NORWICH UNIVERSITY

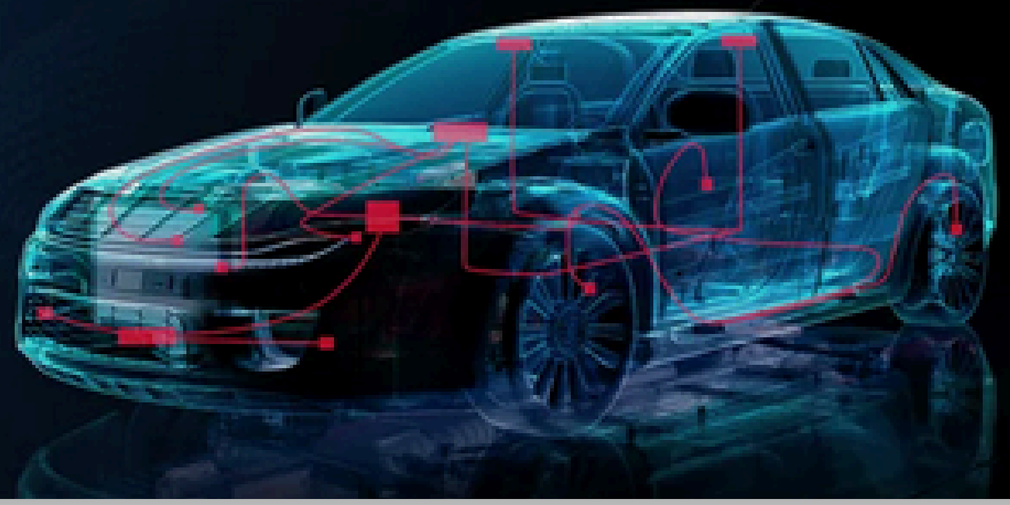
https://github.com/simantkhadka

CAPSTONE PROJECT

CAN-BUS DIAGONOSTIC TOOL

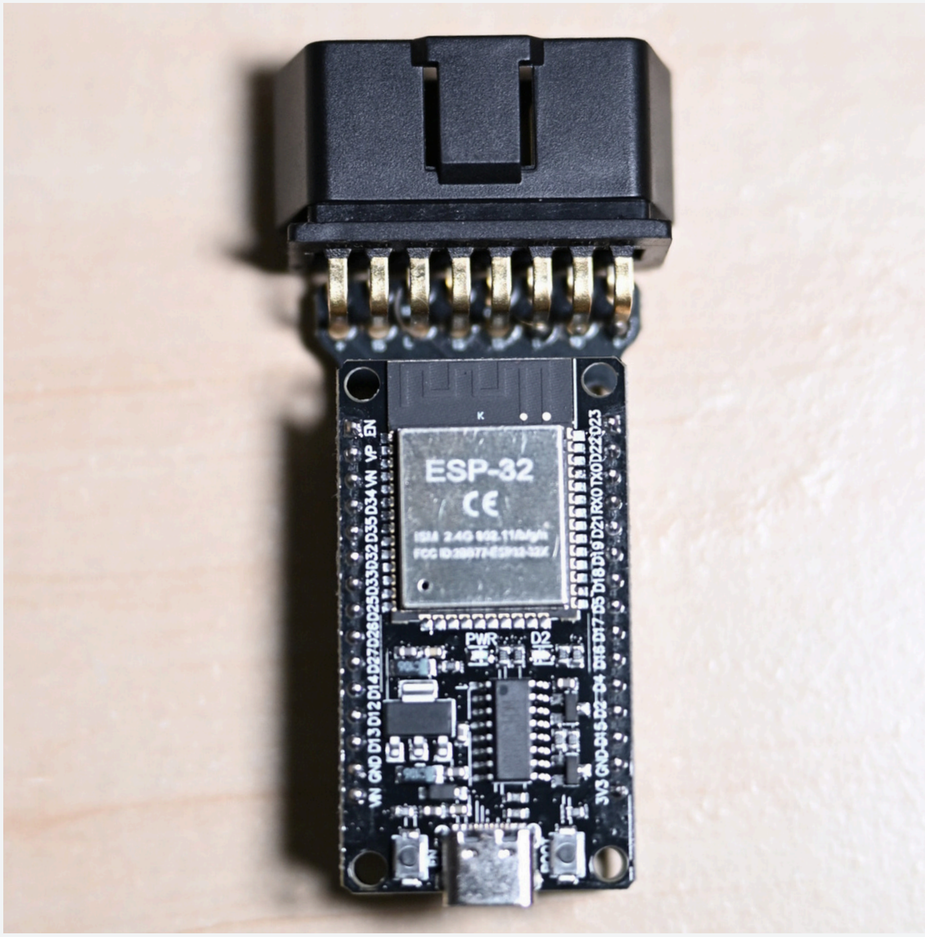
SIMANT KHADKA, PROF. JEREMY HANSEN

CONTENT



OVERVIEW

This capstone project involves the design and development of a compact, open-source CAN Bus diagnostic tool powered by the ESP32 microcontroller. Connecting through a vehicle’s OBD-II port, the device interfaces with the Controller Area Network (CAN) bus to stream real-time operational data, sniff and log CAN messages, and transmit controlled test frames to assess system behavior. These capabilities support detailed diagnostics, reverse engineering, and performance monitoring across multiple vehicle systems. Featuring USB, WIFI and Bluetooth connectivity, the tool provides flexible integration with laptops, mobile devices, and diagnostic platforms, while its small form factor ensures portability and straightforward use on both modern and older vehicles.



