

ICS 29.140.50

CCS K74

团 体 标 准

T/SILA 002—2021

电力线载波通信(PLC)工业照明 互联规范

Intercommunication specification for
Power Line Communication (PLC) industrial lighting

2021-08-24 发布

2021-08-24 实施

上海浦东智能照明联合会 发布

目 次

前言	III
1 范围.....	1
2 规范性引用文件.....	1
3 术语和定义.....	1
4 缩略语.....	2
5 系统组成与架构.....	2
5.1 规范概要.....	2
5.2 PLC 简介	2
5.3 系统架构.....	2
5.4 设备功能定义模型.....	4
6 PLC 模组串口接口参考	18
6.1 范围.....	18
6.2 说明.....	18
6.3 应用帧结构.....	18
6.4 PLC 应用报文	32
7 系统控制协议.....	33
7.1 发送数据.....	34
7.2 接收数据.....	34
7.3 功能命令详解.....	38

前 言

本文件按照 GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由上海浦东智能照明联合会（SILA）制定发布，版权归 SILA 所有，未经 SILA 许可不得随意复制，任何单位或个人引用本标准的内容需指明标准的标准号。

请注意本文件的某些内容可能涉及专利，本文件的发布机构不承担识别专利的职责。

本文件由上海浦东智能照明联合会归口管理。

本文件主编单位：上海浦东智能照明联合会，上海海思技术有限公司，广州力控智电信息科技有限公司

本文件参与起草单位：中山大学半导体照明材料及器件国家联合地方工程实验室，永林电子（上海）有限公司，湖南欧智通科技有限公司，北京四季豆信息技术有限公司，良业科技集团股份有限公司，上海三思电子工程有限公司，深圳微自然创新科技有限公司，广州中大中鸣科技有限公司，广东巨业科技股份有限公司，华荣照明有限公司，青岛鼎鼎安全技术有限公司，深圳市尚为照明有限公司，深圳市奇脉电子技术有限公司，上海亚明照明有限公司，广州飞乐喜万年贸易有限公司，惠州雷士光电科技有限公司，TCL 华瑞照明科技（惠州）有限公司，上海屹立店智能科技有限公司，横店集团得邦照明股份有限公司，深圳市海洋王照明工程有限公司，上海时代之光照明电器检测有限公司，深圳市安百纳智能实业有限公司

本文件主要起草人：薄会健，贺海斌，蔡如海，刘道坤，马小平，代照亮，庄晓波，刘磊，钱佳，周勇，姜玉稀，徐东，谢毅，张成良，张国松，丁淦元，陈建胜，卓凯旋，杨志超，朱华荣，李刚，王春林，叶飞，窦斌，林小科，吕三品，郭虎，陈邓伟，朱春强，孙社涛，陈伟雄，王彩健

电力线载波通信 (PLC) 工业照明互联规范

1 范围

本文件规定了工业照明系统中使用 PLC 控制系统的技术要求。工业照明范围包括 道路照明，园区照明，公共建筑，场馆及各类厂房。

2 规范性引用文件

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，仅所注日期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。

T/SILA 001—2020 电力线载波通信(PLC)全屋互联标准规范
IEEE P1901.1 宽带电力线载波标准 (Broadband PLC IEEE P1901.1)

3 术语和定义

下列术语和定义适用于本文件。

3.1

控制设备 control device

是指连接到 PLC 总线上的设备，并用于发送指令控制其他连接到相同 PLC 总线上的设备。控制设备如控制面板、传感器等。

3.2

受控设备 controlled device

是指连接在电源和一支或若干支灯之间用来变换电源电压，限制灯的电流至规定值，提供启动电压和预热电流，防止冷启动，校正功率因数或降低无线电干扰的一个或若干个部件，如开关控制器、单色调光驱动器、双色调光驱动器、彩色调光驱动器、窗帘驱动器等。

3.3

中央协调节点 central coordinator

是指在 PLC-IoT 通信中的具体体现为头端通信模块，负责末端设备的接入以及数据的接受与发送。

3.4

终端节点 station

是指在 PLC-IoT 通信中的具体体现为尾端通信模块，接受与发送电力载波信号，为终端设备提供统一的接入 PLC-IoT 网络方式。

3.5

代理协调节点 proxy coordinator

是指在PLC-IoT通信中的具体体现为中间代理通信模块，接受与发送电力载波信号，为中央协调节点和终端节点之间提供代理协调功能。

4 缩略语

下列缩略语适用于本文件。

CCO：中央协调节点（Central Coordinator）

CIID：属性实例（Characteristic Instance Identification）

PCO：代理协调节点（Proxy Coordinator）

PLC：电力线载波通信（Power Line Communication）

SIID：服务实例（Service Instance Identification）

STA：终端节点（Station）

5 系统组成与架构

5.1 系统架构

本系统由服务器、管理终端、网关和子设备和滤波器组成，服务器、管理终端、与网关之间基于TCP/IP网络协议通信，网关与子设备之间基于PLC网络协议通信。为了避免各PLC子系统之间的信号串扰，在各PLC子系统供电入口加入滤波器用于PLC信号隔离。系统架构，如图1所示。

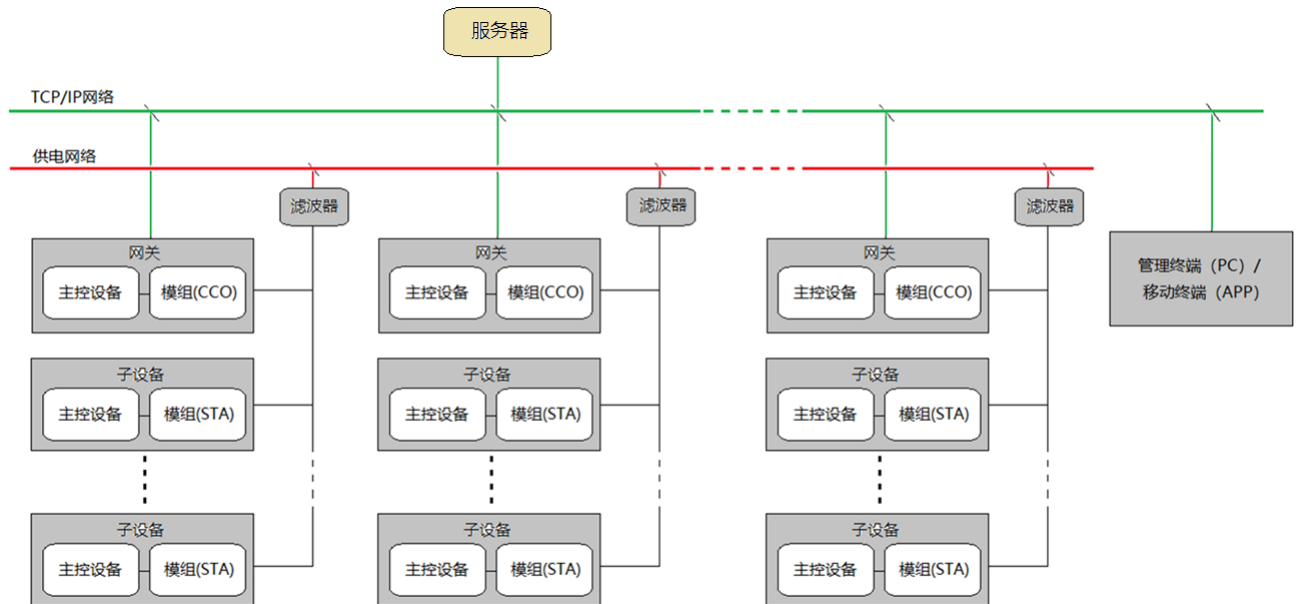


图 1 系统架构

本系统基于 PLC 应用层构建工业照明系统的通讯协议，实现通信单元之间业务数据交互，通过数据链路层完成数据传输，PLC 分层，如图 2 所示。

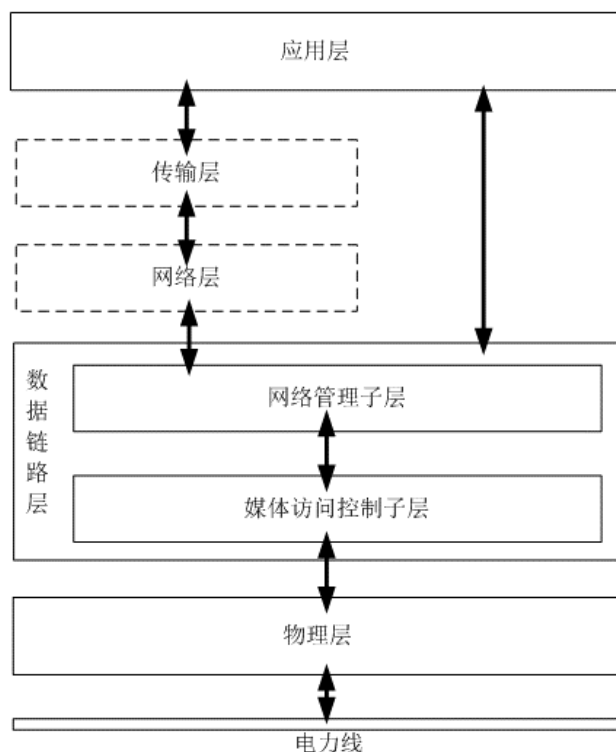


图 2 PLC 分层

PLC 网络中有三种节点，以 CCO（中心节点）、PCO（代理节点）、STA（终端）为组成的树形结构。其通信方式采用中央调度的方式，CCO 上电后会进行全网检测，确定 PCO 和 STA，然后侦听 STA 的报文或者主动询问 STA，通过 CSMA/CA 载波检测多址的方式进行传输管理和控制，PLC-IoT 树形组网及网络节点，如图 3 所示。

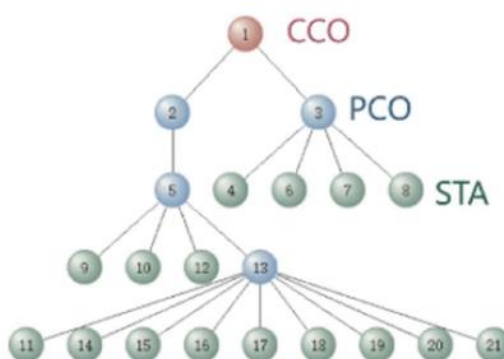


图 3 PLC-IoT 树形组网及网络节点

所有 STA 站点向头端节点 CCO 发起关联入网请求，CCO 确认后方可加入网络，网络建立可立即进行 PLC 通信。站点通信为 CCO 与 STA 站点的之间的相互通信，STA 与 STA 不能直接通信，需要通过 CCO 来转发，PLC 的自组网过程由芯片底层软件实现，无需应用层干预。

入网过程：上电后和 CCO 之间能直接通信的 STA 站点，会首先入网，形成 1 级站点，并评估相互通信成功率，不能和 CCO 直接通信的站点若能和 1 级站点通信，就通过 1 级站点代理入网，以此类推逐级形成多层次网络，目前最大可以支持 15 层级。PCO 站点非指定，由各站点自动形成。

PLC 信道具有时变性，噪声也可能随着电器开闭时有时无，这意味着已经建立起来的路由网络可能存不通，PLC 链路层需有路由评估机制，在路由周期内不断评估代理路由合理性，动态变化拓扑图，以确保通信可靠。路由评估需要时间，因此 CCO 坏掉或者站点拔掉，网络稳定需要一定时间，这个时间与网络规模或者层级深度有关系。

在 PLC 总线网络的每个设备，都有一个固定的物理地址（6 字节 MAC 地址），MAC 地址在 PLC 模块出厂时通过 IANA 或 IEEE 申请分配，使用过程不更改。使用 MAC 地址，在网络中可提供单播寻址（0~FF FF FF FF FE）方式或广播寻址（FF FF FF FF FF FF）方式进行通信。

5.2 系统组成

PLC 系统一般由多个子系统组成，子系统通过 PLC 网关连接到局域网服务器或云服务器组成系统，移动终端通过云端连接系统。一个子系统由一个 PLC 网关、若干个控制设备和若干个受控设备组成。

PLC 网关是集成控制、管理、计算和通信等功能的基础开放平台。网关包含 PLC-CCO 模组、MCU 模块。特性如下：

- a) PLC 网关在系统中通过中央节点 CCO 进行协议转换与 STA 通信；
- b) 具备应用地址配置和管理；
- c) 具备场景配置与控制；
- d) 具备控制程序逻辑配置与控制；
- e) 具备系统设备状态监测功能；
- f) 具备通过网络把系统的指令同步传递到服务器。

场景可通过按键信号、时钟信号、传感器信号等进行触发，场景控制逻辑通过管理终端（PC）进行配置并保存在 PLC 网关，场景信息同时保存在每个受控设备内，当进行场景控制时，被寻址选中的受控设备可以实现同步响应。

5.3 系统要求

PLC 工业照明系统兼容 PLC 全屋互联系统，特性如下：

一个子系统至少含一个 CCO 中央节点；

任一个系统设备都可以主动发送事件上报信息；

一个子系统最多可独立寻址 1023 个的设备；

一个子系统最多可寻址 49150（2 个字节，除去预留的设备地址）个可寻址组；

一个子系统最多可支持 65535（2 个字节）个照明场景，单个子设备至少支持 32 个场景；

系统控制面板或传感器的事件信息发送到 PLC 网关（CCO），由 PLC 网关（CCO）根据控制逻辑进行处理，并由 PLC 网关（CCO）把处理完的控制信息发送到受控设备进行控制处理。

