

HSR-UQ215 系列读写器应用手册



目 录

- 1. 简介 1
 - 1.1 约定 1
 - 1.2 本文档的目的 1
 - 1.3 文档的有效范围 1
 - 1.4 符合性声明 错误！未定义书签。
 - 1.5 修订历史 1
- 2. 安全须知 3
 - 2.1 安全符号说明 3
 - 2.2 通用安全说明 4
 - 2.3 特殊安全说明 4
- 3. 产品概况 6
- 4. 技术参数 7
 - 4.1 HSR-UQ215 规格 7
 - 4.2 HSR-UQ215 LED 定义 8
 - 4.3 HSR-UQ215 安装尺寸 10
 - 4.4 天线方向图 11
- 5. 产品安装 12
 - 5.1 安装注意事项 12
 - 5.1.1 关于安装场所 12
 - 5.1.2 关于应用事项 12
 - 5.1.3 关于使用方法 13
 - 5.2 硬件接口说明 14
- 6. 工业以太网协议 15
 - 6.1 地址设置 15

6.2 PLC 与总线模块通讯格式	15
6.2.1 Output	15
6.2.2 Input	16
6.2.3 时序	18
6.3 支持的命令	20
6.3.1 读标签	20
6.3.2 写标签	22
6.3.3 读 EPC	24
6.3.4 写 EPC	25
6.3.5 读配置	26
6.3.6 写配置	27
6.4 错误代码	30
6.5 应用举例	31
6.5.1 RFID 监控	31
6.5.2 RFID 标签内存读取	32
6.5.3 RFID 标签内存写入	33
7. MODBUS 协议	35
7.1 寄存器定义	35
7.1.1 标签内存区域	35
7.1.2 系统内存区域	39
7.2 MODBUS 协议支持	44
7.2.1 MODBUS RTU 设备配置	44
7.2.2 MODBUS TCP 设备配置	47
7.2.3 设备支持的命令	48
7.3 产品复位	58
7.4 错误码	59
8. 附录	60
8.1 RSSI 值对应表	60

8.2 信道频率对应表	62
8.3 组态文件	63

1. 简介

1.1 约定

以下术语/缩写在本文档中同义使用：

读写器，等同于“读/写设备”、“读/写装置”、“读头”，

电子标签，等同于“载码体”、“响应器”；

本设备，等同于“本产品”，是指本手册所描述的产品型号或系列。

1.2 本文档的目的

本手册包含了正确使用本设备所需的全部信息，包括必要功能、性能、使用方法等信息。它既适用于自己调试系统并将其与其他单元（自动化系统，其他编程设备）连接的编程人员和测试/调试人员，也适用于安装扩展或执行故障/错误分析的服务和维护人员。

在安装本设备并投入运行之前，请仔细阅读本手册。本手册包含说明和注释，可帮助您逐步完成安装和调试。这样可以确保本产品无故障使用。熟悉本手册您将可以获得以下好处：

- ✓ 确保设备的操作安全
- ✓ 帮助您利用设备的全部功能
- ✓ 避免错误和相关故障
- ✓ 减少维修，避免成本浪费

1.3 文档的有效范围

此文档的描述适用于 RF-U 系列的超高频读写器产品。

1.5 修订历史

表格 1.1 文档版本信息

版本	修订日期	修改原因
V1.0	2026.4.1	初版

2. 安全须知

2.1 安全符号说明

在尝试安装、操作、维修或维护设备之前，请仔细阅读这些说明，并认真查看设备。 在本文档中或在设备上可能会出现以下特殊消息，以提示状态信息或警告潜在的危險。

我们将安全提示信息为了：“危险”、“警告”、“注意”、“提示”四个等级。

危险 DANGER	表示严重危险情况，如果不避免，将导致死亡或严重伤害
警告 WARNING	表示危险情况，如果不避免，可能会导致死亡或严重伤害
注意 CAUTION	表示危险情况，如果不避免，可能会导致轻度或中度伤害
提示 NOTICE	用于提示与人身伤害无关的信息



这是“危险”或“警告”符号，表示存在电气危险，如果不遵循说明，将导致人身伤害。



这是“注意”符号。用于警告您潜在的人身伤害危险。 请遵守该符号后的所有安全提示，以免造成伤害或死亡。



这是“提示”符号，此符号用于提示用户可能存在的风险。不遵守该规定可能会导致设备出错，甚至完全故障。

2.2 通用安全说明

本设备只能由合格人员进行安装，操作，维修和维护。合格人员是指，具有与电气设备的构造和操作，及其安装有关的技能和知识，并已接受安全培训以识别和避免所涉及危险的人员。



用户修改和/或修理是危险的，将使保修失效并使制造商免于承担任何责任。



产品维修只能由我司人员进行。
未经授权的打开和不适当的维修产品可能导致大量的设备损坏或可能对用户造成人身伤害。

如果发生严重故障，请停止使用该设备。防止设备意外操作。如果需要维修，请将设备退回本公司在当地的代表或销售办事处。

运营公司有责任遵守当地适用的安全规定。

将未使用过的设备存放在原始包装中。这为设备提供了最佳的防撞击和防潮保护。请确保环境条件符合本相关规定。

2.3 特殊安全说明



以不受控制的方式启动的过程可能会危害其它设备，或遭受其它风险设备的危害，因此，在调试之前，请确保使用该设备不会涉及可能危害其它设备的风险或免遭其它设备危害的风险。

电源供应

根据欧洲安全标准 EN 60950，本设备只能配合受限功率的电流源来操作设备，即电源必须具备过压过流保护功能。以防止本设备发生电源故障时，影响到其它设备的安全；或者外部设备发生故障，影响到本设备的安全。

3. 产品概况

HSR-UQ215 是一款工业级的一体式超高频 RFID 读写头，支持以太网和 RS485 通信，支持 Profinet、Ethernet/IP、EtherCAT、Modbus TCP、Modbus RTU 协议。该产品有两个以太网接口，可串联使用，极大的方便了多产品使用状态下实施，节省了施工成本。同时该产品还可扩展 2 路天线，能覆盖更广的检测范围。各读头支持的通讯方式见第 4 章节。该系列读写器具有以下显著特征：

- ✓ 支持 ISO 18000-6C/EPC C1G2 协议，采用 Impinj 新一代射频芯片 E710，性能强劲。
- ✓ 支持 Profinet、Ethernet/IP、EtherCAT 的工业以太网协议，可直接与 PLC 进行数据交换。
- ✓ 两个 M12 Dcode 4PIN 标准工业以太网接口，可串联使用。
- ✓ 一体式设计，同时还支持 2 路扩展天线。
- ✓ 针对工业环境设计，可应用于自动化线体的感应识别系统。
- ✓ IP65 高防护等级，抗干扰设计，适用于要求苛刻的 RFID 应用环境。

4. 技术参数

4.1 HSR-UQ215 规格

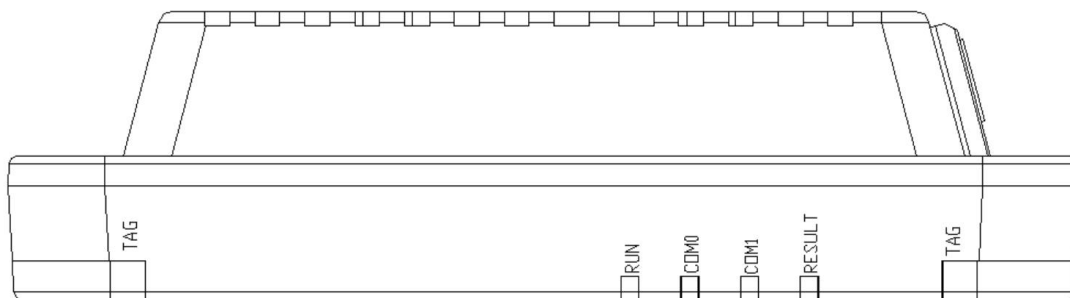
技术规格如下：

产品型号		HSR-UQ215-PN	HSR-UQ215-EIP	HSR-UQ215-ECT
规格 参数	无线协议	ISO 18000-6C (Class 1 Gen 2)		
	工作频率	中国频率：920-925 MHz (SRRC) 北美频率：902-928MHz (FCC Part 15) 欧洲频率：866-868MHz (ETSI)		
	输出功率	5-30dbm 可调，步进 1dbm		
	接收灵敏度	≤-85dBm		
	内部天线增益	8dBi		
	外接天线端口	TNC 母头(外螺内孔) * 2		
	通信接口	RS485*1，以太网*2		
	通信协议	ProfiNET	Ethernet/IP	EtherCAT
	电源电压	9-30V DC		
	平均电流	< 0.5A (24V DC)		
	指示灯	6 个 LED 灯		
物理 参数	外形尺寸	215*215*58mm		
	固定类型	4 个 M6 螺丝		
	外壳材质	底壳：铝合金，面壳：PC+ABS		
	壳体颜色	黑色		
应用 环境	工作温度	-25 ~ 60°C		
	存储温度	-40 ~ 85°C		
	湿度	5% ~ 95%RH(无凝露)		
	防水防水等级	IP65		

订货型号	HSR-UQ215-PN	HSR-UQ215-EIP	HSR-UQ215-ECT
------	--------------	---------------	---------------

4.2 HSR-UQ215 LED 定义

HSR-UQ215 读写器提供 6 个 LED，分别为 RUN、COM0、COM1、RESULT 及 2 个 TAG，其中 2 个 TAG LED 的显示是同步的。LED 的分布如下图所示。



各个 LED 灯具体定义如下：

名称	颜色	状态	描述
RUN	绿-红双色灯 	常亮 	系统电源正常
		常亮 	系统异常
		红色长闪 1 次 	射频模块异常，单次闪烁时红灯亮 1000ms
		红色长闪 2 次  	网络模块异常，单次闪烁时红灯亮 1000ms，间隔 200ms
		红色长闪 3 次   	天线 0 诊断异常，单次闪烁时红灯亮 1000ms，间隔 200ms
		红色短闪 1 次 	Flash 异常，单次闪烁时红灯亮 100ms
		红色短闪 2 次  	MAC 地址未初始化，单次闪烁时红灯亮 100ms
		熄灭 	没有通电或系统供电异常
COM0	绿-红双色灯 		与通讯协议有关，见后文描述
COM1	绿-红双色灯 		与通讯协议有关，见后文描述
RESULT	绿-红双色灯 	绿色闪烁 	指令执行成功
		红色闪烁 	指令执行失败

		熄灭 	无指令执行
TAG	绿-蓝双色灯 	蓝色闪烁 	写标签成功
		蓝色闪烁 	读标签成功
		熄灭 	无 TAG 信号或者

注 1: RUN 有红灯出现时, 表明产品工作异常。若故障一直存在, 请联系厂家进行技术咨询。

注 2: 天线诊断异常只对一体式产品的内部天线接口进行诊断。

■ ProfiNet

协议	名称	颜色	状态	描述
Profinet	COM0 (SF)	红色 	常亮 	看门狗超时; 诊断事件; 系统错误
			闪烁 	总线上正在运行 DCP 服务
			熄灭 	没有出错
	COM1 (BF)	红色 	常亮 	网络模块没有正确配置; 没有物理连接;
			闪烁 	没有通信数据交互
			熄灭 	没有出错

