

应用案例

S7-1200 (固件 v4.x) PLC 网口接入 EMCP 云平台



版本：V1.2

河北蓝蜂信息科技有限公司

2020-08-19



S7-1200 (固件 v4.x) PLC 通过网口 DTU 接入 EMCP 云平台

前言：西门子 S7-1200 PLC (以下简称 S7-1200) 是一款优秀的可编程控制器，广泛应于工业控制领域，是一款性能高，运行稳定的控制器。S7-1200 具备网口进行程序的上下下载和通讯，此次我们要使用 MODBUS-TCP 协议，通过网口把 S7-1200 连接到 EMCP 物联网云平台 (简称 EMCP)，实现电脑 Web 网页、手机 APP 和微信对 S7-1200 内的 MW1000、MW1002、I0.0 寄存器的远程监控和 MW1004 和 Q0.0 的远程读写

一、准备工作。

1.1 在对接前我们需准备如下物品；

- 1) 西门子 S7-1200 (固件 v4.x) PLC 一台，及通讯用 RJ45 网线。
- 2) 河北蓝蜂科技的 GM20 DTU 模块一台，天线和电源适配器 (WM20 DTU 使用方法相同)。
- 3) 4G SIM 卡一张，有流量，大卡，任意运营商均可。
- 4) 联网电脑一台 (WinXP/Win7/Win8/Win10 操作系统)。



1.2 DTU 准备工作

此处参考《GM20-DTU 用户使用手册》进行操作，我们需要对 DTU 网关 (以下均以 GM20-DTU 网关来介绍) 连接天线、插上 SIM 卡、连接 12V 或 24V 的电源适配器。

1.3 PLC 准备工作。

S7-1200 连接 220V 交流电，先使用电脑通过网线连接 PLC 的以太网通讯口进行程序的配置，然后使用网线连接 GM20 的 LAN 口和 PLC 的以太网口，进行 MODBUS-TCP 通讯。



二, PLC 的 MODBUS-TCP 服务器的创建。

第一步, 使用西门子的《TIA Portal》(以下简称博途) 软件, 本文使用的软件版本是 V14。将 S7-1200 设备组态, 设置 PLC 通讯 IP, 如下图:

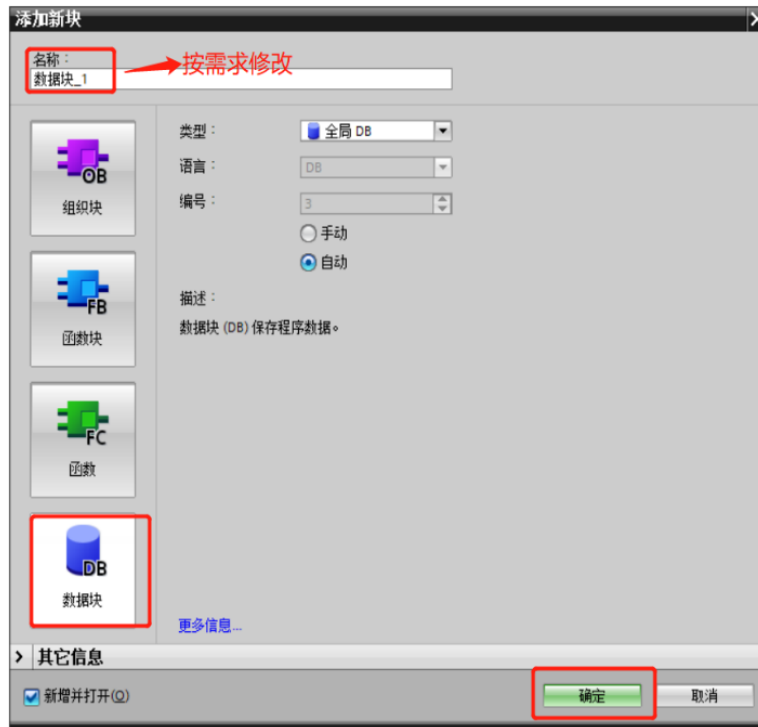
The image consists of two screenshots from the Siemens TIA Portal software interface, illustrating the configuration of a SIMATIC S7-1200 PLC for MODBUS-TCP communication.

Top Screenshot: Shows the main configuration window for the PLC. The left sidebar displays the project tree, including the device configuration for 'PLC_1 [CPU 1214C AC/DC/Rly]'. The main workspace shows a rack configuration with slots 03, 102, 101, 1, 2, and 3. A red box highlights the network port icon in slot 1, with a yellow text overlay '双击网口设置' (Double-click network port settings).

Bottom Screenshot: Shows the 'PROFINET 接口_1 [Module]' properties dialog. The '常规' (General) tab is active. The '以太网地址' (Ethernet address) section is expanded, showing the '接口连接到' (Interface connected to) dropdown set to 'PN/IE_1'. The 'IP 协议' (IP protocol) section is selected, and the '在项目中设置 IP 地址' (Set IP address in project) radio button is chosen. The 'IP 地址' (IP address) field is set to '192.168.2.2' and the '子网掩码' (Subnet mask) field is set to '255.255.255.0'. Both fields are highlighted with a red box and a yellow text overlay '设置PLC的通讯IP' (Set PLC communication IP).



