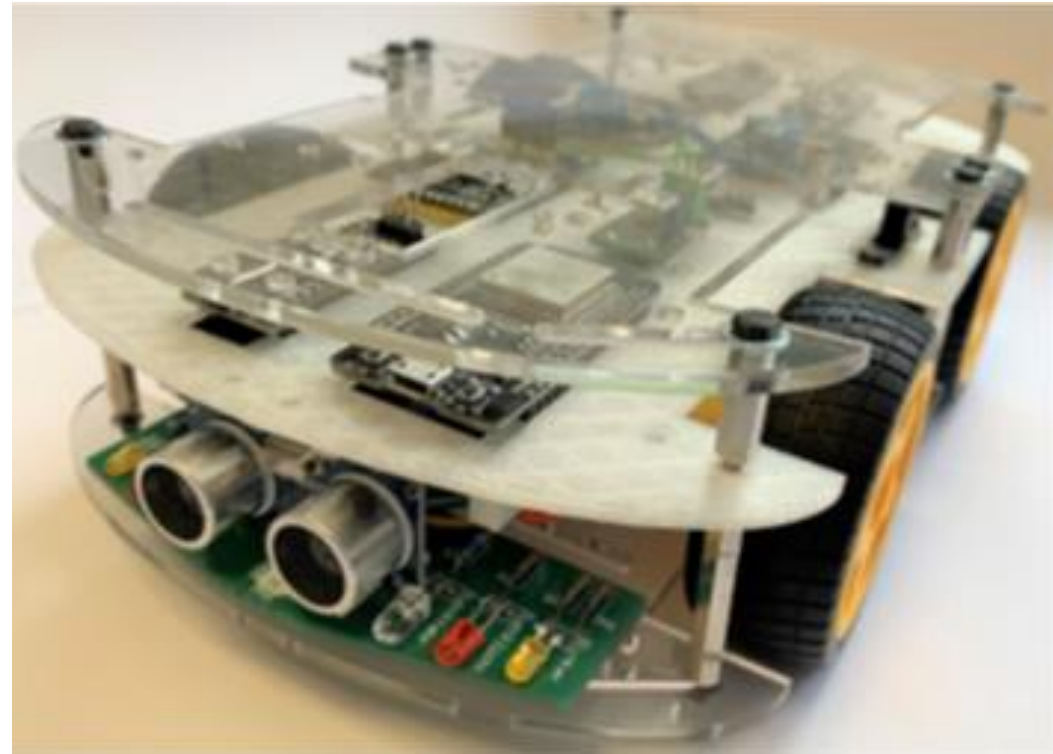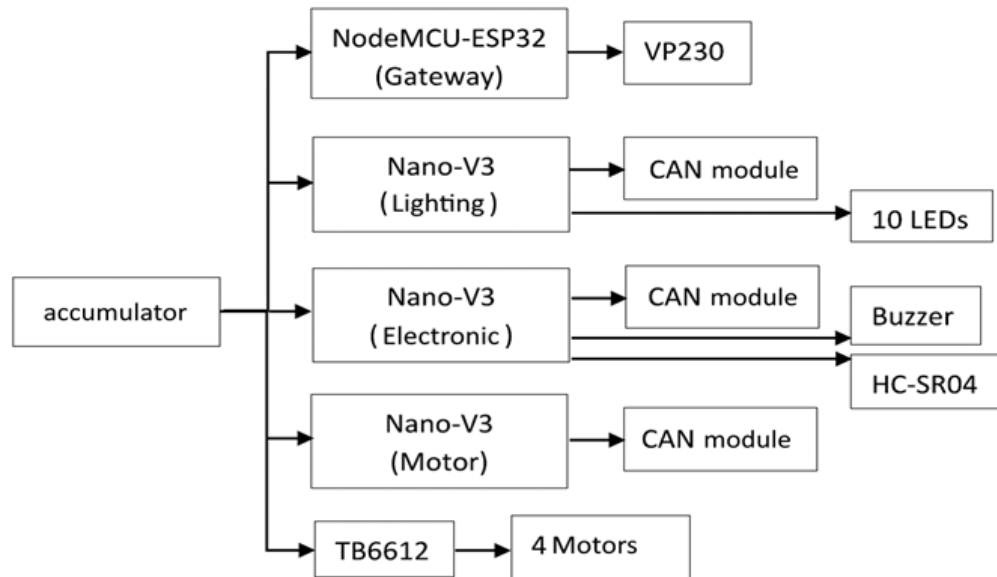 - high-speed CAN transceiver VP230

