面向智能电网的信息安全防护体系建设

刘金长，赖征田，杨成月，李浩松（国网信通亿力吉奥信息科技有限公司，福建 厦门 361009）

摘　要：随着信息化管理手段的不断普及，电网企业网络与业务应用系统中存在的安全隐患日益突出，信息安全防护的重要性开始凸显。针对智能电网信息安全防护需求，提出电网企业信息安全防护体系设计和建设框架，以此为依据建设信息系统，将最大限度地持久保障企业网络与信息系统的安全。

关键词：智能电网；电网企业；信息安全；防护体系

0 引言

近年来，国家电网公司大力推进特高压电网、SG186工程和电力通信等建设，数字化电网、信息化企业的蓝图逐步实现，为智能电网建设奠定了扎实的基础。随着我国智能电网的建设，信息安全问题越来越突出，电网调度自动化、继电保护和安全装置、发电厂控制自动化、变电站自动化、配网自动化、电力负荷控制、电力市场交易、电力用户信息采集、智能用电等多个领域均可能面临信息安全的威胁，信息安全已成为智能电网安全稳定运行和对社会可靠供电的重要基础，是电力企业生产、经营和管理的重要组成部分。本文的“信息安全防护体系”是多年来信息化建设一直关心和重视的问题，并投入了大量人力、物力和财力，今后也将是长期从事研究和建设的领域。随着信息安全的形势日益严峻，信息安全防护还需要进行深入的研究和探讨，做好信息安全防护体系建设，开展关键技术攻关，确保电网企业信息安全工作的系统性、安全性、实用性和创新性。

1 电网企业的信息安全防护需求

电网企业信息安全的总需求是物理安全、通信网安全、计算机系统安全、应用系统安全和数据安全，最终目标是确保信息的机密性、完整性、可用性、可控性和抗抵赖性以及企业对信息资源的控制。

现代企业管理实践证明，任何工作都是三分技术，七分管理。电网企业信息安全防护工作也不例外，技术只是最基本的手段，规范、科学的管理才是最根本的保障。信息安全防护体系设计除应考虑技术体系之外，还应设计相应的管理体系。

2 信息安全防护体系模型

在对多种信息安全防护体系进行研究分析后，根据国家电网公司“电网信息安全等级保护纵深防御示范工程”项目成果，并参照ISO/IEC27001信息安全管理标准，提出了适合电网企业的信息安全防护体系模型，该模型在整体上表现为一个三维立体框架结构（见图1）。

电网企业信息安全防护体系可划分为3个层面，以强调信息安全防护需要人、技术和运作3种要素的均衡。该防护体系具有以下特

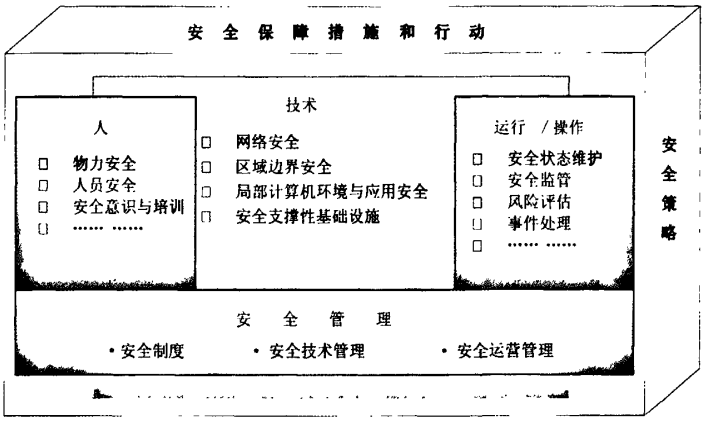

图1 信息安全防护体系模型

点：一是体现了安全管理是纲，安全技术是基础，安全的人和运作是保障；二是强调信息安全防护需要人、技术和运作3种要素的均衡；三是强调安全的过程性和动态性以及防护、检测和反应（PDR）模型的应用；四是强调纵深防御和深度防御的原则。

3 信息安全防护体系设计

电网企业信息安全防护技术体系的设计可以从基础防护和上层防护2个大层面进行考虑。其中，基础防护层即建立信息安全基础支撑平台；上层防护则可以从完善不同防范区域的不同防范措施这个角度进行建设，具体可分为通信网防护措施、区域边界防护措施、企业内部防护措施等（见图2）。

