基于嵌入式 Internet 的变电站智能设备接入技术研究

吴在军[1],窦晓波[1],蒋云贵[2]
(1. 东南大学 电气工程系,江苏 南京 210096;
2. 江苏移动通信有限责任公司 南京分公司,江苏 南京 210037)

摘要: 以嵌入式 Internet 技术为基础,研究变电站内的智能电子设备(IED)如何实现嵌入式 Internet 接入,从而实现现场生产信息在广域范围内的共享。讨论了变电站 IED 嵌入式 Internet 的接入模式,详细阐述了实现 IED 嵌入式 Internet 接入的关键技术,提出采用"胖"客户机"瘦"服务器的系统体系结构满足硬件资源的限制,Web 页面集成嵌入式 Java Applet 解决数据动态更新问题,裁剪 TCP/IP 协议并利用 HTTP1.1 协议持续连接和缓存控制特性解决实时性问题。最后,对变电站内的 IED 嵌入式 Internet 接入后引起的网络安全问题及应采取的安全策略进行了探讨。

关键词: 嵌入式 Internet; 变电站 IED; 网络接入; 网络安全
中图分类号: TM 76 **文献标识码**: A **文章编号**: 1006-6047(2005)07-0017-04

0 引言

随着电力工业市场化运营的推进,以及电力系统调度自动化的不断发展,调度端和厂站端之间传统的通信方式越来越不能适应新形势的需要[1,2]。Internet 的出现并迅速普及在技术上为变电站内智能电子设备 IED(Intelligent Electronic Device)接入 Internet 提供了实现的可能性,如果能将变电站内的 IED 接入 Internet,则可在广域范围内共享现场运行数据。

将变电站内的 IED 与 Internet 结合起来的主要困难在于 Internet 的各种通信协议对于计算机存储器、运算速度等要求较高,而变电站内的 IED 除部分 32 位处理器以外,大量存在的是 8 位和 16 位处理器,支持 TCP/IP 等 Internet 协议将占用大量系统资源,或根本不可能。本文以嵌入式 Internet 技术为基础,研究了变电站 IED 如何实现嵌入式 Internet 接入,重点讨论接入模式、实现接入的关键技术。最后,对变电站内的 IED 接入 Internet 后引起的网络安全问题及安全对策进行了探讨。

收稿日期: 2005-02-21

1 变电站 IED 嵌入式 Internet 接入模式

变电站内 IED 是指由一个或多个处理器组成,具有从外部源接收和传送数据或控制外部源的任何设备,在特定环境下在接口所限定的范围内能够执行一个或多个逻辑节点任务的实体[3]。在物理上,这

Economy and reliability analysis of connection modes in urban distribution networks

XIE Ying-hua[1], WANG Cheng-shan[1], GE Shao-yun[1], WANG Sai-yi[1], LIN Rui-xing[2]
(1. School of Electrical Engineering and Automation, Tianjin University, Tianjin 300072, China;
2. Fujian Electric Power Survey & Design Institute, Fuzhou 350000, China)

Abstract: As viewed from economy and reliability, the connection modes of urban combination systems, which are composed of 110 kV high voltage networks and 10 kV middle voltage networks, are analyzed and compared. A power supply area-adjustable model is adopted, which adapts its supply radius to the associated load density and substation capacity. The economy index of annual cost for unit load and the reliability index of ASAI are adopted and quantified for the combination power system to study their trends by the change of load density and substation capacity. Different connection modes in the same condition are compared. Based on the synthetic analysis of calculative results, several connection modes are commended to different application circumstances.

Key words: distribution networks; connection modes; economy; reliability

些IED分布于变电站内3个不同层次,即过程层的智能传感器和执行器;间隔层的微机保护装置、智能监控装置和智能计费装置等;变电站层的监控主站和远动接口等。本文所述及的IED特指间隔层的数字式继电保护装置、智能监控装置和数字式的表计等。

从理论上讲,变电站IED这类嵌入式系统只要转变为Web服务器,并装载和解释TCP/IP协议就可以实现和Internet互连[4]。具体实现的技术方法有很多,对于8/16位嵌入式系统而言,处理器速度慢和内存小等系统资源有限是必须面对的问题。对32位嵌入式系统,虽然硬件资源较8/16位系统丰富,但需注意到变电站信息通过Internet传输,大部分都具有一定实时性要求,它除了要满足应用的功能需求外,还要满足实时性要求。因此,在实现Internet接入和应用功能需求二者之间需仔细规划和权衡。

