附件8：如何解析和破解车载CAN协议--DBC协议

使用说明书

说明书版本：V2.03

更新日期：2017.06.30

珠海创芯科技有限公司 技术支持邮箱：zhcxgd@163.com

DBC协议解析

每个CAN通道都可以独立支持车载CAN-bus应用协议的解析，只要用户在CANtest或CANpro1.50软件中导入相关的DBC文件，即可实现应用层数据的解析。可用于车辆CAN协议解析、车辆测试维修、破解车辆CAN协议等。

用户使用CANTest或CANPro1.50时，只需替换ControlCAN.dll等库文件（参考：如何兼容使用周立功CANTest/CANpro1.50软件.pdf），并选择型号：USBCAN-2E-U即可。

CANpro1.50功能比较丰富，这里以CANpro1.50为例。

1、操作步骤

打开CANpro1.50软件，选择USBCAN-2E-U接口卡，并且选定总线的波特率（以实际波特率为准，汽车CAN总线一般为500K），点击确定并启动，启动CAN接口卡。如图2所示；

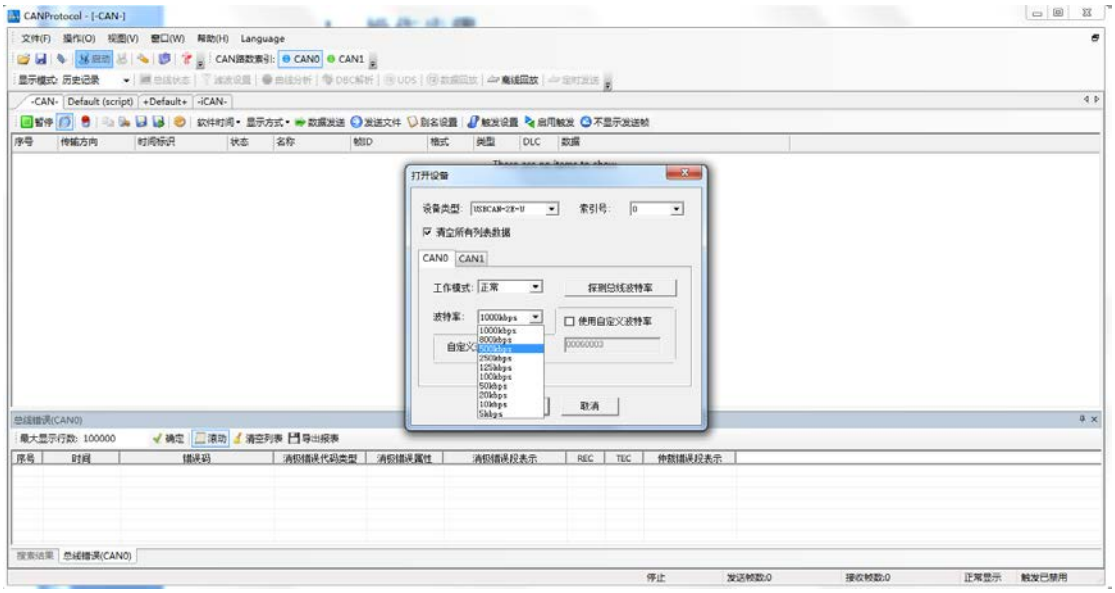


图 2 打开CANpro软件初始化

点击菜单快捷操作中的DBC解析按钮，进入DBC解析界面，如图3所示；

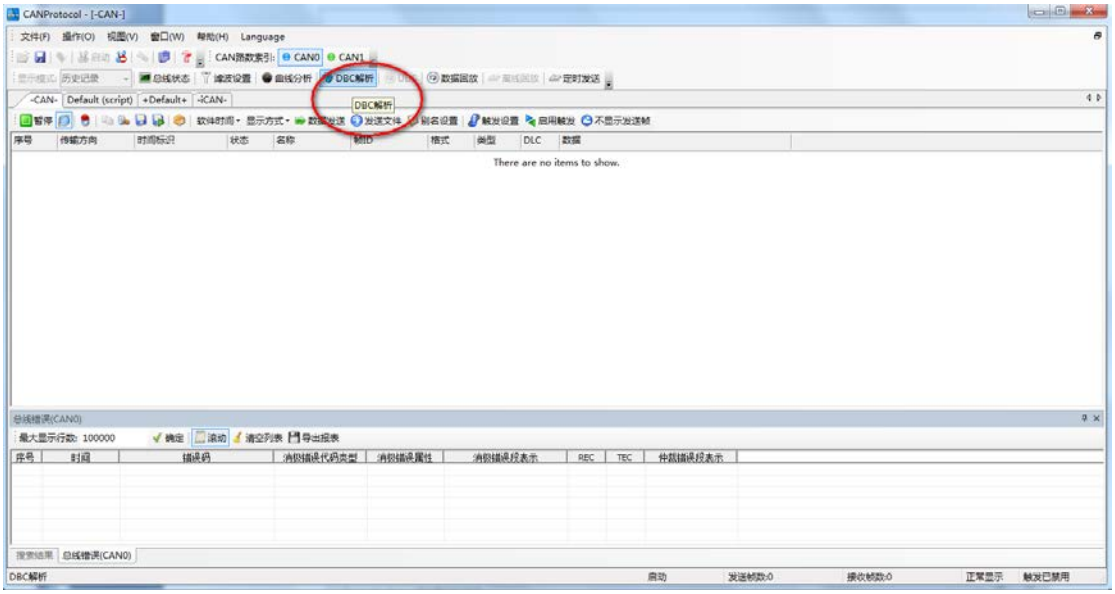


图 3 打开DBC解析

DBC解析界面中，点击加载DBC，选择对应的DBC文件打开，CANpro自带三个DBC文件。本文以J1939协议为例，选择j1939.dbc打开，解析柴油机、卡车或者公交车等协议，如图4所示。

