调控终端安全管控技术研究与应用

王先强,张 睿,张 华
(国网四川省电力公司南充供电公司,四川 南充 637000)

摘 要:在能源互联网和电网智能化的发展趋势下,各类新型电网业务和工作场景访问调度主站系统的需求增多,需要规范调度终端的权限配置,加强操作过程安全审计,完善管理制度和技术手段,有效防范安全攻击,提升应对极端情况的风险防控水平。通过对现有调度终端键盘、显示器、鼠标延伸技术的使用现状分析,提出了一种基于云计算和生物多因子认证的调控终端安全管控技术。该技术根据电网调度自动化的业务场景,融合计算虚拟化、网络虚拟化、存储虚拟化、运维监控管理、云桌面业务流程交付等软件技术,形成标准化的调控终端安全管控系统解决方案。

关键词:调度终端; 调控终端安全管控;云计算;生物多因子认证
中图分类号:TV 171 **文献标志码**:A **文章编号**:1003 - 6954(2021)04 - 0043 - 07
DOI:10.16527/j.issn.1003 - 6954.20210409

Research and Application of Security Control Technology for Dispatching Control Terminal

Wang Xianqiang, Zhang Rui, Zhang Hua
(State Grid Nanchong Electric Power Supply Company, Nanchong 637000, Sichuan, China)

Abstract: Under the intelligent development of energy Internet and power grids, various new power grid services and work scenarios have a increased demand for the access to dispatching master station system. It is necessary to standardize the authority configuration of dispatching terminals, strengthen the safety audit of operation process, improve the management system and technical means, which can effectively prevent security attacks and improve risk prevention level in response to extreme situations. By analyzing the current status of the use of KVM(keyboard, video, mouse) extension technology for dispatching terminals, a regulatory terminal security control technology based on cloud computing and biological multi-factor authentication is proposed. According to the business scenarios of power grid dispatching automation, the proposed technology integrates software technologies such as computing virtualization, network virtualization, storage virtualization, operation and maintenance monitoring and management, and cloud desktop business process delivery to form a standardized regulatory terminal security management and control system solution.

Key words: dispatching control terminal; security control technology for control terminal; cloud computing; biological multi-factor authentication

0 引 言

随着电网业务模式的逐步改革,除传统的县/区调度外,现货交易、检修公司、集控站运维班等调度以外的单位也有着连接访问调度主站系统,并对与之业务相关的电网运行数据、厂站设备信息等进行运行监控和信息查询的需求。

国家电网有限公司在 2020 年提出建设具有中国特色国际领先的能源互联网企业的宏伟目标,各项工作正在加紧步伐开展建设,各类新型电网业务和工作场景中访问调度主站系统的需求将会更多。

在目前国家电网有限公司“调控一体化”的运行管理模式下,县/区调及检修公司等基层调度单位已无独立的调度主站系统,完全依赖地市调度端主站系统,在此应用背景下调控人机工作站终端成为

了基层调度单位工作人员访问主站系统的唯一工具,其重要性不言而喻。

目前各级调度单位所使用的调控人机终端,仍为传统物理图形工作站,以国网四川省电力公司南充供电公司(以下简称南充公司)为例,调度员工作站30台,监控工作站30台,运维工作站18台,培训模拟工作站6台,未来延伸至检修公司及各变电站运维检修工作站需30台,共计114台。

目前,影响调度人机工作站稳定安全运行和无法实现集中统一管控的主要因素有以下4个方面。

1)县供电公司、变电站端与市级调度自动化主站系统之间的调度数据网带宽有限,县供电公司、变电站端工作站与调度自动化主站系统之间发生模型、图形下载、数据更新等批量操作和大数据量更新时,会阻塞站端与主站系统的网络通道,使工作站无法正常操作,影响站端实时数据上传。远端调度终端与主站系统的数据通讯流量峰值超过50 MB,远端查询调度自动化主站系统中历史数据时,从提交查询到出现查询结果超过2 min。

2)现货交易大厅、集控站、第三应急调度大厅等需进行工作站延伸的办公场所,在网络安全防护技术手段、基础设施和运行环境上相较调度中心仍待完善,尚无法达到调度系统安全Ⅰ区的系统运行安全要求,易导致通过非工作站设备的违规接入调度生产大区网络和工作站上的重要数据外露。

