

汽车诊断技术及常用协议介绍

1. 汽车电控诊断系统的产生以及由来

随着汽车电子化控制的不断采用，带来了新的问题。一方面，汽车电控系统日趋复杂，给汽车维修工作带来了越来越多的困难，对汽车维修技术人员的要求越来越高；另一方面，电子控制系统的安全容错处理，汽车不能因为电子控制系统自身的突发故障导致汽车失控和不能运行。针对这种情况，汽车电控技术设计人员，在进行汽车电子控制系统设计的同时，增加了故障自诊断功能模块。它能够在汽车运行过程中不断监测电子控制系统各组成部分的工作情况，同时启动相应故障运行模块功能，维修人员可以利用汽车故障自诊断功能调出故障码，快速对故障进行定位和修复。

1993 年以前的电控汽车的故障自诊断系统自成体系，不具有通用性，给汽车的售后服务和维修工作造成了很大不便，按照美国标准称为第一代随车自诊断系统（OBD-I）。1994 年美国汽车工程师协会（SAE）提出了第二代随车自诊断系统（OBD-II）的标准规范。只要各汽车制造厂执行该规范，其诊断模式和诊断插座，便可得到统一。该系统的自诊断模块不仅能够解决汽车电控系统的安全性和存储汽车记忆故障，还能够实时提供汽车各传感器和开关的运行参数（即我们所说的数据流）和对执行器进行动作测试等功能。目前新的第三代随车自诊断系统（OBD-III）也已经在酝酿之中，它比第二代更完善，更全面。估计在不久将来会付诸实施，被各汽车制造商所采用。

2007 年之后，中国新车开始统一出厂 OBD 接口。

2. 汽车诊断 OBD 位置以及引脚定义

2.1 车辆 OBD 位置

14



A 区域:通用、大众、福特、丰田、现代、雪铁龙、宝马等品牌

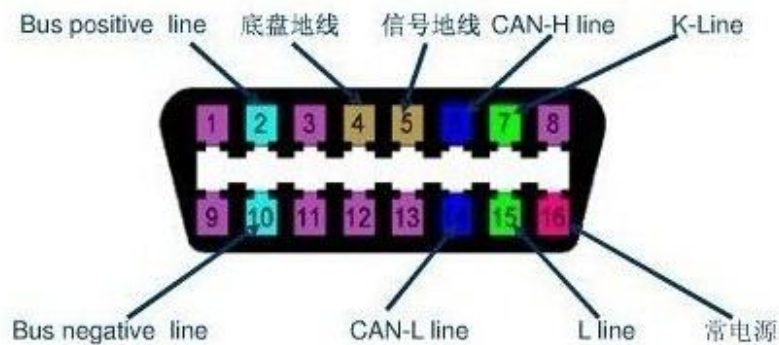
B 区域: 本田、大众途安、进口雷克萨斯等车型

C 区域: 东风雪铁龙、东风标致等少量车型

D 区域: 东风雪铁龙等少量车型

E 区域: 其他少量车型

2.2 OBD 引脚定义



1. Manufacturer discretion. GM: J2411 GMLAN/SWC/Single-Wire CAN.
2. SAE-J1850 PWM 和 SAE-1850 VPW 总线(+)
3. Ford DCL(+) Argentina, Brazil (pre OBD-II) 1997-2000, USA,
4. 车身地
5. 信号地
6. CAN high (ISO 15765-4 and SAE-J2284)
7. ISO 9141-2 和 ISO 14230-4 总线的 K 线
8. -
9. -
10. Bus negative Line of SAE-J1850 PWM only (not SAE-1850 VPW) Europe, etc.
Chrysler CCD Bus(+)
11. Ford DCL(-) Argentina, Brazil (pre OBD-II) 1997-2000, USA, Europe, etc. Chrys
12. -
13. -
14. CAN low (ISO 15765-4 和 SAE-J2284)
15. ISO 9141-2 和 ISO 14230-4 总线的 L 线
16. 蓄电池电压

