北京小桔智能汽车科技有限公司企业标准

Q/DD B01060—2022

基于嵌入式系统的刷写技术要求

General Bootloader Requirement Specification Based on Embedded System

2022-01-28 发布　　2022-02-09 实施

小桔汽车技术标准体系管理委员会　发布

目　　次

前　　言

本文件按照 GB/T 1.1—2020 给出的规则起草。

本文件由北京小桔智能汽车科技有限公司电子电器标准工作组提出。

本文件由北京小桔智能汽车科技有限公司技术标准体系管理委员会归口。

本文件起草单位：北京小桔智能汽车科技有限公司通信与控制架构部、电子电器部。

本文件主要起草人： 施庆国，崔立峰，姬广斌，魏建，蔡军，叶小平。

本文件于 2022 年 01 月首次发布。

General Bootloader Requirement Specification Based on Embedded System
基于嵌入式系统的刷写技术要求

1 Scope/范围

This document introduces the requirements of the FBL of electronic and electrical architecture platform models. The specifications involved apply only to the ECUs based on embedded systems.

本文件规定了电子电器架构平台的刷写技术要求，所涉及的规范条目仅适用于基于嵌入式系统的电子电器控件。

This document is applicable to ECU flash process based on DoIP, CAN(FD) and LIN of Beijing Xiaoju Intelligent Automobile Technology Co., LTD.(The following abbreviations: XiaoJu Auto).

本文档适用于北京小桔智能汽车科技有限公司（以下简称“小桔汽车”）基于DoIP，CAN和LIN的ECU刷写流程。

2 Reference Documents/规范性引用文件

The contents of the following documents constitute essential provisions of this document through normative references therein. Where, only the version corresponding to the date of the reference file is applicable to this file; For undated reference files, the latest version (including all changes) applies to this file (for undated reference files, if the latest version does not contain the referenced content, the last version containing the referenced content applies).

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件（对于不注日期的引用文件，如果最新版本未包含所引用的内容，则包含了引用内容的最后版本适用）。

Q/DD B01194—2022 DoIP 诊断技术要求
Q/DD B01195—2022 以太网路由技术要求
Q/DD B01057—2022 UDS诊断技术要求
Q/DD B01059—2022 LIN诊断技术要求
Q/DD B01058—2022 CAN(FD)诊断技术要求
Q/DD B01055—2022 CAN(FD)-CAN(FD)路由技术要求

3 Terms and Definitions 术语和定义

The following terms and definitions apply to this document.

下列术语和定义适用于本文件。

3.1

Fingerprint

Tester identification information that identifies a certain download attempt.

指纹信息

诊断仪用于标识特定的下载尝试的信息。

3.2

Logical Block

Reserved portion of target memory, where application data can be downloaded (like hard disk partition).

逻辑块

目标内存的预留部分，用于下载应用程序数据（比如硬盘分区）

3.3

Logical Block Table

The target memory is split up in several Logical Blocks. The Logical Block table acts like a file system partition table. If application data is to be downloaded, the Bootloader checks, if there is a valid entry in the Logical Block table for the download.

逻辑块表

目标内存被分割为几个逻辑块。逻辑块表的作用是类似于文件系统分区表。如果要下载应用程序数据，引导加载程序将检查下载的逻辑块表中是否有有效的条目。

3.4

Server

ECU that responds to diagnostic service request for an external diagnostic tool.

服务端

响应外部诊断设备发起的诊断请求的ECU。

3.5

Sleep mode

Mode to reduce power consumption of the ECU in idle state.

睡眠模式

在ECU空闲阶段，用以降低能耗的模式。

3.6

Software Interlock

The software interlock is a protective lockout mechanism by separating critical code segments from other code in order to prevent unintended software execution e.g. after an error occurred.

软件互锁

软件联锁是一种保护性的锁定机制，通过将关键代码段从其他代码中分离出来，以防止意外的软件执行，例如在发生错误之后。

3.7

Client

External diagnostic tool(tester), that transmits service requests to ECUs.

客户端

外部诊断工具（诊断仪），用于向ECU传输服务请求。

4 符号和缩略语

下列符号和缩略语适用于本文件。

API——应用编程接口(Application Programming Interface)

CAN——控制局域网络(Controller Area Network)

CRC——Cyclic Redundancy Check

DID——数据标识符(Data identifier)

DoIP——基于IP的诊断通信(Diagnostic communication Over Internet IP)

DTC——诊断故障码(Diagnostic Trouble Code)

ECU——电子控制单元(Electronic Control Unit)

FBL——闪存引导加载程序(Flash Boot Loader)

ID——标识符(Identifier)

IP——因特网协议(Internet Protocol)

ISO——国际标准化组织(International Organization for Standardization)

NRC——否定响应码(Negative Response Code)

RAM——随机存取存储器(Random Access Memory)

UDS——统一诊断服务(Unified Diagnostic Service)

5 General Requirement/通用需求

5.1 Requirements for non-reprogrammable ECUs/不可重编程 ECU 要求

To ensure the successful execution of reprogramming, the non-reprogramming ECU needs to meet the following requirements:

为确保重编程的成功执行，对不可重编程ECU需要满足如下要求：

1. Support communication control-disable/enable to send and receive diagnostic services (i.e. 0x00/0x01 sub-function of 0x28 services), through which, It reduces the busload during programming;
2. Supports control DTC settings (0x85) diagnostic services, which ensure that when an ECU is programmed, the other ECU does not set DTCs;
3. The non-reprogramming ECU shall not support the diagnostic services associated with reprogramming, such as Diagnostic Session Control-Switching to Programming

Mode (0x10) 02), request download (0x34), transfer data (0x36), request transfer exit (0x37).

4. The non-reprogramming ECU needs to support the diagnostic services specified in the pre-programming process, except for the routine control - “check pre-programming conditions” service.

1. 支持通信控制-禁止/使能发送和使能接收（即0x28服务中的0x00/0x01子功能）的诊断服务，通过此服务，可以降低编程过程中总线的负载；
2. 支持控制DTC设置（0x85）诊断服务，通过此服务，确保当某个ECU处于编程状态时，其他ECU不会设置DTC；
3. 不可支持重编程相关的诊断服务，如：诊断会话控制-切换到编程模式（0x10 02）、请求下载（0x34）、传输数据（0x36）、请求传输退出（0x37）。
   不可重编程ECU需要支持预编程过程中规定的诊断服务，除了“例程控制-检查预编程条件”服务。

Any deviation from the proposed content of this document shall be approved by the chief engineer of XiaoJu Auto.

任何与本文档建议内容背离的设计必须获得小桔汽车主管工程师的认可。

5.2 Requirements for reprogrammable ECUs/可重编程 ECU 要求

5.2.1 General Information/概述

All ECUs that support reprogramming shall include Bootloader software.

所有支持重编程的ECU，应当包含Bootloader软件。

The system shall be able to enter the bootloader on request from normal operating mode .

系统在正常操作模式下发起请求时，必须能够执行bootloader。

The system shall execute boot code if the application code is missing, invalid or corrupt.

系统在应用软件丢失，无效或损坏时，必须执行Bootloader软件。

Application software and application data can be programmed simultaneously or independently of each other, and Bootloader software cannot be updated when reprogramming.

应用软件和应用数据可以同时编程或者相互独立编程，不允许重编程时更新Bootloader软件。

A system executing boot code must not disturb normal communication on the network.

系统执行boot软件必须不能影响总线正常通信。

Any deviation from the proposed content of this document shall be approved by the chief engineer of XiaoJu Auto.

任何与本文档建议内容背离的设计必须获得小桔汽车主管工程师的认可。

5.2.2 Network Requirement /网络需求

For reprogramming ECUs ,the transmission protocol can be LIN, CANFD, or DoIP. It is defined by Xiaoju Auto.

支持重编程的ECU，其传输协议可以为LIN，CANFD或者DoIP， 重编程ECU支持的通信传输协议由小桔汽车定义。

ECUs based on DOIP, refer to Q/DD B01194—2022 ;

ECUs based on CAN(FD), refer to Q/DD B01058—2022 ;

ECUs based on LIN, refer to Q/DD B01059—2022 ;
基于DOIP的ECU，诊断需求参考Q/DD B01194—2022 ；
基于CAN(FD)的ECU，诊断需求参考Q/DD B01058—2022 ；
基于LIN的ECU，诊断需求参考Q/DD B01059—2022 。

5.2.3 Hardware Requirement /硬件要求

The reprogrammable ECU shall provide enough memory to hold the downloading and provide adequate buffer space to meet the reprogramming timing requirements.

可重编程的ECU必须可提供足够的存储空间来保证下载，提供充足的缓冲空间来满足重编程时间的要求。

5.2.4 Software Requirement /软件要求

The FBL shall ensure the software controlling switching from boot software mode to application mode shall only be happened there is a valid application software image in the code flash in ECU. If the application software image is missing, or invalid or corrupted due to partially erasing or programming, then reprogramming shall stay in boot software mode, and allow downloading application software again in anytime.

