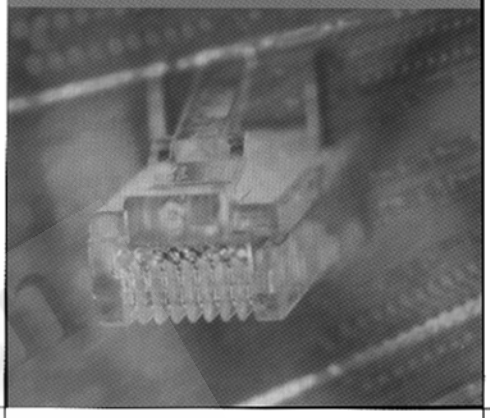
电力信息网络安全的实现(下)

Implementation of Security of Power Information Networks (Upper Part)

刘树吉 潘明惠 （沈阳 辽宁省电力有限公司 110006）



4.2.3 拨号访问安全方案

现有的拨号访问方式如图11所示。

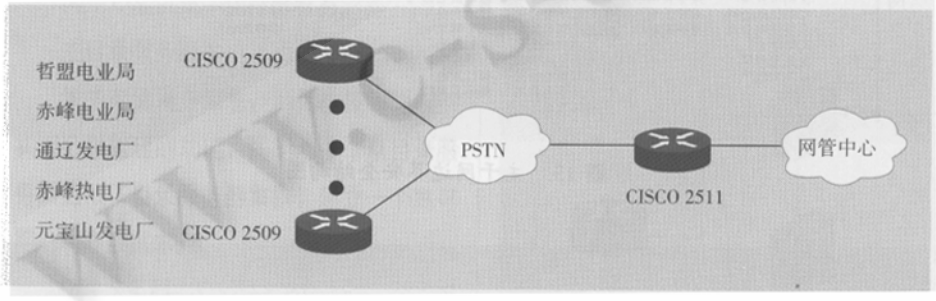


图 11 拨号访问结构图

拨号访问工作方式为：通过电信或系统电话拨号访问主干网，两端路由器使用相同的用户名和口令进行认证，此方式无法对拨号单位及个人赋以不同的访问权限，安全性和管理性有严重缺陷，存在很明显的漏洞。

远程拨号用户接入主干网，其基本安全配置如图12所示。

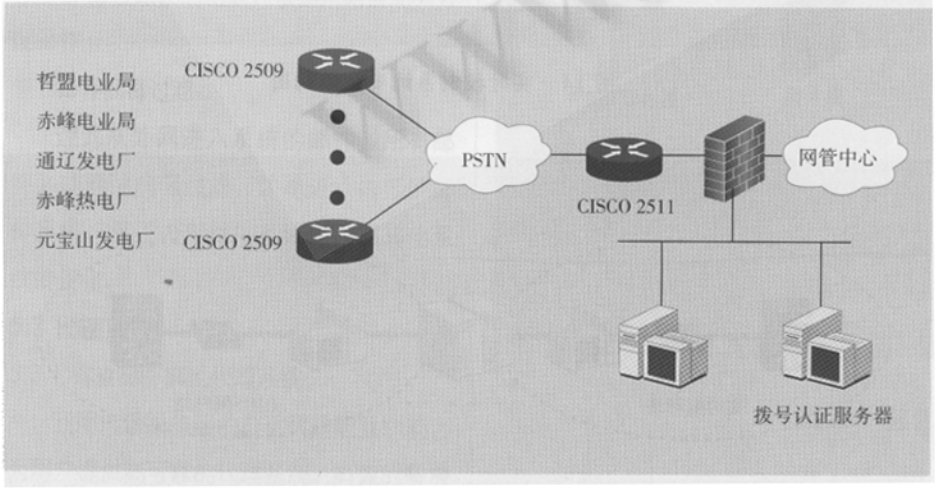


图 12 拨号访问安全结构图

由于远程办公和业务发展的需要，有部分用户可能需要更高的权限，能访问到内部网内的关键主机和服务器，仅靠防火墙和拨号认证服务器可以实现连接需求，但不能有效地保证系统安全。为了在满足特殊用户需求的同时保证系统安全，需要引入安全客户端和安全服务器，这种方案配置如下图所示。其中，安全客户端和安全服务器共同完成更高级用户身份认证功能，并在二者之间形成一安全通道。

