

1、寄存器 PLC 地址

寄存器 PLC 地址指存放于控制器中的地址，这些控制器可以是 PLC，也可以使触摸屏，或是文本显示器。PLC 地址一般采用 10 进制描述，共有 5 位，其中第一位代码寄存器类型。第一位数字和寄存器类型的对应关系如下表所示。**PLC 地址例如 40001、00001 等。**

数据类型	modbus 地址, 寄存器编号	读功能码	写功能码	数据大小
数字量输出(线圈)	00001——09999	01H	05H, 0FH	位, 1bit
数字量输入(触点)	10001——19999	02H		位, 1bit
输入寄存器	30001——39999	04H		字, 16bit
保持寄存器	40001——49999	03H	06H, 10H	字, 16bit

2、寄存器协议地址

寄存器协议地址指通信时使用的寄存器地址，例如 PLC 地址 40001 对应寻址地址 0x0000，40002 对应寻址地址 0x0001，寄存器寻址地址一般使用 16 进制描述。再如，**PLC 寄存器地址 40003 对应协议地址 0002，PLC 寄存器地址 00003 对应协议地址 0002**，虽然两个 PLC 寄存器寄存器通信时使用相同的地址，但是需要使用不同的命令访问，所以访问时不存在冲突。

3、默认通信参数：9600 波特率 8 位数据位 1 位停止位 无校验

(大端模式表示地址和数据项；而 CRC 是低位在前，高位在后。)

(485 接口通信时每帧数据响应时间不能低于 35ms)

4、支持的功能码(十六进制表示):

- 03: 读多个保持寄存器的内容(连续寄存器块)
- 05: 写单个线圈
- 06: 写单个保持寄存器
- 10: 写多个保持寄存器(连续寄存器块)

5、寄存器 PLC 地址分配如下: (1 个寄存器是 16 位的无符号数, 占 2 个字节)

(1) 保持寄存器 (一般用来存放和显示数据)

寄存器编号	定义(对应参数)	读/写
40001	步距角 (比如步距角是 1.8, 写的时候需要扩大 100 倍, 即设置为 180。读的时候缩小 100 倍)	R/W
40002	细分 (驱动器上是多少细分, 就设为多少细分)	R/W
40003	启动频率(单位: HZ)	R/W
40004	加减频率(单位: HZ)	R/W
40005 40006	螺距 (电机转一圈对应的距离)	R/W
40007	机械零点输入信号(有效值 0--5)	R/W
40008	停止模式 (0 缓慢停 1 立即停)	R/W
40009	速度(单位: 转/每分钟)	R/W
40010 40011	距离(即单次运行的距离)	R/W
40012	方向 (0 正向, 1 反向)	R/W
40013	单次运行到位反馈 0 表示没到位 1 表示运行到位	R 只针对单次运行命令
40014	备用	
40015	正限位信号(有效值 0--5)	R/W
40016	反限位信号(有效值 0--5)	R/W
40017	控制器 ID 号 (485 设备号)	R/W
40018	工程启动信号(有效值 0--5)	R/W
40019	工程停止信号(有效值 0--5)	R/W
40020	备用	
40021	系统工作次数计数	R/W
40022	备用	
40023 40024	当前坐标显示	R, 读这个寄存器 会实时显示当前坐标
40025	工程号 (只能为 1)	R/W
40026	工程总步数(有效值 1--33)	R/W
40027	本步启动口信号(有效值 0--5)	R/W
40028	工程本步启动频率, 单位 HZ	R/W

40029	工程本步加减频率, 单位 HZ	R/W
40030	工程本步运行方向 (0 正向, 1 反向)	R/W
40031	工程本步运行速度 (单位: 转/每分钟)	R/W
40032 40033	工程本步运行距离	R/W
40034	备用	R/W
40035 40036	本步延时时间(单位: 毫秒)	R/W
40037	段循环起始步	R/W
40038	段循环结束步	R/W
40039	段循环次数	R/W
40040	设定工程当前步号(有效值 1--33)	R/W
40041	备用	
40042	工程实时步号显示	R (有效值 0—33)
40043	第 1 路输入信号状态显示	R (1--ON 0--OFF)
40044	第 2 路输入信号状态显示	R(1--ON 0--OFF)
40045	第 3 路输入信号状态显示	R(1--ON 0--OFF)
40046	第 4 路输入信号状态显示	R(1--ON 0--OFF)
40047	第 5 路输入信号状态显示	R(1--ON 0--OFF)
40048	备用	R/W
40049	电机运行状态显示	R(1--ON 0--OFF)
40050	工程循环次数	R/W
40051	本步停止口信号(有效值 0--5)	R/W
40052	备用	R/W
40053	备用	R/W
40054	备用	R/W
40055	备用	R/W
40056	备用	R/W
40057	备用	R/W
40058	往返运行的次数	R/W
40074	波特率低 16 位	R/W
40075	波特率高 16 位	R/W
40076	相对/绝对运行 (0 相对 1 绝对)	R/W 只针对单次运行命令
40077	运行方式选择 0 位置 1 速度触发 2 速度点动	R/W (主要是针对正反启动 信号控制的)
40078	正转启动信号 (0 表示无设置) (1—5 对应 IN1—IN5 输入)	R/W 信号有效时, 按上面 选择的运行方式正转
40079	反转启动信号 (0 表示无设置) (1—5 对应 IN1—IN5 输入)	R/W 信号有效时, 按上面 选择的运行方式反转