Fraunhofer
ACADEMY

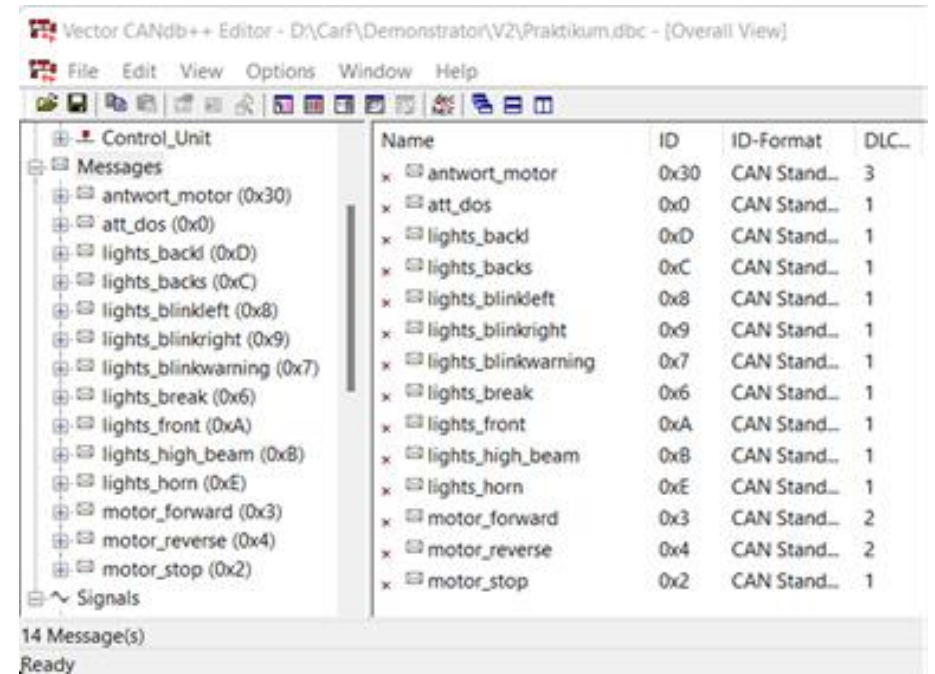# DEVELOPMENT OF THE CAN BUS DEMONSTRATOR

Final assembly of the hardware

DEVELOPMENT OF THE CAN BUS DEMONSTRATOR

Control of the CAN Bus Demonstrator

- CANoe of the company Vector is used

- hardware interface: Vector VN1610

- CANoe allows virtual ECUs to be tested in real CAN bus environments

- Program virtual ECUs with Communication Access Programming Language (CAPL)

- send and receive CAN messages

- environment control with panel

Fraunhofer
ACADEMY

DEVELOPMENT OF THE CAN BUS DEMONSTRATOR

Implementation of the Intrusion Detection System

- Bresch and Salman developed IDS integrated into CANoe

  https://publications.lib.chalmers.se/records/fulltext/251871/251871.pdf

  - message cycle time analysis

  - plausibility analysis of messages

- integration of this IDS in the demonstrator

- Realisation of the following attacks in CANoe:

  - Denial of Service (DoS)

  - creeping increase and decrease of speed

  - maximum and minimum speed

DEVELOPMENT OF THE CAN BUS DEMONSTRATOR
Conclusion

- a real CAN bus demonstrator was created

- Realisation of cyber attacks on CAN bus systems of vehicles with the help of the CANoe environment

- realization of a rule-based intrusion detection system

- tested by students and received positive feedback throughout

- Future:
  - Implementation of additional functionalities in the demonstrator
  - Realization of further attack vectors

Fraunhofer
ACADEMY

Thank you for your attention.

offen

Fraunhofer

ACADEMY