MODBUS 手持式调试器



EMH-301 用户使用手册 大连优为自动化技术有限公司

- 自动侦测Modbus主站通讯配置,并捕捉主站发布的命令
- 自动获取所有Modbus在网从站的信息
- 全面代替Modscan32/Modsim32功能

技术服务电话: 0411-88700019 技术支持邮箱: service@uway.tech



I.	EMH-301 自动获取 Modbus 主站相关信息	. 2
II.	EMH-301 自动获取 Modbus 从站相关信息	. 5
III.	EMH-301 作为一个 Modbus 主站	. 8
IV.	EMH-301 作为一个 Modbus 从站	11
V.	附图	13

EMH-301 自动获取 Modbus 主站相关信息



①EMH-301 的操作过程:

1. 按<电源>键,开机进入"主菜单"界面(见下图)



2. 在"主菜单"界面下,按<自动搜索>键,进入"自动搜索"界面,见下图



3. 在"自动搜索"界面下,按<上下箭头>键,移动焦点至"网络监测"条目,然后按<确定>键,进入"网络监测"界面,见下图



- 4. 在"网络监测"界面下,用户可设置"超时"和"延时"两个参数,这两个参数决定了EMH-301用不同通讯参数 配置,侦听网络上的主站命令时的"放弃时间",(放弃时间=超时+延时,默认放弃时间为1秒),"放弃时间=1 秒"意味着EMH-301以某种通讯配置在Modbus网上侦听主站命令,若在这1秒期间,EMH-301仍未捕捉到主站命令, 则放弃该通讯配置,转而尝试其他通讯配置继续侦听。按<上下箭头>键,移动焦点至这两个参数,按<确定>键 进入设置参数界面,设置好后按<确定>键,确认设置,并返回"网络监测"界面
- 5. 在"网络监测"界面下,按<上下箭头>键,移动焦点至"开始"项,然后按<确定>键,EMH-301进入"侦听主站 工作状态",见下图。此时,界面右上区域的三角图形表明,EMH-301正处于"侦听主站工作状态"。界面中, 波特率和校验下方对应数字会连续变化,这表明EMH-301正在变换各种通讯配置,尝试捕捉网络上的主站命令。 界面中右区域的"■■■"表明,以当前的通讯参数尚未联系到该网络的Modbus主站。



6. 在"侦听主站工作状态下",按<确定>键,EMH-301进入"暂停工作状态",见下图。此时,界面右上区域的双 竖线图形表明,EMH-301正处于"暂停工作状态"。"暂停工作状态"下,再次按下<确定>键,EMH-301则会重 新进入"侦听主站工作状态"



7. "侦听主站工作状态"下的EMH-301,开始遍历通讯配置去侦听网络上主站发布的命令,一旦侦测到,会在当前 通讯配置的右侧区域,出现打勾符号,见下图。以该图为例,<19200 0 √>表明,EMH-301以"19200波特率", "无校验"的通讯配置,成功捕捉到了主站命令。(备注:校验数字0代表"无校验",校验数字1代表"奇校验",校验数字2代表"偶校验")



8. EMH-301成功侦测到主站命令后,按<确定>键,EMH-301会进入"主站命令显示工作状态",见下图。此时,界面右上区域的三角图形表明,EMH-301正处于"主站命令显示工作状态"。"主站命令显示状态"下的EMH-301,按下<确定>键进入暂停显示状态,再次按下<确定>键,EMH-301恢复"主站命令显示工作状态"。该图中,<0014000140099 R>代表,侦测到的主站命令为:主站发布命令,读取,地址1的从站设备的寄存器40001到40999的值;<0014000140099 W>则代表,侦测到的主站命令为:主站发布命令,写值到,地址1的从站设备的寄存器40001到40099中。EMH-301每捕捉到一条新的主站命令,就把该命令显示在屏幕最上端,此前捕捉到的主站命令逐行下移,直至移出屏幕。

地址	一一寄存		jjp-	
001	40001	400)99	R
001	40001	400	<u> 999</u>	W
QQl	40001	4QÇ	jãð.	R
ŬŬ1	40001	4UU	ĩÃÃ.	Ľ.
UUL	40001	400	JAA	К