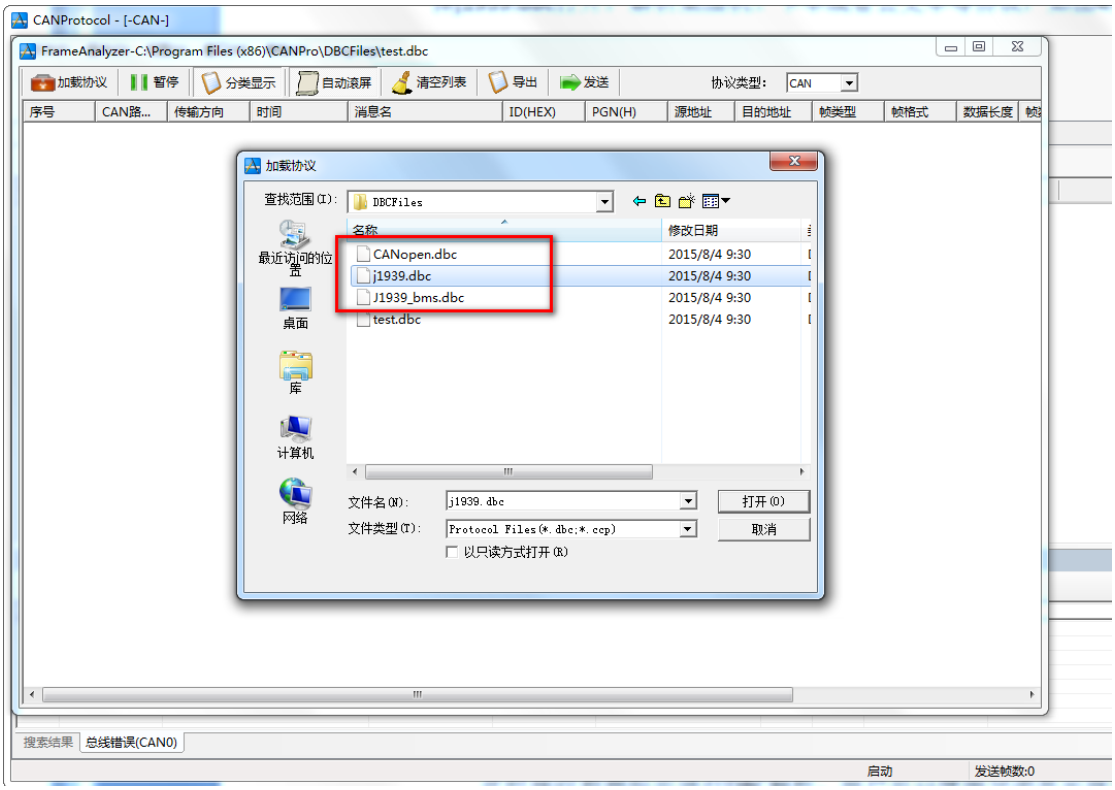


图 4 加载DBC文件

此时接收数据即可进行DBC解析，用户可以使用分类显示或者刷新显示查看。点击某个报文，下方解析框中将这帧包含的应用数据显示出来。如图5所示，ID为0x0CF0041A中第四

个字节为0x6C、第五字节为0xD6。查阅、对照SAE_J1939-71协议得知：电子发动机控制器#1：EEC1（消息名）中第4、5字节代表EngSpeed（发动机转速）。

