应用案例

S7-200 Smart PLC 通过网口接入 EMCP 云平台

版本：V1.2

河北蓝蜂信息科技有限公司

2020-06-08

S7-200 Smart PLC 通过网口接入 EMCP 云平台 V1.2

前言：西门子 S7-200 SMART PLC（以下简称 200-SMART）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。200-SMART 具备网口进行程序的上下载和通讯，此次我们要使用 MODBUS-TCP 协议，通过网口把 200-SMART 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 200-SMART 内的 VW1000、VW1002、I0.0 寄存器的远程监控和 VW1004 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 S7-200 SMART PLC 一台，及通讯用网线。
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）。
5) 电工工具，通讯线材等。

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。

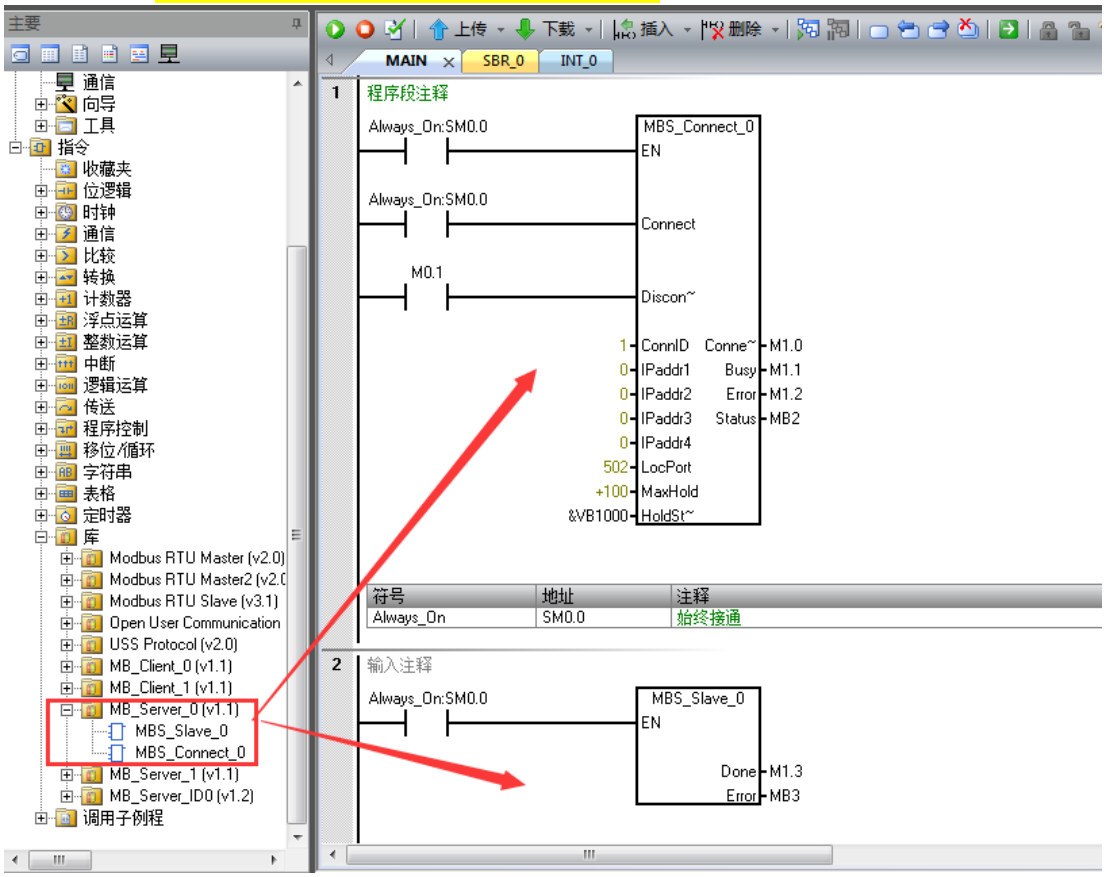
200 SMART 连接 220V 交流电，先使用电脑通过网线连接 PLC 的以太网通讯口进行程序的配置，然后使用网线连接 GM20 的 LAN 口和 PLC 的以太网口，进行 MODBUS-TCP 通讯。

