IEC-104 规约报文

实例分析

版本：V1.00

日期：2016-09-03

目　录

1. 概述 ..... - 1 -
2. 引用标准 ..... - 1 -
3. 信息体基地址范围 ..... - 1 -
4. 报文字节数的设置 ..... - 1 -
5. 类型标示符 ..... - 2 -
6. 传送原因 ..... - 3 -
7. 端口号 ..... - 3 -
8. 报文实例 ..... - 4 -
8.1. 建立网络连接或启动链路 ..... - 4 -
8.2. 停止链路 ..... - 4 -
8.3. U 帧测试帧 ..... - 4 -
8.4. S 帧测试帧 ..... - 4 -
8.5. 总召唤 ..... - 4 -
8.6. 对时 ..... - 5 -
8.7. 全遥测 ..... - 5 -
8.8. 全遥信 ..... - 5 -
8.9. 变化遥信 ..... - 6 -
8.10. SOE ..... - 6 -
8.11. 遥控 ..... - 6 -
8.12. 电度总召唤 ..... - 8 -
9. 规约测试软件 ..... - 9 -
9.1. 测试流程 ..... - 9 -
9.2. 测试软件比较 ..... - 9 -
9.3. KW-2200 配电网自动化模拟测试系统使用说明 ..... - 10 -
9.4. PMA 通信协议分析及仿真软件使用说明 ..... - 15 -

1. 概述

随着通信网络的迅猛发展，IEC-104 规约被广泛采用，本文着重讲解 IEC-104 的规约报文格式和实例分析，详细的交互和应用介绍请参考引用标准。

2. 引用标准

(1) 1997 版：《DLT 634.5101-1997/IEC60870-5-101:1995 远动设备及系统 第 5-101 部分：传输规约采用标准传输协议子集 IEC60870-5-101 网络访问》

(2) 2002 版：《DLT 634.5104-2002/IEC60870-5-104:2000 远动设备及系统 第 5-104 部分：传输规约采用标准传输协议子集 IEC60870-5-101 网络访问》

(3) 2009 版：《DLT 634.5104-2009/IEC60870-5-104:2006 远动设备及系统 第 5-104 部分：传输规约采用标准传输协议子集 IEC60870-5-101 网络访问》

版本对比：

各版本在规约处理流程上没有什么变化，不同之处在于：

（1）2002 版在 1997 版的基础上，扩展了遥测、遥信、遥控等信息体基体址。

（2）2009 版在 2002 版的基础上，增加了协议的传输序列和互操作性的改进，以及对冗余连接处理方面的新功能。

3. 信息体基地址范围

各版本区别如下：

类别	1997 版基地址	2002 和 2009 版基地址
遥信	1H------400H	1H------4000H
遥测	701H------900H	4001H------5000H
遥控	B01H------B80H	6001H------6100H
设点	B81H------C00H	6201H------6400H
电度	C01H------C80H	6401H------6600H

注意：调试主站或用测试软件测试装置的 104 规约时，主站和装置的版本要一致，有的主站和调试软件可通过设置选择规约版本。现在比较常用的是 2002 版。

4. 报文字节数的设置

类别	配置方式一	配置方式二
公共地址字节数	2	1
传输原因字节数	2	1
信息体地址字节数	3	2

注意：主站和测试软件一般都可以通过设置来选择配置方式，测试时注意装置的配置方式

要和主站或测试软件一致。

5. 类型标示符

序号	类型标示	十六进制	十进制	含义
1	建立连接或启动链路	07	07	和装置建立网络连接，或停止链路后再启动链路。
2	停止链路	13	19	网络建立连接成功后，停止链路，只发 U 格式测试帧。
3	召唤全数据	64	100	召唤全数据
4	召唤全电度	65	101	召唤全电度
5	对时	67	103	和主站时钟同步
6	遥测	09	09	带品质描述的测量值，每个遥测值占 3 个字节。
7		0a	10	带 3 个字节时标的且具有品质描述的测量值，每个遥测值占 6 个字节。
8		0b	11	不带时标的标度化值，每个遥测值占 3 个字节。
9		0c	12	带 3 个时标的标度化值，每个遥测值占 6 个字节。
10		0d	13	带品质描述的浮点值，每个遥测值占 5 个字节。
11		0e	14	带 3 个字节时标且具有品质描述的浮点值，每个遥测值占 8 个字节。
12		15	21	不带品质描述的遥测值，每个遥测值占 2 个字节。
13	遥信	01	01	不带时标的单点遥信，每个遥信占 1 个字节， 00：遥信分；01：遥信合。
14		03	03	不带时标的双点遥信，每个遥信占 1 个字节， 01：遥信分；02：遥信合。
15		14	20	具有状态变位检出的成组单点遥信，每个字节 8 个遥信。
16	SOE	02	02	带 3 个字节短时标的单点遥信，每个遥信占 4 个字节， 00：遥信分；01：遥信合。后面 3 个字节短时标。
17		04	04	带 3 个字节短时标的双点遥信，每个遥信占 4 个字节， 01：遥信分；02：遥信合。后面 3 个字节短时标。
18		1e	30	带 7 个字节时标的单点遥信，每个遥信占 4 个字节， 00：遥信分；01：遥信合。后面 7 个字节短时标。
19		1f	31	带 7 个字节时标的双点遥信，每个遥信占 4 个字节， 01：遥信分；02：遥信合。后面 7 个字节短时标。
20	遥控	2d	45	不带时标的单点遥控，每个遥控占 1 个字节， 遥控选择分：0x80；遥控执行或遥控撤销分：0x00。 遥控选择合：0x81；遥控选择或遥控撤销合：0x01。
21		2e	46	不带时标的双点遥控，每个遥控占 1 个字节，

				遥控选择分：0x81；遥控执行或遥控撤销分：0x01。 遥控选择合：0x82；遥控选择或遥控撤销合：0x02。
22		3a	58	带 7 字节长时标的单点遥控，每个遥控占 8 个字节， 遥控选择分：0x80；遥控执行或遥控撤销分：0x00。 遥控选择合：0x81；遥控选择或遥控撤销合：0x01。 遥控命令后带 7 字节的长时标。
23		3b	59	带 7 字节长时标的双点遥控，每个遥控占 8 个字节， 遥控选择分：0x81；遥控执行或遥控撤销分：0x01。 遥控选择合：0x82；遥控选择或遥控撤销合：0x02。 遥控命令后带 7 字节的长时标。
24	遥调	2f	47	双点遥调
25				
26				
27				
28				

注意：只整理了常用报文的类型标示符，没有全部整理，需要时请查阅相关国标标准。

6. 传送原因

序号	十六进制	十进制	含义
1	01	01	周期、循环（全数据主动上送）
2	02	02	背景扫描
3	03	03	突发（变化遥测、变化遥信、SOE 等）
4	04	04	初始化
5	05	05	请求或被请求
6	06	06	激活（遥控选择、遥控执行、对时等）
7	07	07	激活确认（遥控选择返校、遥控执行确认、对时确认等）
8	08	08	停止激活（遥控撤销等）
9	09	09	停止激活确认（遥控撤销确认等）
10	0a	10	激活结束（结束总召、遥控点号超范围、单双点遥控的命令不对等）
11	14	20	响应总召唤
12			

注意：只整理了常用报文的传送原因，没有全部整理，需要时请查阅相关国标标准。

7. 端口号

IEC-104 默认使用端口号为 2404，如果使用者关注由此而可能引起的安全问题，可采取相关的防范措施。

8. 报文实例

以公共地址字节数=2，传输原因字节数=2，信息体地址字节数=3 为例对一些常用的报文进行举例分析：

1）报文中的长度指的是除启动字符与长度字节外的所有字节总数。

2）长帧报文中的“发送序号”与“接收序号”具有抗报文丢失功能。

8.1. 建立网络连接或启动链路

主站发送→激活传输启动： **68**（启动符）**04**（长度）**07**（控制域）**00 00 00**

从站发送→确认激活传输启动： **68**（启动符）**04**（长度）**0B**（控制域）**00 00 00**

8.2. 停止链路

建立网络连接后，可停止链路，只响应 U 帧测试帧。

主站发送→停止链路： **68**（启动符）**04**（长度）**13**（控制域）**00 00 00**

从站发送→确认停止链路： **68**（启动符）**04**（长度）**23**（控制域）**00 00 00**

8.3. U 帧测试帧

如果主站超过一定时间没有下发报文或装置也没有上送任何报文，则双方都可以按频率发送 U 帧测试帧：

主站发送→U 帧测试帧： **68**（启动符）**04**（长度）**43**（控制域）**00 00 00**

从站发送→应答 U 帧测试帧： **68**（启动符）**04**（长度）**83**（控制域）**00 00 00**

8.4. S 帧测试帧

记录接收到的长帧，主站可以按频率发送 S 帧，比如接收 8 帧 I 帧回答一帧 S 帧，也可以要求接收 1 帧 I 帧就应答 1 帧 S 帧。

主站发送→S 帧： **68**（启动符）**04**（长度）**01**（控制域）**00 02 00**

8.5. 总召唤

召唤 YC、YX（可变长 I 帧），初始化后定时发送总召唤，每次总召唤的间隔时间一般设为 15 分钟召唤一次，不同的主站系统设置不同。

主站发送→总召唤：

68（启动符）**0E**（长度）**00 00**（发送序号）**00 00**（接收序号）**64**（类型标示:总召唤）**01**（可变结构限定词）**06 00**（传输原因：激活）**01 00**（公共地址即装置地址）**00 00 00**（信息体地址）**14**（区分是总召唤还是分组召唤，2002 年修改后的规约中没有分组召唤）。

