**诊断协议：**

诊断id分为两部分，11-19，22以上，前者为常规数据读取，安全校验相关服务，后者涉及MCU写入、擦除操作，须在安全校验通过之后才可以进行。

MCU接收CAN数据ID为520，应答ID为521，在收到相关报文后给予应答，66为积极应答，77为消极应答。

STM32F4的CAN通信仅支持8字节数据，CAN报文必须保证每一帧都是8字节，当发送的数据不满足8字节时需对数据帧进行填充，CAN to MCU使用55填充，MCU to CAN使用ff填充。CAN数据帧分为NF、RF、LF、RLF四种。

NF为单帧，在一帧之内包含了所需要的所有数据。

当一帧无法将数据完全发送完毕的时候，需要使用多帧发送，首先发送RF多帧请求，数据格式为：

10 + 数据长度 + 服务id + 数据

MCU收到多帧请求之后，应答RLF数据帧，格式为：

30 00 00 00 ff ff ff ff

上位机收到应答后开始发送长数据帧该次数据传输完毕，格式为：

21（22，23...） + 数据

当MCU向外发送数据时，如若一帧无法将数据发送完毕，也需要采用相同的方式传输数据。

00：0x18U

功能：实现MCU信息的读取，报文格式为：

520 02 18 01 55 55 55 55 55 🡪请求读取数据

521 07 18 01 66 \*\* \*\* \*\* \*\* 🡪积极应答

521 04 18 01 77 \*\* ff ff ff 🡪消极应答

01：0x19U

功能：安全校验，通过之后才能进行MCU修改操作

520 02 19 01 55 55 55 55 55 🡪请求访问，MCU应答此时程序运行位置是boot还是app。

521 05 19 01 66 ab ba ff ff ff 🡪boot为abba

521 05 19 01 66 ac ca ff ff ff 🡪app为acca

MCU应答之后，需要根据应答的数据发送密钥，密钥为三字节数据：

520 05 19 02 \*\* \*\* \*\* 55 55 🡪发送密钥

521 04 19 02 66 10 ff ff ff 🡪密钥验证通过，给予积极应答，10中的1为service id，0表示验证通过，1表示验证失败。状态为通过。

521 04 19 02 77 11 ff ff ff 🡪消极应答，状态为未通过

在安全校验完成之后，对安全校验状态进行设置，为0时可以对MCU进行修改操作，为1时禁止操作，在验证通过后设置一个5秒的定时器，在5秒内未进行相关操作，状态设置为1，下次操作需重新校验

02：0x22U

功能：下发擦除指令，从下发的地址对MCU进行擦除，该地址为APP的起始地址。

520 07 22 d1 1d \*\* \*\* \*\* \*\* 🡪验证d11d通过后，检验地址，只有二者同时满足时才会进行擦除。验证通过后，MCU发送

521 04 22 d1 1d 78 ff ff ff 表示开始擦除MCU，在此期间内MCU不接收CAN报文，直到擦除完成，同时创建一个10秒的定时器，如若10秒后仍然没有擦除完成，视为擦除失败，给予消极应答。

521 05 22 d1 1d 66 20 ff ff 🡪积极应答

521 06 22 d1 1d 77 21 01 ff 🡪地址错误

521 06 22 d1 1d 77 21 02 ff 🡪擦除超时，在定时器handle中发送。

在擦除完成之后，对擦除状态进行设置，只有在擦除完成的情况下才可以进行MCU升级操作。

03：0x23U

功能：请求下载，发送写入起始地址以及写入数据块的大小。

520 10 0b 23 e1 1e xx xx xx 🡪多帧请求

521 30 00 00 00 ff ff ff ff 🡪接收应答多帧请求

520 21 xx yy yy yy yy 55 55 🡪继续发送地址与大小

521 05 23 e1 1e 66 30 ff ff 🡪请求有效

521 06 23 e1 1e 77 31 01 ff 🡪写入地址错误

521 06 23 e1 1e 77 31 02 ff 🡪写入数据超过MCU内存

在请求下载后，对下载相关数组进行初始化，包括写入地址、写入数据大小、和校验计算、数据块次数等。

04：0x24U

功能：数据传输和写入。

采用多帧形式传输数据块，每个数据块的大小为240个字节,加上功能id和数据块编号，实际传输大小为242，写入最小单位为8字节，在每次写入的过程中计算和校验值，写入地址随写入大小递增，调用flash写入函数，在写入前发送78报文，禁止其他报文干扰，定时5秒，入写超时，视为失败。写入成功，应答功能id和数据块编号。

520 10 F2 24 01 \*\* \*\* \*\* \*\*

521 30 00 00 00 ff ff ff ff

520 21 \*\* \*\* \*\* \*\* \*\* \*\* \*\*

……

长数据帧2开头，第四位为序号，在每次传输时还需要校验序号，当序号错误时发送错误报文，传输失败。1—f—0—f—0变化。

521 02 77 89 ff ff ff ff ff 🡪长数据帧序号错误，所有的序号错误都使用该应答

521 03 66 24 40 ff ff ff ff 🡪写入成功

521 03 77 23 41 ff ff ff ff 🡪写入失败

05：0x25U

功能：在最后一个数据块传输完毕，且收到数据写入成功的积极应答之后，向MCU发送请求退出数据传输。

520 01 25 55 55 55 55 55 55 🡪请求退出

521 03 25 66 50 ff ff ff ff 🡪退出传输积极应答

06：0x26U

功能：在收到数据传输退出的积极应答之后，想MCU发送和校验值，与MCU传输过程中计算的和校验值比较，相同则烧写成功，不同则烧写失败。

520 05 26 xx xx xx xx xx 55 🡪发送和校验值

521 03 26 66 60 ff ff ff ff 🡪和校验成功

521 03 26 77 61 ff ff ff ff 🡪和校验失败

08：0x28U

功能：在和校验通过，收到相应积极应答、烧写成功之后，将升级标志设置为JUMP\_APP状态，重启MCU，使得MCU进入升级后的新系统。

520 04 28 ad cd ac 55 55 55 🡪调用软件复位，重启系统