数据长度： 2字节

分辨率： 0.125 rpm/位递增，从0 rpm开始计算（高位字节分辨率=32 rpm/位）

数据范围： 0到8031.875 rpm

可以计算出转速：0xD66C*0.125为6861.50rpm（转/分）。

其它参数的定义与解析，请参照SAE_J1939-71协议：光盘\说明文档目录\16.附件9：SAE_J1939-71协议.pdf

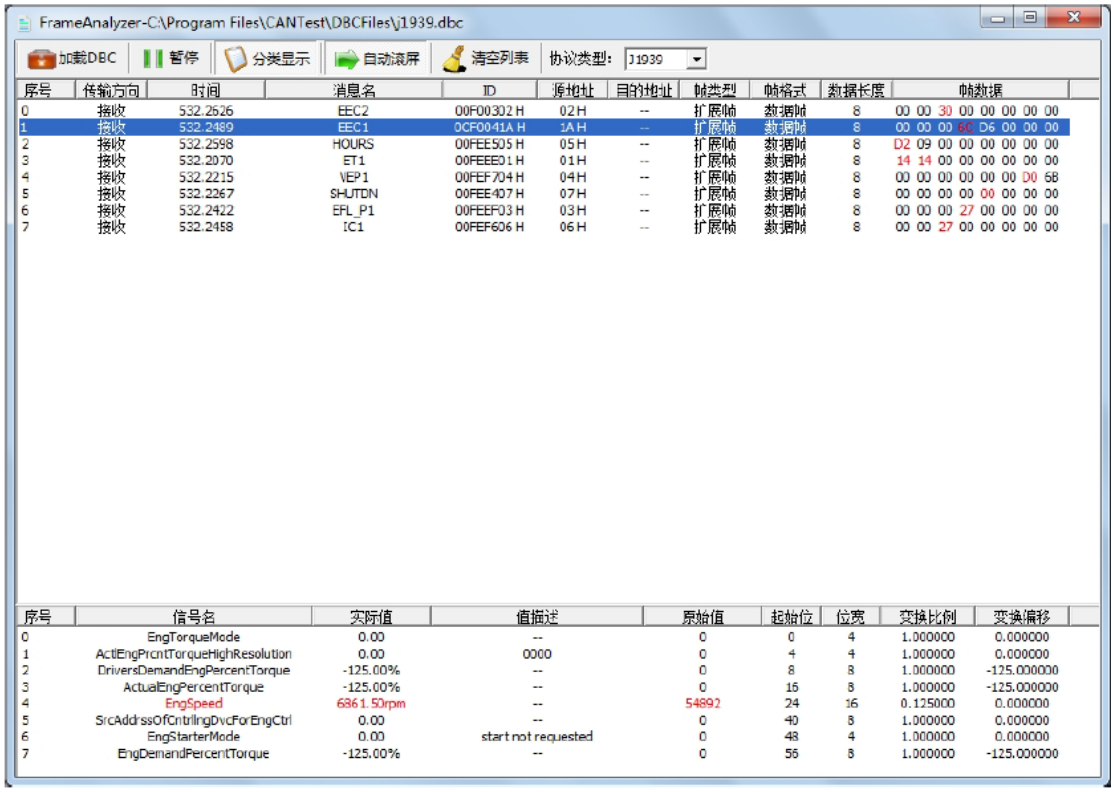
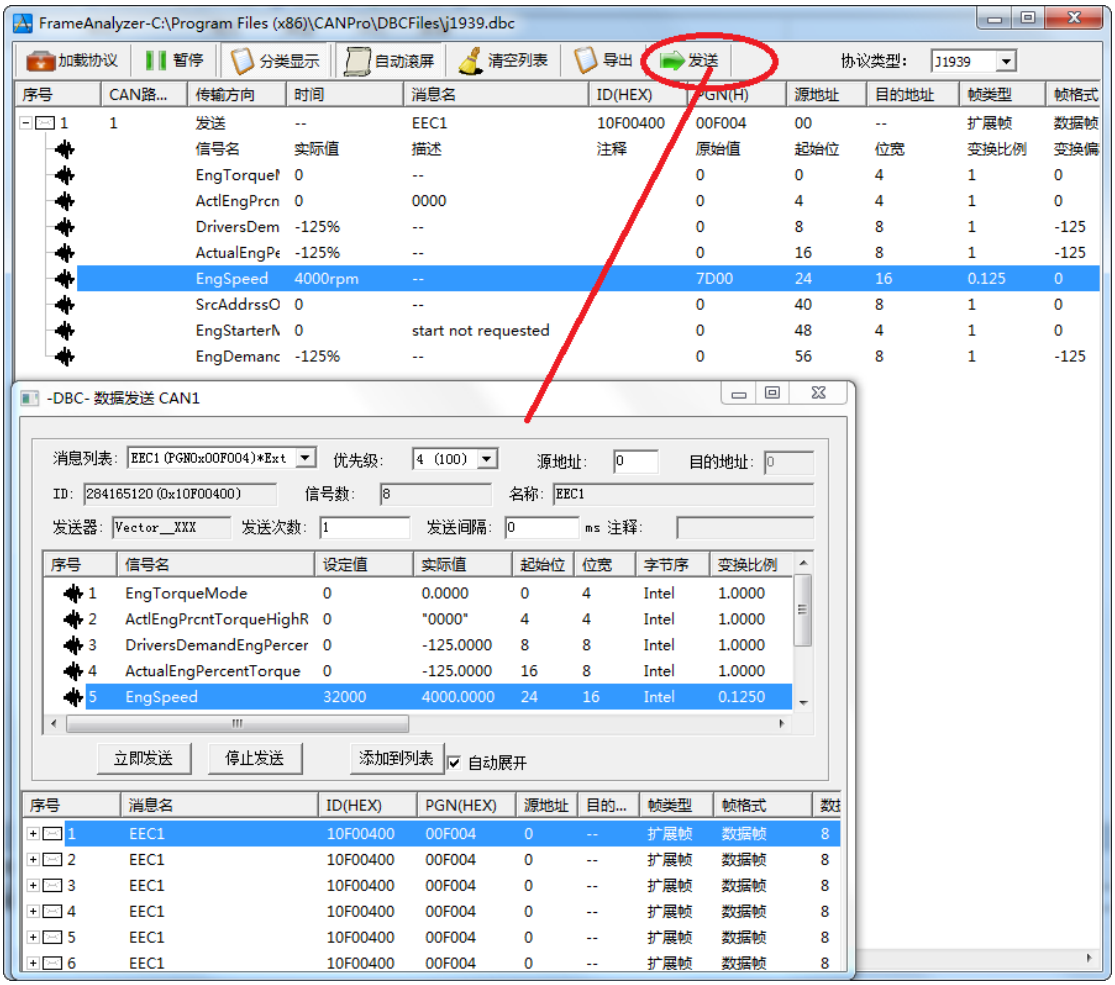


