通信规约实现与系统可靠性、安全性

姚致清

（许昌继电器研究所，河南 许昌 461000）

摘要：随着电力系统自动化技术的发展，通信已经成为各个系统的重要组成部分，承担了信息传递和命令传递的任务，随着IEC61850等规约的发展，通信成为整个系统的关键，不光完成信息的传递，还成为系统功能、甚至保护功能的基础。因此通信规约的实现就越来越成为影响系统可靠性、安全性的重要问题，笔者通过多年与荷兰KEMA公司规约测试合作的经验，总结出一些影响系统可靠性、安全性的问题，拿出来与大家分享，并希望能引起广大制造企业的共鸣，一起提高电力自动化产品的质量。

关键词：通信；规约；规约测试；可靠性

The relationship between communication protocol and system reliability and safety

YAO Zhi-qing

(Xuchang Relay Research Institute, Xuchang 461000, China)

Abstract: With the development of electric power system automation technology, the communication has become an important part of varied automation systems. It bears the tasks of transferring the information and command, with the practice of IEC 61850. The communication became a more important part, not only transferring the information and command, but also becoming the basis of system function, such as protection function. The realization of the communication protocol becomes a big problem that affect the reliability and safety of automation system. With several years corporation between KEMA and NCQTR in protocol testing, this paper summarizes some influencing factors on reliability and safety, and shares with readerss, we hope it could arouse some resonance of some manufacturers, and improve the quality of automation product.

Key words: communication; protocol; protocol testing; reliability

中图分类号：TM73；TM764 文献标识码：B 文章编号：1003-4897(2008)06-0068-03

0 引言

随着电力系统自动化技术的发展，通信已经成为各个系统的重要组成部分，承担了信息传递和命令传递的任务，随着IEC61850等规约的发展，通信成为整个系统的关键，不光完成信息的传递，还成为系统功能、甚至保护功能的基础。因此通信规约的实现就越来越成为系统可靠性、安全性的重要问题，笔者通过多年与荷兰KEMA公司规约测试合作的经验，总结出一些影响系统可靠性、安全性的问题，拿出来与大家分享，并希望能引起广大制造企业的共鸣，一起提高电力自动化产品的质量。

1 电力系统通信规约现状

从20世纪90年代开始，IEC TC57致力于IEC60870系列标准的制定，随着一系列基本标准与配套标准的发布，原本处于混乱局面的变电站自动化系统通信协议逐步趋于统一，制造商与用户都可以从五花八门的通信协议中解脱出来。但由于IEC60870系列标准的制定周期较长（超过10年），各方面对该系列标准的理解与应用情况很不平衡。就我国而言，各用户与厂家对应用IEC60870系列标准投以极高的热情，但标准的应用经历了先配套标准、后基本标准的过程，虽然该系列标准在我国已广泛应用，在很多地区已成为主导性通信标准，但对标准的理解特别是对通信过程的理解存在差异，从而在不同厂家设备互连时出现了或多或少的问题。

目前在电力系统中，远动大量地使用CDT规约，在有些中调系统中采用DNP3.0规约，目前101、

104 规约也越来越多地出现在远动 SCADA 系统中为调度主站提供通信服务，在保护装置中大量使用 103 规约与变电站自动化系统进行通信，在低压领域 MODBUS 以其简单、有效的特点成为比较常用的一种通信规约，在新出现的继电保护故障信息系统[2]中，采用《中国南方电网继电保护故障信息系统通信与接口规范》，这个规范采用了 104 的 APCI 机制和 103 规约的应用层报文结构，并进行了一定的扩充定义。

2　通信及规约在系统中的作用

通信规约在自动化系统中起着越来越重要的作用，总结起来有如下作用：

1) 监视，通过遥测、遥信等信号监视变电站或者其他装置、子系统的工作情况；

2) 控制，通过遥控、遥调等操作控制远方或者装置、子系统的工作；

3) 系统配置，通过参数配置报文或者定值下装报文来修改远方子系统或者装置的参数；

4) 分布功能，在 61850 系统中，有些保护、自动化功能需要通过通信提供数据和信息，如过程层通过数字 PT、CT 提供数字化的电压、电流等数据给保护、测控等装置，有些自动化功能通过装置间通信交换信号和数据完成。

