**客房管理系统Modbus扩展协议说明**

|  |  |
| --- | --- |
| 版本 | V1.0 |
| 所属项目 | 客房管理系统 |
| 作者 |  |
| 时间 | 2017-12-24 |

|  |  |  |
| --- | --- | --- |
| 修订记录 | | |
| 修订时间 | 修订内容 | 修订人 |
| 2017-12-24 | 初稿 |  |
|  |  |  |

本文档用于描述上位机和客房管理设备使用Modbus扩展功能通信约定。

1. 功能码简介
2. 功能码0x65：发送通信密码

利用该功能码，主机可以向从机发送通讯密码，所有写操作都需要先发送通信密码，然后再使用Modbus标准功能下发数据

例如：主机向从机发送修改服务器信息（地址0x0138）命令

主机发送的报文格式：

|  |  |  |  |
| --- | --- | --- | --- |
| 主机 | 字节数 | 发送信息 | 备注 |
| 网络传输标识 | 6 |  |  |
| 从机地址 | 1 | 0x01 | 发送到地址为0x01的从机 |
| 功能码 | 1 | 0x65 | 发送通信密码 |
| 起始地址 | 2 | 0XFFF0 | 起始地址 |
| 写入数据 | 4 |  |  |

从机回应：

|  |  |  |  |
| --- | --- | --- | --- |
| 主机 | 字节数 | 发送信息 | 备注 |
| 网络传输标识 | 6 |  |  |
| 从机地址 | 1 | 0x01 | 来自从机0x01 |
| 功能码 | 1 | 0x65 | 发送通信密码 |
| 操作结果 | 1 | 0x01 | 0x01：操作成功 0x00：操作失败 |

主机发送的报文格式：

|  |  |  |  |
| --- | --- | --- | --- |
| 主机 | 字节数 | 发送信息 | 备注 |
| 网络传输标识 | 6 |  |  |
| 从机地址 | 1 | 0x01 | 发送到地址为0x01的从机 |
| 功能码 | 1 | 0x05 | 写单线圈 |
| 起始地址 | 2 | 0x0138 | 起始地址 |
| 写入数据 | 2 | 0xFF00 | 写入数据 |

从机回应：

|  |  |  |  |
| --- | --- | --- | --- |
| 主机 | 字节数 | 发送信息 | 备注 |
| 网络传输标识 | 6 |  |  |
| 从机地址 | 1 | 0x01 | 来自0x01的从机 |
| 功能码 | 1 | 0x05 | 写单线圈 |
| 起始地址 | 2 | 0x0138 | 起始地址 |
| 写入数据 | 2 | 0xFF00 | 写入数据 |

1. 功能码0x66：下载程序文件

利用下载程序文件功能码，主机可以向从机的备份程序区写入数据

例如：主机写升级文件的前256字节数量数据到从机的升级程序区。

主机发送的报文格式：

|  |  |  |  |
| --- | --- | --- | --- |
| 主机 | 字节数 | 发送信息 | 备注 |
| 网络传输标识 | 6 |  |  |
| 从机地址 | 1 | 0x01 | 发送到地址为0x01的从机 |
| 功能码 | 1 | 0x66 | 下载升级程序文件 |
| 起始地址 | 2 | 0x0000 | 起始地址 |
| 写字节数 | 2 | 0x0100 | 要写入字节个数 |
| 写入数据1 | 1 | 0x01 | 数据0x01写入升级程序0x0000地址 |
| 写入数据2 | 1 | 0x02 | 数据0x02写入升级程序0x0001地址 |
| … | … | … | … |

从机回应：

|  |  |  |  |
| --- | --- | --- | --- |
| 主机 | 字节数 | 发送信息 | 备注 |
| 网络传输标识 | 6 |  |  |
| 从机地址 | 1 | 0x01 | 来自从机0x01 |
| 功能码 | 1 | 0x66 | 下载升级程序文件 |
| 起始地址 | 2 | 0x0000 | 该包升级程序文件的偏移地址 |
| 写入字节数 | 2 | 0x0100 | 写入的字节数 |

1. 功能码0x67：升级操作命令

利用该功能，可以完成从机升级

主机发送的报文格式：

|  |  |  |  |
| --- | --- | --- | --- |
| 主机 | 字节数 | 发送信息 | 备注 |
| 网络传输标识 | 6 |  |  |
| 从机地址 | 1 | 0x01 | 发送到地址为0x01的从机 |
| 功能码 | 1 | 0x67 | 升级操作 |
| 操作码 | 1 | 0x01 | 0x01：启动升级  0x02：升级文件下载完毕 |

从机回应：

|  |  |  |  |
| --- | --- | --- | --- |
| 主机 | 字节数 | 发送信息 | 备注 |
| 网络传输标识 | 6 |  |  |
| 从机地址 | 1 | 0x01 | 来自从机0x01 |
| 功能码 | 1 | 0x67 | 升级操作命令 |
| 操作码 | 1 | 0x01 | 0x01：启动升级  0x02：升级文件下载完毕 |
| 结果 | 1 | 0x01 | 0x01：升级成功 0x00：升级失败 |

1. 功能码0x68：重启设置

利用该功能，可以使从机软复位重启

主机发送的报文格式：

|  |  |  |  |
| --- | --- | --- | --- |
| 主机 | 字节数 | 发送信息 | 备注 |
| 网络传输标识 | 6 |  |  |
| 从机地址 | 1 | 0x01 | 发送到地址为0x01的从机 |
| 功能码 | 1 | 0x68 | 重启设备 |

从机回应：

|  |  |  |  |
| --- | --- | --- | --- |
| 主机 | 字节数 | 发送信息 | 备注 |
| 网络传输标识 | 6 |  |  |
| 从机地址 | 1 | 0x01 | 来自从机0x01 |
| 功能码 | 1 | 0x68 | 重启设备 |
| 结果 | 1 | 0x01 | 0x01：成功 0x00：失败 |

1. 升级流程