■ Ethernet/IP

协议	名称	颜色	状态	描述
Ethernet/IP	COM0 (MS)	红绿双色 	绿灯常亮 	设备正常运行
			绿灯闪烁 	设备没有配置好
			双灯闪烁 	设备正在进行通电自检
			红灯闪烁 	设备检测到一个可恢复的小故障。例如: 一个不正确或不一致的配置可以被认为是一个小故障
			红灯常亮 	设备发生了无法恢复的严重故障
			双灯熄灭 	供电异常
	COM1 (NS)	红绿双色 	绿灯常亮 	设备至少有一个已建立的连接
			绿灯闪烁 	设备没有建立连接, 但获得了一个 IP 地址。
			双灯闪烁 	设备正在进行通电检测自检
			红灯闪烁 	连接超时: 目标设备所在的一个或多个连接超时。只有当所有超时连接

				被重新建立或设备被重置时，此状态才会结束。。
			红灯常亮 	重复 IP:设备检测到它的 IP 地址已经在使用中。
			双灯熄灭 	没有通电或没有分配 IP 地址

■ EtherCAT

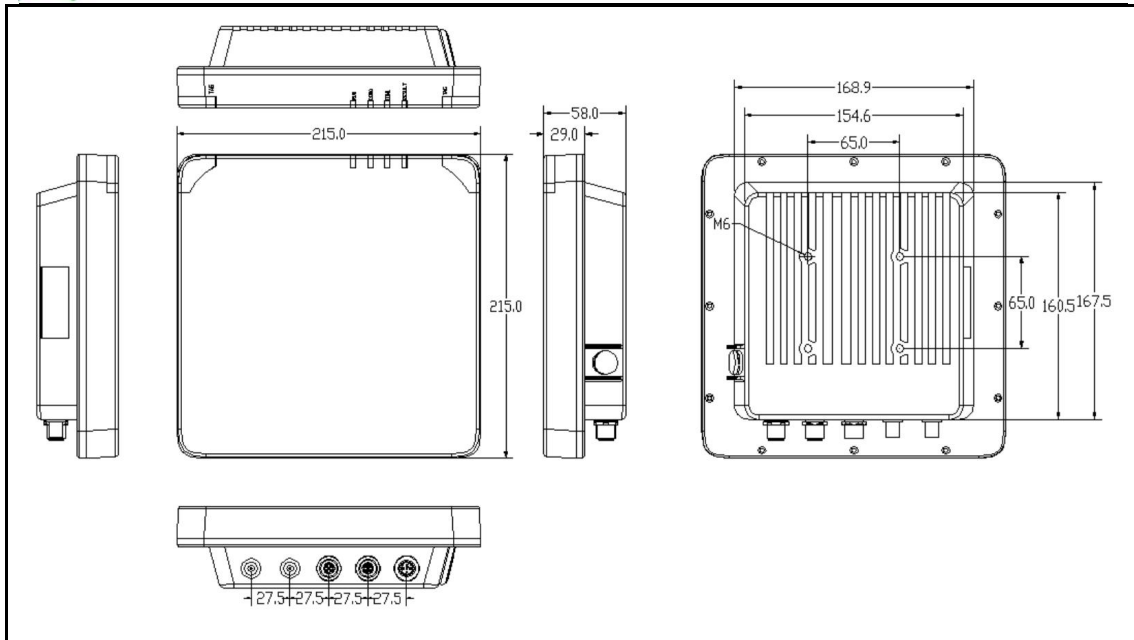
协议	名称	颜色	状态	描述
EtherCAT	COM0 RUN	绿灯 	常亮 	设备处于可操作状态 (OPERATIONAL)
			闪烁 1  	设备处于安全模式 (SAFEOPERATIONAL)
			闪烁 2  	设备处于预可操作状态 (PREOPERATIONAL)
			熄灭 	设备处于初始化状态
	COM2 ERR	红灯 	闪烁 1  	本地错误:从设备应用程序自动改变了 EtherCAT 状态。 可能的原因 1:主机看门狗超时。 可能的原因 2:同步错误，设备自动进入安全运行。
			闪烁 2  	无效配置
			闪烁 3  	应用程序看门狗超时:发生了应用程序看门狗超时。 可能的原因:同步管理器看门狗超时。
			熄灭 	没有出错

闪烁方式定义如下表所示：

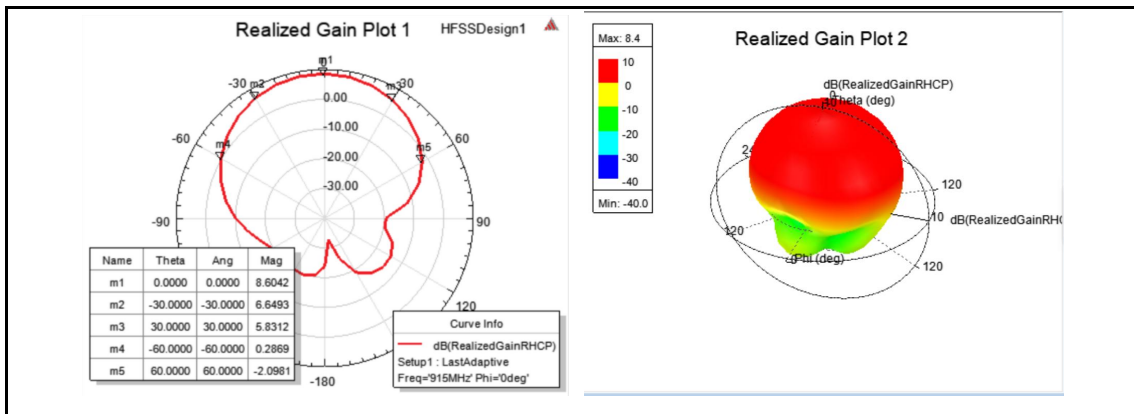
闪烁方式	描述
闪烁 1	LED 亮 200ms,熄灭 1000ms
闪烁 2	LED 以 2.5Hz 的频率在闪烁 (200ms 亮+200ms 灭,循环)
闪烁 3	两个短的闪烁 (每个闪烁由 200ms 亮+200ms 灭组成) +1000ms 的熄灭

4.3 HSR-UQ215 安装尺寸

HSR-UQ215 的尺寸为 215*215*58mm，含 4 个 M6 安装孔，如下图所示。



4.4 天线方向图



5. 产品安装

5.1 安装注意事项

为防止产品动作不良、误动作或对性能、设备带来负面影响，请遵守以下事项。

5.1.1 关于安装场所



请避免安装在散热量高的设备(加热器、变压器、大容量电阻等)附近。

请避免安装在电磁干扰严重的设备(大型电机、变压器、收发器、变频器、开关电源等)附近。



多个读写器安装较近时，请使用传感器进行触发读取，避免多个读写器同时工作相互干扰的情况。

多个标签安装较近且有需要精确读取时，建议标签间距保持在 3 倍应用读取距离以上。

5.1.2 关于应用事项



严禁使用 AC 电源。否则有破裂的危险，严重影响到人身及设备的安全。



请使用受限功率的电流源来操作设备，即电源必须具备过压过流保护功能。以防止本设备发生电源故障时，影响到其它设备的安全；或者外部设备发生故障，影响到本设备的安全。



请避免错误接线。否则有破裂、烧坏的危险。有可能会影响人身及设备的安全。



读写器天线面与标签面平行时，识别距离最远。标签倾斜安装时通信距离会缩短。标签的安装，请考虑倾斜影响后再安装。

5.1.3 关于使用方法



请勿将电缆弯曲至半径 40mm 以内。否则有断线的危险。



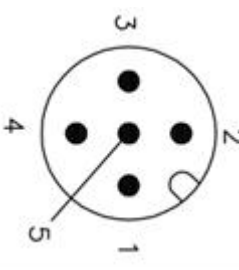
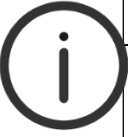
产品有异常时请立即停止使用，并在切断电源后与本公司销售代表联系。

5.2 硬件接口说明

该系列设备通过 M12 连接器同时提供电源与通讯物理接口，通信接口可选支持 RS485 或以太网。

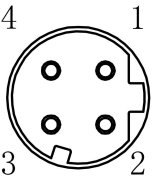
RS-485 通讯接口

RS-485 接口采用 A-CODE M12 公头，5 针连接器，引脚定义如下：

接头类型	管脚	符号	描述
	Pin1	24V	电源正极
	Pin2	RS485_A	RS-485 信号线 A
	Pin3	0V	电源负极
	Pin4	RS485_B	RS-485 信号线 B
	Pin5	NC	/
 注意事项	1) 通信线建议使用屏蔽双绞线； 2) 通讯线缆长度：Max≤50m； 3) 通讯线缆线芯使用 24AWG 及以上		

以太网通讯接口

以太网接口采用 M12Dcode 母头接口，本品有两个以太网接口 LK1 和 LK2，接口引脚定义如下：

M12Dcode 母头	管脚	符号	描述
	Pin1	TD+	发送差分信号正
	Pin2	RD+	接收差分信号正
	Pin3	TD-	发送差分信号负
	Pin4	RD-	接收差分信号负
 注意事项	4) 通信线建议使用工业以太网专用线缆，双屏蔽双绞线； 5) 通讯线缆长度：Max≤100m；		

6. 工业以太网协议

6.1 地址设置

HSR-UQ215 系列 RFID 读写器的设置方法如下：

通讯协议	默认地址	配置方法
Ethernet/IP	IP 地址：192.168.0.10	通过软件配置 IP 地址
ProfiNet	IP 地址：192.168.0.10	通过 TIA 或者 STEP7 配置 IP 地址和 Station Name
EtherCAT	默认站点：0	通过 PLC 编程软件设置站点号

6.2 PLC 与总线模块通讯格式

HSR-UQ215 系列 RFID 读写器与 PLC 使用内存映射的方式进行通讯，PLC 输出给 RFID 读写器的数据以及 RFID 读写器发送给 PLC 的输入数据都由工业总线进行同步，用户只需要负责对 PLC 端的输入输出内存进行存取即可。

6.2.1 Output

PLC 发送给 RFID 读写器的数据将通过输出来传输，输出内存的定义如下：

地址	定义							
	Bit7	Bit6	Bit5	Bit4	bit3	bit2	bit1	bit0
0	RFU	Ant2	Ant1	Ant0	Mode	Trigger	oToggleBit	Enable
1	RFU							
2	Command							
3	Datalen							
4-95	Datas							