从站发送→总召唤确认（发送帧的镜像，除传送原因不同）：

68（启动符）**0E**（长度）**00 00**（发送序号）**00 00**（接收序号）**64**（类型标示:总召唤）**01**（可变结构限定词）**07 00**（传输原因：激活确认）**01 00**（公共地址即装置地址）**00 00 00**（信息体地址）**14**（同上）

从站发送→YC 帧（类型标示符 09 带品质描述的遥测，传输原因：14 响应总召唤）：

68（启动符）**13**（长度）**06 00**（发送序号）**02 00**（接收序号）**09**（类型标示：带品质描述的遥测）**82**（可变结构限定词，有 2 个连续遥测上送）**14 00**（传输原因：响应总召唤）**01 00**（公共地址）**01 40 00**（信息体地址，从 0X4001 开始第 0 号遥测）**A1 10**（遥测值 10A1）**00**（品质描述）**89 15**（遥测值 1589）**00**（品质描述）

从站发送→YX 帧（类型标示符为 01 的单点遥信，传输原因：14 响应总召唤）：

68（启动符）**1A**（长度）**02　00**（发送序号）**02　00**（接收序号）**01**（类型标示：单点遥信）**04**（可变结构限定词，有 4 个遥信上送）**14　00**（传输原因：响应总召唤）**01　00**（公共地址即装置地址）**01 00 00**（信息体基地址）**00**（第 1 号遥信，分）**01**（第 2 号遥信，合）**00**（第 3 号遥信，分）**00**（第 4 号遥信，分）

从站发送→结束总召唤帧（主站发送总召唤命令，从站才对应发送结束总召唤帧）：

68（启动符）**0E**（长度）**08　00**（发送序号）**02　00**（接收序号）**64**（类型标示：总召唤）**01**（可变结构限定词）**0A　00**（传输原因：激活结束）**01　00**（公共地址）**00 00 00**（信息体地址）**14**（区分是总召唤还是分组召唤，02 年修改后的规约中没有分组召唤）

主站发送→S 帧：

68　04　01　00　0A　00

8.6. 对时

主站发送→对时命令：

68（启动符）**14**（长度）**02　00**（发送序号）**0A　00**（接收序号）**67**（类型标示：时钟同步）**01**（可变结构限定词）**06　00**（传输原因：激活）**01　00**（公共地址）**00 00 00**（信息体地址）**01**（毫秒低位）**02**（毫秒高位）**03**（分钟）**04**（时）**81**（日与星期）**09**（月）**10**（年）

从站发送→对时确认：

68（启动符）**14**（长度）**0A　00**（发送序号）**02　00**（接收序号）**67**（类型标示：时钟同步）**01**（可变结构限定词）**07　00**（传输原因：激活确认）**01　00**（公共地址）**00 00 00**（信息体地址）**01**（毫秒低位）**02**（毫秒高位）**03**（分钟）**04**（时）**81**（日与星期）**09**（月）**10**（年）

主站发送→S 帧：

68　04　01　00　0E　00

8.7. 全遥测

从站发送→YC 帧（以类型标示符 09 为例）：

68（启动符）**13**（长度）**06　00**（发送序号）**02　00**（接收序号）**09**（类型标示：带品质描述的遥测）**82**（可变结构限定词，有 2 个连续遥测上送）**01　00**（传输原因：周期、循环）**01　00**（公共地址）**01 40 00**（信息体地址，从 0X4001 开始第 0 号遥测）**A1 10**（遥测值 10A1）**00**（品质描述）**89 15**（遥测值 1589）**00**（品质描述）

主站发送→S 帧（从站发送周期循环数据时，主站发送 S 帧）：

68　04　01　00　04　00

8.8. 全遥信

从站发送→YX 帧（以类型标示符为 01 的单点遥信为例）：

68（启动符）**1A**（长度）**02　00**（发送序号）**02　00**（接收序号）**01**（类型标示：单点遥信）**04**（可变结构限定词，有 4 个遥信上送）**01　00**（传输原因：周期、循环）**01　00**（公共地址即装置地址）**01 00 00**（信息体基地址）**00**（第 1 号遥信，分）**01**（第 2 号遥信，合）**00**（第 3 号遥信，分）**00**（第 4 号遥信，分）

主站发送→S 帧（从站发送周期循环数据时，主站发送 S 帧）：

68　04　01　00　04　00

从站发送→YX 帧（以类型标示符为 03 的双点遥信为例）：

68（启动符）**1C**（长度）**04　00**（发送序号）**02　00**（接收序号）**03**（类型标示：双点遥信）**04**（可变结构限定词，有 4 个遥信上送）**01　00**（传输原因：周期、循环） **01　00**（公共地址）**01 00 00**（信息体基地址）**01**（第 1 号遥信，分）**02**（第 2 号遥信，合）**01**（第 3 号遥信，分）**01**（第 4 号遥信，分）

主站发送→S 帧（从站发送周期循环数据时，主站发送 S 帧）：

68　04　01　00　04　00

8.9. 变化遥信

如果有变化数据产生，装置会主动上送至主站，主动上送的变位遥信如下：

从站发送→变位遥信（以类型标示符为 01 的单点遥信为例）：

68（启动符）**0E**（长度）**16　00**（发送序号）**06　00**（接收序号）**01**（类型标示：单点遥信）**01**（可变结构限定词，有 1 个变位遥信上送）**03　00**（传输原因：表突发事件）**01　00**（公共地址即装置地址）**03 00 00**（信息体地址，第 3 号遥信）**00**（遥信分）

主站发送→S 帧：

68　04　01　00　18　00

从站发送→变位遥信（以类型标示符为 03 的单点遥信为例）：

68（启动符）**0E**（长度）**18　00**（发送序号）**06　00**（接收序号）**03**（类型标示：双点遥信）**01**（可变结构限定词，有 1 个变位遥信上送）**03　00**（传输原因：表突发事件）**01　00**（公共地址即装置地址）**03 00 00**（信息体地址，第 3 号遥信）**01**（遥信分）

主站发送→S 帧：

68　04　01　00　1a　00

8.10. SOE

有 SOE 生成时，装置会主动上送至主站。

从站发送→SOE（以类型标示符为 1e 的单点遥信为例）：：

68（启动符）**15**（长度）**1a　00**（发送序号）**06　00**（接收序号）**1e**（类型标示：单点遥信的 SOE）**01**（可变结构限定词，有 1 个 SOE）**03　00**（传输原因：表突发事件）**01　00**（公共地址即装置地址）**03 00 00**（信息体地址，第 3 号遥信）**00**（遥信分）**ad**（毫秒低位）**39**（毫秒高位）**1c**（分钟）**10**（时）**7a**（日与星期）**09**（月）**10**（年）

主站发送→S 帧：

68　04　01　00　1c　00

从站发送→SOE（以类型标示符为 1f 的双点遥信为例）：：

68（启动符）**15**（长度）**1c　00**（发送序号）**06　00**（接收序号）**1f**（类型标示：双点遥信的 SOE）**01**（可变结构限定词，有 1 个 SOE）**03　00**（传输原因：表突发事件）**01　00**（公共地址即装置地址）**03 00 00**（信息体地址，第 3 遥信）**01**（遥信分）**ad**（毫秒低位）**39**（毫秒高位）**1c**（分钟）**10**（时）**7a**（日与星期）**09**（月）**10**（年）

主站发送→S 帧：

68　04　01　00　1c　00

8.11. 遥控

（1）以类型标示为 2d 不带时标的单点遥控为例：

主站发送→遥控选择：

68（启动符）**0e**（长度）**06　00**（发送序号）**0a　00**（接收序号）**2d**（类型标示：不带时标的单点遥

控）**01**（可变结构限定词）**06　00**（传输原因：激活）**01　00**（公共地址即装置地址）**02 60 00**（信息体地址，遥控号=0x0602-0x0601=1）**81**（控合）

从站发送→遥控返校：

68（启动符）**0e**（长度）**0a　00**（发送序号）**06　00**（接收序号）**2d**（类型标示：不带时标的单点遥控）**01**（可变结构限定词）**07　00**（传输原因：激活确认）**01　00**（公共地址即装置地址）**02 60 00**（信息体地址，遥控号=0x0602-0x0601=1）**81**（控合）

