Automotive Networks

NOTHINGFACE <alpha@area49.net>

$Date: 2004/07/08 23:20:57 $

Abstract

This presentation provides an introduction to the electronic networks present on late model automobiles. These networks will be described loosely following the OSI model of networking. Common uses of these networks will be presented, and the privacy implications of some uses will be questioned. The presentation will conclude with an introduction to OpenOtto, a free software and hardware project implementing the network protocols previously described.

Overview

- About the speaker
- Why should I care?
- Background on automotive electronics
- OBD2
  - Common usage
  - Physical and data link
  - Diagnostic modes
  - Existing products
- OpenOtto

About the Speaker

- Educated in Electrical and Computer Engineering
- Professional experience in hardware and software design
- Saturday afternoon mechanic
- Concerned about privacy

Why Should I Care?

- Automobile maintenance monopoly
  - Service manuals provide mechanical drawings with great accuracy
  - Limited electronic schematics, limited protocol specifications, no source code
- Privacy implications
  - What does a vehicle record?
- Vehicle more under control of manufacturer than owner

Background of Automotive Electronics

- Under the hood
  - Controllers for fuel injection, anti-lock brakes, traction control, air bags
- User visible
  - Climate control, entertainment, navigation, communication
- On-Board Diagnostics (OBD)
  - Implementation not standardized
- On-Board Diagnostics (OBD2)
  - Standardized by Society of Automotive Engineers (SAE)

Scope of SAE OBD2

- Physical connector
- Data link layer (three options), network protocol
- Diagnostics
  - Emission control systems required by U. S. Federal law
  - Standard and manufacturer specific components
- Many packet formats and data types for diagnostic data
- Read and write ECU memory
- Security feature

Common Usage - Scan Tool

- Electronic control unit (ECU) detects fault condition
  - e.g., oxygen sensor detected mixture too rich
- Diagnostic trouble code (DTC) is stored
- Check engine light illuminates, depending on DTC
- Mechanic retrieves DTC with a scan tool
- Mechanic fixes problem and clears DTC

Common Usage - Crash Data Recorder

- Airbag control module senses deployment or non-deployment event
- Vehicle sensor data is stored in airbag control module
  - e.g., vehicle speed, engine speed, throttle position, brake state, driver's seat belt
- Mechanic or law enforcement downloads crash data for analysis
- If vehicle is repaired, airbag control module is reset or replaced

Physical Layer, Diagnostic Busses

- PWM - Pulse Width Modulation (41.6kbps)
  - commonly used by Ford
- VPW - Variable Pulse Width Modulation (10.4kbps)
  - commonly used by GM
- ISO - Asynchronous Serial (10.4kbps)
  - commonly used by Chrysler, imports (European, Japanese)

Physical Layer, Other

- CAN - Controller Area Network
  - High speed (500kbps)
- other (not OBD2)
  - KWP2000 (ISO standard)
  - manufacturer proprietary

Data Link Layer

- OBD2 and ISO (ISO 9141)
- Half duplex (shared) bus
- Carrier sense multiple access (CSMA), non-destructive collisions
- Priority in packet header specified so higher priority packets prevail

Network Layer

- Addressing modes
  - Functional
  - Physical
- Packet format
  - Diagnostic modes: run tests, query sensor, control outputs

Data Formats

- Scaling, limit, offset, table (SLOT)
  - Maps raw data bits/bytes to meaningful magnitude
  - e.g., 8-bit value represents -40 to 87.5 with 0.5 increments
- Parameter reference number (PRN)
  - Maps packet data to useful quantities
  - Includes SLOT (for magnitude), units, label/description

Diagnostic Modes

- Request sensor, diagnostic data
- Freeze frame capability
  - Set triggers, read freeze frame data
- Read and clear DTCs
- On-board monitoring and diagnostic tests
  - Continuously and non-continuously monitored systems
  - Initiate test, read results

Diagnostic Modes (cont'd)

- Read vehicle information
  - Vehicle identification number (VIN), calibration data and memory checksum
- Upload and download memory to ECUs

Existing Products, Hardware

- Proprietary full interface products
  - Highly functional, very expensive
- Complete devices - usually serial to diagnostic bus
- Components - also usually serial to diagnostic bus
- Free designs - a few TIA-232 to ISO interfaces

Existing Products, Software

- Numerous commercial and shareware products
  - Standard support is most common
  - Some specialized for vehicle manufacturer
- freediag [2]
  - Free software (GPL)
  - Supports basic scan tool operation, diagnostic procedures

OpenOtto

- Hardware
  - TIA-232 to ISO bus
  - Repurposed USB serial adapter
- Software
  - Layer 2 and 3 network stack
  - Application software
- Free software/hardware (GPL)

OpenOtto Network Stack

- Common API across networks
- Physical layer
  - ISO, (VPW, PWM, CAN)
- Data link layer
  - OBD2
- Network layer
  - OBD2, (manufacturer extensions)

OpenOtto Applications

- Scan tool
- Network probe and logging tool (a la tcpdump, nmap, etc.)
  - Explore unidentified ECUs, unknown packet formats
- High level monitoring and control
  - Expanded diagnostics
  - Logging
  - Configurable UI for detailed dash board

Conclusion

References

[1] *On-Board Diagnostics for Light and Medium Duty Vehicles Standards Manual, SAE HS-3000*. Society of Automotive Engineers, Inc. http://www.sae.org

[2] FREEDIAG. A suite of vehicle diagnostic protocols and an OBD II (mostly) compliant Scan Tool. http://freediag.sourceforge.net/

[3] OPENOTTO. An open implementation of automotive communication and diagnostic protocols. http://www.area49.net/projects/openotto/

Copyright


```
$Id: presentation.lyx,v 1.9 2004/07/08 23:20:57 alpha Exp $
```