4.2.4 边界安全方案

辽宁电力信息主干网边界安全采用防火墙技术，结构如图13所示。

基层有关单位可根据本单位网络连接情况，配置相应的防火墙，保证安全。

5 应用系统安全解决方案

对每个应用子系统进行安全分析，综合使用防火墙、身份认证、防病毒、加密、漏洞扫描等技术进行安全系统建设。

5.1 实时控制系统

根据国家电力公司要求，为了保证电力实时控制系统的安全性，调度自动化系统必须和管理信息系统之间实现有效的隔离，只能进行单向数据传输，要保证任何人、任何计算机、任何系统不能向调度自动化等控制系统的服务器、控制装置等设备写数据。

为保证实时控制系统的安全，我们采用在调度网络和外部网络汇接点上架设隔离设备，达到保障实时控制系统安全的目的。网络隔离设备可达到在不影响现有电力系统业务的情况下，将实时控制系统中的数据（包括实时数据与历史数据）单相发布到与其相连的MIS网或者其他电力系统业务系统网络中，同时防止信息网络中的非法数据进入调度网络，保障系统业务安全运营的目的。

先将两个网络进行隔离，切断网络路径；然后在隔离的基础上，通过面向调度应用的代理程序进行数据转发，完成数据交换。其中，隔离包括相关的过滤与访问控制，是通用的基础功能；代理功能可以针对不同的业务系统进行定制与增强。

系统实现结构如图14所示。

另外，由于大多数涉及到在调度网络和信息网络之间进行的数据通信都是基于以太网协议和TCP/IP协议的，所以通过指定的主机进行内外网络通信，可以缩小整个系统中发起两网之间通信请求的主机数，从而可以有效控制安全管理的范围。

此外，按照单向数据流通及作业透明的需求，隔离设备按照开放服务越少，系统安全性越高的网络安全原则，为了防止恶意的攻击和无意的数据破坏，仅开放能满足业务需求的服务，同时对指定的通信主机间的通信请求进行必要地控制与过滤，可以达到保证有效业务数据流的通过，阻止无用的数据侵袭和干扰，从而保障调度网络业务的安全运行。