主站发送→遥控执行：

68（启动符）**0e**（长度）**08　00**（发送序号）**0c　00**（接收序号）**2d**（类型标示：不带时标的单点遥控）**01**（可变结构限定词）**06　00**（传输原因:激活）**01　00**（公共地址即装置地址）**02 60 00**（信息体地址，遥控号=0x0602-0x0601=1）**01**（控合）

从站发送→执行确认：

68（启动符）**0e**（长度）**0c　00**（发送序号）**08　00**（接收序号）**2d**（类型标示：不带时标的单点遥控）**01**（可变结构限定词）**07　00**（传输原因：激活确认）**01　00**（公共地址即装置地址）**02 60 00**（信息体地址，遥控号=0x0602-0x0601=1）**01**（控合）

主站发送→遥控撤消：

68（启动符）**0e**（长度）**04　00**（发送序号）**0e　00**（接收序号）**2d**（类型标示：不带时标的单点遥控）**01**（可变结构限定词）**08　00**（传输原因：停止激活）**01　00**（公共地址即装置地址）**02 60 00**（信息体地址，遥控号=0x0602-0x0601=1）**01**（控合）

从站发送→撤消确认：

68（启动符）**0e**（长度）**0e　00**（发送序号）**08　00**（接收序号）**2d**（类型标示：不带时标的单点遥控）**01**（可变结构限定词）**09　00**（传输原因：停止激活确认）**01　00**（公共地址即装置地址）**02 60 00**（信息体地址，遥控号=0x0602-0x0601=1）**01**（控合）

遥控选择时，如果遥控点号超范围或者遥控命令与类型标示符不符时，装置发送激活结束：

从站发送→激活结束：

68（启动符）**0e**（长度）**0e　00**（发送序号）**08　00**（接收序号）**2d**（类型标示：不带时标的单点遥控）**01**（可变结构限定词）**0a　00**（传输原因：激活结束）**01　00**（公共地址即装置地址）**02 60 00**（信息体地址，遥控号=0x0602-0x0601=1）**81**（控合）

（2）以类型标示为 3b 带 7 字节长时标的双点遥控为例：

主站发送→遥控选择：

68（启动符）**15**（长度）**02　00**（发送序号）**06　00**（接收序号）**3b**（类型标示：带 7 字节长时标的双点遥控）**01**（可变结构限定词）**06　00**（传输原因:激活）**01　00**（公共地址即装置地址）**01 06 00**（信息体地址，遥控号=0x06001-0x6001=0）**81**（控分） **f2**（ms 低位） **79**（ms 高位） **1a**（分钟） **0b**（小时） **02**（星期加日） **09**（月） **10**（年）

从站发送→遥控返校：

68（启动符）**15**（长度）**06　00**（发送序号）**02　00**（接收序号）**3b**（类型标示： 带 7 字节长时标的双点遥控）**01**（可变结构限定词）**07　00**（传输原因：激活确认）**01　00**（公共地址即装置地址）**01 06 00**（信息体地址，遥控号=0x06001-0x6001=0）**81**（控分） **f2**（ms 低位） **79**（ms 高位） **1a**（分钟） **0b**（小时） **02**（星期加日） **09**（月） **10**（年）

主站发送→遥控执行：

68（启动符）**15**（长度）**04　00**（发送序号）**08　00**（接收序号）**3b**（类型标示：带 7 字节长时标的双点遥控）**01**（可变结构限定词）**06　00**（传输原因：激活）**01　00**（公共地址即装置地址）**01 06 00**（信息体地址，遥控号=0x06001-0x6001=0）**01**（控分） **f2**（ms 低位） **79**（ms 高位） **1a**（分钟） **0b**（小时） **02**（星期加日） **09**（月） **10**（年）

从站发送→执行确认：

68（启动符）**15**（长度）**08　00**（发送序号）**04　00**（接收序号）**3b**（类型标示：带 7 字节长时标的双点遥控）**01**（可变结构限定词）**07　00**（传输原因：激活确认）**01　00**（公共地址即装置地址）**01 06 00**（信息体地址，遥控号=0x06001-0x6001=0）**01**（控分） **f2**（ms 低位） **79**（ms 高位） **1a**（分钟） **0b**（小时） **02**（星期加日） **09** 主站发送→遥控撤消：

68（启动符）**15**（长度）**06　00**（发送序号）**0a　00**（接收序号）**3b**（类型标示：带 7 字节长时标的双点遥控）**01**（可变结构限定词）**08　00**（传输原因：停止激活）**01　00**（公共地址即装置地址）**01 06 00**（信息体地址，遥控号=0x06001-0x6001=0）**01**（控分） **f2**（ms 低位） **79**（ms 高位） **1a**（分钟） **0b**（小时） **02**（星期加日） **09**（月） **10**（年）

从站发送→撤消确认：

68（启动符）**15**（长度）**0a　00**（发送序号）**06　00**（接收序号）**3b**（类型标示：带 7 字节长时标的双点遥控）**01**（可变结构限定词）**09　00**（传输原因：停止激活确认）**01　00**（公共地址即装置地址）**01 06 00**（信息体地址，遥控号=0x06001-0x6001=0）**01**（控分） **f2**（ms 低位） **79**（ms 高位） **1a**（分钟） **0b**（小时） **02**（星期加日） **09**（月） **10**（年）

遥控选择时，如果遥控点号超范围或者遥控命令与类型标示符不符时，装置发送激活结束：

从站发送→激活结束：

68（启动符）**15**（长度）**0e　00**（发送序号）**08　00**（接收序号）**3b**（类型标示：带 7 字节长时标的双点遥控）**01**（可变结构限定词）**0a　00**（传输原因：激活结束）**01　00**（公共地址即装置地址）**01 60 00**（信息体地址，遥控号=0x0601-0x0601=0）**81**（控分）**f2**（ms 低位） **79**（ms 高位） **1a**（分钟） **0b**（小时） **02**（星期加日） **09**（月） **10**（年）

8.12. 电度总召唤

电度可以在对时之前发送。通过设置参数中"全数据扫描间隔"，单位是分钟，一般是 15 分钟召唤一次电度，如果不需要召唤电度一定要将参数中的电度个数设为 0。

如果没有电度此步骤可以省略。

主站发送→召唤电度：

68（启动符）**0E**（长度）**04　00**（发送序号）**0c　00**（接收序号）**65**（类型标示：召唤全电度）**01**（可变结构限定词）**06　00**（传输原因：激活）**01　00**（公共地址即装置地址）**00 00 00**（信息体地址）**45**（QCC）

从站发送→召唤确认(发送帧的镜像，除传送原因不同) ：

68（启动符）**0E**（长度） **0c　00**（发送序号）**04　00**（接收序号）**65**（类型标示：召唤全电度）**01**（可变结构限定词）**07　00**（传输原因：激活确认）**01　00**（公共地址即装置地址）**00 00 00**（信息体地址）**45**（QCC）

主站发送→S 帧：

68　04　01　00　12　00

从站发送→电度数据：

68（启动符）**1A**（长度）**0e　00**（发送序号）**06　00**（接收序号）**0F**（类型标示：不带时标的电能量，每个电能量占 5 个字节）**02**（可变结构限定词,有两个电度量上送）**05　00**（传输原因：请求或被请求）**01　00**（公共地址即装置地址）**01 64 00**（信息体地址，从 0X6401 开始第 0 号电度）**00 00 00 00**（电度值）**00**（描述信息）**02 64 00**（信息体地址，从 0X6402 开始第 1 号电度）**00 00 00 00**（电度值）**01**（描述信息）