- "主站命令显示工作状态"下的EMH-301,按下<确定>键进入"暂停显示状态"。"暂停显示状态"下的EMH-301,按<上下箭头>键,可翻屏查看其捕捉的主站命令。"暂停显示状态"下的EMH-301,按下<返回>键,返回 上一级菜单。
- 10. "侦听主站工作状态"下的EMH-301,在尚未侦测到主站之前,按下<确定>键,进入"暂停侦听状态",然后按下<返回>键,返回上一级菜单

EMH-301 自动获取 Modbus 从站相关信息



①EMH-301 的操作过程:

1. 按<电源键>开机进入"主菜单",见下图



2. 按<自动搜索>键,进入"自动搜索"界面,见下图



- 4. 在"主站模式"界面下,用户可选择"通讯参数(固定)"或"通讯参数(优先)"这两种方式。EMH-301默认显示"通讯参数(固定)"条目。通过按<上下箭头>键移动焦点至该条目,并按<设置>键,切换优先/固定这两种方式。"通讯参数(固定)"决定了EMH-301只以当前固定的通讯配置,搜索网络上的从站;"通讯参数(优先)"决定了EMH-301会优先尝试当前的通讯配置,然后再遍历其他所有通讯配置,搜索网络上的从站



- 6. 在"主站模式"模式下,用户可选择"数据地址(快速)"或"数据地址(标准)"这两种方式。EMH-301默认显示"数据地址(快速)"条目。通过按<上下箭头>键移动焦点至该条目,并按<设置>键切换快速/标准这两种方式。"数据地址(固定)"决定了EMH-301在探寻某从站时,按当前数据地址配置,逐一尝试读取该从站的数据地址,若有其中任何一个数据地址被成功读取,则说明该从站存在。这也说明了,该从站具有当前设置中的某一数据地址;"数据地址(快速)"决定了EMH-301在探测某从站时,不考虑该从站的数据地址,只要该从站有响应,则说明该从站存在。
- 7. 当用户选择"数据地址(固定)"时,按<确定>键,进入配置界面,见下图。用户可以在该界面做相应的设置。 以该界面为例,该界面的设置决定了,EMH-301在探测某从站时,会读取线圈00001的值,若未成功,则读取线圈 00002,直至线圈00150;若在该过程中,有任何一次读取成功,则EMH-301判断该从站存在,并显示该从站存在 的信息在其屏幕上,然后停止该从站剩余地址数据的读取,转而探测下一个从站设备;当用户选择"数据地址 (快速)"条目,按<确定>键,可进入配置界面,见下图。在"数据地址(快速)"条件下的该配置界面,配 置信息不起作用。



8. 在"主站模式"界面下,按<上下箭头>键,移动焦点至"开始"条目,然后按<确定>键,EMH-301则进入"探测从站工作状态",见下图。此时,界面右上区域的三角图形表明,EMH-301正处于"探测从站工作状态"。"探测从站工作状态"下的EMH-301,按下<确定>键进入"暂停工作状态",再次按下<确定>键,EMH-301恢复"探测从站工作状态"。下图界面表明,正在探测的网络上,已探测出存在的从站设备有3个,地址分别为1,2,3。地址为4的从站设备在遍历各种通讯配置,以及数据地址配置之后,仍未探测到它的存在,因此判断该从站不存在。地址为5的从站设备正在探测中,尚无结果。



9. "暂停工作状态"下的EMH-301,按下<返回键>返回上一级菜单

EMH-301 作为一个 Modbus 主站



EMH-301 的操作过程:

1. 按<电源键>开机进入"主菜单",见下图



2. 按<上下箭头>键选择"主站模式",按<确定>键进入"主站模式"界面,见下图



3. 在"主站模式"界面下,按<上下箭头键>选择"通讯参数设置"条目,按<确定键>进入配置界面,见下图。客户可在此界面配置EMH-301以何种通讯配置,发布主站命令。以下图为例,作为主站的EMH-301,其会向从站地址为1的设备发布主站命令;以19200的波特率,无校验的方式发布主站命令;其slave response time 时间为500ms;其 Delay between polls时间为500毫秒。设置完成后,按<确定>键确认设置。然后按<返回键>返回"主站模式"界面