5.4 系统设备功能定义模型

设备 profile 是设备和其他子系统之间的交互数据定义能力和格式，用于描述设备所具备的能力和状态数据。设备的通过两种方式描述设备具备的特征，服务(service)和属性(characteristic)，设备由若干个服务及其属性组成。

设备 service 用来表示设备中用户可使用的功能函数，其中包含实现该函数输出/输入的数据以及实现该函数的行为。设备可以基于服务进行实例化，实例化后的名称称之为服务实例。

设备 characteristic 表示数据或相关行为的特征，名称之为属性名，是 Service 的基本组成单元，如开关的开或关特性，设备功能定义模型，如图 4 所示。

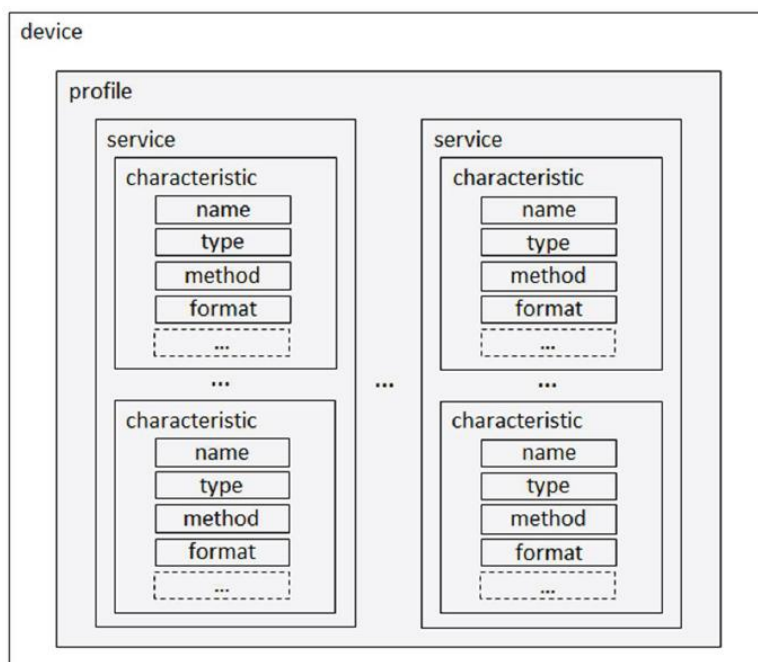


图 4 设备功能定义模型

用户通过 APP 控制设备执行场景时，云端到 PLC-IoT 网关设备的 profile 数据的格式，如图 5 所示

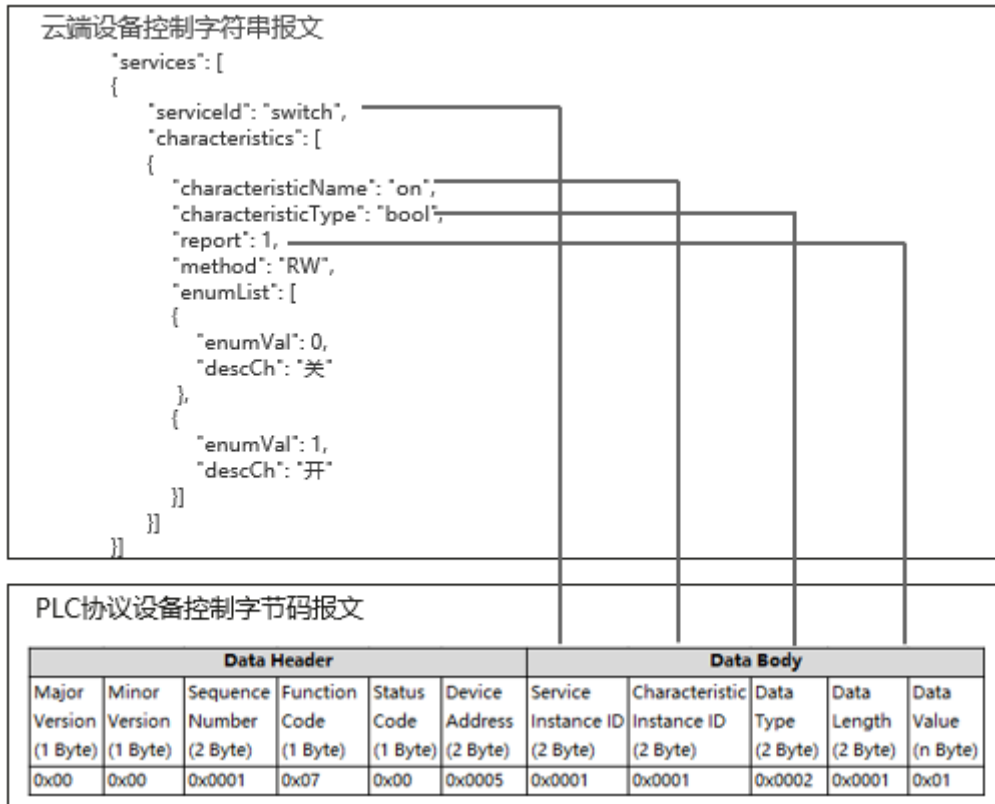


图 5 PLC 协议设备控制报文转换

以下列举了几种典型的子设备器件物模型转换定义，用于示例 PLC 设备与物模型的映射，通过这种方式，可以无限扩展定义灯光控制的属性，例如新增灯光驱动控制器子设备的功率、故障信息，只要新增定义与调节亮度相似的服务属性即可传递到网关，并通过网关传递到云端。SIID 和 CIID 使用两个字节编码见表 1，其中 0x0001~0x1964 用于定义通用范围段，0x1965~0x3FFF 预留团体定义范围段。

0x4000~0xFFFF 预留厂商定义私有不通范围段。

- a) 场景面板属性，见表 1；
- b) 窗帘驱动器属性，见表 2；
- c) 灯光驱动控制器属性，见表 3；
- d) 红外移动传感器属性，见表 4；
- e) 光照传感器属性，见表 5；
- f) 电源开关属性，见表 6；
- g) 智能开关模块属性，见表 7；
- h) 空气质量传感器属性，见表 8。

表 1 场景面板

Siid	服务	服务(中文)	Ciid	属性	数据类型	取值范围	描述
0x0041	scene	按键记录					
			0x008A	num	int	min:1 max:按键数量	按键按下, 上报按键编号
0x0031	button	按键定义					
			0x008A	num	int	min:1 max:按键数量	按键编号
			0x0002	name	string	StringLength:32	按键名
0x0036	Fault	故障服务					
			0x0085	Fault status	enum	0- 设备正常 1- 设备异常	故障状态 (状态变化即上报)
			0x0086	Fault code	enumList	0- 正常 1-N 错误码, 自定义	故障代码
0x0022	Time	时间					
			0x2000	Total time	int	min:0 max: 300000	设备累计工作时间 (小时)-自定义
<p>注 1: 按键定义时, 先定义按键编号 (Siid: 0x03F1, Ciid: 0x008A, 编号), 后定义按键名 (Siid: 0x03F1, Ciid: 0x0002, 键名), 如上定义需要成组出现才有效</p> <p>注 2: 有按键按下时, 将启动上报按键事件, 如果按键一直按下, 则间隔 0.3 秒连续上报按键事件, 直到按键松开。本协议只定义单键, 忽略多键同时按下的情况</p> <p>注 3: 本协议也适合 LCD 面板的按键定义</p>							

表 2 窗帘驱动器

Siid	服务	服务(中文)	Ciid	属性	数据类型	取值范围	描述
0x0013	mode	窗帘开合					
			0x0022	mode	enum	0-关 1-开 2-暂停	窗帘电机控制窗帘的开合
0x000B	opener	开合度					
			0x000E	current	int	min:0 max:100	当前的打开程度，100 为全开 单位：百分比；
			0x000F	target	int	min:0 max:100	目标的打开程度，100 为全开 单位：百分比；
0x0036	Fault	故障服务					
			0x0085	Fault status	enum	0- 设备正常 1- 设备异常	故障状态 (状态变化即上报)
			0x0086	Fault code	enumList	0- 正常 1-N 错误码，自定义	故障代码
0x0022	Time	时间					
			0x2000	Total time	int	min:0 max: 300000	设备累计工作时间(小时)- 自定义

表 3 灯光驱动控制器

Siid	服务	服务(中文)	Ciid	属性	数据类型	取值范围	描述
0x0001	switch	开关					
			0x0001	on	bool	0-关 1-开	电源开关状态； 变化就上报
0x0007	brightness	亮度					
			0x0004	brightness	int	min:1 max:100 步长:1	亮度设置； 变化就上报
0x0005	colour	RGB 颜色					
			0x0007	red	int	min:0 max:255 步长:1	RGB 颜色 红色，变化就上报
			0x0008	green	int	min:0 max:255 步长:1	绿色 变化就上报
			0x0009	blue	int	min:0 max:255 步长:1	蓝色 变化就上报
			0x000A	white	int	min:0 max:255 步长:1	白色 变化就上报
			0x2003	Amber	int	min:0 max:255 步长:1	琥珀色 变化就上报
0x0009	cct	色温					
			0x000D	colorTemperature	int	min:2700 max:6500 步长:1	灯的色温 变化就上报
0x0042	progressSwitch	开关渐变					
			0x008C	range	int	min:0 max:5	亮度变化时长，单 位：秒。默认值：2 秒
0x0019	Electric	电力					
			0x0058	Input Voltage	int	min:0 max:600000	输入电压 (mV)

表 3 灯光驱动控制器（续）

Siid	服务	服务(中文)	Ciid	属性	数据类型	取值范围	描述
			0x0059	Input Current	int	min:0 max:600000	输入电流 (mA)
			0x005A	Consumption	int	min:0 max:600000	总用电量 (KWh)
			0x2001	Output Voltage	int	min:0 max:600000	输出电压 (mV)
			0x2002	Output Current	int	min:0 max:600000	输出电流 (mA)
0x0018	Power	功率					
			0x0056	Power	int	min:0 max:65535	当前功率 (W)
0x0011	Temperature	温度					
			0x000E	Current	int	min:-32767 max:32767	当前温度: °C, 最高位“1”表示负温度。
0x0036	Fault	故障服务					
			0x0085	Fault status	enum	0- 设备正常 1- 设备异常	故障状态 (状态变化即上报)
			0x0086	Fault code	enumList	0- 正常 1-N 错误码, 自定义	故障代码
0x0022	Time	时间					
			0x2000	Total time	int	min:0 max: 300000	设备累计工作时间 (小时)-自定义

表 4 红外移动传感器

Siid	服务	服务(中文)	Ciid	属性	数据类型	取值范围	描述
0x0014	status	有无人状态					
			0x0024	status	enum	0-无人 1-有人	有无人持续的状态 (状态变化即上报)
0x0036	Fault	故障服务					
			0x0085	Fault status	enum	0- 设备正常 1- 设备异常	故障状态 (状态变化即上报)

表 4 红外移动传感器（续）

Siid	服务	服务(中文)	Ciid	属性	数据类型	取值范围	描述
			0x0086	Fault code	enumList	0- 正常 1-N 错误码, 自定义	故障代码
0x0022	Time	时间					
			0x2000	Total time	int	min:0 max: 300000	设备累计工作时间 (小时)-自定义

表 5 光照传感器

Siid	服务	服务(中文)	Ciid	属性	数据类型	取值范围	描述
0x0021	luminance	光照度					
			0x0001	on	bool	0-关 1-开	电源开关状态
			0x000E	current	int	min:0 max:65535 步长:1	光照度, 单位 lux
0x0036	Fault	故障服务					
			0x0085	Fault status	enum	0- 设备正常 1- 设备异常	故障状态 (状态变化即上报)
			0x0086	Fault code	enumList	0- 正常 1-N 错误码, 自定义	故障代码
0x0022	Time	时间					
			0x2000	Total time	int	min:0 max: 300000	设备累计工作时间 (小时)-自定义
注: 光照度传感器参数, 每 5 秒上报一次							

表 6 电源开关

Siid	服务	服务(中文)	Ciid	属性	数据类型	取值范围	描述
0x0001	switch	电源开关					
			0x0001	on	bool	0-关 1-开	电源开关状态 变化就上报
0x0036	Fault	故障服务					
			0x0085	Fault status	enum	0- 设备正常 1- 设备异常	故障状态 (状态变化即上报)

表 6 电源开关 (续)

Siid	服务	服务(中文)	Ciid	属性	数据类型	取值范围	描述
			0x0086	Fault code	enumList	0- 正常 1-N 错误码, 自定义	故障代码
0x0022	Time	时间					
			0x2000	Total time	int	min:0 max: 300000	设备累计工作时间 (小时) -自定义