从功能上考虑，电网企业信息安全防护体系的设计，可重点从7个分支系统的角度来开展，具体包括基本安全防护系统、CA认证系统、授权管理系统、安全保密管理系统、安全监控系统、信息加密系统和信息安全管控平台等。

下面将针对这7个分支系统介绍其设计思路和建设方法。

3.1 基本安全防护系统

3.1.1 防火墙

为保障网络资源安全，电网企业应采用防火墙作为安全保防护体系的第一道防线，通过访问控制，防御网络攻击。防火墙的配备对于

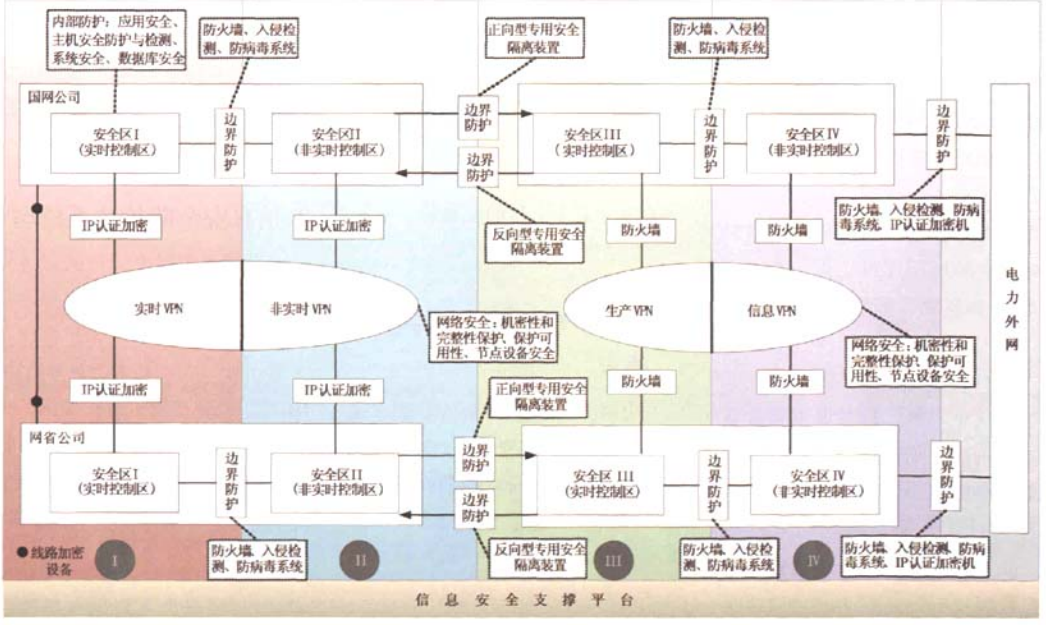

图2 信息安全防护体系

增强内外网络与边界的安全会起到重要作用。防火墙的选型应根据业务数据流量和业务安全性要求的不同，选购不同类型的防火墙。

3.1.2 入侵检测系统

入侵检测系统作为安全检测的最后一道防线，提供安全审计、监视、攻击识别和反攻击等多项功能，可对内部攻击、外部攻击和误操作进行实时监控。入侵检测系统具有事前警告、事中防护和事后取证等特点。建议采用具有高级分析技术的入侵检测系统，例如多个相关事件、相关协议的综合分析。当入侵检测系统检测到攻击时，自动记录攻击，通知网络管理人员，并与防火墙进行联动，及时阻断网络攻击。

3.1.3 脆弱性扫描系统

脆弱性扫描系统通过将网络或主机的配置信息与扫描系统预存的漏洞规则进行匹配和分析，从而挖掘出系统脆弱性。脆弱性扫描系统可以分远程网络扫描和本机扫描。

3.1.4 防病毒系统

计算机病毒问题一直很严峻。随着网络建设的发展和各种业务应用系统的推广，计算机病毒扩散呈现出了新的特征，因此在电网企业内外网的建设中，需要着重考虑计算机病毒防治问题，且要与其他安全防护措施相结合，构建立体的防护体系。