FBL必须确保从引导软件模式切换到应用程序模式时，必须在ECU存在有效的应用程序软件时执行。如果由于部分擦除或编程导致应用程序软件丢失，无效或损坏，则重编程必须停留在引导软件模式下，并允许随时重新下载应用程序软件。

The boot software shall be stored in protected memory and cannot be reprogrammed to ensure that the ECU is always reprogrammable if there is a potential application error. Boot software shall contain protocol stacks which can ensure the reprogramming process be executed correctly.

FBL软件必须存储在受保护的内存中且禁止被更新，以确保应用程序软件潜在错误发生时，ECU始终可重编程。FBL软件必须包含确保重编程流程正确执行的协议栈。

All of programmable ECU, when running in the boot software mode, shall not be impacted by the normal communication of the other ECUs on the vehicle network. In general, no application IP messages shall be supported in the boot software mode.

所有可重编程ECU在引导软件模式下运行时不能受车辆网络上其他ECU正常通信的影响。对于以太网节点来说，在引导软件模式下不应支持任何基于IP的应用报文

The EOL related configuration data shall not be changed after ECU is reprogrammed successfully.

ECU重编程完成后，下线相关的配置数据必须不能被改变。

5.2.5 Security Requirement /安全需求

5.2.5.1 Security Access/安全访问

All reprogrammable ECU should support the security features of seeds and keys, and can be accessed through secure access services (27h), thereby protecting ECU is protected from unauthorized programming actions.

Security level 11h/12h is used for programming session mode, refer to Q/DD B01057—2022 for details.

The security access algorithm used by the 0x27 service refers to the ECU diagnostic function definition.

所有可重编程的ECU应该支持种子和密钥的安全特性，并且可以通过安全访问服务（27h）进入访问，从而保护ECU免遭未授权的编程动作影响。

安全等级11h/12h用于编程会话模式，详细的要求请参考Q/DD B01057—2022 。

安全解锁算法参考电控部件诊断功能定义文档。

5.2.5.2 Programming preconditions/编程预条件

The ECU should ensure that reprogramming is executed in a safe state. If programming preconditions are not met, reprogramming requests will be rejected.

Activate the test of ECU programming preconditions by routine control “Check Programming Precondition”, please refer to 7.3.1 for details.

ECU应该确保重编程的执行是处于安全状态。如果编程预条件不满足，那么重编程请求将被拒绝。

通过一个“检查编程预条件”例程控制来激活ECU编程预条件的检验，详细信息请参考7.3.1。

5.2.5.3 Integrity Verification/完整性验证

The ECU needs to check the integrity of the downloaded data. When a logical block is downloaded, the CRC32 algorithm is used to verify whether all the data bytes of the current logical block are correctly transmitted and written. Activate ECU integrity validation with a routine control “Check Memory Integrity”. When the ECU receives this service request, Boot software calculates the CRC32 value of the downloaded data and compares the results with the validation value sent in the diagnostic request message. For more information, please refer to 7.3.2.

ECU需要检查下载到存储器中的数据的完整性。当一个逻辑块下载后，将使用CRC32算法验证当前逻辑块的所有数据字节是否被正确传输和写入。通过一个“检查编程完整性”例程控制来激活ECU完整性验证。当ECU接收到此服务请求时，引导程序软件将计算下载数据字节的CRC32值，并将计算结果与诊断仪请求报文中发送的校验值进行比较，详细信息请参考7.3.2。

The ECU that follows the AUTOSAR architecture, the CRC module shall routine based on the IEEE-802.3 CRC32 Ethernet Standard as follow：

遵循AUTOSAR架构的ECU，CRC模块必须基于如下IEEE-802.3 CRC32以太网标准：

表1 CRC algorithm description/CRC 算法说明

CRC result widthCRC 结果长度	32bits
Polynomial 多项式	04C11DB7h
Initial value 初始值	FFFFFFFFh
Input data reflected 输入数据反映	Yes
Result data reflected 结果数据反映	Yes
XOR value 异或值	FFFFFFFFh
Check 检查	CBF43926h
Magic check*：魔法检查*：	2144DF1Ch

5.2.5.4 Dependency check/依赖性检查

Incompatible software must not be used together, and if used together, it can cause dysfunction or fatal errors. Therefore, the ECU should examine reprogramming dependencies by validating software compatibility, including applications and Bootloader, and data with applications and so on. Dependency checks are developed by the ECU supplier and should approved by Xiaoju Auto.

When the ECU receives a request for a routine control-" Check Programming Dependence ", the ECU performs the dependency check. Please refer to 7.3.2 for detailed definitions.

不兼容的软件不能配合使用，如果配合使用可能会使功能异常或产生致命性错误。因此，ECU应该通过验证软件兼容性来检查重编程依赖性，包括应用软件与引导程序软件、应用数据与应用软件等。依赖性检查机制由ECU供应商制定，并经得小桔汽车批准。

当ECU收到例程控制—“检查编程依赖性”诊断服务的请求时，ECU将执行依赖性检查。详细的定义请参考7.3.2。

5.2.5.5 Programming Attempt Counter/重编程计数

Each reprogramming ECU should store the reprogramming count in non-volatile memory. The reprogramming count describes the number of programming attempts. The ECU should set reprogramming count to 0 at the time of production. Once the memory erasure is performed, the reprogramming count increases by 1. The maximum number of reprogramming attempts shall be defined by the OEM and indicated in the ECU diagnostic specification.

Note: The reprogramming count can only increase by 1 per reprogramming event.

每个可重编程的ECU应将重编程计数存储于非易失性存储器。重编程计数描述了已执行重编程事件的次数。电控单元在生产时应置重编程计数为0。一旦执行存储器擦除操作，重编程计数增1。ECU最大可刷新次数应获得诊断工程师的认可并在ECU诊断规范中注明。

注：重编程计数在每次重编程事件中仅能增1。

5.2.5.6 Software validation/软件有效性验证

The ECU defines a flag bit to identify whether the application is valid. If the reprogramming integrity check and the reprogramming dependency check are correct, the ECU will set the flag position of the application to be valid. The application software can run only if the flag bit is valid, defining reference 7.3.2 in detail.

ECU内部定义一个标志位，用于标识应用软件是否有效。如果重编程完整性检查和重编程依赖性检查都正确，ECU将设置应用软件的标志位为有效。只有标志位为有效时，应用软件才可以运行，详细定义参考7.3.2。

5.2.5.7 Download Flash Driver/闪存驱动下载

The flash driver is a hardware-dependent module that provides the functionality of erasing and programming the ECU flash memory.

闪存驱动程序是一个硬件相关的模块，它提供了擦除和编程ECU闪存的功能。

The flash memory contents must be secured against unintended erasure and overwriting. Therefore, a software interlock mechanism is implemented in the bootloader code that stores critical code outside of the ECU memory. The complete flash driver code or critical parts

are not stored in the ECU flash memory but are downloaded into an ECU RAM buffer during the download procedure.

闪存内容必须防止意外的删除和覆盖。因此，必须将关键代码存储在ECU内存之外的FBL中以实现了软件联锁机制。完整的闪存驱动程序代码或关键部分并不存储在ECU闪存中，而是在下载过程中下载到ECU RAM缓冲区中。

After the download is completed the flash driver code shall be explicitly removed from the RAM buffer before the ECU returns to normal operation mode.

下载完成后，应在ECU恢复正常操作模式之前明确地从RAM缓冲区中删除闪存驱动程序代码。

Downloading flash drives into RAM when needed has the advantage of saving memory space. Additionally, on most microcontroller platforms, flash memory cannot be erased or programmed by code stored in flash memory or at least in the same flash bank.

当需要时将闪存驱动器下载进RAM中具有节省内存空间的优势。另外，对于大多数微控制器平台来说，闪存内存不能被存储于闪存内存中的或同一个闪存库中的代码擦写或重编程。

The flash driver shall provide a special API to be invoked by the FBL. At least the following four routines are required:

Initialization: The initialization routine is called by the FBL after the flash driver has been downloaded to the ECU to perform hardware specific initializations for flash programming.

De-Initialization: After the download is completed, the FBL calls the de-initialization to perform hardware-specific operations to finish flash programming.

Erase: The erase routine is called by the FBL to erase the requested flash area.

Write: All download data is programmed by the FBL using the write routine of the flash driver.

闪存驱动程序必须提供一个特殊的应用程序接口供FBL调用。至少需要以下四个例程:

初始化：在将闪存驱动程序下载到ECU后，FBL将调用初始化例程来执行针对闪存编程的特定硬件初始化。

反初始化：下载完成后，FBL调用反初始化来执行特定于硬件的操作来完成闪存编程。

擦除：擦除例程由 FBL 调用，以擦除所请求的闪存区域。

写入：所有下载数据是由 FBL 使用闪存驱动器的写例程进行编程。

5.2.5.8 I/O requirements/输入输出端口要求

When an ECU executes the FBL all I/O shall be set into state where components shall not be damaged and the area is safe for people working on the vehicle. The FBL shall also enable any I/O that is required to power other ECUs that support software download.