基层有关单位必须按照国家电力公司的要求，在调度自动化系统和管理信息系统之间实现有效的隔离，具体实施由各单位根据具体情况采取相应措施，保证实时控制系统的安全。

5.2 邮件系统

（1）建立集中服务的邮件系统。现有邮件系统有两台设备，并为3个域提供服务。新的邮件系统将采用集中管理的模式，在一台

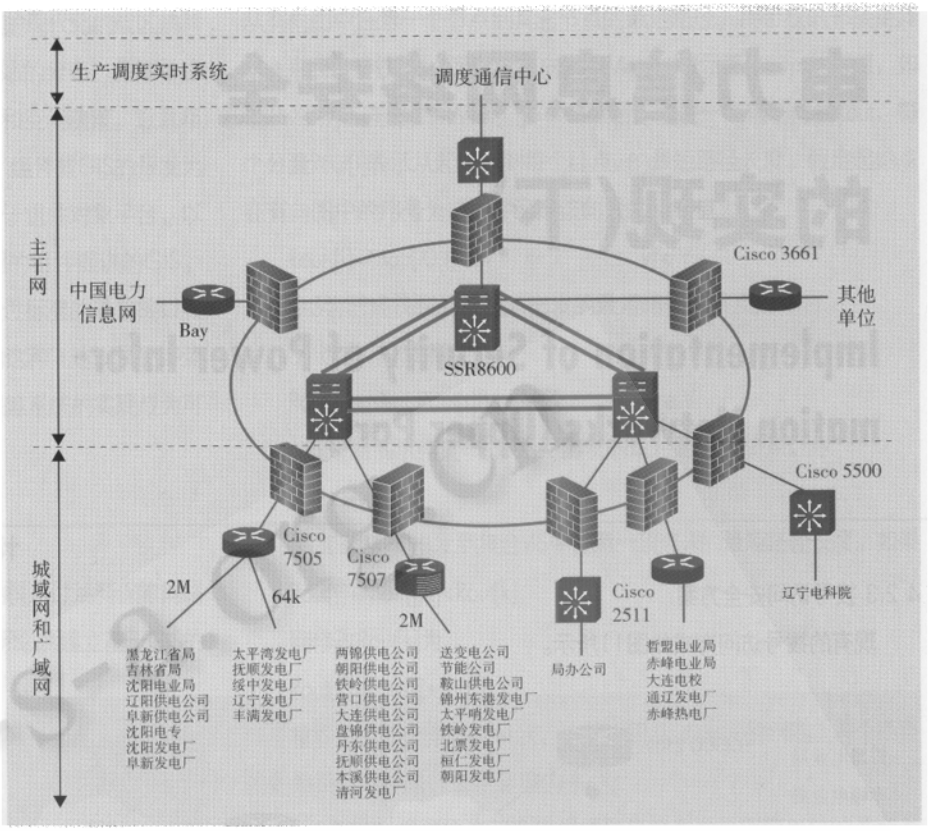


图 13　主干网边界安全结构图

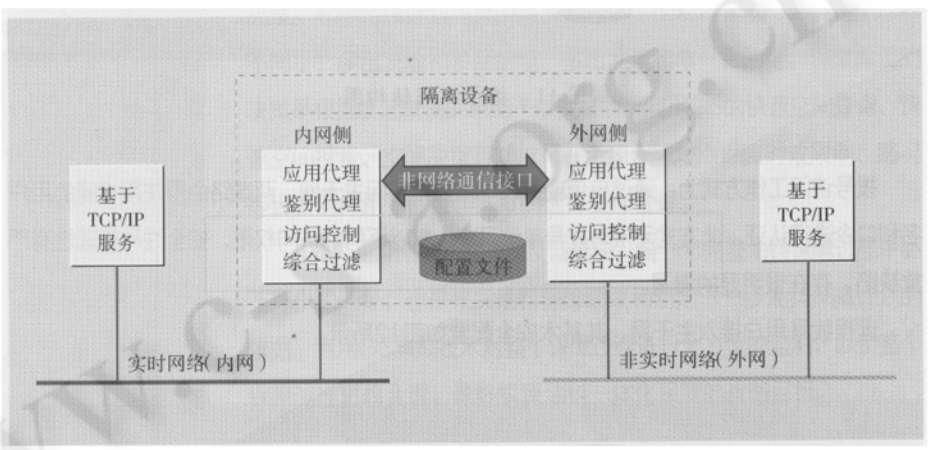


图 14　实时控制系统安全结构图

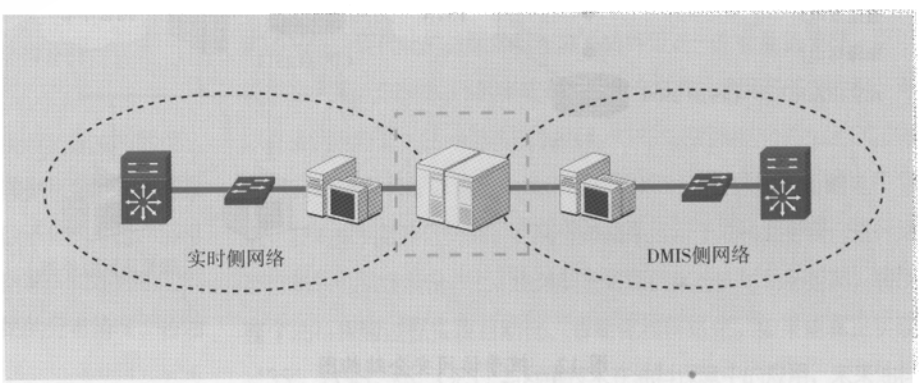


图 15

设备上运行，为多个域的用户提供集中的服务。利用邮件服务器邮件转发的功能，实现一个邮件服务器可以同时处理内网和外网的邮件。

（2）提供随时随地的访问能力。为企业用户提供基于浏览器访问和收发邮件的服务能力，用户可以在内网和Internet的任何地方，随时访问邮件系统，及时处理邮件。

（3）防病毒能力。新的邮件系统要能够对进入系统的邮件进行病毒扫描，保障内部系统的安全。

邮件系统体系结构如图16所示：

各服务器功能描述：

主邮件服务器：

为用户提供集中化存储服务。

主目录服务器：

集中存储用户信息，利用委托管理机制实现分级管理的功能，同时与多个从目录服务器组成了目录服务器集群，建立一个高可用的用户数据库。

邮件服务器：

防火墙外面的邮件服务器，主要提供下面的功能：

① 提供用户通过浏览器访问邮件系统的功能

② 为用户提供使用POP3、IMAP4访问内部邮件系统的功能

③ 邮件路由的功能，根据策略自动的分配邮件

邮件病毒过滤：

过滤从外网进入系统的邮件，所有邮件必须通过病毒过滤，才能进入内部的邮件系统，保证内部邮件系统和内部其他系统的安全。

5.3 代理系统

5.3.1 建立高可靠的代理系统

利用代理服务器的自动代理配置功能，为用户提供高可靠的代理系统，有效的解决一台代理服务器失效后，另外一台服务器可继续提供服务。

