

以太网 IP 层及链路层通信技术在变电站综自系统的应用

魏勇¹, 郭赞², 马力³, 李志超¹

(1. 许继电气股份有限公司, 河南 许昌 461000; 2. 许昌市高级技工学校, 河南 许昌 461000;
3. 河南省许昌供电公司, 河南 许昌 461000)

摘要: 分析了以太网两种常见的通信技术应用模式: 基于数据链路层的应用及基于 IP 层的 TCP/UDP 传输方式应用, 比较了他们之间的差别, 给出了各自的应用场合, 并针对变电站自动化系统的主要业务进行了通信层面的业务分析, 结合 CBZ-8000A 系统中 IEC 60870-104 及 IEC 60870-103/TCP 的通讯网络技术应用情况进行了具体说明, 对数字化、智能化变电站围绕 IEC 61850 的通讯技术发展方向进行了探讨。

关键词: 变电站通信; IEC 61850; TCP/UDP 传输; IEEE 802.3; 数据链路层

Application of IP layer and data link layer communication technology in substation automation system

WEI Yong¹, GUO Bin², MA Li³, LI Zhi-chao¹

(1. XJ Electric Corporation Limited, Xuchang 461000, China; 2. Xuchang Advanced Technical School, Xuchang 461000, China;
3. Xuchang Power Supply Company, Xuchang 461000, China)

Abstract: This paper analyzes the two common Ethernet communication technology application modes, one is based on data link layer, and the other is based on TCP / UDP transmission mechanism in IP layer. The paper compares the differences between them, and gives their respective application situation, and conducts an analysis of substation automation system's primary business in view of communication business combining with the application of IEC 60870-104 and IEC60870-103/TCP network technology of CBZ-8000A system. Finally, the development trend of digital and smart substation communications technology such as IEC 61850 is also discussed.

Key words: substation communication; IEC 61850; TCP/UDP transmission; IEEE 802.3; data link layer

中图分类号: TM764 文献标识码: B 文章编号: 1674-3415(2010)16-0143-04

0 引言

近些年, 变电站自动化系统网络通信技术的应用得到了长足的发展, 站内的通信网络由原来的串行方式, 如 RS-485 等, 及现场总线方式, 如 LonWorks、CAN 等统一发展到工业以太网方式, 无论是从通信传输速率、带宽、通信设备成本、网络物理拓扑结构, 还是通信交互方式(问答式的非平衡 POLLING 模式发展到平衡式主动/定时上送模式)、系统开放互连性都体现出了极大的益处^[1-3]。变电站以太网网络的信息传输方式从 OSI 协议栈分层模型的传输控制层来区分基本有两种工作模式: 基于流传输的 TCP (Transportation Control Protocol, TCP) 方式和基于包传输的 UDP (User Data Packet, UDP) 方式^[4]。最新的数字化变电站系统中, 还引入了过程层的概念, 为实现快速实时性, 采样值

SMV 和状态量 GOOSE 信息采用了将通信直接透传映射到 OSI 分层模型的第二层(数据链路层)^[5]。

本文分析了以太网通信常用的 IP 层通信技术和数据链路层通信技术, 重点比较了 IP 层通信技术和 TCP/UDP 传输方式的差异及各自适用的业务领域, 以及链路层通信技术主要应用领域, 围绕变电站自动化系统的主要业务进行了通信层面的应用分析, 最后结合变电站自动化技术的发展方向, 分析了数据链路层通信技术在数字化、智能化变电站过程层实时通信传输业务领域的应用。

1 基于 IP 层的 TCP 及 UDP 通信技术

TCP 和 UDP 是 TCP/IP 协议中的两个传输层协议, 它工作在 OSI 分层模型的 IP 层之上, 使用 IP 路由功能把数据包发送到目的地, 从而为应用程序及应用层协议(包括: HTTP、FTP、SMTP、SNMP

和 Telnet) 提供网络服务。TCP 提供的是面向连接的、可靠的数据流传输, 而 UDP 提供的是非面向连接的、不可靠的数据报文传输。

面向连接的协议在数据开始传输前即建立了点到点地连接。需要注意的是面向连接不专指传输层的传输方式, 如 ATM 和帧中继是面向连接的协议, 但它们工作在数据链路层, 而不是在传输层。另外, 普通的音频电话也是另一层面的面向连接。