其中各个字段的功能说明如下：

Enable	使能 RFID，使能后方可使用；
--------	------------------

	1: 启用; 0: 禁用;
oToggleBit	翻转位, 用于长数据分包传输的握手。在分包传输过程中, 若此位翻转, 表示已准备好下一帧数据 (已接收完上一帧数据)
Trigger	命令触发位: 上升沿: 触发当前命令。 下降沿: 若当前命令仍在执行则结束当前的命令。否则无效。
Mode	读写器的工作模式: 0: 主动工作模式 (在主动工作模式的状态下, 有标签在可读区域, 将自动上传标签在位信号和标签 UID) ; 主动工作模式下上传的数据与读 EPC 命令响应上传的数据格式一致; 1: 被动工作模式 (根据命令执行读卡操作, 不主动监测标签状态);
Ant0-Ant2	主动工作模式时, 使用的天线。 1: 使用 0: 不使用
RFU	预留
Command	需要执行的命令;
DataLen	数据长度(Datas 字段)
Datas	执行的命令需要的参数, 每个命令都不一样, 具体见后文“支持的命令”章节

6.2.2 Input

RFID 读写器发送给 PLC 的数据通过输入来传输, 输入内存的定义如下:

地址	定义
----	----

	bit6-7	bit5	bit4	bit3	bit2	bit1	bit0
0	RFU	iToggleBit	Err	Done	Busy	TP	Ready
1	RFU						IsPassiveMode
2	Errcode						
3~95	Read datas						

其中各个字段的功能说明如下：

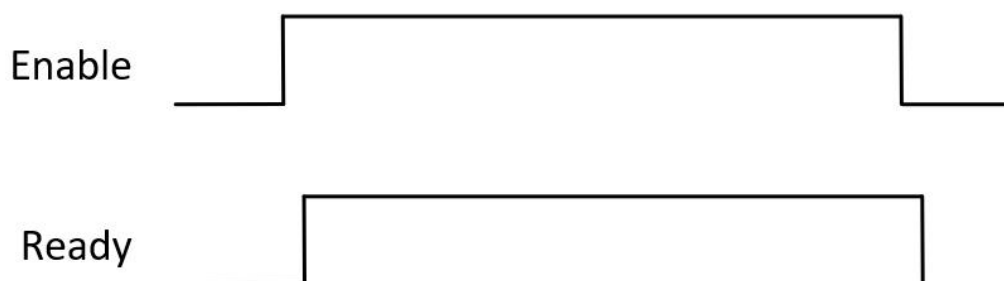
Ready	读写器状态信号，指示读写器是否准备好工作： 1：正常； 0：异常；
TP	标签信号，指示当前标签是否在可读区域； 1：在可读区域； 0：不在可读区域；
Busy	指示网关当前的状态； 1：已接收到命令，正在执行； 0：空闲；
Done	指示当前命令是否执行完毕； 1：执行完毕； 0：正在执行/无有效命令；
Err	指示当前命令是否正确执行； 1：异常；(具体见 ErrCode) 0：正确执行；
iToggleBit	翻转位，用于长数据分包传输的握手。在分包传输过程中，若此位翻转，表示已准备好下一帧数据（已接收完上一帧数据）
IsPassive Mode	指示读头当前的工作模式，工作模式可通过输出区的 Mode 进行修改： 0：自动读卡模式；

	1: 非自动读卡（触发一次读取一次）；
RFU	预留
Errcode	错误码： 0x00:无错误 其他：发生错误，具体错误定义见后文
Read datas	读取的数据或配置，其中包含多个字段，具体见“支持的命令”章节；

6.2.3 时序

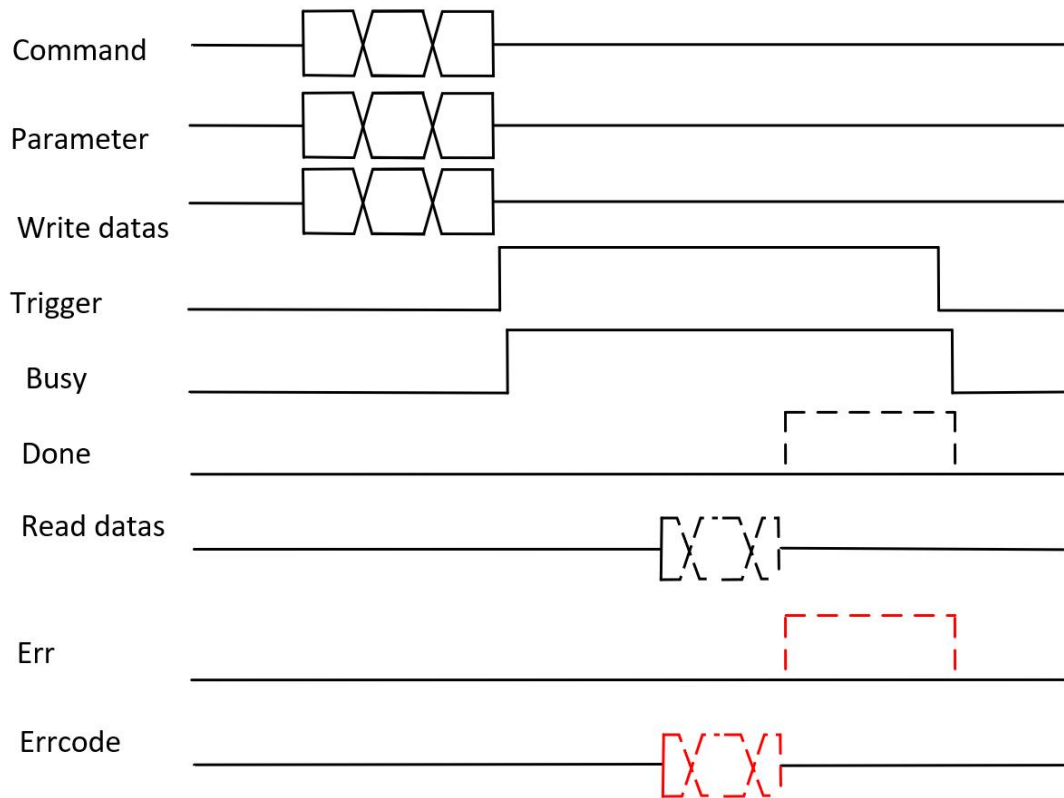
1、使能 RFID

使能是使 RFID 工作的必要条件，在整个工作期间需要保持 RFID 使能。使能 RFID 涉及到 Enable 和 Ready 两个信号，具体的时序如下所示。若 Enable 置位后，Ready 未置位，则可能总线模块与 RFID 通讯异常。



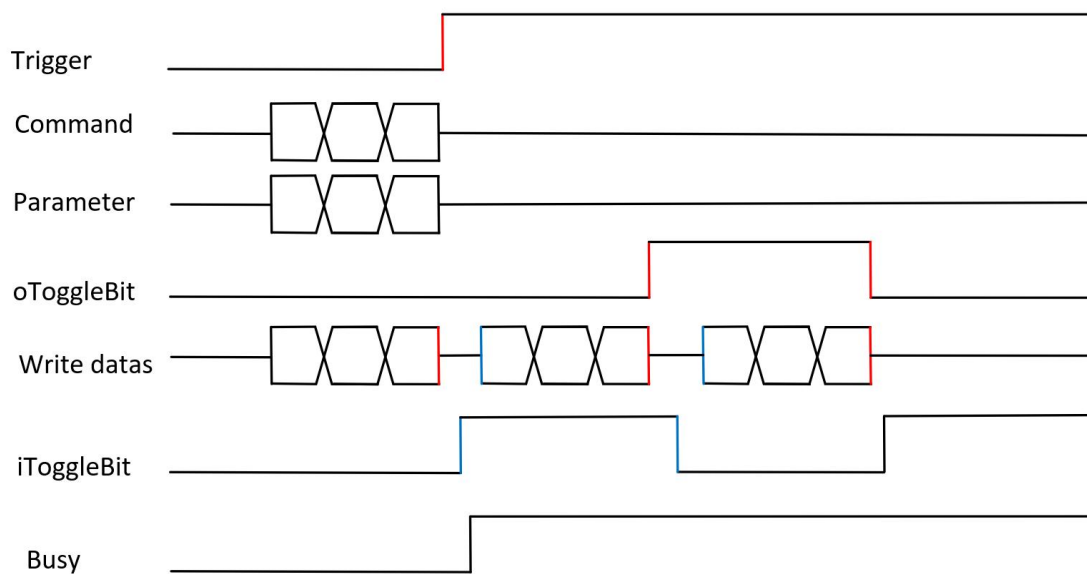
2、命令执行

命令的执行以 Trigger 上升沿信号开始，在给 Trigger 信号置位之前，先将命令/参数/数据填充好。在命令执行期间保持 Trigger 信号置位，若取消当前命令的执行，将 Trigger 复位即可，Trigger 后输入数据取的状态信息将复位。命令执行完后可从 Read datas/Errcode 取命令执行的结果。



3、长数据分包传输

在实际应用的过程中，可能存在一次无法传输完数据的情况，此时需要分包进行传输。以 PLC 启动长数据传输为例，时序图如下：



6.3 支持的命令

Command 字段 (Output_byte2) 的定义如下:

地址	字段	定义
Bit7	Match	是否使用匹配 1: 使用 0: 不使用
Bit6-0	Cmd	命令码: 0x42: 读标签 0x43: 写标签 0x41: 盘存 EPC 0x44: 写 EPC 0x45: 读配置 0x46: 写配置

6.3.1 读标签

读标签命令可以用来读取标签各个区域的内存, 具体的命令格式如下:

地址	定义							
	Bit7	Bit6	Bit5	Bit4	bit3	bit2	bit1	bit0
0	RFU	Ant2	Ant1	Ant0	Mode	Trigger	oToggleBit	Enable
1	RFU							
2	Matc h	0x42						
3	DateLen							
4	Bank_R							
5	Addr_H_R							

6	Addr_L_R
7	Number_R
8	[Bank_M], Match=1 此字段出现, 否则不出现
9	[Addr_H_M], Match=1 此字段出现, 否则不出现
10	[Addr_L_M], Match=1 此字段出现, 否则不出现
11	[Number_M], Match=1 此字段出现, 否则不出现
12~9 5	[Data_M], Match=1 此字段出现, 否则不出现

其中参数部分字段定义如下:

字段	定义	备注
DateLen	数据长度, 单位 字节 , 从 Bank_R 到 [Data_M] 字段	
Bank_R	需要读取的区域: 0: Reserved 1: EPC 2: TID 3: USER DATA	
Addr_H_R	读取数据的 字 地址高字节	
Addr_L_R	读取数据的 字 地址低字节	
Number_R	读取的 字 数量	
Bank_M	需要匹配的区域: 0: Reserved 1: EPC 2: TID 3: USER DATA	仅在 Match=1 时, 此字段有效
Addr_H_M	匹配数据的 位 地址高字节	
Addr_L_M	匹配数据的 位 地址低字节	
Number_M	匹配数据的 位长度	
Data_M	需要匹配的数据	