3)人机工作站的管理和维护完全依赖地市级调度中心,以四川南充地调与所属阆中县供电公司为例,两地相距近90 km,人机工作站被广泛应用在各区县供电公司、现货交易大厅、集控站、第三应急调度大厅等地后,造成工作站出现故障后无法及时响应且维护成本高、周期长。

4)为满足网络安全要求,需定期对工作站操作系统、应用客户端进行安全漏洞检查、补丁加固、程序版本升级等工作,手工进行此类频繁且琐碎的工作容易出现纰漏,并需占用大量的人力资源。

下面研究了应用于调控人机交互终端安全管控领域的关键技术,提出基于能源互联网的调控终端集中管控系统整体框架,重点研究了调控终端集中管控软件的架构及功能,并在南充公司地、县两级调度中心进行了示范应用,为后期调控终端运行工况及调控人机交互终端安全管控领域的发展提供实时数据。

1 调控终端安全管控技术现状

国家电网有限公司各级调控中心本部或是延伸至县、区供电公司及检修公司、运维班、集控站等地所使用的调控终端主要采用物理工作站结合键盘、显示器、鼠标(keyboard video mouse,KVM)延长器的技术形式进行安全管控。

1)该技术形式需要为每位调度员及相关运维人员均分配1台独立的图形工站,每台工作站的硬件操作系统、应用、补丁均需逐个在现场进行安装、维护和调试。

2)工作站集中部署在调度机房中,工作站1台占用2U机柜位置,大量工作站会占据大量机房空间。

3)使用KVM延长器进行显示画面延伸,实现人员和设备之间进行简单的物理距离、空间隔离。但使用时网络带宽占用高,无法满足目前国家电网公司变电站通道多为2 M的窄带宽通讯现状,且通讯链路无加密等安全防护手段。

4)调度台及各办公工位无工作站主机,通过KVM延长器连接相应人机交互外设。主站系统操作确权所需的安全ukey识别率较低影响工作效率。USB外部设备可随意接入使用,存在数据漏风险。延长器无生物因子安全认证功能,账号密码易泄漏。

5)操作人员使用KVM延长器操作工作站时,对调度控制主站系统的操作过程无法进行审计和记录,无不合规操作进行责任追溯和源头分析能力,无法实现危险指令的阻截。

2 基于云计算和生物多因子认证的调控终端安全管控技术

针对目前调度终端工作站分布广、数量多、维护困难且成本高,新应用安装部署繁琐、周期长,外设无法有效管控,违规操作无法追踪,安全事故无法回溯等问题,将计算虚拟化、网络虚拟化、存储虚拟化、融合运维监控管理、云业务流程交付等软件技术应用于调控终端安全管控,形成基于云计算技术的终端操作系统桌面交付与“云桌面”管理解决方案,并可以根据电网调度自动化的业务场景,定制标准化的调度人机交互终端系统模板。利用调度数据专网聚合多套X86设备,实现资源模块化的横向弹性伸

缩,形成统一的计算与存储资源池。

2.1　调控应用集中管控技术

针对人机工作站被广泛应用在各区县供电公司、现货交易大厅、集控站、第三应急调度大厅等不同地理区域的问题,采用云桌面技术将所有工作站都集中虚拟化到终端管控系统上,可集中管理不同场所中的所有调度人机终端。

1)在安全加固、补丁升级等操作过程中,相较传统物理工作站,无需逐台进行安全加固和补丁升级,可通过管理策略统一下发功能,集中对所有虚拟工作站进行安全策略和补丁的分发,进而快速便捷地完成所有虚拟工作站的安全加固和补丁升级,可靠性高,减少了人工加固、升级时误操作可能性,极大缩减了人力投入。

2)通过终端管控系统的虚拟工作站克隆复制功能,可在短时间完成工作站的批量安装和部署。工作站系统出现故障时也可通过此功能进行快速恢复,有效地节约自动化人员的时间和维护工作量。

