基于TCP/IP的IEC60870-5-104远动通信协议在直调厂站中的应用

杜 龙[1]，施鲁宁[2]，杨晋柏[1]

（1.中国南方电网电力调度通信中心，广东 广州 510623 2.河南省巩义市供电局，河南 巩义 451200）

摘要： 介绍了国际电工委员会制定的基于TCP/IP网络的调度主站和远方子站远动通信协议－IEC60870-5-104的体系结构、参考模型、传输帧格式及在南方电网直调厂站中的应用。针对通过TCP/IP网络访问传输远动信息存在的安全问题，对其传输模式进行了深入研究，提出了一种基于加密和身份认证的安全报文传送方法。在南方电网应用的经验表明，该方法是合理和有效的。

关键词： IEC60870-5-104；远动协议；TCP/IP；信息安全；报文

Application of IEC60870-5-104 telecontrol protocol based on TCP/IP in direct dispatching station

DU Long[1], SHI Lu-ning[2], YANG Jin-bai[1]

(1.SG Power Dispatching & Communication Center, Guangzhou 510623, China;
2. Henan Gongyi Power Supply Bureau,Gongyi 451200,China)

Abstract: General structure ,the network reference model, the frame format and the application of IEC60870-5-104 telecontrol protocol , which is published by IEC and used in the communication between the dispatching center and remote station based on TCP / IP network , are introduced in this paper. Aiming at the information security of remote transmission based on TCP / IP network access, the mode of transmission is in-depth studied. A practical method for packet transmission based on encryption and authentication is proposed. The application experience on China Southern Power Grid shows that the method is reasonable and effective.

Key words: IEC60870-5-104; telecontrol protocol; TCP/IP; information security; packet

中图分类号： TM73 文献标识码： A 文章编号： 1674-3415(2008)17-0051-05

0 引言

目前我国电厂、变电站远动系统普遍采用基于电路的独立64kbit/s专线通道进行串口通信，串口通信协议多数为IEC60870-5-101和DNP3.0等，这些协议遵循基于ISO参考模型的增强性能结构（EPA），仅用了OSI模型7层中的3层（物理层、链路层、应用层）来实现数据传输。随着网络技术的迅猛发展和变电站IEC61850标准的逐步推广，为满足网络技术在电力系统中的应用，通过网络传输远动信息，以欧洲大型电力巨头公司（ABB，SIEMENS，ALSTOM）为首的IEC国际电工委员会在IEC60870-5-101基本远动任务配套标准[1~5]的基础上制定了IEC60870-5-104远动传输规约[6]，采用平衡传输模式通过TCP/IP协议实现网络传输远动信息，适用于调度主站（中心站）EMS系统和子站（远方站）RTU或计算机监控系统之间采用专用Intranet网络进行通讯[7~9]。

1 IEC60870-5-104远动规约分析

IEC60870-5-104规约标准定义了开放的TCP/IP接口的使用，包含一个由传输IEC 60870-5-101 ASDU的远动设备构成的局域网的例子。包含不同广域网类型,例如X.25、帧中继、综合范围数据网络ISDN(integrated service data network)等）的路由器可通过公共的TCP/IP—局域网接口互联，图1所示为一个冗余的主站配置与一个非冗余的主站配置。

IEC60870-5-104规约使用的参考模型源于开放式系统互联的ISO-OSI参考模型，只采用其中的5层，它处于应用层协议的位置。基于TCP/IP的应用层协议很多，每一种应用层协议都对应着一个网络端口号。IEC60870-5-104规约在传输层采用TCP协议，其对应的网络端口号为2404，其结构如图2