3. 汽车 OBD 诊断模式

3.1 OBD 诊断模式

OBD 9种诊断模式

9种诊断模式		
模式	Service ID	说明
MODE 1	\$01	请求动力系统当前数据
MODE 2	\$02	请求动力总成的冻结帧数据
MODE 3	\$03	请求排放相关的动力系统诊断故障码
MODE 4	\$04	清除/复位排放相关的诊断信息
MODE 5	\$05	请求氧传感器监测测试结果
MODE 6	\$06	请求非连续监测系统OBD测试结果
MODE 7	\$07	请求连续检测系统OBD测试结果
MODE 8	\$08	请求控制车载系统，测试或者部件
MODE 9	\$09	读取车辆和标定识别号

模式 Service ID 说明

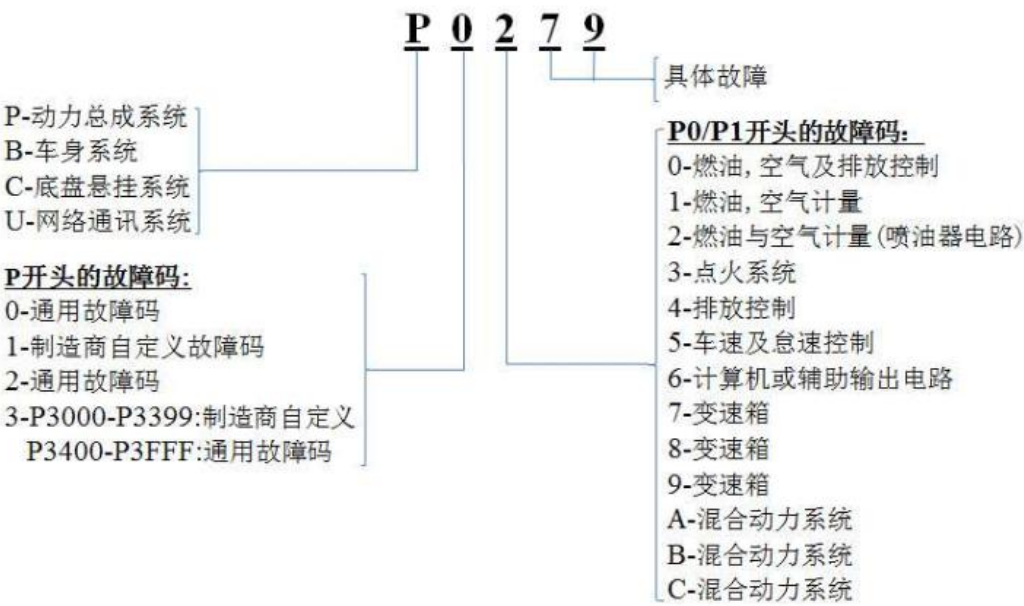
- MODE 1 \$01 请求动力系统当前数据
- MODE 2 \$02 请求动力总成的冻结帧数据
- MODE 3 \$03 请求排放相关的动力系统诊断故障码
- MODE 4 \$04 清除/复位排放相关的诊断信息
- MODE 5 \$05 请求氧传感器监测测试结果
- MODE 6 \$06 请求非连续监测系统OBD测试结果
- MODE 7 \$07 请求连续检测系统OBD测试结果
- MODE 8 \$08 请求控制车载系统，测试或者部件
- MODE 9 \$09 读取车辆和标定识别号

3.2 OBD 故障码解析

OBD-II故障码解析

OBD-II故障码解析

一般来讲, OBD-II故障码由一位字母和四位数字组成。举例说, P0279



3.3 OBD II 系统的监测功能

装备 OBD II 计算机系统具有发现部件和系统故障的能力，而 OBD II 的计算机系统具有探测部件和系统的能力，以维持很低的排放水平。

具有 OBD II 能力的计算机系统与以前的计算机系统大体相似，只不过 PCM 模块中增加了范围广泛的监测系统和策略。

OBD II 系统主要有以下监测器：

- 1) 催化剤效率监测器
- 2) 发动机缺火监测器
- 3) 燃油系统监测器
- 4) 加热型氧传感器监测器
- 5) 综合部件监测器
- 6) 燃油蒸发排放系统监测器
- 7) 二次空气喷射监测器
- 8) 排气再循环监测器

4. 常用协议介绍

使用外部诊断设备来读取汽车电控单元中存储的故障码以及通过和电控单元直接对话来获得数据流信息，成为最流行的诊断技术方式。这些与汽车电控单元的直接对话，就需要通信协议的支持。标准协议的产生，就由此而来。

