基于B/S模式的电力设备在线监测通用安全信息系统的研究

袁兆强， 张雯

(三峡大学电气信息学院，湖北 宜昌 443002)

摘要：随着Internet/Intranet技术的普遍应用，电力行业中各种电力设备的在线监测信息系统都朝着基于Web的方向发展，当前各种在线监测信息系统都是采用传统的三层B/S结构。针对传统B/S三层体系结构的在线监测信息系统在安全性上存在的问题和不足，提出了一种新的B/S结构的四层安全体系结构，并对各层功能进行了定义，描述了四层通用安全信息系统的工作流程，并将此四层安全体系结构应用于实际的在线监测系统之中，效果良好。

关键词：B/S模式；在线监测；通用安全信息系统；四层安全体系结构

Research on electrical equipment on-line monitoring common secure information system based on B/S

YUAN Zhao-qiang, ZHANG Wen

(College of Electrical Engineering & Information Technology, China Three Gorges University, Yichang 443002, China)

Abstract: With the universal application of Internet/Intranet technology, various electrical equipment on-line monitoring information system are developed towards to web direction. Nowadays, various on-line monitoring information systems all use the traditional three-layer B/S mode. This paper proposes a new four-layer security architecture based on B/S mode, in view of the insufficiency on security problems of traditional three-layer architecture of on-line monitoring information system. It then defines the function of each layer and the workflow of four-layer security information system. Finally, this four-layer security architecture has been successfully applied in actual on-line monitoring information system and has achieved good effect.

Key words: B/S mode; on-line monitoring; common secure information system; four-layer security architecture

中图分类号： TM769；TP309.2 文献标识码： A 文章编号： 1003-4897(2007)06-0059-05

0 引言

近年来，变压器、断路器、互感器和输电线路等主要电力设备的在线监测系统一直是国内外研究的热点[1~9]。电力设备的可靠性是电网安全运行的保证，因此及时对设备实施状态监测，尤其是对关键的大型电力设备，是非常重要的。引入Internet技术是电气设备状态监测与诊断系统的发展趋势，它顺应电力系统自动化、信息化的发展需求，在信息处理能力、系统开放性和远程监控方面已初步显示了其优越性[1~9]。这些在线监测信息系统是电力设备关键特征信号的采集、处理、诊断、信息管理的综合监测系统，在整个电力行业综合自动化系统中占有重要地位。

随着计算机技术、网络技术和通讯技术的飞速发展，促进了我国电力行业朝着电气化程度越来越高的方向发展。许多变电站、变电所、电厂纷纷都进行了电气化改革，都开发出了针对一些主要电力设备的基于B/S模式的在线监测信息系统，以提高电力系统运行、维护的效率和降低运行、维护的成本，使得管理部门能在网络上快捷、直观地了解所需的有关电力设备实时运行的各项数据和信息，强化了电网的管理工作。系统的投运提高了管理水平，减轻了工作人员的工作压力，为管理和决策分析提供真实、准确、实时的信息。

虽然B/S模式的在线监测信息系统与C/S模式的在线监测信息系统相比，具有了很多优点[3~9]：B/S模式简化了系统的开发和维护，只需开发基于Web的中间层的应用软件，无需考虑客户端的兼容性及后台数据库的变化，降低了开发和维护的成本，并且特别适用于网上信息分布和远程对系统的维护和管理，但是传统三层B/S模式在安全性方面

存在不足[2, 4]。

1 传统 B/S 结构应用体系结构的分析

采用 B/S（Browser/ Server）模式的在线监测信息系统，解决了传统 C/ S(Client/ Server)模式管理系统维护困难、工作量大、使用不方便、可扩展性差等缺点，但传统三层 B/S 结构的信息流是在浏览器—Web 服务器—DB 服务器之间进行，无统一的安全系统（如图 1），因此，存在明显的安全性问题。