所示。

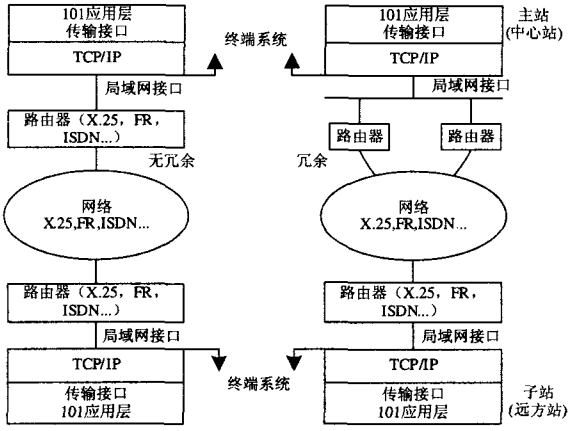

图 1 一般体系结构

Fig.1 General structure for IEC60870-5-104

根据IEC60870-5-101从IEC60870-5-5中选取的应用功能	初始化	用户进程
从IEC60870-5-101和IEC60870-5-104中选取的ASDU		应用层（第7层）
APCI(应用规约控制信息） 传输接口（用户到TCP的接口）		
TCP/IP协议子集（RFC2200）		传输层（第4层） 网络层（第3层） 链路层（第2层） 物理层（第1层）
注：第5，6层未用		

图 2 IEC60870-5-104 规约的网络参考模型

Fig.2 The network reference model for IEC60870-5-104

由图 2 可见，IEC60870-5-104 实际上是将 IEC60870-5-101 与 TCP/IP（Transmission Control Protocol/Internet Protocol）/Internet Protocol）提供的网络传输功能相结合，使得 IEC60870-5-101 在 TCP/IP 内各种网络类型均可使用，包括 X.25、FR（帧中继）、ATM（异步传输模式）和 ISDN（综合业务数据网）。

IEC60870-5-104 规定一个 APDU 报文最长为 255 个字节（包括启动字符和长度标识），所以 APDU 的最大长度为 253，APDU 长度包括 APCI 的 4 个控制域 8 位位组和 ASDU，因此 ASDU 的最大长度为 249，这一规定限制了一个 APDU 报文最多能发送 121 个不带品质描述的归一化测量值或 243 个不带时标的单点遥信信息，如果子站 RTU 或监控系统采集的信息量超过此数目，则须分成多个 APDU 进行发送。应用规约数据单元结构如图 3 所示。

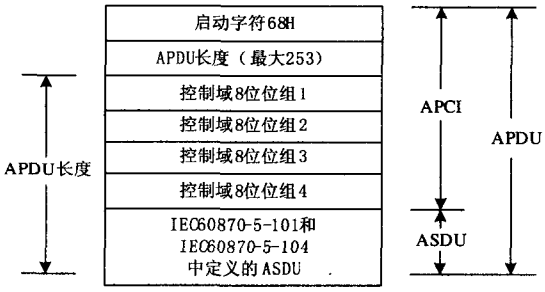

图 3 应用规约数据单元结构

Fig.3 The sructrure of APDU

APDU 控制域定义了保护报文不至丢失和重复传送的控制信息、报文传送启停、传输连接的监视等，包括 4 个 8 位位组，根据其定义，将 APDU 分为 3 种报文格式，即 I 格式（编号的信息传输）、S 格式（编号的监视功能）、U 格式（未编号的控制功能）。

2 IEC60870-5-104 规约在直调厂站中的应用

2.1 规约通信方案

随着电力通信网络技术的发展及为满足南方电网未来 10 至 15 年的电网安全运行和电力市场运作的要求，新 EMS 系统数据采集范围将覆盖南方电网内所有 500 kV 厂站，现有的串行通信已不满足日益增加的数据容量、高速率数据通信要求。为了更好的推广和规范南方电力系统 IEC60870-5-104 协议的使用，在经过充分论证和研究的基础上，由南网总调组织制订了 DL634.5.104-2002 远动传输规约配套标准《南方电网实施细则》[10]，根据南方电网的实际情况，对 DL634.5.104-2002 中的报文类型及参数的选用作了适当的规定，并扩充定义了部分报文。