表 7 智能开关模块

Siid	服务	服务(中文)	Ciid	属性	数据类型	取值范围	描述
0x03E9	Switch1	回路开关(1)					
			0x0001	on	bool	0-关 1-开	开关状态 变化就上报
			0x0002	name	string	字符串长度:16	插口名称, 默认为空, 可选
			0x0059	current	int	min:0 max:65535	回路电流 (mA/A 自定义)
			0x2000	Total time	int	min:0 max: 300000	回路累计工作时间 (小时) - 自定义
0x03EA	Switch2	回路开关(2)					
			0x0001	on	bool	0-关 1-开	开关状态 变化就上报
			0x0002	name	string	字符串长度:16	插口名称, 默认为空, 可选
			0x0059	current	int	min:0 max:65535	回路电流 (mA/A 自定义)
			0x2000	Total time	int	min:0 max: 300000	回路累计工作时间 (小时) - 自定义
0x03EB	Switch3	回路开关(3)					
			0x0001	on	bool	0-关 1-开	开关状态 变化就上报
			0x0002	name	string	字符串长度:16	插口名称, 默认为空, 可选
			0x0059	current	int	min:0 max:65535	回路电流 (mA/A 自定义)
			0x2000	Total time	int	min:0 max: 300000	回路累计工作时间 (小时) - 自定义

表7 智能开关模块(续1)

Siid	服务	服务(中文)	Ciid	属性	数据类型	取值范围	描述
0x03EC	Switch4	回路开关(4)					
			0x0001	on	bool	0-关 1-开	开关状态 变化就上报
			0x0002	name	string	字符串长度:16	插口名称, 默认为空, 可选
			0x0059	current	int	min:0 max:65535	回路电流(mA/A 自定义)
			0x2000	Total time	int	min:0 max: 300000	回路累计工作时间(小时) - 自定义
0x03ED	Switch5	回路开关(5)					
			0x0001	on	bool	0-关 1-开	开关状态 变化就上报
			0x0002	name	string	字符串长度:16	插口名称, 默认为空, 可选
			0x0059	current	int	min:0 max:65535	回路电流(mA/A 自定义)
			0x2000	Total time	int	min:0 max: 300000	回路累计工作时间(小时) - 自定义
0x03EE	Switch6	回路开关(6)					
			0x0001	on	bool	0-关 1-开	开关状态 变化就上报
			0x0002	name	string	字符串长度:16	插口名称, 默认为空, 可选
			0x0059	current	int	min:0 max:65535	回路电流(mA/A 自定义)
			0x2000	Total time	int	min:0 max: 300000	回路累计工作时间(小时) - 自定义
0x03EF	Switch7	回路开关(7)					
			0x0001	on	bool	0-关 1-开	开关状态 变化就上报
			0x0002	name	string	字符串长度:16	插口名称, 默认为空, 可选
			0x0059	current	int	min:0 max:65535	回路电流(mA/A 自定义)
			0x2000	Total time	int	min:0 max: 300000	回路累计工作时间(小时) - 自定义

表7 智能开关模块(续2)

Siid	服务	服务(中文)	Ciid	属性	数据类型	取值范围	描述
0x03F0	Switch8	回路开关(8)					
			0x0001	on	bool	0-关 1-开	开关状态 变化就上报
			0x0002	name	string	字符串长度:16	插口名称, 默认为空, 可选
			0x0059	current	int	min:0 max:65535	回路电流 (mA/A 自定义)
			0x2000	Total time	int	min:0 max: 300000	回路累计工作时间 (小时) -自定义
0x2010	Switch9	回路开关(9)					
			0x0001	on	bool	0-关 1-开	开关状态 变化就上报
			0x0002	name	string	字符串长度:16	插口名称, 默认为空, 可选
			0x0059	current	int	min:0 max:65535	回路电流 (mA/A 自定义)
			0x2000	Total time	int	min:0 max: 300000	回路累计工作时间 (小时) -自定义
0x2011	Switch10	回路开关(10)					
			0x0001	on	bool	0-关 1-开	开关状态 变化就上报
			0x0002	name	string	字符串长度:16	插口名称, 默认为空, 可选
			0x0059	current	int	min:0 max:65535	回路电流 (mA/A 自定义)
			0x2000	Total time	int	min:0 max: 300000	回路累计工作时间 (小时) -自定义
0x2012	Switch11	回路开关(11)					
			0x0001	on	bool	0-关 1-开	开关状态 变化就上报
			0x0002	name	string	字符串长度:16	插口名称, 默认为空, 可选
			0x0059	current	int	min:0 max:65535	回路电流 (mA/A 自定义)
			0x2000	Total time	int	min:0 max: 300000	回路累计工作时间 (小时) -自定义

表 7 智能开关模块 (续 3)

Siid	服务	服务(中文)	Ciid	属性	数据类型	取值范围	描述
0x2013	Switch12	回路开关(12)					
			0x0001	on	bool	0-关 1-开	开关状态 变化就上报
			0x0002	name	string	字符串长度:16	插口名称, 默认为空, 可选
			0x0059	current	int	min:0 max:65535	回路电流 (mA/A 自定义)
			0x2000	Total time	int	min:0 max: 300000	回路累计工作时间 (小时) -自定义
0x2014	Switch13	回路开关(13)					
			0x0001	on	bool	0-关 1-开	开关状态 变化就上报
			0x0002	name	string	字符串长度:16	插口名称, 默认为空, 可选
			0x0059	current	int	min:0 max:65535	回路电流 (mA/A 自定义)
			0x2000	Total time	int	min:0 max: 300000	回路累计工作时间 (小时) -自定义
0x2015	Switch14	回路开关(14)					
			0x0001	on	bool	0-关 1-开	开关状态 变化就上报
			0x0002	name	string	字符串长度:16	插口名称, 默认为空, 可选
			0x0059	current	int	min:0 max:65535	回路电流 (mA/A 自定义)
			0x2000	Total time	int	min:0 max: 300000	回路累计工作时间 (小时) -自定义
0x2016	Switch15	回路开关(15)					
			0x0001	on	bool	0-关 1-开	开关状态 变化就上报
			0x0002	name	string	字符串长度:16	插口名称, 默认为空, 可选
			0x0059	current	int	min:0 max:65535	回路电流 (mA/A 自定义)
			0x2000	Total time	int	min:0 max: 300000	回路累计工作时间 (小时) -自定义

表 7 智能开关模块 (续 4)

Siid	服务	服务(中文)	Ciid	属性	数据类型	取值范围	描述
0x2017	Switch16	回路开关 (16)					
			0x0001	on	bool	0-关 1-开	开关状态 变化就上报
			0x0002	name	string	字符串长度:16	插口名称, 默认为空, 可选
			0x0059	current	int	min:0 max:65535	回路电流 (mA/A 自定义)
			0x2000	Total time	int	min:0 max: 300000	回路累计工作时间 (小时) - 自定义
0x0036	Fault	故障服务					
			0x0085	Fault status	enum	0- 设备正常 1- 设备异常	故障状态 (状态变化即上报)
			0x0086	Fault code	enumList	0- 正常 1-N 错误码, 自 定义	故障代码
0x0022	Time	时间					
			0x2000	Total time	int	min:0 max: 300000	设备累计工作时间 (小时) - 自定义

表 8 空气质量传感器

Siid	服务	服务(中文)	Ciid	属性	数据类型	取值范围	描述
0x001F	Air Quality	空气质量	0x0035	AirQuality	enum	min: 0 max: 4	0 - "未知" 1 - "优" 2 - "良" 3 - "较差" 4 - "差"
0x001A	PM2.5 Sensor	PM2.5 检 测器	0x000E	Current	int	min: 0 max: 1000	

表8 空气质量传感器（续1）

Siid	服务	服务(中文)	Ciid	属性	数据类型	取值范围	描述
			0x0010	Level	enum	min: 1 max: 6	1 - "优, 0~80 μg/m ³ " 2 - "良, 80~120 μg/m ³ " 3 - "轻度污染, 120~180 μg/m ³ " 4 - "中度污染, 180~240 μg/m ³ " 5 - "重度污染, 240~320 μg/m ³ " 6 - "严重污染, > 320 μg/m ³ "
0x001B	CO2 Sensor	CO2 检测器	0x000E	Current	int	min: 0 max: 10000	
			0x0010	Level	enum	min: 1 max: 5	1 - "理想, < 500ppm" 2 - "正常, 500~1000ppm" 3 - "浑浊, 1000~1800ppm" 4 - "中度污染, 1800~5000ppm" 5 - "严重污染, > 5000ppm"
0x001C	HCHO Sensor	HCHO 检测器	0x000E	Current	int	min: 0 max: 10000	
			0x0010	Level	enum	min: 1 max: 4	1 - "理想" 2 - "一般" 3 - "有害" 4 - "严重有害"
0x001D	TVOC Sensor	TVOC 检测器	0x000E	Current	int	min: 0 max: 10000	
			0x0010	Level	enum	min: 1 max: 4	1 - "理想" 2 - "轻度污染" 3 - "中度污染" 4 - "严重污染"
0x001E	PM10 Sensor	PM10 检测器	0x000E	Current	int	min: 0 max: 500	
			0x0010	Level	enum	min: 1 max: 6	1 - "优, 0~80 μg/m ³ " 2 - "良, 80~120 μg/m ³ " 3 - "轻度污染, 120~180 μg/m ³ " 4 - "中度污染, 180~240 μg/m ³ " 5 - "重度污染, 240~320 μg/m ³ " 6 - "严重污染, > 320 μg/m ³ "

表 8 空气质量传感器（续 2）

Siid	服务	服务(中文)	Ciid	属性	数据类型	取值范围	描述
0x0036	Fault	故障服务					
			0x0085	Fault status	enum	0- 设备正常 1- 设备异常	故障状态 (状态变化即上报)
			0x0086	Fault code	enumList	0- 正常 1-N 错误码, 自定义	故障代码
0x0022	Time	时间					
			0x2000	Total time	int	min:0 max: 300000	设备累计工作时间(小时)-自定义
注: 空气质量指数, 每 5 秒上报一次							

6 PLC 模组串口接口参考

6.1 范围

本协议规定了 MCU 与 PLC CC0（主节点）之间串口通信数据传输的帧格式、数据编码及传输规则。

6.2 说明

本协议中所有保留字段都需要填 0。

6.3 应用帧结构

6.3.1 字节格式

应用帧的基本单元为 8 位字节。链路层传输顺序为低位在前，高位在后；低字节在前，高字节在后。串口传输时：字节传输按异步方式进行，通信速率默认为 115200bps，基本单元包含 1 个起始位“0”、8 个数据位、一个偶校验位 P 和 1 个停止位“1”，格式定义，见表 9。

表 9 字节格式

0	D0	D1	D2	D3	D4	D5	D6	D7	P	1
起始位	8 个数据位							偶校验位	停止位	

6.3.2 帧格式定义

数据帧采用小端序，帧格式定义，见表 10。

表 10 帧格式定义

长度 (byte)	1	1	2	2	2	L	2
含义	Head	Ctrl	Cmd	Seq	L	Data	CRC
<p>注 1: Head: 帧头, 固定为 48H。</p> <p>注 2: Ctrl: 控制域。</p> <p>注 3: Cmd: 命令码。</p> <p>注 4: Seq: 帧序列号, 用以匹配上下行报文的请求应答关系, 取值 0~65535, 循环使用。</p> <p>注 5: L: 数据域 Data 的长度, 不超过 502 字节。</p> <p>注 6: Data: 数据域。</p> <p>注 7: CRC: 报文的 CRC16 校验和, 从帧头开始到 Data 段结束。CRC 校验生成多项式采用 CRC16-CCITT(0x1021), $x^{16}+x^{12}+x^5+1$。</p>							

6.3.2.1 控制域 (Ctrl)

控制域 (Ctrl) 表示帧的传输方向、启动标志, 由 1 字节组成, 控制域定义, 见表 11。

表 11 控制域

D7	D6	D5	D4	D3	D2	D1	D0
Dir	Prm	Rsv					
<p>注 1: Dir: Dir=0 表示此帧报文是由主控设备发出的下行报文; Dir=1 表示此帧报文是由通信模组发出的上行报文。</p> <p>注 2: Prm: Prm=1 表示此帧报文来自启动站; Prm=0 表示此帧报文来自从动站。</p> <p>注 3: Rsv: 保留</p>							

6.3.2.2 命令码 (Cmd)

命令码定义, 见表 12。

表 12 命令码

Cmd	说明	命令类别
0001H	读取模组版本信息	本地通信命令
0002H	读取模组 MAC 地址	
0003H	读取模组通信地址	
0004H	设置模组通信地址	
0005H	模组重启	
0006H	传输文件	
0007H	读取模块上电时间	
0010H	读取白名单中节点数量	
0011H	读取白名单中节点信息	
0012H	添加节点到白名单	
0013H	删除白名单中节点	
0014H	清空白名单	
0015H	自组网功能开启	
0016H	设置白名单状态	
0017H	获取白名单状态	
0020H	读取拓扑中节点数量	
0021H	读取拓扑中节点信息	
0100H	发送数据	
0101H	接收数据	
0110H	远程发送命令	
0111H	远程接收命令	
0120H	总线数据通信命令	