1.1 TCP 传输方式

TCP 是一种可靠的传输协议, 可从机制上有效避免数据传输错误。具体实现方式是: 在构造数据包时在其中定义校核码, 到达目的地后再采用特定的算法重新计算校核码, 通过比较二者的差异, 就可以发现被破坏了的数据。因为此过程需要重发被破坏和丢失的数据, 所以在重发数据时协议必须能够使信宿给出信源的一个确认信号。考虑到部分数据包不一定按照顺序到达, 所以协议必须具备探测出乱序的数据包能力, 先把这些数据临时暂存起来, 然后把它们再依照正确的次序送到应用层。另外, 协议还必须能够找出并丢弃重复发送的数据。一组定时器可以限制针对不同确认数据帧的等待时间, 这样就允许开始重新发送或重新建立连接。

由于 TCP 传输模式属于数据流传输模式, 所以不支持位传输方式, 不能在一个包内以字节或位为单位构造数据, 它只负责传输未经构造的 8 位字符串。

总结起来, TCP 的工作过程类似打电话, 存在大量的握手联络交互过程, 这在通信上叫做信令控制信号, 多少会带来一定的“overhead”开销, 但却可以确保通信质量。

1.2 UDP 传输方式

UDP 是一种非面向连接的传输协议, 这种传输模式在数据传输之前并不建立连接, 而是在每个中间节点对非面向连接的数据包进行路由。没有点到点的连接, 所以是一种不可靠的连接。当一个 UDP 数据包在网络中传输时, 发送者并不知道它是否已经到达了目的地, 除非应用层发出确认它已到达的信息。非面向连接的协议也不能探测到重复的和乱序的数据包。标准的专业术语用“不可靠”来描述 UDP。在现代通信网络环境中, 虽然 UDP 并不易于导致传输失败, 但是即使这样也不能肯定地说它是可靠的。

1.3 TCP 及 UDP 方式的选择

当数据传输的性能必须让位于数据传输的完整性、可控制性和可靠性时, 应当选择 TCP 模式。当强调传输性能而不是传输的完整性时, 如: 音频和多媒体应用, 应当选择 UDP 模式, 当前互联网上得

到广泛应用的流媒体业务就是采用 UDP 传输模式。另外, 在数据传输时间很短, 以至于此前的连接过程成为整个流量主体的情况下, 也应当选择 UDP 方式, 比如通信业务中常见的“握手”、“心跳”信息传递也采用 UDP 传输模式。

从技术发展及应用情况分析, TCP 可靠的点对点连接将会用于绝大多数的网络应用。

基于 IP 层通信应用一般基于 socket 实现, 在 windows 操作系统上有封装好的 winsock 库, 使用简单、方便。

2 基于数据链路层的通信技术

数据链路层 (Data Link Layer) 位于 OSI 网络协议栈模型的物理层与网络层之间, 它是 OSI 中比较重要的一层, 数据链路层在物理层提供的服务的基础上向网络层提供服务, IEEE 802.3 协议定义了以太网物理层和数据链路层的技术标准。

由于数据链路层位于网络层之下, 因此基于数据链路层的通信协议的传输效率比较高, 实时性好。基于 IEEE 802.3 以太网链路层的通信应用要比基于以太网上层网络协议的 TCP/IP 通信应用传输效率高, 缺点是灵活性、开放互联性差。基于该通信技术的典型应用当属“设备发现”, 主要用途是进行网络设备初始化时, 网络上层信息如 IP 地址等自动分配部署, 动态调整等, 另外还用在高实时性信息传递, 如 IEC 61850 通信体系中的 SMV 及 GOOSE 信息传递, 以及高精度的网络对时 (PTP1588 V2 在支持 IP 层通信映射实现的基础上, 还支持 IEEE 802.3 的通信映射实现)。

基于 IEEE 802.3 以太网数据链路层通信应用一般基于 RawSocket 实现, pcap 是个开源的第三方 RawSocket 开发库, 在 windows/linux/unix 等操作系统上均有封装好的库可直接使用。

