

某 110kV 智能站遥测及通讯异常分析

曾 飞，张小易，袁宇波，彭志强

(江苏省电力公司电力科学研究院，江苏 南京 211103)

摘 要：某 110 千伏智能站自投运以来，在调度主站 EMS 经常出现 10kV 母线电压由 10 点几变成整数 10 的取整现象，且 10kV 母线电压数据刷新缓慢；此外，站内 A 厂商的保护测控一体装置在与 B 厂商的监控后台、远动机通讯的过程中，出现不定期通讯中断，然后又恢复的情况。经过对调度主站与远动机、监控后台与保测装置在遥测及通讯异常时间段的交互报文进行分析，找出了异常原因。最后给出了解决问题的建议，并在基础模型构建上提出根本解决此类问题的探讨。

关键词：智能变电站；保测一体装置；调度主站；监控后台

1 异常现象一：10kV 母线电压遥测值跳变取整

1.1 异常描述

某 110kV 智能站电站自投运以来，在调度主站 EMS（型号为 OPEN-3000）经常出现 10kV 母线电压由 10 点几变成整数 10 的现象。表 1 为 10 月 24 日 OPEN-3000 系统 10kV I 段母线电压一分钟采样值，图 1 为当日电压曲线。

表 12013-10-24 OPEN-3000 系统 10kV I 段母线电压

时	分	10kVII 母线电压幅值	状态
17	30	10.54	正常
17	31	10.54	正常
17	32	10.56	正常
17	33	10.56	正常
17	34	10.56	正常
17	35	10.00	不变化
17	36	10.00	不变化
17	37	10.00	不变化
17	38	10.00	不变化
17	39	10.00	不变化
17	40	10.55	正常
17	41	10.55	正常

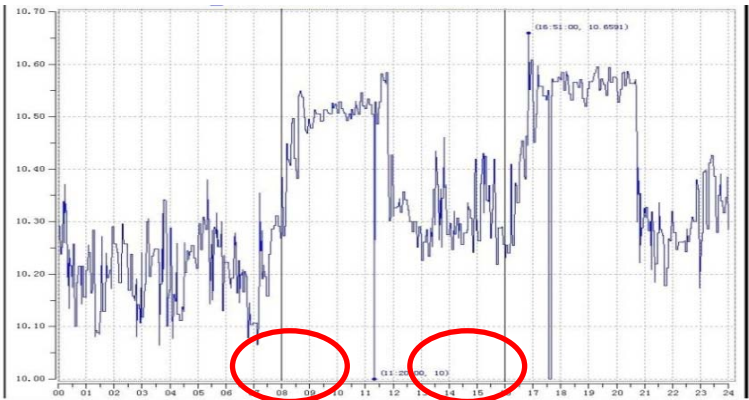


图 1 电压跳变时刻 OPEN-3000 曲线截图

1.2 异常分析

为分析是调度主站原因还是厂站远动装置原因导致电压跳变异常，需同时对主站与厂站的数据进行监视。

10 月 22 日 XX 市调度控制中心联系 B 厂商完成了如下检查工作：在该智能站远动装置上加装一套监视软件，该软件每 30 秒监视一次 10kV 母线

电压值，同时母线电压发生抖动的时候，进行记录此时的电压数据。10 月 22 日至今为止，从该软件记录看，未发现该智能站母线电压有抖动现象。

同时，在 OPEN-3000 调度主站侧，对该智能站的报文进行保存，并每 30 秒打印出 10kV I 段母线 U_a 、 U_b 、 U_c 、 U_{ab} 、 U_{bc} 和 U_{ca} 的值，且如有 0.4kV 的突变，则打印出相应电压记录，在主站侧

微小波动而装置上送的遥测数据不刷新。经沟通，B 厂商将死区数值重新调整，由 0.5% 修改为 0.2%。将修改程序发到现场升级后，从 OPEN-3000 观察，电压数据刷新缓慢问题有所改善。

3 异常现象三：保测一体装置与监控后台、远动机不定期通讯中断

现场问题描述

A 厂商保护测控装置在与 B 厂商监控后台、远动机通讯过程中，出现间隔不定期时间（几天、几小时间隔时间不等）报与 B 厂商监控后台和远动机通讯中断的信号，然后过一段时间又恢复的情况。

经过 A 厂商对通讯中断时间段的交互报文进行分析，通信中断信号产生的直接原因为 B 厂商监控后台发送的 61850 心跳报文，A 厂商保护测控装置没有及时回复，发生了报文回复迟滞的情况，

B 厂商监控后台发现报文没回复判为通讯中断。

3.1 问题分析

关于 IEC61850 装置心跳报文的两点说明：

1) IEC61850 MMS 通讯协议本质上是 tcp/ip 通讯，是一种在 102 端口进行的 tcp 应用^[2]。装置作为 tcp server，监控后台系统是 tcp client。由 client 端主动发起 tcp 连接。

