基于通信协议多元接入的计量自动化远程控制研究

梁 捷[1],梁广明[2]
(1. 广西电网有限责任公司计量中心,广西 南宁 530023;
2. 南宁百会药业集团有限公司,广西 南宁 530003)

摘 要: 广西电网计量自动化"两覆盖"工作中需对多种通信协议设备并存的复合网络进行远程控制,应用时常出现电能表拉合闸失败的问题。首先分析了广西电网常见的电表和计量终端通信协议的特点,然后从广西97规约电能表"先告警后控制"控制机制与南方电网公司规约电能表的差异性,以及费控体系安全防护要求等方面分析了多元接入条件下计量终端对电能表远程控制方案的可行性,并据此给出了推荐控制方案和流程。接着通过实例分析了不同集中器和载波通信模块厂家拉闸平均响应时间的特点和差异,最后对计量主站远程控制功能调试时发现的安全认证失败等常见异常问题进行了上下行通讯报文的实例分析,为计量自动化系统远程费控功能开发提供经验。

关键词: 通讯协议多元接入; 安全防护; 远程控制; 拉闸响应时间
中图分类号: TM933 **文献标志码:** A **文章编号:** 1003-6954(2019)04-0090-05
DOI:10.16527/j.cnki.cn51-1315/tm.2019.04.017

Research on Remote Control of Metrology Automation Based on Multi-source Access of Communication Protocol

Liang Jie[1], Liang Guangming[2]
(1. Electric Power Research Institute of Guangxi Power Grid Corporation, Nanning 530023, Guangxi, China;
2. Nanning Baihui Pharmaceutical Group Co., Ltd., Nanning 530003, Guangxi, China)

Abstract: Aiming at the problems existing in the application of remote control function in the "two coverage" work of metering automation in Guangxi power grid, three kinds of electric energy meters and two types of communication protocols for metering terminals commonly used in the field application of Guangxi power grid are firstly introduced. And then, from the aspects pf the compatibility of equipment communication protocols, the difference of "alarm before pull" control mechanism of Guangxi 97 protocol electric energy meter, and the security protection requirements of fee control system, the feasibility of remote control scheme for watt-hour meter by metering terminal is analyzed, and the recommended scheme and the switching-on process are given accordingly. The characteristics and difference of average response time between different communication modules and concentrator manufacturers are analyzed by testing. In addition, when commissioning the communication protocol of remote control function of the metering master station, the common abnormal problems found are analyzed with examples of upstream and downstream. It can provide experiences for the development of remote cost control function of metering automation system.

Key words: multi-source access of communication protocol; security protection; remote control; switching response time

0 引 言

为响应南方电网公司"十三五"科技发展规划对计量信息安全防护体系的建设要求[1],广西电网正大力推进费控电能表和低压集抄终端100%覆盖的"两覆盖"工作。随着广西省集中计量主站的建设和费控电能表的推广使用,广西电网存在现场安装的计量设备的通讯协议和技术要求不统一,现行的电能表和低压集抄系列技术规范通信协议费控控制功能定义不明确的问题[2]。为保障广西电网公司计量自动化系统远程费控功能模块的正常应用,针对不同类型的电能表和计量终端模拟现场条件组织开展了远程拉合闸功能测试试验;针对不同仪表设备组合给出可行的远程控制方案,并结合通讯报文分析了试验中拉合闸失败案例的原因,为各地计

量自动化系统远程费控功能开发提供经验。

1 广西电能表远程控制现状

目前广西电网在用的支持远程拉合闸的电能表通讯规约类型包括: 1) 符合南方电网技术规范的费控电能表(简称南网费控表) ,采用 07 规约带南网规范 ESAM 安全模块,其大多数的参数修改和远程控制过程需通过密文 + MAC 的方式进行数据的传输和验证,需经过密码机进行拉合闸[3] 。2) 符合南方电网规范的 DL/T 645 – 2007 规约普通电子式电能表(简称南网 07 表) [4] ,不带安全模。广西电网在南网规范的基础上结合大用户“先购电再用电”的需求制定了预付费电能表的技术规范,其远程拉合闸的机制与南网 07 表一致[5] 。3) 符合广西电网公司电子式电能表通信规约的电能表(简称广西 97 表) ,该规约是在 DL/T 645 – 1997 规约基础上扩展而来,为广西特有,不带安全模块。