3.1.5 安全审计系统

安全审计系统通过网络数据的采集、分析和识别，实时、动态监测通信内容、网络行为和网络流量，发现和捕获各种敏感信息、违规行为，实时报警响应，全面记录网络系统中的各种会话和事件，实现对网络信息的智能关联分析、评估及安全事件的准确全程跟踪定位，为整体网络安全策略的制定提供权威可靠的支持。

3.1.6 Web信息防篡改系统

Web信息防篡改系统监控Web服务器和应用服务器上的文件目录，并通过可信部署进行合法更新。Web信息防篡改系统可实现对Web服务器的监视功能、检知功能、防篡改和破坏功能、复原功能、自动报警功能等。

3.2 基于PKI技术的CA认证系统

基于PKI技术的CA认证系统[2]对于保障电网企业的信息安全具有非常重要的作用，《电力二次系统安全防护规定》将其建设放到了一个相当重要的位置。电网企业CA认证系统的建设应遵照国家有关部门的规定统一部署。电网企业根CA与国家根CA进行逻辑上的连接，在安全策略等方面接受国家根CA的指导；电网企业内网根CA与其他CA系统（包括外网根CA）物理分离，采用不同的安全策略和不同的安全保障措施保障各自CA系统的安全。电网企业CA之间的关系如图3所示。

CA认证系统基于非对称密码学的安全属性，通过引入数字证书可实现电网中用户身份的有效识别，以及保障电网信息传输的安全性、完整性和保密性等。电网的CA认证系统主要包括以下部分：CA证书签发系统、KMC密钥管理中心、RA证书管理系统以及证书在线注册系统等。

3.3 基于PMI的授权管理系统

授权管理系统通过在数字证书的扩展项增加用户的属性和权限信息，为信息系统提供针对资源的授权管理及访问控制服务。它提供用户管理、审核管理、资源管理、角色管理等功能。

根据资源的具体特点和应用的实际需要，授权管理系统采用2种工作模式：集中式授权服务和分布式授权服务。针对电网企业的主干通信网络，在授权服务方式上可以采用集中式授权服务；针对八大业务应用系统的局部计算环境，在授权方式上可以采用分布式授权服务。授权管理服务系统应根据电网企业实际业务需要，满足基本的授权服务。

3.4 安全保密管理系统

安全保密管理系统提供自动化的安全资产管理、安全策略管理、安全状态管理和技术规范管理等功能，可以有效提高电力内外网的可控性和可管理性。其中，安全资产管理对电力内外网涉及的安全设备建立数据库，自动化管理安全设备

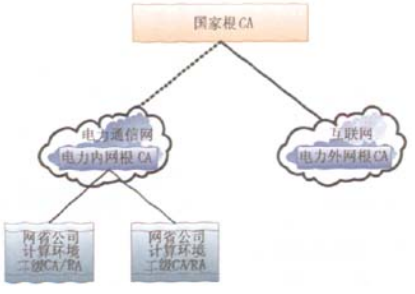

图3 电网企业CA关系图

的配置状况、操作规范、技术支持信息和与设备相关的人员信息；安全策略管理建立安全策略管理系统，维护和管理电力内外网的安全策略；安全状态管理建立安全状态管理系统，对电网企业涉及的系统和网络设施的安全状态变化进行管理；安全规章管理和技术规范管理是通过建立安全规章管理系统，对影响电网企业的法律、法规、制度与技术规范进行统一管理，明确各安全规章与有关设备、系统和环境的关系，保证安全规章的变化能在安全策略中得到体现。

3.5 安全监控系统

安全监控系统是为了在日常工作中对系统平台进行安全方面的有效监控而建立的一种防护性系统。针对通用操作系统环境存在的安全隐患，采取主动的操作系统行为监管方法，利用系统引导固件技术、操作系统底层技术和智能软件代理(Agent)技术等，设计并实现一个面向主流通用操作系统的安全监测与管制平台。通过在系统引导层、操作系统核心层、应用层等多个层面，对操作系统启动前、操作系统启动过程中和操作系统运行中的操作行为（特别是输入/输出信息流）实行安全监测和管制，达到保障信息系统安全的目的。