读取标签命令的响应如下:

地址	定义						
	bit6-7	bit5	bit4	bit3	bit2	bit1	bit0
0	RFU	iToggleBit	Err	Done	Busy	TP	Ready

1	RFU	IsPassiveMode
2	Errcode	
3	TagCnt	
4	DataLen	
5	Antenna	
6	PC_H	
7	PC_L	
8~8+x	EPC	
9+x	RSSI	
10+x ~ 10+x+n	Datas	

其中响应数据部分字段的定义如下：

字段	定义
TagCnt	此次读取响应的标签个数。有多个标签响应时，翻转 oToggleBit 将上传下一个标签的数据，TagCnt 也会随之减少。
DataLen	当前上传的标签占的 字节 总数：从 Antenna 到 Datas 字段。当 DataLen 字段的长度大于 91 时，需要翻转 oToggleBit 接收超过 91 部分的数据
Antenna	当前标签读取的天线
PC_H	响应标签的 PC 高字节
PC_L	响应标签的 PC 低字节
EPC	响应标签的 EPC
RSSI	响应标签的信号强度。此处需要通过计算才可得到功率值，计算公式为：-39.9+6log ₂ (Y/190)，也可从附件查询对应的值。
Datas	读取的数据

6.3.2 写标签

写标签命令可以用来写标签各个区域的内存，具体的命令格式如下：

地址	定义							
	Bit7	Bit6	Bit5	Bit4	bit3	bit2	bit1	bit0
0	RFU	Ant2	Ant1	Ant0	Mode	Trigger	oToggleBit	Enable
1	RFU							
2	Match	0x43						
3	DateLen							

4	Bank_W
5	Addr_H_W
6	Addr_L_W
7	Number_W
8~8+N	Write Data
9+N	[Bank_M], Match=1 此字段出现, 否则不出现
10+N	[Addr_H_M], Match=1 此字段出现, 否则不出现
11+N	[Addr_L_M], Match=1 此字段出现, 否则不出现
12+N	[Number_M], Match=1 此字段出现, 否则不出现
13+N ~95	[Data_M], Match=1 此字段出现, 否则不出现

其中参数部分字段定义如下:

字段	定义	备注
DateLen	数据长度, 单位 字节 , 从 Bank_W 到[Data_M] 字段	
Bank_W	需要写入的区域: 0: Reserved 1: EPC 2: TID 3: USER DATA	
Addr_H_W	写入数据的 字 地址高字节	
Addr_L_W	写入数据的 字 地址低字节	
Number_W	写入的 字 数量	
Write Data	需要写入的数据, 长度为 Number_W*2 字节	
Bank_M	需要匹配的区域: 0: Reserved 1: EPC 2: TID 3: USER DATA	仅在 Match=1 时, 此字段有效
Addr_H_M	匹配数据的 位 地址高字节	
Addr_L_M	匹配数据的 位 地址低字节	
Number_M	匹配数据的 位长度	
Data_M	需要匹配的数据	

写入标签命令的响应如下：

地址	定义						
	bit6-7	bit5	bit4	bit3	bit2	bit1	bit0
0	RFU	iToggleBit	Err	Done	Busy	TP	Ready
1	RFU						IsPassiveMode
2	Errcode						
3-95							

6.3.3 读 EPC

读 EPC 命令可以用来读取标签各个区域的内存，具体的命令格式如下：

地址	定义							
	Bit7	Bit6	Bit5	Bit4	bit3	bit2	bit1	bit0
0	RFU	Ant2	Ant1	Ant0	Mode	Trigger	oToggleBit	Enable
1	RFU							
2	Matc h	0x41						
3	DataLen = 0							
4~95	NC							

读取 EPC 命令的响应如下：

地址	定义						
	bit6-7	bit5	bit4	bit3	bit2	bit1	bit0
0	RFU	iToggleBit	Err	Done	Busy	TP	Ready
1	RFU						IsPassiveMode
2	Errcode						
3	TagCnt						
4	DataLen						
5	Antenna						
6	PC_H						
7	PC_L						
8~8+x	EPC						
9+x	RSSI						
10+x	NC						

其中响应数据部分字段的定义如下：

字段	定义
----	----

TagCnt	此次读取响应的标签个数。有多个标签响应时，翻转 oToggleBit 将上传下一个标签的数据，TagCnt 也会随之减少。
DataLen	当前上传的标签占的 字节 总数：从 Antenna 到 RSSI 字段。
Antenna	当前标签读取的天线
PC_H	响应标签的 PC 高字节
PC_L	响应标签的 PC 低字节
EPC	响应标签的 EPC
RSSI	响应标签的信号强度。此处需要通过计算才可得到功率值，计算公式为：-39.9+6log2(Y/190)，也可从附件查询对应的值。

6.3.4 写 EPC

写标签命令可以用来写标签各个区域的内存，具体的命令格式如下：

地址	定义							
	Bit7	Bit6	Bit5	Bit4	bit3	bit2	bit1	bit0
0	RFU	Ant2	Ant1	Ant0	Mode	Trigger	oToggleBit	Enable
1	RFU							
2	Match	0x44						
3	DataLen							
4	EPCLen							
5~5+x	EPC							
6 + x	[Bank_M]，Match=1 此字段出现，否则不出现							
7 + x	[Addr_H_M]，Match=1 此字段出现，否则不出现							
8 + x	[Addr_L_M]，Match=1 此字段出现，否则不出现							
9 + x	[Number_M]，Match=1 此字段出现，否则不出现							
10+x ~ 95	[Data_M]，Match=1 此字段出现，否则不出现							

其中参数部分字段定义如下：

字段	定义	备注
DateLen	数据长度,从 EPCLen 到[Data_M]字段,单位 字节	
EPCLen	需要写入的 EPC 的长度,单位 字	

EPC	EPC, 长度为 EPCLen*2 字节	
Bank_M	需要匹配的区域: 0: Reserved 1: EPC 2: TID 3: USER DATA	仅在 Match=1 时, 此字段有效
Addr_H_M	匹配数据的位地址高字节	
Addr_L_M	匹配数据的位地址低字节	
Number_M	匹配数据的位长度	
Data_M	需要匹配的数据	

写入标签命令的响应如下:

地址	定义						
	bit6-7	bit5	bit4	bit3	bit2	bit1	bit0
0	RFU	iToggleBit	Err	Done	Busy	TP	Ready
1	RFU						IsPassiveMode
2	Errcode						
3-95							

6.3.5 读配置

读配置命令可以用来读取产品的配置参数, 具体的命令格式如下:

地址	定义							
	Bit7	Bit6	Bit5	Bit4	bit3	bit2	bit1	bit0
0	RFU	Ant2	Ant1	Ant0	Mode	Trigger	oToggleBit	Enable
1	RFU							
2	0x45							
3	DataLen = 0							
4~95	NC							

读配置命令的响应如下:

地址	定义						
	bit6-7	bit5	bit4	bit3	bit2	bit1	bit0
0	RFU	iToggleBit	Err	Done	Busy	TP	Ready
1	RFU						IsPassiveMode

2	Errcode
3	DataLen
4	ReadPower_0
5	WritePower_0
6	ReadPower_1
7	WritePower_1
8	ReadPower_2
9	WritePower_2
10	RFU
11	RFU
12	Region
13	ChannelCnt
14~95	ChannelLst

其中响应数据部分字段的定义如下：

字段	定义
DataLen	配置的总数据长度，单位字节
ReadPower_ x	读取功率，x 表示对应的天线
WritePower_ x	写入功率，x 表示对应的天线
RFU	预留
Region	频段，支持以下地区： 0: PRC (920 ~ 925MHz) [默认] 3: FCC (902 ~ 928MHz) 4: ETSI (866~868MHz) 8: RUS(866.6~867.4MHz)
ChannelCnt	信道数量，数量为 0 是使用自动跳频： PRC：最多 16 个信道 FCC：最多 50 个信道 ETSI：最多 4 个信道 RUS：最多 5 个信道
ChannelLst	信道列表，信道列表长度与 ChannelCnt 值一致。与各频率值对应的信道编号参见附录

6.3.6 写配置

写配置命令可以用来设置产品的配置参数，具体的命令格式如下：

地址	定义							
	Bit7	Bit6	Bit5	Bit4	bit3	bit2	bit1	bit0
0	RFU	Ant2	Ant1	Ant0	Mode	Trigger	oToggleBit	Enable
1	RFU							
2	0x46							
3	DataLen							
4	ReadPower_0							
5	WritePower_0							
6	ReadPower_1							
7	WritePower_1							
8	ReadPower_2							
9	WritePower_2							
10	RFU							
11	RFU							
12	Region							
13	ChannelCnt							
14~95	ChannelLst							

其中参数部分字段定义如下：

字段	定义	备注
DataLen	配置的总数据长度，单位字节	
ReadPower_ x	读取功率，x 表示对应的天线	3 个端口的功率都需要同时设置。未使用端口可用默认设置，读取 12dbm，写入 18dbm。
WritePower_ x	写入功率，x 表示对应的天线	
RFU	预留	
Region	频段，支持以下地区： 0: PRC (920 ~ 925MHz) 3: FCC (902 ~ 928MHz) 4: ETSI (866~868MHz)	0xFF：保持配置不变， Channel 相关的参数也不配置

	8: RUS(866.6~867.4MHz)	
ChannelCnt	信道数量，数量为 0 是使用自动跳频： PRC：最多 16 个信道 FCC：最多 50 个信道 ETSI：最多 4 个信道 RUS：最多 5 个信道	若 Region 不变，则信道配置不变，ChannelCnt 和 ChannelLst 字段不出现； 若 Region 改变，则信道配置也改变；
ChannelLst	信道列表，信道列表长度与 ChannelCnt 值一致。与各频率值对应的信道编号参见附录	

写配置命令的响应如下：

地址	定义						
	bit6-7	bit5	bit4	bit3	bit2	bit1	bit0
0	RFU	iToggleBit	Err	Done	Busy	TP	Ready
1	RFU						IsPassiveMode
2	Errcode						
3-95							