6.3.3 本地通信命令详细说明

本地命令数据交互流，如图 6。

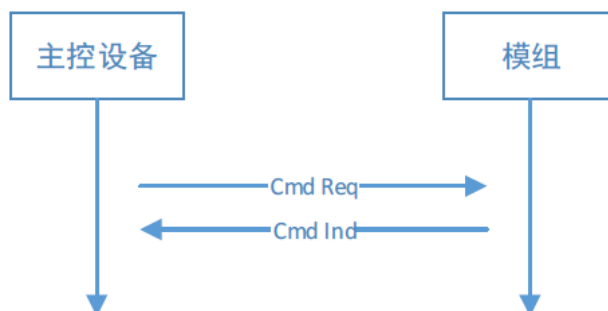


图 6 本地命令数据交互流程

6.3.3.1 读取模组版本信息（0001H）

读取模组版本信息，见表 13。

表 13 读取模组版本信息

方向	主控设备下发到模组	模组应答
Cmd	0001H	0001H
Data	空	厂商代码（2bytes）
		芯片类型（2bytes） 3921H
		软件版本号（2bytes） BCD 格式
		保留（2bytes） 0000H

6.3.3.2 读取模组 MAC 地址（0002H）

读取模组 MAC 地，见表 14。

表 14 读取模组 MAC 地址

方向	主控设备下发到模组	模组应答
Cmd	0002H	0002H
Data	空	MAC 地址（6bytes）
		保留（2bytes） 0000H

6.3.3.3 读取模组通信地址（0003H）

读取模组通信地址，见表 15。

表 15 读取模组通信地址

方向	主控设备下发到模组	模组应答
Cmd	0003H	0003H
Data	空	通信地址（6bytes）
		保留（2bytes） 0000H

6.3.3.4 设置模组通信地址（0004H）

设置模组通信地址，见表 16。

表 16 设置模组通信地址

方向	主控设备下发到模组	模组应答
Cmd	0004H	0004H
Data	通信地址 (6bytes)	设置结果 (1byte) 0: 成功, 1: 失败
	保留 (2bytes) 0000H	失败原因 (1byte), 见 6.3.8 Rsv (2bytes)
注: 模组通信地址保存在模组非易失性存储器中		

6.3.3.5 模组重启 (0005H)

模组重启, 见表 17。

表 17 模组重启

方向	主控设备下发到模组	模组应答
Cmd	0005H	0005H
Data	Delay Time (1byte)	State (1Bte)
	Rsv (3bytes)	Rsv (3bytes)
注 1: Delay Time: 延时等待重启时间, 单位: 秒。0 代表立即重启。 注 2: State: 0-重启成功; 1-重启失败。 注 3: 注: 模组收到报文后, 先应答再重启。		

6.3.3.6 传输文件 (0006H)

传输文件, 见表 18。

表 18 传输文件

方向	主控设备下发到模组	模组应答
Cmd	0006H	0006H
Data	Fn (1byte)	Fn (1byte)
	User Data	User Data

Fn 为功能码, 不同功能码对应的 User Data 格式如下。

6.3.3.6.1 启动文件传输

启动文件传输, 见表 19。

表 19 启动文件传输

方向	主控设备下发到模组	模组应答
Fn	01H	01H
Data	File Attr (1bytes)	State (1byte)
	Segment Total (2bytes)	Reason (1byte)
	File Length (4bytes)	Rsv (1byte)
	File Crc (4bytes)	
	Trans Timeout (4bytes)	
<p>注 1: File Attr: 0 表示清除下装; 1 表示本地升级文件; 2 表示全网升级文件; 3 表示列表升级文件(升级部分 STA)。</p> <p>注 2: Segment Total: 文件传输内容的总段数。</p> <p>注 3: File Length: 文件的总长度, 单位字节。</p> <p>注 4: File Crc: 文件所有内容的 CRC32 校验和。</p> <p>注 5: Trans Timeout: 文件传输超时时间, 单位: 分钟。</p> <p>注 6: State: 0 表示成功; 1 表示失败, 失败原因见 Reason。</p> <p>注 7: Reason: 取值含义请参见“异常状态代码”。</p>		

6.3.3.6.2 传输文件内容

传输文件内容, 见表 20。

表 20 传输文件内容

方向	主控设备下发到模组	模组应答
Fn	02H	02H
Data	Rsv (1byte)	State (1byte)
	Segment Num (2bytes)	Reason (1byte)
	Segment Size (2bytes)	Rsv (1byte)
	Segment Crc (2bytes)	
	Segment Data	
<p>注 1: Segment Num: 文件内容的传输帧序号, 取值范围 0 至 n-1 (n 为总段数)。</p> <p>注 2: Segment Size: 该帧文件内容的大小, 除最后一帧外, 其他帧必须为固定大小。</p> <p>注 3: Segment Crc: Segment Data 的 CRC16 校验和。CRC 校验生成多项式采用 CRC16-CCITT(0x1021), $x^{16}+x^{12}+x^5+1$。</p> <p>注 4: Segment Data: 该帧传输的文件内容, 长度为 L 字节。实际传输时, 不足 4 字节的倍数时通过末尾补 0x00 的方式补充为 4 字节的整数倍。</p> <p>注 5: State: 0 表示成功; 1 表示失败, 失败原因见 Reason。</p> <p>注 6: Reason: 取值含义请参见“异常状态代码”。</p>		

6.3.3.6.3 查询处理进度

查询处理进度，见表 21。

表 21 查询处理进度

方向	主控设备下发到模组	模组应答
Fn	03H	03H
Data	Rsv (3byte)	State (1byte)
		Fail STAs (2byte)
注 1: State: 文件处理进度: 0 全部成功; 1 正在处理, 不能接收新文件; 2 未全部成功, 存在失败节点。 注 2: Fail STAs: 失败节点数。		

6.3.3.6.4 配置升级列表

配置升级列表，见表 22。

表 22 配置升级列表

方向	主控设备下发到模组	模组应答
Fn	04H	04H
Data	Mac Cnt (1bytes)	State (1byte)
	Mac List (6 * N Bytes)	Reason (1byte)
		Rsv (1byte)
注 1: Mac Cnt: 升级列表个数; 注 2: Mac List: 升级列表 注 3: State: 0 表示成功; 1 表示失败, 失败原因见 Reason。 注 4: Reason: 取值含义请参见“异常状态代码”。 注 5: 此指令为在列表升级时用于配置 STA 升级列表, 本地升级和全网升级时无效。		

6.3.3.7 读取模块上电时间 (0007H)

读取模块上电时间，见表 23。

表 23 读取模块上电时间

方向	主控设备下发到模组	模组应答
Cmd	0007H	0007H
Data	本次查询报文序号 (2byte)	MAC (6 byte)
		frame_index (2 byte)
		on_power_ms_time (4 byte)
注 1: MAC: 本站点 MAC 地址。 注 2: frame_index 本次查询报文序号。 注 3: on_power_ms_time 站点 上电时间, 单位 ms。		

6.3.3.8 读取白名单中节点数量 (0010H)

读取白名单中节点数量, 见表 24。

表 24 读取白名单中节点数量

方向	主控设备下发到模组	模组应答
Cmd	0010H	0010H
Data	空	节点数量 (2bytes)
		保留 (2bytes) 0000H

6.3.3.9 读取白名单中节点信息 (0011H)

读取白名单中节点信息, 见表 25。

表 25 读取白名单中节点信息

方向	主控设备下发到模组	模组应答
Cmd	0011H	0011H
Data	Start Seq (2Bytes)	Total (2Bytes)
		Start Seq (2Bytes)
	Req Cnt (2Bytes)	Ind Cnt (2Bytes)
		保留 (2bytes) 0000H
		Ind Data (6 * N Bytes)
注 1: Start Seq: 起始序号, 从 0 开始。 注 2: Req Cnt: 本次查询的节点数量。 注 3: Total: 白名单中节点总数量。 注 4: Ind Cnt: 本次应答的节点数量。 注 5: Ind Data: 本次应答的白名单数据, 每个节点 6 个字节 (大端)。		

6.3.3.10 添加节点到白名单 (0012H)

添加节点到白名单，见表 26。

表 26 添加节点到白名单

方向	主控设备下发到模组	模组应答
Cmd	0012H	0012H
Data	Req Cnt (2bytes)	State (1byte)
	Req Data (6 * N Bytes)	Reason (1byte), 见 5.3.6
		Rsv (2bytes)
注 1: Req Cnt: 本次设置的节点数量。 注 2: Req Data: 本次设置的白名单节点数据，每个节点 6 个字节（大端）。 注 3: State: 0 表示成功；1 表示失败，失败原因见 Reason。 注 4: Reason: 取值含义请参见“异常状态代码”。		

6.3.3.11 删除白名单中节点 (0013H)

删除白名单中节点，见表 27。

表 27 删除白名单中节点

方向	主控设备下发到模组	模组应答
Cmd	0013H	0013H
Data	Req Cnt (2bytes)	State (1byte)
	Req Data (6 * N Bytes)	Reason (1byte), 见 5.3.6
		Rsv (2bytes)
注 1: Req Cnt: 本次删除的节点数量。 注 2: Req Data: 本次删除的白名单节点数据，每个节点 6 个字节（大端）。 注 3: State: 0 表示成功；1 表示失败，失败原因见 Reason。 注 4: Reason: 取值含义请参见“异常状态代码”。		

6.3.3.12 清空白名单 (0014H)

清空白名单，见表 28。

表 28 清空白名单

方向	主控设备下发到模组	模组应答
Cmd	0014H	0014H
Data	空	State (1byte)
		Reason (1byte), 见 5.3.6
		Rsv (2bytes)
注 1: State: 0 表示成功；1 表示失败，失败原因见 Reason。 注 2: Reason: 取值含义请参见“异常状态代码”。		

6.3.3.13 自组网功能开启（0015H）

自组网功能开启，见表 29。

表 29 自组网功能开启

方向	主控设备下发到模组	模组应答
Cmd	0015H	0015H
Data	空	ret_code (1byte)
		reason (1 byte)
		reserved (2 byte)
注 1: 本命令只能在 CCO 端操作，操作后需要重启生效，自组网结束后自组网功能自动关闭。 注 2: Data 域字段说明： 注 3: ret_code: 清除结果。0 表示成功；1 表示失败，失败原因见 Reason。 注 4: Reason: 取值含义请参见“异常状态代码”。 注 5: reserved: 保留。		

6.3.3.14 设置白名单状态（0016H）

设置白名单状态，见表 30。

表 30 设置白名单状态

方向	主控设备下发到模组	模组应答
Cmd	0016H	0016H
Data	Whitelist State (1byte)	State (1Bte)
	Rsv (3bytes)	Rsv (3bytes)
注 1: Whitelist State: 白名单状态，0 表示关闭白名单，1 表示开启白名单。 注 2: State: 0-表示成功；1-表示失败。		

6.3.3.15 获取白名单状态（0017H）

获取白名单状态，见表 31。

表 31 获取白名单状态

方向	主控设备下发到模组	模组应答
Cmd	0017H	0017H
Data	空	Whitelist State (1bte)
		Rsv (3bytes)
注: Whitelist State: 白名单状态，0 表示白名单为关闭状态，1 表示白名单为开启状态。		

6.3.3.16 读取拓扑中节点数量 (0020H)

读取拓扑中节点数量，见表 32。

表 32 读取拓扑中节点数量

方向	主控设备下发到模组	模组应答
Cmd	0020H	0020H
Data	空	节点数量 (2bytes)
		保留 (2bytes) 0000H

6.3.3.17 读取拓扑中节点信息 (0021H)

读取拓扑中节点信息，见表 33。

表 33 读取拓扑中节点信息

方向	主控设备下发到模组	模组应答
Cmd	0021H	0021H
Data	Start Seq (2Bytes)	Total (2Bytes)
	Req Cnt (2Bytes)	Start Seq (2Bytes)
		Ind Cnt (2Bytes)
		Rsv (2bytes) 0000H
		Ind Data (12 * N Bytes)
注 1: Start Seq: 起始序号，从 1 开始，其中 1 为主节点，后续为从节点。每次查询必须从序号 1 起始查询。 注 2: Req Cnt: 本次查询的节点数量。 注 3: Total: 拓扑中节点总数量。 注 4: Ind Cnt: 本次应答的节点数量。 注 5: Ind Data: 本次应答的拓扑数据，每个节点 11 个字节。		

应答的拓扑数据格式，见表 34。

表 34 应答的拓扑数据

数据内容	格式	字节数
MAC Addr	BIN	6
Tei	BIN	2
Proxy Tei	BIN	2
Node Info	BIN	1
Rsv	BIN	1
注 1: MAC Addr: 6 字节，大端序。 注 2: Tei: 本节点的节点标识，最大不超过 512。 注 3: Proxy Tei: 本站点的代理站点节点标识 注 4: Node Info: 节点信息，[3:0]代表本站点的网络层级，0 代表 0 层级，依次类推； [7:4]表示本站点的网络角色，0 无效，1 表示末梢节点(STA)，2 表示代理节点，3 保留，4 表示主节点。		