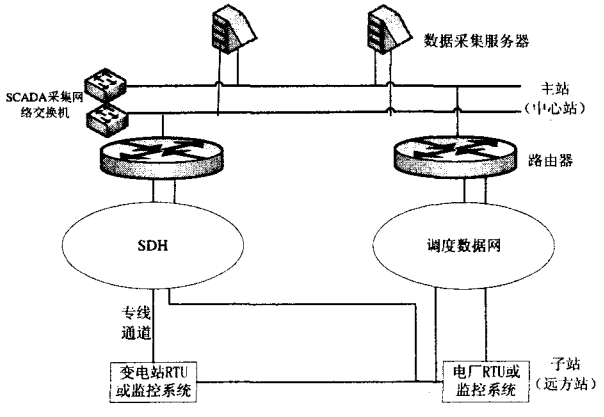

图 4 调度主站与子站通信结构图

Fig.4 The communication structure between dispatching center and station

南网总调新 EMS 系统基于 IEC61970 标准，应用快速数据采集的 SCADA 和数据存储访问的数据库技术，对网内全部 500 kV 厂站 RTU 实现网络通信。调度主站 EMS 系统通过一路调度数据网及一路 2M 专线通道与子站 RTU 实现通信，如图 4 所示。调度主站与子站 RTU 通信是一种典型的 C/S 模式，即被控站（子站 RTU）是服务器端，控制站（调度主站）是客户机端，传输层使用 TCP 协议，固定端口 2404。

图 4 中，数据采集系统模式具有灵活、合理的运行切换方式，能根据统计的子站 RTU 通道的误码率和投退状态选择较好的通道作为传输主通道其它通道作为备用通道，不仅满足了负荷管理系统可靠性、可维护性、可扩充性要求，同时也提高了系统的实时性。

2.2 规约通信实施过程

TCP 连接的建立过程。调度主站作为客户端不断向子站 RTU 发出连接请求，一旦连接请求被接收，则应监测 TCP 连接的状态，以便 TCP 连接被关闭后重新发出连接请求。每次连接被建立后，主站与子站 RTU 应将发送和接收序号清零，并且子站只有在接收到主站 STARTDT 后，才能响应数据召唤及循环上送数据，但在接收 STARDT 前，子站对遥控、遥调等命令仍然进行响应。

变化遥测数据上送过程。按照南网细则要求，总调对接入的500 kV厂站遥测量统一使用类型标识 36，即采用带 7 位长时标的浮点数。

总召唤过程。主站向子站发送总召唤命令（类型标识 100，传送原因 6），子站回应确认（类型标识 100，传送原因 7），然后子站向主站发送单点遥信（类型标识 1），全遥测数据（类型标识 13，不带时标的浮点数），最后向主站发送总召唤结束命令（类型标识 100，传送原因 10，表示执行结束）。

子站事件主送上送过程。当子站发生突发事件，将根据现场具体情况向主站发送以下报文：单点遥信（类型标识 1，传送原因 3），SOE（类型标识 30，传送原因 3）。

遥控、遥调过程。单点设值：主站发送遥调命令（类型标识 48，归一化值，传送原因 6），子站执行确认（类型标识 48，传送原因 7）。多点设置：主站发送遥调命令（类型标识 136，传送原因 6），子站执行确认（类型标识 136，传送原因 7）。单点遥控：分为预置和执行两步操作，首先主站发送遥控预置命令（类型标识 45，传送原因 6），子站收到遥控预置命令后确认（类型标识 45，传送原因 7），然后主站发送遥控执行命令（类型标识 45，传送原因 6），子站收到遥控执行命令后确认（类型标识 45，传送原因 7），遥控命令具体流程如图 5 所示。

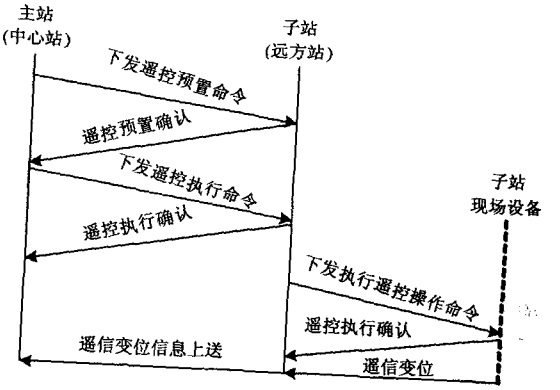

图 5 遥控命令执行过程图

Fig.5 Implementation process of remote control

计划曲线下发过程。南网细则对 IEC60870-5-104 规约中类型标识进行了扩充，规定用类型标识 137 来实现对子站的曲线下发，采用带长时标的多点设点命令下发计划值，给每个计划值分配一个固定地址，从 0 时 0 分开始到 23 时 55 分，一共 288 个量，具体流程见图 6。主站发送计划曲线（类型标识 137，传送原因 6），子站接收到计划曲线后以镜像报文确认（类型标识 137，传送原因 7）。