3　规约测试工作中发现的问题

案例 1：MODBUS 写操作引起装置不能启动

现象：主站利用功能码 06 写寄存器值，当主站写入的寄存器地址超出子站允许的范围时，这时子站正常响应，并进行了修改，结果装置不能正常启动。

原因：在通信规约层面是没有问题的，但是从 MODBUS 通信规约的地址空间向装置地址空间映射过程中未进行地址范围检查，这样当进行超地址范围的写操作时，数据就被写入到装置的其他地址空间，如果这个空间正好是配置数据时，配置数据就可能被覆盖，这样装置不能正常启动。

案例 2：104 规约中 STARTDT 启停机制和定时器处理不当、导致子站中断重连后不能通信

现象：在主站、子站正常通信过程中，如果子站重新启动后，主站虽然能与子站建立 TCP 连接，但是不再发 STARTDT 命令，导致子站不能上送数据。

原因：有的企业 104 规约在实现时分 2 部分，一部分处理底层 TCP/IP 连接，一部分处理 104 规约，当 TCP 连接中断后，底层自动重连，但未能及时将这一变化告知 104 规约应用层，这样本应该发送 STARTDT 命令，却由于不知道底层重连这一变化，所以应用层不能发送，而子站重新启动后要等待主站发送 STARTDT 命令才能开始 I 帧传输，所以子站就不能发送数据，必须到主站重新启动。

造成这一问题的原因还有就是发送序列号和接收序列号处理、检查不严格导致，因为当主站发送一个 I 帧后会启动 T1 定时器，这时由于子站不能进行确认，因此主站 T1 会超时，这样主站应该挂断 TCP 连接，然后重新建立连接，主站和子站就能够正常通信，但是由于主站在检查 T1 定时器时不严格，导致主站不轻易挂断连接，造成主站、子站不能进行 I 帧通信。

案例 3：在 103 规约 RII 和 SCN 不正常使用导致的问题

现象：在多次总召唤/总查询过程中，状态发生变化，但是总召唤完毕后，当前状态与实际现场状态不一致。

原因：在 103 规约中，使用 SCN 扫描序列号和 RII 返回信息标识来区分不同批次的数据，有些厂家对这些信息不检查，这样在同时有多个总查询/总召唤命令存在的情况下，同一个点的信息有多个报文，当信号有变化时，状态会不一样，由于在接收处理过程中不能对 SCN 或者 RII 号进行检查，导致最终状态不是现场实际状态。

案例 4：104 规约中，子站未合理使用流控制机制，导致主站通信缓冲区溢出，丢失数据

现象：当子站有大量数据上送时，尤其是文件传输等操作，主站经常发生丢失报文的现象，导致文件传输失败，或者丢失数据，严重时由于缓冲区溢出导致主站故障。

原因：在 104 规约中，主站和子站通过对发送序列号和接收序列号的判断和确认机制来控制对方发送数据的速度，也就是规约中的 K、W 参数，一般为 12 和 8。由于主站不能严格按照这一参数进行确认，子站也不按照这一机制发送数据，导致发送的数据量超过主站缓冲区大小，这样就会发生上面所说的现象，另外在工程中也要根据主站、子站的能力来配置 K、W 值，并且严格按照这一机制工作，这样才能保证主站和子站数据传输不重复、不丢失。

案例 5：透明文件传输给系统安全性带来危害

现象：在南网 103 规约实验中，透明文件传输可以指定文件路径，这样就可以给对端系统发送一个病毒、或者覆盖一个系统文件，造成对端系统受到侵害。

原因：在规约设计之初未考虑这个情况，在允

许指定路径的情况下，通过规约可以将一个文件写到任何一个目录下，这样会降低系统的安全性，给系统留下一个后门，存在安全隐患。

案例 6：时钟同步报文中时间值不合理，导致装置异常

现象：在时钟同步报文中，当给装置下发一个不合理的时间信息，如 2007 年 13 月 5 日 10 时 50 分 68 秒时，装置接受时间，并显示在装置人机接口上，发现时间显示异常，然后做一个保护动作，发现上送时标也不正确。

