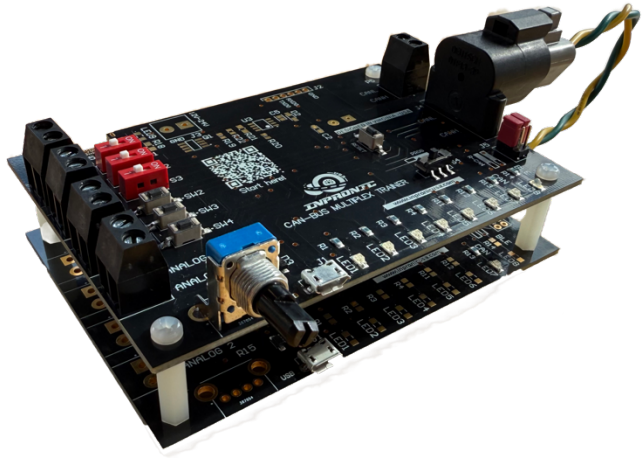
CAN-BUS

A Hands-On Approach to Automotive and Industrial Networks



INPRONIC USA LLC

sales@inpronicusa.com

www.inpronicusa.com

ISBN 979-8-89901-487-1

DEDICATION

To Claudia Vallejo S.,

Your unwavering support, patience, and encouragement have been the foundation of this journey. Through every challenge and late-night endeavor, your belief in me has been a source of strength and inspiration.

This book is dedicated to you—not only for your love and understanding but for the countless ways you have stood beside me, making every achievement more meaningful.

With deepest gratitude love and admiration,

SANTY

TABLE OF CONTENTS

Preface

The modern era of vehicle communication, industrial automation, and marine navigation has been shaped by one fundamental advancement: the Controller Area Network (CAN-BUS) protocol. Originally developed to streamline automotive electronics, CAN-BUS has evolved into a versatile and widely adopted standard across multiple industries, ensuring robust, efficient, and scalable data exchange between electronic control units (ECUs).

This book provides a comprehensive exploration of CAN-BUS and its primary protocols—OBD-II, J1939, CAN-Open, and NMEA 2000—offering both theoretical knowledge and practical application. Designed for engineers, technicians, developers, and industry professionals, this text serves as a definitive guide to understanding and implementing CAN-BUS communication systems.

What distinguishes this book is its applied approach. Beyond conceptual understanding, it introduces hands-on simulations using the CAN-BUS Multiplex Trainer, a powerful tool for monitoring, analyzing, and simulating CAN network behavior. Each chapter delves into:

Fundamental principles of CAN-BUS architecture, arbitration, and error handling.

Protocol-specific communication methods, including message structures, PGNs, PIDs, and addressing schemes.

Practical simulations and analysis using the CAN-BUS Trainer to replicate real-world communication scenarios.

Industry case studies, illustrating the application of CAN-BUS in vehicle diagnostics, industrial control systems, and marine electronics.

By the conclusion of this book, readers will not only possess an in-depth understanding of CAN-BUS but will also be equipped with the practical skills necessary to develop, troubleshoot, and optimize CAN communication networks.

As industries continue to embrace automation, data integration, and intelligent diagnostics, the relevance of CAN-BUS will only grow. Whether for professional development, research, or system implementation, this book provides the essential foundation to master CAN-BUS technology and its applications.

Santiago Corrales V.