4.1 Kwp2000

1: 快速方式进入系统

Req: c1 33 f1 81 66

Ans: 83 F1 12 C1 E9 8F BF

4.2 ISO9141

Req: 0X33 (TOOLS 发地址码0X33)

Ans: 55 08 08 (ECU 返回0X55, KWORD1, KWORD2)

Req: F7 (TOOLS 将KWORD2取反0XF7发出)

Ans: CC (ECU 将地址码取反0XCC返回)

4.3 CAN_STD_250/500K

REQ: 00 00 07 DF 02 01 00 00 00 00 00 00

RSP: 00 00 07 E8 06 41 00 FF FF FF FF 00

直接发送读取支持字命令指令进去。此时过去对应的 ECU 的 CANID 为 07 E8

4.4 CAN_STD_250/500K

REQ: 18 DB 33 F1 02 01 00 00 00 00 00 00

RSP: 18 DA F1 11 06 41 00 FF FF FF FF 00

通过发送读取支持字直接进去。

4.5 标准数据流 ID

PID ^①	名称 ^②	长度 ^③	描述 ^④
0x00 ^⑤	PIDs supported [01 - 20] ^⑥	4 ^⑦	后续 31 字段是否被支持 ^⑧
0x01 ^⑤	Monitor status since DTCs cleared ^⑥	4 ^⑦	故障灯状态和故障码个数 ^⑧
0x02 ^⑤	DTC that caused required freeze frame data storage ^⑥	2 ^⑦	快照模式标识 ^⑧
0x03 ^⑤	Fuel system status ^⑥	2 ^⑦	燃油系统状态 ^⑧
0x04 ^⑤	Calculated engine load value ^⑥	1 ^⑦	动力负荷计算值 (%) ^⑧ 有效值范围: 0 至 100 ^⑨
0x05 ^⑤	Engine coolant temperature ^⑥	1 ^⑦	冷却液温度(水温) (° C) ^⑧ 有效值范围:-40 至 215 ^⑨
0x06 ^⑤	Short term fuel % trim-Bank 1/3 ^⑥	2 ^⑦	短期燃油修正 B1 ^⑧ 有效值范围:-100 至 99.22 ^⑨
0x07 ^⑤	Long term fuel % trim-Bank 1/3 ^⑥	2 ^⑦	长期燃油修正 B1 ^⑧ 有效值范围:-100 至 99.22 ^⑨
0x08 ^⑤	Short term fuel % trim-Bank 2/4 ^⑥	2 ^⑦	短期燃油修正 B2 ^⑧ 有效值范围:-100 至 99.22 ^⑨
0x09 ^⑤	Long term fuel % trim-Bank 2/4 ^⑥	2 ^⑦	长期燃油修正 B2 ^⑧ 有效值范围:-100 至 99.22 ^⑨
0x0A ^⑤	Fuel pressure ^⑥	1 ^⑦	燃油压力(仪表板指示) (kPa) ^⑧ 有效值范围:0 至 765 ^⑨