二，PLC 的 MODBUS-TCP 通讯创建。

第一步，创建 PLC 的 MODBUS-TCP 服务器；

1.当使用西门子的《STEP 7-MicroWIN SMART V2.2 或 V2.3》编程软件：

在 PLC 程序中添加 MB_Server 指令库，MB_Server 指令库包含 MBS_Connect 和 MBS_Slave 等 2 个指令。如下图：（下图为一个能够正常通讯的指令块设置）



MBS_Connect 指令各个参数定义如下：

- EN 使能：必须保证每一扫描周期都被使能。
- Connect：启动 TCP 连接建立操作。
- Disconnect: 断开 TCP 连接操作。
- ConnID: TCP 连接标识。

  注意：Modbus TCP 属于 TCP 通信，也是开放式用户通信中的一种，所以 ConnID 参数不能与其他 TCP、ISO-on-TCP、UDP 通信相同。
- IPaddr1~IPaddr4: Modbus TCP 客户端的 IP 地址，IPaddr1 是 IP 地址的最高有效字节，IPaddr4 是 IP 地址的最低有效字节。建议设置为 0.0.0.0，这样任意一个客户端均可以访问。
- LocPort： 本地设备上端口号（必须设置为 502）

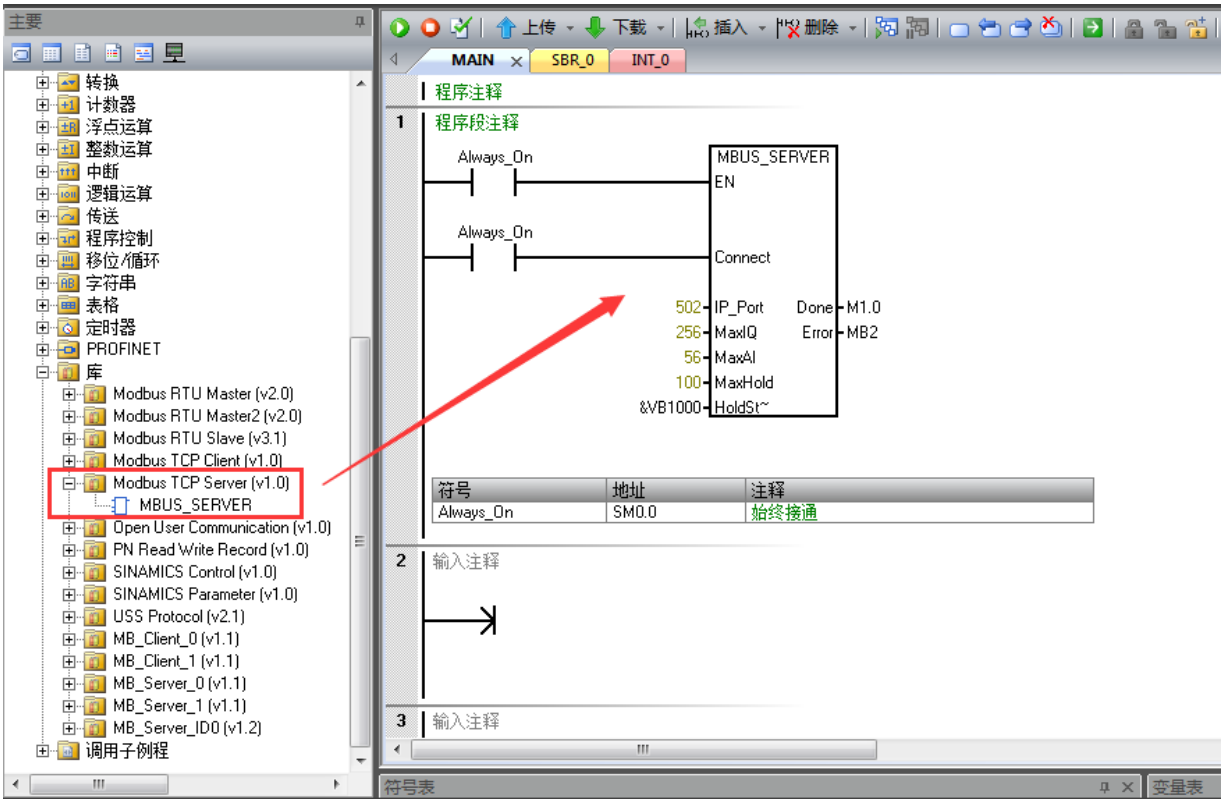
- MaxHold: 用于设置 Modbus 地址 4xxxx 或 4yyyyy 可访问的 V 存储器中的字保持寄存器数。此数值必须设置大于等于需要读取的所有数据的长度，例如，需要监控 100 个字的 V 区数据，此数据必须设置大于等于 100。
- HoldStart: 间接地址指针，指向 CPU 中 V 存储器中保持寄存器的起始地址。本例中 VW1000 即对于 Modbus 地址 40001 。（即 VW1000 对应 40001,VW1002 对应 40002）。(其他寄存器，如 I 寄存区可通过功能码 02，Q 寄存区可使用功能码 01，AI 寄存器可通过功能码 04 进行直接访问)。
- ConnectDone：Modbus TCP 连接已经成功建立。
- Busy: 连接操作正在进行时。
- Error: 建立或断开连接时，发生错误。
- Status：如果指令置位 “Error” 输出，Status 输出会显示错误代码。