图 1 三层 B/S 体系结构

Fig.1 Architecture of three-layer B/S

在上述三层结构的基础上，有人提出了许多新型的体系结构[4]，如“B/S和C/S混合结构”[2,8]和“浏览器—Web服务器—中间件服务器—DB服务器”[11]等。B/S和C/S的混合结构主要解决的是传统三层结构在数据库维护上性能差、工作量大且不够方便等问题。浏览器—Web服务器—中间件服务器—DB服务器结构，采用JSP技术和JavaBean组件的结合[10]，其主要解决的是传统三层结构在软件重用性差等方面的问题。因此，这些结构并没有在系统的整体安全性上进行完整的考虑或设计。

2 通用安全四层信息系统的设计

在B/S结构信息中，安全问题是系统发展的主要障碍。在传统的三层B/S结构的信息系统中，浏览器与Web服务器之间及Web服务器与数据库服务器之间没有专门的体系与机制来保证系统的安全性。针对该问题，提出了四层安全体系结构，通过在传统三层B/S结构的应用系统基础上的扩展，引入加/解密模块和安全认证模块，来保障系统的总体安全。

2.1 系统的总体结构

图 2 给出了基于 B/S 结构的四层通用安全信息系统结构。

由图 2，系统被划分为四层，即表示层、功能层、数据层、安全层。下面就这四个层次的功能进行介绍。

2.1.1 表示层的功能定义

表示层负责客户端信息的显示以及在客户端和Web服务器之间保障信息传输的安全性。客户端的浏览器与服务端的Web服务器除了进行通常的HTML文件交流通信外，增加了由认证模块控制的安全通道。安全通道实现客户端与Web服务器之间关键数据的加/解密、身份认证、数据的完整性保护和传输控制。

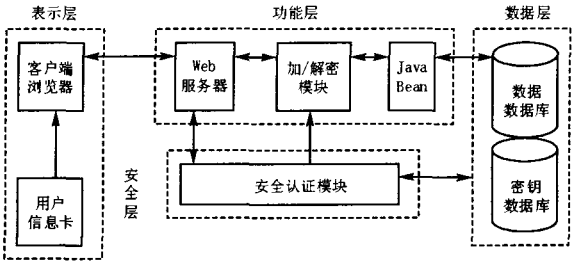

图 2 四层通用安全信息系统结构

Fig.2 Architecture of four-layer common security information system

在用户信息卡中封装了数字证书和数字签名算法，用户信息卡是一个具有USB接口的即插即用的设备。证书中提供了每个特定用户的相关信息，包括用户名、口令、用户公钥和私钥，认证模块可通过Web服务器提取其中的相关信息进行身份认证。本系统为了保证电力行业中的在线监测信息系统的安全运行，尽可能保证系统不被网络上的恶意攻击者攻击和破坏，保证数据在Internet上安全保密地传输和关键数据传输和存储的不可否认性，给系统的每个用户都分配一张用户信息卡，每个用户进入相应系统时，都需按网页页面上的要求插入用户信息卡，客户端计算机负责从用户信息卡中提取身份鉴别信息，间接送到认证模块进行验证，只有通过验证的合法用户才能做下一步操作。在用户信息卡中封装的数字签名算法是为了实现关键数据的不可否认性。

2.1.2 功能层的功能定义

与传统三层B/S结构信息系统的体系结构类似，功能层完成系统的基本业务处理。本系统的Web编程采用JSP编程，与PHP、ASP不同的是JSP的脚本语言是Java语言，JSP很方便地存取可重用的JavaBean组件，可以很方便地将JSP页面的表现和逻辑处理完全分开，所以采用JSP和JavaBean组件相结合开发的动态页面比ASP和PHP开发的页面要短小得多。

为满足安全性的要求，新的功能层对外的接口包括:Web 接口、安全认证接口以及数据接口。Web 服务器通过 CGI、ISAPI 或直接的 Java 程序实现用

户请求和数据响应。

数据库连接模块由 JavaBean 构成，主要任务是和数据库进行连接，并读取和存入数据，将用户数据请求转换为相应的 SQL 语句，对数据库进行查询、添加、删除和修改等操作。