安全监控系统的功能主要包括系统输入/输出监管功能、安全配置监管和外流信息监管功能、应用系统完整性监管功能以及远程主机监测功能等。

3.6 信息加密系统

为了保障数据的安全性，在电网企业信息安全防护体系中，信息加密技术是不可缺少的安全保障手段，尤其是在数据传输和存储这2个关键阶段。

在电网企业中，大量的数据需要进行传输，而传输过程中数据的安全性是非常重要的，这就需要采用有效的传输手段保障信息传送的安全。而数据在终端、关键节点的保存，也同样需要安全有效的保存，保障数据的安全存储。为此在电网企业中VPN加密协议的应用，以及数据加密存储、传输成为需要考虑的重要环节。

在电网企业信息安全防护体系中，可根据电网企业实际情况，对电网信息节点的数据存储开发数据加密软件，采用高强度的3DES、AES、Blowfish等算法对数据进行加密，保障数据存储的安全性。数据加密技术和身份认证技术相结合，在进行了合法的身份认证后才可进行正常的数据解密。数据安全存储和个人身份识别结合，可避免同一机构不同人员间数据的不安全访问，实现数据的分层安全机制。

3.7 信息安全管控平台

在电网企业信息安全防护体系中，信息安全管控平台是其中的核心部分。通过信息安全管控平台，可以对电网企业的各组成部件即资产进行有效管理；同时，可以对用户访问资产进行有效控制，对所有访问行为进行统一日志管理，对电网企业所提供的安全服务进行统一监控和管理，也能对各种事件的响应机制进行统一管理。从而将各种信息安全资产、事件、服务、响应都融合到此信息安全管控平台中，为用户提供统一管理的平台和手段。其主要功能包括资产管理、账号管理、统一日志管理、安全服务集中管理、响应设置、访问控制等。

4 结语

尽管电网企业信息安全防护工作逐步受到重视，但由于其动态性和复杂性等特点，以及信息化工作职能定位、功能划分还需要在实践中不断完善等原因，导致信息安全防护工作尚存在诸多问题。为此，本文提出了基于7个防护系统建设完整的电网企业信息安全防护体系的建设思路，可指导电网企业有效解决由于信息系统规模扩大所带来的信息系统安全性维护问题。

参考文献：

[1] 陈树勇，宋书芳，李兰欣，等. 智能电网技术综述[J]. 电网技术，2009，33(8)：1-7.

[2] 周　杨，王春枝. PKI体系下的电子政务信息安全研究[J]. 软件导刊，2009，8(3)：161-162.

责任编辑 张钦芝

收稿日期：2010-05-10

作者简介：

刘金长（1962-），男，广西柳州人，高级工程师，从事电力信息化建设及管理工作；

赖征田（1965-），男，福建永安人，工程师，从事电力信息化建设及管理工作；

杨成月（1977-），男，安徽安庆人，工程师，从事电力信息化建设及管理工作。

面向智能电网的信息安全防护体系建设

作者： 刘金长， 赖征田， 杨成月， 李浩松
作者单位： 国网信通亿力吉奥信息科技有限公司,福建厦门,361009
刊名： 电力信息化
英文刊名： ELECTRIC POWER INFORMATION TECHNOLOGY
年，卷(期)： 2010，(9)
被引用次数： 0次

参考文献(2条)

1. 陈树勇. 宋书芳. 李兰欣. 沈杰 智能电网技术综述 2009(8)

2. 周杨. 王春枝 PKI体系下的电子政务信息安全研究 2009(3)

相似文献(10条)

1. 期刊论文 唐慧. 肖超群. 汪桥红 新形势下电网企业增销策略研究 -苏州大学学报（哲学社会科学版）2010,31(4)
随着电力市场改革的进一步深入,金融危机影响以及替代能源的出现使得电力市场中的电力营销遇到了前所未有的挑战,如何在新环境下稳定并发展电力销售是电网企业需要考虑的问题之一.智能电网的建设和发展给电网企业带来了新的契机.本文首先对电力市场的环境进行了分析,接下来结合智能电网环境的特点给出了电网企业增销的几点策略建议.对电网公司进一步实现社会效益和经济效益有一定的借鉴意义.