MBS_Slave 指令各个参数定义如下：

- EN 使能：必须保证每一扫描周期都被使能。
- Done：当 MB_Server 指令响应 Modbus 请求时，Done 完成位在当前扫描周期被设置为 1 ； 如果未处理任何请求，Done 完成位为 0 。
- Error： 错误代码，只有在 Done 位为 1 时错误代码有效。

2.当使用西门子的《STEP 7-MicroWIN SMART V2.4》编程软件：

在 PLC 程序中添加 MBUS_SERVER 指令。如下图：（下图为一个能够正常通讯的指令块设置）



MBUS_SERVER 指令各个参数定义如下：

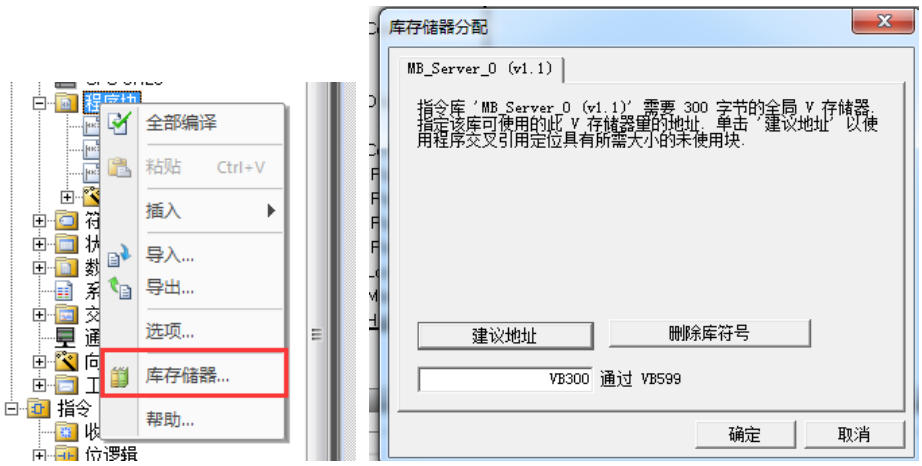
- EN 使能：必须保证每一扫描周期都被使能。
- Connect：如果 Connect=TRUE，且客户端尚未与服务器建立连接，则服务器将被动监听 TCP 连接请求。如果 Connect=FALSE 且存在连接，则服务器将发起断开连接操作。
- IP_Port：客户端将尝试连接、且使用 Modbus 应用协议进行通信的服务器的端口号（必须设置为 502）。
- MaxIQ：可用于 Modbus 地址 0xxxx 到 1xxxx 的 I 和 Q 点数设置为 0 至 256。值 0 表示禁用对输入和输出的所有读取和写入。建议将 MaxIQ 值设置为 256。
- MaxAI：可用于 Modbus 地址 3xxxx 的字输入 (AI) 数设置为 0 至 56。值 0 表示禁用对模拟量输入的读取。要允许访问所有 CP 模拟量输入，MaxAI 的建议值如下： 对于 CPU CR40 和 CR60，为 0；对于所有其它 CPU 型号，为 56。
- MaxHold:可用于设置 Modbus 地址 4xxxx 或 4yyyyy 的 V 存储器中的字保持寄存器数。此数值必须设置大于等于需要读取的所有数据的长度，例如，需要监控 100 个字的 V 区数据，此数据必须设置大于等于 100。
- HoldStart: 间接地址指针，指向 CPU 中 V 存储器中保持寄存器的起始地址。本例中 VW1000 即对于 Modbus 地址 40001 。（即 VW1000 对应 40001,VW1002 对应 40002）。(其他寄