加/解密模块包括 SQL 语句的语法分析，数据加/解密，加密字典和密钥管理四个子模块，数据字典子模块是将初始化时的一些参数在加/解密时提供给加/解密子模块使用，这此参数一般是单独保存在数据字典表中，数据内容主要包括待加密表内行、列信息，待加密字段，数据类型，是否加密等。为了保证加密数据有更高的安全性，选择加密强度比较高的算法 AES 加密算法。SQL 语句分析子模块是根据数据字典的内容对用户提交的 SQL 语句进行分析。加/解密子模块是整个功能层的核心部件，通过它来保障敏感数据的加/解密操作，从而保障数据的安全性。密钥管理子模块主要是对数据密钥的产生和存储进行管理。

2.1.3 数据层的功能定义

数据层是由传统的 Client/Server 模式演化来的。在主要功能上，继承了客户/服务器数据库管理系统的优秀性能和开发工具，与传统的数据层的功能有相同之处，都是用来存储数据的，本系统中数据层包括数据数据库和密钥数据库。数据数据库专门用来存放在线监测信息系统中电力设备的实时状态和参数等数据，有些比较敏感的数据以加密形式存放于数据库中；密钥数据库中存放有用户的基本信息，比如用户名、口令、数据密钥、用户密钥对（公钥和私钥）以及用户的权限、待加密字段等，其中口令（MD5 加密）、数据密钥、用户私钥均以加密形式存放在密钥数据库中，数据密钥是被用户公钥加密过的密文形式，此时只有用户私钥才能解开获得数据库密钥，为了保证用户私钥的安全，通过用户口令加密私钥，并且用户口令也通过 MD5 加密算法进行加密，这样一来密钥的安全性可以得到有效保证，从而保障了整个系统的安全性。

在安全性上，数据层提供了与JavaBean连接模块进行数据交换的普通数据接口和与安全认证模块进行用户身份认证信息和密钥交换的安全接口。

2.1.4 安全认证层的功能定义

安全认证层在整个B/S结构的在线监测信息系统的业务处理过程中，处于重要的地位。安全认证模块与Web服务器和数据库通过安全接口连接，主要提供三个方面的安全服务。首先，提供用户的身份认证功能，即验证不同用户信息卡中封装的证书信息，保证合法用户的操作资格；其次，提供用户数据加密的密钥，当在线监测信息系统的用户通过浏览器第一次登录系统界面时，通过Web服务器自动从认证模块中下载公钥证书，利用公钥可以对敏感信息进行加密，确保敏感数据在客户端浏览器和Web服务器之间传递的安全，给敏感数据提供了第一重保护；敏感数据在Web服务器和数据库之间通过加/解密模块来进行对敏感数据的加/解密，加密用的数据密钥通过安全认证模块从密钥数据库中下载，从而可以实现对敏感数据的第二重保护，确保敏感信息的安全性。最后，为不同用户提供了不同的数字签名算法，认证模块中的数字签名算法是和用户信息卡中封装的数字签名算法一一对应的，主要是提供签名的验证功能，保证电力行业在线监测信息系统中数据的完整性和不可否认性。