广西常见终端规约类型包括: 1) 符合南网规范的计量终端(简称南网终端) ,采用南网 2013 版上行通信规约,支持写控制参数和中继转发的方式对电表进行远程控制[6] 。2) 符合广西电网技术规范的计量终端(简称广西终端) ,采用 2008 年广西地方自行发布施行的计量终端上行数据传输规约,大部分可通过远程通断电控制命令和数据转发的方式对电表进行拉合闸; 但由于广西 2017 年省集中计量主站建设之前,旧主站一直采用控制命令方式,因此部分终端在验收时未对数据转发功能做强制要求。

由于上述多种上行通讯协议的计量终端和下行协议的电能表同时接入计量系统使用,不同设备不同协议的配合在通讯应用时缺乏完整有效的组合控制方案,无法保证拉合闸功能的实现,给新计量主站的远程费控功能开发带来困难。

2 计量终端与电表的控制方案

广西常见计量终端与电能表的 6 种控制组合见表 1。控制方案的选择需考虑电能表和计量终端通讯协议的兼容性、升级改造的成本和对费控安全防护体系的硬件需求等方面。

如表 1 所示,对于南网费控表,由于目前计量终端缺少安全模块的型式定义,故无法安装安全模块与费控密码机交互实现传输数据的加密和解密,故只能通过计量主站连接加密机,以中继转发的方式进行远程控制。广西上行通信规约的数据转发与南网规约对中继转发命令的功能定义大体相同,区别仅在于广西规约未对中继类型进行区分。但由于第 1 节所述的历史管理问题,部分广西终端不支持数据转发功能,由于这部分终端在现场广泛使用,现场升级人力成本高,故广西终端常采用远程升级方式,常见方式有两种: 方案 A 为搭建升级专用临时服务器,修改终端 IP 地址,连接该服务器,服务器升级程序远程发送升级包进行升级; 方案 B 为计量主站新建一个专用升级 TCP 端口并在原应用服务器上部署升级程序,利用原来的上行链路进行升级。由于方案 B 对主站服务器存在信息安全风险,需经电网公司严格审核,故常选择方案 A。

表 1 计量终端与电表的控制方案

设备类型	南网费控表	南网 07 表	广西 97 表
南网终端	中继转发	中继转发、写控制参数	中继转发
广西终端	数据转发	通断电控制命令(推荐) 、数据转发	通断电控制命令(推荐) 、数据转发

对南网 07 表,根据技术规范要求,理论上南网终端和广西终端均支持通过数据转发/中继转发和控制命令方式进行远程控制。广西上行通信规约的数据转发功能与南网规约的中继转发的定义大体相同,区别仅在于广西规约未对中继类型进行区分。与广西规约的通断电控制命令不同,南网规约的控制命令是以写测量点控制参数的方式实现的,且补充了测量点和测量点地址匹配验证的功能和控制有效时间的定义。但通过方案 A 升级终端需到现场修改终端 IP,广西部分终端安装在偏远山区,给升级带来困难,目前部分终端存在未及时升级的情况,故广西终端控制南网 07 表以及广西 97 表,推荐优先采用通断电控制命令方式。

广西97表主要应用于国家发改委2008年DL/T 645 – 2007 电能表通信规约实施之前,广西电网根据应用需求对 DL/T 645 – 1997 规约进行增补,自行定义了通断电控制机制,且对密码权限等级没有明确定义,需向电表资产管理方确认控制权限密码等级和密码。且其拉合闸机制与其他电能表不同(见图 1) ,拉合闸时遵循“先告警后控制”机制[7] ,即需先对电表下发产生/解除断电控制告警命令,然后电能表才能响应拉合闸命令。如表 1,由于南网终端规范主要针对南网通用表型制定,未考虑对广西 97 表规约控制机制的兼容性,故南网终端目前不

