

基于电力通信网的电力调度数据网安全传输

郭亮

国网陕西西咸新区供电公司 陕西 西咸新区 712000

[摘要]在电力资源成为大众日常不可缺少的重要能源的背景下,为保证电网可靠、安全的运行,需要加强对电力调度数据网安全传输的关注度,并且选择科学的方式,提高网络传输水平。

[关键词]电力通信网; 电力调度数据网; 安全传输

[DOI] 10.12252/j.issn.2096-627X.2021.10.358

1 电力通信网

电力通信网是国家专用通信网之一,是电力系统不可缺少的重要组成部分,是电网调度自动化、电网运营市场化和电网管理信息化的基础,是确保电网安全、稳定、经济运行的重要手段。电力通信网最重要的特点是高度的可靠性和实时性;另一特点是用户分散、容量小、网络复杂。电力通信主干网络基本上成树形与星形相结合的复合型网络结构。电力系统通信网按业务的种类分为电话及传真网、数据通信网、图像通信网、可视电视电话网等等;按服务区域范围分为本地通信网、长途通信网、移动通信网等等。电力系统中常见的通信网络有电话交换网、电力数据网、电视电话会议网、企业内联网INTRANET等。电力数据网包含传统的远动信息网(SCADA系统)、EMS、MIS等。

2 电力调度数据网安全防护设计原则

电力调度数据网为确保数据传输安全性进行防护设计,应严格遵循“安全分区、网络专用、横向隔离、纵向认证”的基本原则,构建电力调度数据网的安全防护工作体系,避免出现电力调度数据传输期间业务数据瞬时性中断影响网点正常运转的情况。此外,还需要确保电力调度数据网所对应外部防护级别符合规约要求,避免因恶意攻击数据网出现系统瘫痪或数据泄漏问题。电力通信网的工作人员必须高度重视电力调度数据网安全防护的有关工作,以免干扰电力系统的正常运转。

3 电力调度数据网安全防护设计措施

安全二区与三区的隔离,优先选择电力专用安全隔离装置。二区数据搭载电力专用正向物理隔离装置实现与三区的同步,三区数据在电力专用反向物理隔离装置的辅助下实现与二区的同步。需要特别注意的是,电力调度数据网运行过程将CC-2000A系统的CIM模型和潮流数据传输至电能采集系统时,遵循安全防护基本原则进行逻辑隔离。为避免CC-2000A受到系统的不良影响,提高数据传输的安全性水平,将相关潮流数据文件及CIM模型从SCADA服务器终端传输至内平台服务器时,需要通过正向隔离装置传输至Web服务器平台,再通过电能采集系统三区网关和反向物理隔离装置的处理,最后传输至二区网关机内完成数据传输任务。整套安全防护系统的运行应满足现行规范中4级安全防护等级要求,关系数据库应满足现行规范中3级安全防护等级要求。电力调度数据网安全传输防护设计结构示意图,如图1所示。

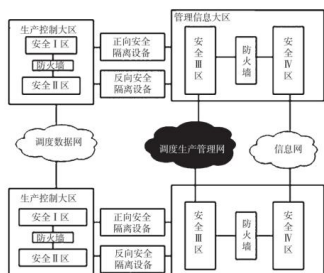


图1 电力调度数据网安全传输防护设计结构示意图

3.1 专网专用

基于互联网地址构架,专网以RFC4193和RFC1918为互联网规范标准,遵循IP协议应用私有地址网络。需要注意的

是,数据传输过程中,基于IP协议的私有地址网络无法直接与互联网进行联通,经公网转发后才能正常传输与使用。因此,在电力调度数据网传输期间必须搭载专用光纤通道满足网络的通信需求,提高数据传输的高效性。基于专网专用的构建模式尽可能提升安全防护等级,以专网专用的方式连接私有地址网络和互联网,避免网络数据传输期间遭受不良攻击与破坏,虽然成本相对偏高,但可保障数据调度的安全性。

3.2 横向隔离

在专网专用的基础上,可通过横向隔离的方式进一步提升电力调度数据网安全防护工作水平。横向隔离措施的应用提升了生产网络安全习惯,将恶意破坏信息拦截在专网之外,确保内部网络信息交流传输的安全性。可以选择的隔离措施包括路由器隔离、防火墙隔离以及DCS系统隔离等。通过过滤互联网中的恶意信息,不仅可提升生产效率,还提升了数据网络安全性水平。在安全防护系统构建过程中引入横向隔离,就好比为电力调度数据网的数据传输提供了一层保护罩,是切实保障电力调度数据网传输安全性的关键。

3.3 纵向认证设计

纵向认证措施的关键在于提升电力调度数据网安全防护工作等级,避免信息在传输过程中出现被恶意盗用的现象。电力调度数据网设置期间,可以沿主路由器和交换机的中间区域增设一定比例的纵向加密网关,加密处理电力调度数据传输期间的所有节点,从而提升安全防护整体等级。受保护机制的影响,一旦出现交换机收发报文不一致的情况,通信网关会立即发送安全预警的工作指令,将安全保护切换至自动启动状态。因此,纵向认证可以隔离互联网数据传输期间的恶意信息,提升安全性水平。

3.4 安全分区

遵循电力调度数据网安全设计的相关原则,以电力调度数据网安全区域为基准进行合理划分,形成管理信息分区和生产分区两个部分。它们在防护要求及防护标准上存在一定的差异性,可满足安全防护的实际工作需求。从安全防护职责的角度上来说,管理信息分区应当参考电力调度数据网实际运行期间的非实时性子网状态实现系统化运转,以电力资源的合理调度为业务核心,负责包括极端天气检测、电力统计报表制作生成、客户服务以及自动化服务等在内的系统运转。生产分区以电力调度自动化系统维持运行为核心工作任务,兼顾变电站自动化控制和安全自发性控制等功能的实现。相较于非实时性子网安全防护等级而言,实时性子网对应等级和标准更高,因此只有合理划分安全区域,才能使整个电力调度数据网安全防护系统状态达到最佳。

4 结束语

调度数据网的传输是否安全可靠,会直接影响电网运行的安全性和稳定性。因此对基于电力通信网的电力调度数据网安全传输进行探讨具有重要的现实意义。

参考文献

[1]江浩,邓翔,黄斌,等.有关大数据的电力信息通信预警技术分析[J].网络安全技术与应用,2020(1):112-113.
[2]沈霏.基于电网运行稳定性的电力通信综合网管系统设计[J].各界,2020(2):161-161.