2.2 四层通用安全信息系统的工作流程

系统工作流程如图 3 所示。

四层通用安全信息系统的工作流程描述如下：

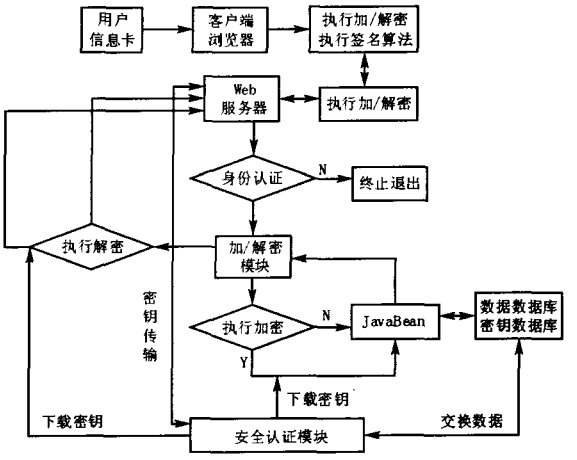

图 3 四层通用安全系统工作流程

Fig.3　Workflow of four-layer common secure system

1）用户进入系统时都需按网页页面上的要求插入用户信息卡，客户端计算机负责从用户信息卡中提取身份鉴别信息，通过 Web 服务器送到认证模块进行验证，只有通过验证的合法用户才能做下一步操作。

2）用户在浏览器上发出数据存取请求，这些请求通过 HTTP 协议送到 Web 服务器上。

3）Web 服务器收到请求后，对请求用户的身份和类型进行验证，若用户请求合法，则自动从认证模块(第一次登录)下载公钥证书，对于非常重要的

数据（普通数据可不选择公钥加密），用户可使用公钥对数据进行加密，密文传送到 Web 服务器，确保敏感数据在客户端浏览器和 Web 服务器之间传递的安全。

4) Web 服务器在接受到用户请求后，将请求交给加/解密模块进行处理。

5) SQL 语句的语法分析子模块对 Web 服务器传过来的 SQL 语句进行分析，对照数据字典子模块中的信息分析该语句中是否涉及到待加密字段，如果有，则执行加密操作，加密的密钥通过安全认证模块从密钥数据库中下载，并通过安全认证模块和加/解密模块之间的安全接口进行密钥传输；如果没有，则将数据通过 JavaBean 连接模块直接存入数据数据库。

6) 加/解密子模块对数据加密完之后，通过 JavaBean 连接将数据存入数据数据库。

7) 对于需要解密的数据，解密的密钥也需要通过安全认证模块从密钥数据库中下载，并通过安全认证模块和加/解密模块之间的安全接口进行密钥传输；加/解密子模块对数据通过数据密钥解密之后，将数据传递给 Web 服务器；Web 服务器通过安全认证模块下载用户的公钥和私钥，并通过它们之间的安全接口传递；对于用公钥加密的敏感信息可以用私钥对数据进行解密，如不是敏感信息，可不用解密；最后，Web 服务器将明文数据传递给客户端浏览器显示。

8) 对于不需要解密的数据，加/解密子模块直接将数据传递给 Web 服务器；Web 服务器通过安全认证模块下载用户的公钥和私钥，并通过它们之间的安全接口传递；对于用公钥加密的敏感信息可以用私钥对数据进行解密，如不是敏感信息，可不用解密；最后，Web 服务器将明文数据传递给客户端浏览器显示。

3　B/S 四层结构的电力设备在线监测信息系统

电力设备的可靠性是国家电网安全运行的保证，是保证国民经济建设的稳定、健康、快速发展的保证，因此及时对电力设备实施状态监测，尤其是对关键的大型电力设备，是非常重要的。近年来，各种电力设备在线监测系统纷纷涌现出来，该系统对保障电力设备正常、稳定运行起到了重要作用。因此电力设备在线监测系统的安全、稳定运行有力保障了我国国民经济建设的稳定、健康、快速地发展，但是传统三层结构的电力设备在线监测系统没有考虑到安全性方面，没有有效的措施来保护信息系统的安全，存在很大的安全隐患，所以本文所提出的基于 B/S 四层结构的电力设备在线监测信息系统便应运而生了。