当ECU执行重编程时，必须将所有I/O设置为不应损坏组件的状态，并且该区域对于车辆上的工作人员是安全的。重编程还必须启用为支持软件下载的其他ECU供电所需的任何I/O。

5.2.5.9 Error Handling/容错处理

No matter due to the abnormal voltage, the abnormal communication, or the ECU is reset abnormally, or the flash device failure, once reprogramming sequence cannot be performed normally, the whole of the FBL download procedure shall always be started from the beginning after hard reset or power on reset, until the target application has been downloaded and flashed successfully.

无论是由于电压异常，通信异常，ECU异常复位，内存设备故障等导致无法正常完成重编程时序，硬复位或上电复位后，ECU必须始终可以从头开始整个重编程下载过程，直到有效的目标软件已成功下载并成功刷新为止。

When ECU failed in reprogramming and reentered FBL, the watchdog shall work properly.

ECU在重编程失败重新进入FBL时，必须保证看门狗工作正常。

ECU should improve the compatibility checking method, correctly identify the validity of the application so as to avoid the execution of invalid applications.

ECU应完善兼容性检查方法，正确识别应用程序的有效性，避免执行无效应用程序。

The application should ensure that the external reprogramming flag can be set to be valid by diagnostic request.

应用程序应保证可以通过诊断请求，将外部重编程标志位置为有效。

The ECU shall set the application flag invalid before erasing flash memory and cannot set the application flag valid until all reprogramming processes are performed correctly.

ECU必须先将应用程序有效标志位置为无效，再执行flash擦除操作，且在正确执行所有重编程流程前，不能将应用程序有效标志位置为有效。

5.2.6 Sleep Mode/睡眠模式

ECU shall not enter the sleep mode in the reprogramming process.

ECU在重编程过程中不能休眠。

The sleep mode in the FBL should be used to reduce power consumption when the ECU is idle and no diagnostic messages are received and no valid application could be started.

当ECU处于空闲状态，没有接收到任何诊断消息，也没有有效的应用程序可以启动时，应该进入FBL中的睡眠模式来降低功耗。

The FBL enters sleep mode after an internal sleep timer has expired. The initial value of the timer should be 300 seconds.

在内部睡眠定时器超时后，FBL进入睡眠模式。定时器的初始值应该为300秒。

The internal sleep timer is started during the FBL initialization procedure.

内部睡眠定时器在FBL初始化过程中启动。

With each diagnostic message received by the ECU the sleep timer is reset.

ECU接收到的每个诊断消息都将重置睡眠定时器。

When the sleep timer expires, the FBL shall enter the sleep mode. The sleep mode shall be implemented as required by the specific hardware in order to wake up correctly on any activity, e.g. Ethernet communication or ignition-on.

当睡眠定时器超时，FBL必须进入睡眠模式。睡眠模式必须根据特定硬件的要求来实现，以便在任何活动(如以太网通信或启动)中可以被正确唤醒。

5.2.7 Source File Format Requirement/源文件格式要求

Xiaoju Auto recommend that the format of source file should be the intel Hex format (*.hex) or the Motorola format (*. s19). The starting address, length, and type of each data block in the source file (e.g. application software or calibrated data, etc.) should be described in the description document, the document should be released with the source file.

发布给小桔汽车的源文件格式是Intel格式（*.hex）或者Motorola格式（*.s19）。源文件中每个数据块的起始地址、长度以及类型（例如：应用软件或标定数据等）应在描述文档中进行说明，一份描述文档应和源文件一同释放。

5.2.8 Gateway ECU Requirements/网关 ECU 要求

According to the communication protocol supported by the gateway, the diagnostic requirements of Gateway refer to Q/DD B01195—2022,Q/DD B01059—2022,and Q/DD B01055—2022 for the definition of routing requirements.

依据网关支持的通信协议，网关ECU的诊断需求参考Q/DD B01195—2022,Q/DD B01059—2022和Q/DD B01055—2022中相关章节关于路由需求的定义。

The diagnostic request for a functional address needs to be processed and routed, even if the gateway itself is being reflashed.

功能寻址的诊断请求网关需要处理，也必须被路由，即使是网关节点自身在被刷写。

If the gateway enters its bootloader for reprogramming, the bootloader in a gateway shall route or generate TesterPresent（3Eh） messages on the networks connected to the gateway.

如果对网关节点自身进行重编程,网关的Bootloader必须在其连接的各个网段上发出诊断在线报文（3Eh）。

6 UDS Services/UDS 服务

6.1 Defition of UDS Services/UDS 服务定义

Below UDS services and sub-functions shall be supported by all ECUs' FBL. the 1st column describe the UDS service and sub-function parameter which shall be support, the 2nd column describe the protocol control information which shall be supported; the 3rd and 4th columns to define if this service and sub-function shall be supported in the physical addressing mode or functional addressing mode respectively; the columns from 5th to 7th defines , if the current active diagnostic session mode is default mode , programming mode, or extended mode , whether this service and the relating sub-function shall be supported or not in this platform. The 8th column describes the security access requirement of this service.

所有ECU的FBL必须支持以下UDS服务和子功能。第1列描述了必须支持的UDS服务及子功能参数，第2列描述了刷写服务必须支持的相对应的协议控制信息。第3列和第4列分别定义在物理寻址模式或功能寻址模式下是否必须支持该服务和子功能;第5到7列定义了,如果当前活动的诊断会话模式是默认模式,编程模式或扩展模式，则此平台是否必须支持此服务和相关的子功能。第8列定义了该服务是否需要安全访问解锁后才可以执行。

表2 UDS service in FBL/FBL 下的 UDS 服务

DiagnosticServiceDescription 诊断服务描述 Sub function Parameter 子功能参数	Hex value 十六进制值	Phy Req 物理寻址.	Func Req 功能寻址	Supported in session 支持的会话			Security Access 安全访问
				$01 默认会话	$02 编程会话	$03 扩展会话	
DiagnosticSessionControl 诊断会话控制	10						
Default Session 默认会话	10 01	√	√	√	√	√	-
Programming Session 编程会话	10 02	√	-	-	√	√	-
Extended Session 扩展会话	10 03	√	√	√	-	√	-
ECUResetECU 复位	11						
Power On Reset 电源复位	11 01	√	√	√	√	√	-
ReadDataByIdentifier 通过数据标识符读服务	22						
Data Identifier 数据标识符	22 xx yy	√	-	√	√	√	-
SecurityAccess 安全访问	27						
Request Seed (for reprogramming) 请求种子（用于重编程）	27 11	√	-	-	√	-	-
Send Key (for reprogramming) 发送秘钥（用于重编程）	27 12	√	-	-	√	-	-
CommunicationControl 通信控制	28						
DisableRxAndTx 禁止发送和接收	28 03 03	√	√	-	-	√	-
EnableRxAndDisableTx 使能接收和禁止发送	28 01 03	√	√	-	√	-	
EnableRxAndTx 使能发送和接收	28 00 03	√	√	-	-	√	-
WriteDataByIdentifier 通过标识符写服务	2E						
ApplicationSoftwareFingerprintDataIdentifier 应用程序指纹数据标识	2E F0 12	√	-	-	√	-	√
RoutineControl 例程控制	31						
CheckProgrammingPreconditions 检查预编程条件	31 01 02 00	√	√	-	-	√	-
Start Erase Memory 启动擦除内存	31 01 FF 00	√	-	-	√	-	√
Start Check Routine 启动检查例程	31 01 02 01	√	-	-	√	-	√

表2 UDS service in FBL/FBL 下的 UDS 服务（续）

DiagnosticServiceDescription 诊断服务描述	Hex value 十六进制值	Phy Req 物理寻址.	Func Req 功能寻址	Supported in session 支持的会话			Security Access 安全访问
Sub function Parameter 子功能参数				$01 默认会话	$02 编程会话	$03 扩展会话	
CheckProgrammingDependencies 检查编程依赖性	31 01 FF 01	√	-	-	√	-	√
RequestDownload 请求下载服务	34						
No sub functionparameter 无子功能参数	-	√	-	-	√	-	√
TransferData 数据传输服务	36						
Block Sequence Counter 逻辑块序列数	36 xx	√	-	-	√	-	√
RequestTransferExit 退出数据传输	37						
No sub function parameter 无子功能参数	-	√	-	-	√	-	√
Tester Present 诊断仪在线	3E						
ZeroSubFunction 子功能参数	00	√	√	√	√	√	-
	80	√	√	√	√	√	-
ControlDTCSetting 控制 DTC 设置	85						
DTCSettingType = on DTC 设置类型=开启	85 01	√	√	-	-	√	-
DTCSettingType = off DTC 设置类型=关闭	85 02	√	√	-	-	√	-
Note: √ in the table means support. 注：表格中的√代表支持。							

Below UDS services and sub-functions shall be supported by all ECUs' App. the 1st column describe the UDS service and sub-function parameter which shall be support, the 2nd column describe the protocol control information which shall be supported; the 3rd and 4th columns to define if this service and sub-function shall be supported in the physical addressing mode or functional addressing mode respectively; the columns from 5th to 7th defines , if the current active diagnostic session mode is default mode , programming mode, or extended mode , whether this service and the relating sub-function shall be supported or not in this platform. The 8th column describes the security access requirement of this service.

