

电力数据通信网安全分析及解决方案

电力数据通信网承载着电力企业管理、办公、会议系统、软交换电话等多类业务，一旦发生异常或中断，将影响公司经营甚至社会用户的正常生活。对电力数据通信网进行安全分析，提出了建立安全管理体系、利用层次化模型加固以及动态安全管理模型³类解决办法，为提升电力数据通信网的安全可靠性提供借鉴。

王伟¹ 张敬² 李妍¹ / 1. 国网天津市电力公司信息通信公司 2. 中国电力财务有限公司华北分公司



王伟/工程师

关键词/Keywords

电力数据通信网 ·
安全分析 ·
解决办法 ·

0 引言

随着信息网络的不断发展，企业信息化与工业化不断深入融合，国家电网公司的信息化程度不断加深，信息网络已经与公司的生产、管理、经营、服务等各个环节紧密结合，成为电力系统不可或缺的重要基础设施和保障手段，发挥着越来越重要的作用。信息化应用的不断深入可以为公司带来很多优势，如提高工作效率、降低生产经营成本、开拓业务、提升服务质量和水平等，但是在信息化过程中如果缺乏对信息网络安全的高度重视，网络安全问题将会对公司产生十分严重的后果。网络异常或中断可能导致电网监控中断或异常停电，用户电表采集数据不及时、不准确甚至丢失，公司商业机密的泄露，公司对外服务中断、公司形象受影响，甚至可能导致公司整体工作的瘫痪等。因此，确保信息网络安全可靠非常重要。

1 电力数据通信网简介

电力数据通信网作为国网公司建

设的专用信息网络，用于承载企业信息内网、视频会议、音频软交换等多种业务。国网公司电力数据通信网分为骨干数据通信网（以下简称骨干网）和本地数据通信网（以下简称本地网）。骨干网用于连接各调度机构、基层单位、变电站、电厂以及独立通信站等节点，主要通过路由器组网形成的三层网络。本地网一般指范围较小的局域网，主要通过交换机组网形成的二层网络。

2 电力数据通信网的特点

(1) 网络规模大而复杂

电力数据通信网可分为骨干网和本地网，而骨干网又分为一级骨干网和省级骨干网。其中，一级骨干网覆盖全国所有省会城市及直辖市，省级骨干网覆盖省内各调度机构、变电站、电厂、基层单位以及独立通信站。本地网覆盖某个单位或某个数据中心或某个办公室。本地网接入到骨干网中实现整个电力系统内数据共享及业务访问。电力数据网的设备类型多种多样，既有国外的CISCO、Juniper等设备，又有国内华为、华三和中兴等设备，且同厂家的设备类型也各不相同。电力数据网使用的路由协议不但包括OSPF、ISIS、BGP和静态路由等，还运用MPLS VPN、隧道技术和IP SEC等。每个省级骨干网的设备数多达数百台，全国二十多个省/直辖市的设备总数多达数千台。

(2) 承载业务多而重要

按照电力二次系统安全防护规定中业务系统划分原则，电力数据通信网承

载除I、II区以外的管理信息大区业务。与调度数据网物理隔离，承载企业信息网、通信专网（视频、语音）等数据业务。其中，企业信息网包含企业办公OA及各个业务部门使用的应用系统，涉及到日常工作的方方面面，一旦出现问题，将会影响企业的正常生产和经营；电视电话会议系统作为公司提高工作效率的重要手段，如果网络不能正常运行，将会影响各单位之间的沟通交流，影响工作进度；软交换电话系统的网络发生故障，电话无法与外界联系，极大地影响调度生产和日常办公。

(3) 管理难度大而烦琐

电力数据通信网中一级骨干网以及每个省级骨干网的运维单位均不同，每个本地网的运维单位也不同，众多人的日常行为都有可能对电力数据网带来不安全的因素。如办公人员误将一根网线2端同时接入1台本地网交换机导致形成二层环路引发网络瘫痪；网络设备数据配置错误导致网络大面积中断，等。变电站及部分基层单位的本地网络规模较小，运维人员少，运维能力较差，存在较大的安全隐患。

3 安全风险分析

(1) 网络外部攻击

通过网络传播的病毒、木马等日益猖獗，不法分子对电力企业网的入侵及攻击的形势也越来越严峻。网络攻击者通过篡改公司对外网站会干扰公司正常的对外业务，影响公司形象；通过对网络进行攻击可造成网络系统瘫痪，影响公司的正常工作和经营。

(2) 网络内部安全风险

目前，网络内部的安全问题已越来越突出，来自内部的安全风险主要包括：①终端中病毒或木马后自动向网络进行攻击；②窃取者利用局域网中的一台主机，通过网络攻击或欺骗的手段非法取得内网中其他主机或服务器的数据；③破坏者将非法网络设备接入网络，获取网络信息，破坏网络的正常连通。