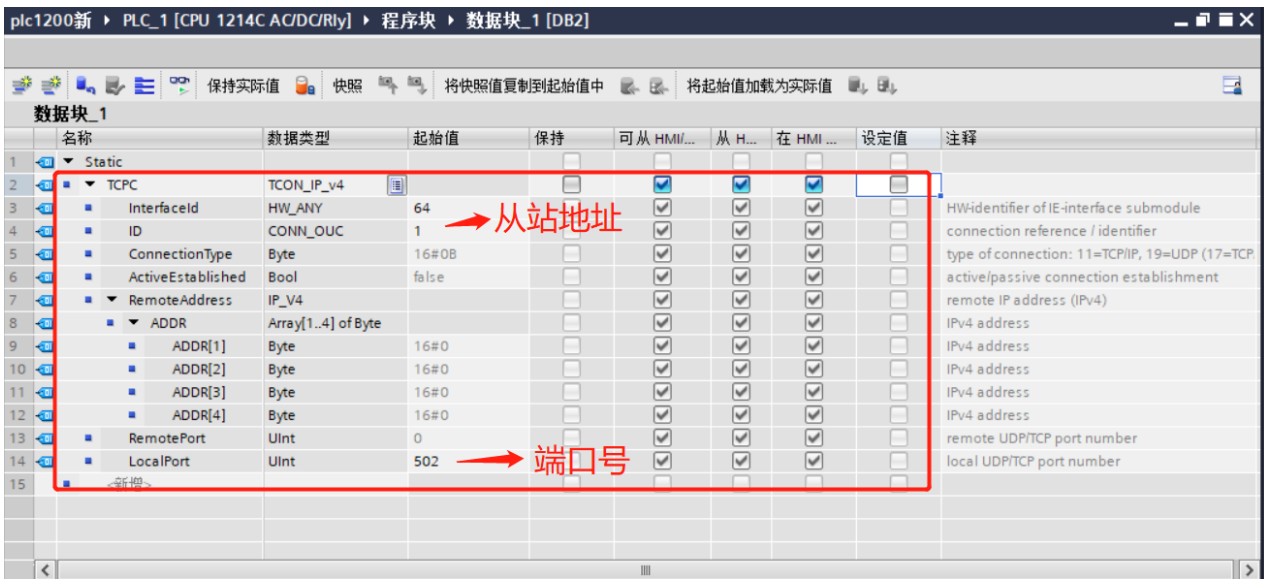
第二步，在程序块中添加数据块，点击确认。如图进行设置。



在 DB 块参数中直接**手动输入**“TCON_IP_v4”，即可创建一个 TCON_IP_v4 类型的数据，然后点开“TCP”前面的箭头，展开后进行填写，如下图所示。



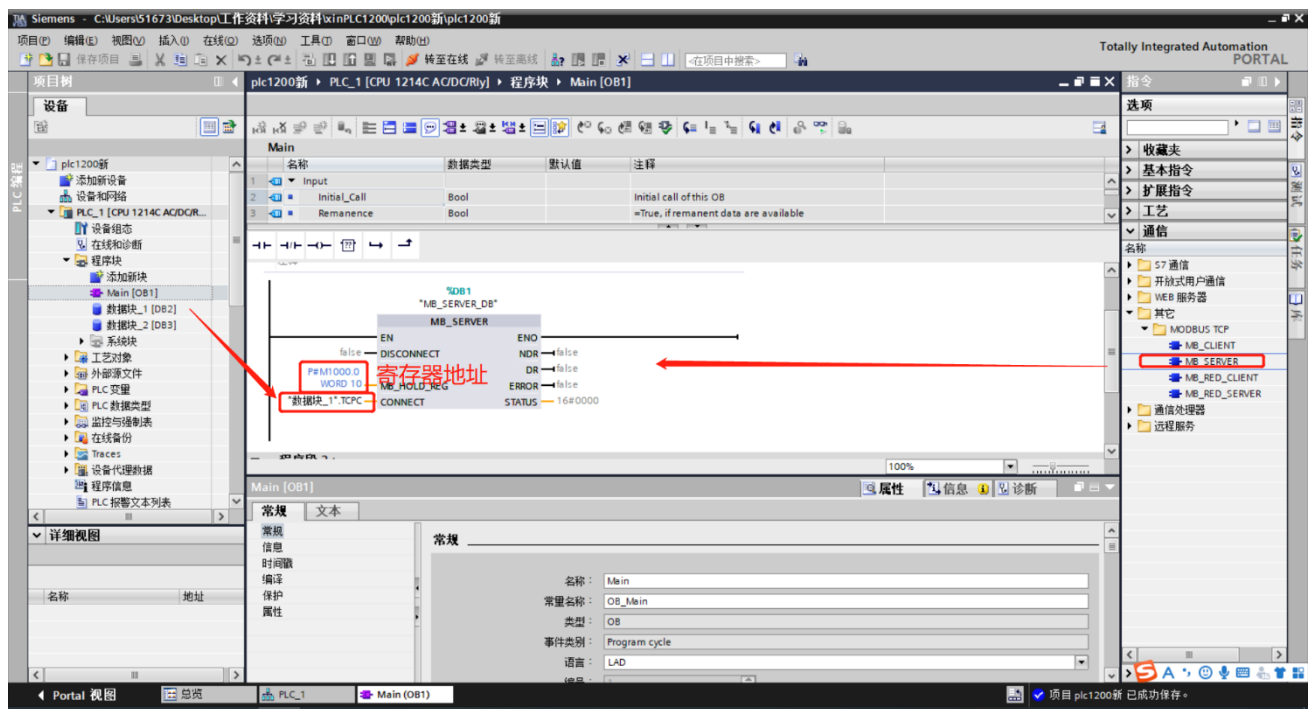
展开数据中包含了建立通讯连接时的所有参数，按下图修改其中的参数。



注意:数据块中的 ID 为连接 ID 编号,要与程序中其他的通讯连接编号区分开,此处默认设置为 1。LocalPort 为本地端口号,此处设置为 502。ADDR 为客户端的 IP 地址,这里可以默认为 0.0.0.0。