支持对广西 97 表的写参数控制方式，只能通过中继转发方式实现拉合闸。此外，与南网规范的电能表相比，广西终端上行规约的通断电命令方式有延时控制参数定义，故广西终端对广西 97 表可实现延时拉闸；但广西 97 表的技术规范中无拉闸延时参数定义，南网终端上行规约的写控制参数方式无延时控制参数定义，故南网终端对广西 97 表目前无法实现延时拉闸。

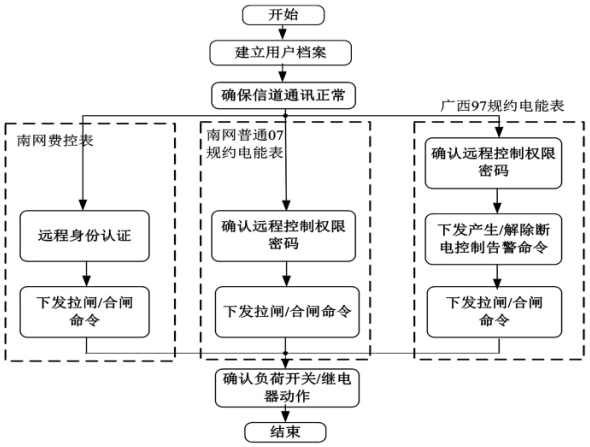

图 1　3 种类型电表的拉合闸流程

如图 1，上述 3 种类型电能表的远程拉合闸流程为：首先由计量自动化系统主站核对用户档案无误且电能表的用电信息数据能正常采集，然后对不同类型的电表采取不同的拉合闸控制方式。

1) 南网费控表：拉闸时首先经计量主站连接密码机获取密钥更新数据和随机数，然后以中继命令的方式对电能表下发远程身份认证指令；电能表内的安全模块对该随机数进行加密，并与主站的加密结果进行密文匹配认证，若身份认证通过，则更新密钥并返回认证信息；接着由主站下发控制命令，电表执行相应动作。此外，当终端收到主站的远程控制命令后，若目标电表具备拉合闸功能，集中器将立即向主站正常应答，而不必考虑受控电能表是否已经真正动作。若目标电能表不具备拉合闸功能，集中器应向主站返回异常应答。接着，在控制生效时间内，终端将下发相应的下行控制命令给目标电表，并持续检测目标电能表的控制状态，若控制执行成功，电能表将更改电能表状态字 3 的继电器状态位；若控制失败，电能表将形成“开关误动作”事件，终端产生“电能表拉合闸失败”告警。可见，主站下发控制命令后，终端回复确认应答，并不一定说明电能表已经成功拉合闸，可参考电能表状态字和终端告警数据确定该状态，最稳妥的做法是去现场确认电能表外置负荷开关或内置继电器的状态。

2) 南网 07 表：在南方电网 2016 年费控表正式推广前应用较广，它支持 6 位密码口令防护，密码分二级管理，出厂默认密码统一为 000000，但各地根据管理需求可能会更改密码，拉合闸前需向资产管理方确认 03 级控制权限密码，它支持主站的写控制参数命令和中继转发下行控制命令两种远程控制方式。