所有ECU的App必须支持以下UDS服务和子功能。第1列描述了必须支持的UDS服务及子功能参数，第2列描述了服务必须支持的相对应的协议控制信息。第3列和第4列分别定义在物理寻址模式或功能寻址模式下是否必须支持该服务和子功能；第5到7列定义了，如果当前活动的诊断会话模式是默认模式，编

程模式或扩展模式，则此平台是否必须支持此服务和相关的子功能。第8列定义了该服务是否需要安全访问解锁后才可以执行。

表3 UDS service in APP/APP 下的 UDS 服务

DiagnosticServiceDescription 诊断服务描述 Sub function Parameter 子功能参数	Hex value	Phy Req 物理寻址.	Func Req 功能寻址	Supported in session 支持的会话		Securiy Access 安全访问
				$01 默认会话	$03 扩展会话	
DiagnosticSessionControl 诊断会话控制	10					
Default Session 默认会话	10 01	√	√	√	√	-
Programming Session 编程会话	10 02	√	-	-	√	-
Extended Session 扩展会话	10 03	√	√	√	√	-
ECUResetECU 复位	11					
Power On Reset 电源复位	11 01	√	√	√	√	-
ReadDataByIdentifier 通过数据标识符读服务	22					
Data Identifier 数据标识符	22 xx yy	√	-	√	√	-
CommunicationControl 通信控制	28					
DisableRxAndTx 禁止发送和接收	28 03 03	√	√	-	√	-
EnableRxAndDisableTx 使能接收和禁止发送	28 01 03	√	√	-	√	-
EnableRxAndTx 使能发送和接收	28 00 03	√	√	-	√	-
RoutineControl 例程控制	31					
CheckProgrammingPreconditions 检查预编程条件	31 01 02 00	√	√	-	√	-
Tester Present 诊断仪在线	3E					
ZeroSubFunction 子功能参数	00	√	√	√	√	-
	80	√	√	√	√	-
ControlDTCSetting 控制 DTC 设置	85					
DTCSettingType = on DTC 设置类型=开启	85 01	√	√	-	√	-
DTCSettingType = off DTC 设置类型=关闭	85 02	√	√	-	√	-
Note: √ in the table means support. 注：表格中的√代表支持。						

UDS Services with sub-function are shown below:
使用 UDS 子功能的服务如下表所示：

表4 Diagnostic services with sub-function parameters/使用子功能的 UDS 服务

Diagnostic Service Description 诊断功能描述	SID（Hex） 服务标识符（Hex）
DiagnosticSessionControl 诊断会话模式切换	10
ECUReset ECU 复位	11
SecurityAccess 安全访问	27
CommunicationControl 通信控制	28
RoutineControl 例程控制	31
Tester Present 诊断仪在线	3E
ControlDTCSetting DTC 控制	85

Although the UDS specification Q/DD B01057—2022 defines that all services can be functional addressing. Table 3 restricts the addressing types of single services (e.g. 0x10 02) to physical only. If the tester sends an “invalid” functional request, the ECU shall ignore this request.

虽然规范Q/DD B01057—2022定义了所有服务都可以进行功能寻址，但表3将单一服务的寻址类型（例如0x10 02）限制为仅物理寻址，如果诊断仪发送“无效”功能请求，则ECU必须忽略该请求。

For all of the ECUs which is supporting the FBL downloading features, when the software running mode is switched from the FBL boot software running mode into application running mode or exit the boot software mode by service 0x11, shall use the 0x11 01 hard reset, i.e. the initialization result of reset shall be same as the power on reset.

对于所有支持FBL下载功能的ECU，当使用0x11服务实现软件运行模式从FBL引导软件运行模式切换到应用程序运行模式或退出引导软件模式时，必须使用0x11 01硬复位，即复位的初始化结果必须与上电复位一致。

If the ECU supporting the FBL cannot support the 0x11 01 hard reset, but only 0x11 03 soft reset, then this shall be confirmed with Xiaoju Auto, and allowed by Xiaoju Auto.

如果支持FBL的ECU无法支持0x11 01硬复位，而只能支持0x11 03软复位，则必须与小桔汽车确认，并由小桔汽车允许。

The below sub functions for the requesting seeds and the submitting keys shall be supported: 0x03, and 0x04. Please refer to Q/DD B01057—2022 for details of 0x27 service.

ECU必须支持以下用于请求种子和提交密钥的子功能： 0x03和0x04。0x27服务相关定义请参考Q/DD B01057—2022 。

ECU shall support the DataFormatIdentifier value of service 0x34 to be set as 0x00.

ECU必须支持0x34服务的DataFormatIdentifier值为0x00。

The addressAndLengthFormatIdentifer of 0x34 shall be 0x44, that means the MemoryAddress parameter and MemorySize parameter of 0x34 shall be 4 Byte.

0x34的addressAndLengthFormatIdentifer必须为0x44，这意味着MemoryAddress参数和0x34的MemorySize参数必须为4字节。

The MemoryAddress parameter shall represent a physical address location within the ECU. However, if the address parameter does not correspond to the physical location, this parameter shall be filled with 0x00.

MemoryAddress参数必须表示ECU中的物理地址位置。如果address参数与物理位置不对应，则该参数必须填充0x00。

6.2 Data Identifiers/数据标识符

ReadDataByIdentifier“FingerPrint” (0xF013).

通过DID读取“指纹”数据（0xF013。

表5 Read FingerPrint request/读取指纹数据请求

Data byte 字节	Parameter Name 参数名称	Hex Value 十六进制
#1	ReadDataByIdentifier Request Service ID	22
#2	FingerPrint DID(HByte)	F0
#3	FingerPrint DID(LByte)	13

表6 Read FingerPrint Response/读取指纹数据响应

Data byte 字节	Parameter Name 参数名称	Hex Value 十六进制
#1	ReadDataByIdentifier Response Service ID	62
#2	FingerPrint DID(HByte)	F0
#3	FingerPrint DID(LByte)	13
#4	blockID 0	00 - FF
#5	programmingDate YY (byte 0, BCD-coded)	00 - 99
#6	programmingDate MM (byte 1, (BCD-coded)	01 - 12
#7	programmingDate DD (byte 2, BCD-coded)	01 - 31

表6 Read FingerPrint Response/读取指纹数据响应（续）

Data byte 字节	Parameter Name 参数名称	Hex Value 十六进制
#8-13	TesterSerialNumber	00 - FF
#14	blockID 1	00 - FF
#15	programmingDate YY (byte 0, BCD-coded)	00 - 99
#16	programmingDate MM (byte 1, (BCD-coded)	01 - 12
#17	programmingDate DD (byte 2, BCD-coded)	01 - 31
#18-23	TesterSerialNumber	00 - FF
…	…	…
#4+(N-1)*10	blockID N-1	00 - FF
…	…	…

WriteDataByIdentifier“FingerPrint” (0xF012).

通过DID写入“指纹”数据（0xF012）。

表7 Write FingerPrint request/写入指纹数据请求

Data byte 字节	Parameter Name 参数名称	Hex Value 十六进制
#1	WriteDataByIdentifier Request Service ID	2E
#2	FingerPrint DID(HByte)	F0
#3	FingerPrint DID(LByte)	12
#4	programmingDate YY (byte 0, BCD-coded)	00 - 99
#5	programmingDate MM (byte 1, (BCD-coded)	01 - 12
#6	programmingDate DD (byte 2, BCD-coded)	01 - 31
#7-12	TesterSerialNumber	00 - FF

表8 Write FingerPrint response/写入指纹数据响应

Data byte 字节	Parameter Name 参数名称	Hex Value 十六进制
#1	WriteDataByIdentifier Response Service ID	6E
#2	FingerPrint DID(HByte)	F0
#3	FingerPrint DID(LByte)	12

ReadDataByIdentifier“ECUType” (0xF1D9).

通过DID读取“ECU类型”（0xF1D9。

表9 Read ECUtype request/读取 ECU 类型请求

Data byte 字节	Parameter Name 参数名称	Hex Value 十六进制
#1	ReadDataByIdentifier Request Service ID	22
#2	ECUType DID(HByte)	F1
#3	ECUType DID(LByte)	0E

表10 Read ECUtype response/读取 ECU 类型响应

Data byte 字节	Parameter Name 参数名称	Hex Value 十六进制
#1	ReadDataByIdentifier Response Service ID	62
#2	ECUType DID(HByte)	F1
#3	ECUType DID(LByte)	0E
#4	ECU Type ECU with file system (such as Linux, QNX, Android) ECU without file system	 00 01

6.3 Routines/例程

The flash shall be erased before data download. 在下载数据之前必须先擦除内存。

表11 Erase flash memory request/擦除内存请求

Data byte 字节	Parameter Name 参数名称	Hex Value 十六进制
#1	RoutineControl Request Service Id	31
#2	routineControlType startRoutine	 01
#3 - #4	routineIdentifier eraseMemory	 FF00
#5	addressAndLength FormatIdentifier lengthFormat: bit 7 - 4: number of bytes of the memorySize parameter addressFormat: bit 3- 0: number of bytes of the memoryAddress parameter Recommended fix value	 0x - 4x x0 - x4 44
#6-n1	memoryAddress 1 - 4 bytes erase address	00 - FF
#n2-n3	memorySize 1 - 4 bytes erase size	00 - FF

表12 Erase flash memory response/擦除内存响应

Data byte 字节	Parameter Name 参数名称	Hex Value 十六进制
#1	RoutineControl Response Service Id	71
#2	routineControlType startRoutine	 01
#3 - #4	routineIdentifier eraseMemory	 FF00
#5	routineStatusRecord correctResult incorrectResult	 00 01

ECU shall check the programming dependency by verifying the software compatibility, including application software with the FBL software, the application data with the application software. The dependency check mechanism is defined by the ECU supplier and shall be approved by the Xiaoju Auto diagnostic engineer.