(2) 线圈输出寄存器 (一般用来控制操作)

线圈输出值表示请求的 ON/OFF 状态。十六进制值 0XFF00 请求线圈为 ON；十六进制值 0X0000 请求线圈为 OFF。其它所有值均为非法的，并且对线圈不起作用。

寄存器编号	定义(对应参数)	说明
00001	数据保存	断电保存所有参数
00002	工程参数读取	
00003	工程参数清零	
00004	(工程)停止/急停	
00005	正转点动	置 ON，电机一直正转 置 OFF，电机停止
00006	反转点动	置 ON，电机一直反转 置 OFF，电机停止
00007	回数据零	电机运行到坐标零点
00008	单次运行(按 40009 的速度和 40010 40011 的距离运行 1 次)	可选择相对/绝对运行 2 种方式运行
00009	工程启动	按设定好的每一个步骤运行。直到所有步骤完毕或急停。
00010	回机械零	电机一直反转，碰到机械零点信号停止。
00011	坐标清零	将 40023 40024 的值设为 0
00012	备用	
00013	备用	
00014	备用	
00015	备用	
00016	备用	
00017	备用	
00018	工程上一步	将 40040 的值减 1
00019	工程下一步	将 40040 的值加 1

6、通信实例说明

(1) 使用 03 功能码读取 2 个寄存器 40001H 40002H 中的数据内容。即步距角 细分值

设备号/站号 (1 个字节)	功能码 (1 个字节)	从站数据起始地址 (2 个字节,高位在前)	读寄存器个数 (2 个字节,高位在前)	CRC 校验 (2 个字节,低位在前)
01	03	00 00	00 02	C4 0B

回应信息格式: 回字节个数=5+2*N N 为读的寄存器个数

设备号/站号	功能码	数据字节个数	回数据内容(高位在前)	CRC 校验
--------	-----	--------	-------------	--------

(1 个字节)	(1 个字节)	(1 个字节)	40001 地址的数据	40002 地址的数据	
01	03	04	00h B4h	00h 08h	BBH D3H

(2) 写单个线圈 05 功能码 (比如: 控制电机单次运行的命令)

请求数据域中的常量说明请求的 ON/OFF 状态。十六进制值 FF 00 请求输出为 ON。

十六进制值 00 00 请求输出为 OFF。其它所有值均是非法的, 并且对输出不起作用

设备号/站号 (1 个字节)	功能码 (1 个字节)	输出线圈地址 (2 个字节,高位在前)	输出值 (2 个字节)	CRC 校验 (2 个字节)
01	05	00 07	ff 00	3D FB

回信息格式: 和发送的数据一样。 回字节个数=8 个

(3) 写单个保持寄存器 06 功能码 (比如: 设定细分值设为 4)

设备号/站号 (1 个字节)	功能码 (1 个字节)	从站数据地址 (2 个字节,高位在前)	数据内容 (2 个字节)	CRC 校验 (2 个字节)
01	06	00 01	00 04	D9 C9

回信息格式: 和发送的数据一样。 回字节个数=8 个

(4) 写多个寄存器 10 功能码

(比如: 设定运行距离的值为 200, 等于十六进制 0x00c8。)

地址 40010 对应低 16 位数据, 40011 对应高 16 位数据;

设备号/站号 (1 个字节)	功能码 (1 个字节)	从站数据起始地址 (2 个字节,高位在前)	寄存器个数 (2 个字节)	数据字节个数 (1 个字节)	数据内容 数据 1 数据 2,,,,,,	CRC 校验 (2 个字节)
01	10	00 09	00 02	04	00 C8 00 00	B2 3B

回应信息格式: 回字节个数=8 个

设备号/站号 (1 个字节)	功能码 (1 个字节)	从站数据起始地址 (2 个字节,高位在前)	寄存器个数 (2 个字节)	CRC 校验 (2 个字节)
01	10	00 09	00 02	91 CA

注意 1: 485 设备地址的修改操作以及波特率修改操作:

出厂默认设备号为 1。首先使用 06 功能码或 10 功能码写设备号, 然后再使用 05 功能码发送 1 条数据保存命令, 再断电重启。

注意 2: 读/写一个 32 位的参数(即占 2 个寄存器)时, 低 16 位在前,

高 16 位在后