主站发送→S 帧：

68　04　01　00　14　00

从站发送→结束总召唤帧：

68（启动符）**0E**（长度）**14　00**（发送序号）**06　00**（接收序号）**65**（类型标示示：召唤全电度）**01**

（可变结构限定词）**0A　00**（传输原因：激活结束）**01　00**（公共地址即装置地址）**00 00 00**（信息体地址）**45**（QCC）

主站发送→S 帧：

68　04　01　00　16　00

9. 规约测试软件

9.1. 测试流程

1）　打开测试软件；

2）　选择 104 规约；

3）　建立网络连接；

4）　发送总召唤；

5）　发送对时；

6）　循环数据的主动上送测试；

7）　遥测、遥信、遥控、电度的测试；

8）　变化遥测、变化遥信、SOE 的测试；

9）　客户特殊要求的测试（如停止链路，启动链路等）；

10）　可借助测试软件的报文解析分析报文的传送处理是否与要求相符。

9.2. 测试软件比较

（1）　KW-2200 配电网自动化模拟测试系统

（2）　PMA 通信协议分析及仿真软件

两个软件的相同点：

设置和测试流程基本相同，常用的功能基本都能测试。

两个软件的不同点：

（1）　KW-2200 配电网自动化模拟测试系统：

优点：

A、界面比较友善，快捷方式很多，通道数据、遥测、遥信、遥控、事件、输出分界面显示，每个功能都可单独测试，灵活方便。

B、报文内容解析的很详细，清晰易懂，可以和规约要求进行对比，是否满足设计要求。

C、终端参数设置界面中的“同步对时”不起作用，需要手动选择“即时命令”中的“时钟同步”进行对时。

D、个别报文（停止链路，启动链路等）可以通过手动输入报文进行测试。

缺点：遥控类型默认为不带时标的双点遥控，其他遥控类型测试不了。

（2） PMA 通信协议分析及仿真软件

优点：手动方式可以测试各种遥控类型（不带时标的单点遥控；不带时标的双点遥控；带 7 字节长时标的单点遥控；带 7 字节长时标的双点遥控都可以测试）。

缺点：

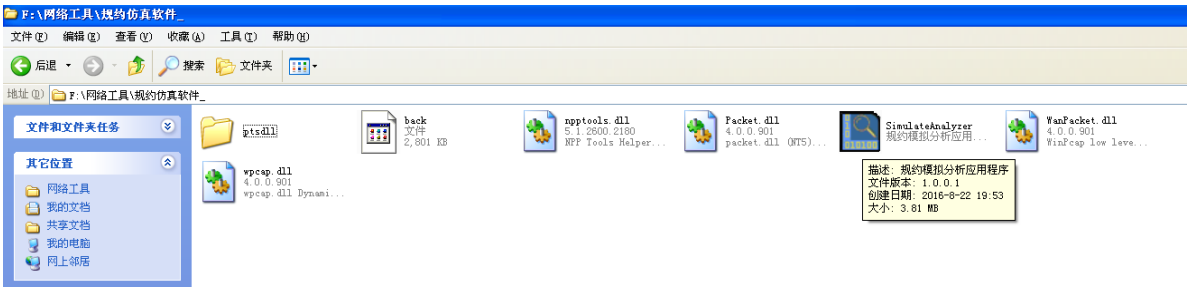
A、只有报文收发的显示界面，总召、对时、遥控等测试需要手动选择类型标示符，并输入传送原因、点号等信息，才能正确测试。

B、报文的解析不是非常清晰明了，需要对照实际报文进行分析。

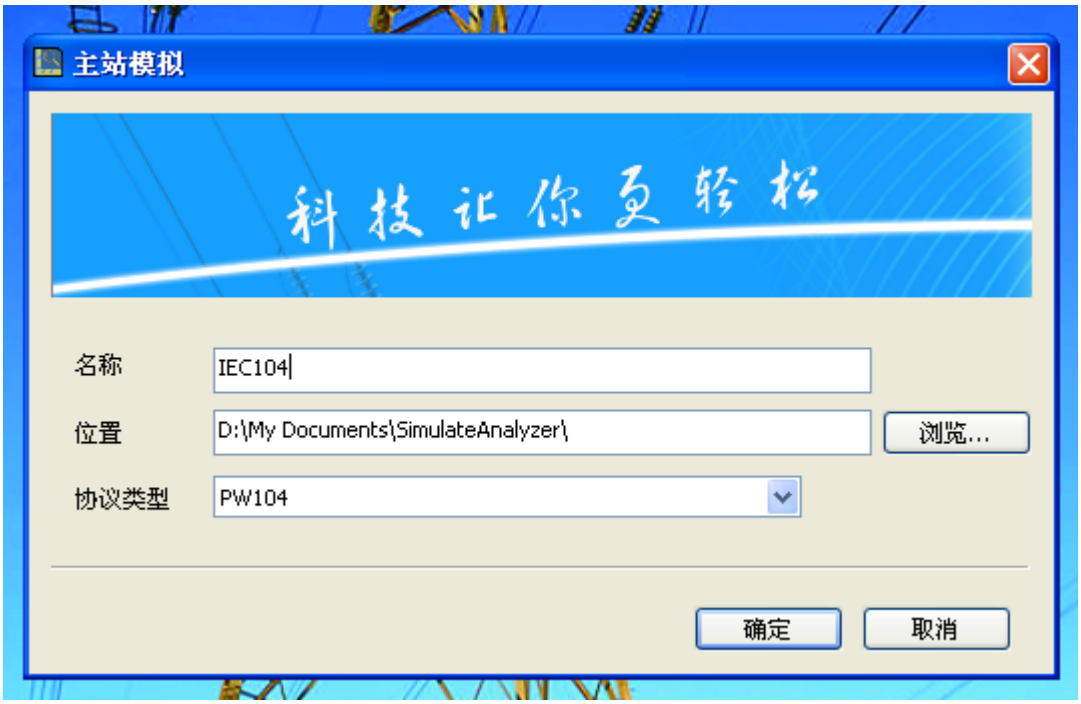
C、多数情况下，提示“链路连接失败”信息后，再次连接也连接不上了，需要关闭软件重新打开才有效。

9.3. KW-2200 配电网自动化模拟测试系统使用说明

（1） 打开软件



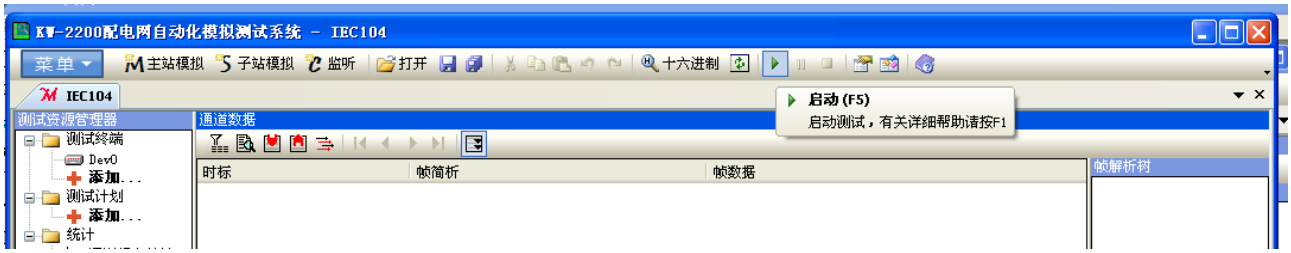
（2） 选择规约，输入名称


主站模拟
科技让你更轻松
名称
IEC104
位置
D:\My Documents\SimulateAnalyzer\
浏览...
协议类型
PW104
确定
取消

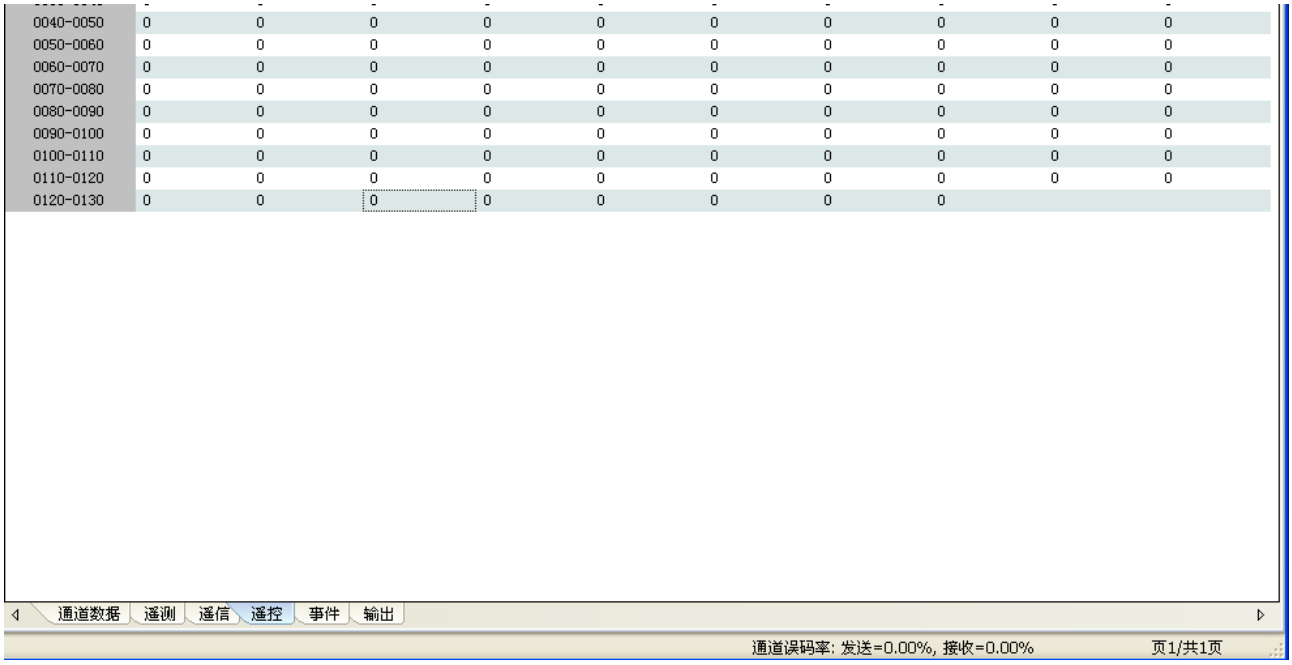
（3） 设置参数


通讯参数配置
通讯参数定义
端口定义
终端IP地址
192.168.0.250
端口号
2404
连接建立超时t0(秒)
10
发送或测试超时t1(秒)
12
无数据报文超时t2(秒)
5
长期空闲超时t3(秒)
15
应用报文确认超时t4(秒)
8
发送I帧最大未确认个数K
12
接收I帧最大未确认个数W
8
协议定义
公共地址长度
2字节
传送原因长度
2字节
信息体地址长度
3字节
确定
取消
十六进制
终端IP地址