B/S 四层结构的电力设备在线监测信息系统结构，如图 4 所示。

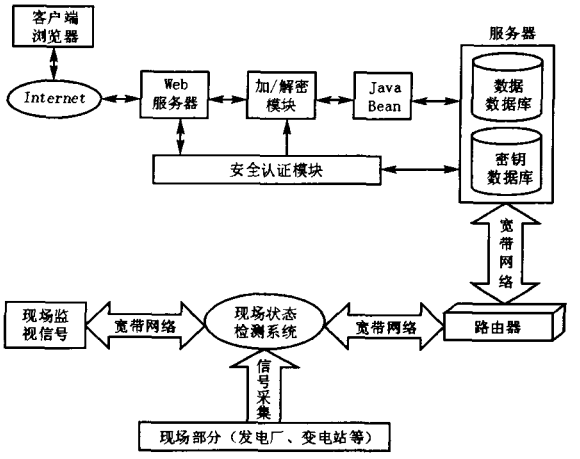

图 4　B/S 四层结构的电力设备在线监测系统结构

Fig.4　Architecture of electrical equipment on-line monitoring system based on four-layer B/S mode

基于 B/S 四层结构的电力设备在线监测信息系统的突出特点如下：

1) 该四层结构可以有效地保证电力设备在线监测信息系统的数据的保密性，对敏感的信息，在存储和传输过程中进行加密，即数据在客户端—Web 服务器和 Web 服务器—数据库这 2 个传输阶段中均被加密，数据库中存放的敏感信息也被加密，这样一来即使数据被窃取或截获也无法得到其明文内容，极大地保证了系统的安全性。这是传统三层结构电力设备在线监测信息系统所无法比拟的第一个优点，传统三层结构的信息系统中的数据都是以明文形式存储和传输，如果数据一旦被非法用户截获或非法用户入侵了数据库服务器，那么将会对信息系统中的数据造成无法弥补的损失。

2) 该四层结构可以有效地保证电力设备在线监测信息系统的用户身份的真实性，有效地防止来自系统外的恶意攻击，给系统的每个合法用户分配一张用户信息卡，用户的身份信息均被封装在用户信息卡中，且被加密，这样一来用户的身份信息不容易被泄露，有效阻止了来自系统内部和外部的恶意攻击者窃取用户身份信息的途径，每个用户进入

相应系统时，都需按网页页面上的要求插入用户信息卡，客户端计算机负责从用户信息卡中提取身份鉴别信息，间接送到认证模块进行验证，只有通过验证的合法用户才能做下一步操作，这是传统三层结构电力设备在线监测信息系统所无法比拟的第二个优点，传统三层结构仅仅通过用户名和密码验证来登陆系统，并且用户名和密码以明文形式存放于数据库中，这样很容易泄露，给系统带来了很大的安全隐患。

3）该四层结构可以有效地保证电力设备在线监测信息系统的数据的完整性和不可否认性，有效地防止了来自系统内部的恶意攻击和破坏，因为在四层结构中使用了数字签名技术，安全认证模块中的数字签名算法是和用户信息卡中封装的数字签名算法一一对应的，这样一来就可以提供签名的验证功能，通过验证被篡改或破坏数据的数字签名可以找出篡改者或破坏者，确保了系统不被内部合法用户恶意攻击和破坏，保证数据在 Internet 上安全保密地传输和关键数据传输和存储的完整性和不可否认性，从而确保了电力设备在线监测信息系统的安全运行，这是传统三层结构电力设备在线监测信息系统所无法比拟的第三个优点，传统三层结构对来自系统内部合法用户所造成的数据库信息的破坏和篡改没有采取有效措施，或者说根本无法阻止来自内部的破坏和篡改，但往往系统最大的威胁来自系统内部。

此基于B/S模式的数据库四层安全结构已成功应用于湖北黄冈电力公司的在线监测系统中，取得了比较好的效果。

5　结束语

本文提出的基于B/S结构的在线监测通用安全信息系统克服了传统三层及B/S与C/S混合结构的在线监测信息系统在安全性上的不足，就目前来说，可以满足电力行业中在线监测信息系统对信息安全的要求。

参考文献

[1] 张艾萍，万瑞军. 基于数字温度传感器的电缆故障在线监测及火灾预警系统[J]. 电力自动化设备，2003，23（10）：57-61.
ZHANG Ai-ping，WAN Rui-jun.Cable Fault On-line Monitoring and Fire Pre-warning System Based on Digital Temperature Sensor[J].Electric Power Automation Equipment，2003，23（10）：57-61.