2.2　瘦终端安全防护技术

针对传统图形工作站维护成本高、故障修复周期长问题,将基于云计算的瘦安全终端作为调控终端。该设备使用免维护式设计,设备中内嵌了独立的嵌入式、精简化的国产安全操作系统基础内核,仅保留了网络通讯、屏幕操作等基本功能,即插即用,不存在其他的繁琐配置过程。瘦安全终端是提供给调度员和运维人员使用的前端基本操作设备,通过此设备连接访问地调侧的虚拟调度工作站桌面。

瘦安全终端采用人脸识别和指纹识别的生物多因子认证技术进行登录。终端加电启动时,使用图像识别人脸检测算法完成人脸检测功能,人脸识别库完成人脸特征提取的功能,完成人脸特征识别检测。瘦安全终端配套的指纹识别鼠标,将射频传感器内嵌在鼠标装置内,通过传感器发射微量的射频信号,可以穿透手指的表皮层获取里层的纹路以获取信息。相对于传统光学识别等传统指纹技术,射频传感器对手指的干净程度要求较低,具有更高的识别率和准确度。生物多因子特征识别检测认证成功后方可对瘦安全终端进行操作,可有效避免非授权人员通过终端进行违规操作。

2.3　图形压缩编码安全传输技术

基于目前地调与站端通讯时,调度数据网带宽较窄(≤2 MB)的特点,研究并验证通过新一代虚拟桌面传输协议,通过采用基于图形库的软件处理方式,使用 CPU 计算资源,提供 2D 图形数据的渲染处理能力。同时也提供了基于 GPU 的硬件处理方法。通过分类压缩技术提供 3 种无损图像压缩算法,分别是 Quic、LZ 和 Glz 压缩算法。优化视频数据传输方式,直接把视频数据以流媒体的方式发送到终端设备,避免解码操作,图像渲染性能优化通过图形区域的刷新频率来侦测视频区域,采用 MJPEG 压缩算法。

通过该协议可以实现瘦安全终端远程访问虚拟调度工作站桌面,并具有文字与图像显示更清晰细腻、视频播放更清晰流畅、声音音质更真实饱满、兼容性更好、带宽低等特点。

2.4　基于国密的可信接入和通信加密技术

通过基于国密算法的可信接入和通道加密技术,再结合在各网络边界国家电网专用纵向加密装置,实现调度人机终端在不同工作场所通过人机交互网或调度数据网与主站系统之间的信息通讯安全可控,且无需对生产控制大区的网络安全架构进行调整。

基于国密的可信接入和通信加密技术隔离了终端与调控主站系统之间的直接通讯。基于国密算法的加解密技术以识别、匹配、认证和授权接入的终端,彻底杜绝使用笔记本等设备的违规、非法接入调度专网。

2.5　多屏幕扩展跨屏操作时的实时安全审计

通过深入研究多屏操作实时安全审计功能,实现人机安全终端开机即可以自动开启运维审计模式,前端操作人员无感知,不需经浏览器等第三方工具跳转,图形化操作等使用习惯和之前一致。对所有图形和字符操作进行审计,支持双屏、四屏扩展显示操作时实时录屏审计,并可对操作指令及输出结果进行搜索、定位和查询,实现对危险指令的阻截。根据工作需要对 USB 外设进行管控,选择是否启用相应的 USB 外设。对于 U 盘等存储设备还可记录数据的上传和下载记录。

进一步加强对维护人员的安全监管,扩大行为审计范围,加强事前授权与事后行为记录的合规性审计能力和评估各类角色人员的专业度能力,全面提升规范化管理水平。

3　调控终端安全管控系统架构

根据电网调度自动化的业务场景,融合计算虚

拟化、网络虚拟化、存储虚拟化、运维监控管理、云桌面业务流程交付等软件技术，形成标准化的调控终端安全管控系统架构。实现调控终端从物理工作站转换为虚拟化工作站，并对其进行集中安全管控。一台虚拟工作站对应传统的一台物理调度工作站。