图 5 DBC协议解析结果

小技巧：运用分类显示功能时，软件会将有变化的数据标红，这样对于破解未知协议时，可以帮助用户快速完成变量识别工作。比如，要想知道方向盘所对应CANID和数据段，即可使用此方法运行，转动方向盘，观察变红的变量，即对应。

最新版本的CANPro1.50软件，支持DBC协议发送功能。

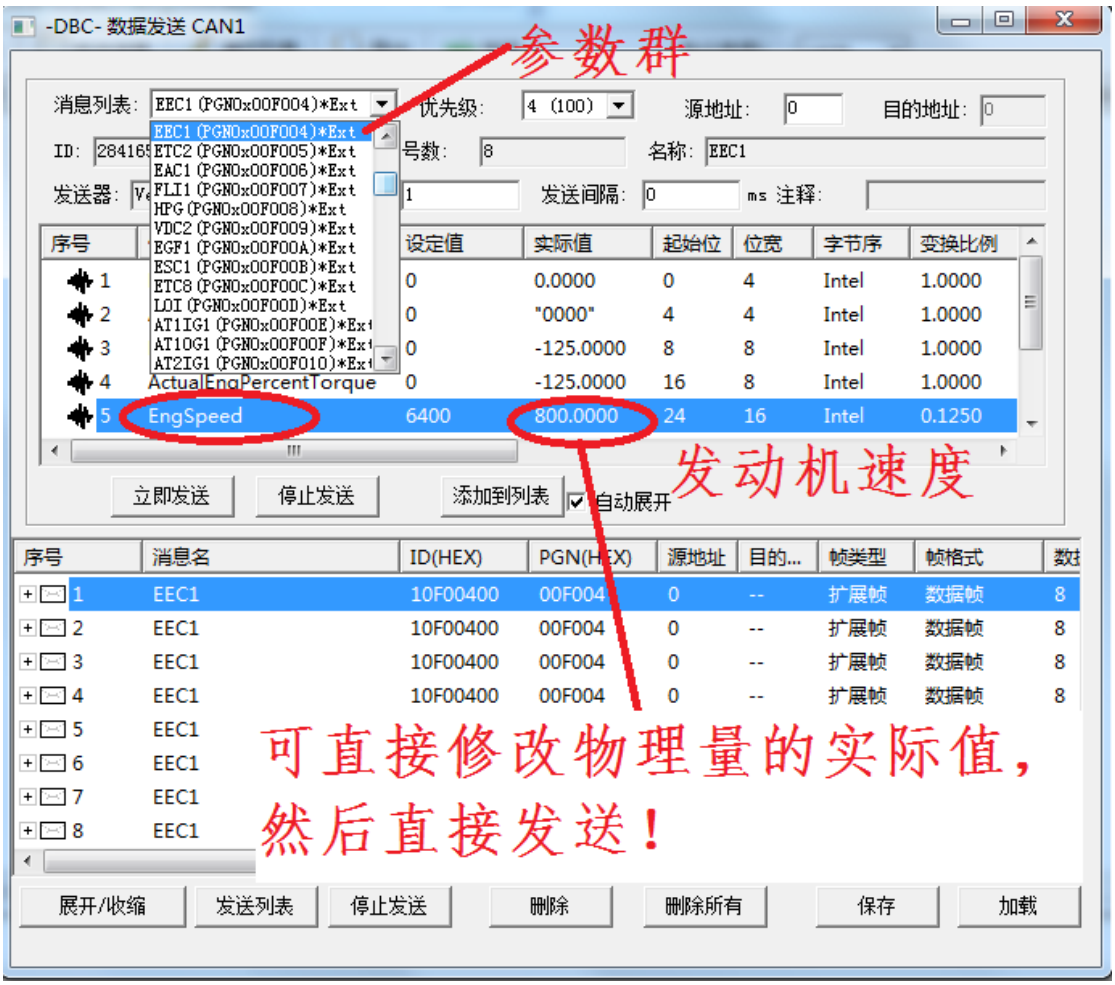