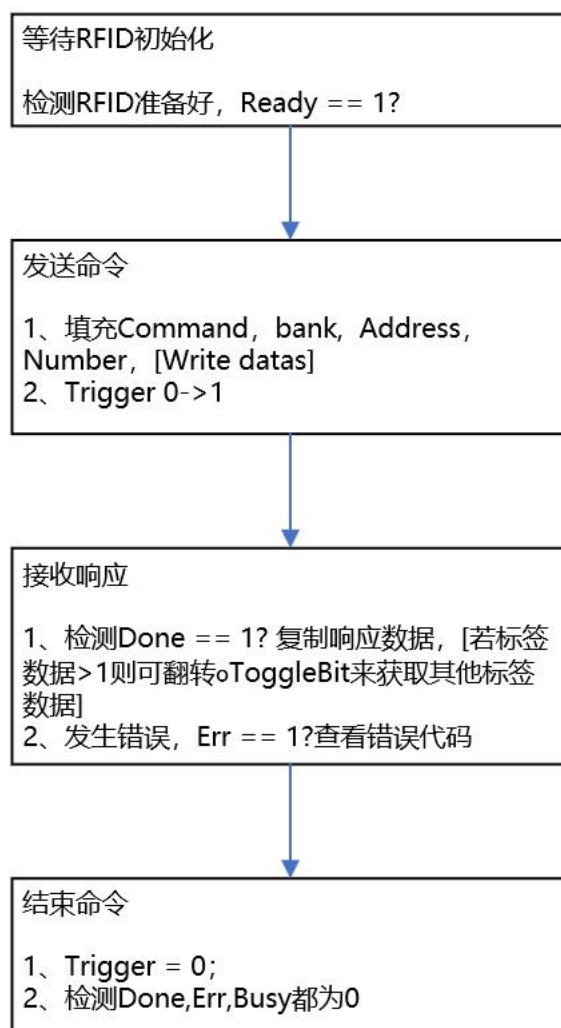
6.4 错误代码

总线模块支持的错误码如下：

错误码		定义	说明
十进制	十六进制		
0	0x00	无错误	
176	0xB0	参数错误	参数错误
177	0xB1	RFID 读取参数错误	RFID 操作时，参数设置错误
178	0xB2	RFID 模块故障	RFID 模块异常，一般出现了硬件故障
179	0xB3	无标签响应	没有标签响应命令
226	0xE2	RFID 数据 CRC 错误	发生在读取时，标签返回给读头的数据出现校验错误
228	0xE4	RFID 数据区溢出	发生在读取时，读取范围超出标签数据区
229	0xE5	RFID 访问密码错误	发生在读取时，标签访问密码错误
241	0xF1	天线端口错误	发生在写入时，天线端口错误
242	0xF2	选择参数错误	发生在写入时，匹配的参数设置错误
245	0xF5	功率不足	发生在写入时，读头功率不足，致使写入失败
246	0xF6	数据区溢出	发生在写入时，写入范围超出标签数据区
257	0xF7	RFID 数据区被锁定	发生在写入时，RFID 内存被锁定，无法写入
248	0xF8	RFID 访问密码错误	发生在写入时，标签访问密码错误
250	0xFA	标签丢失	发生在写入时，无法检测到标签

6.5 应用举例

在实际应用时，建议按照如下的流程进行操作。



6.5.1 RFID 监控

1、RFID 工作状态控制

Output	Input
Enable:1/0	Ready:1/0

2、将 RFID 设置为主动工作模式，并对 RFID 进行监控

Output	Input
使能读写器并设置为主动工作模式 Enable:1 Mode:0	Ready:1

	检测到有 RFID 标签 TagCnt: 标签数量 Datalen: 当前标签信息长度 Antenna: 读取该标签的天线端口 PC+EPC: 标签数据 RSSI: 信号强度 TP: 1
检测到 TP 置 1, 获取标签 EPC 信息 oToggleBit 翻转, 获取下一条标签信息	检测到 oToggleBit, 填充下一条标签信息, TagCnt-1, iToggleBit 翻转

6.5.2 RFID 标签内存读取

从 RFID 标签的 USER 区域地址 0x00 开始, 读取 16 个字节

Output	Input	
Enable:1	Ready:1	
发送读取命令 Command:0x42 DateLen:0x04 Bank_R:0x03 Start Address:0x0000 Number: 0x08(字) Trigger:1	置 Busy:1	
	读取正确 Errcode:0x00 TagCnt: 响应的标签数量 Datalen: 当前标签信息和 读取数据长度总和	读取出错 Errcode:非 0x00 Err:1 Done:1

	Antenna: 读取该标签的天线端口 PC+EPC: 标签数据 RSSI: 信号强度 Datas:读取的数据 Err:0 Done:1	
拷贝数据 翻转 oToggleBit, 获取下一条标签响应的数据	检测到 oToggleBit, 填充下一条标签信息, TagCnt-1, iToggleBit 翻转	
拷贝数据, 若仍有其他标签数据, 继续翻转 oToggleBit; 若结束任务: Trigger:0	Done:0 Busy:0 Err:0	

6.5.3 RFID 标签内存写入

从 RFID 标签的地址 0x0000 开始, 写入 16 个字节

Output	Input
Enable:1	Ready:1
发送读取命令 Command:0x43 DataLen:0x14 Bank_R:0x03 Start Address:0x0000 Number: 0x08(字) Write Data: 需要写入的数据, 16 字节	置 Busy:1

Trigger:1		
	写入成功 Errcode: 0x00 Datalen: 0x00 Err:0 Done:1	写入失败 Errcode:非 0x00 Datalen: 0x00 Err:1 Done:1
结束任务 Trigger:0	Done:0 Busy:0 Err:0	

7. MODUBS 协议

7.1 寄存器定义

对于载码体的读写操作和对读头的配置是通过访问寄存器来完成的，寄存器主要分为 2 个区域：

- 标签内存区域
- 系统内存区域

各个区域具体的地址范围定于如下所示：

System Memory Zone	F000 H ~ F4FF H
Tag Memory Zone	0000 H ~ E37F H

7.1.1 标签内存区域

标签内存区域分为四个部分：EPC 读取区域、EPC 写入区域、TID 读取区域和用户内存区域。

EPC Read Zone	0000 H ~ 04FF H
EPC Write Zone	7F00 H ~ 7F83 H
TID Read Zone	E300 H ~ E37F H
USER Memory Zone	1000 H ~ 4FFF H

EPC 读取区域

	起始寄存器地址	寄存器数量	说明
天线 1	0000 H	256	单独控制天线 1（本体天线）读取 EPC 标签的寄存器地址空间
天线 2	0100 H	256	单独控制天线 2 读取 EPC 标签的寄存器地址空间

天线 3	0200 H	256	单独控制天线 3 读取 EPC 标签的寄存器地址空间
天线 4	0300 H	256	单独控制天线 4 读取 EPC 标签的寄存器地址空间
天线组合	0400 H	256	控制一个天线组合读取 EPC 标签的寄存器地址空间，天线组合的设置请参考地址 F324 H

EPC 读取区域主要是对标签 EPC 读取结果的映射，此区域只读。具体的映射关系如下：

各个地址空间内的寄存器地址定义如下：

偏移地址 ^①	结束地址	寄存器数量	操作类型	说明
00 H	00 H	1	R ^②	读取触发 ^③
01 H	01 H	1	R	标签数量
02 H	02 H	1	R	所有标签占的字节总数
03 H	03 H	1	R	第一个标签，PC
04 H	04+x1	x1	R	第一个标签，EPC，标签实际 EPC 长度
05+x1	05+x1	1	R	第一个标签，RSSI ^④
06+x1	06+x1	1	R	第二个标签，PC
07+x1	07+x1+x2	x2	R	第二个标签，EPC，标签实际 EPC 长度
08+x1+x2	08+x1+x2	1	R	第二个标签，RSSI
.....				以此类推，最多可存 32 个标签

注①：实际使用地址需要用相应天线的起始地址+偏移地址。如触发天线 1

读取，应该读取地址 0000 H；触发组合天线读取，应该读取地址 0400 H。

注②：R 为 Readable 的缩写，标识该寄存器可进行读取操作；W 为 Writable

的缩写，表示该寄存器可进行写入操作；

注③：需要对各天线区域偏移地址为 0000H 寄存器进行读取才会触发重新读

取 EPC，否则读取就是上次读取 EPC 的结果；

注④：此处需要通过计算才可得到功率值，计算公式为： $-39.9+6\log_2(Y/190)$ ，
也可从附件查询对应的值。



使用建议

在正式使用时，先确认好单个标签的 EPC 长度 N 个字，读取 N+5 个寄存器，则刚好可读取一个标签。

EPC 写入区域

EPC 读取区域主要是对标签 EPC 读取结果的映射，此区域只读。具体的映射关系如下：

天线端口	起始地址	结束地址	寄存器 数量	操作 类型	说明
天线 1	7F00 H	7F00 H	1	W	PC ^①
	7F01 H	7F20 H	32	W	EPC
天线 2	7F21 H	7F21 H	1	W	PC ^①
	7F22 H	7F41 H	32	W	EPC
天线 3	7F42 H	7F42 H	1	W	PC ^①
	7F43 H	7F62 H	32	W	EPC
天线 4	7F63 H	7F63 H	1	W	PC ^①
	7F64 H	7F83 H	32	W	EPC

注①：PC 的高 5 位用来定义 EPC 的长度，高 5 位的值即为 EPC 占的寄存器数量。如 PC 为 0x3000，高 5 位为“00110 B”，则 EPC 的长度为 6 个寄存器，即 12 个字节。EPC 的最大长度取决于标签芯片，具体参见该标签的技术手册。

TID 读取区域

TID 读取区域主要是对标签 TID 读取结果的映射，此区域只读。具体的映射关系如下：

	起始地址	结束地址	寄存器数量	操作类型	说明
天线 1	E300 H	E31F H	32	R	
天线 2	E320 H	E33F H	32	R	
天线 3	E340 H	E35F H	32	R	
天线 4	E360 H	E37F H	32	R	

注：TID 读取区域的大小跟标签实际的 TID 内存区域大小有关，不同的标签可能 TID 的大小不一样，一般不会超过 496bits。

用户内存区域

用户内存区域的定义是根据标签用户内存的大小，映射到读头内部的用户内存区域，来对标签进行访问，可读可写。Alien H3 芯片为例，用户内存为 64 字节，映射到用户内存区域的最小偏移地址为 0，最大偏移地址为 31 (1F H)。若访问超过标签的最大内存地址，将返回错误。

各天线对用户内存区域进行读写的映射地址如下：

	起始地址	结束地址	寄存器数量	操作类型	读取用户区偏移地址 2 的访问地址
天线 1	1000 H	1FFF H	4096	RW	0002 H
天线 2	2000 H	2FFF H	4096	RW	1002 H
天线 3	3000 H	3FFF H	4096	RW	2002 H
天线 4	4000 H	4FFF H	4096	RW	3002 H

7.1.2 系统内存区域

系统内存区域分为两个部分：RFID 状态区域和配置区域，其中配置区域包括基本配置区域、工作模式配置区域和超高频参数配置区域。

Configuration Zone	F100 H ~ F4FF H
RFID Status Zone	F000 H ~ F07B H

基本配置区域

基本配置主要包括设备信息和连接相关的参数配置，此部分的寄存器掉电可保存，配置后断电重启生效。具体的寄存器及分配地址如下：

字段	起始地址	结束地址	寄存器数量	操作类型	说明
厂商名字	F100 H	F109 H	10	R	
产品代码	F10A H	F113 H	10	R	
版本号	F114 H	F115 H	2	R	
产品序列号	F116 H	F11B H	6	R	
MAC 地址	F11C H	F11E H	3	R	
端口号	F11F H	F11F H	1	R	固定值 502
IP 地址	F120 H	F121 H	2	RW	默认：192.168.0.10
子网掩码	F122 H	F123 H	2	RW	默认：255.255.255.0
网关	F124 H	F125 H	2	RW	默认：192.168.0.1
设备地址	F126 H	F126 H	1	RW	MODBUS 从站地址,取值[1,16],默认值为 1,0 为广播地址