3 变电站自动化系统通信技术的应用分析

变电站自动化系统信息传输的最重要特点是可靠性, 不丢包, 其次是快速实时性, 满足各种基于网络通信的分布式功能实现及信息远传要求。在数字化、智能化变电站领域, 由于在过程层采用了光通信及交换式以太网技术来实现采样值的快速上传, 及 GOOSE 跳合闸、联锁信息快速传递, 所以对于快速性和实时性有了更迫切的要求。

3.1 主要通信业务

变电站自动化系统需要进行通信的业务目前主要有: 远动四遥信息, 继电保护动作信息, 故障录波信息, 逻辑互锁信息、遥视信息, 变电运行管理

信息,站控层功能主站间通信信息,IED 设备固件加载、地址分配等设备管理信息,对时信息,网络设备通用管理信息(一般基于 SNMP 简单网络管理协议)等。

3.2 通信业务分析

远动四遥信息和继电保护动作信息要求非常可靠,对快速实时性也有一定要求,在各种网络工况环境下不丢失数据信息,如重要的设备异常信息,开关变位信息,继电保护动作、跳闸信息等,毫无疑问,这类信息的传输应当采用 IP/TCP 模式。

故障录波信息由于是事后分析信息,且数据流非常大,占用带宽较多,对数据的完备性也要求较高,不过对快速性要求较低,所以也推荐采用 IP/TCP 方式。

设备互锁信息主要指间隔层 IED 设备,如测控装置间的遥控闭锁信息,这些信息一般要求快速传递,并且经常要求一发多收,所以采用 IP/UDP 方式,单播或者多播传递信息比较合适。IEC 61850 通信建模标准里引入的 GOOSE 信息快速传递机制,非常适合于这类信息的传递。

巡视信息属于视频点播类型业务应用,特点是数据流非常大,占用带宽很多,快速实时性也有一定要求,否则易造成画面不流畅的问题,一般巡视系统不走变电站监控网络,单独组网,通过 G703.1/G703.6(64 k/2 M)接口经由 PCM 数字复用设备远传,如果采用 IP 方式的巡视应用,推荐采用 UDP 方式。

变电站运行管理信息一般是基于 HTTP 协议的 WWW 服务,B/S 模式业务应用,基本采用 IP/TCP 方式。

站控层功能主站间通信一般采用了“订阅/发布”模型,快速性要求较高,数据流量一般较小,采用短帧报文,通过心跳交互和确认机制保证信息的完整性和实现通信连接的工况监视,并通过多次重发及接收方的确认来保证信息传递的可靠性。另外大部分的站控层软件组件技术模型,如 DCOM/EJB 等都采用了 IP/UDP 方式,所以推荐站控层站间通信采用 UDP 方式。

IED 设备固件加载、地址分配等管理协议一般采用类似 DHCP、BOOTP、HDLC 等的协议,专业名称是设备发现(device discovery)协议,主要有两种实现方式,基于 OSI 模型链路层的发现协议(大部分的通信设备厂商采用此模式,因为可以跨域 IP 层)和基于传输层 UDP 方式的发现协议(只能用于 IP 技术组网的业务应用),由于变电站自动化系统采用了 IP 组网技术,所以站内设备发现协议推荐采

用 IP/UDP 方式,当然为了实现初始 IP 地址等信息的自动分配功能,一般采用链路层通信技术实现最初 IP 地址的分配。

站内对时系统一般采用 IGIG-B 码方式或“脉冲+网络方式”,对于后者,网络方式的对时技术一般采用 SNTP/NTP 或者自定义对时协议,SNTP/NTP 方式基于 UDP 方式(最新的 PTP 1588 V2 为了配合硬件打时间戳实现高精度网络对时,还支持到链路层的技术映射),所以一般的网络对时推荐采用 IP/UDP 方式,对实时性要求极高的环境下可采用 IEEE 802.3 链路层方式。