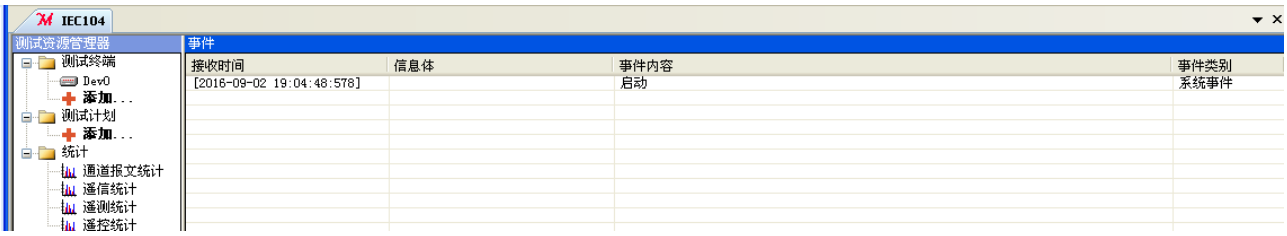
（4）启动测试



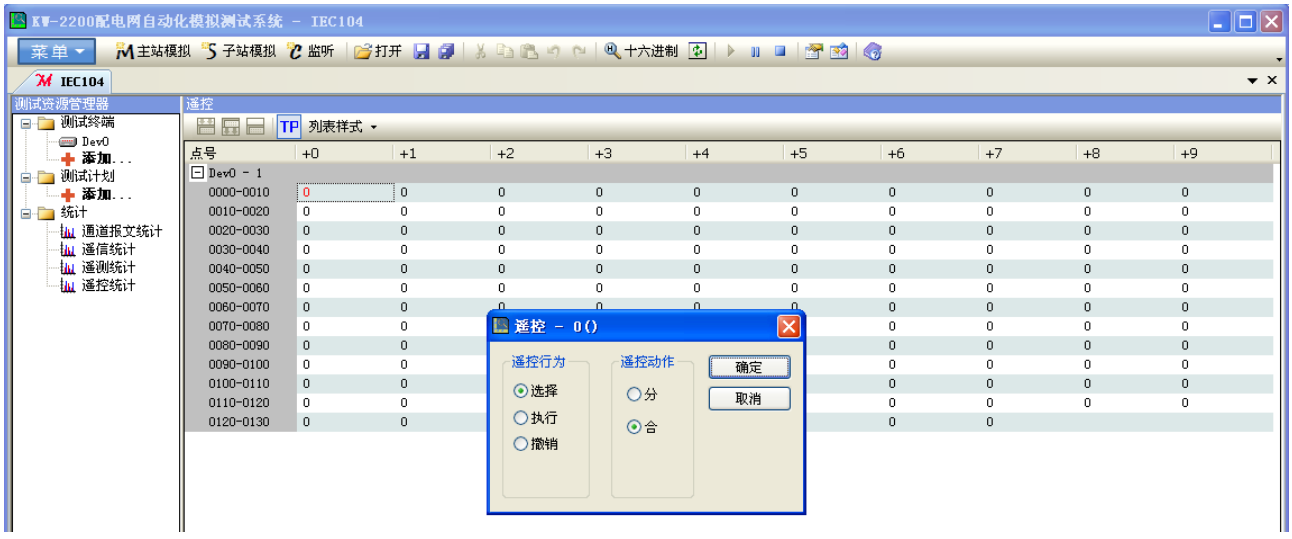
(5)功能测试的子菜单选择



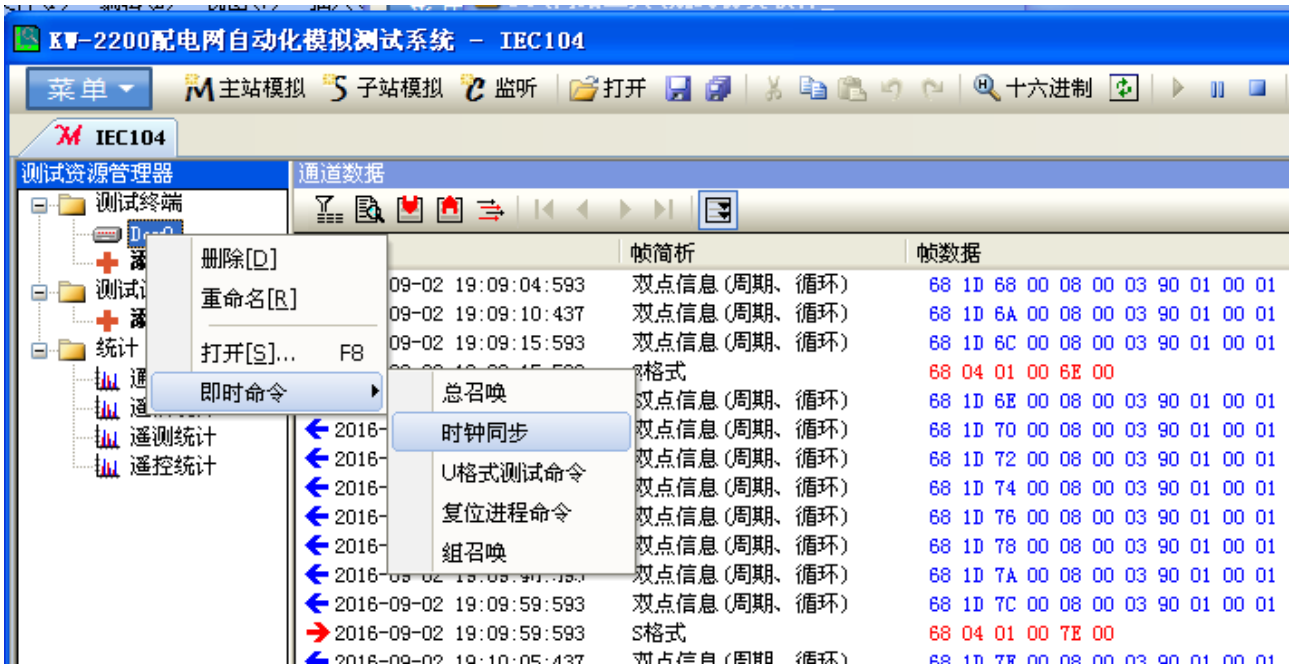
(6)事件输出（启动、变化遥信、SOE、遥控等信息均可显示）



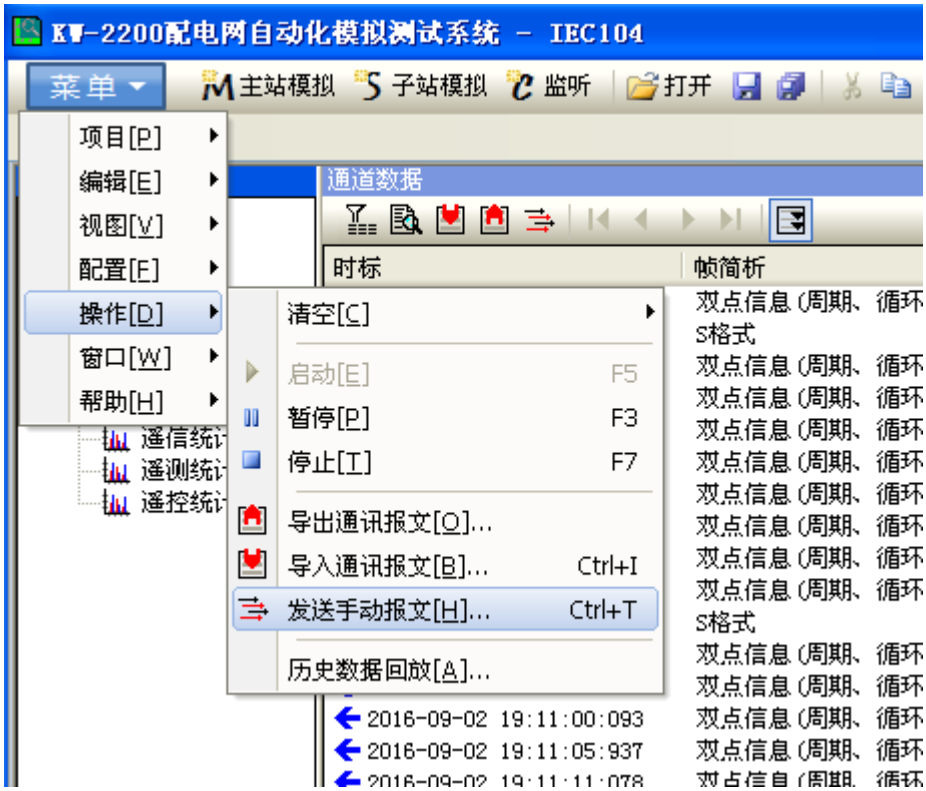
(7)遥控测试



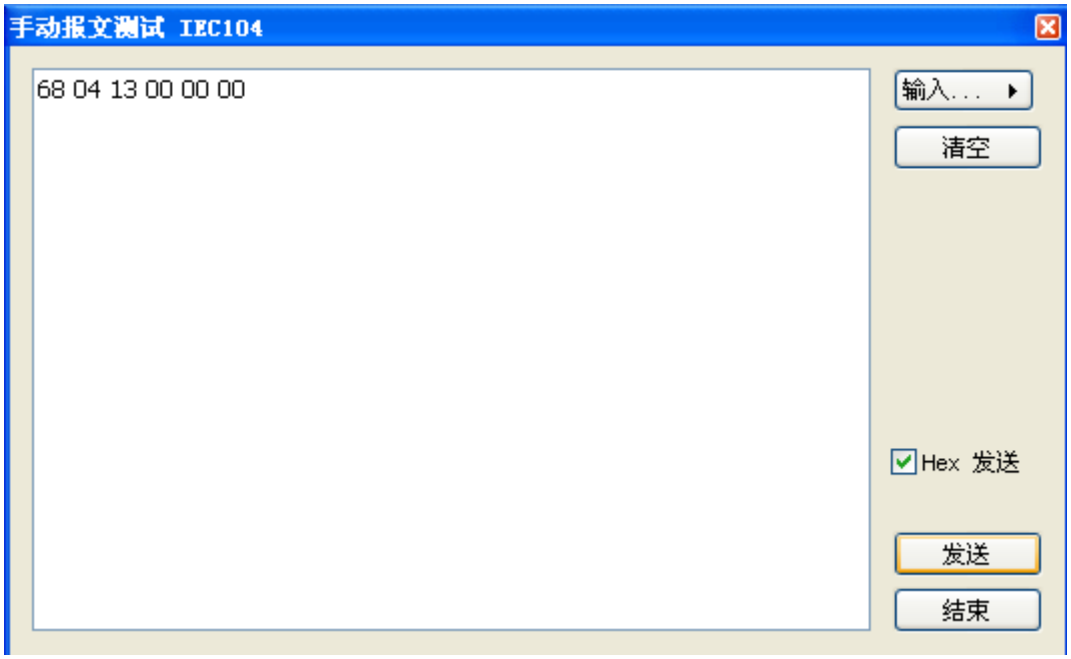
(8)对时



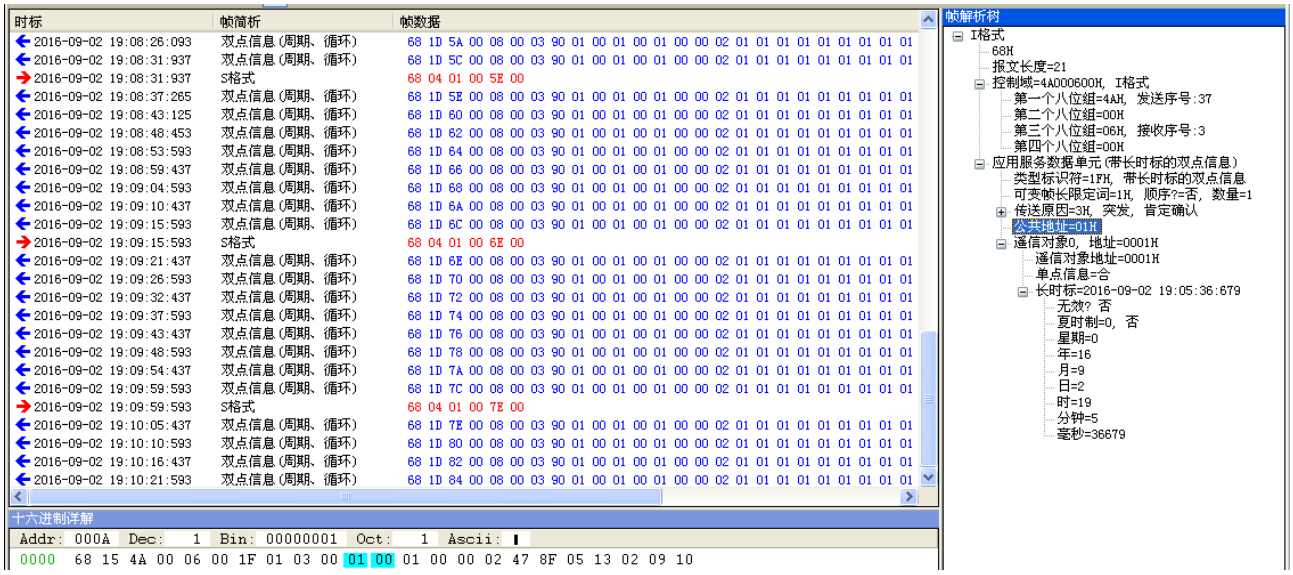
（9）手动输入报文



（10）停止链路等报文手动输入

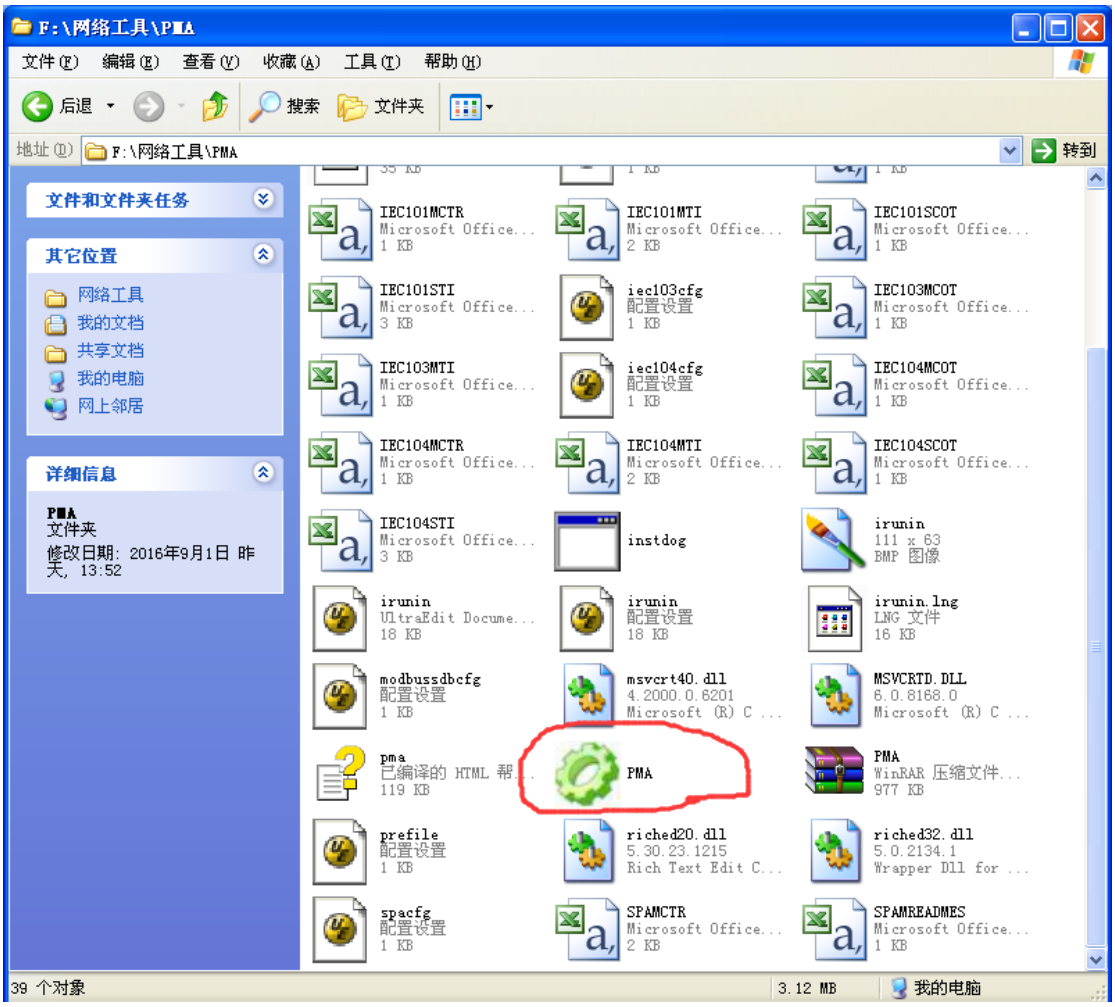