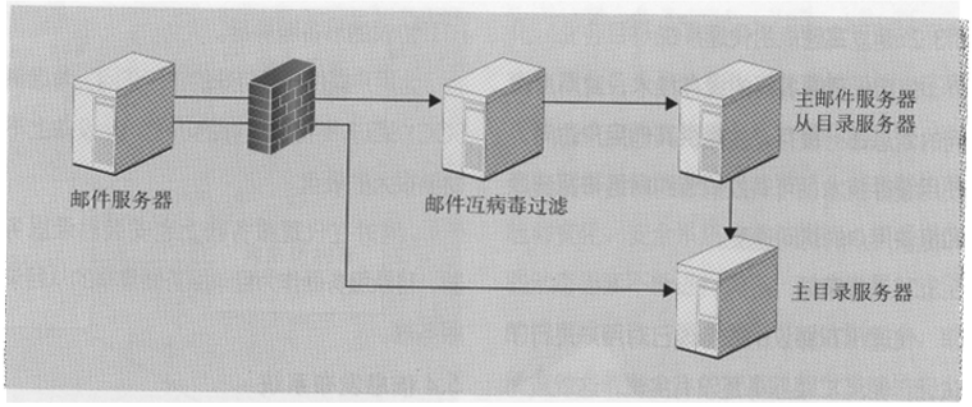


图 16　邮件系统安全体系结构图

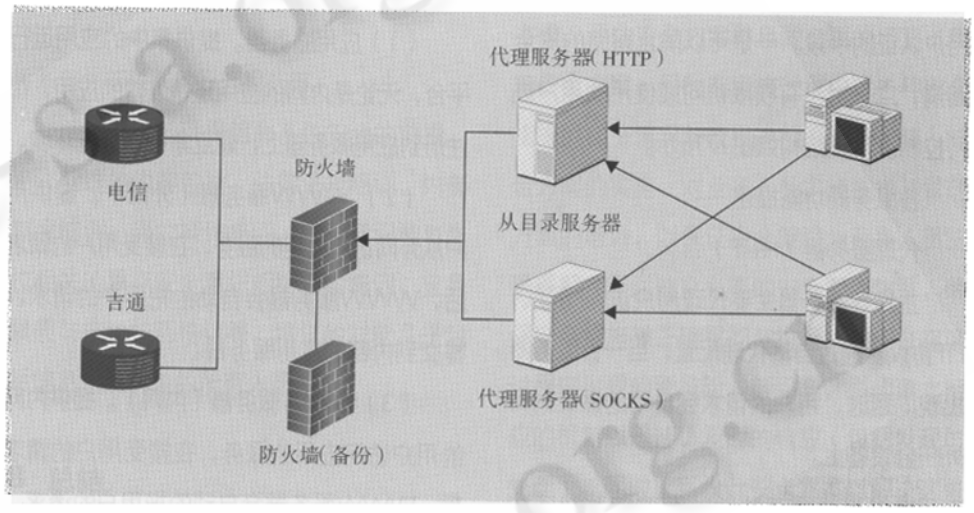


图 17　代理系统安全结构图

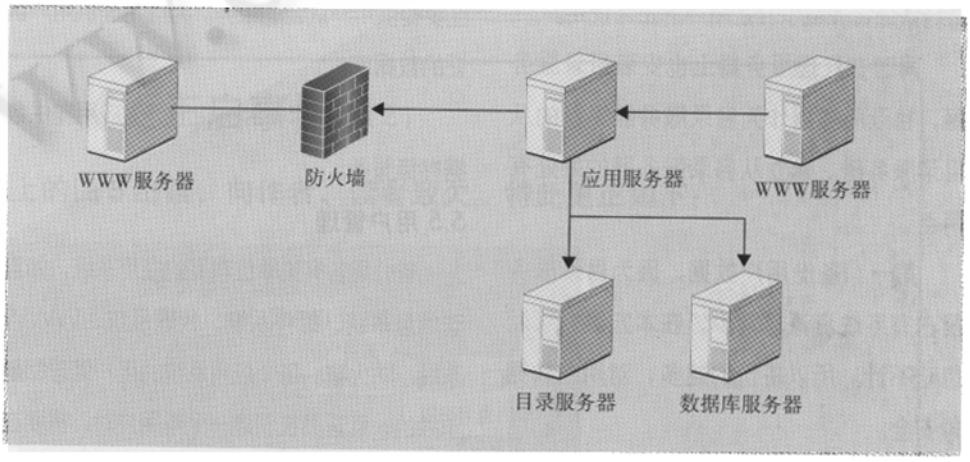


图 18　信息发布系统安全结构图

5.3.2 .建立高性能的代理系统

使用代理服务器的缓存技术，对用户访问的信息进行缓存，并提供其他用户访问，使用缓存技术，可有效的节约网络带宽资源和提供用户的访问速度。

5.3.3 认证策略

代理HTTP协议的服务现已对用户进行了认证，但SOCKS服务还没有实施，这就成为网络的一个安全漏洞，用户只要知道SOCKS服务的地址和端口，就可以在没有任何限制的情况下访问Internet。

在新的系统中，建议对SOCKS服务采取用户认证的手段。一是可以防止网络的安全漏洞，二是对没有权限访问或使用的用户进行控制。系统结构如图17所示。

各服务器功能描述：

代理服务器（HTTP）：

主代理服务器主要代理用户访问HTTP、FTP协议。通过自动代理配置，当一台服务器出现问题时，用户的请求会自动的提交到另外一台设备上。

提供高速缓存功能，有效的解决多个用户访问同一资源时，系统浪费网络带宽问题。

用户在使用代理系统时，系统会对用户进行认证，保障了合法用户的正常使用。

同时在代理服务器上也安装目录服务器，目录服务器作为目录服务器集群的从目录服务器。建立从目录服务器的好处有两点：

第一：备份用户数据，因为目录服务器占有系统资源非常少，在本方案中可以忽略不计。所以备份的越多，对用户数据越安全。

第二：提供用户认证。用户认证可以在本机完成，不用访问主目录服务器，节省网络资源。

代理服务器（SOCKS）

代理非HTTP、FTP协议的访问。同时作为HTTP协议的后备服务器。

为用户提供一些特殊的协议访问，考虑到SOCKS服务不提供缓存的功能，此设备上不需要很大的硬盘。

