

# 基于终端安全的省级电力公司信息安全防护体系建设

随着信息化技术在企业中的不断深化,电力系统信息化水平日趋提高,业务开展和办公环境对信息技术的依赖显著提升,信息安全工作对信息化的保障已成为保障业务成果的重要手段。从终端基础设施安全防护的基本特征出发,分析了公司当前信息安全管理情况和主要面临的安全威胁,针对终端安全防护,规划了相应的信息安全管理策略,提出了一种基于终端安全的信息安全防护体系建设,提升了公司信息安全自主可控能力,进一步加强公司信息安全体系建设及信息系统的安全稳定运行。

解思江 焦阳 李晓辉 张继涛/国网北京市电力公司



解思江/高级工程师

## 关键词/Keywords

信息化·  
信息安全·  
防护技术·

## 0 引言

随着电力公司信息化程度的不断深入,公司越来越依赖于信息技术的支撑,网络、信息系统与公司业务的紧密结合趋势日益显现,信息安全已经成为影响促进信息化进一步深入、保障信息化成果的重要手段,信息安全工作也越来越成为省级电力公司业务安全稳定运营的重要组成部分。

“十一五”前,省级电力公司信息安全工作尚处于起步阶段,信息网络直接与互联网相连,安全工作也主要集中在基础安全防御方面。

“十一五”期间,省级电力公司加快信息化建设,同时高度重视信息安全工作,全面开展信息安全体系化建设并取得了显著的成效,为了落实国家对信息安全保障的要求,提高电力系统网络和信息系

统安全防护能力,保障电力行业信息化建设的安全稳定运行,强化内部信息安全,省级电力公司严格贯彻公安部、国家保密局、国家密码管理局和

电监会等国家有关部门的信息安全工作要求,落实国网公司“双网双机、分区分域、等级保护和多层防护”的安全防护策略。

## 1 基于终端信息安全防护体系建设的不研究和设计

### 1.1 信息安全防护体系建设规划指导思想

省级电力公司信息系统部署于管理信息大区和生产控制大区。管理信息大区用以支撑省级电力公司,不涉及国家秘密企业的管理信息业务应用,划分为用于一体化平台及业务应用和内部办公的信息内网(可涉及企业商业秘密)以及用于支撑对外业务和互联网用户终端的信息外网(不涉及企业商业秘密)。本文所要考虑的安全防护目标为省级电力公司的管理信息大区。其网络分区示意图如下图所示。

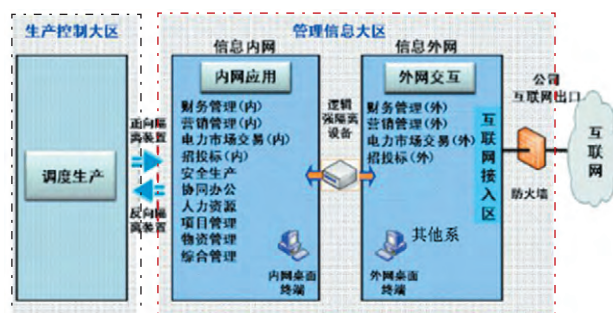


图 省级电力公司网络分区示意图

安全机制可以分为两类：一类与安全服务有关，是实现安全服务的技术手段；另一类与管理功能有关，用于加强对安全系统的管理。建立企业信息系统安全长效机制，不仅需要技术上的支持和实现，同时也需要管理上组织机构、人员、业务逻辑和法令规章制度的支持和实现。信息安全保障体系建设是一项复杂的系统工程，本文在

表 终端信息安全需求分析

| 业务系统层次 | 风险描述                          | 风险类型 | 对业务的影响            | 安全需求       |
|--------|-------------------------------|------|-------------------|------------|
| 终端     | 终端计算机、笔记本电设备和存储介质遗失、被盗导致信息泄露。 |      |                   | 对终端进行安全加固， |
|        | 内部人员泄密、外部人员窃密和导致终端内敏感数据泄露风险。  | 机密性  | 终端非授权使用、          | 实现用户的身份认证、 |
|        | 数量多，环境复杂。                     | 认证性  | 误操作或者其他因素造成敏感信息泄露 | 访问权限的控制以及防 |
|        | 操作人员复杂，终端识别及认证机制不完善           |      |                   | 泄密         |

在技术安全方面，主要从终端接入和桌面终端两方面进行安全防护。首先，实施基于强制策略的控制，确保接入终端可管；其次，加强终端的安全防护能力，采取全过程的管理控制措施，提高免疫能力，确保终端可用和可信。

1.3 网络隔离技术

网络隔离技术主要用于对网络边界进行防护，其首要的防护任务是明确网络的安全边界，同时进行边界完整性检查，实现严格的访问控制。

在管理信息大区网络中，通过正、反向隔离装置实现了信息内网与信息外网的网络隔离，在各个子网边界部署防火墙实现了安全防护，并在交换机上划分VLAN实现了子网隔离管控。