6.3.4 信道转发命令详细说明

信道转发命令通过模组转发数据到对端设备，数据交互流程，如图 7。

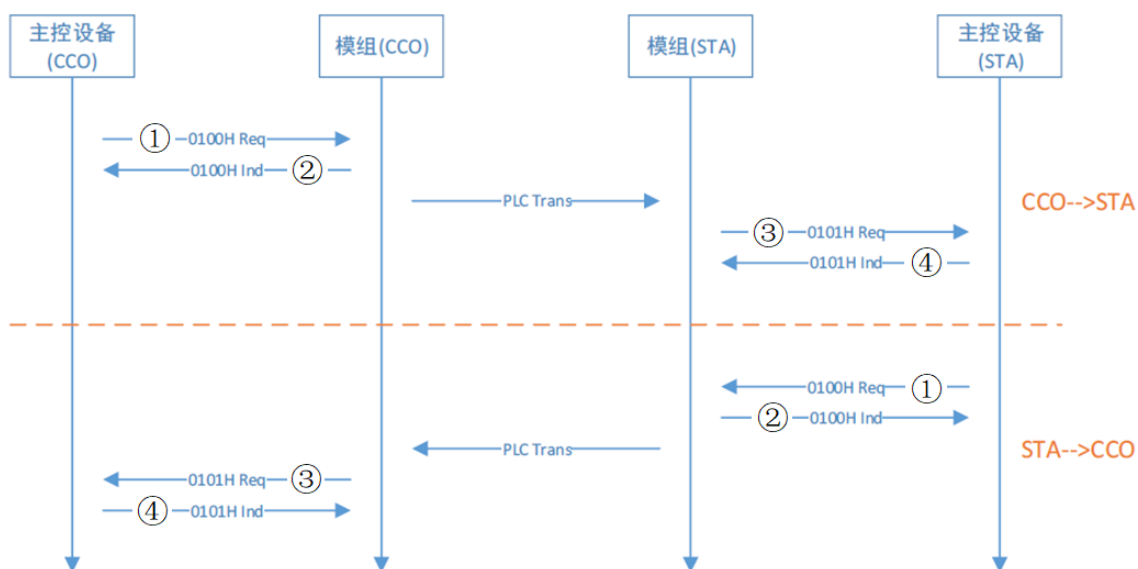


图 7 信道转发命令数据交互流程

6.3.4.1 发送数据 (0100H)

当主控设备需要发送报文给模组时，发送数据格式，见表 35。

表 35 发送数据

方向	主控设备下发到模组	模组应答
Cmd	0100H ①	0100H ②
Data	Dest Addr (6bytes)	State (1byte)
	User Data Len (2bytes)	Reason (1byte)
	User Data	Rsv (2bytes)
注 1: Dest Addr: 对端目的设备 MAC 地址; FF FF FF FF FF FF 表示全网广播。 注 2: User Data Len: User Data 数据长度, 最大值为 488。 注 3: User Data: 待发送的用户数据。 注 4: State: 0 表示成功; 1 表示失败, 失败原因见 Reason。 注 5: Reason: 取值含义请参见“异常状态代码”。		

6.3.4.2 接收数据 (0101H)

当模组需要发送报文给主控设备时，接收数据格式，见表 36。

表 36 接收数据

方向	模组发送到主控设备	主控设备应答
Cmd	0101H ③	0101H ④
Data	Src Addr (6bytes)	State (1byte)
	User Data Len (2bytes)	Reason (1byte)
	User Data	Rsv (2bytes)

注 1: Src Addr: 发送数据设备的 MAC 地址。
注 2: User Data Len: User Data 数据长度。
注 3: User Data: 待发送的用户数据。
注 4: State: 0 表示成功; 1 表示失败, 失败原因见 Reason。
注 5: Reason: 取值含义请参见“异常状态代码”。

6.3.5 远程调测命令

远程命令是通过中心节点转发本地命令到远程节点, 用于远程调试时通过 CCO 发送指令到 STA。数据交互流程, 如图 8。

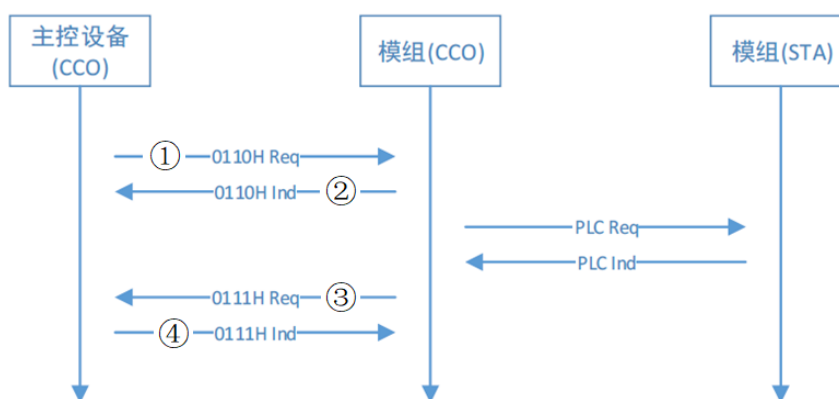


图 8 远程调测命令数据交互流程

6.3.5.1 远程发送命令 (0110H)

远程发送命令, 见表 37。

表 37 远程发送命令

方向	主控设备下发到模组	模组应答
Cmd	0110H ①	0110H ②
Data	Dest Addr (6bytes)	State (1byte)
	User Data Len (2bytes)	Reason (1byte)
	User Data	Rsv (2bytes)
注 1: Dest Addr: 目的设备 MAC 地址; FF FF FF FF FF FF 表示全网广播。 注 2: User Data Len: User Data 数据长度。 注 3: User Data: 待转发的本地通信命令。 注 4: State: 0 表示成功; 1 表示失败, 失败原因见 Reason。 注 5: Reason: 取值含义请参见“异常状态代码”。		

6.3.5.2 远程接收命令 (0111H)

远程接收命令, 见表 38。

表 38 远程接收命令

方向	模组发送到主控设备	主控设备应答
Cmd	0111H ③	0111H ④
Data	Src Addr (6bytes)	State (1byte)
	User Data Len (2bytes)	Reason (1byte)
	User Data	Rsv (2bytes)
注 1: Src Addr: 发送数据设备的 MAC 地址。 注 2: User Data Len: User Data 数据长度。 注 3: User Data: 待转发的本地通信命令应答。 注 4: State: 0 表示成功; 1 表示失败, 失败原因见 Reason。 注 5: Reason: 取值含义请参见“异常状态代码”。		

6.3.5.3 调测支持的本地命令

调测支持的本地命令, 见表 39。

表 39 调测支持的本地命令

Cmd	说明
0001H	读取模组版本信息
0002H	读取模组 MAC 地址
0003H	读取模组通信地址
0004H	设置模组通信地址
0005H	模组重启
0006H	传输文件

6.3.6 系统控制数据通信命令

系统控制数据通信命令是在信道转发命令的基础上，简化其通信流程。数据交互流程，如图 9。

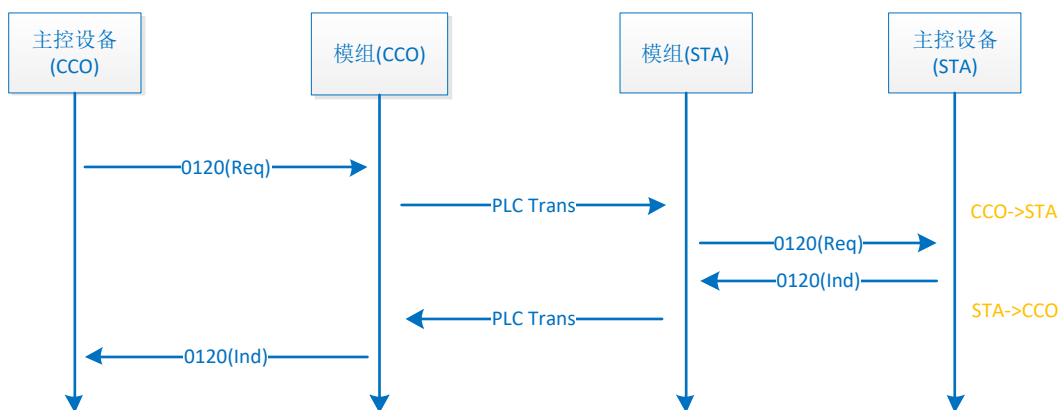


图 9 系统控制数据通信命令数据交互流程

6.3.6.1 系统控制数据通信命令（0120H）

系统控制数据通信命令，见表 40。

表 40 系统控制数据通信命令

方向	主控设备 (CCO) 到主控设备 (STA)	主控设备 (STA) 到主控设备 (CCO)
Cmd	0120H ①	0120H ②
Data	Dest Addr (6bytes)	Src Addr (6bytes)
	User Data Len (2bytes)	User Data Len (2bytes)
	User Data	User Data
注 1: Dest Addr: 对端目的设备 MAC 地址; FF FF FF FF FF FF 表示全网广播。		
注 2: User Data Len: User Data 数据长度。		
注 3: User Data: 待发送的用户数据。		

6.3.7 异常状态代码

异常状态代码，见表 41。

表 41 异常状态代码

取值	说明
00H	状态正常
01H	通信超时
02H	错误的格式
03H	节点忙
FFH	其它错误

6.4 PLC 应用报文

6.4.1 PLC ID

PLC ID 定义，见表 42。

表 42 PLC ID

取值	说明
50H	数据转发
51H	远程命令
55H	系统控制数据通信

6.4.2 报文格式

PLC 应用报文格式，见表 43。

表 43 PLC 应用报文格式

长度 (byte)	2	2	L
含义	CRC	L	User Data
注 1: CRC: User Data 的 CRC16 校验和, 从帧头开始到 Data 段结束。CRC 校验生成多项式采用 CRC16-CCITT(0x1021), $x^{16}+x^{12}+x^5+1$ 。			
注 2: L: User Data 长度。			
注 3: User Data: 待发送的报文。			

7 系统控制协议

系统由受控设备和控制设备组成，以下以照明系统作为参考。PLC 网关由主控处理器和 PLC 模组组成，主控处理器与 PLC 模组之间通过 UART 串口进行通信。其他控制设备的主控单元可以是 PLC 模组，也可以是 PLC 模组加外挂处理器。当控制设备的主控单元是 PLC 模组时，PLC 模组需完成控制设备的全部通信和控制功能。当控制设备的主控单元是 PLC 模组加外挂处理器时，PLC 模组通信数据通过 UART 接口与处理器进行通信，处理器完成数据处理和控制功能。

主控处理器与 PLC 模组之间的通信遵循“PLC 模组接口协议”。照明系统 PLC 网关与 STA 控制设备之间的控制数据包采用协议“6.3.6 总线数据通信命令”中的“6.3.6.1 总线数据通信命令 (0120H)”来完成。总线数据通信命令数据交互流程，如图 10。

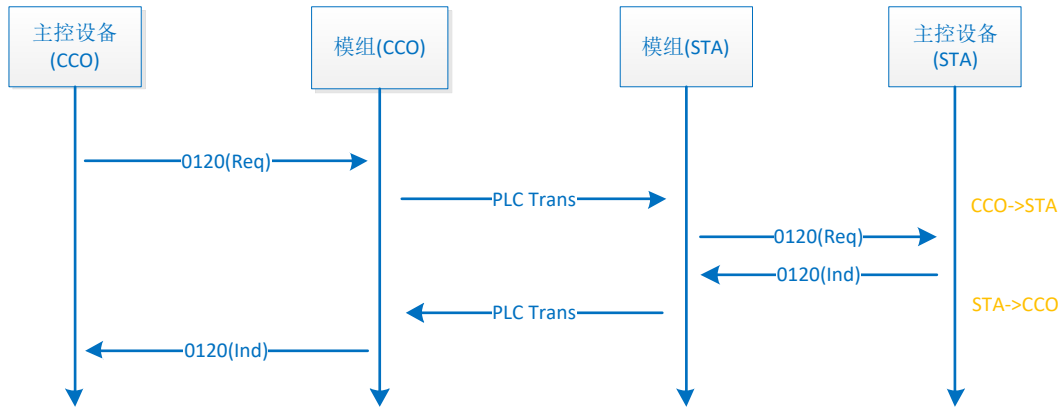


图 10 总线数据通信命令数据交互流程

7.1 发送数据

当一个设备需要发送“控制报文”给远端设备时，使用格式，见表 44。

表 44 发送数据

方向	主控设备下发到模组	
Cmd	0120H ①	
Data	Dest MAC Addr (6bytes)	
	UserData Len (2bytes)	
	UserData	PLC 协议主版本号 (1byte)
		PLC 协议次版本号 (1byte)
		Sequence Number (2bytes)
		Func Code (1byte)
		Status Code (1byte)
		DEV Addr (2bytes)
Data Body		

7.2 接收数据

当模组需要转发远端设备发来“控制报文”给主控设备时，使用格式，见表 45。

表 45 接收数据

方向	模组发送到主控设备	
Cmd	0120H ③	
Data	Src MAC Addr (6bytes)	
	UserData Len (2bytes)	
	UserData	PLC 协议主版本号 (1byte)
		PLC 协议次版本号 (1byte)
		Sequence Number (2bytes)

表 45 接收数据（续）

方向	模组发送到主控设备	
Data	UserData	Func Code (1byte)
		Status Code (1byte)
		DEV Addr (2bytes)
		Data Body