存器，如 I 寄存区可通过功能码 02，Q 寄存区可使用功能码 01，AI 寄存器可通过功能码 04 进行直接访问)。

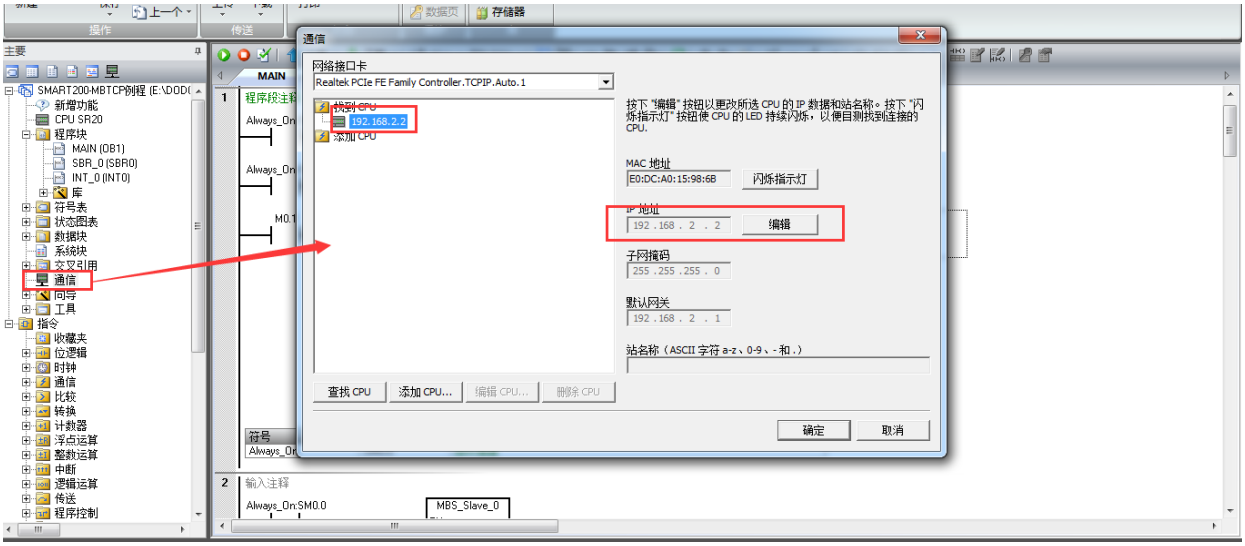
- Done：当 TRUE 时，MBUS_SERVER 执行下列操作之一：连接至客户端设备；与客户端断开连接；响应 Modbus 请求；返回错误。当 FALSE 时，没有请求用于此程序周期。
- Error: 指令执行结果。仅在发生错误后的一个周期内有效。

第二步，分配库地址区

在编程软件右侧，在【程序块】功能点击鼠标右键，调用【库存储区】功能，使用【建议地址】，保证库存储区与程序中数据存放区没有重叠即可，点击【确定】，完成整个 MODBUS-TCP 服务器配置。如下图：



第三步，将修改好的程序下载到 PLC 中，下载时请记录 PLC 的 IP 地址。 本文案例，PLC 的 IP 地址为 192.168.2.2。



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 200 SMART 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 200 SMART 的话，直接设置为与 200 SMART 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 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，MBS_Connect 的 HoldSt`指向的区域对应 03 功能码（上文 PLC 程序指向的是 VW1000 到 VW1198），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 VW1000 到 VW1018。

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“S7-200 SMART”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）。