C.E.O. INPRONIC USA

CHAPTER 1

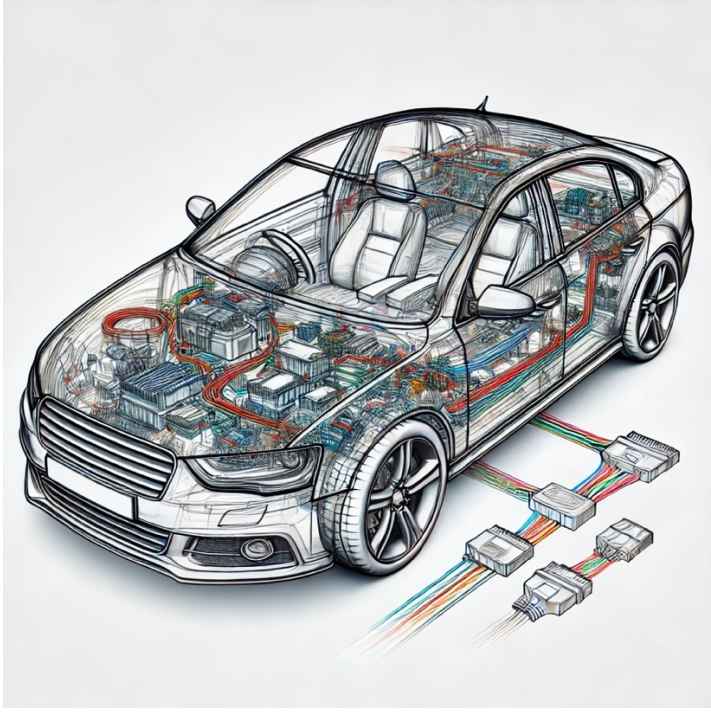
Introduction to CAN-BUS

1. Understanding the CAN-BUS Network

The Controller Area Network (CAN) is an advanced and highly efficient communication protocol that has revolutionized how electronic devices communicate and interact within complex systems. Originally developed by Bosch in the 1980s, the CAN protocol was designed to simplify the growing complexity of automotive wiring by reducing the number of wires required for communication between various electronic control units (ECUs). It provides a reliable, robust, and efficient means of data exchange between multiple devices, known as nodes, within a network.

The CAN protocol uses a two-wire system, known as CAN-High (CAN-H) and CAN-Low (CAN-L), to facilitate differential communication, ensuring high noise immunity and data integrity. Over the decades, CAN technology has evolved beyond its automotive origins and has become a standard protocol in industrial automation, marine applications, medical

equipment, and aerospace systems. Its scalability, reliability, and real-time communication capabilities make CAN a fundamental technology in modern electronic and automation systems.



1.1 The Origin and Evolution of CAN

Before the introduction of CAN, automotive systems relied on complex and bulky wiring harnesses to connect individual components. As vehicles became more sophisticated, with an increasing number of electronic control units (ECUs), the traditional point-to-point wiring approach became unsustainable. This led to the development of the CAN protocol, which

significantly reduced wiring complexity while improving reliability and scalability.

CAN was initially designed to handle the demanding requirements of automotive applications, such as real-time data exchange and robust error handling. It has since evolved into a versatile communication standard used in protocols like J1939 (heavy-duty vehicles), CAN-open (industrial automation), and NMEA 2000 (marine electronics). These adaptations demonstrate the flexibility of CAN in addressing diverse industry needs.

1.2 How CAN-BUS Works

The CAN-BUS is a multi-master, message-oriented protocol. Unlike traditional networks, where a central controller manages communication, CAN allows any node to transmit data whenever the bus is free. This decentralized architecture ensures high levels of reliability and fault tolerance.

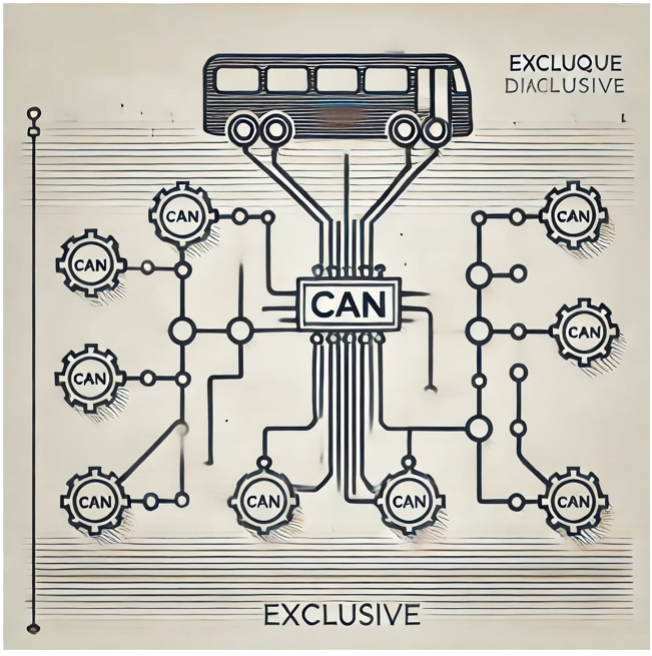
Each message transmitted on the CAN bus contains:

- ***Identifier:*** A unique value that determines the priority of the message.