网络设备的通用管理信息,一般采用 SNMP 协议进行信息传输,SNMP 基于 IP/UDP 方式,所以网络管理推荐采用 UDP 方式。

4 CBZ-8000 变电站自动化系统通信应用

CBZ-8000 变电站自动化系统是国内该领域比较成熟的系统之一,在线运行系统达数千套。该系统从站内通信协议的角度划分,主要包括 CBZ-8000A 变电站自动化系统和 CBZ-8000B 变电站自动化系统,前者用于常规的综自站,站内规约采用 IEC 60870-5-104(局部扩展)传输测控及保护动作事件和动作值(扩展部分)信息;IEC 60870-5-103/TCP 传输继电保护信息,都采用 TCP 方式;后者用于基于 IEC 61850 的数字化变电站,站内规约采用 IEC 61850 通信协议^[6-7]。下面主要分析用于常规综自的 CBZ-8000A 系统的通信应用情况。CBZ-8000A 变电站自动化系统站内通信方案简图如图 1 所示。

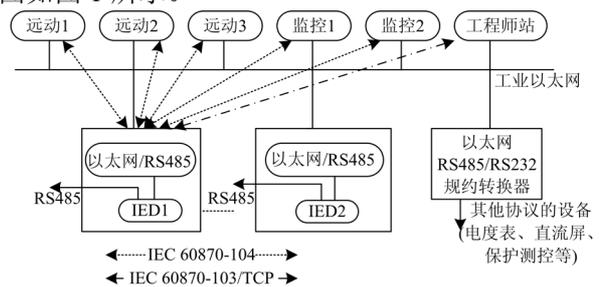


图 1 CBZ-8000A 变电站自动化系统站内通信方案简图

Fig.1 CBZ-8000A SAS communication scheme

CBZ-8000A 系统中,变电站最核心的业务数据,远动四遥信息及继电保护信息的传输都采用了 TCP 方式(IEC 60870-5-104 及 IEC 60870-5-103/TCP 均采用了 TCP 传输方式),摒弃了同类产品采用的 UDP 方式,通过前面的技术分析可知,从底层技术上保证了信息的传输可靠性,重要信息不会丢失,且没必要在应用层采用信息多次发送、选择过滤后

再处理的低效通信方式，提高了通信的传输效率，尤其是大幅降低了监控系统在发生跳闸事故时海量信息上送导致的网络风暴问题。利用 TCP 通信机制可以实现通信的在线链路状态监测，避免了 UDP 方式需要进行的大量心跳监测报文，使得重要信息可以在较短时间内快速到达目的网络通信节点。

IEC 60870-5-104 及 IEC 60870-5-103/TCP 采用 APCI (Application Protocol Control Interface, APCI) 应用协议控制接口^[8]，实现了完备的通信链路控制，APCI 的结构如图 2 所示。

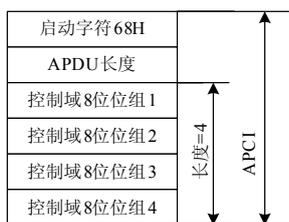


图 2 APCI 数据结构定义

Fig.2 APCI data structure definition

控制域定义了保护报文不至丢失和重复传送的控制信息，报文传输启动/停止，以及传输连接的监视等。控制域的计数器机制是根据 ITU-T X.25 标准中推荐的相关定义。通过发送计数及接收计数机制和滑动窗口机制，保证数据不会丢失。

随着电力系统调度数据网及光纤传输通道的建设，IEC 60870-5-104 最初被规划用于站内 RTU 到调度中心间远动信息的传输规约^[8]，随着工业以太网技术在变电站内应用的迅猛发展，该规约同样用于站内四遥信息的传递，辅以局部的扩展后，还可以传递各类继电保护信息，且更具有开放性。CBZ-8000A 系统在全国数千个变电站/电厂的成功运行业绩也充分印证了这一点。

5 变电站通信技术的发展趋势

随着计算机网络通信技术、信息建模技术、电子互感器技术、智能开关技术、信息化技术的发展及 IEC 61850 变电站通信标准的颁布实施，各种应用模式、实现程度的数字化变电站试点工程如雨后春笋般蓬勃开展。变电站自动化进入了数字化、智能化发展时期，国家将建设环境友好，资源节约的坚强智能电网作为电网建设的指导方略，作为智能电网的基础接点，数字化/智能化变电站发展空间巨大。