(3) 网络结构风险

网络设计存在缺陷，路由协议选择不正确导

致运维难度较大；网络层次不清导致路由混乱；网络结构单点故障隐患等薄弱点导致网络的效率较差等。

(4) 设备及物理风险

网络设备存在单电源、单引擎，设备的物理环境较差，温度、湿度、灰尘和防小动物等方面难以满足设备运行条件等。可能导致设备断电引发数据丢失甚至设备损坏。

(5) 网络操作风险

新设备接入网络、网络结构调整等网络操作时，如果方案论证不够细致，可能导致网络承载业务异常中断。

(6) 管理安全风险

没有管理的约束，会导致一些员工或外来人员轻易进入机房重地，或者随意将设备接入网络，可能引发网络的突发问题，导致网络中断。

4 解决方案

4.1 建立完善的网络安全管理体系

电力数据通信网安全需要通过一套体系进行保障，体系中包含了方针、目标、职责、过程和监控五个部分，如图1所示。

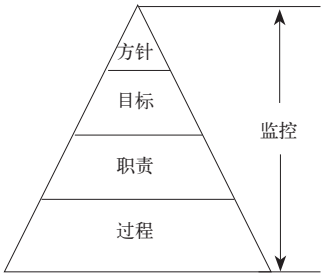


图1 网络安全管理体系

网络安全管理体系的方针为：安全第一、预防为主、综合治理。这“十二字方针”也是自2014年12月1日起施行的新修订《中华人民共和国安全生产法》的方针。

网络安全管理体系的目标要符合SMART（Specific、Measurable、Attainable、Relevant、Time-bound）原则，即明确的、量化的、可行的、相关性和时限性。网络安全管理体系的职责即通过公司制订、下发相关的规章制度来明确。过程即依照职责分工开展网络安全管理

的各项工作。监控即及时掌控方针、目标、职责、过程的科学性、合理性、先进性及符合度，不断提高完善。

4.2 利用TCP/IP模型分层加固

网络接入层与OSI模型的物理层、数据链路层相对应。物理层的功能是传输在线缆上的电子信号。用于传输的线缆类型包括光纤、双绞线和同轴电缆。物理层的安全一方面从设备选型、板卡冗余度、环境可靠性、机房管理规范性等方面加强，另一方面可使用加密、流量填充等技术实现信息有效的保护。数据链路层提供了网络实体间互操作和与其他层互联的功能化和程序化传输数据的方法。交换机作为数据链路层典型设备，其安全性直接影响上面各层。可通过风暴控制、受保护端口、专用虚拟局域网、端口阻塞和端口安全特性加固交换机安全。

网络层即IP层，典型设备为路由器和三层交换机。数据通信网由路由器或三层交换机组网形成，通过设计科学、可靠、清晰的网络架构，部署边界防火墙、访问控制列表（Access Control List，ACL）等加强网络层安全。

传输层包括两个协议：TCP和UDP，这两个协议均通过端口号来标识主机上的不同服务。一般通过多层防火墙控制端口的访问，提高安全性。

应用层直接面向用户，最常见和最常用的有Telnet、FTP、SMTP和HTTP等。应用层的多样化为用户提供了丰富的服务，但同样带来了大量的安全风险。病毒、木马、蠕虫、SYN flood攻击、Smurf攻击等危害很大。可通过部署防病毒系统、流量过滤系统、多因素验证系统、认证加密系统等，使用SSH、HTTPS等安全性较高的协议，提升安全等级。

4.3 利用动态安全管理模型

PDRR模型是一个常见的安全模型，由Protection（防护）、Detection（检测）、Response（响应）、Recovery（恢复）四个方面组成了一个信息安全周期，如图2所示。

通过实时检测数据通信网，及时发现安全问题并进行响应，消除问题恢复业务使用，总结经验教训增强防护。每一步都是依照安全策略去执行，而每完成一步反过来优化、更新安全策略，

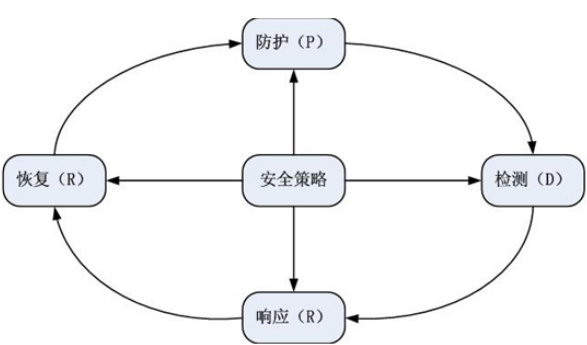


图2 PDRR安全管理模型

实现数据通信网安全的动态管理，不断提升网络安全可靠性。

5 结束语

随着电力数据通信网的规模及作用越来越大，其安全性也愈发重要。只有实时掌握网络安全状态，及时分析并消除网络安全隐患，才能确保网络运行的安全稳定。本文通过对电力数据通信网安全风险分析，提出了管理体系化、技术层次化、管理与技术相结合的安全管理模型，为提升电力数据通信网安全性提供了参考和借鉴。

参考文献

[1] Yusuf Bhaiji. 网络安全技术与解决方案(Network Security Technologies and Solutions)[M]. 罗进文, 王喆, 张媛, 等, 译. 北京: 人民邮电出版社, 2009.

[2] 李威, 顾海林. 辽宁电力数据通信网安全体系研究与建设[J]. 电信技术, 2014(12): 88-91.

[3] 康洸. 对数据通信网络维护及网络安全的探析[J]. 中国新通信, 2013, 15(16).

[4] 李彪. 电力信息网络安全防范措施分析[J]. 才智, 2013(23): 315.

[5] 杜昭. 电力企业的信息网络安全与防护[J]. 科技风, 2013(3): 260.

作者简介

王伟 (1983-), 男, 工程师, 主要研究方向为电力系统信息通信运维。

张敬 (1981-), 女, 工程师, 主要研究方向为电力系统信息通信运维。

(收稿日期: 2015-12-10) EA

(编辑: 鞠佳)