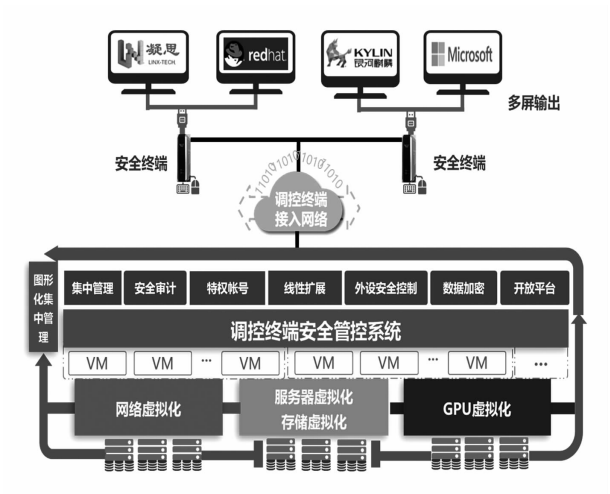

图 1 调控终端安全管控系统架构

调度主站系统相关数据、应用均运行在虚拟工作站上。统一部署在调控终端安全管控系统上由省、地市统一管控，调度台、变电运维班、现货交易大厅等办公场景，仅需通过精简的安全终端（瘦客户机）设备，复用现有电力专网通道，连接至地调侧的终端管控系统，终端管控系统对申请接入的调控安全终端进行识别和安全认证，接入成功后将虚拟工作站的操作界面传递给安全终端，调度员即可按传统物理工作站的使用习惯进行日常的监控和调度操作。安全终端与终端管控系统之间通讯带宽要求较低，具有与后端调度自动化主站系统之间数据交互简单的技术特性。

4 调控终端安全管控系统应用方式

4.1 整体应用架构

遵循国家电网有限公司要求的“安全分区、网络专用、横向隔离、纵向认证”[1-3]的电力调度数据网络安全规范，在生产控制内部署；终端管控系统通过安全区内核心交换机接入安全Ⅰ区和Ⅱ区，平台内虚拟工作站按使用需求可同时配置Ⅰ区和Ⅱ区IP地址，在防火墙上配置访问策略，并安装相应调度主站系统客户端程序后通过调度主站系统配置连接相应的主站系统。

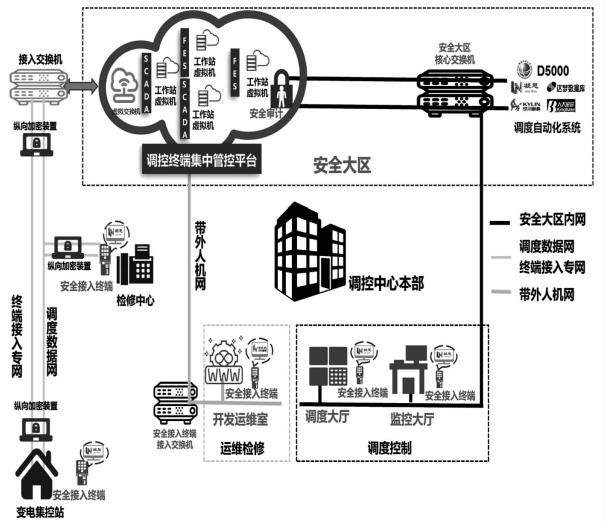

图 2 整体应用架构

4.1.1 网络接入

1）终端管控系统通过多网口冗余绑定方式扩展数据交互带宽。

2）终端管控系统通过虚拟交换机的方式接入生产控制大区内的核心交换机。

4.1.2 数据交互

1）虚拟工作站通过终端管控系统虚拟交换机与安全分区内的调度自动化系统主站系统进行数据交互。

2）虚拟工作站与调度自动化系统主站系统的业务、数据交互模式，维持与物理工作站方式一致。

3）无需对调度自动化系统主站系统进行改造，不影响调度自动化系统主站系统的正常运行。

4.2 全分布式的存储技术应用

研究新一代的基于X86架构的分布式存储技术应用技术，采用基于业界标准的X86服务器，彻底抛弃了很多系统仍在使用的存在性能和可靠性问题的集中化元数据处理节点架构，借鉴业界最先进的全分布式、无共享（share nothing）架构设计理念，采用基于策略的分布式哈希表数据路由算法，使得客户端无需查找元数据节点，通过计算就能直接寻址到数据所在的存储节点，大大缩短了数据IO访问路径，提升了系统性能。