同时在代理服务器上也安装目录服务器，目录服务器作为目录服务器集群的从目录服务器。

5.4 信息发布系统

建立集中的信息发布系统，为内网和外网的信息发布系统提供统一的应用平台。系统结构如图18所示。

各服务器功能描述：

（1）应用服务器。提供集中的应用运行平台，无论是内网的应用还是外网的应用，都注册到应用服务器上，建立集中的运行环境。

（2）WWW服务器（外网）。提供用户从外网访问应用的服务，在接受用户的请求后，WWW服务器会自动的把用户的请求，提交到内部的应用服务器。

（3）WWW服务器（内网）。提供内网的用户访问应用的服务，在接受用户的请求后，WWW服务器会自动的把用户的请求，提交到内部的应用服务器。

（4）目录服务器。提供集中管理用户信息的服务，在应用系统的环境里，目录服务器主要提供用户认证的服务。为应用提供用户认证的数据库。

（5）数据库（Sybase）。为应用提供数据存储服务。

5.5 用户管理

省公司各有关单位现有的应用系统，如管理信息系统、邮件系统、代理系统、WWW系统、防火墙。每个应用系统的用户管理都是单独的，管理员在创建一个新用户时，需要在多个系统上创建，当用户离去时，如果不能及时把多个数据库中的用户删除，可能会造成一些非常严重的影响。因此，各辽宁电力信息网广域网连接有关单位必须逐步建立集中管理的用户数据库，提供用户认证服务，实现用户的单点登录。

6 逐步建立辽宁电力系统信息安全实验室

建立一个集信息网络平台和信息系统应用平台为一体的电力系统信息安全实验室，为研究信息安全提供环境，实现对网络安全产品和网络设备的功能与性能评测，对技术人员进行培训，模拟仿真事故，结合电网“黑启动”措施做好应急措施和紧急恢复，为制定各种信息安全反事故措施提供依据。并实时监测辽宁电力信息网络系统的安全状况。

通过建立信息安全实验室，对信息安全技术及其应用、信息安全与系统安全的策略和实施方案等领域展开深入的研究。争取在两年时间内进入国家级或省级、国家电力公司重点实验室行列。