2) IEC61850 MMS 的通讯协议本身没有心跳报文的说法。client 端为了确保通讯通畅，采用读取装置中某一个 ref 值的方式进行。

分析文件“0-6-01-20130618072316.pcap”的通信全过程，发现 1 号主变低压二侧保护与监控后台通信异常状况如下（以下过程描述仅限于此文件中的报文）：

1) 由图 3，监控后台(10.10.5.201)以读服务器目录服务作为判断通信正常与否的判据，周期为 15s。

[读服务器目录GetServerDirectory-Request]confirmed-RequestPDU	1号主变低压二侧保护	IP-10.10.5.201	IP-10.10.5.75	104	2013-06-18 15:24:23.1610379880
[读服务器目录GetServerDirectory-Response+]confirmed-ResponsePDU	1号主变低压二侧保护	IP-10.10.5.75	IP-10.10.5.201	66	2013-06-18 15:24:23.2104764416
报告 - [遥测] (数据改变-本侧测量A相电压)	1号主变低压二侧保护	IP-10.10.5.75	IP-10.10.5.201	153	2013-06-18 15:24:23.243189416
报告 - [保护遥测] (数据改变-本侧A相电压)	1号主变低压二侧保护	IP-10.10.5.201	IP-10.10.5.75	66	2013-06-18 15:24:23.123014584
		IP-10.10.5.75	IP-10.10.5.201	529	2013-06-18 15:24:27.1974093480
		IP-10.10.5.201	IP-10.10.5.75	66	2013-06-18 15:24:27.1668923480
		IP-10.10.5.75	IP-10.10.5.201	326	2013-06-18 15:24:27.1840607520
		IP-10.10.5.201	IP-10.10.5.75	66	2013-06-18 15:24:27.2145777520
		IP-10.10.5.201	IP-10.10.5.75	66	2013-06-18 15:24:32.406270520
		IP-10.10.5.201	IP-10.10.5.75	66	2013-06-18 15:24:35.711478520
		IP-10.10.5.201	IP-10.10.5.75	66	2013-06-18 15:24:38.1294675776
[读服务器目录GetServerDirectory-Request]confirmed-RequestPDU		IP-10.10.5.201	IP-10.10.5.75	104	2013-06-18 15:24:38.323709808

图 3 监控后台判断通信正常与否的时间周期为 15s

1 号主变低压二侧保护测控装置(10.10.5.75)的交互报文包括监控后台请求的读服务器目录服务(心跳报文，请求应答双向报文)和数据改变触发的报告(多为遥测数据集以及保护遥测数据集触发，

单向报文)；总体的报文流量不是很大；心跳周期的请求应答报文占很少一部分。遥测报告触发的周期比较均匀，约为 8s。

报告 - [遥测] (数据改变-本侧测量A相电压)	1号主变低压二侧保护	IP-10.10.5.75	IP-10.10.5.201	529	2013-06-18 15:24:27.1974093480
报告 - [保护遥测] (数据改变-本侧A相电压)	1号主变低压二侧保护	IP-10.10.5.201	IP-10.10.5.75	66	2013-06-18 15:24:27.1668923480
		IP-10.10.5.75	IP-10.10.5.201	326	2013-06-18 15:24:27.1840607520
		IP-10.10.5.201	IP-10.10.5.75	66	2013-06-18 15:24:27.2145777520
		IP-10.10.5.201	IP-10.10.5.75	66	2013-06-18 15:24:32.406270520
		IP-10.10.5.201	IP-10.10.5.75	66	2013-06-18 15:24:35.711478520
		IP-10.10.5.201	IP-10.10.5.75	66	2013-06-18 15:24:38.1294675776
[读服务器目录GetServerDirectory-Request]confirmed-RequestPDU		IP-10.10.5.201	IP-10.10.5.75	104	2013-06-18 15:24:38.323709808
		IP-10.10.5.201	IP-10.10.5.75	104	2013-06-18 15:24:39.2098561864
		IP-10.10.5.201	IP-10.10.5.75	104	2013-06-18 15:24:39.2043872448
		IP-10.10.5.201	IP-10.10.5.75	104	2013-06-18 15:24:40.1466515120
		IP-10.10.5.201	IP-10.10.5.75	104	2013-06-18 15:24:42.125155632
		IP-10.10.5.201	IP-10.10.5.75	104	2013-06-18 15:24:45.1575296720

图 4 1 号主变低压二侧保护触发一个保护遥测报告后不再有任何报文回应

2) 问题时间：由图 4，15:24:27，1 号主变低压二侧保护触发一个保护遥测报告后，不再有任何报文回应，即应用层的周期性(周期约为 8s)遥测报告触发报文没有出现，TCP/IP 底层的 TCP-Keep-

Alive 报文也没有回应；即从 15:24:32 到 15:24:51 这 19 秒的时间段内没有发现 1 号主变低压二侧保护的任

可能的原因有：保护装置的自身问题，或是交换机的原因。

如果是保护装置的问题，则这种现象从技术层面分析应该是装置系统级的没有回应，如装置系统重启、系统挂起或是 TCP/IP 协议栈问题。从下面第 3 点的分析看，系统重启的原因可以排除。

