# 论网络安全架构

**摘要：**

省级电力企业系统网络变得越来越庞大，结构也越来越复杂，管理变得十分困难，网络安全问题凸现。由于缺乏统一的网络建设规划，省级电力企业系统内的各局域网络架构各异，采用技术各不相同，网络安全布防不规范，安全产品不统一，给安全体系建设带来了极大的挑战。因此本文主要介绍了如何建立以安全策略为核心、以安全技术为支撑、以安全管理为手段的网络安全体系。同时根据**省电网综合业务数据网络总体项目，来介绍启动局域网络标准化改造、统一互联网出口、综合业务数据网络安全防护建设及网络安全管理模式建立等一批网络安全措施。同时，制定了“安全分区、网络专用、横向隔离、纵向认证”的总体防护策略，并提出了“三层四区”安全防护体系的总体框架，这对电力企业网络安全体系建设进行了有益的探索和实践。

**正文：**

2007 年开始，**省电网公司启动了**省电网公司企业信息化工程。目的是为了实现在省级电力企业系统内，进行一体化管理，实现各分支网络之间互联互通。项目重点是建设好电网综合数据网络，同时实现所属单位局域网及厂、站信息传输通道全面接入；形成**省电网公司综合业务处理广域网络。同时还将进一步建设专门的调度数据网络，实现“专网专用”，从而确保电力生产安全有序的开展。本人为**省电网公司总工，负责**电网公司的信息化的规划和管理。

**省电网生产、办公等各个领域当中，无论是企业内部管理还是各级机构间的远程信息交互，都将建立在网络基础之上，而通过网络进行交互的信息范围也涵盖了包括生产调度数据、财务人事数据、办公管理数据等在内的诸多方面，在这样的前提下，进一步完善企业网络架构，全局性和系统性地构建网络安全体系，使其为企业发展和信息化提供有力支持，已成为当前需要开展的首要工作之一。

**1．网络安全技术架构策略**

规范网络技术架构、互联标准及安全区域划分、统一 Internet 出口是电力企业广域网络安全面临的主要任务，网络安全建设是一项系统工程，贵州电网广域网络安全体系建设按照“统一规划、统筹安排、统一标准、相互配套”的原则组织实施，采用先进的“平台化”建设思想、模块化安全隔离技术，避免重复投入、重复建设，充分考虑整体和局部的关系，坚持近期目标与远期目标相结合。在贵州电网广域网络架构建设中，为了实现可管理的、可靠的、高性能网络，采用层次化的方法，将网络分为核心层、分布层和接入层 3 个层次，这种层次结构划分方法也是目前国内外网络建设中普遍采用的网络拓扑结构。在这种结构下，3 个层次的网络设备各司其职又相互协同工作，从而有效保证了整个网络的高可靠性、高性能、高安全性和灵活的扩展性。

**2. 局域网络标准化**

局域网络标准化以网络拓扑结构模块化、层次化为设计原则，网络结构主要由核心层、分布层和接入层组成，在网络结构层次化的基础上根据数据中心各业务功能分区的不同把网络分为多个功能模块化分区。

（1）中心交换区域。局域网的中心交换区域负责网络核心层的高性能交换和传输功能，提供各项数据业务的交换，同时负责连接服务器区域、网络管理区域、楼层区域、广域网路由器和防火墙设备等，此外还要提供分布层的统一控制策略功能。具体到安全防护层面，可通过部署防火墙模块、高性能网络分析模块、入侵探测系统模块实现安全加固。

（2）核心数据服务器区域。因为数据大集中和存储中心已经势在必行，可建设专门的核心数据区域，并采用 2 台独立的具有安全控制能力的局域网交换机，通过千兆双链路和服务器群连接。在安全防护方面，可在通过防火墙模块实现不同等级安全区域划分的同时，部署 DDoS 攻击检测模块和保护模块，以保障关键业务系统和服务器的安全不受攻击。

（3）楼层区域。楼层交换区域的交换机既做接入层又做分布层，将直接连接用户终端设备，如 PC 机等，因此设备需要具有能够实现 VLAN 的合理划分和基本的 VLAN 隔离。

（4）合作伙伴和外包区域。提供合作伙伴的开发测试环境、与内部数据中心的安全连接及与 Internet 区域的连接通路。

（5）外联网区域。电力营销系统需要与银行等外联网连接，建议部署银行外联汇接交换机，通过 2 条千兆链路分别连接到核心交换机。并通过防火墙模块划分外联系统安全区域。

（6）网络和安全管理区域。为了对整个网络进行更加安全可靠的管理，可使用独立的安全区域来集中管理，通过防火墙或交换机模块来保护该区域，并赋予较高的安全级别，在边界进行严格安全控制。