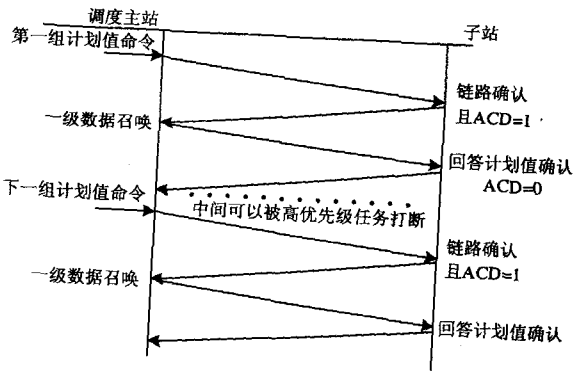

图 6 计划曲线下发流程

Fig.6 The process of sending for plan curve

时钟同步，时差召唤过程。主站发出时钟同步命令（类型标识 103，传送原因 6），子站收到同步命令后确认（类型标识 103，传送原因 7），然后将时差以变化遥测数据上送（类型标识 36，传送原因 3）。

分组召唤过程。南网细则定义 1 到 8 组是遥信，9 到 12 组是遥测数据。分组召唤结束后子站以确认报文（类型标识 100，传送原因 10）上送主站。

远方复位进程。主站发出复位进程命令（类型标识 105，传送原因 6），子站收到复位命令后确认

（类型标识 105，传送原因 7）。

2.3 规约报文传送过程中存在的问题和解决方案

由于 IEC60870-5-104 规约本身不涉及到安全传输机制，而通过调度数据网传输远动信息过程中，如何保证调度主站与子站 RTU 之间报文的安全传输成为当前需要考虑和解决的问题。IEC TC-57 技术委员会第 15 工作组正在着手制定 IEC TS6235－1 标准[11]，该标准目的是为解决 IEC60870-5 系列标准中的数据通信安全问题，目前该标准仍在征集与讨论过程中。

根据电监会 5 号令－《电力二次系统安全防护规定》的要求，电力二次系统的安全防护规定须坚持安全分区、网络专用、横向隔离、纵向认证的原则[12]，及电力二次系统安全防护总体方案要求，调度中心、发电厂、变电站在生产控制大区与广域网的纵向连接处应当设置经过国家制定部门检测认证的电力专用纵向加密认证装置或者加密认证网关及相应措施，实现双向身份认证、数据加密和访问控制[13]，重点抵御病毒、黑客通过各种形式发起的恶意破坏和攻击，尤其是集团式攻击，保护电力实时闭环监控系统及调度数据网络的安全，防止由此导致电力二次系统的崩溃或瘫痪，继而造成一次系统事故或大面积停电事故。

为保障生产控制大区与广域网纵向数据传输过程中的数据机密性、完整性和真实性，根据实际情况，南网总调选择在调度主站和所直接采集信息的 500 kV 子站两侧电力控制系统的内部局域网与电力调度数据网络的路由器之间部署纵向加密认证装置，如图 7 示。