波特率	F127 H	F127 H	1	RW	从站波特率，串口配置采用 N，8，1； 5:115200[默认]； ELSE：预留
-----	--------	--------	---	----	---

工作模式配置区域

工作模式配置主要用来对 RFID 的工作模式及参数进行配置，此部分的寄存器掉电可保存。RFID 有主动工作模式和被动工作模式。在主动工作模式下，RFID 将自动读取进入到可读区域的标签 EPC。在被动工作模式下，读写器默认处于空闲状态，按照接收的指令来执行工作。具体的寄存器定义如下：

字段	起始地址	结束地址	寄存器数量	操作类型	说明
工作模式	F200 H	F200 H	1	RW	工作模式： 0:被动工作模式； 1:主动工作模式[默认]，F201 有效。在主动工作模式下，使用 F324 H 寄存器配置的天线组合进行工作。
缓存时间	F201 H	F201 H	1	RW	设置自动读取的数据在标签离开后的存储时间，单位 ms[默认 100]

RFID 协议配置区域

RFID 协议配置区域主要用于配置 RFID 所支持的协议。具体的寄存器定义如下：

字段	起始地址	结束地址	寄存器数量	操作类型	说明
RFID 协议	F300 H	F300 H	1	R	RFID 支持的协议：

					3: ISO 18000-6C
读功率_天线 0	F301 H	F301 H	1	RW	读写器的读取功率，默认 12dBm。取值范围 5~30dBm
写功率_天线 0	F302 H	F302 H	1	RW	读写器的写入功率，默认 18dBm。取值范围 5~30dBm
频段	F303 H	F303 H	1	RW	读写器当前的频段： 0: PRC (920 ~ 925MHz) [默认] 3: FCC (902 ~ 928MHz) 4: ETSI (866~868MHz) 8: RUS(866.6~867.4MHz)
信道数量 ^①	F304 H	F304 H	1	RW	读写器使用的信道数量： PRC 最大 16 个，FCC 最大 50 个 当配置信道数量为 0 时，表示使用自动跳频。默认 0
频点 ^①	F305 H	F31D H	25	RW	读写器使用的信道编号，每个寄存器占 2 个信道，先填充高字节。信道数量不为 0 时有效
空口参数 ^①	F31E H	F31E H	1	RW	0: 40K, tari 25us, FM0 编码 1: 250K, tari 25us, M4 编码[默认] 2: 300K, tari 25us, M4 编码 3: 400K, tari6.25us, FM0 编码 4: 320K, tari25us, M4 编码
Q 值 ^①	F31F H	F31F H	1	RW	进行盘存时使用的 Q 值，取值范围[0, 15]，默认 0。当 Q=0 时，读取 EPC (E200H 寄存器触发) 仅会读取 1 个标签。

会话层 ^① (Session)	F320 H	F320 H	1	RW	0: session_0[默认] 1: session_1 2: session_2 3: session_3
盘存标志 ^①	F321 H	F321 H	1	RW	0: A 1: B 2: A 和 B[默认]
重复标签过滤 时间	F322 H	F322 H	1	RW	表示在一个读卡指令执行周期内，在指定的重复过滤时间内相同的标签内容只上传一次，时间单位：10ms
RSSI ^①	F323 H	F323 H	1	RW	标签 RSSI 值低于阈值时标签数据将不上传并丢弃。
使能的天线	F324 H	F324 H	1	RW	用于配置读取 EPC 时的天线组合，见 EB00 H 寄存器，每一个 bit 代表一个天线使能的开关，0：不使用；1：使用。 Bit 与天线的对应关系如下，该寄存器默认值是 0x0001（使用天线 0）。
					Bit0 Bit1 Bit2 Bit3 Bit4:15
					Ant0 Ant1 Ant2 Ant3 RFU
读功率_天线 1	F325 H	F325 H	1	RW	读写器的读取功率，默认 12dBm。取值范围 5~30dBm
写功率_天线 1	F326 H	F326 H	1	RW	读写器的写入功率，默认 18dBm。取值范围 5~30dBm
读功率_天线 2	F327 H	F327 H	1	RW	读写器的读取功率，默认 12dBm。取值范围 5~30dBm

写功率_天线 2	F328 H	F328 H	1	RW	读写器的写入功率，默认 18dBm。取值范围 5~30dBm
读功率_天线 3	F329 H	F329 H	1	RW	读写器的读取功率，默认 12dBm。取值范围 5~30dBm
写功率_天线 3	F32A H	F32A H	1	RW	读写器的写入功率，默认 18dBm。取值范围 5~30dBm

a)：此部分的配置不建议对射频或者 ISO 18000-6C 不熟悉的用户使用。

RFID 状态区域

RFID 状态区域主要用来记录设备当前的工作状态，控制系统可通过状态来

对设备和应用环境进行诊断。RFID 状态区域具体的寄存器定义如下：

字段	起始地址	结束地址	寄存器数量	操作类型	说明
RFID 状态	F000 H	F000 H	1	R	指示当前 RFID 的状态
错误码	F001 H	F001 H	1	R	具体定义见后续章节
RFU	F002 H	F002 H	1	R	
EPC_LEN	F003H	F003 H	1	R	EPC 的占的内存数量
EPC	F004 H	F023 H	32	R	标签 EPC

其中 RFID 状态(F000 H)的详细定义如下：

位地址	标识	定义
bit0	Ready	运行状态,读写器运行正常置位
bit1-2	Mode	工作模式,同寄存器 F200 H: 0:被动工作模式; 1:主动工作模式
bit3	RFU	取值为 0

bit4	TP	Tag Present, 指示是否有标签在读取区域: 0: 无标签 1: 有标签, 不代表已经读取完指定标签内存;
bit5	Cached	指示当前是否有缓存标签: 0: 未缓存 1: 已缓存, 指定标签内存读取完成, 此信号在标签离开后的缓存时间(F201 H 寄存器)结束时消失
bit6-15	RFU	取值为 0

内存映射区域主要是在主动工作模式下使用, 它是对主动工作模式读取参数及读取结果的一个内存映射, 当 Cached 信号(F000H,bit5)置位时, 内存映射区域内的数据有效。

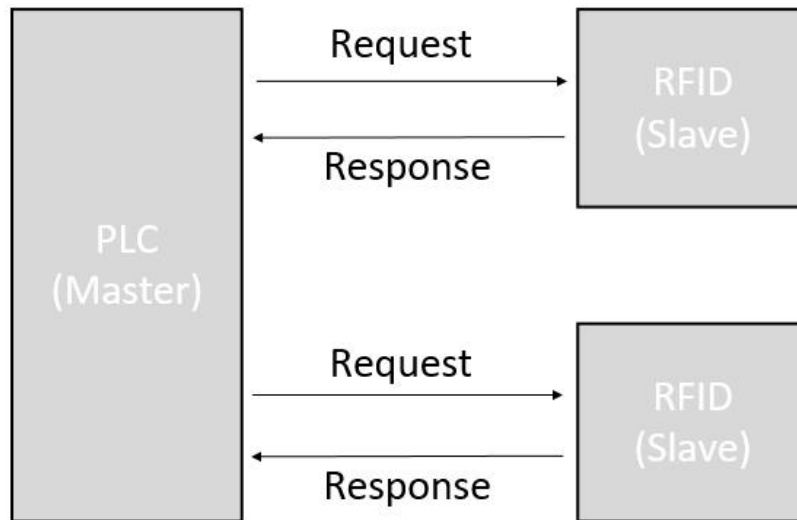
7.2 MODBUS 协议支持

不同的通讯方式的设备使用不同的通讯协议, 在实际应用前, 请先确认设备所支持的通讯方式。对于串口通讯的设备, 包括 RS485 和 RS232, 支持 MODBUS RTU 协议。对于网口设备, 支持 MODBUS TCP 协议。

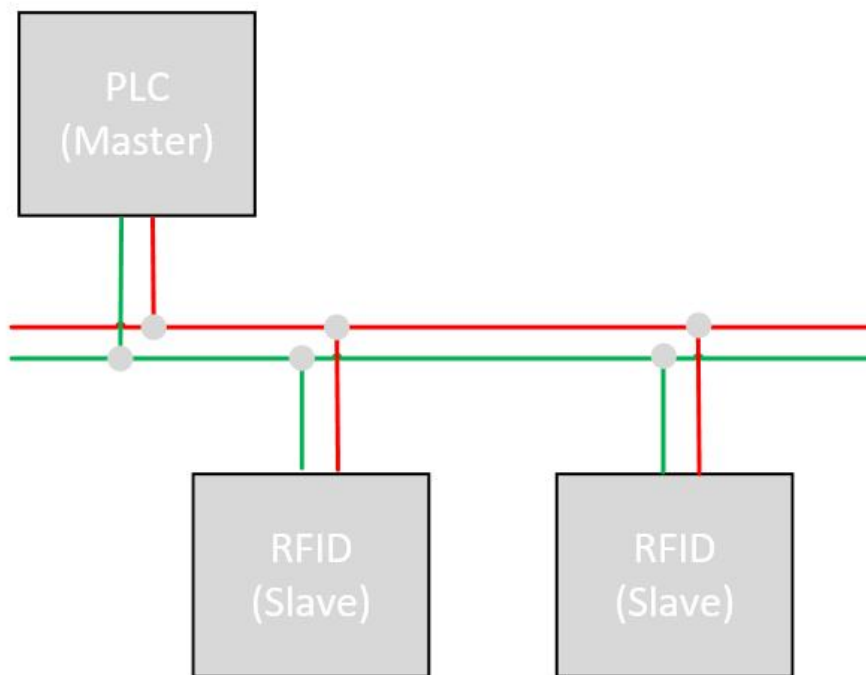
通讯方式	串口(RS485)	以太网
通讯协议	MODBUS RTU	MODBUS TCP

7.2.1 MODBUS RTU 设备配置

在一个串行的通讯网络里面, RFID 设备作为从站使用。在与 PLC 等主设备进行通讯时, 采用问答的方式, 由主设备发起。



建立通讯需要注意设备地址和串口配置参数。默认的设备地址是 1，在使用时可根据实际的情况配置设备地址。当网络里面存在多个设备时，需要将每个从站设备都配置不同的地址，主设备通过地址轮流来控制各个从站设备。多个设备采用并联的方式接入串行网络。