ECU必须通过验证软件兼容性来检查编程依赖性，包括与FBL软件一起使用的应用程序软件，与应用程序软件一起的应用程序数据。依赖性检查机制由ECU供应商定义，并必须由小桔汽车诊断工程师批准。

表13 Check programming dependency request/检查编程依赖性请求

Data byte 字节	Parameter Name 参数名称	Hex Value 十六进制
#1	RoutineControl Request Service Id	31
#2	routineControlType startRoutine	 01

Data byte 字节	Parameter Name 参数名称	Hex Value 十六进制
#3 - #4	routineIdentifier checkProgrammingDependency	 FF01

表14 Check programming dependency response/检查编程依赖性响应

Data byte 字节	Parameter Name 参数名称	Hex Value 十六进制
#1	RoutineControl Response Service Id	71
#2	routineControlType startRoutine	 01
#3 - #4	routineIdentifier checkProgrammingDependency	 FF01
#5	routineStatusRecord correctResult incorrectResult	 00 01

Check FBL PreCondition (0x0200) Used to check if the environment conditions mean that the ECU shall confirm that the ECU is safety and do not threat to the safety of personnel and actuator and vehicle, and confirm the memory before to execute actual programming actions.

检查编程预条件（0x0200）用于检查环境条件，意味着ECU必须确认ECU是安全的，并且不会威胁到人员，执行器和车辆的安全，并在执行实际编程操作之前确认内存。

表15 Check programming precondition request/检查编程预条件请求

Data byte 字节	Parameter Name 参数名称	Hex Value 十六进制
#1	RoutineControl Request Service Id	31
#2	routineControlType startRoutine	 01
#3 - #4	routineIdentifier checkFBLPreCondition	 0200

表16 Check programming precondition response/检查编程预条件响应

Data byte 字节	Parameter Name 参数名称	Hex Value 十六进制
#1	RoutineControl Response Service Id	71
#2	routineControlType startRoutine	 01
#3 - #4	routineIdentifier checkFBLPreCondition	 0200
#5	routineStatusRecord correctResult incorrectResult	 00 01

检查编程预条件例程控制需要检查车速，发动机/电机转速，电源模式，档位信息以及手刹状态（EPB卡钳夹紧），具体条件参考电控部件诊断功能定义文档。如果任何以上条件的检查结果不满足，需要使用NRC 0x22回复。

The programming precondition routine control should check the vehicle speed, Motor speed, power mode ,Gear information and brake status (EPB status: Closed) , refer to ECU Diagnostic function definition. If any of the conditions cannot match the requirement from Xiaoju Auto, NRC code 0x22 should be sent.

没有文件管理系统的可重编程ECU必须检查内存驱动器及软件数据的完整性。下载内存驱动程序或软件数据后，将使用CRC32算法（参考5.2.5.3）来确保内存驱动程序或软件数据的所有数据均已正确传输和写入。收到此服务后，FBL将计算下载的数据字节的CRC32值。将结果值与在服务请求消息中发送的相应值进行比较。

Without the file management system, the reprogrammable ECU shall check the integrity of flash driver and app data. After flash driver or app data download, a CRC32 algorithm (Please refer to chapter 5.2.5.3) is used to ensure that all data of flash driver or app have been transferred and written correctly. After receiving this service, the FBL would calculate the CRC32 value of the downloaded data bytes. The resulting value is compared with corresponding value, which is transmitted in the service request message.

表17 Check memory integrity request/检查内存完整性请求

Data byte 字节	Parameter Name 参数名称	Hex Value 十六进制
#1	RoutineControl Request Service Id	31
#2	routineControlType startRoutine	 01
#3 - #4	routineIdentifier checkMemoryIntegrity	 0201
#5~#8	CRC value, 4 bytes	00 - FF

表18 Check memory integrity response/检查内存完整性响应

Data byte 字节	Parameter Name 参数名称	Hex Value 十六进制
#1	RoutineControl Response Service Id	71
#2	routineControlType startRoutine	 01
#3 - #4	routineIdentifier checkMemoryIntegrity	 0201
#5	routineStatusRecord correctResult incorrectResult	 00 01

7 Reprogramming Progress/重编程流程

7.1 General Information/概述

本章定义了将一个或多个应用程序软件或应用程序数据下载到ECU内存中的ECU重新编程流程。

This chapter defines reprogramming process for the ECU download of one or multiple application software or application data into ECU memory.

7.2 Bootloader Startup Sequence /Bootloader 启动时序

Figure 1 is FBL startup sequence; this type of sequence is generally applied to ECU without file management system.

图1是FBL的启动时序，这种时序通常应用于没有文件管理系统的ECU。

In the application mode, there exist two diagnostic sessions: default session, extended session. In the Boot software mode, there exist three diagnostic sessions: default session, extended session and programming session.

在应用程序模式下，存在两个诊断会话：默认会话，扩展会话。在Boot软件模式下，存在三个诊断会话：默认会话，扩展会话和编程会话。

From the point view of diagnostic session, the entering into programming session, shall via extended session, which means ECU doesn't support switch from default session to programming session directly. The same, ECU doesn't support switch from programming session to extend session directly.

从诊断会话的角度来看，进入编程会话必须通过扩展会话进行，这意味着ECU不支持直接从默认会话切换到编程会话。同样，ECU不支持从编程会话直接切换为扩展会话。

If ECU has received "0x10 02" in the correct condition, the ECU shall set external reprogramming flag valid and perform ECU reset internal.

如果ECU在正确的条件下收到"0x10 02"，则ECU必须设置外部重编程标志位为有效，并在内部执行ECU复位。

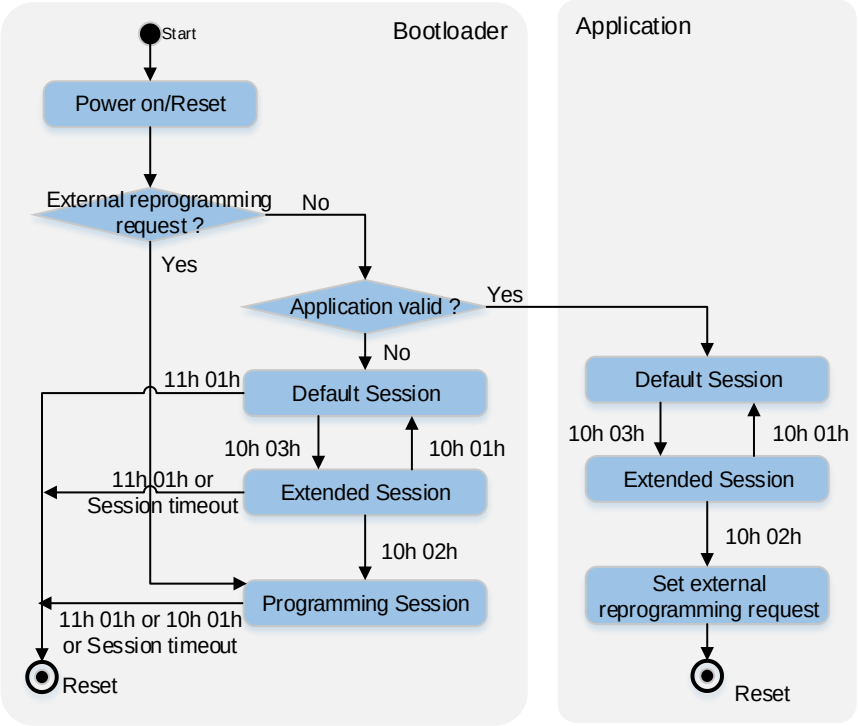

图1　FBL 启动时序/FBL startup sequence

After a power on or reset, firstly ECU shall start up the FBL, then check the external reprogramming flag;

上电或复位后，首先ECU必须启动FBL，然后检查外部重编程标志；

If the external reprogramming flag is valid, then enter the programming session of the Boot software mode despite application valid or not. Then, the external reprogramming flag shall be set to invalid after ECU enter programming session immediately;

如果外部重编程标志有效，则不管应用程序有效与否，都进入Boot软件模式的编程会话。然后，外部重编程标志必须立即设置为无效；

If the external reprogramming flag is invalid, then check the validity of application;

如果外部重编程标志无效，则检查应用程序的有效性；

If the Application is valid, then the application is started in default session;

如果应用程序有效，则进入应用程序的默认会话；

If the application is invalid, then keep in the Boot software mode, and the ECU enter default session;

如果应用程序无效，则保持在Boot软件模式下，同时ECU进入默认会话模式；

In the Boot software mode, the diagnostic session switching rule is the same with that in application mode;

在Boot软件模式下，诊断会话切换规则与在应用程序模式下相同。

In the Boot software mode, there are some ways that can lead to ECU reset:

1. “0x11 01” shall lead ECU reset in spite of the current session;
2. S3server timeout shall lead ECU reset if in extend session and programming session;
3. “0x10 01” shall lead ECU reset if in programming session.