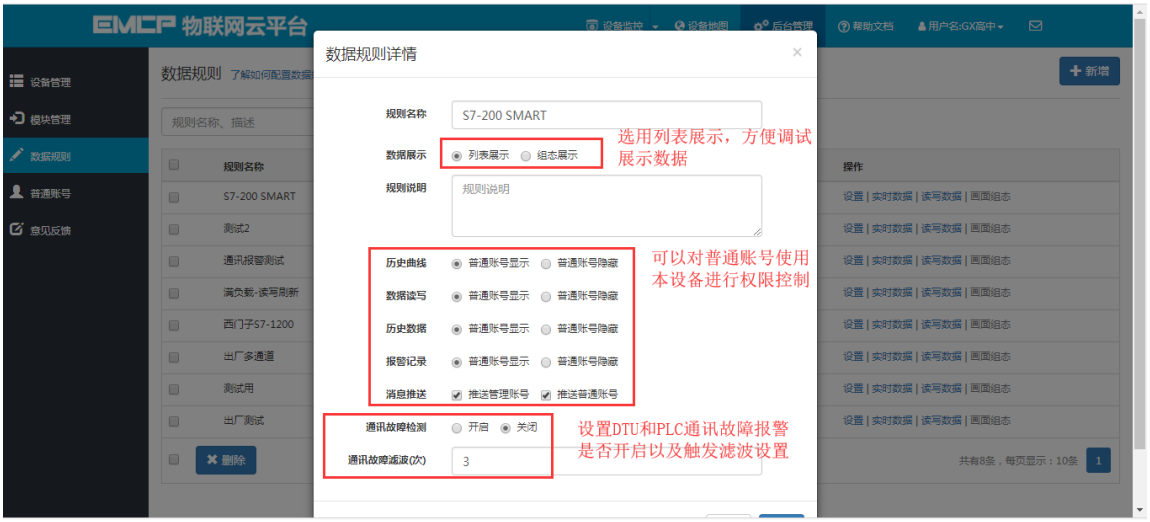
组态展示：我们可以任意绘制设备数据的展示样式比如添加图形、图片、仪表盘、柱状填充和文字等内容（此功能类似传统的组态软件可参考《EMCP 平台画面组态使用说明》文档）。

数据规则新建完后点击【实时数据】新增实时数据解析规则（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规则。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）。

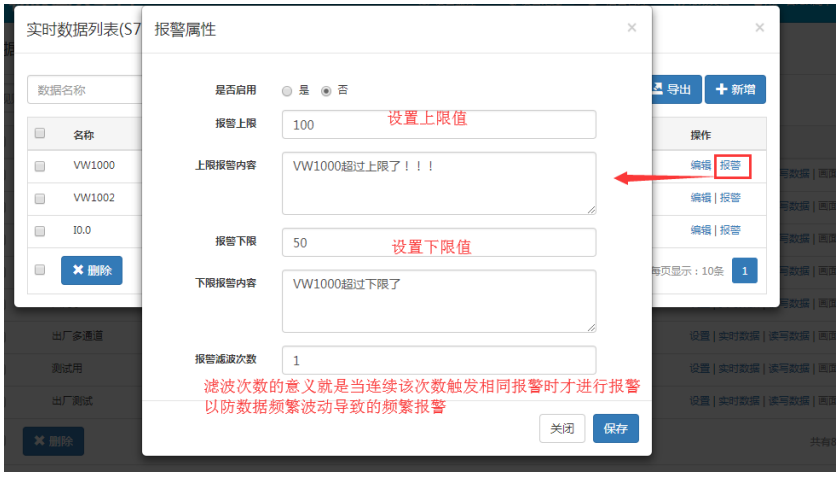



实时数据列表(S7-200 SMART)
数据名称
搜索
上移
下移
导入
导出
新增
名称
从站
功能码
寄存器地址
数据类型
解码顺序
单位
操作
VW1000
VW1002
I0.0
删除
共有3条，每页显示：10条
实时数据


数据名称
VW1000
名称任意编辑
选择图片
选择图标
图库
只支持gif，png，jpg
格式图片
设备从站地址
1
从站地址与MODBUS配置一致
功能码
03:读保持寄存器
01功能码对应Q点
02功能码对应I点
03功能码对应V区
04功能码对应A区
该数据的MODBUS地址
寄存器地址
数据类型
16位整型(无符号)
根据实际数据类型选择
解码顺序
单位
默认即可
小数位数
3
换算系数
1
了解如何使用数据处理公式？
数据处理公式
显示值和实际传输值之间的对应公式，如：(X-4)
状态列表
状态映射列表
可以对特定数据展示为特定文字
历史记录是否展示
是
否
此数据是否记录在历史记录表中