1.4 访问控制技术

访问控制是指对限定的访问者限制所访问的资源或功能，主要实现于TCP/IP网络架构的网络层、主机层和应用层，可以决定发起访问的主体、访问的资源以及访问的方式，也可以有效地阻止非授权用户的非授权访问。

省级电力公司在访问控制方面，对所有的在运用系统均设置了严格的访问权限，对所有主机进行了IP、MAC绑定，并通过交换机（802.1.x协议）、软件（终端控制软件）和安全系统（违规外联阻断）等方式实现了对主机终端的访问控制；在网络方面，通过划分子网和不同的安全域加强资源

信息安全保障体系研究和设计上主要基于终端，从强制技术控制手段和安全管理防护出发，构建一套有效的信息安全防护体系。

1.2 终端安全技术控制防护建设策略

终端的可管、可用和可信是终端安全的基础，终端信息安全风险与需求分析如下表所示。

的访问控制；在边界上，架设防火墙、IPS和IDS等安全设备并进行过滤，严格执行访问控制规则。

1.5 安全接入技术

安全接入主要用于对智能电网业务终端、通信通道和边界接入进行防护，实现智能电网业务终端安全、通道可信和接入可控，包括对接入的支撑平台、接入终端和传输通道的安全防护。

通过采取多种信息安全接入方式，包括企业专网传输通道的加密、终端非法外联阻断、纵向网络边界基于数字证书的接入认证以及7×24 h实时的安全监测与审计措施，以解决对非公司信息内网区域信息采集类、移动作业类终端以及安全专网方式接入信息内网的问题，保证接入的信息传输安全、接入数据安全和接入平台安全。

1.6 身份认证技术

身份认证是确认访问主体身份的过程，分为用户和主机之间的认证以及主机之间的认证两种。其具体过程是识别访问主体（访问发起者）的身份并对其进行认证，以确定是否为被许可的访问主体，之后确认访问主体允许访问的资源范围和可执行的操作。

省级电力公司在信息外网部署了代理服务器，使用账号/密码、IP/MAC绑定等方式对终端进行身份认证，同时，在应用系统中对每个账号设置密码、密码复杂度要求、登录错误锁定、会话超时断开及口令生存周期，重要应用采用数字证

书、动态口令等强认证机制进行身份认证。

### 1.7 入侵检测技术

入侵检测是针对系统闯入或其闯入企图进行的检测,可通过对闯入行为、系统日志、审计数据或其他残余信息等方式分析检测进而获得结果,按其实现方式可分为网络入侵检测和主机入侵检测两种,其目的均是实时地检测非授权的访问和攻击。

建立日常入侵检测监控和应急响应机制,不同安全级别的事件以不同形式处理,如一般事件仅进行日志记录,而发现缓冲区溢出等高级级别安全事件攻击则以短信等实时呼叫方式及时通知管理员处理。

### 1.8 病毒防范技术

计算机病毒是一段程序,它通过嵌入的方式隐藏在另一正常应用程序中,从而实现破坏被感染终端安全性和完整性的目的。病毒代码具有破坏性、复制性和传染性等特征,能够进行自我复制传播。

针对病毒木马的威胁,省级电力公司统一部署了桌面终端管控系统来扫描病毒木马,强制提醒安装防病毒软件,并在信息内网和信息外网均部署了防病毒软件服务器,提供防病毒软件的安装和升级服务。

### 1.9 监控审计技术

物理安全是指公司信息资产所处的物理环境的安全,主要涉及公司硬件设备,公司通常通过物理隔离方式实现网络安全,它是信息安全的基础保证,实现了信息设备硬件自身的安全,进而保障了信息系统硬件的安全稳定运行。虽然物理安全在信息安全控制中相对简单且容易理解,但其往往是内部人员恶意入侵攻击链中很重要的起始环节,是内部安全控制中不可或缺的重要内容。

本文所述“监控”是对部署于公司信息内网和信息外网中的服务器、桌面终端和网络设备等安全状态的感知、检测和控制,通过实时数据反馈分析实现信息安全事件的提前预警;“审计”意为审查和核定,是对恶意行为和操作的事后追查稽核,为重建事件和恢复系统提供条件。

省级电力公司在信息内网和信息外网均部署了信息运维综合监管系统,将大部分安全系统集成、集中展现,信息化设备的监控审计是信息安全全生命周期中不可或缺的一环。同时还部署了一套审计系统,主要通过访问控制的管理制度进

行物理访问授权、限制、跟踪和记录,实现对恶意行为和操作的事后追查稽核。

### 1.10 资源控制技术

资源控制的对象是主机终端,为保证资源的有效共享和充分利用,必须在主机层面和应用层面对资源使用情况进行监视和控制,以确保业务正常运行。

省级电力公司主要采用限制最大会话连接数、限制单个用户的多重并发会话数和根据服务优先级分配系统资源并对系统资源的使用限度、登录超时或鉴别失败锁定等措施实现资源控制。