第三步,在程序块中的 Main[OB1],添加 Modbus-TCP 服务器指令块“MB_SERVER”。在创建过程中会提示生成相应指令块的背景数据块,点确认进行生成。

注意: MODBUS-TCP 指令库在指令库中的“其他”分组中。



上面指令设置的参数是:通过 MODBUS-TCP 进行通讯,【CONNECT】指向包含建立连接所需参数的 TCON_IP_v4 地址,此处的“数据块_1”.TCPC 即指向的 DB2 里的 TCPC 数据;【MB_HOLD_REG】是指保持寄存器区域起始地址为 MW1000,长度为 10 个字,即为 MW1000 到 MW1018。

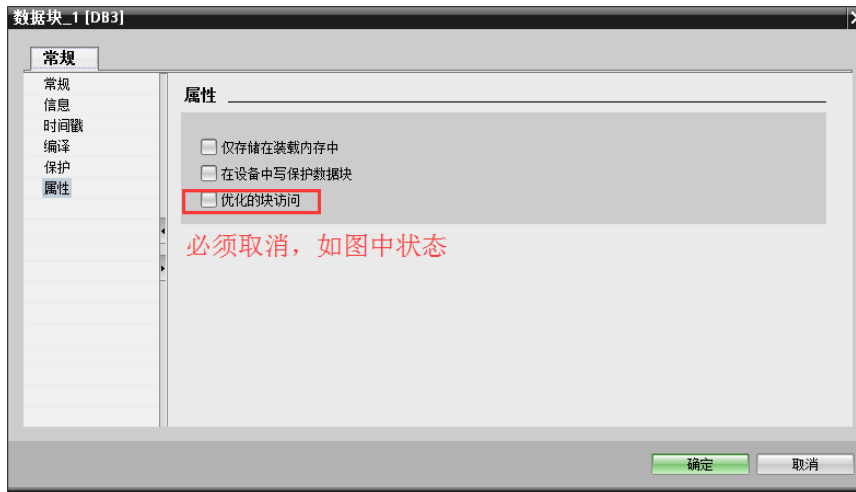
注 1: MB_SERVER 指令块详细使用说明请参考博图帮助文档,如下图,信息系统的路径是:“对 PLC

进行编程” → “指令” → “通讯 (S7-1200, S7-1500)” → “通讯处理器 (S7-1200, S7-1500)” → “MODBUS (TCP) (S7-1200, S7-1500)”



注 2: 如果想要试用 MODBUS-TCP 访问全局数据块 (DB)，需要满足以下两个条件:

首先: 数据块 DB 的属性中的优化访问必须取消;



然后: 在 MB_SERVER 的寄存器指向中，使用指针指向该 DB 地址，如下图，同时在 CONNECT 处添加 TPC 数据块。



上图设置的指令就是通过 MODBUS-TCP 进行通讯，【CONNECT】指向包含建立连接所需参数的 TCON_IP_v4 地址，此处的“数据块_1”.TCPC 即指向的 DB2 里的 TCPC 数据；【MB_HOLD_REG】是指保持寄存器区域起始地址为 DB3.DBW0，长度为 10 个字，即为 DB3.DBW0 到 DB3.DBW9。

第三步，将修改好的程序下载到 PLC 中，此处需要注意，一定要使用“在线 (O)”选项中的“下载并复位 PLC 程序”，如图：



三、EMCP 平台设置。

用管理员账号登录 EMCP 平台 www.lfemcp.com（建议使用 IE9 以上浏览器或谷歌浏览器），对 EMCP 云平台进行设置。具体操作参照《EMCP 物联网云平台用户手册》。登录 EMCP 后首先进入设备列表显示页面，因为我们未创建任何设备，所以是一个空页面。点击右上角的“后台管理”按钮（只有管理账号才有此权限），进入 EMCP 平台的后台。



3.1 远程配置 DTU

打开“后台管理—>模块管理”页面，将 DTU 绑定至此管理员账号，然后就可以使用“远程配置”功能来配置 DTU 的各项通讯参数和功能参数。最主要两个地方需要配置，一是与 PLC 通讯口参数，二是设置 DTU 定时采集 PLC 数据的 MODBUS 通道参数，下面分步骤对此功能进行讲解。**注：模块只有在线后才可**



以进行远程配置。

3.1.1 模块绑定



模块初始绑定密码是 111111，直接点击绑定即可。

3.1.2 模块远程配置

在【模块管理】中使用对应 DTU 的【远程管理】功能来进行 DTU 各项通讯参数的设置；模块的远程配置最好先【读取】再【写入】，只有写入成功后才表示该参数成功配置到 DTU 中，执行写入后也可以通过读取操作来检查之前的操作是否成功。第一步进入状态信息页，查看 DTU 状态，如下图：



第二步,进行【通讯设置】,将 DTU 的通讯口设置为 LAN 网口通讯,因为 PLC 的 IP 地址为 192.168.2.2,需要设置 DTU 的通讯 IP 为同一个子网内的 IP,此时设置为 192.168.2.254。然后在 Modbus-TCP Server 参数设置列表中,添加 S7-1200 的从站号、IP 地址和通讯端口号 (MODBUS-TPC 标准为 502 端口号)



数据通讯口: 设置为与 PLC 通讯口类型, 可选 RS485、RS232 或 LAN 网口, 此处使用 LAN 网口进行 MODBUS-TCP 通讯;

本机 IP: DTU 作为 MODBUS-TCP 通讯的客户端的 IP 地址, 此 IP 必须要在通讯局域网的子网段内, 且不与子网内的其他设备 IP 重复, 直连 S7-1200 的话, 直接设置为与 PLC 同一个子网段即可, 本案例设置为 192.168.2.254;

Modbus-TCP Server 参数:

从站号: 为 PLC 的从站号, 此从站号不与其他参与通讯的 PLC 重复即可, 本案例设置为 1;

IP 地址: PLC 作为 MODBUS-TCP 服务器的 IP 地址, 本案例为 192.168.2.2;

端口号: PLC 通讯端口, MODBUS-TPC 协议标准端口为 502, 本案例也是用 502 端口;

第三步, 进行【Modbus 配置】, 配置 DTU 定时读取 PLC 的数据发送到平台的各项参数。如下图:





实时数据定制采集列表中的参数说明:

设备从站号: DTU 连接的 PLC 的从站号, 与【通讯设置】中 PLC 的从站号一致。本案例为 1;

功能码: 为模块读取设备 MODBUS 寄存区的标志符。“功能码 01”对应“线圈”(0XXXX)，“功能码 02”对应“离散量输入”(1XXXX)，“功能码 03”对应“保持寄存器”(4XXXX)，“功能码 04”对应“输入寄存器”(3XXXX)。西门子 PLC 中, Q 点对应 01 功能码, I 点对应 02 功能码, MB_SERVER 的【MB_HOLD_REG】指向的区域对应 03 功能码(上文 PLC 程序指向的是 MW1000 到 MW1008), AI 区对应 04 功能码。

起始地址: 为模块所连设备的 MODBUS 寄存器读取的起始地址(不包含寄存区标识符)。图中第一个 MODBUS 指令地址 1 代表 00001, 第二个 MODBUS 指令地址 1 代表 10001, 第三个 MODBUS 指令地址 1 代表 40001。

数据长度: 为 DTU 读取设备数据的连续长度, 图中的长度为 8 和 10, 既连续读取从 00001 到 00008、10001 到 10008 以及 40001 到 40010。

标准 DTU 可连接多个从站(最多 4 个), 可点击“新建”创建 MODBUS 指令通道, 配置规则按上述说明。

结合上文 PLC 从站的建立, 这里实时监控的是 PLC 的 Q0.0 到 Q0.7、I0.0 到 I0.7 和 MW1000 到 MW1018。

注: 当 DTU 出现异常时, 如无法连接网络在线, 或者无法与 PLC 正常通讯, 此时可以使用配置口(默认 RS232)连接 PC, 使用“DTU 配置软件”来查看状态及异常报警, 详见《DTU 配置软件使用手册》。

3.2 新建数据规则

点击网页左侧的“数据规则”进入规则设置页面, 点击右上角的“新增”, 在弹出的窗口中设置该数据规则的名称“S7-1200”和展示样式“列表展示”, 我们可以选择列表展示或组态展示:

列表展示: 我们所添加的数据会以固定的列表样式展示, 列表展示方式简单方便(数据测试阶段可选用列表展示)。

组态展示: 我们可以任意绘制设备数据的展示样式比如添加图形、图片、仪表盘、柱状填充和文字等内容(此功能类似传统的组态软件可参考《EMCP 平台画面组态使用说明》文档)。数据规则新建完后点击“实时数据”新增实时数据(3.1.2 中设置的 Modbus 配置), 点击“读写数据”创建平台对设备手动读写操作的数据。创建规则展示如下。

注: 实时数据: 是 DTU 根据所配置的 Modbus 采集通道(参考上面的 3.1 介绍), 按设定的采集间隔定时读取从站数据并上传到平台所显示的内容;



读写数据：无需在 DTU 配置 Modbus 定时采集通道，可直接通过平台对下位设备进行数据的手动读写操作；

EMCP 平台所有"寄存器地址"设置均不需要带寄存器区标识符，如读写“保持寄存器”（03 功能码）中 40019 的数据，在平台数据规则中的"寄存器地址"填写 19 即可（注：如果设备 Modbus 地址计数是从 0 开始的，则需要做加 1 处理，即填写 20）。

数据规则详情

规则名称: 西门子公司57-1200

数据展示: 列表展示 组态展示

规则说明: 规则说明

实时数据: 普通账号显示 普通账号隐藏

数据读写: 普通账号显示 普通账号隐藏

历史数据: 普通账号显示 普通账号隐藏

报警记录: 普通账号显示 普通账号隐藏

消息推送: 推送管理账号 推送普通账号

通讯故障检测: 开启 关闭

通讯故障延迟(次): 3

操作: 设置 | 实时数据 | 读写数据 | 画面组态

+ 新增

实时数据列表

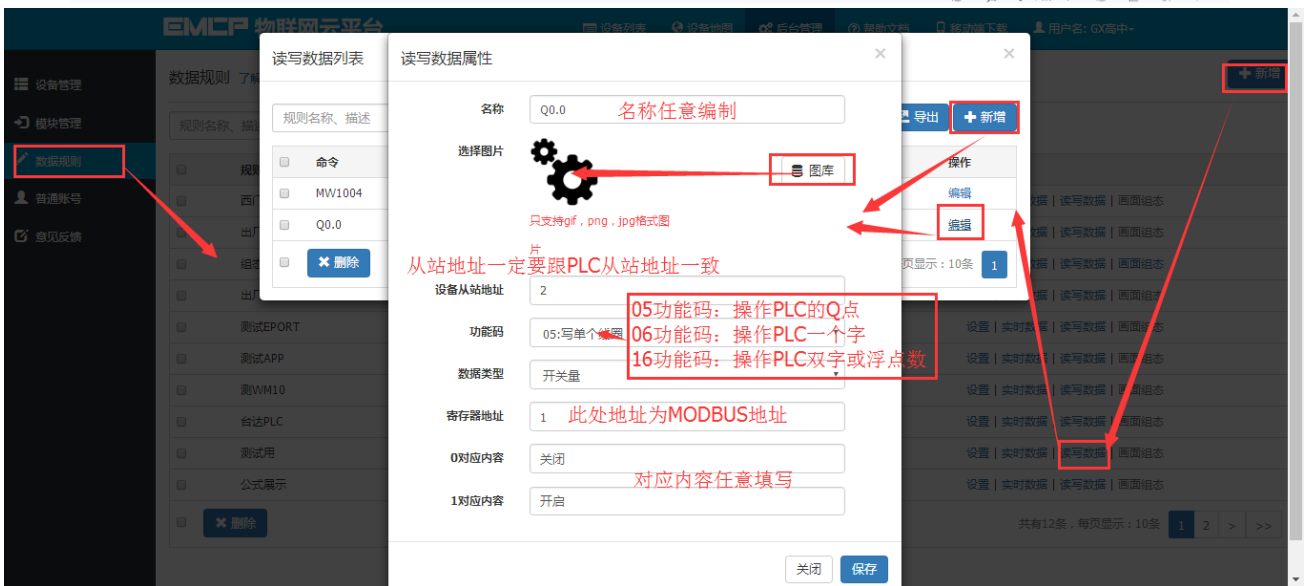
数据名称: [搜索]