3) 广西 97 表：它对密码权限等级没有明确定义，需向资产管理方确认控制权限密码等级和密码。控制机制为“先告警后控制”机制。

3　案例分析

3.1　拉合闸设备配合情况测试

为研究不同厂家设备通信的兼容性，对 3 个不同电能表通信模块和集中器厂家组合的拉合闸配合情况进行测试，测试地点为某城市居民试点小区，集中器上行通过移动 4G 信号与主站通信，下行通过载波方式与电能表通信。将 3 个厂家的集中器分别与 3 个厂家的载波通讯模块两两组合进行拉合闸测试，反复操作 100 次，记录从命令下发到电能表拉/合闸动作的时间，计算每种组合的平均拉闸时间如图 2 所示，同时可见：1) 集中器并不能支持所有类型的载波模块，即不能实现所有厂家的互联互通，如组合 3，即威胜电气南网规约集中器不识别深圳阳光智慧 SG3000 型载波模块，原因是集中器不兼容国网 1376.2 载波协议的通信模块，从而无法通信。2) 大部分集中器的拉闸平均时间集中在 8 ~ 16 s 范围内，可见该拉闸时间范围可代表该条件下的正常控制响应时间。从整体上看，南网规约集中器拉闸响应速度比广西规约集中器快，但差别不大。3) 组合 2(中电华瑞集中器 + 阳光智慧载波通讯模块) 的平均拉闸时间超过 16 s，原因是这两个厂家的设备载波网络参数匹配性较差[8]，通讯延时较长，建议通过磨合优化组网交互流程。

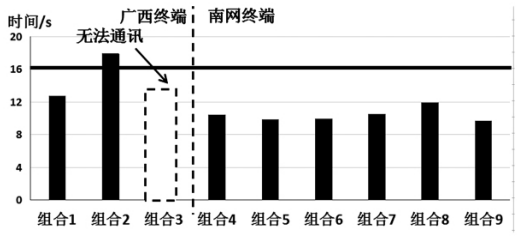

图 2　集中器拉闸响应时间比较

3.2　远程控制异常问题分析

在对计量主站远程控制功能的通讯规约进行调

试时，发现的常见异常问题如下：

1）主站下发抄读电能表运行状态字3后，发现终端返回的数值为FFFF，即不支持该数据项，报文如图3所示。根据南网2013上行规约，应用层功能码AFN分类定义了16种类型的数据采集应用功能，AFN=0AH表示读参数（H表示0A为16进制数据），AFN=0CH表示读当前数据。电能表运行状态字应属于测量点当前数据，AFN应为0CH，图中错误的报文是主站通讯规约研发人员对规范理解有误，认为电能表状态字3属于测量点参数造成的。

异常报文：

主站发送：68 10 00 10 00 68 7B 00 01 45 02 00 00 01 0A 64 04 01 03 05 00 04 43 16 //**主站发送抄读运行电能表运行状态字3命令**

终端回复：68 12 00 12 00 68 98 00 01 45 02 00 00 01 0A 64 04 01 03 05 00 04 FF FF 5E 16

正确报文：

主站发送：68 10 00 10 00 68 7B 00 01 45 02 00 00 01 0C 64 04 01 03 05 00 04 45 16

终端回复：68 12 00 12 00 68 98 00 01 45 02 00 00 01 0C 64 04 01 03 05 00 04 50 C0 72 16

图3 主站抄读电能表运行状态字报文

2）对某批南网费控表（单相表，内置负荷开关）进行拉合闸测试时发现存在负荷开关误动作事件记录异常的问题。根据南网2017年8月对费控电能表拉合闸控制的要求“电能能表拉闸动作时，若第一次检测结果为断路器成功拉闸，电能表持续检测，如检测到断路器误动或拒动，上报并做负荷开关误动作事件记录”。由于电能表只能存储最近10次事件，为避免事件重复生成挤占电能表存储空间[9]，要求电能表“在合闸动作前只记录1次”。

为测试电能表能否满足上述要求，测试方法如表2，电能表在合闸后首先第1次下发拉闸命令，成功收到命令后电能表运行状态字3中的继电器命令状态位b_{RC}变为1，然后短接电能表的强电1和2端子（电流L和N端子），由于此时内置开关的费控电能表继电器状态检测回路检测到费控表的电流回路状态为通，从而误认为没有拉闸成功，将继电器状态位b_R置0，当$b_{RC} \neq b_R$时产生负荷开关误动作事件，事件中记录了负荷开关误动作总次数、发生时刻、结束时刻等。通过这种方式模拟电能表拉闸失败，此时生成1次负荷开关误动作事件，然后再重复模拟电能表拉闸失败2次，检查电能表记录情况。测试发现该功能异常的厂家随着模拟操作次数的增加不断形成开关误动作事件，负荷开关误动作总次数不断增加，从1次增加到3次。而正常厂家的误动作总次数在第1次事件后记录1次，然后在下一次合闸前保持不变。合闸后再进行第2次拉闸，重复上述事件模拟，情况依旧。异常厂家与正常厂家的电能表运行状态字3变化测试情况见表2。