数字化/智能化变电站将 IEC 61850 作为变电站内唯一的通信协议，采用通信业务 (Abstract Communication Service Interface, ACSI 抽象通讯服务接口) 与实现技术 (Specific Communication

Service Mapping, SCSM) 相分离的思想，保证通信实现技术能够与时俱进。如图 3 所示。

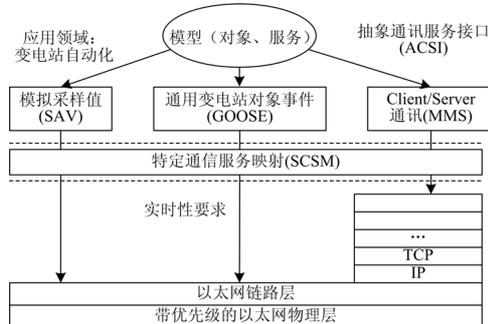


图 3 IEC 61850 现阶段通信服务映射

Fig.3 IEC 61850 communication service mapping

在现阶段，变电站通信网络采用工业以太网技术，间隔层设备与站控层通讯采用 IEC 61850-8-1，将通讯服务映射到通用的 MMS (制造厂商报文协定)，采用 TCP 方式，过程层通讯为了实现从合并器送出的数字化采样值快速、实时到达间隔层保护控制单元，采用 IEC 61850-9-1/2 通信协议，将数字化的采样值 SMV “透传”映射到 OSI 模型的数据链路层，不经过中间的 IP 层等几个协议层，实现了采样值的实时传输；采用高速有效的 GOOSE 通信机制实现了网络化的跳合闸及间隔级的控制联锁功能。

另外，对于站内对时，IEC 61850 在 V1 版本中，推荐采用 SNTP 方式进行网络方式的对时，过程层辅以对时脉冲实现全站的时间同步。在 IEC 61850 V2 版本中，又推荐 IEEE 1588 (后被 IEC 等同采纳为 IEC 61588) 作为数字化变电站网络方式的高精度对时方案。SNTP 网络对时技术采用 IP/UDP 通信方式，IEEE 1588 网络对时技术可以采用 IP/UDP 通信方式，为了提高实时性，也可以直接映射到数据链路层 (IEEE 802.3)^[9]。

6 结论

在变电站自动化系统中，在工业以太网作为站内网络通信骨干通信体系的基础上，根据不同的通信业务类型，应当选用不同的通信实现方式：实时性要求极高的业务应当选用直接映射到 OSI 分层模型的 IEEE 802.3 数据链路层的通信技术；远动四遥信息及重要的继电保护信息从可靠性、实时性、开放性角度综合考虑应当选用基于 IP 的 TCP 传输方式；对于短帧、快速性实时性要求较高、可靠性要求一般的业务应当选用基于 IP 的 UDP 传输方式；UDP 方式在应用层加入传输可靠性保证措施基础上，可以在部分业务实现方面得到应用。

(下转第 162 页 continued on page 162)

[3] 李九虎, 郑玉平, 古世东, 等. 电子式互感器在数字化变电站的应用[J]. 电力系统自动化, 2007, 31 (7): 94-98.
LI Jiu-hu, ZHENG Yu-ping, GU Shi-dong, et al. Application of electronic transformers in digital substation[J]. Automation of Electric Power Systems, 2007, 31 (7): 94-98.

[4] IEC 60044-7 互感器(第7部分): 电子电压互感器[S]. IEC 60044-7 instrument transformers (part 7): electronic voltage transformers[S].

[5] IEC 60044-8 互感器(第8部分): 电子电流互感器[S]. IEC 60044-8 instrument transformers (part 8): electronic current transformers[S].

[6] GB 1207 电压互感器[S]. GB 1207 voltage transformers[S].

[7] GB 1208 电流互感器[S]. GB 1208 current transformers[S].

[8] IEC 61850-2003 变电站的通讯网络和系统[S]. IEC 61850-2003 communication networks and systems in substations[S].