（11）报文解析

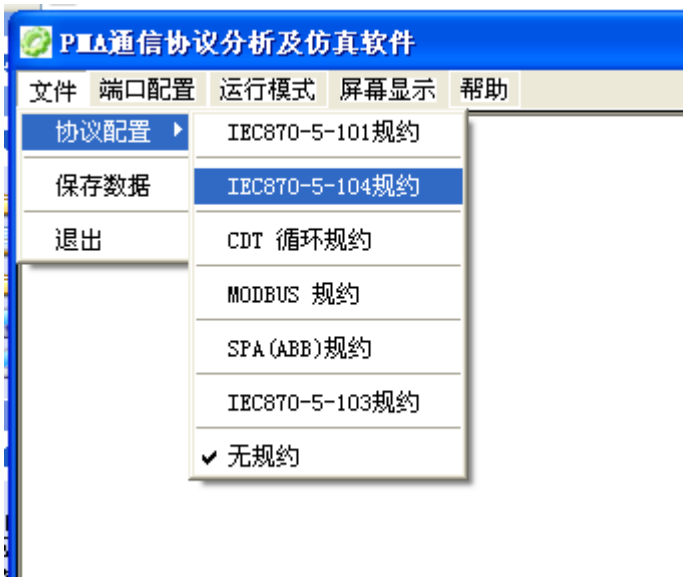


9.4. PMA 通信协议分析及仿真软件使用说明

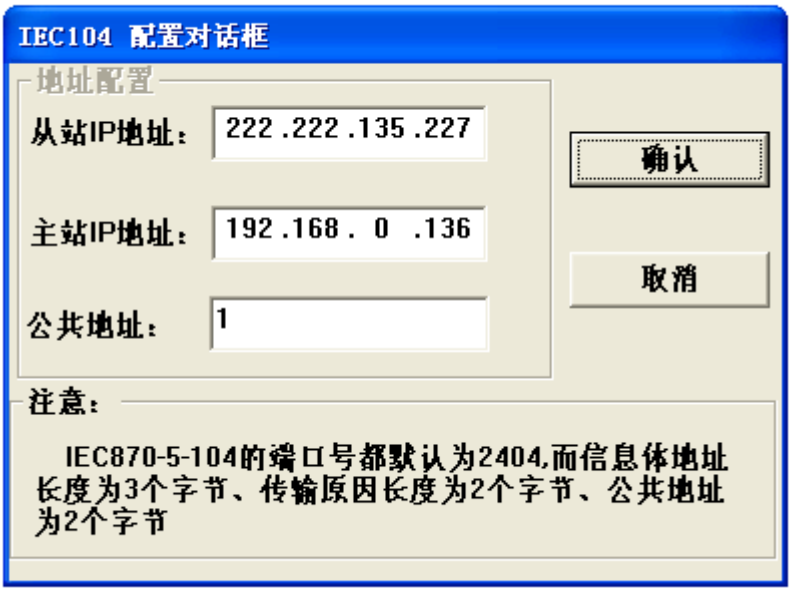
（1）打开软件


F:\网络工具\PMA
文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)
后退 搜索 文件夹
地址(D) F:\网络工具\PMA
转到
文件和文件夹任务
其它位置
网络工具
我的文档
共享文档
我的电脑
网上邻居
详细信息
PMA
文件夹
修改日期: 2016年9月1日 昨天, 13:52
IEC101MCTR
IEC101MTI
IEC101SCOT
IEC101STI
iec103cfg
配置设置
IEC103MCOT
IEC103MTI
iec104cfg