操作: 上移 | 下移 | 导入 | 导出 | + 新增

名称	从站	功能码	寄存器地址	数据类型	解码顺序	单位	操作
MW1000	2	03:读保持寄存器	1	unshort	12		编辑 报警
MW1002	2	03:读保持寄存器	2	unshort	12		编辑 报警
I0.0	2	02:读离散量输入	1	bit	12		编辑 报警

共有3条, 每页显示: 10条 1

操作: 设置 | 实时数据 | 读写数据 | 画面组态



报警设置，在创建好的实时数据中，点击“报警”选项，进入报警设置页面。我们可以设定该数据的报警上下限和报警内容以及是否启用此报警。设定报警后当该数据超出报警上下限后平台会自动记录报警的时间和报警值，同时平台会向用户登录的 APP 或微信推送报警消息。



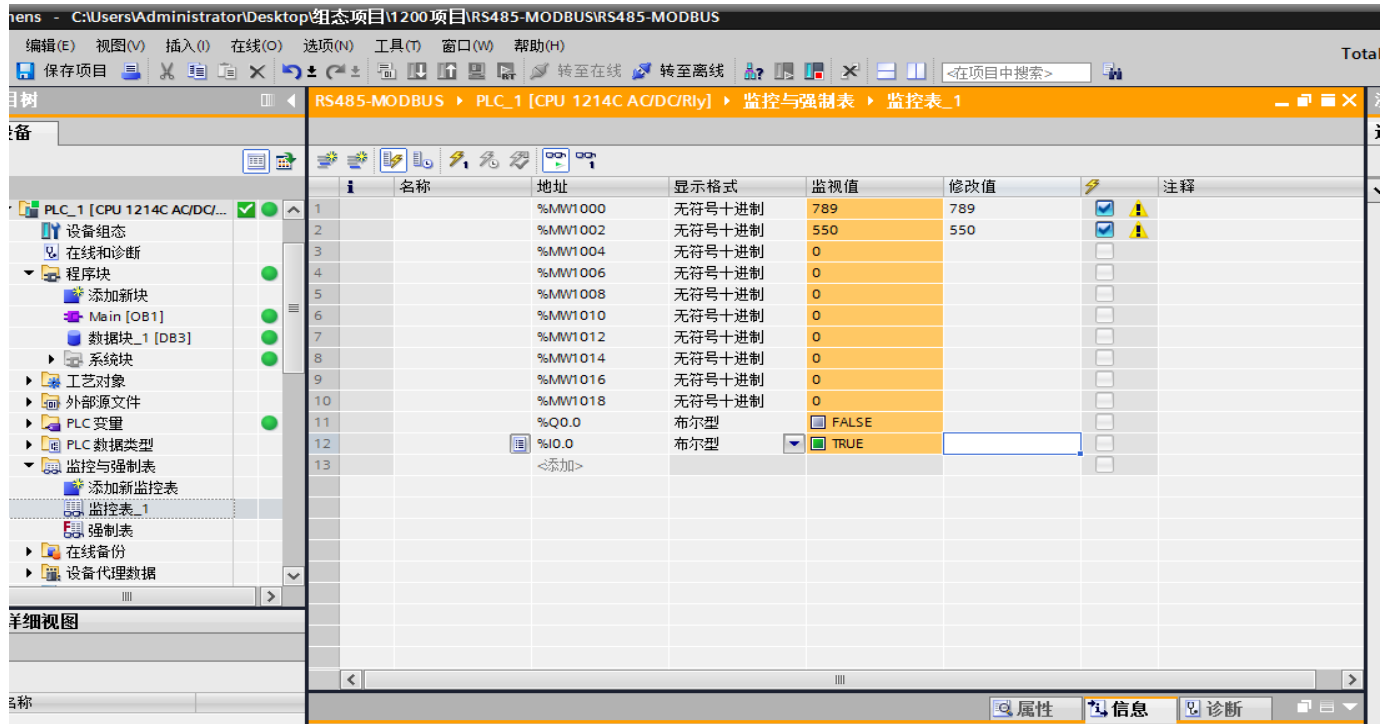
3.3 新建设备

- 1 新建“设备”，选择菜单“设备管理” -> “新增” 新建一个设备“西门子 S7-1200 ”。新建设备是填写设备的基本信息，1 选择设备匹配的图片（从本地上传，也可不选择，系统会以默认图片显示）；
- 2 输入模块 SN，输入要绑定的 SN 的编码，如果此 SN 之前未绑定，则会弹出绑定窗口进行绑定；
- 3 选择上面创建的数据规则；
- 4 点击“地图”按钮选择设备所在的地理位置。完成后点击“保存”。