2. 期刊论文 魏加项. 纪洪. 刘小鹰. 叶蕾. 任自勇. WEI Jia-xiang. JI Hong. LIU Xiao-ying. YE Lei. REN Zi-yong 浅析电网企业在当前经济形势下提升服务价值 -电力需求侧管理2009,11(3)
在金融危机的影响下,我国经济的增长速度放缓,电网公司面临新的挑战和机遇.从开发潜在用户、开拓新业务、加强营销服务等角度对电网公司的机遇进行了分析并提出对策.

3. 期刊论文 唐林. 孙睿 国际智能电网互操作性标准化的进展 -科技创新导报2010(28)
本文在阐释智能电网及其互操作性概念的基础上,明确了智能电网互操作性技术标准的制定原则,对北美在该领域开展工作的相关机构及其进展进行了综述,最后对电网企业促进智能电网互操作性实践提出了可行建议.

4. 期刊论文 李瑾. 杜成刚. 张华. LI Jin. DU Chenggang. ZHANG Hua 智能电网与电动汽车双向互动技术综述 -供用电2010,27(3)
车辆到电网(V2G)技术实现了电网与电动汽车的双向互动,是智能电网技术的重要组成部分.从V2G技术的概念出发,分析了V2G技术的工作原理、充放电业务流程,指出了要发展和推广V2G技术,电动汽车企业和电网企业应在相关标准制定方面加强研究和合作.最后阐述了V2G相关技术国外研究应用现状、V2G技术对电动汽车产业、智能电网的重要意义.

5. 期刊论文 徐翀. Xu Chong 坚强智能电网下的资产管理探讨 -中国电力教育2009(17)
随着坚强智能电网战略目标的提出、建设和未来全面实施,我国电网资产规模将更加庞大,在如此庞大的资产面前,如何科学管理是电网企业亟待解决的先行问题,尽早建立相应的管理理念和管理措施,将起到防患于未然的作用.

6. 期刊论文 傅前明. 李津瑶. FU Qian-ming. LI Jin-yao 国家责任和社会责任视角下的"坚强智能电网" -佳木斯大学社会科学学报2010,28(4)
以国家电网公司为主体推行的"坚强智能电网"建设,实质性地承担了中国减少温室气体排放的国家责任;而且电网企业承担着引领"低碳经济"发展的社会责任."坚强智能电网"建设应当提升到国家战略层面,统筹推进.

7. 期刊论文 朱彬若. 张慎明. 王虎. Zhu bing ruo. Zhang shen ming. Wang hu 智能用电楼宇节能综合控制的实现方式 -上海节能2010(4)
智能用电楼宇是智能电网用电环节的重要组成部分.在上海世博园智能电网综合示范工程中,以国家电网企业馆为建设对象,通过开发楼宇智能用电能量管理系统,采用双向互动技术实现楼宇节能综合控制,展示楼宇节能减排的效果.文章从系统设计角度,阐述了楼宇用电智能化的实现方式.

8. 期刊论文 陈庆彬 智能电网与"大规划"体系 -中国电力企业管理2010(8)
智能电网是电力工业未来的重要发展方向,它将使电网的功能形态发生许多改变,对电网企业方方面面都将产生深远的影响.

9. 期刊论文 李坤. 董宇波. 姚尧 动态业务流程管理在电力企业中的应用 -电力信息化2010,08(7)
面对智能电网和现代化企业管理的挑战,电力企业各环节业务流程贯通的需求愈加强烈,新能源接入、客户双向互动等创新型业务流程对企业管理提出了越来越多的挑战.通过对面向服务架构(SOA)的动态业务流程管理的方案设计,并结合智能停电管理具体业务利用动态业务流程管理,实现流程贯通和数据一致的成功实施案例,在建设敏捷型电网企业,提高公司业务灵活应变和创新能力方面进行了探索.

10. 期刊论文 吴疆 对智能电网若干基础性问题的思考 -中国能源2010,32(2)
本文在学习多方观点与意见的基础上,从技术进步、产业分工与社会使命的层面追根溯源正本清源,就当前智能电网的历史演变、现实背景、核心技术归类、主导机制、国家战略以及电网企业、监管机构的不同使命等基础性问题进行了思考.