读写数据列表(S7
读写数据属性
名称
Q0.0
名称任意编辑
选择图片
ON
图标从图库选择或上传
图库
只支持gif，png，jpg格式图片
设备从站地址
1
从站地址与【通讯配置】里面的PLC从站号一致
功能码
05:写单个线圈
05功能码：操作Q点；
06功能码：操作V区一个字；
16功能码：操作V区双字
数据类型
开关量
寄存器地址
1
此地址为数据的MODBUS地址
0对应内容
关闭
对应文字可以任意编辑
1对应内容
开启
规则名称、描述
VW1004
Q0.0
删除
新增
导出
操作
编辑

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

在后台管理中，选择【设备管理】-> 【新增】新建一个设备“S7-200 SMART ”。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;

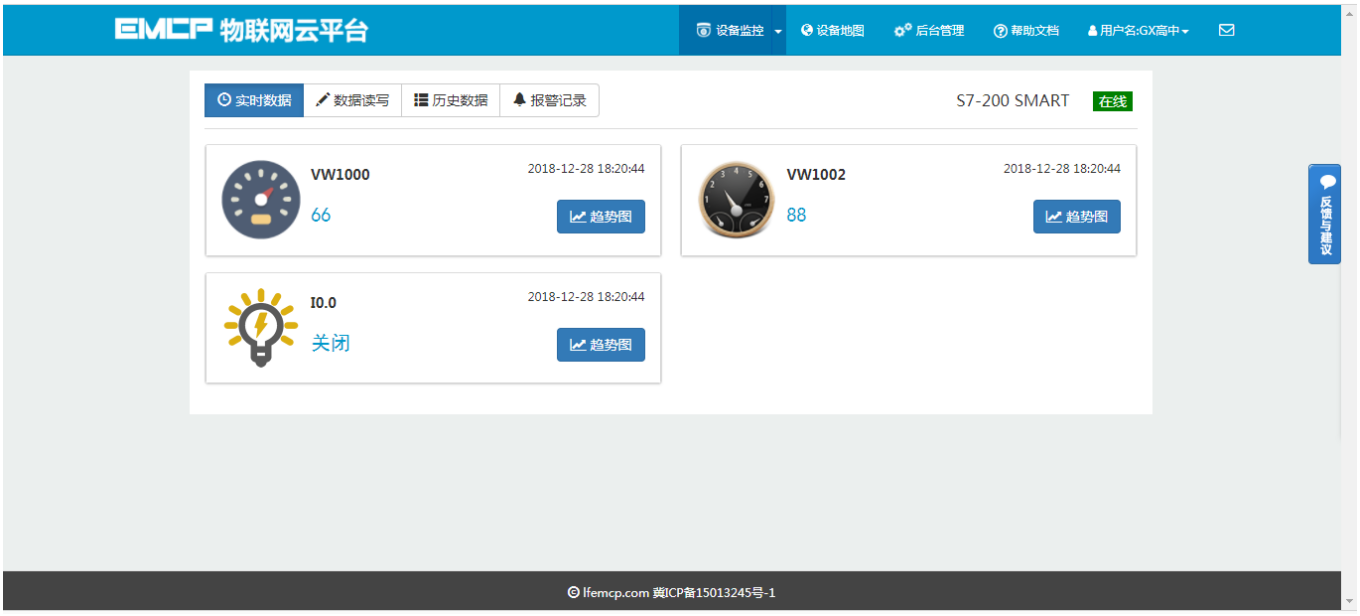
3 选择上面创建的数据规则;