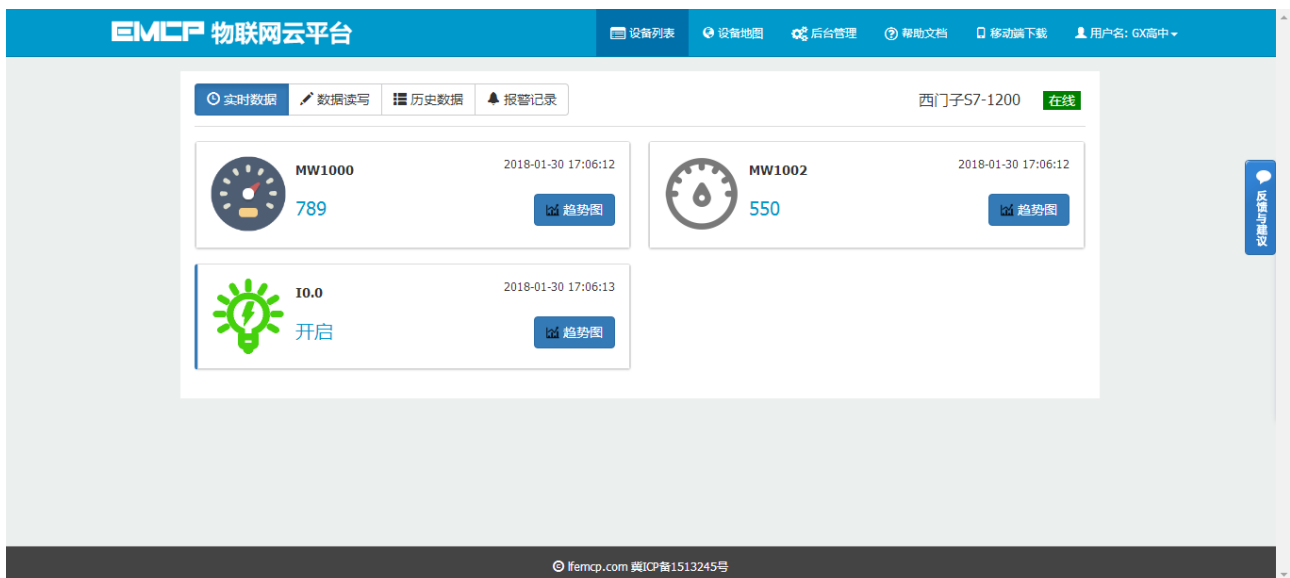


四，实验效果。

打开博图软件，将 PLC 转至在线，并且从监控表中监控当前 PLC 的数据，如下图：



用户登录 EMCP 平台 (www.lfemcp.com)，点击“西门子 S7-1200”设备的图片或设备名称进入设备。首先看到的是 PLC 定时采集数据的显示（实时数据），通过点击“读写数据”对台达 PLC 进行读写操作，点击“历史数据”查看设备定时存储数据的历史数据报表，点击“报警记录”进入报警信息记录报表页面，显示如下。





EMCP 物联网云平台

设备列表 设备地图 后台管理 帮助文档 移动端下载 用户名: GX高中

实时数据 数据读写 历史数据 报警记录 西门子S7-1200 在线 全部读取

MW1004

666 写入成功

读取 写入

Q0.0

开启 关闭 写入成功

读取 写入

反馈与建议

EMCP 物联网云平台

设备列表 设备地图 后台管理 帮助文档 移动端下载 用户名: GX高中

实时数据 数据读写 历史数据 报警记录 西门子S7-1200 在线 导出数据

开始时间 结束时间 搜索

采集时间	MW1000	MW1002	IO.0
2018-01-30 17:11:34	789	550	0
2018-01-30 17:11:02	789	550	0
2018-01-30 17:10:32	789	550	0
2018-01-30 17:10:01	789	550	0
2018-01-30 17:09:39	789	550	
2018-01-30 17:09:30			0
2018-01-30 17:09:09	789	550	0
2018-01-30 17:08:38	789	550	0
2018-01-30 17:08:07	789	550	0
2018-01-30 17:07:36	789	550	0