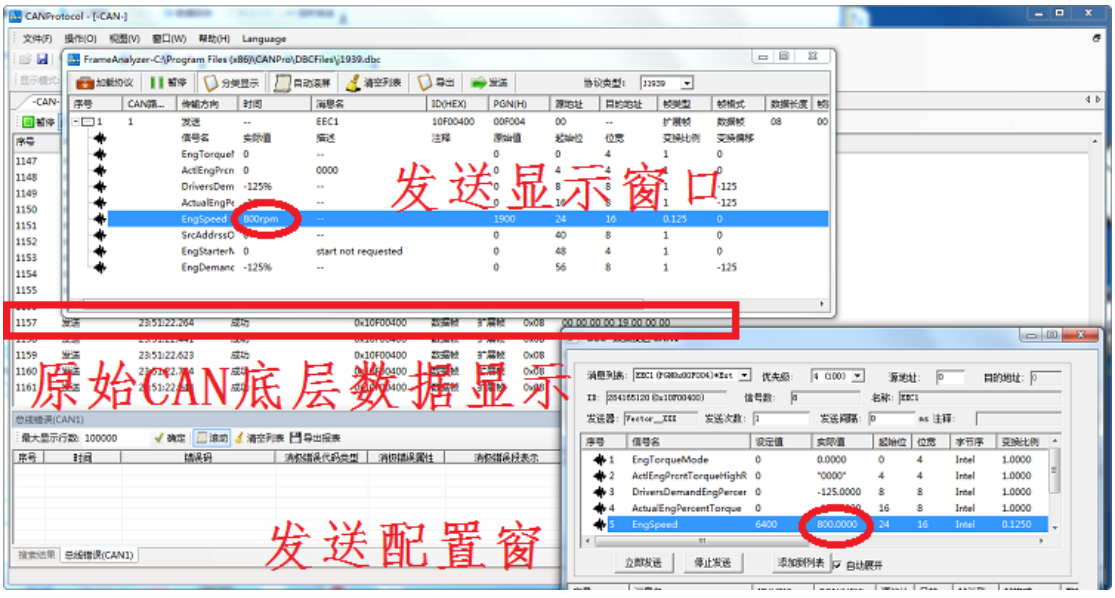
支持按J1939协议直观配置发送数据。

J1939协议发送界面：

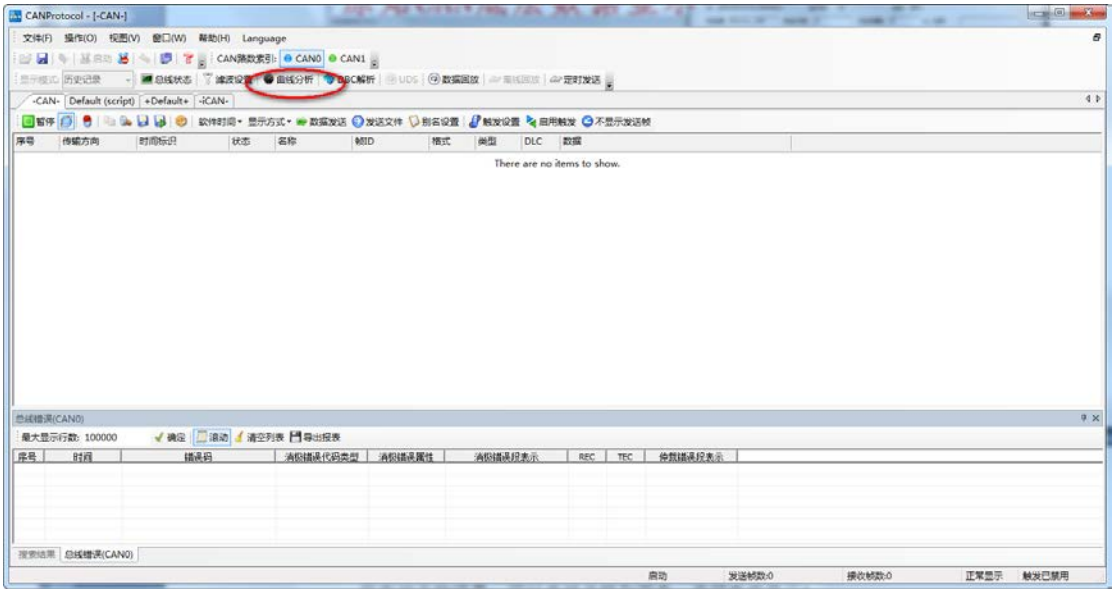
参数群的任意物理参数进行实际值定义，并发送。不理用理会J1939协议的原理。可以直接模拟J1939设备进行测试。