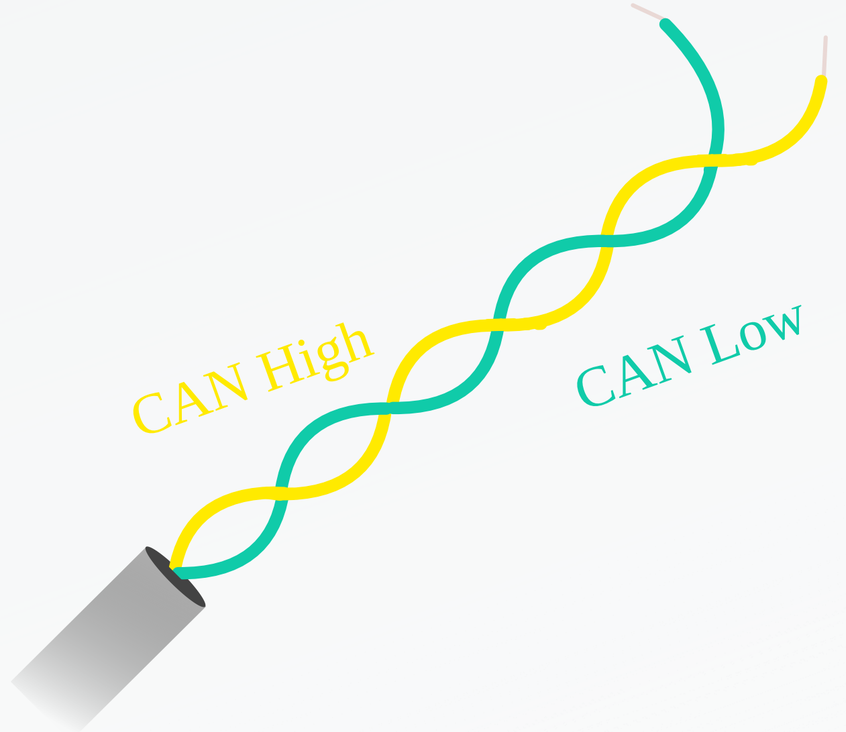
CAR COMMUNICATIONS 101

The Controller Area Network Bus aka the CAN Bus

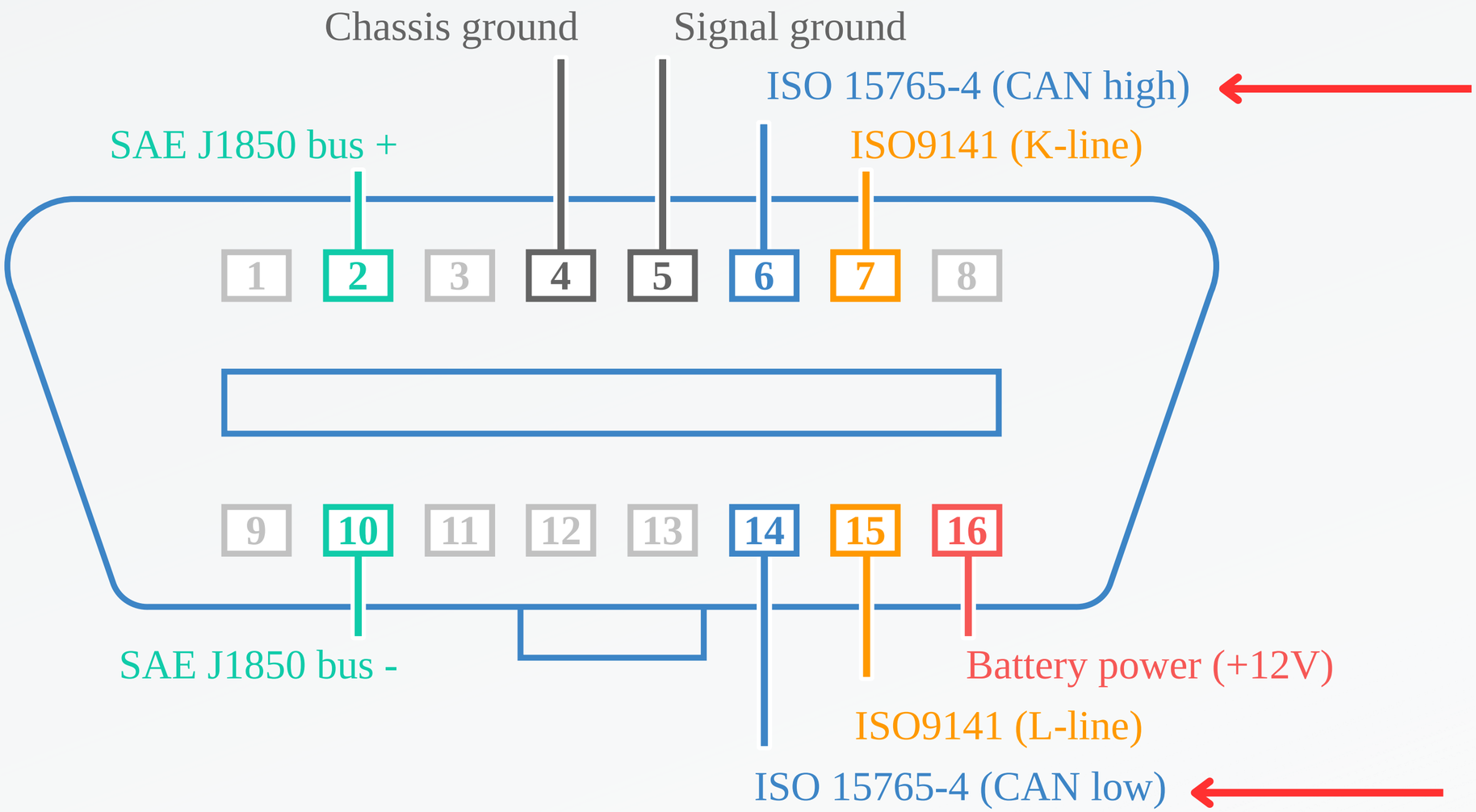
The CAN Bus is a communication standard that excels at long range and robust wired data transmission. It is a 2-wire protocol making it simple and easy to implement.