IEC104MCOT
IEC104MCTR
IEC104MTI
IEC104SCOT
IEC104STI
instdog
irunin
irunin
irunin.lng
modbussdbcfg
msvcrt40.dll
MSVCRTD.DLL
pma
PMA
prefile
riched20.dll
riched32.dll
spacfg
SPAMCTR
SPAMREADMES
39 个对象
3.12 MB
我的电脑

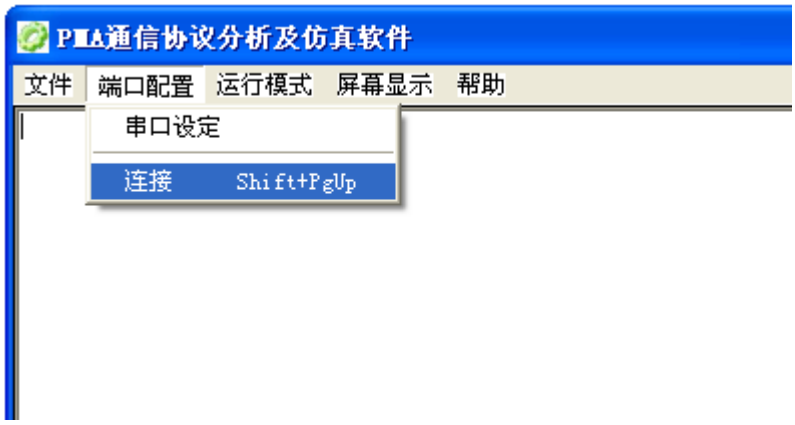
(2)选择规约


PMA通信协议分析及仿真软件
文件
端口配置
运行模式
屏幕显示
帮助
协议配置
保存数据
退出
IEC870-5-101规约
IEC870-5-104规约
CDT 循环规约
MODBUS 规约
SPA(ABB)规约
IEC870-5-103规约
无规约