同时，整个系统也无集中管理和控制节点，每一个数据节点都有能力承担另一数据节点的功能，节点之间通过内部高效的分布式协议完成相互协作和通信。这种去中心化、无状态的全分布式数据处理架构是系统能实现水平、线性扩展能力的关键，有力地保证了整个系统无单点故障，无性能瓶颈。

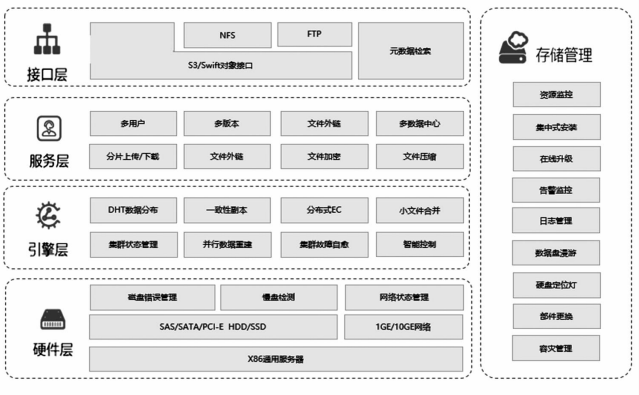

图 3　全分布式存储

4.3　GPU 虚拟化技术应用

计算机图形处理器(graphic processing unit,GPU),1999 年由 NVIDIA 公司提出。GPU 虚拟化即将 GPU 进行切片,并将这些 GPU 时间片分配给虚拟机使用的过程。

调控终端集中终端管控系统的桌面虚拟化解决方案中,基于 NVIDIA 公司提供的 GPU 虚拟化技术,即 vCUDA(virtual CUDA)技术,采用在用户层拦截和重定向 CUDA API 的方法,在虚拟机中建立物理 GPU 的逻辑映像——虚拟 GPU,实现 GPU 资源的细粒度划分、重组和再利用,支持多机并发、挂起恢复等虚拟机高级特性[4]。

其 vCUDA 的实现原理大概包括 3 个模块:CUDA 客户端、CUDA 服务端和 CUDA 管理端。

调控终端集中终端管控系统基础服务器,能够直接控制硬件,系统内安装着原生的 CUDA 库以及 GPU 驱动,使得 Host OS 可以直接访问 GPU 和使用 CUDA。其他的虚拟机属于非特权虚拟机(guest VM),其上运行的操作系统(guest OS)不能直接操纵 GPU。CUDA 客户端称之为客户端驱动,CUDA 服务端称之为宿主机的驱动,CUDA 管理端称之为 GPU 管理器[5-7]。

在调控人机交互终端领域由于调度终端工作站必须采用国产安全操作系统,针对国产操作系统(麒麟、凝思等)在云桌面使用场景中对图形显示和图形运算进行优化,以满足在电力调度控制应用场景下对图形显示和图形运算的高标准、高性能需求。

国产安全操作系统在生产销售之前需要通过公安部计算机信息系统安全产品质量监督检验中心的检测,基本功能需符合 GB/T 20272—2006《信息安全技术操作系统安全技术要求》第四级结构化保护级的安全功能的相关要求,因此其内核驱动接口已被重新封装和改造,研究根据国产操作系统的内核驱动接口开发安全规范,根据内核中 platform. c 提供的平台总线(platform_bus)以及注册平台设备(platform_device)和平台驱动(platform_driver)的相关接口,对平台设备(platform_device)和平台驱动(platform_driver)进行编码,重新开发 vGPU 设备驱动,并使其可在国产安全操作系统中得以应用。

5　实验数据

为了验证调控终端安全管控系统效果,在南充公司智能电网调度控制系统场景下进行实验。运用所提的基于云计算和生物多因子认证的调控终端安全管控技术,构建调控终端安全管控系统典型应用架构,如图 4 所示。