[2] 赵文彬，张冠军，严璋. 基于因特网技术的电气设备远程在线状态监测与诊断系统[J]. 中国电力，2003，36（4）：60-63.
ZHAO Wen-bin，ZHANG Guan-jun，YAN Zhang.Remote On-line Condition Monitoring and Diagnosis System Based on Internet Techniques for Power Equipment[J].Electric Power，2003，36(4)：60-63.

[3] 卫少华，申晓波. 变电站电气设备在线监测的方法[J]. 西北电力技术，2005（2）：60-62.
WEI Shao-hua，SHEN Xiao-bo.The Research of Electrical Equipment on Line Supervision in Transformer Substation[J].Northwest China Electric Power, 2005(2)：60-62.

[4] 李岚，刘松堂，王太勇，等. 基于 Internet 和状态监测的设备管理系统研究[J]. 组合机床与自动化加工技术，2004（1）：20-21.
LI LAN, LIU Song-tang, WANG Tai-yong.Search of Plant Management Based Internet and Condition Monitoring System[J].Modular Machine Tool & Automatic Manufacturing Technique, 2004（1）：20-21.

[5] 郑萍，潘世永，李世伟，等. 基于 WEB 的大型电力变压器绕组温度远程监控系统研究[J]. 高压电器，2006，42（2）：125-127.
ZHENG Ping,PAN Shi-yong,LI Shi-wei,et al. Research on The Remote Monitoring System of the Large Power Transformer Winding Temperature Based on Web Service[J]. High Voltage Apparatus, 2006，42（2）：125-127.

[6] 于璞.基于 B/S 模式的变电站远程监测系统研究[J]. 煤矿机电，2005（3）：33-34.
YU Li.Study of Remote Monitoring System of Substation Based on Browser/Server Mode[J]. Colliery Mechanical & Electrical Technology, 2005（3）：33-34.

[7] 李艳涛，栗然，赵敏. 基于 Web 的继电保护管理信息系统研究与实现[J]. 电力自动化设备，2003，23（11）：41-43.
LI Yan-tao,LI Ran,ZHAO Min. Study and Implementation of Web-based Relay Protection Management Information System[J]. Electric Power Automation Equipment, 2003，23（11）：41-43.

[8] 李征. 基于 C/S 和 B/S 模式的输电线路管理系统[J]. 微计算机信息，2006，22（8-3）：138-139.
LI Zheng. The Management System of Power Line Based on C/S and B/S[J]. Control & Automation, 2006，22（8-3）：138-139.

[9] 程景清，林振和，刘前进. 基于 C/S 和 B/S 模式的继电保护定值管理系统[J]. 继电器，2006，34（1）：18-21.
CHENG Jing-qing,LIN Zhen-zhi,LIU Qian-jin. Setting Management System of Relay Protection Based on the Mode of C/S and B/S[J].Relay, 2006，34（1）：18-21.

（下转第 79 页 · continued on page 79）

工时，#1 主变一直在带负荷运行，未能将母联断路器电流互感器的二次回路接入差动保护电流回路中。这种情况如图 4 所示，当母联断路器合环后，假定电流从线路 XL_3 经 DL_M 流向 XL_1，流过 CT_1 二次侧进入差动保护的电流为 $I_{a1}=I_m-I_{b1}$，其中的 I_{b1} 可以被主变低压侧的二次电流 I_{b2} 平衡掉，则流入差动继电器的电流为 $I_{cj}=(I_m-I_{b1})-I_{b2}=I_m$，正好是母联互感器的二次电流，当 I_m 等于或大于差动保护整定的动作值时，就会使保护动作。