[9] 曹团结, 尹项根, 张哲, 等. 电子式互感器数据同步的研究[J]. 电力系统及其自动化学报, 2007, 19 (2): 108-113.
CAO Tuan-jie, YIN Xiang-gen, ZHANG Zhe, et al. Discussion on data synchronization of electronic instrument transformers[J]. Proceedings of the CSU-EPSA, 2007, 19 (2): 108-113.

[10] 张沛超, 高翔. 数字化变电站系统结构[J]. 电网技术, 2006, 30 (24): 73-77.
ZHANG Pei-chao, GAO Xiang. System architecture of digitized substation[J]. Power System Technology, 2006, 30 (24): 73-77.

[11] 高翔, 张沛超. 数字化变电站的主要特征和关键技术[J]. 电网技术, 2006, 30 (23): 67-71.
GAO Xiang, ZHANG Pei-chao. The main characteristics and key technology of digitized substation[J]. Power System Technology, 2006, 30 (23): 67-71.

[12] 王大鹏, 栗俊凯, 晁军征. 浅谈数字化变电站的发展及应用[J]. 山东电力技术, 2007, 153 (1): 14-18.
WANG Da-peng, LI Jun-kai, CHAO Jun-zheng. Brief introduction of development and application of digital transformer substation[J]. Shandong Power System Technology, 2007, 153 (1): 14-18.

[13] 孙一民, 李延新, 黎强. 分阶段实现数字化变电站系统的工程方案[J]. 电力系统自动化, 2007, 31 (5): 90-93.
SUN Yi-min, LI Yan-xin, LI Qiang. A grading solution for building digital station[J]. Automation of Electric Power Systems, 2007, 31 (5): 90-93.

收稿日期: 2009-08-27

作者简介:

李文升(1978-), 男, 本科, 工程师, 从事继电保护生产技术工作。E-mail: lwsfqd@yahoo.com.cn

(上接第 146 页 continued from page 146)

参考文献

[1] Dolezilek D J. Power system automation[M]. Schweitzer Engineering Laboratories, Inc.

[2] Skeie T, Johannedden S, Brunner C. Ethernet in substation automation[J]. IEEE Control System Magazine, 2002, 22 (3): 43-51.

[3] 辛建波. 基于以太网的变电站自动化系统时延不确定性研究(博士学位论文)[D]. 武汉: 华中科技大学, 2005.
XIN Jian-bo. Research on ethernet-based substation automation system communication delay uncertainty[D]. Wuhan: Huazhong University of Science and Technology, 2005.

[4] TCP/IP 协议详解[M]. 北京: 清华大学出版社, 2004.
TCP/IP protocol in detail[M]. Beijing: Tsinghua University Press, 2004.

[5] IEC 61850 communication networks and systems in substations[S].

[6] 廖泽友. IEC 60870-5-103和IEC 60870-5-104协议应用经验[J]. 电力系统自动化, 2003, 27(4): 69-71.
LIAO Ze-you. Experience of using IEC 60870-5-103 and IEC 60870-5-104 transmission protocols[J]. Automation of Electric Power Systems, 2003, 27(4): 69-71.

[7] 胡明. 变电站自动化系统采用IEC 60870-5-103、104协议的优势[J]. 继电器, 2003, 31(5): 65-67.
HU Ming. The experience of using IEC 60870-5-103 and IEC 60870-5-104 transmission protocols in substation automation[J]. Relay, 2003, 31(5): 65-67.

[8] IEC60870-5-104 变电站远动通信规约[S]. IEC60870-5-104 substation RTU communication protocol[S].

[9] IEEE 1588 精确网络对时协议-V2[S]. IEEE 1588 standard for a precision clock synchronization protocol for networked measurement and control systems[S].

收稿日期: 2009-12-25; 修回日期: 2010-01-13

作者简介:

魏勇(1973-), 男, 硕士, 研究方向为数字化变电站系统方案及相关产品研发; E-mail: yongw@xjgc.com

郭赞(1966-), 女, 副教授, 从事工业自动化方面的教学及科研工作;

马力(1976-), 男, 本科, 研究方向为调度管理及继电保护整定。