- ***Data Field:*** The actual information being transmitted, which can be up to 8 bytes in standard CAN.

- ***Control and Error Fields:*** Additional bits used for arbitration, error checking, and acknowledgment.

Messages are broadcast to all nodes on the network, and each node decides whether to process the message based on its identifier. This approach simplifies communication and ensures real-time data exchange, even in complex systems.



1.3 Physical Characteristics of the CAN-BUS

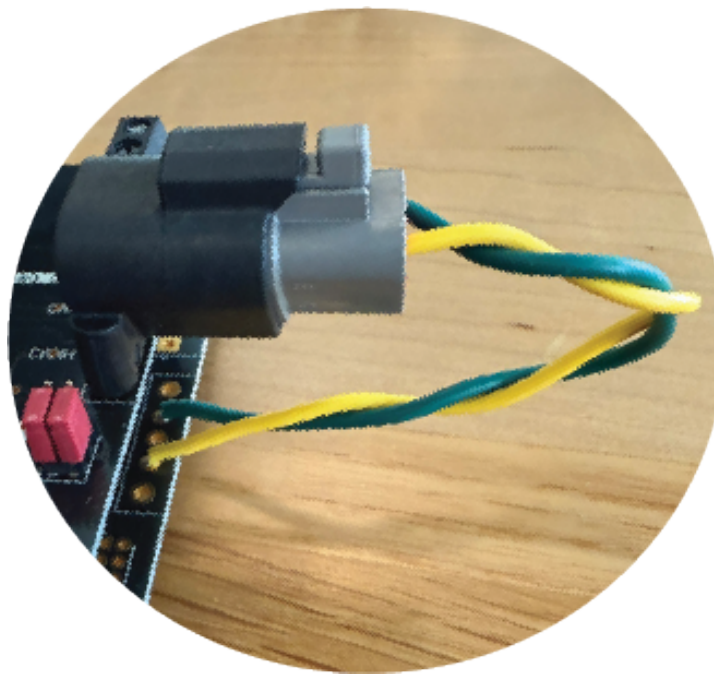
The physical layer of the CAN-BUS typically consists of two twisted wires: CAN High and CAN Low. These wires form a

differential pair, meaning the signal on one wire is the inverse of the other. This design provides several advantages:

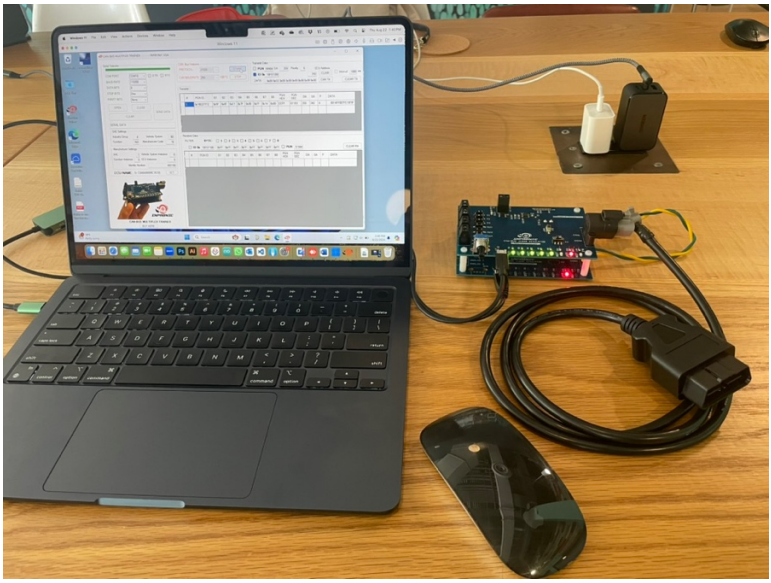
- ***Noise Immunity:*** Differential signaling cancels out electromagnetic interference, ensuring reliable communication in electrically noisy environments.

- ***Fault Tolerance:*** The network can continue to operate even if one of the wires is damaged.