在Boot软件模式下，有几种方法可以导致ECU复位：

1. 在任何会话模式下，“ 0x11 01”都必须导致ECU复位；
2. 如果在扩展会话和编程会话中，S3server超时必须导致ECU复位；
3. 编程会话模式下，“ 0x10 01”必须导致ECU复位。

Note： The software should have the policy of Secure Boot, the implementation Progress should be informed to Xiaoju Automobile diagnosis engineer.

注：软件应该具备secure boot的策略，具体的实现方式需要告知小桔汽车诊断工程师。

7.3 Rprogramming Sequence/重编程流程

This reprogramming sequence is generally applied to ECU based on Embedded System (without file management system). The reprogramming sequence is divided into 3 phases:

Pre-programming step: setup of network for programming;

Programming step: data transmission and software installation;

Post-Programming step: Re-synchronize of network.

本章重编程时序通常适用于基于嵌入式系统的ECU（无文件管理系统）。重编程时序分为三个阶段：

预编程阶段：重编程网络准备；

重编程阶段：数据传输及软件安装；

后编程阶段：重新同步网络。

These three phases are described in detail in the following chapters. In the sequences depicted in Figure 2 and Figure4, the orange block represents physical addressing, green block represents functional addressing.

For LIN node, LIN master shall route the functional or physical addressed request to LIN slave, the LIN diagnostic routing process can refer to Q/DD B01059—2022.

For DoIP node, Tester (or other reprogramming client) shall send functional addressing request to all the DoIP nods in turn.

以下各章将详细介绍这三个阶段。如图2和图4所示的时序中，橘色色表示物理寻址，绿色表示功能寻址。

对于LIN节点， 需要由LIN主节点将功能寻址或物理寻址的诊断请求路由给LIN从节点，LIN诊断路由过程可以参考Q/DD B01059—2022。

对于DoIP节点，诊断仪需要向所有DoIP节点逐个发送功能寻址请求。

7.3.1 Pre-programming Step/预编程阶段

The pre-programming step is used to prepare the network for a programming of ECU. The request messages of this step contain the physically addressing requests and functionally addressing requests. If any errors occur in pre-programming step with the physical addressing request and response, then all the sequence shall be repeated.

The pre-programming step is shown in Figure 2.

预编程阶段用于为ECU重编程准备网络。此步骤的请求报文包含物理寻址请求和功能寻址请求。物理寻址的请求和响应发生任何错误，则必须重新执行所有时序。

预编程阶段如图2 所示。

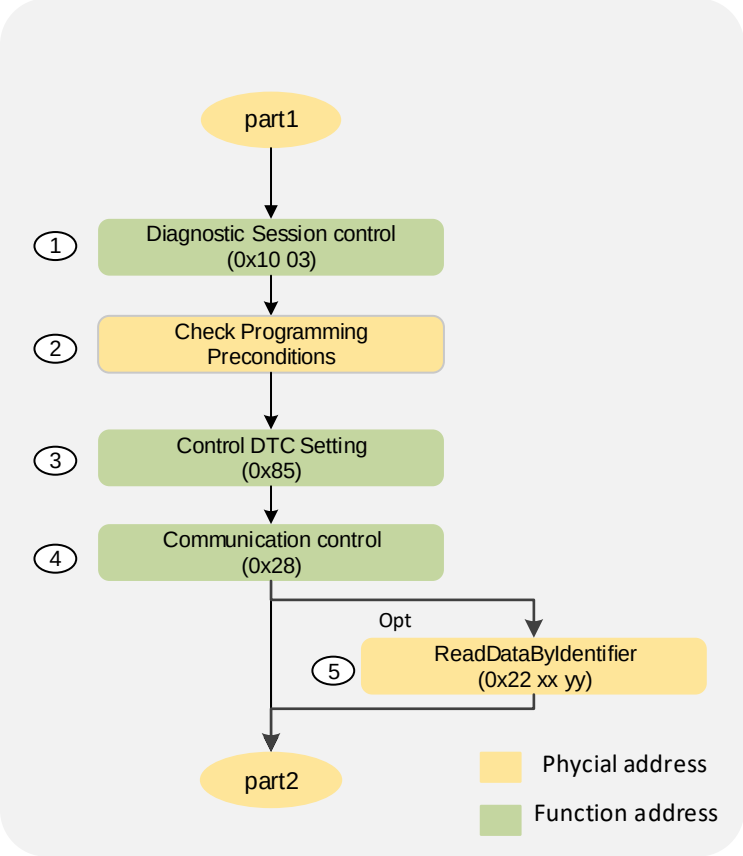

图2　预编程阶段/ Pre-programming step

Step 1: DiagnosticSessionControl 0x10 03: In order to disable the setting of DTCs and communication, it shall be required to start a non-default session for all ECU. Therefore, the request is functionally addressed. Tester shall continue to periodically transmit the Tester-Present request (0x3E 80) to maintain the non-default diagnostic session mode of all ECUs using functional address, after enter extendedDiagnosticSession.

The LIN slave node shall not give any response to this functional addressing DiagnosticSessionControl 0x10 03 request even though it supports.

步骤1：诊断会话控制 0x10 03：为了禁用DTC设置和通信，所有ECU都必须启动一个非默认会话模式。因此，该请求是一个功能寻址的请求。在进入拓展诊断会话之后，诊断仪必须继续定期通过功能寻址发送“诊断仪在线”请求（0x3E 80），以维持所有ECU的非默认诊断会话模式。

LIN从节点不应该响应功能寻址请求，即使支持0x10 03请求。

Step 2: RoutineControl – “Check FBL PreCondition” 0x31 01 02 00: this routine is inquiring ECU the condition for programming to ensure the system safety, the condition is estimated by ECU, if there have any insecurity factor, the ECU shall reject programming.

Note: If the ECU does not receive the Checking Programming Preconditions routine (0x31 01 02 00), but received ″0x10 02 request, the ECU should refuse to enter the Bootloader and send a negative response.

The LIN master mode is responsible for periodically sending programming conditions, the conditions shall be set as part of network design.

步骤2：例程控制-“检查编程预条件”0x31 01 02 00：该例程通过查询ECU的编程条件以确保系统安全，该条件由ECU估算，如果有任何不安全因素，则ECU必须拒绝编程。

注意：如果ECU在未收到“检查编程预条件”例程（0x31 01 02 00）的情况下，收到“0x10 02”请求，ECU应该拒绝进入Bootloader模式，并且发送否定响应。

LIN主节点能够周期性发送用于LIN从节点的预编程条件，应将其设置为网络设计的一部分。

Step 3: ControlDTCSetting 0x85 02: the tester disables the setting of DTCs in each ECU using the ControlDTCSetting (0x85) service with DTCSettingType equal to “off”. The request is functionally addressed.

The LIN slave node shall not give any response to this functional addressing ControlDTCSetting 0x85 02 request even though it supports.

步骤3：控制DTC设置 0x85 02：诊断仪使用DTC设置类型等于“关”的控制DTC设置（0x85）服务禁用每个ECU中DTC的设置。该请求是一个功能寻址的请求。

LIN从节点不应该响应功能寻址请求，即使支持0x85 02请求。

Step 4: CommunicationControl 0x28 01 03: Tester shall inhibit transmit and receive all normal communication message. The request is functionally addressed.

LIN master node shall stop normal communication schedule and switch to diagnostic only mode. By switching to diagnostic only mode, the full bandwidth of the bus is available for the download and the download is not disturbed by non-diagnostic messages. The LIN slave node shall not give any response to this functional addressing method 0x28 01 03 request even though it supports.

步骤4：通信控制0x28 01 03：诊断仪必须禁止发送和接收所有正常的通信消息。该请求是一个功能寻址的请求。

LIN主节点应该停止正常通信调度，切换至纯诊断调度模式。这样可以保证LIN总线全部用于刷写调度。LIN从节点不应该响应功能寻址请求，即使支持0x28 01 03请求。

Step 5(Option): The ReadDataByIdentifier service is optional and used to acquire identification information from the ECU that is be reprogrammed. ECU identification information is applied by the flash process infrastructure to determine the suitable software update that shall be programmed and to document the download event.

步骤5（可选）：ReadDataByIdentifier服务是可选的，用于重新编程的ECU获取标识信息。ECU标识信息由刷写流程使用，以便确定必须被重编程的适当软件更新并记录下载事件。

7.3.2 Programming Step/重编程阶段

Following the pre-programming step, the programming of ECU is performed. The programming sequence applies for a programming event of a single ECU and is therefore physically oriented.