Cmd: 0120H 是主控设备和模组直接的串口通信命令码。

Dest MAC Addr: 远端目的设备通信 MAC 地址; FF FF FF FF FF FF 表示全网广播。

当 CCO 给 STA 发送报文时, 目的设备通信地址指 STA 的 MAC 地址。

当 STA 给 CCO 发送报文时, 目的设备通信地址指 CCO 的 MAC 地址。

Src MAC Addr: 发送数据设备通信的 MAC 地址。

当 CCO 给 STA 发送报文时, 发送数据设备通信地址指 CCO 的 MAC 地址。

当 STA 给 CCO 发送报文时, 发送数据设备通信地址指 STA 的 MAC 地址。

UserDataLen: UserData 数据长度。

UserData: 待接收的用户数据。是模组 (CCO) 和模组 (STA) 通过 PLC 通信传输的系统控制协议报文。

PLC 协议主/次版本号: 用于 PLC 协议版本兼容性扩展预留, 需要根据 PLC 协议版本解析响应报文。当前分别为 1 和 0。

Sequence Number: 网关 CCO 向 STA 发送报文的递增序号, STA 在响应报文时返回此序号, 用于网关标识报文响应。

Func Code: 功能码, 用于定义该指令的操作功能。

Status Code: 状态码, 用于定义该指令应答状态。

State: 0 表示成功; 1 表示失败, 失败原因见 Reason。

Reason: 取值含义请参见“异常状态代码”。

DEV Addr: 设备应用地址。

Data Body: 功能命令数据。

7.2.1 功能码 (Func Code) 格式,

功能码格式, 见表 46。

表 46 功能码格式

B7	B6	B5	B4	B3	B2	B1	B0
F	x						
注 1: “F” 数据方向位: “F” =0 表示数据帧来自发起设备。 “F” =1 表示数据帧来自响应设备。 注 2: “x” 表示功能代码							

功能代码定义，见表 47。

表 47 功能码具体定义

发起设备 Func Code	功能名称	响应设备 Func Code
0x01	查询设备信息	0x81
0x02	写入设备应用地址	0x82
0x03	读取设备应用地址	0x83
0x04	添加 N 个组地址	0x84
0x05	读取全部组地址	0x85
0x06	删除 N 个组地址	0x86
0x07	写入设备属性	0x87
0x08	读取设备属性	0x88
0x09	上报设备属性	0x89
0x0A	上报设备事件	0x8A
0x0B	N 个设备添加/删除 1 个组地址	0x8B
0x0C	设置场景	0x8C
0x0D	查询场景校验值	0x8D
0x0E	执行场景	0x8E
0x0F	删除场景	0x8F
0x10	获取心跳	0x90
0x11	重启设备	0x91
0x12	转发报文	无
0x13	查询场景	0x93
0x14	设备初始化	0x94

7.2.2 响应状态码 (Status Code)

响应状态码，见表 48。

表 48 Status Code 响应状态码定义

Status Code	描述
0x00	成功
0x01	无法解析此请求
0x02	设备控制受限中
0x03	属性不可读
0x04	属性不可写
0x05	参数值错误
0x06	未定义

接收端按照上面的响应状态定义返回 Status Code 信息。

发送端的 Status Code 用于保留承载特殊指令，目前使用了 Bit0 和 Bit1。

Bit0: 表示控制目标设备不响应报文，“1”不回应，用于避免批量设备响应导致信道拥塞；“0”回应，用于单设备控制；

Bit1: “1”表示控制目标设备收到指令后的静默时间内（5 秒）不主动上报设备属性变化，静默时间后，直到再次有属性变化才上报，用于避免批量设备同时上报属性变化导致信道拥塞，后续可以通过读设备属性的命令码获取设备属性；“0”表示允许主动上报属性变化，用于单设备控制。

发送端的 Status Code 示例：

0x00 即 0b00000000（返回响应报文，允许上报属性变化）

0x01 即 0b00000001（不返回响应报文，允许上报属性变化）

0x03 即 0b00000011（不返回响应报文，此时不上报属性变化）

7.2.3 数据类型（Data Type）

数据类型长度列表定义，见表 49。

表 49 Data Type 数据类型长度列表定义

Data Type	数据类型	Data Value 长度值 (byte)	取值范围	描述
0x0001	int	4	-2147483648~2147483647	整数
0x0002	Bool	1	0, 1	布尔
0x0003	string	n 可变长度		字符串
0x0004	emun	1	0—255	枚举
0x0005	array	n 可变长度		数组

7.2.4 应用地址（DEV Addr）

应用地址（DEV Addr）范围定义，见表 50。

表 50 应用地址（DEV Addr）范围定义

DEV Addr	应用地址定义
0x0000	保留
0x0001~0x000F	保留给 CCO 使用
0x0010~0x03FF	通过设备标识被分配使用的设备应用地址，
0x0400~0x07FF	无设备标识被分配使用的设备应用地址
0x0800~0x0BFF	设备标识冲突后被分配使用的设备应用地址
0x4000~0x40FF	组播地址（网关支持 256 个组，终端设备存储 32 个组）
0x4100~0xFFFFD	保留
0xFFFFE	出厂未分配应用地址时的值
0xFFFFF	广播地址

在 PLC 总线网络内每个设备需要一个应用地址（2 字节），不同于物理地址，应用地址对应用层提供可见的逻辑地址，方便设备的管理和数据的传输。在 PLC 设备处于应用状态时（非配置状态），使用 MAC 广播寻址方式，并通过使用应用地址在网络中提供单播、组播和广播的通信控制。

7.3 功能命令详解

7.3.1 查询设备信息（Func Code =0x01）

PLC网关（CC0）查询某个（STA）设备信息，低字节在前，高字节在后。格式，见表51。

表 51 查询设备信息

方向	主控设备MCU下发到CC0模组		
Cmd	0120H ①	0x0120	
Data	Dest MAC Addr (6bytes)	xx xx xx xx xx xx (STA MAC Addr)	
	UserData Len (2bytes)	xx xx	
	UserData	PLC协议主版本号 (1byte)	xx
		PLC协议次版本号 (1byte)	xx
		Sequence Number (2bytes)	xx xx
		Func Code (1byte)	0x01
		Status Code (1byte)	0x00
DEV Addr (2bytes)		0x0000	

（STA）设备响应，把应用地址（2BYTES）反馈给 CC0。格式，见表 52。

表 52 查询设备信息响应

方向	设备MCU下发到STA模组		
Cmd	0120H ①	0x0120	
Data	Dest MAC Addr (6bytes)	xx xx xx xx xx xx (CC0 MAC Addr)	
	UserData Len (2bytes)	xx xx	
	UserData	PLC协议主版本号 (1byte)	xx
		PLC协议次版本号 (1byte)	xx
		Sequence Number (2bytes)	xx xx
		Func Code (1byte)	0x81
		Status Code (1byte)	0x00 ~ 0x06
		DEV Addr (2bytes)	xx xx
		Data Type (2bytes)	0x03 (String)
		Data Len (2bytes)	xx xx
Dev Infor String (n bytes)		设备信息字符串，格式为： key:value, key:value	

（1）设备信息字符串

返回设备信息由ASCII码字符串组成，格式为：key:value, key:value, key和value直接使用英文冒号分割，两组之间使用英文逗号分割，字符串总长度不超过255。

示例：

sn:12345678,prodId:1234,model:Model5,devType:075,manu:123,mac:00D8613E897B,hiv:1.0.0,fwv:1.0.0,hwv:1.0.0,swv:1.0.0,protType:1,subProdId:01,devCode:01

设备信息字段说明，见表 53。

表 53 设备信息字段说明

设备信息 key 名称	设备信息 value 说明	是否必填	设备信息 value 示例
sn	设备唯一标识，比如 sn 号，长度范围 (0, 40]	是	12345678
prodId	设备产品 ID，即 ProductId，长度为 4	是	1234
model	设备型号，长度范围 (0, 32]	是	Model5
devType	设备类型 ID，长度为 3	是	075
manu	设备制造商 ID，长度为 3	是	123
mac	设备 MAC 地址，固定 12 字节	是	00D8613E897B
hiv	设备协议版本，长度范围 (0, 32]	是	1.0.0
fwv	设备固件版本，长度范围 [0, 64]	是	1.0.0
hwv	设备硬件版本，长度范围 [0, 64]	是	1.0.0
swv	设备软件版本，长度范围 [0, 64]	是	1.0.0
protType	设备协议类型，取值范围 [1, 3]	是	1
subProdId	设备子型号 ID，长度为 2，如果不支持则不返回此字段	可选	01
devCode	设备标识编码，长度为 4，范围 0001-FFFF，使用 Hex String 表示两个字节的四位，例如：000F 表示十进制的 15，如果不支持则不返回此字段	可选	000F

7.3.2 写入设备应用地址 (Func Code =0x02)

PLC网关 (CCO) 远程对设备 (STA) 写入应用地址 DEV Addr (2bytes)，低字节在前，高字节在后。格式，见表54。

表 54 写入设备应用地址

方向	主控设备MCU下发到CCO模组		
Cmd	0x0120H ①	0x0120	
Data	Dest MAC Addr (6bytes)	xx xx xx xx xx xx (STA MAC Addr)	
	UserData Len (2bytes)	xx xx	
	UserData	PLC协议主版本号 (1byte)	xx
		PLC协议次版本号 (1byte)	xx
		Sequence Number (2bytes)	xx xx
		Func Code (1byte)	0x02
		Status Code (1byte)	0x00
DEV Addr (2bytes)		xx xx	

远程设备（STA）响应，把应用地址(2BYTES)反馈给CCO。格式，见表55。

表 55 写入设备应用地址响应

方向	设备MCU下发到STA模组		
Cmd	0x0120H ①	0x0120	
Data	Dest MAC Addr (6bytes)	xx xx xx xx xx xx (CCO MAC Addr)	
	UserData Len (2bytes)	xx xx	
	UserData	PLC协议主版本号 (1byte)	xx
		PLC协议次版本号 (1byte)	xx
		Sequence Number (2bytes)	xx xx
		Func Code (1byte)	0x82
		Status Code (1byte)	0x00 ~ 0x06
DEV Addr (2bytes)		xx xx	

7.3.3 读取设备应用地址 (Func Code =0x03)

PLC 网关（CCO）读取某个远程设备（STA）应用地址，低字节在前，高字节在后。格式，见表56。

表 56 读取设备应用地址

方向	主控设备MCU下发到CCO模组		
Cmd	0x0120H ①	0x0120	
Data	Dest MAC Addr (6bytes)	xx xx xx xx xx xx (STA MAC Addr)	
	UserData Len (2bytes)	xx xx	
	UserData	PLC协议主版本号 (1byte)	xx
		PLC协议次版本号 (1byte)	xx
		Sequence Number (2bytes)	xx xx
		Func Code (1byte)	0x03
		Status Code (1byte)	0x00
DEV Addr (2bytes)		0000	

远程设备（STA）响应，把应用地址(2bytes)反馈给CCO。格式，见表57。

表 57 读取设备应用地址响应

方向	设备MCU下发到STA模组		
Cmd	0x0120H ①	0x0120	
Data	Dest MAC Addr (6bytes)	xx xx xx xx xx xx (CCO MAC Addr)	
	UserData Len (2bytes)	xx xx	
	UserData	PLC协议主版本号 (1byte)	xx
		PLC协议次版本号 (1byte)	xx

表 57 读取设备应用地址响应（续）

方向	设备MCU下发到STA模组		
Data	UserData	Sequence Number (2bytes)	xx xx
		Func Code (1byte)	0x83
		Status Code (1byte)	0x00 ~ 0x06
		DEV Addr (2bytes)	xx xx

7.3.4 添加 N 个组地址（Func Code =0x04）

PLC网关（CCO）远程对单个设备（STA）写入N个组地址Group Addr。见表58。

表 58 添加 N 个组地址

方向	主控设备MCU下发到CCO模组		
Cmd	0x0120H ①		0x0120
Data	Dest MAC Addr (6bytes)		xx xx xx xx xx xx (STA MAC Addr)
	UserData Len (2bytes)		xx xx
	UserData	PLC协议主版本号 (1byte)	xx
		PLC协议次版本号 (1byte)	xx
		Sequence Number (2bytes)	xx xx
		Func Code (1byte)	0x04
		Status Code (1byte)	0x00
		DEV Addr (2 bytes)	xx xx
		Group Number (2byte)	xx xx
		Group Addr1 (2bytes)	xx xx
		Group Addr2 (2bytes)	xx xx
		
Group AddrN (2bytes)	xx xx		

远程设备（STA）在写入组地址后，给 CCO 的响应报文。见表 59。

表 59 添加 N 个组地址响应

方向	设备MCU下发到STA模组		
Cmd	0x0120H ①		0x0120
Data	Dest MAC Addr (6bytes)		xx xx xx xx xx xx (CCO MAC Addr)
	UserData Len (2bytes)		xx xx
	UserData	PLC协议主版本号 (1byte)	xx
		PLC协议次版本号 (1byte)	xx
		Sequence Number (2bytes)	xx xx
		Func Code (1bytes)	0x84
		Status Code (1byte)	0x00 ~ 0x06
		DEV Addr (2 bytes)	xx xx

7.3.5 读取全部组地址 (Func Code =0x05)

PLC网关 (CCO) 远程读取某个设备 (STA) 全部组地址Group Addr (2bytes)。见表60。

表 60 读取全部组地址

方向	主控设备MCU下发到CCO模组		
Cmd	0x0120H ①	0x0120	
Data	Dest MAC Addr (6bytes)	xx xx xx xx xx xx (STA MAC Addr)	
	UserData Len (2bytes)	xx xx	
	UserData	PLC协议主版本号 (1byte)	xx
		PLC协议次版本号 (1byte)	xx
		Sequence Number (2bytes)	xx xx
		Func Code (1byte)	0x05
		Status Code (1byte)	0x00
DEV Addr (2bytes)		xx xx	