共有4436条, 每页显示: 10条 1 2 3 4 5 > >>

© femcp.com 冀ICP备1513245号

反馈与建议

EMCP 物联网云平台

设备列表 设备地图 后台管理 帮助文档 移动端下载 用户名: GX高中

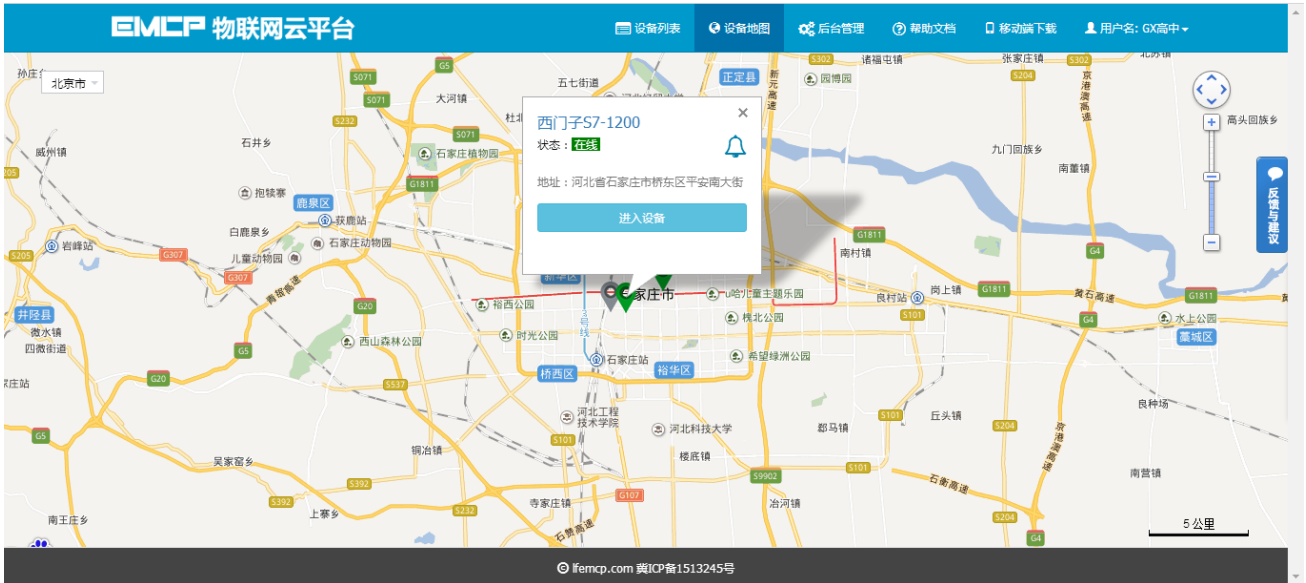
实时数据 数据读写 历史数据 报警记录 西门子S7-1200 在线

开始时间 结束时间 未解除的报警 搜索

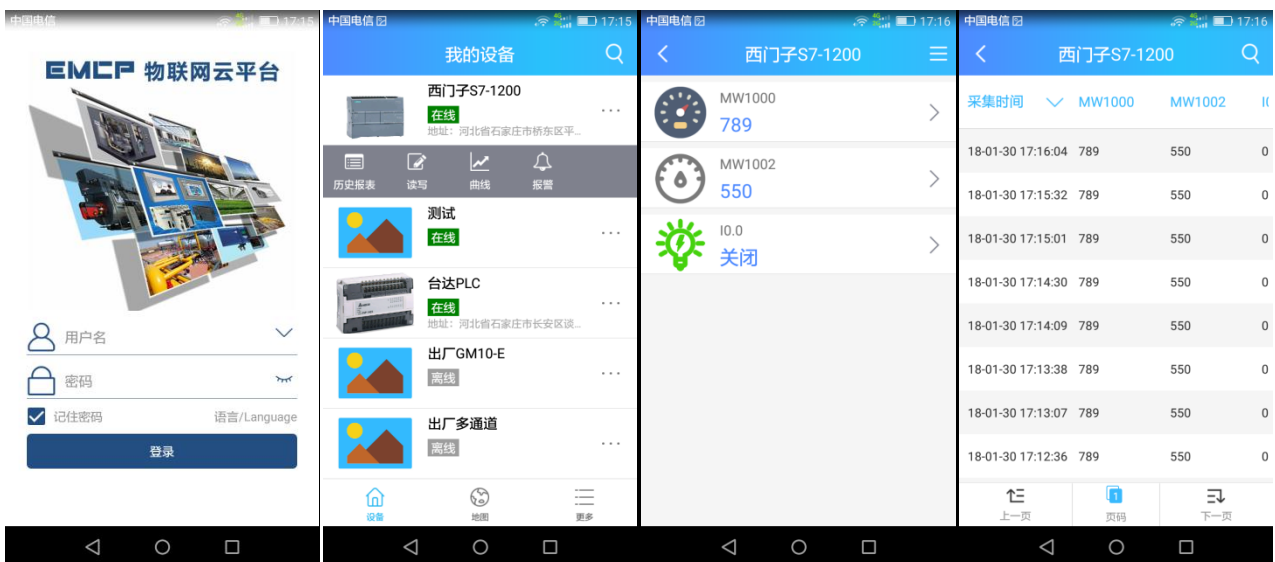
报警时间	报警解除时间	报警值	报警详情	操作
2018-01-30 15:24:41	2018-01-30 17:05:31	0	MW1002下限报警!!!	
2018-01-30 13:40:42	2018-01-30 13:43:51	11	从站2; 功能码:3; 从站设备读取超时	

共有2条, 每页显示: 10条 1

反馈与建议



在手机安装《云联物通》手机 APP(可通过电脑网页平台登录页右上角的二维码扫描下载，或各大应用商店下载)，凭用户名和密码登录，进入设备列表后点击“西门子 S7-1200”设备，直接进入的是实时数据列表页面或组态画面（组态展示方式下），点击右上角菜单栏“三杠按钮”，弹出功能菜单，在菜单中点击“读写数据”对读写数据进行读写操作，点击“历史报表”查看设备的历史存储数据报表，点击“历史曲线”可查看各数据的历史趋势图，点击“报警信息”查看该设备的报警记录，点击“设备详情”查看设备的详细信息或视频画面。





五，辅助功能介绍

5.1 画面组态功能。

通过“后台设置->数据规则->设置->组态展示”这几个步骤来选择使用组态展示形式来展示对应数据规则。选择为组态展示后，规则的画面组态选项变为可用，点击“画面组态”选项，进入编辑页面。通过组态编辑页面我们可以任意绘制图片、文字、数显框、按钮、指示灯、管道、设备等等空间，详细功能请参考《EMCP 平台画面组态使用说明》<http://www.lanfengkeji.com/h-col-135.html>。