下图中，配置模拟发动机转速为800转/分，并发送。

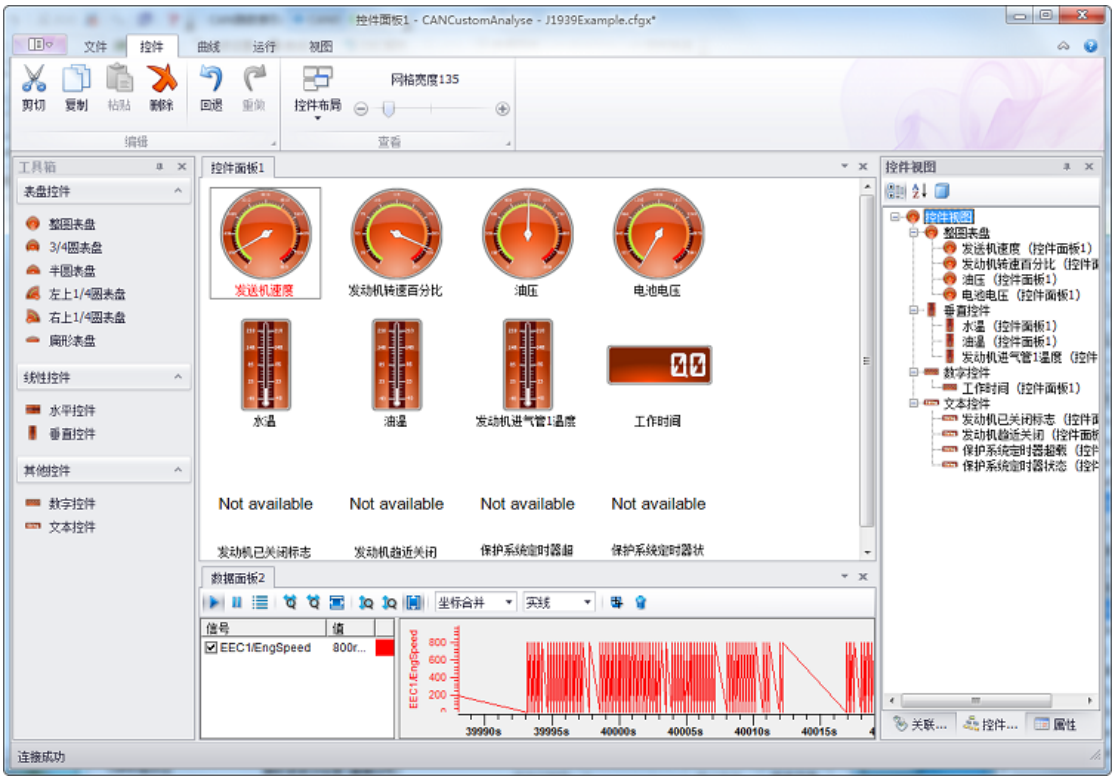




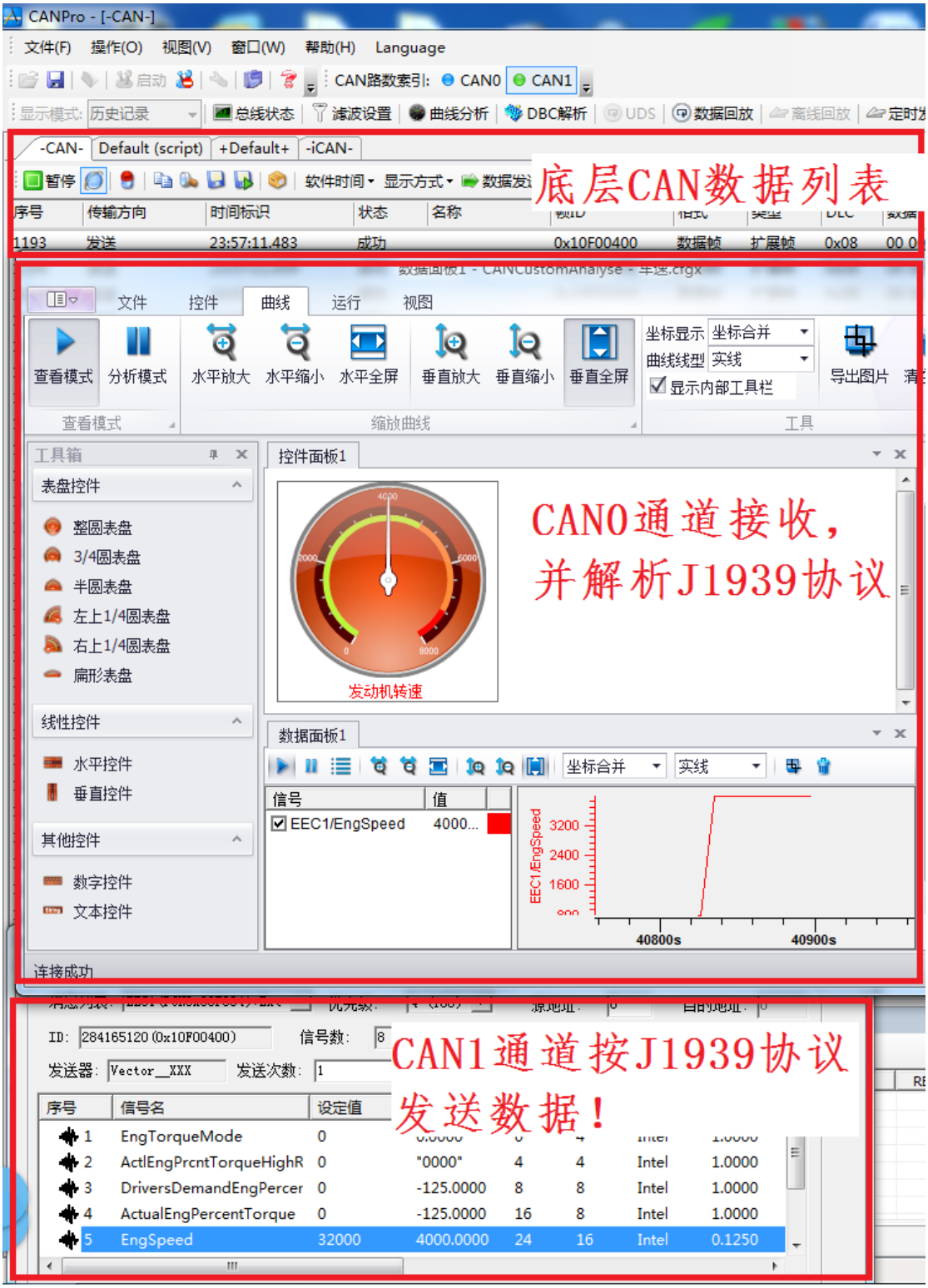
最新版本的CANPro1.50软件，支持DBC协议曲线、图表显示。



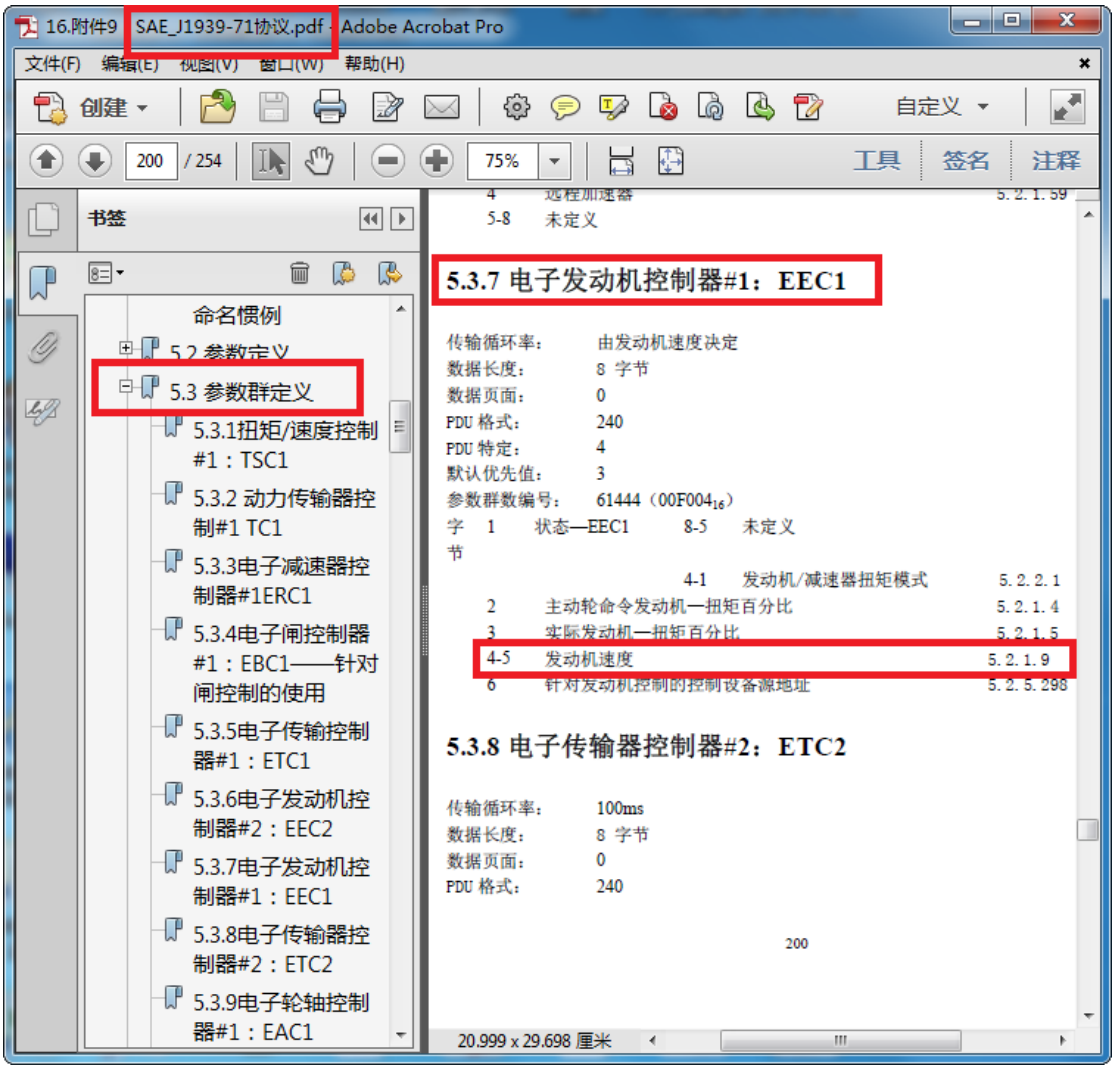
所有相关物理量，可以直接关联到图表、曲线直观显示！

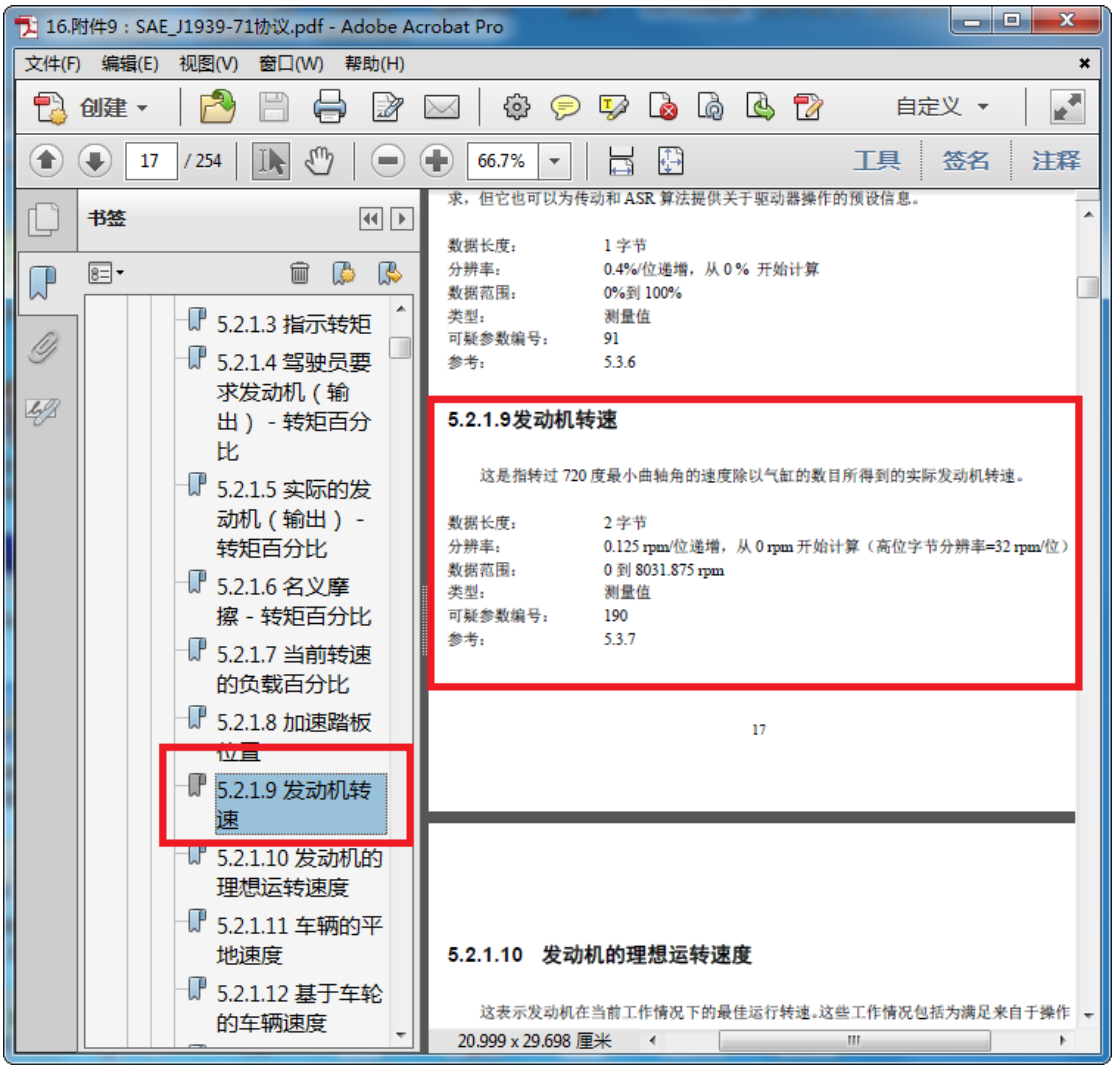


如果没有实车，也可以调试学习J1939协议，购买双通道的产品，两个通道间即可以收发数据。



软件中的参数群为全英文显示，控件面板的控件名称可以自行修改为中文，这里提供中文版协议供对照。