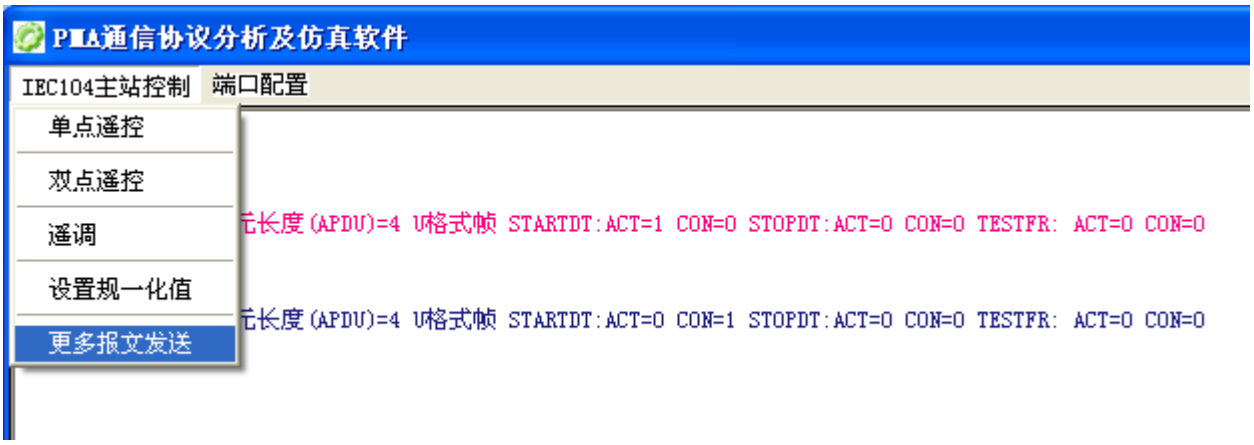
（3）配置参数



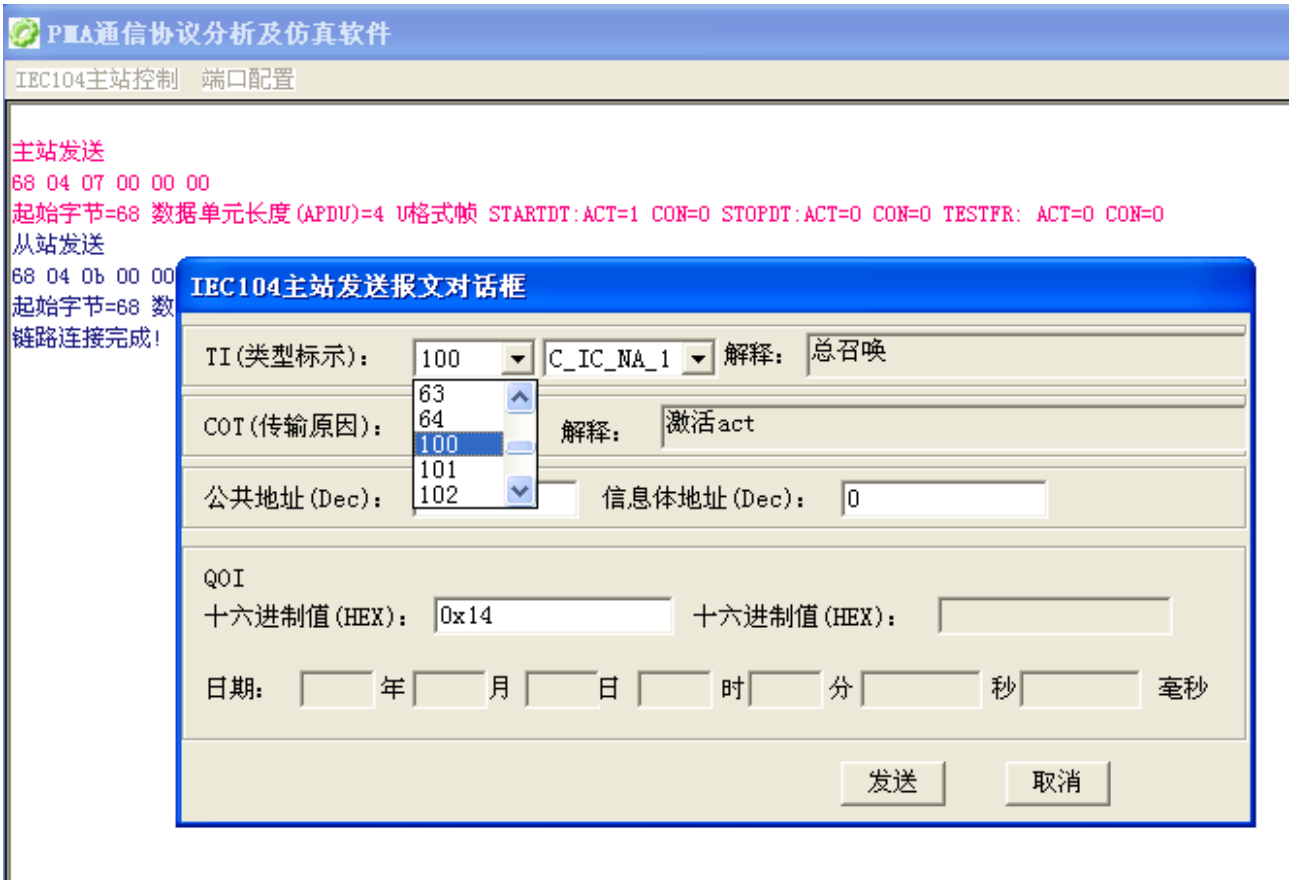
（4）建立网络连接



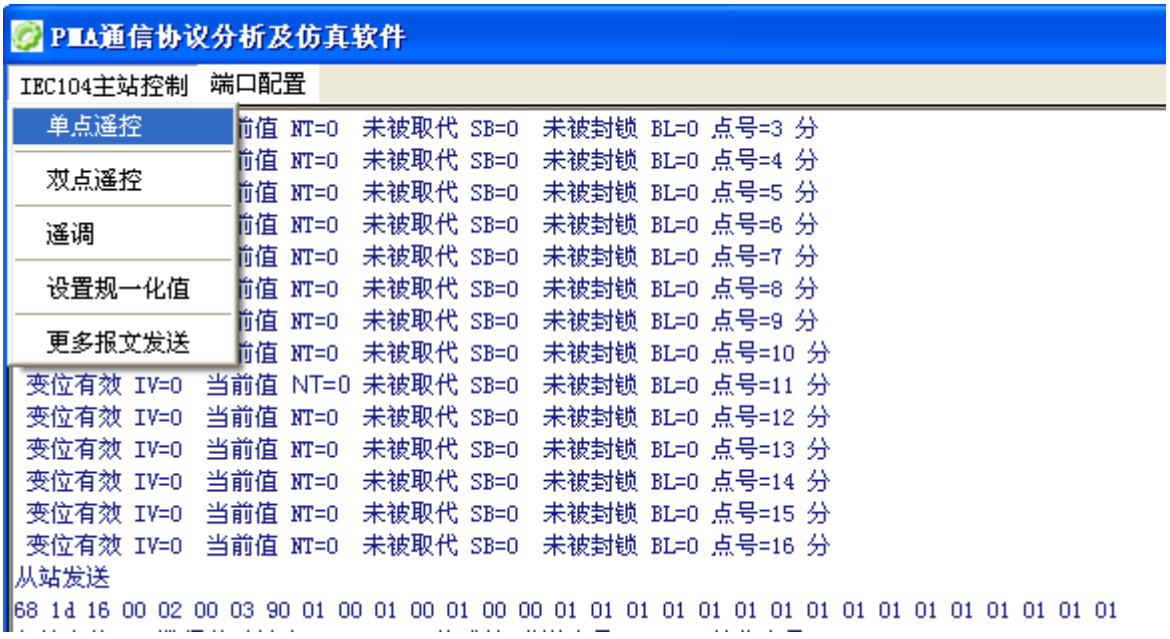
（5）手动发送报文（建立连接后需要手动发送总召唤命令）



（6）发送总召唤



（7）选择遥控测试



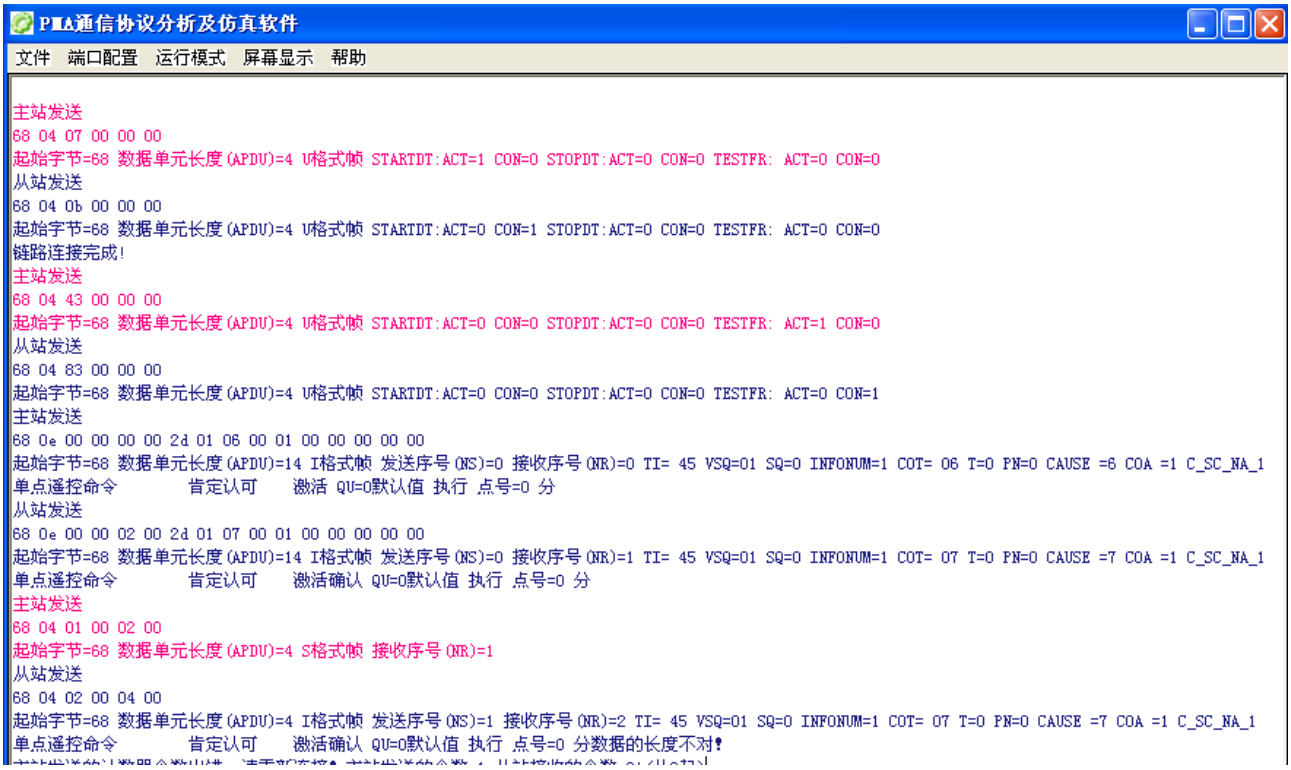
（8）带时标的遥控需要手动输入报文格式


IEC104主站发送报文对话框
TI(类型标示)：
59
C_DC_TA_1
解释：
带长时标双点遥控(CP56)
类型标示
COT(传输原因)：
6
解释：
激活act
公共地址(Dec)：
1
信息体地址(Dec)：
24577
遥控点号，2002版
从0x006001开始
装置ADDR
输入：遥控选择分，遥控选择合，遥控执行分，遥控执行合
DCO
十六进制值(HEX)：
0x81
十六进制值(HEX)：
日期：
2016
年
9
月
2
日
12
时
50
分
51
秒
453
毫秒
发送
取消

(9)对时


IEC104主站发送报文对话框
TI(类型标示)：
103
C_CS_NA_1
解释：
时钟同步命令
COT(传输原因)：
6
解释：
激活act
公共地址(Dec)：
1
信息体地址(Dec)：
0
十六进制值(HEX)：
十六进制值(HEX)：
日期：
2016
年
9
月
2
日
18
时
58
分
51
秒
328
毫秒
发送
取消

（10）报文解析



（11）遥测、遥信、遥控等没有单独的显示菜单，只有总的报文收发显示。