*1.	从站地址: 001 🔳
2.	波特率: 19200
3.	奇偶校验: 无校验
4.	超时(ms):00500
5.	延时(ms):00500

4. 在"主站模式"界面下,按<上下箭头键>选择"数据地址设置"条目,按<确定>键进入"数据地址设置"界面,见下图。客户可在此界面配置EMH-301发布主站命令时,要访问从站的线圈/寄存器。以下图为例,作为主站的EMH-301,其要读取某从站的4型寄存器,以1为起始,长度为15个。即,EMH-301要读取某从站40001^{~40015}寄存器的值。该设置完成后,按<确定>确认设置并返回,然后按<返回键>返回"主站模式"界面



5. "主站模式"界面下,按<上下箭头>键,移动焦点至"开始"条目,按<确定>键,EMH-301进入"主站工作状态",见下图。以该界面为例,工作状态下的EMH-301,以用户设置好的通讯配置以及数据地址配置,读取上来某从站寄存器的值并显示在它的屏幕上。用户可按<上下箭头>键,翻屏。

起始:000	1 十进制	
40001:	13107	
40002:	00012	
40003:	00000	
40004:	16403	
40005:	12300	

6. 工作状态下的EMH-301, 若在某一时刻, 其未获得从站响应,则它的屏幕右上区域, 会呈现一个"叉"符号,见下 图。以此图为例, "叉号"说明EMH-301未成功读取从站寄存器的值,界面上寄存器的值是以前时刻通讯正常时, 读上来的值。一旦通讯失败,这些值会被保持。



7. 工作状态下的EMH-301,焦点放置在寄存器上,比如40001,见下图左。按<设置>键,进入数据修改界面,见下 图右。修改数据后,按<确定键>返回工作界面。该操作使得EMH-301把某从站40001寄存器的值修改成23





8. 工作状态下的EMH-301,焦点放置在"进制显示"上,见下图左。按<设置键>,EMH-301可在各种数值的进制显示间切换,见下图右。

起始:0001 - 进制	■ 起始:0001 影 2000 ■
	40001: 65.0999984
40002: 00012 40003: 00000	40003: 2.29999995
$ \begin{array}{cccccccccccccccccccccccccccccccccccc$	40005: 0.00000000

10. 工作状态下的 EMH-301, 按<返回>键, 返回上一级菜单。

EMH-301 作为一个 Modbus 从站



EMH-301 的操作过程:

1. 按<电源键>开机进入"主菜单",见下图



2. 按<上下箭头键>选择"从站模式",按<确定键>进入"从站模式",见下图



 按<上下箭头>键选择"从站参数设置"条目,按<确定>键进入"从站参数配置"界面。客户可在该界面配置EMH-301作为一个modbus从站设备时的相关参数。见下图。例如,按该界面的相关配置,EMH-301作为modbus从站时的 地址为1;按19200波特率接收主站发来的命令并返回响应;按无校验方式通讯。该界面设置完成后,按<确定>键, 确认当前配置并返回上一级菜单。



- 4. EMH-301作为Modbus从站时,无需设置其数据地址等相关参数。EMH-301默认提供全范围数据地址,且每个数据 地址对应有默认的数值。这些数据地址是,00001~09999;10001~19999;30001~39999;40001~49999;每个数据 地址都对应有默认的数值。
- 按 <上下箭头>键,移动焦点至"开始"项,然后按<确定>键,EMH-301进入"从站工作状态"。工作状态下的EMH-301,每获得modbus主站发来的1条请求,把"接到主站请求"条目对应的数字自加1;EMH-301每返回一条响应, 把"发出从站响应"条目对应的数字自加1。见下图。



6. "从站工作状态"下的EMH-301,其具有的默认数据地址范围为00001~09999; 10001~19999; 30001~39999;
40001~49999;每个数据地址都有对应的默认数值。用户可以在此基础上,修改这些默认数值。在"从站工作状态"下的EMH-301,按<设置>键,进人"从站数据修改"界面,见下图。按<上下箭头>键,移动焦点到相应位置,
键入要修改的数值。然后按<确定>键确认修改。修改即时生效。



7. "从站工作状态"下的EMH-301,按<返回>键,返回上一级菜单。