远程设备 (STA) 给 CCO 的响应报文。见表 61。

表 61 读取全部组地址响应

方向	设备MCU下发到STA模组		
Cmd	0x0120H ①	0x0120	
Data	Dest MAC Addr (6bytes)	xx xx xx xx xx xx (CCO MAC Addr)	
	UserDataLen (2bytes)	xx xx	
	UserData	PLC协议主版本号 (1byte)	xx
		PLC协议次版本号 (1byte)	xx
		Sequence Number (2bytes)	xx xx
		Func Code (1bytes)	0x85
		Status Code (1byte)	0x00 ~ 0x06
		DEV Addr (2 bytes)	xx xx
		Group Number (2byte)	xx xx
		Group Addr1 (2bytes)	xx xx
		Group Addr2 (2bytes)	xx xx
		
Group AddrN (2bytes)	xx xx		

7.3.6 删除 N 个组地址 (Func Code =0x06)

PLC 网关 (CCO) 删除某个远程设备 (STA) 的 N 个组地址, 低字节在前, 高字节在后。见表 62。

表 62 删除 N 个组地址

方向	主控设备MCU下发到CCO模组		
Cmd	0x0120H ①	0x0120	
Data	Dest MAC Addr (6bytes)	xx xx xx xx xx xx (STA MAC Addr)	
	UserData Len (2bytes)	xx xx	
	UserData	PLC协议主版本号 (1byte)	xx
		PLC协议次版本号 (1byte)	xx
		Sequence Number (2bytes)	xx xx
		Func Code (1byte)	0x06
		Status Code (1byte)	0x00
		DEV Addr (2 bytes)	xx xx
		Group Number (2byte)	xx xx
		Group Addr1 (2bytes)	xx xx
		Group Addr2 (2bytes)	xx xx
.....			
Group AddrN (2bytes)	xx xx		

远程设备 (STA) 给 CCO 的响应报文。见表 63。

表 63 删除 N 个组地址响应

方向	设备MCU下发到STA模组		
Cmd	0x0120H ①	0x0120	
Data	Dest MAC Addr (6bytes)	xx xx xx xx xx xx (CCO MAC Addr)	
	UserDataLen (2bytes)	xx xx	
	UserData	PLC协议主版本号 (1byte)	xx
		PLC协议次版本号 (1byte)	xx
		Sequence Number (2bytes)	xx xx
		Func Code (1bytes)	0x86
		Status Code (1byte)	0x00 ~ 0x06
DEV Addr (2 bytes)	xx xx		

7.3.7 写入设备属性 (Func Code =0x07)

PLC 网关 (CCO) 单播或广播方式对设备写入多组属性参数, 受控设备 (STA) 地址可以是单地址、组地址或广播地址。见表 64。

表 64 写入设备属性

方向	主控设备MCU下发到CCO模组		
Cmd	0x0120H ①	0x0120	
Data	Dest MAC Addr (6bytes)	广播: FF FF FF FF FF FF 单播: xx xx xx xx xx xx (STA MAC Addr)	
	UserData Len (2bytes)	xx xx	
	UserData	PLC协议主版本号 (1byte)	xx
		PLC协议次版本号 (1byte)	xx
		Sequence Number (2bytes)	xx xx
		Func Code (1byte)	0x07
		Status Code (1byte)	0x00 (返回响应报文, 允许上报属性变化) 0x03 (不返回响应报文, 此时不上报属性变化, 组控设备时使用)
		DEV Addr (2bytes)	xx xx (单地址、组地址、广播地址)
		Siid (2bytes)	
		Ciid (2bytes)	
		Data Type (2byte)	
		Data Len (2bytes)	
		Data Value (n byte)	
		...	
		Siid (2bytes)	
		Ciid (2bytes)	
		Data Type (2byte)	
		Data Len (2bytes)	
		Data Value (n byte)	
		注1: Siid: 服务(service) ID, 用来表示设备中用户可使用的功能函数, 其中包含实现该函数输出/输入的数据以及实现该函数的行为。	
注2: Ciid: 属性(characteristic) ID, 表示数据或相关行为的特征, 名称之为属性名, 是Service的基本组成单元, 如开关的开或关特性。			

远程设备（STA）给 CCO 的响应报文。见表 65。

表 65 写入设备属性响应

方向	设备MCU下发到STA模组		
Cmd	0x0120H ①	0x0120	
Data	Dest MAC Addr (6bytes)	xx xx xx xx xx xx (CCO MAC Addr)	
	UserDataLen (2bytes)	xx xx	
	UserData	PLC协议主版本号 (1byte)	xx
		PLC协议次版本号 (1byte)	xx
		Sequence Number (2bytes)	xx xx
		Func Code(1bytes)	0x87
		Status Code (1byte)	0x00 ~ 0x06
DEV Addr (2 bytes)		xx xx	

7.3.8 读取设备属性 (Func Code =0x08)

PLC 网关 (CCO) 单播或广播方式读某个 (DEV ADDR) 设备多个属性参数到 CCO。见表 66。

表 66 读取设备属性

方向	主控设备MCU下发到CCO模组		
Cmd	0x0120H ①	0x0120	
Data	Dest MAC Addr (6bytes) ^{#a}	广播: FF FF FF FF FF FF 单播: xx xx xx xx xx xx (STA MAC Addr)	
	UserData Len (2bytes)	xx xx	
	UserData	PLC协议主版本号 (1byte)	xx
		PLC协议次版本号 (1byte)	xx
		Sequence Number (2bytes)	xx xx
		Func Code (1byte)	0x08
		Status Code (1byte)	0x00
		DEV Addr(2bytes)	xx xx
		Siid (2bytes)	
		Ciid (2bytes)	
		
		Siid (2bytes)	
Ciid (2bytes)			

注: # a: Dest MAC Addr 目标地址可以是广播地址, 也可以是 STA 的 MAC 地址。当不填写 Siid 和 Ciid 时, 表示要求返回所有服务和属性的值。

远程设备（STA）给CCO的响应报文。见表67。

表 67 读取设备属性响应

方向	设备MCU下发到STA模组		
Cmd	0x0120H ①	0x0120	
Data	Dest MAC Addr (6bytes)	xx xx xx xx xx xx (CCO MAC Addr)	
	UserDataLen (2bytes)	xx xx	
	UserData	PLC协议主版本号 (1byte)	xx
		PLC协议次版本号 (1byte)	xx
		Sequence Number (2bytes)	xx xx
		Func Code (1byte)	0x88
		Status Code (1byte)	0x00 ~ 0x06
		DEV Addr (2bytes)	xx xx
		Siid (2bytes)	
		Ciid (2bytes)	
		Data Type (2byte)	
		Data Len (2bytes)	
		Data Value (n byte)	
		
		Siid (2bytes)	
		Ciid (2bytes)	
		Data Type (2byte)	
Data Len (2bytes)			
Data Value (n byte)			

7.3.9 上报设备属性 (Func Code =0x09)

STA 设备 (DEV ADDR) 上报属性数据给 CCO。见表 68。

表 68 上报设备属性

方向	主控设备MCU下发到STA模组		
Cmd	0x0120H ①	0x0120	
Data	Dest MAC Addr (6bytes)	xx xx xx xx xx xx (CCO MAC Addr)	
	UserData Len (2bytes)	xx xx	
	UserData	PLC协议主版本号 (1byte)	xx
		PLC协议次版本号 (1byte)	xx
		Sequence Number (2bytes)	xx xx
		Func Code (1byte)	0x09
		Status Code (1byte)	0x00 ~ 0x06
		DEV Addr(2bytes)	0x00
		Siid (2bytes)	
		Ciid (2bytes)	
		Data Type (2byte)	
		Data Len (2bytes)	
		Data Value (nbyte)	
		
		Siid (2bytes)	
		Ciid (2bytes)	
Data Type (2byte)			
Data Len (2bytes)			
Data Value (nbyte)			

CCO 给远程设备 (STA) 的响应报文。见表 69。

表 69 上报设备属性

方向	设备MCU下发到STA模组		
Cmd	0x0120H ①	0x0120	
Data	Dest MAC Addr (6bytes)	FF FF FF FF FF FF	
	UserDataLen (2bytes)	xx xx	
	UserData	PLC协议主版本号 (1byte)	xx
		PLC协议次版本号 (1byte)	xx
		Sequence Number (2bytes)	xx xx
		Func Code (1byte)	0x89
		Status Code (1byte)	0x00 ~ 0x06
		DEV Addr(2bytes)	xx xx

7.3.10 上报设备事件 (Func Code =0x0A)

STA 设备 (DEV ADDR) 上报事件数据给 CCO。见表 70。

表 70 上报设备事件

方向	主控设备MCU下发到STA模组		
Cmd	0x0120H ①	0x0120	
Data	Dest MAC Addr (6bytes)	xx xx xx xx xx xx (CCO MAC Addr)	
	UserData Len (2bytes)	xx xx	
	UserData	PLC协议主版本号 (1byte)	xx
		PLC协议次版本号 (1byte)	xx
		Sequence Number (2bytes)	xx xx
		Func Code (1byte)	0x0A
		Status Code (1byte)	0x00
		DEV Addr (2bytes)	xx xx
		Siid (2bytes)	
		Ciid (2bytes)	
		Data Type (2byte)	
		Data Len (2bytes)	
		Data Value (n byte)	
		
		Siid (2bytes)	
		Ciid (2bytes)	
		Data Type (2byte)	
Data Len (2bytes)			
Data Value (n byte)			

CCO 给远程设备（STA）的响应报文。见表 71。

表 71 上报设备事件响应

方向	设备MCU下发到STA模组		
Cmd	0x0120H ①	0x0120	
Data	Dest MAC Addr (6bytes)		FF FF FF FF FF FF
	UserDataLen (2bytes)		xx xx
	UserData	PLC协议主版本号 (1byte)	xx
		PLC协议次版本号 (1byte)	xx
		Sequence Number (2bytes)	xx xx
		Func Code (1byte)	0x8A
		Status Code (1byte)	0x00 ~ 0x06
		DEV Addr (2bytes)	xx xx

7.3.11 N 个设备添加/删除 1 个组地址 (Func Code =0x0B)

PLC网关（CCO）对远程N个设备（STA）添加或删除1个组地址Group Addr (2bytes)。见表72。

表 72 N 个设备添加/删除 1 个组地址

方向	主控设备MCU下发到CCO模组		
Cmd	0x0120H ①	0x0120	
Data	Dest MAC Addr (6bytes)		FF FF FF FF FF FF
	UserData Len (2bytes)		xx xx
	UserData	PLC协议主版本号 (1byte)	xx
		PLC协议次版本号 (1byte)	xx
		Sequence Number (2bytes)	xx xx
		Func Code (1byte)	0x0B
		Status Code (1byte)	0x00
		DEV Addr (2bytes)	xx xx
		Group Action (2bytes)	xx xx (操作类型) 0x0001: 表示添加组 0x0002: 表示删除组
		Group Addr (2bytes)	xx xx (添加的组地址)
		Group Dev Number (2bytes)	xx xx (下面包含的设备数量)
		DEV Addr1 (2bytes)	xx xx (第1个设备地址)
		
DEV AddrN (2bytes)	xx xx (第N个设备地址)		
注：如果设备数量多，可以通过多个报文设置。			

远程设备（STA）给 CCO 的响应报文。见表 73。

表 73 N 个设备添加/删除 1 个组地址响应

方向	设备MCU下发到STA模组		
Cmd	0x0120H ①	0x0120	
Data	Dest MAC Addr (6bytes)	xx xx xx xx xx xx (CCO MAC Addr)	
	UserDataLen (2bytes)	xx xx	
	UserData	PLC协议主版本号 (1byte)	xx
		PLC协议次版本号 (1byte)	xx
		Sequence Number (2bytes)	xx xx
		Func Code (1bytes)	0x8B
		Status Code (1byte)	0x00 ~ 0x06
DEV Addr (2bytes)		xx xx	

7.3.12 设置场景 (Func Code =0x0C)

每个受控设备至少可配置多个个场景，场景可通过按键信号、时钟信号、传感器信号等进行触发，场景控制逻辑通过 PLC 网关进行配置，场景配置信息保存在每个受控设备内，当进行场景控制时，被寻址选中的受控设备可以实现同步响应。

PLC网关（CCO）对某类型设备（STA）写入若干场景。对不同类型的设备，场景需要分开设置。Siid、Ciid是设备物模型定义中的服务和属性编码，见表74。

表 74 设置场景

方向	主控设备MCU下发到CCO模组		
Cmd	0x0120H ①	0x0120	
Data	Dest MAC Addr (6bytes)	xx xx xx xx xx xx	
	UserData Len (2bytes)	xx xx	
	UserData	PLC协议主版本号 (1byte)	xx
		PLC协议次版本号 (1byte)	xx
		Sequence Number (2bytes)	xx xx
		Func Code (1byte)	0x0C
		Status Code (1byte)	0x00
		DEV Addr (2bytes)	xx xx
		Scene ID (2byte)	1- 65535
		Siid (2bytes)	
Ciid (2bytes)			

表 74 设置场景 (续)