5.2 微信功能。

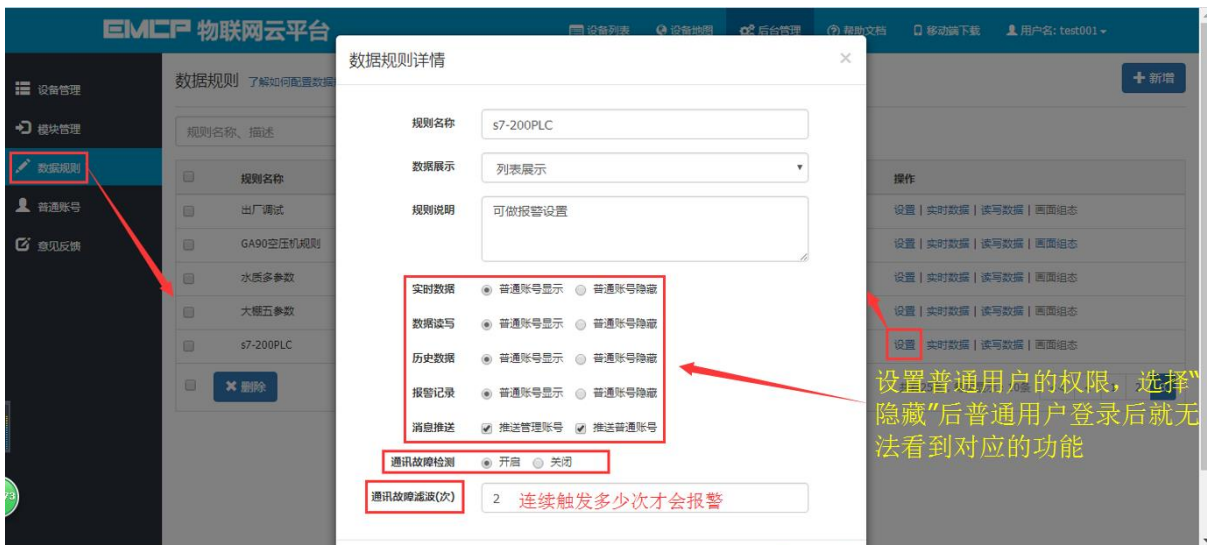


微信关注“EMCP 物联网云平台”公众号，按照提示绑定平台账号，即可使用微信监控设备，接收报警信息。为了便于对设备的管理建议将“EMCP 物联网云平台”公众号“置顶”。



5.3 数据规则中开启通讯报警和授权普通用户功能。

通讯报警功能就是当 DTU 与 PLC 通讯异常时，在相应设备中会进行报警，根据通讯异常的原因在报警内容中进行注释，方便调试。设置及效果如下：



2017-09-08 15:25:23	2017-09-08 15:26:54	10	从站:3; 功能码:3; 从站设备读取返回乱码
2017-09-08 15:25:20	2017-09-08 15:26:53	11	从站:2; 功能码:2; 从站设备读取超时
2017-09-08 15:25:14	2017-09-08 15:26:52	11	从站:1; 功能码:1; 从站设备读取超时
2017-09-08 15:21:36	2017-09-08 15:21:52	10	从站:4; 功能码:4; 从站设备读取返回乱码

5.4 设备公开功能。

在设备管理中，可以将设备的属性设置为公开，公开后会生成设备所属的 url 连接和二维码，通过该连接和二维码可实现免登陆打开设备，同样也可将设备分享到社交圈。



5.5 新增普通账号及设备授权。

管理员账号创建完设备后，可以通过“普通账号”选项为用户创建一个单独的账号供其访问所属的设备。此功能主要为用户开通一个专属的账号，用户查看自己所属的设备。



5.6 视频监控功能。

EMCP 平台可实现萤石云摄像头的接入，从而实现 web、APP、微信等终端对现场视频监控功能。详情请浏览《EMCP 物联网云平台视频使用说明 V3.3》

5.7 风格定制/系统定制服务。

对于大中型企业，我们还为用户提供平台和软件定制服务，介绍如下；

风格定制服务：风格定制是在原有 EMCP 平台基础上实现用户个性化风格的显示，整个服务依旧运行在原 EMCP 平台服务器上的，布局、功能和架构等基础内容不做改变。风格定



制内容主要体现在电脑网页、手机网页、安卓 APP、微信公众平台的登录域名、登录页、平台名称、平台图标等。适合企业品牌建设。

私有云部署服务：为将 EMCP 系统部署到用户的服务器上，除了显示风格的定制，还可以更改系统的功能的增加、布局显示的改变以及数据分析等服务。

如有需求可联系蓝蜂销售人员。

六，故障分析。

6.1 设备离线的原因

1. SN 码和密码绑定错误，EMCP 平台所建设备的 SN 码必须和所连 GM20 模块的 SN 码相同（SN 位于 GM20 侧面标签），密码必须和 DTU 配置软件设置的密码相同（默认 111111）。

2. 网络信号差，DTU 在信号强度低于 50 或误码率高于 3 时会出现掉线或无法联网的情况，最好保证信号强度在 70 以上误码率为 0（可通过改变天线的安放位置调整信号强度，信号强度可通过 DTU 配置软件或平台模块远程配置中获得。）

6.2 如平台无法读取 PLC 的数据的原因。

1. PLC 的 Modbus-TCP 服务器没有创建成功。此时我们可以通过 Modscan32 主站软件对 PLC 进行通讯测试，如果无法读取 PLC 的数据那么说明 PLC 的 Modbus-TCP 服务器没有创建成功。

2. 接线问题，请确认使用的网线接头接线定义正确无虚接。

3. 数据创建失败，检查数据规则中所创建的设备是否正确。

4, 如果显示“数据未采集”，请检查模块的“远程配置”是否设置了 Modbus 采集通道，参考 3.1.2 中的设置。

-----END-----

河北蓝蜂信息科技有限公司

技术支持：0311-68025711

QQ: 3226776165/2166638849

官方网站: www.lanfengkeji.com