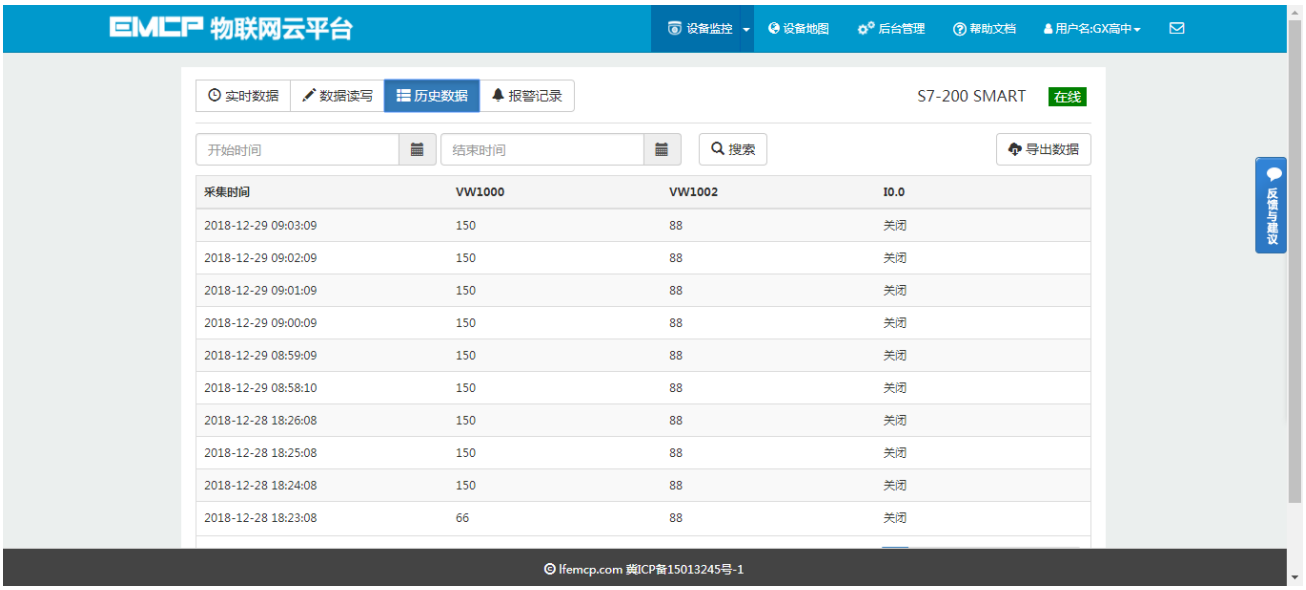
4 点击“地图”按钮选择设备所在的地理位置。完成后点击【保存】。

四，实验效果。

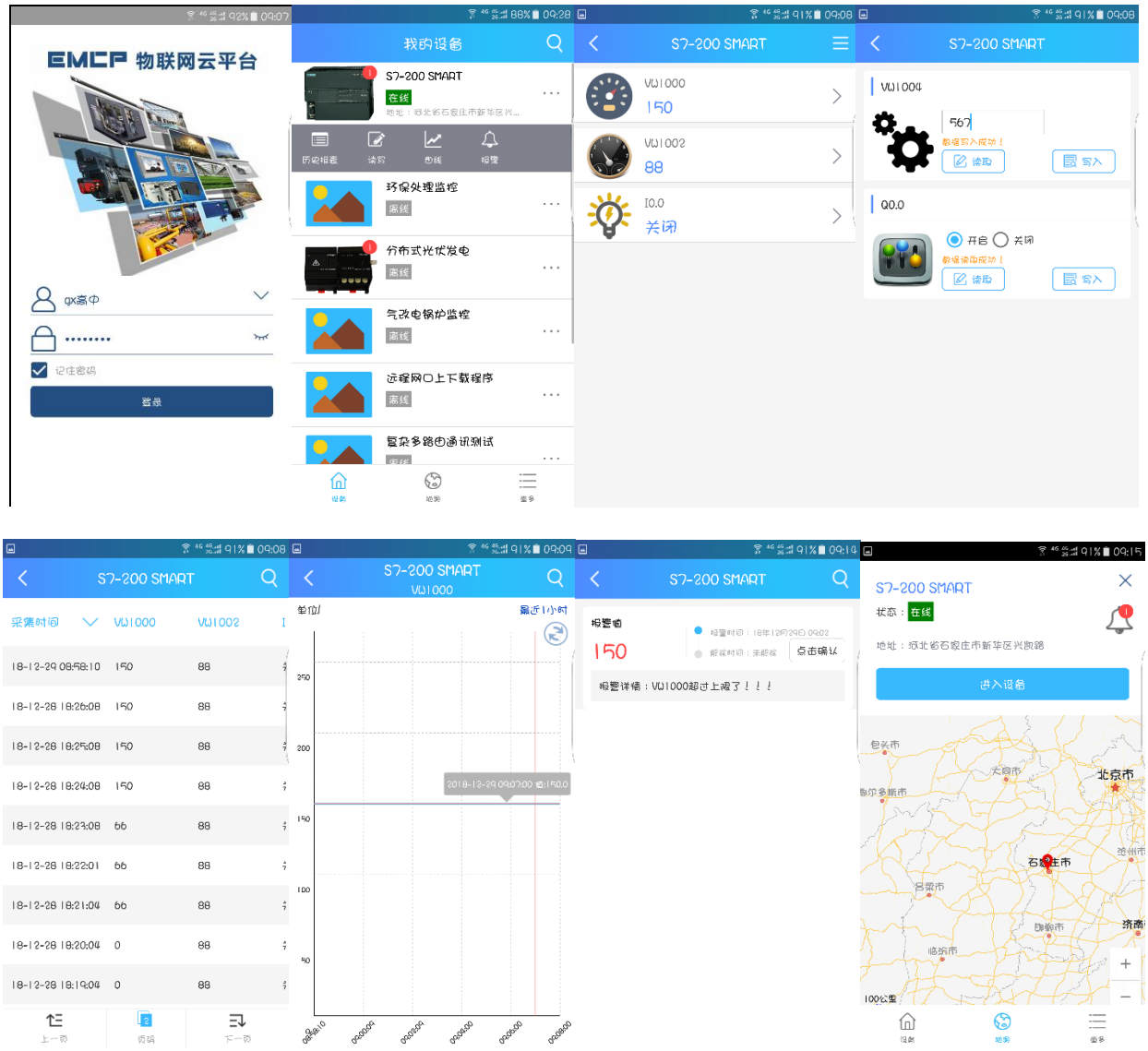
打开 PLC 编程软件，将 PLC 转至在线，并且从监控表中监控当前 PLC 的数据，如下图：