If an error occurs in steps 6), 7), 13) retry the service; If an error occurs in step 8) - step 12), restart execution from step 8). After a failure, the number of reattempts to flash shall not exceed 2 times.

在预编程阶段之后，执行ECU的重编程阶段。该重编程时序适用于单个ECU的编程事件，因此是物理寻址的。

如果步骤6）、7）、13）发生错误，则重新尝试该服务；步骤8）-步骤12）发生错误，则从步骤8）重新开始执行。失败后重新尝试刷写的次数不能超过2次。

Figure 3 graphically depicts the functionality embedded in the programming step.
图3以图表方式描绘了重编程阶段中的各个步骤。

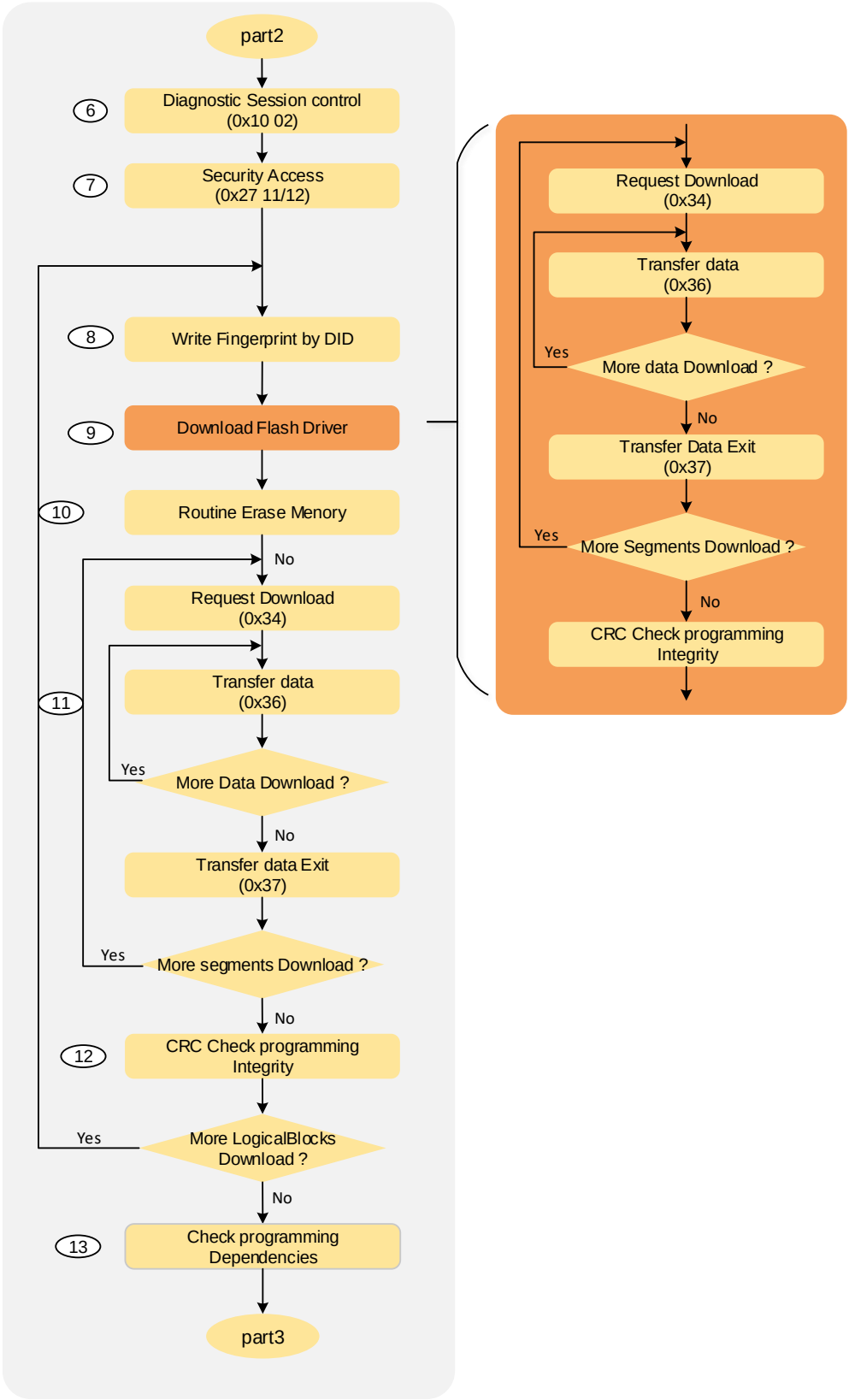

图3 编程阶段/ Programming step

Step 6: DiagnosticSessionControl 0x10 02: The programming event is started in the ECU via a physically addressed request of the DiagnosticSessionControl (0x10) service with session type equal to programmingSession. When the ECU receive the request, it shall allocate all necessary resources required for programming. The positive response shall give and the external reprogramming flag shall be set to valid before ECU performs the action of switching into programming session.

When performing the reprogramming process based on DoIP, tester Tester (or other reprogramming client) shall establish TCP link within 4s after receiving the positive response of session control. After the TCP link is established, routing activation shall be performed. Just 1 time of routing activation shall be allowed.

After a successful session mode switch, the external reprogramming flag shall be set to invalid.

步骤6：诊断会话控制0x10 02：重编程事件通过物理寻址的诊断会话控制（0x10）服务请求在ECU中启动，会话类型等于编程会话。当ECU收到请求时，它必须分配编程所需的所有必要资源。在ECU执行进入编程会话的动作之前，必须先给出肯定响应，并将外部重编程标志位置为有效。

采用DoIP协议执行重编程流程时，诊断仪（或其他上位机）在收到模式切换正响应后，必须在4s内建立TCP连接。TCP连接建立完成后必须进行路由激活，路由激活尝试次数必须仅为1次。

完成会话模式切换后，外部重编程标志位必须被置为无效。

Step 7: SecurityAccess 0x27 11/12: A programming event shall be secured. The security access process is mandatory before download, and the security access can ensure only valid tester can download the ECU.

步骤7：安全访问0x27 11/12：编程事件必须是受保护的。下载之前必须执行安全访问过程，安全访问可以确保只有有效的诊断仪才能对ECU执行下载。

Step 8: WriteDataByIdentifier 0x2E F0 12: It is mandatory to write a “fingerprint” into the ECU memory prior to erase routine. The “fingerprint” identifies the related information when modifies the ECU memory. Before logic block (except driver) download, the tester shall write “fingerprint”. When trace the “fingerprint” of logic blocks, tester shall send “0x22 F013”, and the ECU shall give logic block fingerprint via “0x62 F013....”, the detailed format please see chapter 6.2.

步骤8：通过DID写指纹 0x2E F0 12：必须在擦除程序之前将“指纹”写入ECU存储器。“指纹”标识了修改ECU内存时的相关信息。在下载逻辑块（驱动程序除外）之前，诊断仪必须写入“指纹”。跟踪逻辑块的“指纹”时，诊断仪必须发送“ 0x22 F013”，ECU必须通过“ 0x62 F013 ....”给出逻辑块指纹，详细格式请参见6.2章。

Step 9: Download of Driver 0x34, 0x36, 0x37, and 0x31: This is a mandatory step to download the flash driver into the designated RAM buffer of the ECU. This step consists of several service requests, RequestDownload, TransferData and RequestTransferExit. After all bytes are transferred, a verification procedure is started with a “Check Memory Integrity” Routine (0x31 01 02 01) to ensure that all bytes are download correctly.

步骤9：下载驱动程序0x34、0x36、0x37和0x31：ECU必须执行驱动程序下载步骤，将驱动程序下载到指定的RAM缓存区。使用到0x34, 0x36, 0x37和0x31服务。当下载完所有字节后，将使用“检查内存完整性”例程（0x31 01 02 01）来检查所有字节的下载是否正确。

Step 10: RoutineControl – “Erase Flash Memory” 0x31 01FF 00: The memory of the ECU shall be erased in order to allow application software or data download. This is achieved via the routine, using the RoutineControl (0x31) service to execute the erase routine. Before the erase routine of the flash driver is called, the validity status of the logical block shall be set to invalid. Before erasing the memory, if the fingerprint is not written to the ECU memory, the erasing routine control should be rejected.

Note: The erasure is performed in logical blocks, and if multiple logical blocks are continuous in the address space, they can be considered as one logical block; Otherwise, it should be thought of as multiple different logical blocks, and need to be erased separately.

步骤10：例程控制 - “擦除内存” 0x31 01 FF 00：ECU的存储器必须被擦除，以允许应用软件或数据下载。这可以通过使用例程（0x31）服务执行擦除例程的例程来实现。如果调用了擦除存储器例程，则必须将应用程序有效标志位置为无效。在内存驱动的擦除例程被调用前，逻辑块的有效状态必须被置为无效。在擦除程序之前，若“指纹”未写入ECU存储器，则应拒绝擦除例程执行。

注：擦除内容以逻辑块为单位执行，若多个逻辑块在地址空间上是连续的，可视作一个逻辑块；否则应视作不同的逻辑块分多次擦除。

Step 11: Download Process 0x34, 0x36, 0x37: All segments of a logical block are downloaded to the ECU by a sequence of the services RequestDownload, TransferData and RequestTransferExit. The download of one segment that consists of a contiguous set of data bytes is started with a RequestDownload service request. The RequestDownload service informs the bootloader about the start address in memory and the length of the segment. After RequestDownload, all data bytes of the segment are transferred by one or more subsequent TransferData requests. After all segment bytes are transferred, the download of a segment is terminated with a RequestTransferExit request. This sequence can be repeated for several times depending on the number of segments in a logical block (this is the case if the length of the block exceeds the maximum network layer buffer size).