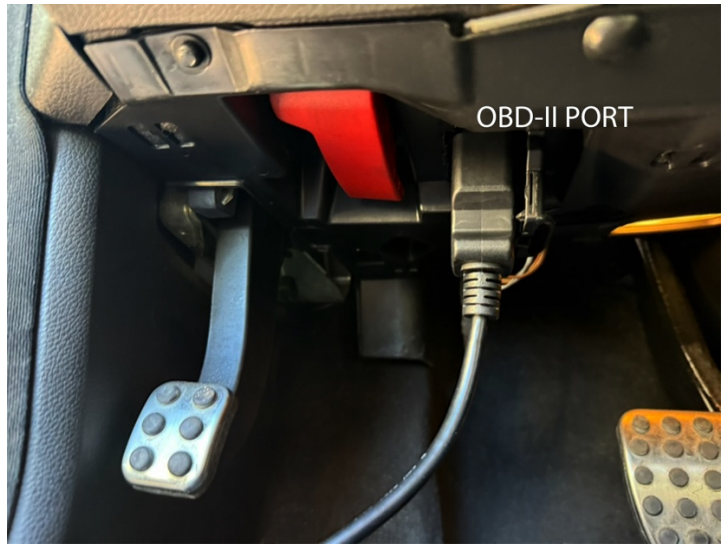
- ***Scalability:*** The twisted-pair configuration allows long cable runs and supports the addition of new nodes without significant reconfiguration.



Hacking my CAR using a Trainer and OBD-II CAN Data



In this experiment, I'll demonstrate how to use the CAN-BUS Multiplex Trainer to send custom messages through the OBD-II port to control vehicle functions—specifically, locking the doors. By utilizing the Trainer Tab in the software and configuring one of the control buttons, I can transmit the exact CAN message that triggers the door lock. This process showcases how CAN data can be used to interact with and control vehicle systems, providing insights into how ECUs respond to specific commands.

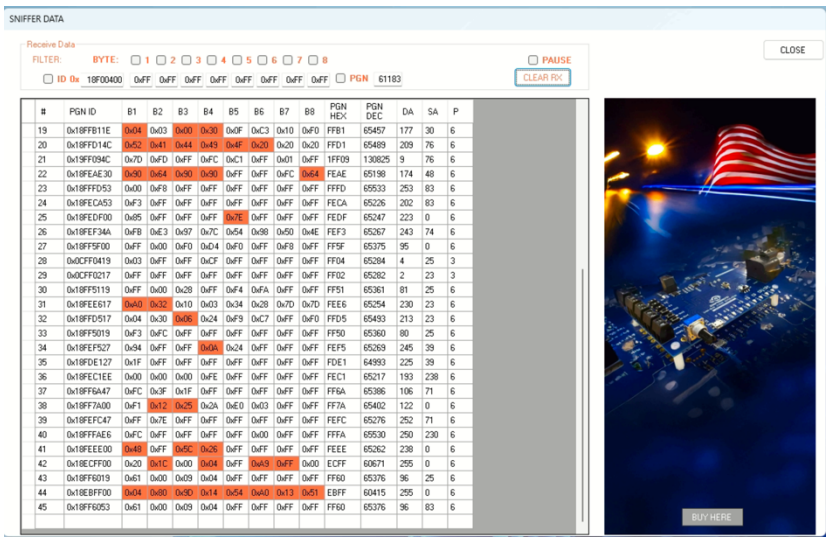


I’ll connect the trainer to the OBD-II port into my vehicle, I use this cable to connect the Trainer into a CANH, and CANL terminals.

Step 2: Identify the Turn Signal Messages

Activate the Turn Signals: Toggle the left and right turn indicators in the vehicle.