表2 负荷开关误动作事件测试结果

模拟操作		电能表运行状态字3		负荷开关误动作总次数	
		b_R	b_{RC}	厂家1（正常）	厂家2（异常）
合闸		0	0	0	0
第1次拉闸命令下发后	次数1	0	1	1	1
	次数2	0	1	1	2
	次数3	0	1	1	3
合闸		0	0	1	3
第2次拉闸命令下发后	次数1	0	1	2	4
	次数2	0	1	2	5
	次数3	0	1	2	6

3）南网规约的集中器对广西97表拉合闸失败的问题。如图4，根据广西电能表规约要求，电能表进行拉闸，即断电控制时应先产生断电控制报警（数据区控制参数为6D F3），再进行拉闸操作（数据区控制参数为6F F3），此时电能表返回正常应答帧（控制码C=84H）。合闸时应先清除断电控制报警（数据区控制参数为6E F3），再进行通电控制，即合闸操作（数据区控制参数为70 F3）。图4的异常报文未产生断电控制报警就直接进行拉闸操作，故电能表回复异常应答帧（控制码C=C4H），故拉闸失败。

异常报文：

终端发送：68 16 46 70 00 00 00 68 04 06 6F F3 33 33 33 33 D4 16 //**断电控制命令**

电表回复：68 16 46 70 00 00 00 68 C4 01 37 98 16 //**电表回复异常应答**

正确报文：

终端发送：68 16 46 70 00 00 00 68 04 6D F3 33 33 33 33 CC 16 //**产生断电控制告警命令**

电表回复：68 16 46 70 00 00 00 68 84 00 20 16

终端发送：68 16 46 70 00 00 00 68 04 06 6F F3 33 33 33 33 D4 16 //**断电控制命令**

电表回复：68 16 46 70 00 00 00 68 84 00 20 16 //**电表回复正常应答**

图4 广西97规约电能表拉闸报文

4）南网上行规约集中器对南网费控表拉合闸失败的问题。根据南网技术要求，南网费控表拉合闸采用密文方式，但由于南网计量终端目前未有配

置安全模块的技术要求，故计量终端目前无法进行密钥更新，从而无法通过身份认证和生成密文，故无法实现通过写控制参数的方式拉合闸。图 5 中案例的异常报文以明文组成写拉闸控制参数的方式对电表进行远程拉闸控制（信息体数据标识编码 FN = E0001100），终端此时虽然回复确认帧（错误码 = 00），这里仅表示终端收到了正确格式的报文，但电能表实际没有拉闸成功，因为此时终端下发给电能表的是明文方式的拉闸命令，此时返回异常应答帧（错误码 ERR = 37H），对应的错误原因是未授权操作。根据表 1，正确的方式应为中继转发方式且需先进行身份认证。此外，根据南网发布的费控电能表系列技术标准答疑，费控表可通过明文合闸，此时应对应采用 03 级控制密码。

异常报文:

主站发送: 68 34 00 34 00 68 4A 00 01 45 F2 61 1E 0A 04 F0 01 17 00 11 00 E0 83 93 77 00 00 00 03 00 00 00 00 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 08 30 08 19 00 F7 16 // 写控制参数方式发送拉闸命令，明文方式，密级为 03。

终端回复: 68 16 00 16 00 68 88 00 01 45 F2 61 1E 0A 04 E0 01 17 00 11 00 E0 00 08 30 08 19 00 8F 16 // 终端回复确认帧。

终端下发给电表: 68 03 10 00 16 27 12 68 1C 10 36 33 33 33 AB 89 67 45 4D 33 43 64 4A 3A 3B 48 3B 16 // 明文方式的拉闸命令（控制码 C = 1C）。

电表回复: 68 03 10 00 16 27 12 68 DC 01 37 46 16 //异常应答帧。

正确报文:

主站发送: 68 59 00 59 00 68 4A 00 01 45 F2 61 1E 0A 10 F0 00 00 01 00 02 E3 00 1F 08 01 08 00 64 2C 68 37 49 78 02 17 00 68 03 20 32 33 33 3A 33 33 33 33 7E 58 BD 1A 3E 7C 5C C1 24 A7 7D FF 6A AF 85 5B 6A 7C AB 35 4A 33 33 33 0F 16 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 53 09 17 00 58 16 //。中继转发方式发送：身份认证。

终端回复: 68 3D 00 3D 00 68 88 00 01 45 F2 61 1E 0A 10 E0 00 00 01 00 02 E3 00 1C 68 37 49 78 02 17 00 68 83 10 32 33 33 3A 91 00 C2 6F 41 99 84 33 43 64 35 33 A8 16 00 00 00 00 00 00 00 00 00 00 00 00 53 09 17 00 14 16 // 中继回复，认证成功（控制码：C = 83H）

主站发送: 68 55 00 55 00 68 4A 00 01 45 F2 61 1E 0A 10 F0 00 00 01 00 02 E3 01 1F 08 01 08 00 64 28 68 37 49 78 02 17 00 68 1C 1C C9 33 33 33 33 33 33 33 AB 15 C5 2B 22 22 10 17 7F A9 56 68 87 84 4F 45 3A D7 DA B7 89 16 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 53 09 17 00 4C 16 // 中继转发方式发送：拉闸命令。

终端回复: 68 2D 00 2D 00 68 88 00 01 45 F2 61 1E 0A 10 E0 00 00 01 00 02 E3 01 0C 68 37 49 78 02 17 00 68 9C 00 7D 16 00 00 00 00 00 00 D6 56 83 33 03 53 09 17 00 94 16// 终端回复电表的中继报文，报文中电表做正常应答

图 5　南网费控表拉闸报文

4　结　语

随着广西电网计量自动化“两覆盖”和计量信息安全防护体系建设的深入，通讯协议多元化计量设备的接入将对计量系统功能的正常发挥带来新的问题。前面分析了广西电网常见的电能表和计量终端远程控制通信协议的特点，并给出了推荐控制方案和流程。接着通过实例分析了不同通信模块和集中器厂家组合的拉闸平均响应时间的差异特点，最后对开关误动作事件异常、拉合闸机制不匹配、安全认证失败等异常问题进行了通讯报文的实例分析。可见，只有提高运维人员的规约解析能力和故障分析水平，准确识别和处理故障，才能确保用户的正常用电。

参考文献

[1] 胡飞雄，周保荣，卢斯煜. 南方电网促进可再生能源消纳的实践及发展展望[J]. 中国电力，2018，51(1)：22－28.

[2] 梁捷，李刚，黄柯颖. 费控电能表费控功能检测中的若干问题分析[J]. 广西电力，2017，40(6)：44－48.

[3] 梁捷. 基于椭圆曲线加密的电能表数据传输系统设计[J]. 工业仪表与自动化装置，2018(5)：112－114.

[4] 中国南方电网有限责任公司市场营销部. 中国南方电网有限责任公司多功能电能表通信协议扩展协议：Q/CSG 1130－2011[S]，2015.

[5] 梁捷. 基于 ZigBee 的电子式电能表能耗研究[J]. 青海电力，2018，37(2)：41－44.

[6] 梁 捷，李 刚. 计量终端自动化功能测试系统的功能测试研究[J]. 电气应用，2017，36(3)：83－87.

[7] 白俊然. 智能预付费电能表的应用及修校技术探究[J]. 通讯世界，2017(17)：232－233.

[8] 张皓岚，贺慧英，陈涛，等. 舰船电力载波通信的阻抗匹配设计[J]. 电力系统保护与控制，2014，42(2)：104－110.

[9] 张一利. 基于智能电表的电力机车能耗管理优化系统[J]. 山东工业技术，2015(24)：114－114.

作者简介:

梁　捷(1987)，工学硕士，工程师，主要从事电能计量管理方面的工作。

(收稿日期: 2019－04－28)