用户登录 EMCP 平台（www.lfemcp.com），点击“S7-200 SMART ”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 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。





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“S7-200 SMART”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。



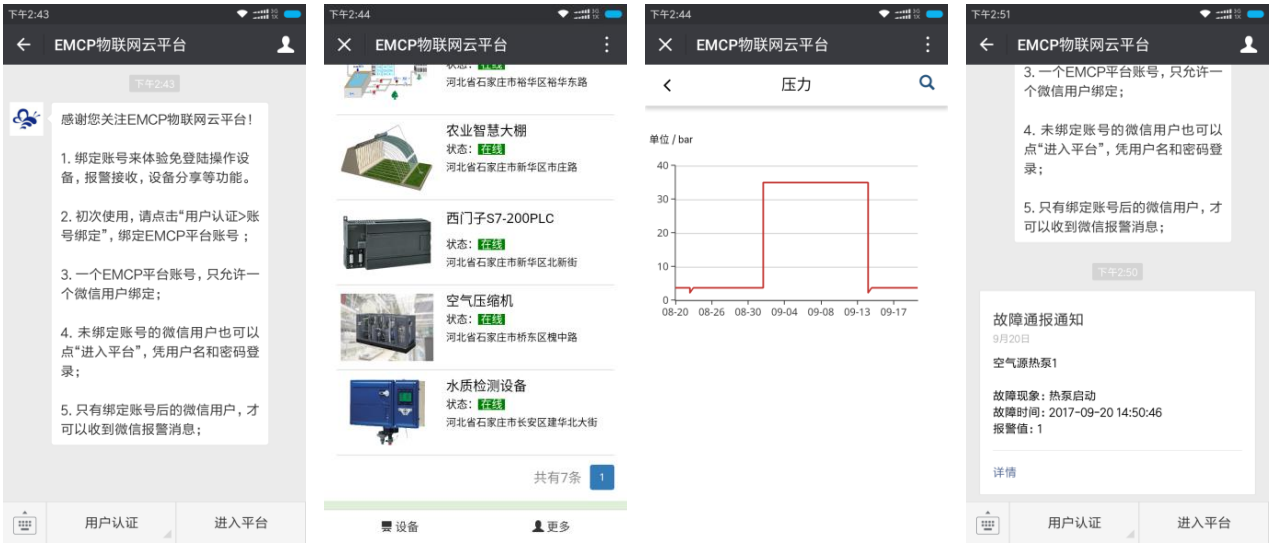
五，辅助功能介绍

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】”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 V3.6》

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 GM10 模块的 SN 码相同（SN 位于 GM10 右侧面标签），密码必须和 DTU 配置软件设置的密码相同（默认 111111）。

2．SIM 卡选择不对，必须选择移动或联通的 SIM（部分联通卡不兼容，建议选用移动卡）。

3．SIM 欠费。

4．网络信号差，DTU 在信号强度低于 15 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 20 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