**3．统一互联网出口**

对于省级电网公司的广域网络，统一互联网络出口，减少企业广域网络与互联网络接口，能够有效减少来自外网的安全威胁，对统一出口接点的安全防护加固，能够集中实施安全策略。面对各个供电企业局域网络都与互联网络连接的局面，将会给电力企业广域网络安全带来更大的威胁。由于综合业务数据网络作为相对独立的一个大型企业网络，设置如此众多的互联网出口，一方面不利于互联网出口的安全管理，增加了安全威胁的几率；另一方面也势必增加互联网出口的租用费用，提高了运营成本。

在省中心设立统一的互联网接入区域，通过多条链路连接到不同的互联网接入提供商，实现多条链路的负载均衡，提供可靠的互联网进出服务；并在此基础上逐步取消供电局的本地接入，最终实现到省中心互联网接入区服务的平滑过渡。由于**电网综合数据网的骨干带宽是 622 M，在综合数据网络上利用 MPLS VPN 开出一个“互联网 VPN”，使各供电局的互联网访问都通过这个 VPN 通道建立链接。通过统一互联网络出口，强化互联网接入区域安全控制，可防御来自 Internet 的安全威胁，DMZ 区的安全防护得到进一步加强；通过提供安全可靠的 VPN 远程接入，互联网出口的负载均衡策略得到加强，对不同业务和不同用户组的访问服务策略控制，有效控制 P2P 等非工作流量对有限带宽的无限占用，能够对互联网访问的 NAT 记录进行保存和查询。

**4．三层四区规划**

提出“安全分区、网络专用、横向隔离、纵向认证”的总体防护策略，并提出了“三层四区”安全防护体系的总体框架。基于这一设计规范，并结合**电网的实际情况，未来公司的网络区域可以划分为电力生产系统和电力管理信息系统，其中电力生产系统包括 I 区和 II 区的业务；电力管理信息系统包括 III 区和 IV 区的业务。I 区到 IV 区的安全级别逐级降低，I 区最高，IV 区最低。

在上述区域划分的基础上，可在横向和纵向上采用下列技术方式实现不同安全区域间的隔离。

（1）纵向隔离。可考虑在未来调度数据网建成后，将安全区 I 和安全区 II 运行在独立的调度数据网上，安全区 III 和安全区 IV 运行在目前的综合数据网上，达到 2 网完全分开，实现物理隔离。在调度数据网中，采用 MPLS VPN 将安全区 I 和安全区 II 的连接分别分隔为实时子网和非实时子网，在综合数据网中，则采用 MPLS VPN 将互联网连接和安全区 III 及安全区 IV 的连接分开，分为管理信息子网和互联网子网。

（2）横向隔离。考虑到 I 区和 II 区对安全性的要求极高，对于 I 区和 II 区进行重点防护，采用物理隔离装置与其他区域隔离；而在 I 区和 II 区之间可采用防火墙隔离，并在变电站以上的级别部署 IDS/IPS 模块，配合分布式威胁防御机制，防范网络威胁；考虑到 III 区和 IV 区之间频繁的数据交换需求，III 区和 IV 区之间视情况采用交换机防火墙模块进行隔离，并在区域内部署 IDS 等安全监控设备，在骨干网上不再分成 2 个不同的 V P N；由于外部的威胁主要来自于 Internet 出口，因此可在全省 Internet 出口集中的基础上，统一设置安全防护策略，通过防火墙与 III 区、I V 区之间进行隔离。

**5．综合数据网安全防护**

综合业务数据网，主要承载了 OA、95598、营销、财务等应用系统，同时也在进行 SCADA/EMS 等调度业务的接入试点。

采用网络安全监控响应中心为核心的分布式威胁防御技术，对全网的病毒攻击和病毒传播进行主动防护，通过关联网络和安全设备配置信息、NetFlow、应用日志和安全事件，从中心的控制台实时发现、跟踪、分析、防御、报告和存储整个企业网络中的安全事件和攻击。同时分布式威胁防御手段不但用于对综合数据骨干网进行安全防护，而且通过建立 2 级安全监控响应中心，对包括综合数据网、省公司局域网、供电局局域网、分县局和变电站局域网、分县局和变电站接入网在内的全网设备进行监控。

**6．总结**

局域网、广域网、互联网以及电力系统特有的三层四区架构从技术层面形成了一套较为完备的网络安全防护体系，但“三分技术、七分管理”，在进行技术改良的同时，还需要对公司的网络信息安全管理进行相应的优化调整，可将目前分散化的管理模式转变为合乎未来发展趋势的集中式管理模式，并通过设置专门的网络信息安全管理职能部门加强对相关规章制度执行效果的管控，突出安全管理主线，从而真正实现技术与管理的齐头并进，为企业营造一个高效、安全的网络环境。