16.附件9 SAE_J1939-71协议.pdf - Adobe Acrobat Pro
文件(F) 编辑(E) 视图(V) 窗口(W) 帮助(H)
创建
自定义
200 / 254
75%
工具
签名
注释
书签
命名惯例
5.2 参数定义
5.3 参数群定义
5.3.1扭矩/速度控制#1：TSC1
5.3.2 动力传输器控制#1 TC1
5.3.3电子减速器控制器#1ERC1
5.3.4电子闸控制器#1：EBC1——针对闸控制的使用
5.3.5电子传输控制器#1：ETC1
5.3.6电子发动机控制器#2：EEC2
5.3.7电子发动机控制器#1：EEC1
5.3.8电子传输器控制器#2：ETC2
5.3.9电子轮轴控制器#1：EAC1
5-8 未定义
5.3.7 电子发动机控制器#1：EEC1
传输循环率： 由发动机速度决定
数据长度： 8 字节
数据页面： 0
PDU 格式： 240
PDU 特定： 4
默认优先值： 3
参数群数编号： 61444（00F004$_{16}$）
字节 1 状态—EEC1 8-5 未定义
4-1 发动机/减速器扭矩模式 5.2.2.1
2 主动轮命令发动机—扭矩百分比 5.2.1.4
3 实际发动机—扭矩百分比 5.2.1.5
4-5 发动机速度 5.2.1.9
6 针对发动机控制的控制设备源地址 5.2.5.298
5.3.8 电子传输器控制器#2：ETC2
传输循环率： 100ms
数据长度： 8 字节
数据页面： 0
PDU 格式： 240
200
20.999 x 29.698 厘米



2、应用范围

- 工业控制测试
- 汽车电子维护维修
- 协议破解