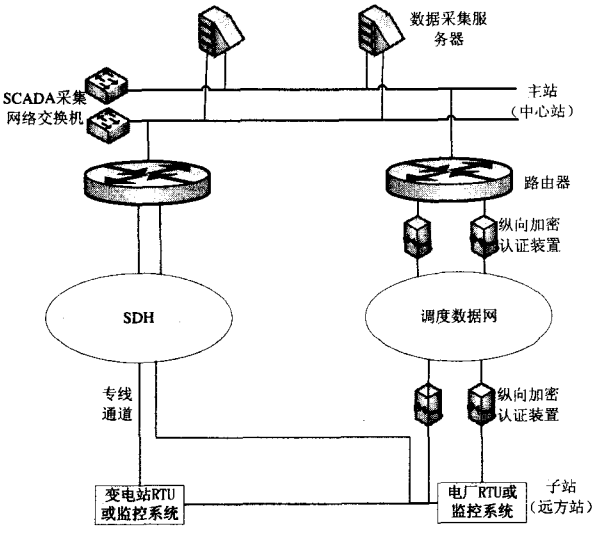

图 7 主站与子站两侧配置纵向加密装置图

Fig.7 Configuration of authentication device

由第 1 节中可知，APDU 分为 3 种报文格式，其中 I 格式包含 ASDU，这部分远动信息需要加密，因此，需要对 I 格式报文进行加密以及对发送方的身份进行认证；而对于 S 格式和 U 格式，由于其中不含 ASDU，因此在报文发送过程中不涉及到必要的加密信息，只需要对报文发送方进行身份认证。对于 I 格式报文，由于包含 ASDU，首先对整个数据包进行加密，产生加密信息包 P，然后通过 MAC 计算，将生成的 MAC 与 APDU 一起打包发送，接受方在收到发送方送出的报文后，首先对报文的完整性和发送者的身份进行验证，然后对信息包 P 解密，得到 ASDU。报文的加密和认证过程如图 8 所示。

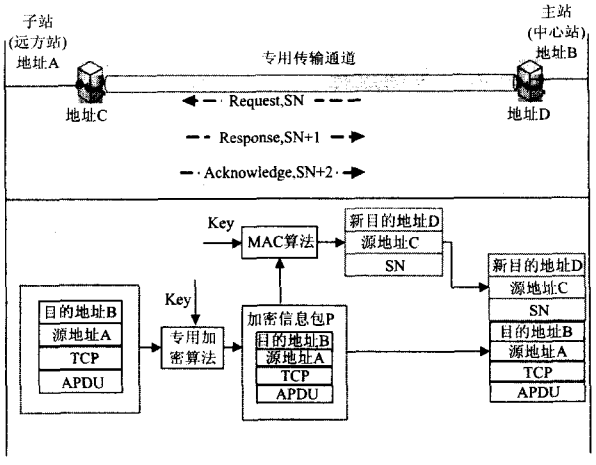

图 8 报文加密与认证过程图

Fig.8 Process of authentication and eneryption

2.4 主站与子站网络通信报文的安全传输过程

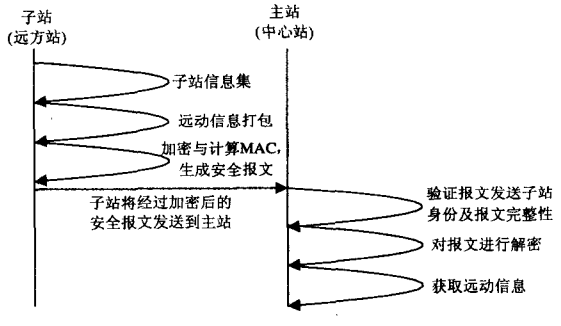

图 9 调度主站与子站通信数据包流程图

Fig.9 The transmission of packet between dispatching center and station

纵向加密认证装置基于链路层的数据访问控制原理，支持透明接入和加密两种工作模式并采用过滤技术，提供应用层的安全访问控制机制。根据上述对远动信息报文的加密和认证过程后，经过验证，

这种安全机制在不影响原有报文传送结构的前提下在实际应用中实现了端到端的选择性保护，保证电力实时数据传输的实时性、安全性、可靠性。调度主站与子站之间网络通信数据包流程图如图 9 所示。

2.5 纵向加密认证装置的应用情况

目前包括国电南瑞、电科院等国内厂家的纵向加密认证装置均通过了相关部门的测试，南瑞科技有限公司开发的Netkeeper－2000纵向加密认证装置已在南网总调、花都变电站、广东省电力调度通信中心及广州、佛山地调投入试运行。上述装置自投运以来，运行情况稳定，根据用户设定的控制策略实现了主站对子站端数据集中的统一管理和运行监测、记录，达到了预期效果。