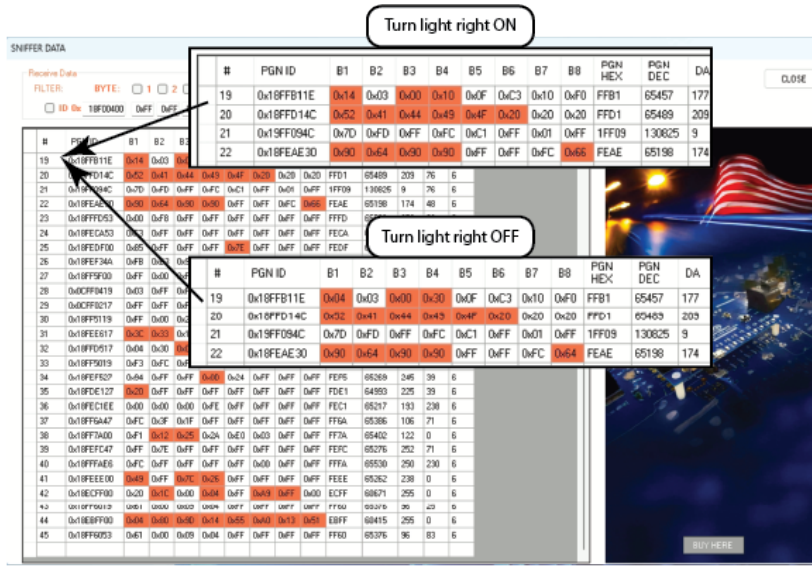
Look for Changing Data Rows: The Sniffer Tool will highlight the rows where data changes when the indicators are activated.



In this case, when the turn signal lever is activated, row **19** will change dynamically, and it will be highlighted in **orange**. This visual indication helps identify the specific row associated with the turn signal function, allowing us to focus on the exact CAN message responsible for controlling the lights.

Analyze the Data Bytes:

Look for a specific byte change that corresponds to left or right signals,



In this case:

Right Turn Signal ON: Byte 1 changes to 0x14

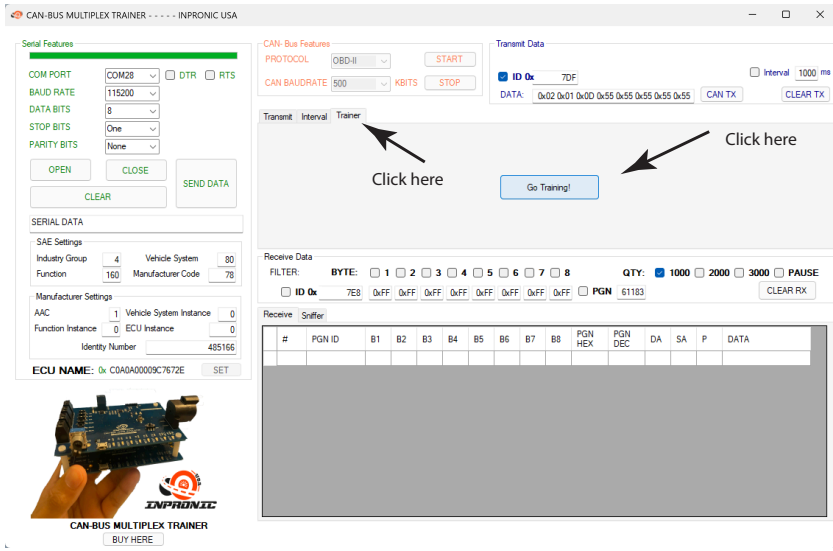
Right Turn Signal OFF: Byte 1 changes to 0x04

Hacking my TRUCK using a Trainer and J1939 CAN Data

The modern truck is more than just an engine and wheels it's a rolling network of electronic control units (ECUs) communicating over the J1939 CAN bus. By tapping into this data stream with a CAN-BUS Trainer, I can decode, manipulate, and even control key vehicle functions in real time. From monitoring sensor values to intercepting and modifying messages like turn signals or engine parameters, this journey into J1939 reveals the immense power of CAN data and the risks and

opportunities it presents for diagnostics, customization, and security.

Connect the upper board to the computer and navigate to the Training Tab within the software to begin configuring and sending CAN messages for simulation and analysis.



Select TX-SW4 to transmit the data, simulating the action of moving the lever to activate the **right turn signal**. This ensures the system recognizes the command as if the turn signal lever were physically engaged.

world scenario. By using the Trainer, you can refine your design, troubleshoot potential issues, and ensure optimal performance without delays, enabling a smooth transition from simulation to actual implementation.


ENCENDIDO DE VEHÍCULO

system is functioning correctly. This confirms that the data is being transmitted accurately, processed without errors, and properly reflected on the display, ensuring seamless integration and validation of the seat belt monitoring system.