根据变电站规模、电压等级,及其在电力系统中地位的不同,变电站内IED通常有以下不同的Internet接入模式。

1.1 基于PC网关体系结构的接入模式

基于PC网关体系结构是早期变电站IED实现Internet接入常采用的接入模式。

嵌入式Web服务器的PC网关体系结构作为现有变电站自动化系统实现网络化的技术手段或许可以接受,但从严格意义上而言,并不是真正意义上的嵌入式Web服务器。由嵌入式系统自身实现Web服务器功能是真正意义上的嵌入式Web服务器。

1.2 基于通信服务器的接入模式

变电站自动化系统中设置一台或多台配置较高的嵌入式设备作为通信服务器,完成嵌入式Web服务器功能。变电站内常规的IED完成数据采集、控制和保护功能,并通过RS-232/485总线或现场总线和这些通信服务器相连,形成变电站内部的Intranet,再通过嵌入式Web服务器接入Internet,系统结构如图1所示。

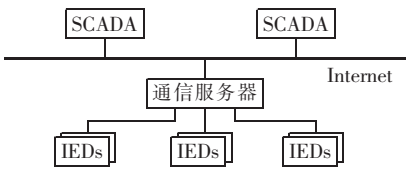

图1 基于通信服务器的接入模式

Fig.1 The interconnection mode based on embedded communication server

文献[5]中,笔者基于嵌入式实时操作系统和软硬件协同设计方法设计了一种此类通信服务器,详细阐述嵌入式以太网接口的硬件设计和嵌入式TCP/IP协议栈实现,其功能原型如图2所示。

1.3 基于嵌入式Web服务器的接入模式

嵌入式Internet技术的发展和实时操作系统不断成熟,使得Internet已经可以延伸到8位和16位

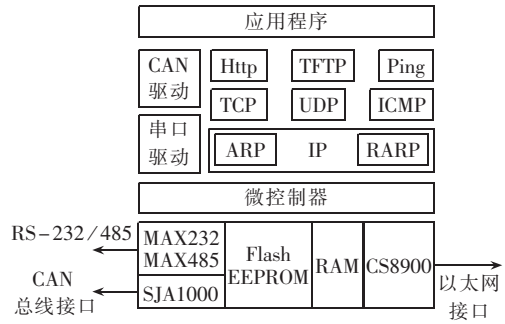

图2 通信服务器的功能原型

Fig.2 The function prototype of communication server

MCU中,原先在8位和16位设备中难以实现TCP/IP和HTTP协议的现状已经得以改变。同时性价比较高的32位或64位高性能处理器的出现,尤其是集成了以太网控制器的高性能MCU的出现,为变电站内IED设备实现Internet接入提供了更灵活的实现途径。其系统结构如图3所示。

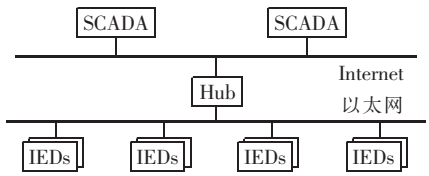

图3 基于嵌入式Internet的接入模式

Fig.3 The interconnection mode based on embedded Internet

这种接入方式采取的是每个IED都直接连到Internet上的技术路线,每个IED设备上都有完整的TCP/IP和HTTP网络协议栈。采用这种接入方式必须把Web服务器缩小到它本身的器件之中,并且只占用设备存储器中的部分字节。

比较这些不同的接入模式,并没有绝对的优劣之分,在不同的应用场合,各有其优越性。

2 实现IED嵌入式Internet接入的关键技术

上述接入模式,尤其后两种接入模式,从技术实现上讲,系统结构和核心关键技术基本类似。必须设计嵌入式以太网接口,基于嵌入式系统的硬件资源实现嵌入式TCP/IP协议栈,并在此基础上实现Web服务器。

2.1 系统体系结构

在嵌入式设备上实现Internet必须采取“瘦”服务器,“胖”客户机的策略。服务器端只负责各种数据的处理和维护,而由客户端程序发送、请求和分析从服务器接收的数据,在客户端以图表曲线等各种方式动态显示现场模拟量值和各断路器、隔离开关分合状态。

因此,变电站IED实现嵌入式Internet接入采用图4所示的应用程序/Web服务器/Web浏览器三层结构,其中Web浏览器和嵌入在IED中的Web服务器EWS(Embedded Web Server)之间采用HTTP1.1

协议进行通信，而应用程序和 EWS 之间根据不同情况通过 CGI（Communication Gateway Interface），SSI（Server-Side Include），HCPA（HTML-to-C Preprocessor Approach）[6]交互。

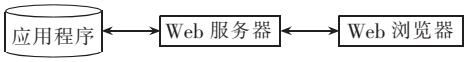

图 4 嵌入式 Internet 体系结构

Fig.4 The architecture of embedded Internet

2.2 数据动态刷新

IED 中嵌入式 Web 服务器需要将现场的实时数据和历史数据以网页形式发布到 Internet 上，且动态实时刷新，远方客户通过接入 Internet 浏览该服务器发布的系统实时信息[7]。为此，引入数据推送技术，以实现客户端浏览器中网页的自动粒状更新。