Without the CAN Bus each sensor/device/component of the vehicle would need its own wiring directly to the ECU. The CAN Bus greatly reduces this by utilizing daisy chaining of the two wires, thus allowing 2 wires to connect every device to the ECU.

These 2 wires are referred to as CAN High and CAN Low. They actually transmit the exact same information at the exact same time, but CAN Low is inverted. This creates a very redundant system with few fail points. -Differential Signaling



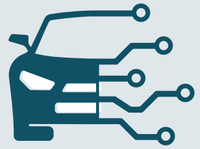
OBD-II CONNECTOR PINOUTS



KEY FEATURES

DIAGNOSTICS

Performs comprehensive analysis of vehicle systems, retrieving fault codes, and providing detailed insights into component performance for accurate troubleshooting.



SNIFFING

Captures and monitors raw CAN Bus traffic in real time, enabling detection of messages, anomalies, and hidden signals for in-depth system understanding.

CONNECTIVITY

Offers seamless communication via USB, WIFI and Bluetooth, ensuring flexible integration with various platforms and devices without complex setup.

CONVENIENCE

Designed for straightforward operation with minimal configuration, making advanced diagnostics accessible to users of all technical backgrounds.

CONTRIBUTION

- **Hardware Integration** – Adapted the firmware from the original ESP32RET hardware to work with the Custom Shield and ESP-32, including correct CAN bus pin mapping, LED indicators, and bus configuration

- **Protocol & Communication Fixes** – Corrected an incorrect ECU address in the CAN communication logic, ensuring proper requests and accurate diagnostic data from the vehicle.

- **Bluetooth Reliability** – Fixed a Bluetooth connection error in the ELM327 emulator, enabling stable pairing and consistent data exchange with mobile diagnostic apps.

- **Feature Optimization** – Retained essential capabilities such as CAN bus sniffing/logging, Bluetooth ELM327 emulation, and Wi-Fi connectivity while removing unused features for stability and simplicity.

- **User Configuration** – Enabled persistent storage for Wi-Fi credentials and Bluetooth device name, making the tool easy to set up and customize for different users or vehicles.

- **Testing & Validation** – Verified hardware and firmware operation together, confirming reliable CAN communication, Bluetooth stability, and Wi-Fi-based data streaming.

CHALLENGES

Obstacles Encountered and Lessons Learned

01 **Bench-Testing Incident**

While the diagnostic tool functioned as intended, an error during the CAN Bus sniffing and bench-testing of the instrument cluster created a major setback. I had wired the ignition pin directly without using a dedicated switch, causing both bench circuits to be tied together. This resulted in damage to the instrument cluster, preventing further sniffing and significantly impacting the reverse-engineering process.

02 **Modern Vehicle Gateway Complexity**

Many modern vehicles use multiple CAN gateways that separate data between systems such as the engine, body controls, and infotainment. To access all available data, you must connect to several different CAN lines located in various parts of the vehicle. This adds time, requires partial disassembly, and can risk damaging components or voiding the car’s warranty. In comparison, older vehicles usually have a single CAN gateway, so connecting through the OBD port provides complete network access without extra steps.

TAKEAWAY

- Learned the entire process from scratch — from understanding CAN Bus protocols to implementing hardware and firmware solutions.
- Gained in-depth knowledge of CAN Bus architecture, including real-time data acquisition, multi-gateway complexities, and reverse engineering techniques.
- Developed skills in embedded firmware design, hardware integration, and efficient data parsing for live diagnostics.
- Overcame hardware failures and adapted to modern vehicle network constraints through research and problem-solving.
- Understood that real-world engineering demands persistence, adaptation, and continuous implementation to turn ideas into results.
- Delivered a functional CAN Bus diagnostic tool with USB, WIFI and Bluetooth connectivity for versatile diagnostic and research applications.

THANK YOU!
QUESTIONS?