方向	主控设备MCU下发到CCO模组		
Data	UserData	Data Type (2byte)	
		Data Len (2bytes)	
		Data Value (n byte)	
		
		Siid (2bytes)	
		Ciid (2bytes)	
		Data Type (2byte)	
		Data Len (2bytes)	
		Data Value (n byte)	

远程设备 (STA) 给 CCO 的响应报文。见表 75。

表 75 设置场景响应

方向	设备MCU下发到STA模组		
Cmd	0x0120H ①	0x0120	
Data	Dest MAC Addr (6bytes)		xx xx xx xx xx xx (CCO MAC Addr)
	UserDataLen (2bytes)		xx xx
	UserData	PLC协议主版本号 (1byte)	xx
		PLC协议次版本号 (1byte)	xx
		Sequence Number (2bytes)	xx xx
		Func Code(1bytes)	0x8C
		Status Code (1byte)	0x00 ~ 0x06
		DEV Addr (2bytes)	xx xx

7.3.13 查询场景校验值 (Func Code =0x0D)

PLC网关 (CCO) 查询某个设备 (STA) 的全部场景校验值。见表76。

表 76 查询场景校验值

方向	主控设备MCU下发到CCO模组		
Cmd	0x0120H ①	0x0120	
Data	Dest MAC Addr (6bytes)		xx xx xx xx xx xx
	UserData Len (2bytes)		xx xx
	UserData	PLC协议主版本号 (1byte)	xx
		PLC协议次版本号 (1byte)	xx
		Sequence Number (2bytes)	xx xx
		Func Code (1byte)	0x0D
		Status Code (1byte)	0x00
		DEV Addr (2bytes)	xx xx

远程设备 (STA) 给 CCO 的响应报文。见表 77。

表 77 查询场景校验值响应

方向	设备MCU下发到STA模组		
Cmd	0x0120H ①	0x0120	
Data	Dest MAC Addr (6bytes)		
	xx xx xx xx xx xx (CCO MAC Addr)		
	UserDataLen (2bytes)		
	xx xx		
	UserData	PLC协议主版本号 (1byte)	xx
		PLC协议次版本号 (1byte)	xx
		Sequence Number (2bytes)	xx xx
		Func Code (1byte)	0x8D
Status Code (1byte)		0x00 ~ 0x06	
DEV Addr (2bytes)		xx xx	
CRC 校验码 (2byte)	按场景 ID 从小到大 (升序) 排序的所有场景数据 CRC 校验和, CRC 校验生成多项式采用 CRC16-CCITT(0x1021), $x^{16}+x^{12}+x^5+1$ 。		

7.3.14 执行场景 (Func Code =0x0E)

PLC网关 (CCO) 控制设备 (STA) 执行某个场景 (场景号)。见表78。

表 78 执行场景

方向	主控设备MCU下发到CCO模组		
Cmd	0x0120H ①	0x0120	
Data	Dest MAC Addr (6bytes)		
	FF FF FF FF FF FF		
	UserData Len (2bytes)		
	xx xx		
	UserData	PLC协议主版本号 (1byte)	xx
		PLC协议次版本号 (1byte)	xx
		Sequence Number (2bytes)	xx xx
		Func Code (1byte)	0x0E
Status Code (1byte)		0x03 (不返回响应报文, 此时不上报属性变化)	
DEV Addr (2bytes)		xx xx	
Scene ID (2byte)	xx xx		

远程设备 (STA) 给 CCO 的响应报文。见表 79。

表 79 执行场景响应

方向	设备MCU下发到STA模组			
Cmd	0x0120H ①	0x0120		
Data	Dest MAC Addr (6bytes)		xx xx xx xx xx xx (CCO MAC Addr)	
	UserDataLen (2bytes)		xx xx	
	UserData	PLC协议主版本号 (1byte)		xx
		PLC协议次版本号 (1byte)		xx
		Sequence Number (2bytes)		xx xx
		Func Code(1bytes)		0x8E
		Status Code (1byte)		0x00 ~ 0x06
		DEV Addr (2bytes)		xx xx

7.3.15 删除场景 (Func Code =0x0F)

PLC网关 (CCO) 删除控制设备 (STA) 若干场景。见表80。

表 80 删除场景

方向	主控设备MCU下发到CCO模组			
Cmd	0x0120H ①	0x0120		
Data	Dest MAC Addr (6bytes)		FF FF FF FF FF FF	
	UserData Len (2bytes)		xx xx	
	UserData	PLC协议主版本号 (1byte)		xx
		PLC协议次版本号 (1byte)		xx
		Sequence Number (2bytes)		xx xx
		Func Code (1byte)		0x0F
		Status Code (1byte)		0x00
		DEV Addr(2bytes)		xx xx
Scene ID (2byte)		0表示删除所有场景		

远程设备 (STA) 给 CCO 的响应报文。见表 81。

表 81 删除场景响应

方向	设备MCU下发到STA模组			
Cmd	0x0120H ①	0x0120		
Data	Dest MAC Addr (6bytes)		xx xx xx xx xx xx (CCO MAC Addr)	
	UserDataLen (2bytes)		xx xx	
	UserData	PLC协议主版本号 (1byte)		xx
		PLC协议次版本号 (1byte)		xx
		Sequence Number (2bytes)		xx xx
		Func Code(1bytes)		0x8F
		Status Code (1byte)		0x00 ~ 0x06
		DEV Addr (2bytes)		xx xx

7.3.16 获取心跳 (Func Code =0x10)

PLC网关 (CCO) 获取设备 (STA) 心跳信号。见表82。

表 82 控制心跳

方向	主控设备MCU下发到CCO模组		
Cmd	0x0120H ①	0x0120	
Data	Dest MAC Addr (6bytes)		FF FF FF FF FF FF
	UserData Len (2bytes)		xx xx
	UserData	PLC协议主版本号 (1byte)	xx
		PLC协议次版本号 (1byte)	xx
		Sequence Number (2bytes)	xx xx
		Func Code (1byte)	0x10
		Status Code (1byte)	0x00
		DEV Addr (2bytes)	xx xx
Mode (2byte)		xx xx	

远程设备 (STA) 给 CCO 的响应报文。见表 83。

表 83 获取心跳响应

方向	设备MCU下发到STA模组		
Cmd	0x0120H ①	0x0120	
Data	Dest MAC Addr (6bytes)		xx xx xx xx xx xx (CCO MAC Addr)
	UserDataLen (2bytes)		0x0006
	UserData	PLC协议主版本号 (1byte)	xx
		PLC协议次版本号 (1byte)	xx
		Sequence Number (2bytes)	xx xx
		Func Code (1bytes)	0x90
		Status Code (1byte)	0x00 ~ 0x06
		DEV Addr (2bytes)	xx xx
注 1: Mode 设备心跳响应模式:			
注 2: 0x00 00: 即时响应, 设备收到报文后立即返回响应报文, 通常用于查询单个设备的心跳。			
注 3: 0x01 06: 随机延时响应, 第一个字节为 0x01 表示设备随机延时响应, 第二个字节的值 x 乘以 10 表示随机延时的最大秒数, 范围是 [10, 2550] 秒, 例如: 0x06 表示 x=6, 6*10=60 秒, CCO 广播控制心跳报文, 设备收到此报文之后, 生成小于 1 的随机数*60, 使所有设备在 0-60 秒范围内返回心跳结果, 通过此方式减少 CCO 的心跳查询报文, 同时分散设备的响应报文, 避免同时响应导致网络拥塞。			

7.3.17 重启设备 (Func Code =0x11)

PLC网关 (CCO) 控制设备 (STA) 重启。可以单控、组控、广播。见表84。

表 84 重启设备

方向	主控设备MCU下发到CCO模组		
Cmd	0x0120H ①	0x0120	
Data	Dest MAC Addr (6bytes)	FF FF FF FF FF FF	
	UserData Len (2bytes)	xx xx	
	UserData	PLC协议主版本号 (1byte)	xx
		PLC协议次版本号 (1byte)	xx
		Sequence Number (2bytes)	xx xx
		Func Code (1byte)	0x11
		Status Code (1byte)	0x00
DEV Addr (2bytes)		xx xx	

远程设备 (STA) 给 CCO 的响应报文。见表 85。

表 85 重启设备响应

方向	设备MCU下发到STA模组		
Cmd	0x0120H ①	0x0120	
Data	Dest MAC Addr (6bytes)	xx xx xx xx xx xx (CCO MAC Addr)	
	UserDataLen (2bytes)	xx xx	
	UserData	PLC协议主版本号 (1byte)	xx
		PLC协议次版本号 (1byte)	xx
		Sequence Number (2bytes)	xx xx
		Func Code (1bytes)	0x91
		Status Code (1byte)	0x00 ~ 0x06
DEV Addr (2bytes)		xx xx	

7.3.18 转发报文 (Func Code =0x12)

子设备A (STA) 通过CCO转发报文给子设备B (STA)。见表86。

表 86 转发报文

方向	主控设备MCU下发到CCO模组		
Cmd	0x0120H ①	0x0120	
Data	Dest MAC Addr (6bytes)		FF FF FF FF FF FF
	UserData Len (2bytes)		xx xx
	UserData	PLC协议主版本号 (1byte)	xx
		PLC协议次版本号 (1byte)	xx
		Sequence Number (2bytes)	xx xx
		Func Code (1byte)	0x12
		Status Code (1byte)	0x00
		DEV Addr (2bytes)	xx xx
		Source DEV Addr (2bytes)	xx xx
		Dest DEV Addr (2bytes)	xx xx
		Data Len (2bytes)	xx xx
Data Value (n bytes)			
注：不支持返回响应报文			

7.3.19 查询场景 (Func Code =0x13)

PLC网关 (CCO) 查询某个设备 (STA) 的全部场景。见表87。

表 87 查询场景

方向	主控设备MCU下发到CCO模组		
Cmd	0x0120H ①	0x0120	
Data	Dest MAC Addr (6bytes)		xx xx xx xx xx xx
	UserData Len (2bytes)		xx xx
	UserData	PLC协议主版本号 (1byte)	xx
		PLC协议次版本号 (1byte)	xx
		Sequence Number (2bytes)	xx xx
		Func Code (1byte)	0x13
		Status Code (1byte)	0x00
		DEV Addr (2bytes)	xx xx

远程设备 (STA) 给 CCO 的响应报文。Siid、Ciid 是设备物模型定义中的服务和属性编码。见表 88。

表 88 查询场景的响应

方向	设备MCU下发到STA模组		
Cmd	0x0120H ①	0x0120	
Data	Dest MAC Addr (6bytes)		
	xx xx xx xx xx xx (CCO MAC Addr)		
	UserData Len (2bytes)		
	xx xx		
	UserData	PLC协议主版本号 (1byte)	xx
		PLC协议次版本号 (1byte)	xx
		Sequence Number (2bytes)	xx xx
		Func Code (1byte)	0x93
		Status Code (1byte)	0x00
		DEV Addr (2bytes)	xx xx
		Scene Quantity (2byte, 场景数)	xx xx (场景总数 0- 65535)
		Scene ID (2byte, 场景号)	1 (第1个场景)
		Scene Len (2bytes)	(场景1数据长度)
		Siid (2bytes)	
		Ciid (2bytes)	
		Data Type (2byte)	
		Data Len (2bytes)	
		Data Value (n byte)	
		
		Siid (2bytes)	
		Ciid (2bytes)	
		Data Type (2byte)	
		Data Len (2bytes)	
		Data Value (n byte)	
	
		Scene ID (2byte, 场景号)	n (第n个场景)
		Scene Len (2bytes)	(场景n数据长度)
Siid (2bytes)			
Ciid (2bytes)			
Data Type (2byte)			
Data Len (2bytes)			
Data Value (n byte)			
.....			

表 88 查询场景的响应（续）

方向	设备MCU下发到STA模组		
Data	UserData	
		Siid (2bytes)	
		Ciid (2bytes)	
		Data Type (2byte)	
		Data Len (2bytes)	
		Data Value (n byte)	
注：Siid、Ciid 是设备物模型定义中的服务和属性编码。			

7.3.20 设备初始化 (Func Code =0x14)

PLC网关 (CCO) 控制设备 (STA) 初始化。可以单控、组控、广播。见表89。

表 89 初始化设备

方向	主控设备MCU下发到CCO模组		
Cmd	0x0120H ①		0x0120
Data	Dest MAC Addr (6bytes)		FF FF FF FF FF FF
	UserData Len (2bytes)		xx xx
	UserData	PLC协议主版本号 (1byte)	xx
		PLC协议次版本号 (1byte)	xx
		Sequence Number (2bytes)	xx xx
		Func Code (1byte)	0x14
		Status Code (1byte)	0x00
		DEV Addr (2bytes)	xx xx

远程设备 (STA) 给 CCO 的响应报文。见表 90。

表 90 初始化设备响应

方向	设备MCU下发到STA模组		
Cmd	0x0120H ①	0x0120	
Data	Dest MAC Addr (6bytes)	xx xx xx xx xx xx (CCO MAC Addr)	
	UserDataLen (2bytes)	xx xx	
	UserData	PLC协议主版本号 (1byte)	xx
		PLC协议次版本号 (1byte)	xx
		Sequence Number (2bytes)	xx xx
		Func Code(1bytes)	0x94
		Status Code (1byte)	0x00 ~ 0x06
DEV Addr (2bytes)		xx xx	