解决的方法是采用嵌入式 Java Applet 技术，Applet 实际是用 Java 语言编写若干小程序，能提供动画、实时更新和双向交互功能。在客户端浏览器同 EWS 连接时，Applet 作为 HTML 页面的一部分传到用户的浏览器上，在客户端执行。当 EWS 中与这些 Applet 对应的对象发生改变时，客户端浏览器数据可得以实时更新。

2.3 实时性问题

变电站 IED 实现嵌入式 Internet 接入的关键在于 IED 能转变为 EWS，而 EWS 技术的核心是 HTTP 引擎。设计 EWS 时解决实时性问题的一个主要方法在于对协议栈作合适的选择和裁剪，降低对系统资源的占用。在设计和实现过程中，一方面对 TCP/IP 协议栈作了精心裁剪，只保留必须的最小子集；另一方面，充分利用了 HTTP 1.1 不同于 HTTP 1.0 的改进之处，不为每一个 Web 页面的获取建立一个新的连接，而是采用可持续连接的方法，即客户端建立持续连接后，进行第一次请求应答后并不立即关闭连接，而是可以进行多次请求应答后再关闭连接。此外，充分利用了 HTTP1.1 新增加的对于缓存的支持。可持续连接、缓存控制等明显减少了响应的时间，同时也提高了嵌入式设备中资源的利用。

3 IED 嵌入式 Internet 接入的网络安全

变电站 IED 是电力系统的数据源和各种控制行为的执行者，因此，变电站 IED 接入 Internet 以后，网络安全问题日益突出[8]。

3.1 网络安全问题

变电站内 IED 接入 Internet 以后所面临的网络安全问题主要可分为两个方面，即系统安全和信息安全，具体而言主要包括以下几类。

a. 中断：对系统的可用性进行攻击，使变电站和其他系统的通信发生中断，如调度端或数据中心无法获知现场信息，厂站端也无法接收来自调度端的命令。

b. 窃听：对系统的保密性进行攻击，在变电站 IED 和其他系统进行通信时，非法窃取敏感信息。

c. 篡改：对系统的完整性进行攻击，更改变电站与其他系统之间传输的信息，使调度主站得到错误的运行工况，威胁电网的安全运行。如果篡改的是来自调度端的遥控命令、修改定值命令等，更有可能造成严重的后果。

d. 伪造：对系统的真实性进行攻击，在网络中插入伪造“合法”信息发往变电站或主站，可能造成与篡改信息类似的后果。

e. 恶意软件入侵：包括后门、逻辑炸弹、特洛伊木马、病毒和蠕虫等，可能造成系统拒绝服务，数据进行未被授权的修改甚至系统瘫痪等。

3.2 网络安全对策

针对不同类别的网络安全问题，可以从不同方面加以解决，如优化系统结构、采用安全性协议、进行数据加密等。

3.2.1 系统结构

根据变电站的功能、保密水平、安全水平等要求的差异，可以通过专用的内部网络、Extranets、防火墙和代理服务器、VPN（Virtual Private Network）等方法将网络进行隔离，实现更为细化的安全控制体系，提高网络整体的安全水平。

防火墙作为用在变电站内部网络和 Internet 之间实施安全的一种策略，它决定内部服务哪些可以被外界访问，外界的哪些人可以访问内部的哪些可以访问的服务，同时还决定内部人员可以访问哪些外部服务。为使防火墙有效，所有来自或发往 Internet 的业务流都必须通过防火墙接受防火墙的检查。

VPN 以费用低廉的公用网络作为传输媒体，通过 L2TP（Layer2 Tunneling Protocol），IPSec 等协议及加密技术的处理，向用户提供虚拟的专用网络服务技术。变电站 IED 接入 Internet 以后，未授权用户可能会非法访问运行、计费等敏感数据，甚至对开关设备执行操作。利用 VPN 技术可以鉴别哪些数据请求和命令来自授权用户，哪些来自非授权用户。同时，VPN 对数字证书集中管理的机制，可以在内部员工解职或计算机被窃的情况下，立即撤销数字证书，确保数据安全。

3.2.2 安全性协议

在嵌入式设备环境下，可用的安全协议包括 SSL，S-HTTP（Secure HTTP），IPSec，SET 等。嵌入 Web 服务器可以根据嵌入式设备的特点和应用的需求，采用不同的设计架构和实现方法，实现不同安全等级的安全协议。