5. 私有协议介绍

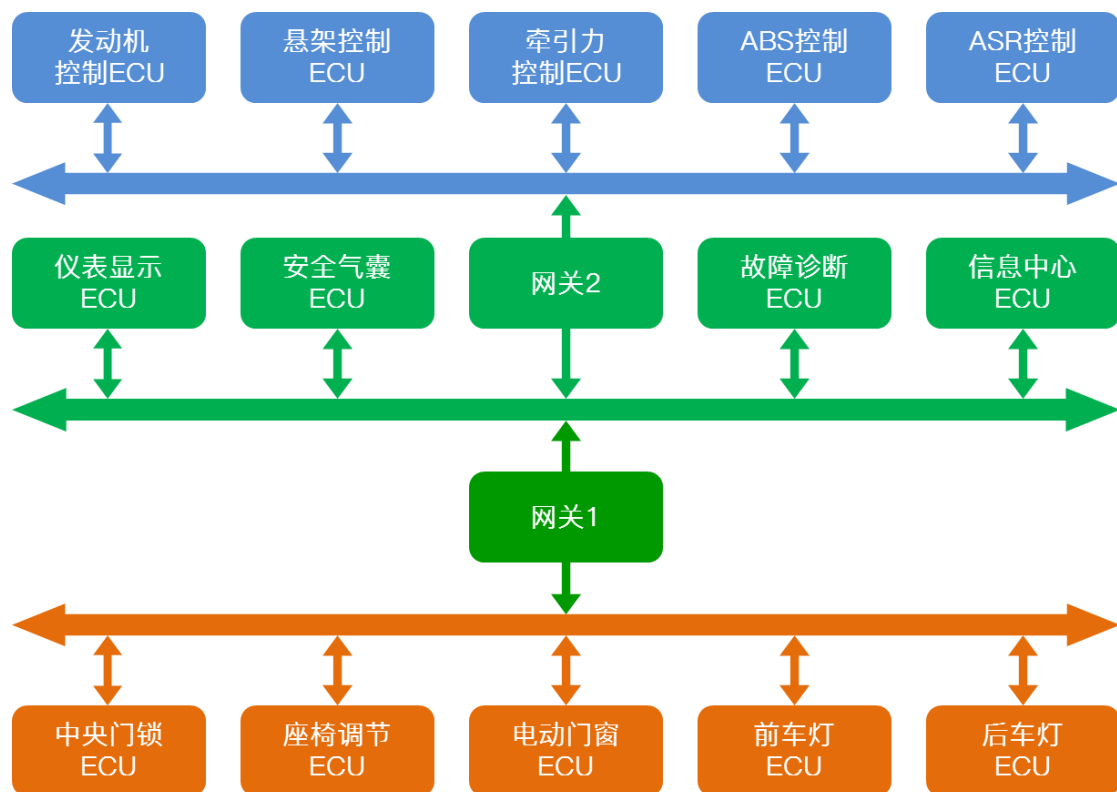
公开规定的就是通用的标准协议，但是车厂会根据自己的设计在保留部分自己定义，也就是私有协议，所以每个车厂每个系列的车都有自己的通讯协议。

针对私有协议的开发，要做专车专用的车型。

目前市面上高档汽车全面淘汰了 K 线协议，而采用速度更快、信号更稳定的 CANBUS 总线。开发汽车 CANBUS 系列总线产品是汽车电子领域目前比较热门的一个趋势。

利用汽车 OBD 接口，与汽车 ECU 通过 CANBUS 协议通讯，就可以达到控制汽车某些部件的目的，并可衍生大量的新产品，如 OBD 自动升窗器、中控防盗模块等。

整车系统控制



5.1 福特车破解用例

5.1.1 车门

原始数据

0X00000366-C0-40-3E-00-C9-36-F8-8A	驾驶位车门
0X00000366-C0-42-3C-00-C9-36-F8-8A	驾驶位车门+副驾驶位车门
0X00000366-C0-42-B4-00-C9-36-F8-8A	驾驶位车门+副驾驶位车门+副驾驶位后车门
0X00000366-C0-43-B0-00-C9-36-F8-8A	驾驶位车门+副驾驶位车门+副驾驶位后车门+驾驶位后车门
0X00000366-C0-43-E0-00-C9-36-FC-8A	驾驶位车门+副驾驶位车门+副驾驶位后车门+驾驶位后车门+后

Data1 Data2

车门	关闭	打开
驾驶位车门	40-3F	40-3E
副驾驶位车门-	40-3F	42-3D
驾驶位后车门	40-3F	41-3B
副驾驶位后车门	40-3F	40-B7
后备箱门	40-3F	40-6F

5.1.2 车灯

0X000000C3-DC-87-32-F0-20-30-C6-00-
0X000000C3-C7-87-32-F0-20-30-C6-01-
0X000000C3-C7-87-36-F0-20-30-C6-02

Data7

车灯	两侧车灯	近光灯
关	打开	打开
00	01	02

车灯的状态有三个，关闭 拧两侧小灯，在拧近光灯。



5.2 别克车破解用例

5.2.1 车钥匙

状态	ID	数据
解锁	0x00000133	0x02
锁车	0x00000133	0x04 延迟 30 秒左右变为 0x01

5.2.2 车窗打开关闭

状态	ID	数据
升窗	0x00000243	3B 0F 01 01 01 01 (四个字节代表四个车窗)
关窗	0x00000243	3B 0F 02 02 02 02 (02 代表关闭) -