如果是交换机的原因，则可能是由于镜像不完整，或是与装置相连的通信口有问题导致的。目前从报文过程还无法理清原因所在。

3) 由图 5，监控后台在上一个请求服务器目

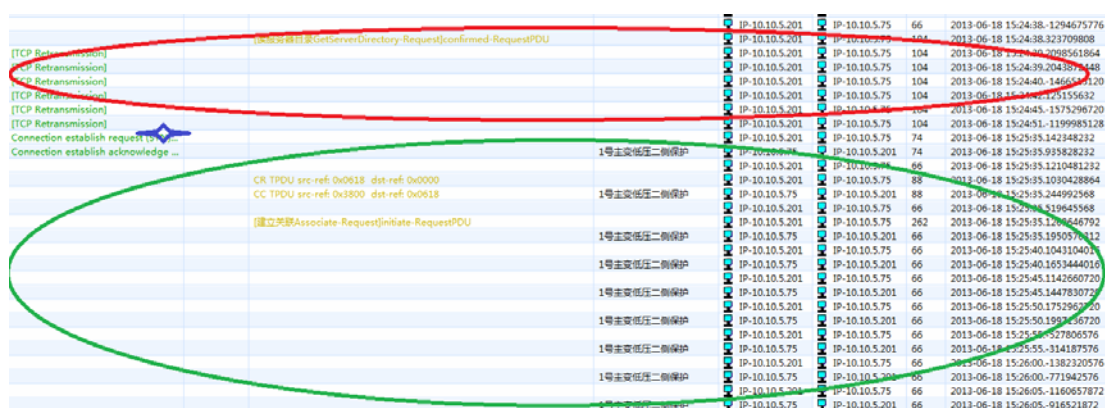


图 5 监控后台重新请求建立关联服务但 1 号主变低压二侧保护的应用层服务一直未恢复

4) 由图 5，从问题发生(15:24:38)到报文结束(15:26:05)这段 87s 的时间，从报文上看 1 号主变二侧保护的应用层服务包括遥测报告触发在内，一直没有恢复。A 厂商自描述的自检机制为 60~90s，由于没有后续报文，不能确认是否存在这样的机制。A 厂商又描述“一般可能是现场报文量比较大时，可能会出现板件网口缓冲队列缓存的一些报文，在缓冲区中排队等待，没及时解析处理，此时为了及时处理报文，需要提高系统中网口处理的优先级，加速报文的回复”；从通信过程看，该装置的报文量不大(15 秒才周期性的收到心跳请求报文)；而且它的周期性数据改变触发的遥测报告报文也没有出现；A 厂商所描述的问题只是接收缓冲的机制，装置自身触发的报告和接收缓冲没有关系，只与发送缓冲有关；从这些现象应该可以确认装置的应用层处理是有问题的，比如死锁。

3.2 建议

1) 报文回复迟滞的原因，有可能是因为管理板上的 CPU 在处理其它任务，调用和消耗了大量的系统资源，导致系统没有对网口报文进行及时处

理。若不是这种情况，则可能是程序存在 BUG，A 厂商需要对此进行更加深入的分析，明确原因。

2) 在条件允许的情况下考虑延长监控后台系统监测装置 MMS 服务（即心跳）的间隔。根据华东电网公司 2008 年的测试，建议心跳检测周期为 15-30s。

3) 由图 5，当监控后台认为和装置通信中断后，大概 1 分钟后建立了新的连接。但是从报文过程看没有看到监控后台主动关闭 TCP 的过程（应该在蓝色星处），那么原来的 TCP 资源就一直被占用，直到程序退出或系统重启。设想如果站内有大量的这样的通信中断，最后都由于某种异常，导致有大量的 TCP 资源没被释放，最后造成的结果就是 TCP 资源耗尽，新的 TCP 连接无法建立，后续通信瘫痪。

3.3 探讨

监控后台以周期性请求服务器目录作为心跳周期来验证通信是否正常，这个也是目前没有统一规范的做法，可能每个监控后台厂商解决方案都不一致。TCP/IP 层自身的保持激活(TCP Keep-Alive)只

是维护操作系统底层协议的连接状况，并不能反映其上层协议的状况；当然要解决这个问题，需要监控后台与保护装置共同努力，比如在模型上构想建立一个装置自身健康状况报告块，通过周期性的上送这个报告块作为一个心跳报文，如果监控后台在 2 个周期内收不到这个心跳报文，则认为装置通信中断

参考文献：

- [1] 国家电网公司人力资源部.电网调度自动化主站运行[M].北京:中国电力出版社,2010.
- [2] 冯军.智能变电站原理及测试技术[M].北京:中国电力出版社,2011.

版社,2011.

作者简介：

曾 飞（1984-），男，通信作者，从事继电保护、调度自动化相关生产、科研工作， E-mail：15105168878@163.com；

张小易（1978-），男，高级工程师，从事电力系统继电保护、调度自动化相关生产、科研工作；

袁宇波（1975-），男，博士，高级工程师，从事电力系统继电保护相关生产、科研工作；

彭志强（1987-），男，从事智能变电站自动化专业的生产、科研工作。