3.2.3 数据加密

加密技术是最基本、最常用而又最有效的信息安全技术，可以有效地限制截获、中断、篡改、伪造的

概率,从而达到保证信息安全的目的。在公共密码体制基础上发展而来的数字签名技术,不但保留了公共密码体制密钥易于管理的优点,同时还可确认消息的来源和内容。数字签名使接收者能够核实发送者对报文的签名,并且接收者不能伪造对报文的签名,发送者事后也不能抵赖对报文的签名[9]。

对变电站计算机网络,可以采用数字签名技术,对威胁电网安全运行的信息和影响生产经营决策的敏感数据进行加密处理,并可借此加强网络安全管理。

必须指出,通常安全性和易用性成反比,系统越安全使用就越不方便。此外,在变电站环境中,有些网络应用是为实时业务服务的,如SCADA系统。这种应用要求具有很高的可靠性、较小的响应时延(通常在毫秒级)等特殊要求。而网络安全措施中的加密解密技术,相互认证技术、数字签名技术的使用都需要许多时间开销,信息安全的考虑会降低系统的性能,所以需要在安全和性能之间折衷。

4 结语

本文分析了变电站内IED嵌入式Internet接入的不同模式,重点讨论了实现过程中的关键技术,包括系统结构、数据动态刷新、保证实时性的措施等。文章最后对变电站内的IED嵌入式Internet接入后而引起的网络安全问题及应采取的安全策略进行了探讨。

参考文献:

[1] SHAW T. Using internet technologies for secure substation access and control[A]. **Power Engineering Society Summer Meeting[C]**. Seattle,USA:IEEE,2000. 363-368.

[2] QIU B,GOOI H B,LIU Y,*et al*. Internet-based SCADA display system[J]. **IEEE Computer Applications in Power**,2002,15(1):14-19.

[3] IEC61850,Communication networks and system in substations,Part5[S].

[4] 栗大超,宋光德,靳世久. 嵌入式系统的Internet互连技术[J]. 微计算机信息,2000,16(6):4-6.
LI Da-chao,SONG Guang-de,JIN Shi-jiu. The Internet connecting of embedded system[J]. **Micro Computer and Information**,2000,16(6):4-6.

[5] 郑建勇,吴在军,胡敏强,等. 一种能实现异种网络互联的通信控制器[J]. 电力系统自动化,2003,27(12):58-62.
ZHENG Jian-yong,WU Zai-jun,HU Min-qiang,*et al*. Implementation of a communication controller for heterogeneous network interconnection[J]. **Automation of Electric Power Systems**,2003,27(12):58-62.

[6] JU H T,CHOI M J,HONG J W. An efficient and lightweight embedded web server for web-based network element management[J]. **International Journal of Network Management**,2000,(10):261-275.

[7] 王 瑞,聂 钢,李国富. 基于B/S模式的远程数据采集系统的研究[J]. 计算机应用,2003,23(4):128-130.
WANG Rui,NIE Gang,LI Guo-fu. Study on remote data acquisition system based on B/S model[J]. **Computer Applications**,2003,23(4):128-130.

[8] 高 卓,罗 毅,涂光瑜,等. 变电站的计算机网络安全分析[J]. 电力系统自动化,2002,26(1):53-57.
GAO Zhuo,LUO Yi,TU Guang-yu,*et al*. Analysis of computer network security in substation[J]. **Automation of Electric Power Systems**,2002,26(1):53-57.

[9] 杨 波. 网络安全理论与应用[M]. 北京:电子工业出版社,2002.

(**责任编辑**:戴绪云)

作者简介:

吴在军(1975-),男,江苏南京人,讲师,博士,主要从事变电站自动化、实时系统等方面研究工作(**E-mail**:wuzaijun@yahoo.com.cn);

窦晓波(1979-),男,江苏南京人,博士研究生,主要从事变电站自动化研究;

蒋云贵(1971-),男,江苏南京人,硕士,主要从事通信电源系统建设及变电站自动化系统研究。

Interconnection of substation IEDs based on embedded Internet

WU Zai-jun[1],DOU Xiao-bo[1],JIANG Yun-gui[2]

(1. Department of Electrical Engineering,Southeast University,Nanjing 210096,China;
2. Nanjing Branch of Jiangsu Mobile Communication Co.,Ltd.,Nanjing 210037,China)

Abstract: The interconnection of IEDs(Intelligent Electronic Devices) in substation is studied based on the embedded Internet technology to realize sharing for field operation information in wide areas. The interconnection mode is discussed and the key implementation technologies are described,such as adopting the architecture of thin server/fat client to satisfy the constraints of source in IED,integrating embedded Java Applet into Web pages to update dynamic information, cutting TCP/IP protocol and using persistent connection and cache control characteristics of HTTP1.1 to meet the real-time requirements. The network security after interconnection is discussed and some security strategies and measures are proposed.

Key words: embedded Internet; IED in substation; interconnection; network security