3　结束语

本文详细介绍了基于 TCP/IP 的 IEC60870-5-104 远动通信协议在总调直调厂站中的具体应用及扩充，针对 IEC60870-5-104 规约本身并没有考虑网络传输信息安全问题，围绕如何保证电力实时传输数据过程中信息的机密性、完整性和真实性三方面的问题，对调度主站 EMS 系统与子站 RTU 或计算机监控系统之间报文传输的各种安全因素进行分析，并根据工程实践，提出了一种满足实际需要的安全通信模式。

参考文献

[1] IEC60870-5-1，远动设备及系统（第 5 部分：传输规约，第 1 篇：传输帧格式）[S].
IEC60870-5-1, Telecontrol Equipment and Systems(Part5: Transmission Protocols, Section 1:Transmission Frame Formats) [S].

[2] IEC60870-5-2，远动设备及系统（第 5 部分：传输规约，第 2 篇：链路传输规则）[S].
IEC60870-5-2, Telecontrol Equipment and Systems(Part5: Transmission Protocols, Section 2:Link Transmission Procedure) [S].

[3] IEC60870-5-3，远动设备及系统（第 5 部分：传输规约，第 3 篇：应用数据的一般结构）[S].
IEC60870-5-3, Telecontrol Equipment and Systems(Part5: Transmission Protocols, Section 3:General Structure of Application Data) [S].

[4] IEC60870-5-4，远动设备及系统（第 5 部分：传输规约，第 4 篇：应用数据的定义和编码）[S].
IEC60870-5-4, Telecontrol Equipment and Systems(Part5: Transmission Protocols, Section 4:Definition and Coding of Appli- cation Information Elements) [S].

[5] IEC60870-5-5，远动设备及系统（第 5 部分：传输规约，第 5 篇：基本应用功能）[S].
IEC60870-5-5, Telecontrol Equipment and Systems(Part5: Transmission Protocols, Section 5:Basic Application Functions) [S].

[6] IEC60870-5-104，远动设备及系统（5－104 部分：传输规约，采用标准传输文件集的 IEC60870－5－101 网络访问）[S].
IEC60870-5-104, Telecontrol Equipment and Systems (Part 5-104: Transmission Protocols, Network Access for IEC 60870-5-101 Using Standard Transport Profiles) [S].

[7] 谭文恕.远动信息的网络访问[J]. 电力系统自动化，2001,25(12):51-52.
TAN Wen-su. Network Access for Telecontrol Information[J]. Automation of Electric Power Systems, 2001,25(12):51-52.

[8] 谢大为，杨晓忠. 调度自动化系统中远动技术网络化的实现[J]. 电网技术，2004，28（8）：33-38.
XIE Da-wei, YANG Xiao-zhong. Implementation of Networking Telecontrol Technique in Dispatching Automation System[J].Power System Technology, 2004, 28（8）：33-38.

[9] 赵渊，沈智建.基于 TCP/IP 的 IEC60870-5-104 远动规约在电力系统中的应用[J].电网技术，2003，27(20):56-60.
ZHAO Yuan, SHEN Zhi-jian.Application of TCP/IP Based IEC60870-5-104 Telecontrol Protocol in Power System[J].Power System Technology, 2003，27(20):56-60.

[10] 中国南方电网 DL/T634.5101-2002 远动传输规约实施细则[Z].南网总调，2007.

[11] IEC 62351-1，Data and Communication Security-Part1: Security for IEC 60870-5 and Derivates(Work in Progress[S].

[12] 电力二次系统安全防护规定[Z]. 国家电力监管委员会，2004.

[13] 电力二次系统安全防护总体方案[Z]. 国家电力监管委员会，2006.

收稿日期：2007-11-26；　修回日期：2007-12-25

作者简介：

杜　龙（1978－），男，硕士，工程师，从事电网调度自动化工作；　E-mail: dulong@csg.cn

施鲁宁（1965-），男，工程师，本科，从事电力系统继电保护和自动化工作；

杨晋柏（1973－），男，硕士，高级工程师，从事电力系统技术研究与管理工作。