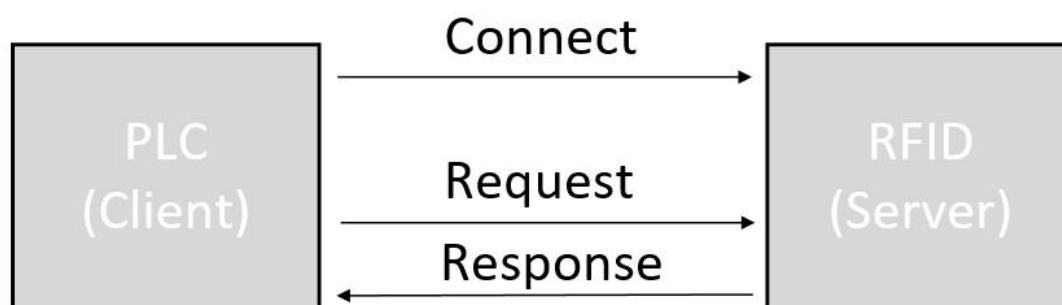
从站设备默认的串口配置如下：

指标	取值
波特率	默认 115200，可配置
校验位	NONE

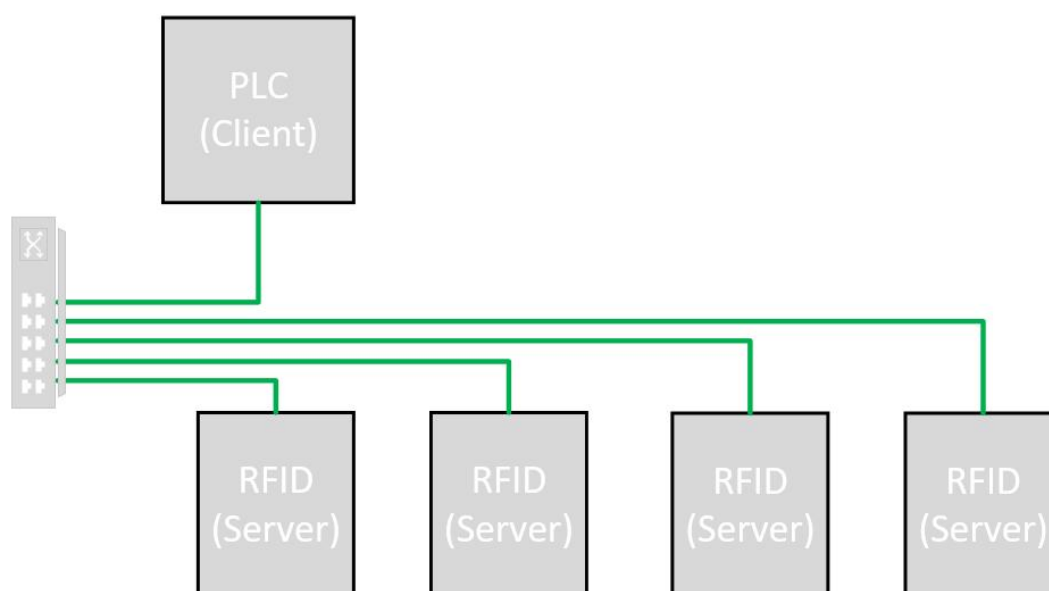
数据位	8 位
停止位	1 位

7.2.2 MODBUS TCP 设备配置

在一个以太网的通讯网络里面，RFID 设备作为服务器，PLC 作为客户端。
在通讯之前需要先建立连接，连接由客户端发起。通讯采用问答的方式，由 PLC 发起。



建立通讯需要配置好 IP 地址，RFID 的默认 IP 地址是 192.168.0.10，
MODBUS TCP 固定的端口号为 502。在建立连接前，需要确认 PLC 与 RFID 在
同一个网段。当有多个设备接入到网络时，需要将每个 RFID 都配置不同的 IP
地址，多个设备可以通过交换机连接到一起。



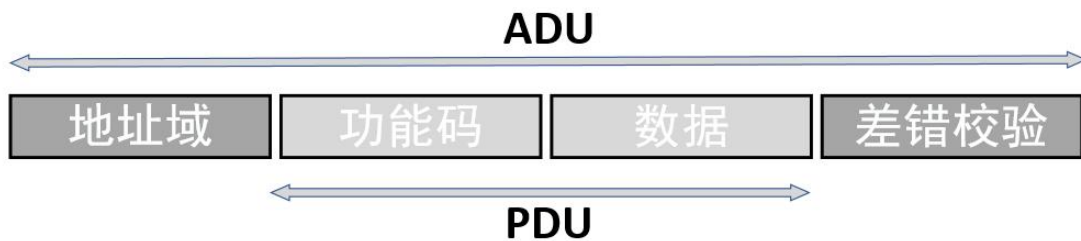
7.2.3 设备支持的命令

此设备支持的 MODBUS 指令如下：

命令码		说明
十六进制	十进制	
03	3	读多个寄存器
06	6	写单个寄存器
10	16	写多个寄存器
5	5	写单个线圈

MODBUS 协议定义了一个与基础通信层无关的简单协议数据单元 (PDU)。

特定总线或网络上的 MODBUS 协议映射能够在应用数据单元 (ADU) 上引入一些附加域。



MODBUS RTU ADU

MODBUS RTU 的 ADU 包含地址域、PDU 和差错校验，其中地址域为设备地址，差错校验位 CRC 校验。

设备地址	功能码	数据	CRC 校验
			Lo Hi
1byte	1byte	N bytes	2 bytes
			MODBUS RTU

- 设备地址：从站设备地址，组网应用 1-16，点对点通讯 0
- CRC 校验：CRC16-MODBUS，对前面的所有数据进行校验

MODBUS TCP ADU

MODBUS RTU 的 ADU 包含地址域、PDU，其中地址域为 MBAP 报文头

MBAP 报文头				功能码	数据
事务元标识符	协议标识符	长度	单元标识符		
Hi Lo	Hi Lo	Hi Lo			
2 bytes	2bytes	2bytes	1byte	1byte	N bytes

- 事务元标识符：事务处理的识别码
- 协议标识符：MODBUS = 0
- 长度：以下字节的数量
- 单元标识符：默认 FFH

1、读多个寄存器

读取多个寄存器的请求 ADU 如下：

协议	地址域					功能码	数据		差错校验
	事务元标识符	协议标识符	长度	单元标识符	设备地址	命令码 3H	地址 Hi Lo	数量 Hi Lo	CRC Lo Hi
RTU	---	---	---	---	1byte	1byte	2 bytes	2 bytes	2 bytes
TCP	2bytes	2bytes	2bytes	1byte	---				---

- 事务元标识符：事务处理的识别码
- 协议标识符：MODBUS = 0
- 长度：以下字节的数量，此处为 6
- 单元标识符：默认 FFH
- 地址：从站设备地址，组网应用 1-16，点对点通讯 0
- 命令码：读取多个寄存器的命令码固定为 3
- 首寄存器地址：需要读取的第一个寄存器的地址
- 寄存器数量：需要读取的寄存器的数量，当读取的区域为标签内存区域时，

取值范围为 $1 \leq N \leq 120$ ，其他情况下，取值范围为 $1 \leq N \leq 123$

读取多个寄存器的正常响应 ADU 如下：

协议	地址域					功能码	数据		差错校验
	事务元标识符	协议标识符	长度	单元标识符	设备地址	命令码 3H	字节数	寄存器值 Hi Lo	CRC Lo Hi
RTU	---	---	---	---	1byte	1byte	1 bytes	2bytes (寄存器 1)	2 bytes
TCP	2bytes	2bytes	2bytes	1byte	---				---

.....
2bytes (寄存器 N)

- 命令码：与请求一致
- 读取的字节数：寄存器数量的 2 倍
- 寄存器值：需要读取的寄存器的值

读取多个寄存器的异常响应 ADU 如下：

协议	地址域					功能码	数据	差错校验
	事务元标识符	协议标识符	长度	单元标识符	设备地址	命令码 83H	错误码	CRC Lo Hi
RTU	---	---	---	---	1byte	1byte	1byte	2 bytes
TCP	2bytes	2bytes	2bytes	1byte	---			---

2、写单个寄存器

写单个寄存器的请求 ADU 如下：

协议	地址域					功能码	数据		差错校验
	事务元 标识符	协议标 识符	长度	单元标 识符	设备 地址	命令码 6H	地址 Hi Lo	寄存器值 Hi Lo	CRC Lo Hi
RTU	---	---	---	---	1byte	1byte	2 bytes	2 bytes	2 bytes
TCP	2bytes	2bytes	2bytes	1byte	---				---

- 命令码：读取多个寄存器的命令码固定为 6
- 寄存器地址：需要操作的寄存器地址
- 寄存器值：需要操作的寄存器的值

写单个寄存器的正常响应 ADU 如下：

协议	地址域					功能码	数据		差错校验
	事务元 标识符	协议标 识符	长度	单元标 识符	设备 地址	命令码 6H	地址 Hi Lo	寄存器值 Hi Lo	CRC Lo Hi
RTU	---	---	---	---	1byte	1byte	2 bytes	2 bytes	2 bytes
TCP	2bytes	2bytes	2bytes	1byte	---				---

- 地址：与请求一致
- 命令码：与请求一致
- 寄存器地址：与请求一致
- 寄存器值：与请求一致

写单个寄存器的异常响应 ADU 如下：

协议	地址域					功能码	数据	差错校验
	事务元 标识符	协议标 识符	长度	单元标 识符	设备 地址	命令码 86H	错误码	CRC Lo Hi
RTU	---	---	---	---	1byte	1byte	1byte	2 bytes
TCP	2bytes	2bytes	2bytes	1byte	---			---

4、写多个寄存器

写多个寄存器的请求 ADU 如下：

协议	地址域					功能码	数据				差错校验
	事务元标识符	协议标识符	长度	单元标识符	设备地址	命令码 10H	寄存器地址 Hi Lo	寄存器数量 Hi Lo	字节数	寄存器值 Hi Lo	CRC Lo Hi
RTU	---	---	---	---	1byte	1byte	2 bytes	2 bytes	1byte	2bytes (第 1 个寄存器)	2 bytes
TCP	2bytes	2bytes	2bytes	1byte	---						---
										2bytes (第 1 个寄存器)	

- 命令码：读取多个寄存器的命令码固定为 10H
- 寄存器地址：需要操作的首个寄存器地址
- 寄存器数量：需要操作的寄存器的数量，当操作的区域为标签内存区域时，取值范围为 $1 \leq N \leq 120$ ，其他情况下，取值范围为 $1 \leq N \leq 121$
- 字节数：寄存器值总共占用的字节数， $2 \times \text{寄存器数量}$
- 寄存器值：需要操作的寄存器的值

写多个寄存器的正常响应 ADU 如下：

协议	地址域					功能码	数据		差错校验
	事务元标识符	协议标识符	长度	单元标识符	设备地址	命令码 10H	寄存器地址 Hi Lo	寄存器数量 Hi Lo	CRC Lo Hi
RTU	---	---	---	---	1byte	1byte	2 bytes	2 bytes	2 bytes