步骤11：下载过程0x34、0x36、0x37：逻辑块的所有的段都要通过0x34、0x36、0x37的序列下载到ECU。一个段由一组连续的数据字节组成，段的下载是从一个0x34服务请求开始的。0x34服务携带一个段的起始地址和长度发送给引导程序。然后，由一个或多个0x36服务请求传输段的所有数据字节。在所有段字节被下载传输后，通过0x37请求终止下载过程。根据逻辑块中的段的个数，这个序列可以重复多次（当逻辑块的长度超出网络层最大缓存的情况）。

Step 12: RoutineControl – “Check Memory Integrity” 0x31 01 02 01: A RoutineControl (0x31) is used to check whether the download of the logic blocks was successful, this function of the routine checks the integrity of download.

步骤12：例程控制 - “检查内存完整性” 0x31 01 02 01：使用例程控制（0x31）检查逻辑块的下载是否成功，这个例程的功能是检查下载的完整性。

Step 13: RoutineControl– “Check Programming Dependency” 0x31 01 FF 01: Once all application software or data blocks/modules are completely downloaded, the tester shall verify if the download has been performed successfully by initiating a routine. This routine either triggers the ECU to check the programming dependencies. The check content is defined by ECU supplier, but shall ensure the compatibility and consistent of all the logical blocks. The application valid flag shall be set to be valid, only when the routine “Check Programming Dependency” implements successful and the result is correct.

步骤13：例程控制 - “检查编程依赖性” 0x31 01 FF 01：一旦所有应用软件或数据块/模块都被完全下载，诊断仪必须通过启动例程来验证下载是否已成功执行。该例程会触发ECU检查编程依赖关系。检查内容由ECU供应商定义，但必须确保所有逻辑块的兼容性和一致性。仅当例程“检查编程依赖性”成功执行且结果正确时，应用程序有效标志位必须置为有效。

7.3.3 Post-Programming Step/后编程阶段

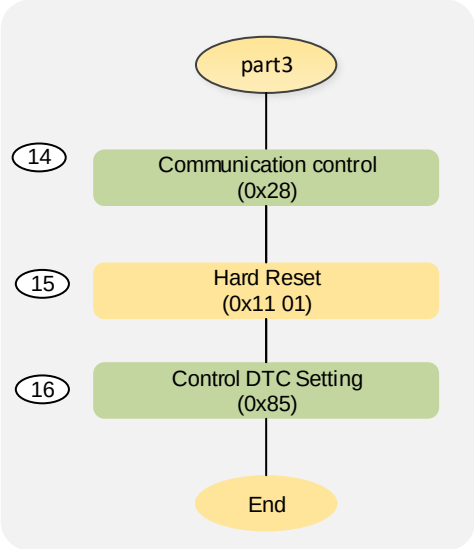

图4 后编程阶段/ Post-Programming step

If any errors occur in the post-programming phase, the entire post-programming process is executed again. The total number of attempts shall not exceed 2 times.

后编程阶段发生任何错误，则重新执行整个后编程流程。总尝试次数不应超过2次。

Step 14: CommunicationControl 0x28 00 03: All ECUs connected to the network shall transmit and receive all normal communication message normally. The request is functionally addressed.

The LIN master node shall exit diagnostic only mode after receiving the diagnostic request0x28 00 03. The LIN slave node shall not give any response to this functional addressing CommunicationControl 0x28 00 03 request even though it supports.

步骤14：通信控制0x28 00 03：所有节点必须恢复正常的发送和接收通信消息。该请求是一个功能寻址的请求。

LIN主节点收到0x28 00 03请求后应该退出纯诊断模式回到正常通信调度，从节点不应该响应功能寻址请求0x28 00 03，即使支持的情况。

Step 15: EcuReset 0x11 01: Tester transmits an ECUReset (0x11 01) service request message to reset ECU. The request is transmitted physically addressed.

For DoIP nodes, Tester (or other reprogramming client) shall establish TCP link within 4s after receiving the positive response of session control. After the TCP link is established, routing activation shall be performed. Just 1 time of routing activation shall be allowed.

The flash driver code shall be removed completely from its buffer to avoid accidental activation of the code that might end up in unintended erase or program operations.

步骤15：ECU重启0x11 01：诊断仪向ECU发送ECU重启（0x11 01）服务请求报文重启ECU，该请求使用物理寻址发送。

诊断DoIP节点，诊断仪（或其他上位机）在收到模式切换正响应后，必须在4s内建立TCP连接。TCP连接建立完成后必须进行路由激活，路由激活尝试次数必须仅为1次。

内存驱动代码必须从其缓存区中完全删除，以避免意外激活代码，导致意外擦除或编程操作。

Step 16: ControlDTCSetting 0x85 01: Tester enables the setting of DTCs in each ECU using the ControlDTCSetting (0x85) service with DTCSettingType equal to “on”. The request is functionally addressed.

The LIN slave node shall not give any response to this functional addressing ControlDTCSetting 0x85 01 request even though it supports.

步骤16：控制DTC设置 0x85 01：诊断仪使用DTC设置类型等于“开”的控制DTC设置（0x85）服务开启每个ECU中DTC的设置。该请求是一个功能寻址的请求。

LIN从节点不应该响应功能寻址请求，即使支持0x85 01请求。

8 General Non-Volatile FBL Status Information/一般非易失 FBL 状态信息

The system shall store the following fields in the non-volatile memory. Each field in Table19 is mandatory, but the in-memory order is an example.

系统应将以下字段存储在非易失性存储器中。表 19 中的每个字段都是强制支持的，但是在内存中的顺序只是一个例子。

表19 一般非易失性 FBL 状态信息/General non-volatile FBL status information

Offset/bytes	Size/bytes	Field	Coding/ hex	Description
+0	1	External Reprogramming request flag 扩展编程请求标志	00/FF B5	No external reprogramming request present . The external reprogramming request flag indicates that the ECU application started the FBL for reprogramming. 没有外部重新编程的请求 。 外部重编程请求标志表明 ECU 应用程序启动 FBL 进行重编程。
			01-B4 B6-FE	Reserved 预留 Reserved 预留
+1	n1	Validity Flags 有效性标志	b7-b0	Inverted validity bits of all logical blocks 所有逻辑块的反向有效性位
			bx=0 bx=1	Logical block valid 逻辑块有效 Logical block invalid 逻辑块无效

表19 一般非易失性 FBL 状态信息/General non-volatile FBL status information(续)

Offset/bytes	Size/bytes	Field	Coding/ hex	Description
+1+n	1	Reset Response Flag 复位响应标志		This flag specifies if a positive response shall be transmitted after reset 此标志指示复位后是否应该发送一个正响应
			00/FF 01 02	Reset response not required Response for start default session (0x10 01) Response for EcuReset (0x11 01) 不需要复位响应 启动默认会话的响应(0x10 01) ECU 复位响应(0x11 01)
+2+n	1	Security Access Delay Flag 安全访问延迟标志	FF A7	Security access delay not active Security access delay active 安全访问延迟不活跃 安全访问延迟激活
			00-A6 A8-FE	Reserved 预留 Reserved 预留
+3+n	1	Security Access Invalid Attempt Counter 安全访问无效尝试次数	FF-00	Count of failed seed-key identifications (inverted) 失败的种子-密钥标识计数(反向)
1. n depends on the number of logical blocks.				

The handling of validity information is shown in Table 20 in more detail. Validity information is used by the FBL to determine if the application can be started after PowerOn/Reset. Depending on the number of logical blocks, there are n bytes reserved to store this information. Each logical block is represented by one bit as represent in Table 23.

FBL使用有效性信息来确定在电源供电/重置之后是否可以启动应用程序。根据逻辑块的数量，有n个字节被保留来存储这些信息。表20中所示，每个逻辑块由一位表示。

表20 字节有效状态/Validity status byte(s)

Bit	7	6	5	4	3	2	1	0
Validity Flags	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1

The bits b7 – b0 represent the validity of the corresponding logical block. If more than eight logical blocks are configured, additional bytes according to this schema are used.

位b7 – b0表示相应逻辑块的有效性。如果配置了超过8个逻辑块，那么将根据该模式使用额外的字节。

参 考 文 献

[1] ISO 14229-1:2013 Road Vehicles -- Unified Diagnostic Services (UDS) -- Part 1: Specification and requirements.

[2] ISO 13400-2：Diagnostic communication over Internet Protocol(DoIP) services ：Transport protocol and network layer services.

[3] ISO 14229-5:2013 Road Vehicles -- Unified Diagnostic Services (UDS) -- Part 3: Unified diagnostic services on Internet protocol implementation (UDSonIP)