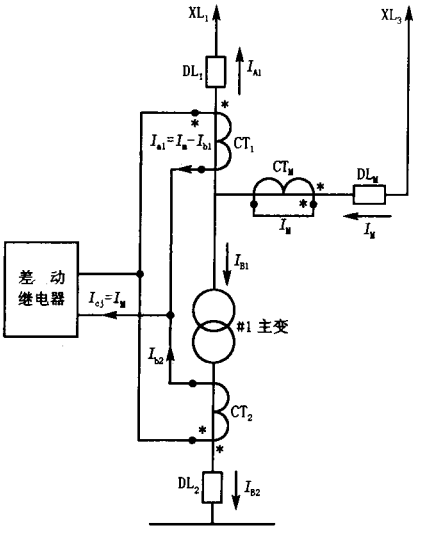

图 4 主变差动保护误动原因分析图

Fig.4　Analysis of the transformer differential protection maloperation

根据系统当时运行情况，母联断路器合上后，通过母联开关的电流为 154 A，方向从 II 母流向 I 母，差动回路的电流为 $I_{cj}=I_M/n=154/60=2.57$ A。#1 主变差动保护电流启动值整定为 $0.3I_e=0.3*165.3/60=0.83$ A，差动电流远大于其启动值，故一合上母联断路器，便报出“#1 主变差动保护启动”的信号。还好，因差动速断整定值为 $8I_e$，母联电流小于其动作整定值，差动出口并未动作。但是在这种情况下，一旦线路上出现故障，#1 主变差动保护出口继电器将会动作，但因跳闸压板已经退掉，不会再跳主变开关。

3　防范措施

1）一条线路或一个元件经两台断路器接入系统时（主接线为桥式或多角形接线的情况下），该线路和元件保护装置的二次电流回路，必须注意两台电流互感器的变比、极性和绕组连接方式，如果变比不一致、极性和二次回路连接有误，将会使继电保护装置误动或拒动，造成设备和系统事故。

2）凡是从两台电流互感器二次引入电流回路的保护装置，当其中一台互感器退出运行，要做变比或通流试验时，一定要先做好安全措施，把停运的电流互感器二次回路与运行的保护装置脱离开，以防止在试验过程中使运行的保护误动，跳开运行设备。

3）调度编制新设备投运方案，一定要非常清楚有关设备继电保护装置的基本原理，熟悉其二次回路的来龙去脉，尤其要注意新投运设备同正在运行的设备二次回路之间的联系，以及新设备投运后对运行设备会造成什么影响，必要时，采取有效措施，如退出保护、改变定值、调整运行方式等，以保证新设备安全投运，正在运行的设备正常工作，确保对用户可靠供电。

收稿日期：2006-05-15

作者简介：

孙　茁（1955-），男，高级工程师，长期从事地区供电网运行和技术管理工作；

李文兴（1977-），男，工程师，从事电网继电保护运行维护和技术管理工作；E-mail:smallstar88@eyou.com

李国海（1977-），男，助理工程师，从事继电保护设计工作。

（上接第 63 页　continued from page 63）

[10] 张波，张福炎. 基于 JSP 技术的 Web 应用程序的开发[J]. 计算机应用研究，2001，18（5）：99-101.
ZHANG Bo,ZHANG Fu-yan.Development of JSP-based Web Applications[J]. Application Research of Computers, 2001，18（5）：99-101.

[11] 张宏森，朱征宇. 四层 B/S 结构及解决方案[J]. 计算机应用研究，2002，19（9）：21-22.
ZHANG Hong-sen,ZHU Zheng-yu. The 4-tier Browser/Server Architecture and Its Scheme[J]. Application Research of Computers, 2002, 19(9): 21-22.

收稿日期：2006-10-14；　修回日期：2006-12-05

作者简介：

袁兆强（1957-），男，副教授，硕士研究生导师，从事电力系统计算机继电保护和综合自动化的教学和研究工作；

张　雯（1982-），女，硕士研究生，研究方向为电力系统继电保护及其综合自动化。E-mail:xfh_02@163.com