### 1.11 终端安全技术

终端安全技术主要包括以下几类:

1) 终端系统加固与防护技术。通过安装主机级的安全软件实现终端系统层面的防护,主要有基于主机的防火墙、防病毒和入侵检测等技术。

2) 终端可信与虚拟技术。基于可信组件、虚拟化等技术构造终端可信环境,主要有可信计算、沙箱、虚拟机、无盘工作站和桌面云等技术。

3) 终端安全管理。通过统一安全策略,对接入网络的终端进行统一管理,实现网络和终端安全,主要包括准入控制、补丁管理和用户行为管理等技术。

### 1.12 完善和落实规章制度

制定和完善网络信息安全相应管理制度及措施,并监督公司人员严格执行。与部室及员工签订信息安全责任书,确保责任落到实处。通过组织职工收看信息安全方面的教育片和邀请专家来公司做安全报告,提高员工对信息安全的认知,增强员工遵守信息安全各项规章制度的自觉性。

### 1.13 设备隐患排查管理

1) 应建立健全设备隐患排查管理工作组织机构,制定并落实设备隐患排查管理方案,逐级落实从主要负责人到每个具体责任人的隐患管理责任。

2) 应制定完善设备技术和管理标准体系,建立健全安全生产责任体系。

3) 应广泛开展设备隐患排查管理教育培训,明确隐患排查评估、治理防范等各环节人员职责和工作标准,实现设备隐患的全过程管理。

4) 应切实落实设备隐患排查管理的主体责任,建立健全设备隐患排查治理体系,推进设备隐患分级分类管理。

5) 应实现设备隐患的检查发现、风险评估、

(下转第275页)

当频率增加到49.00 Hz时，J2（报警参数）及上行通道故障灯灭，如图5所示。



图5 频率升至定值区间，故障报警灯灭

再逐步增加，当增加至51.01 Hz时，信号灯重新亮起（即通道故障），如图6所示。



图6 频率超出定值区间，再次故障报警

3 展望

为更好地适应现场环境，更有易于运行人员掌握报警信息，将在以下几个方面逐步改进该装置的外观、大小和性能，具体如下：

- 1) 将两通道屏幕合并为单屏幕，并采用双显循环液晶显示，或者改进为触摸显示，更加人性化，便于运行人员观察。
- 2) 输入电源改为24 V或电池，适用的范围更加广泛。

(上接第257页)

分类评级、重点监控和治理改进各环节责任落实的闭环管理。

6) 应建立隐患统计分析和通报制度，对排查出的集中性或危险性较大的隐患，组织开展有针对性的专项整治活动。

7) 要会同有关部门对重大设备隐患进行挂牌督办和销号管理，实现重大设备隐患的闭环监管。

2 结束语

信息安全是一个相对的概念，通过努力构建一套不断完善的防护体系，使系统越来越安全。为了保护计算机系统里各种信息，通过管理、制度、技术和人多种层面的防护，使企业的信息系统受到最大程度的保护，从而保障企业及个人信息的安全。

参考文献

[1] 李展，刑博特. 防火墙与VPN[M]. 北京：清华大学

3) 从单一固定式安装到便携固定式安装，便于检修人员随身携带，易于故障的诊断。

4) 增加手机短信告知功能，通信中断后通过无线将报警发送至值班人员手机中，报警的时效性更强。

4 结束语

针对当前电力自动化通信抢修过程存在的困难和问题，提出了通信监控装置设计思路，通过对电源模块、采集模块和显示模块的分析研究和设计，最终实现通信监控装置的研制，现场测试表明，该装置的确能够对通信故障的类型进行准确判断，并在故障发生后，为变电站运行人员判断故障类型及通知相关维护部门提供直接的参考依据，降低了相关班组的通信故障抢修量，同时也降低了调度车辆及人员的经济成本。

(收稿日期：2015-05-26) EA

作者简介

卫春（1982-），男，工程师，从事电力系统继电保护与自动化运维管理工作。  
何涛（1982-），男，工程师，从事电力系统继电保护与自动化运维管理工作。

出版社，2008.

[2] 冯小安，祁兵. 电力信息系统安全体系的构建[J]. 电网技术，2008，32（S1）：77-80.  
[3] 夏婷婷，祁兵. 信息安全管理及平台研究[J]. 数字图书馆论坛，2009(9)：1-5.  
[4] GB/T 22239-2008信息安全等级保护基本要求[S].  
[5] GB/T 20269-2006信息安全管理体系要求[S].  
[6] GB/T 20271-2006信息安全通用安全技术要求[S].  
[7] GB/T 20272-2006操作系统安全技术要求[S].

(收稿日期：2015-05-26) EA

作者简介

解思江（1974年-），男，研究生，高级工程师，信息运行安全管理。  
焦阳（1983年-），男，本科，工程师，信息运行安全管理。