原因：装置对时间值的有效性判定不严谨，导致在错误时间值下进行了错误的操作，从而影响了装置的时间系统运行。

4 如何提高通信规约的实现水平

通过多年规约测试和现场工作经验总结，我们认为，要想提高通信规约实现水平要从如下方面做好工作：

1) 按照国际、国家、行业标准实现产品规约；

2) 认真学习标准、并与同行业厂家积极进行交流，充分理解标准；

3) 科学地、严谨地按照规约标准的要求设计产品，并合理地将产品功能与通信规约进行映射和协调；

4) 在使用标准的同时，要结合不同地区、不同电网的规约应用要求进行考虑，使产品能够灵活地适应这些地区规范；

5) 在规约产品开发完毕后，到专门检测机构进行规约测试工作，通过规约测试可以发现规约产品中实现的不完善之处，同时能够加深对规约的理解和应用；

6) 对规约软件进行严格的版本管理，做到不轻易改动、改动后要进行测试。

7 结论

随着 61850、61970 标准的颁布和执行，通信在系统中的作用越来越重要，为了全面提高电力系统可靠性和安全性，必须在自动化产品通信功能、通信规约上加强实现力度和检测力度，使整个电力自动化系统成为一个健康、稳定的系统，保证电力生产持续、稳定发展。

参考文献

[1] 杨剑峰,贺春.规约应用中存在的问题及解决方法的探讨[J].继电器，2004, 32(19)：71-73.
YANG Jian-feng, HE Chun. Problems and Solutions in Protocol Implementation[J].Relay, 2004 ,32(19):71-73.

[2] 赵有铖，赵曼勇,贺春.继电保护故障信息系统建设经验谈[J].继电器，2006, 34(6):64-66,70.
ZHAO You-cheng, ZHAO Man-yong, HE Chun. Experience in the Project Construction of Fault Information System for Relay Protection[J]. Relay, 2004, 34(6):64-66,70.

[3] 贺春,任春梅,张冉.MODBUS 协议在电动机保护装置中的应用[J].继电器，2006,34(12):73-76.
HE Chun, REN Chun-mei, ZHANG Ran. Application of Modbus Protocol in Motor Protection Equipment[J]. Relay, 2006,34(12):73-76.

[4] IEC60870-5-104 Telecontrol Equipment and Systems Part 5:Transmission Protocol Section104:Network Access for IEC 60870-5-101 Using Standard Transport Profiles[S].

[5] 中国南方电网有限责任公司.中国南方电网继电保护故障信息系统通信与接口规范[S].

收稿日期：2007-08-20； 修回日期：2007-10-25

作者简介：
姚致清（1960-），男，EMBA，高级工程师，主要研究方向为特高压直流输电、特高压交流输电，系统可靠性。

（上接第 67 页 continued from page 67）

LU Guang-yin,HAN Xu-li, ZHU Zi-qiang,et al. Synthetical Evaluation and Classification Model of Geological Hazards[J]. Journal of Central South University of Science and Technology, 2005,36(5).

[4] 王成山，王赛一.基于空间 GIS 的城市中压配电网络智能规划[J].电力系统自动化,2004,28(5):45-50.
WANG Cheng-shan, WANG Sai-yi.Intelligent Plan of City Power Distribute Grid Based on GIS[J]. Automation of Electric Power Systems, 2004,28(5):45-50.

[5] 陈述彭，鲁学军，周成虎.地理信息系统导论[M].北京:科学出版社,2000.
CHEN Shu-peng, LU Xue-jun, ZHOU Cheng-hu. GIS An Introduction[M].Beijing:Science Press,2000.

[6] 冶成斌.专业的 Utility 逻辑示意图解决方案[J]. ESRI 中国通讯,2005,15.
YE Cheng-bin. Professional Blue Print of Logic Sketch Map[J].ESRI China Communication,2005,15.

收稿日期：2007-08-21； 修回日期：2007-11-15

作者简介：
李晓凯（1975-），男，本科，工程师，研究方向为电厂电气自动化；E-mail:shandlxk@yahoo.com.cn

周长建(1977-)，男，本科，助理工程师，研究方向为电力系统自动化；

许和炎（1975-），男，硕士，工程师，研究方向为地理信息系统及应用。