在实验室的基础上建立一个信息安全监控中心，将各项信息安全应用技术进行有机整合，不论出现什么可能影响信息安全问题，均可尽快解决。对可能出现的异常或故障，按可监视的信息，提出预防措施，消除可能发生问题的条件，防止发生系统异常或故障，这可以称为信息安全预防性控制。另外，可根据国内、外出现过的网络信息安全事例，结合自身信息系统可能存在的问题和当前运行状态，编制各种运行方式，各类可能出现异常或故障的反事故措施，一旦出现威胁系统安全的异常或故障，采取措施，尽快处理，减少异常或故障对系统造成的影响。使由于异常或故障对系统运行造成的损失降到最低程度。这一措施可称为紧急性控制。

电力系统信息安全监控中心功能结构如图19所示。

7 安全管理（规范）

安全管理贯穿在安全的各个层次，实践一再告诉人们仅有安全技术防范，而无严格

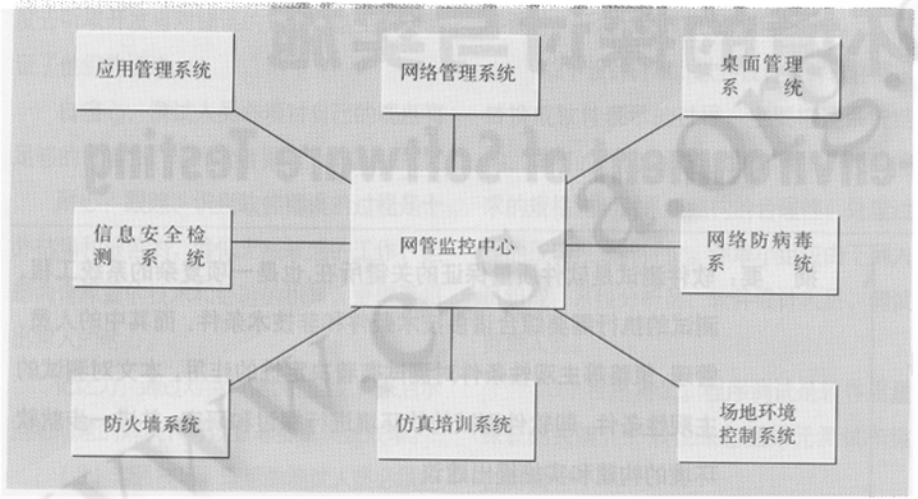


图 19　电力系统信息安全监控中心功能结构图

的安全管理体系相配套，是难以保障信息系统的安全的。必须制定一系列安全管理制度，对安全技术和安全设施进行管理。

管理是信息系统安全的灵魂。信息系统安全的管理体系包括法律管理、制度管理和培训管理等组成。

辽宁电力系统信息安全要严格遵守国家有关法律、法规。按国家和企业的安全需要，根据国家有关法律、法规制定一系列企业内部规章制度，主要内容包括：信息安全管理组织机构和执行机构的行为规范，岗位设定及其操作规范，岗位人员的素质要求及行为规范，内部关系与外部关系的行为规范等。

培训管理是确保信息系统安全的前提。培训管理的内容包括：法律法规培训、内部制度培训、岗位操作培训、安全意识和与岗位相关的重点安全意识相结合的培训，业务素质与技能技巧培训等。培训的对象几乎包括信息系统有关的所有人员。

8 总结

信息系统的安全不是一个状态或目标，而是一个持续不断的动态过程。其动态性不仅表现在企业信息系统的业务环境的不断变化，业务目标的不断变化，安全策略的不断变化及业务人员的变化，管理的变化，还表现系统安全的实施是个反复循环的过程：每个时期都有特定的目标与策略，都有新的风险与变化，安全系统方案与措施必须根据这些动态因素不断进行调整，以达到更加安全的程度或状态，而永远不可能达到安全，或所谓的“最安全”的状态。信息系统的安全过程就是这种趋于更加安全的过程。

辽宁电力信息安全系统将根据当前业务环境与安全目标，确定整体安全策略；然后在策略的指导下分析主要的风险，设计安全方案，评估安全方案并且做必要的修正；实施安全方案，同时在实施过程中对各种安全措施的实施情况与效果进行跟踪与审核；结合方案的实施，对业务人员实施技术与管理方面的培训，以保证安全策略为业务人员正确理解；同时建立必要的安全管理体系，确保安全措施被正确贯彻与执行；对于在实施过程中出现的新风险，新问题，必须建立相应的机制以迅速、及时的响应（包括发现与处理），同时重新设计安全方案以解决这些新的风险，开始又一个动态安全循环。