TCP	2bytes	2bytes	2bytes	1byte	---				---
-----	--------	--------	--------	-------	-----	--	--	--	-----

- 命令码：与请求一致
- 寄存器地址：与请求一致
- 寄存器数量：与请求一致

写多个寄存器的异常响应 ADU 如下：

协议	地址域					功能码	数据	差错校验
	事务元标识符	协议标识符	长度	单元标识符	设备地址	命令码 90H	错误码	CRC Lo Hi
RTU	---	---	---	---	1byte	1byte	1byte	2 bytes
TCP	2bytes	2bytes	2bytes	1byte	---			---

5、写单个线圈

写单个线圈的请求 ADU 如下：

协议	地址域					功能码	数据		差错校验
	事务元 标识符	协议标 识符	长度	单元标 识符	设备 地址	命令码 5H	线圈地址 Hi Lo	线圈值 Hi Lo	CRC Lo Hi
RTU	---	---	---	---	1byte	1byte	2 bytes	2 bytes	2 bytes
TCP	2bytes	2bytes	2bytes	1byte	---				---

- 地址：从站设备地址，组网应用 1-16，点对点通讯 0
- 命令码：读取多个寄存器的命令码固定为 5
- 线圈地址：需要操作的线圈地址
- 线圈值：需要操作的线圈的值，0 或者 1

写单个线圈的正常响应 ADU 如下：

协议	地址域					功能码	数据		差错校验
	事务元 标识符	协议标 识符	长度	单元标 识符	设备 地址	命令码 5H	线圈地址 Hi Lo	线圈值 Hi Lo	CRC Lo Hi
RTU	---	---	---	---	1byte	1byte	2 bytes	2 bytes	2 bytes
TCP	2bytes	2bytes	2bytes	1byte	---				---

- 命令码：与请求一致
- 线圈地址：与请求一致
- 线圈值：与请求一致

写单个线圈的异常响应 ADU 如下：

	地址域					功能码	数据	差错校验
协议	事务元 标识符	协议标 识符	长度	单元标 识符	设备 地址	命令码 85H	错误码	CRC Lo Hi
RTU	---	---	---	---	1byte	1byte	1byte	2 bytes
TCP	2bytes	2bytes	2bytes	1byte	---			---

7.3 产品复位

此读写器使用线圈来模拟 RFID 设备的复位脚，将该线圈拉低，此 RFID 将立刻进行软件重启。

线圈地址	操作方式	操作命令
0xFFFF	置 0	写单个线圈，命令值 5



注：读写器将不会对复位操作进行指令响应。

7.4 错误码

错误码包括两个部分：MODBUS 指令返回的错误码，此部分是为了兼容

MODBUS 协议存储在 F001H 寄存器的自定义错误码 MODBUS 错误码定义如

下：

错误码	定义	说明
00H	无错误	
01H	命令码错误	所使用的命令码不支持
02H	地址错误	使用了不存在的地址，或对只读的地址进行写操作
03H	数据错误	使用了非法制进行系统配置寄存器的写操作
04H	设备异常	设备出现故障
0BH	无响应	当标签不在读取区域或标签未对指令进行正确响应时，将出现该错误。此时可从自定义错误码(F001H 寄存器)获取更详细的信息。

8. 附录

8.1 RSSI 值对应表

值	RSSI(dBm)	值	RSSI(dBm)	值	RSSI(dBm)	值	RSSI(dBm)
1	-85.31913365	65	-49.18492677	129	-43.25177012	193	-39.76439143
2	-79.31913365	66	-49.05276893	130	-43.18492677	194	-39.7196566
3	-75.80935865	67	-48.92259851	131	-43.11859564	195	-39.67515177
4	-73.31913365	68	-48.7943566	132	-43.05276893	196	-39.63087459
5	-71.38756508	69	-48.66798691	133	-42.98743904	197	-39.58682273
6	-69.80935865	70	-48.54343555	134	-42.92259851	198	-39.54299393
7	-68.47500412	71	-48.42065093	135	-42.85824007	199	-39.49938593
8	-67.31913365	72	-48.29958364	136	-42.7943566	200	-39.45599651
9	-66.29958364	73	-48.1801863	137	-42.73094115	201	-39.4128235
10	-65.38756508	74	-48.06241346	138	-42.66798691	202	-39.36986475
11	-64.56254394	75	-47.94622151	139	-42.60548721	203	-39.32711815
12	-63.80935865	76	-47.83156857	140	-42.54343555	204	-39.2845816
13	-63.11649534	77	-47.71841441	141	-42.48182554	205	-39.24225305
14	-62.47500412	78	-47.60672034	142	-42.42065093	206	-39.20013049
15	-61.87779008	79	-47.49644916	143	-42.35990563	207	-39.1582119
16	-61.31913365	80	-47.38756508	144	-42.29958364	208	-39.11649534
17	-60.7943566	81	-47.28003363	145	-42.23967911	209	-39.07497886
18	-60.29958364	82	-47.17382162	146	-42.1801863	210	-39.03366054
19	-59.83156857	83	-47.06889706	147	-42.12109958	211	-38.99253852
20	-59.38756508	84	-46.96522911	148	-42.06241346	212	-38.95161092
21	-58.96522911	85	-46.86278803	149	-42.00412253	213	-38.91087593
22	-58.56254394	86	-46.76154512	150	-41.94622151	214	-38.87033173
23	-58.17776191	87	-46.66147267	151	-41.88870521	215	-38.82997655
24	-57.80935865	88	-46.56254394	152	-41.83156857	216	-38.78980864
25	-57.45599651	89	-46.46473306	153	-41.77480659	217	-38.74982626
26	-57.11649534	90	-46.36801507	154	-41.71841441	218	-38.7100277
27	-56.78980864	91	-46.27236581	155	-41.66238722	219	-38.67041129
28	-56.47500412	92	-46.17776191	156	-41.60672034	220	-38.63097537
29	-56.17124768	93	-46.08418078	157	-41.55140916	221	-38.59171829
30	-55.87779008	94	-45.99160054	158	-41.49644916	222	-38.55263845
31	-55.59395579	95	-45.9	159	-41.44183592	223	-38.51373425
32	-55.31913365	96	-45.80935865	160	-41.38756508	224	-38.47500412
33	-55.05276893	97	-45.7196566	161	-41.33363238	225	-38.4364465
34	-54.7943566	98	-45.63087459	162	-41.28003363	226	-38.39805988
35	-54.54343555	99	-45.54299393	163	-41.22676472	227	-38.35984273
36	-54.29958364	100	-45.45599651	164	-41.17382162	228	-38.32179356
37	-54.06241346	101	-45.36986475	165	-41.12120036	229	-38.28391092

38	-53.83156857	102	-45.2845816	166	-41.06889706	230	-38.24619334
39	-53.60672034	103	-45.20013049	167	-41.0169079	231	-38.2086394
40	-53.38756508	104	-45.11649534	168	-40.96522911	232	-38.17124768
41	-53.17382162	105	-45.03366054	169	-40.91385703	233	-38.13401678
42	-52.96522911	106	-44.95161092	170	-40.86278803	234	-38.09694533
43	-52.76154512	107	-44.87033173	171	-40.81201856	235	-38.06003197
44	-52.56254394	108	-44.78980864	172	-40.76154512	236	-38.02327535
45	-52.36801507	109	-44.7100277	173	-40.71136428	237	-37.98667416
46	-52.17776191	110	-44.63097537	174	-40.66147267	238	-37.95022707
47	-51.99160054	111	-44.55263845	175	-40.61186698	239	-37.9139328
48	-51.80935865	112	-44.47500412	176	-40.56254394	240	-37.87779008
49	-51.63087459	113	-44.39805988	177	-40.51350035	241	-37.84179763
50	-51.45599651	114	-44.32179356	178	-40.46473306	242	-37.80595423
51	-51.2845816	115	-44.24619334	179	-40.41623899	243	-37.77025863
52	-51.11649534	116	-44.17124768	180	-40.36801507	244	-37.73470962
53	-50.95161092	117	-44.09694533	181	-40.32005833	245	-37.69930602
54	-50.78980864	118	-44.02327535	182	-40.27236581	246	-37.66404662
55	-50.63097537	119	-43.95022707	183	-40.22493462	247	-37.62893026
56	-50.47500412	120	-43.87779008	184	-40.17776191	248	-37.59395579
57	-50.32179356	121	-43.80595423	185	-40.13084489	249	-37.55912206
58	-50.17124768	122	-43.73470962	186	-40.08418078	250	-37.52442794
59	-50.02327535	123	-43.66404662	187	-40.03776689	251	-37.48987233
60	-49.87779008	124	-43.59395579	188	-39.99160054	252	-37.45545411
61	-49.73470962	125	-43.52442794	189	-39.9456791	253	-37.4211722
62	-49.59395579	126	-43.45545411	190	-39.9	254	-37.38702553
63	-49.45545411	127	-43.38702553	191	-39.85456068	255	-37.35301303
64	-49.31913365	128	-43.31913365	192	-39.80935865		

8.2 信道频率对应表

PRC		FCC					
信道	频率 (KHz)	信道	频率 (KHz)	信道	频率 (KHz)	信道	频率 (KHz)
0	920625	0	902750	17	911250	34	919750
1	920875	1	903250	18	911750	35	920250
2	921125	2	903750	19	912250	36	920750
3	921375	3	904250	20	912750	37	921250
4	921625	4	904750	21	913250	38	921750
5	921875	5	905250	22	913750	39	922250
6	922125	6	905750	23	914250	40	922750
7	922375	7	906250	24	914750	41	923250
8	922625	8	906750	25	915250	42	923750
9	922875	9	907250	26	915750	43	924250
10	923125	10	907750	27	916250	44	924750
11	923375	11	908250	28	916750	45	925250
12	923625	12	908750	29	917250	46	925750
13	923875	13	909250	30	917750	47	926250
14	924125	14	909750	31	918250	48	926750
15	924375	15	910250	32	918750	49	927250
		16	910750	33	919250		
ETSI		RUS					
信道	频率 (KHz)	信道	频率 (KHz)				
0	865700	0	866600				
1	866300	1	866800				
2	866900	2	867000				
3	867500	3	867200				
		4	867400				

8.3 组态文件

组态文件请联系销售人员获取。

协议	订货型号	文件类型	文件名称
ProfiNet	HSR-UQ215-PN	GSDML 文件	GSDML-V2.32-HSR-UQ215-PN-20250826.xml
Ethernet/IP	HSR-UQ215-EIP	EDS 文件	HollySys HSR-UQ215-EIP_V1.1.EDS
EtherCAT	HSR-UQ215-ECT	ESI 文件	HollySys HSR-UQ215-ECT_20250826.xml

注：不同地区的订货型号可能不一样