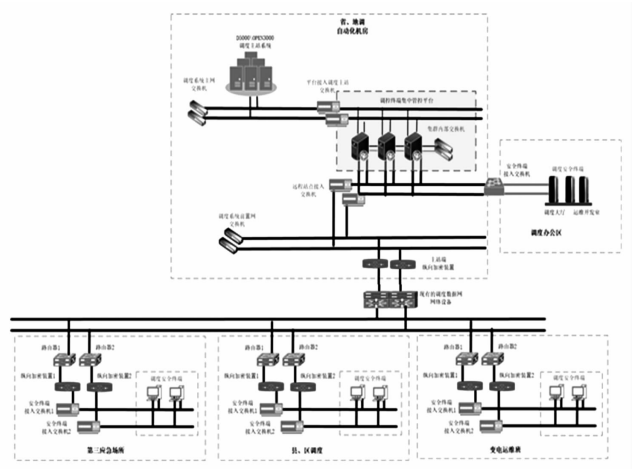

图 4　调控终端安全管控系统典型应用架构

系统关键指标参数如下:

1)实现基于凝思、麒麟等多个版本国产安全操作系统的 GPU 虚拟化功能,支持双屏和四屏显示。一块 Nvidia M10 32 G 显存 GPU,虚拟化后可分配给 64 台虚拟工作站同时使用。

2)一台双路 CPU、128 G 内存配置的通用 X86 服务器支持同时运行 32 台调度虚拟工作站。

3)在阆中(距南充地调 80 km)县供电公司,30 MB 网络带宽条件下访问调度主站系统并进行数据查询、曲线调阅等日常调度操作时,传统物理工作站模式与瘦安全终端模式的对比数据如表 1 所示。

表1 实验耗时对比 单位:s

测试项	物理工作站	瘦安全终端
查询历史数据	54.80	2.27
打开电网图形	31.53	3.13
打开曲线图	28.81	3.26
警告查询	34.60	2.13
今日越限查看	20.44	1.44

4)在阆中县供电公司,分别进行2 M、4 M、6 M、8 M、10 M带宽限制,通过县调安全终端访问和操作调度主站系统。显示画面分辨率设置为3840×1080的双屏显示。

(1)2 M带宽限制的情况下进行日常操作及维护,告警声音、告警弹窗、告警信息、报表生成、潮流图、接线图等功能正常可用,画面拖动有轻微拖影操作稍有卡顿。

(2)4 M和6 M带宽限制的情况下终端可正常操作使用应用,操作频繁时稍有卡顿,无延迟,告警声音、告警弹窗、告警信息、报表生成、潮流图、接线图等功能正常可用。画面拖动以及操作使用应用正常流畅,画面拖动无拖影。

(3)8 M和10 M以上系统画面流畅,清晰度高,无延迟,无卡顿,告警声音、告警弹窗、告警信息、报表生成、潮流图、接线图等功能正常可用。

5)瘦安全终端开机自启动实时操作安全审计,平均一小时审计视屏占用60 MB磁盘空间,审计视频调阅无延迟,可搜索定位。

6 方案对比

从规范权限配置,加强操作过程安全审计,完善管理制度和技术手段,防范安全攻击,应对极端风险防控,加密网络传输,完善对延伸至外部的远程接入安全终端设备进行集中、统一的安全管控和运维管理等多个维度,综合对比传统物理工作站与调控终端安全管控系统两种技术方案,对比数据如表2所示。

7 示范应用

南充公司于2019年12月开始本系统的试点建设部署和应用,通过多轮的技术交流、现场收资、方案制定,最终完成调控终端集中终端管控系统在智能电网调度控制系统“地县一体化”模式下和基于国产安全操作系统GPU虚拟化、生物多因子特征安全认证等关键技术的适应性定制。经过测试验证,于2020年1月正式投入上线试运行,目前使用场景包括部分地调调度席位、地调自动化值班席位、四川电网备调中心运维席位以及阆中县等6个分公司。该系统示范应用拓朴如图5所示。

在调度坐席、值班席位和运维席位等不同应用场景的实际使用过程中,调度员、运维开发人员通过在

表2 方案对比

功能项	物理工作站	调控终端安全管控系统
多屏显示	仅限双屏	支持双屏、四屏及以上
USB等外设安全管控	不支持	支持,可对终端上任意外设接口进行安全管控和行为审计
操作行为审计	不支持	支持,可对终端屏幕图形化、字符界面命令行操作录像、并记录鼠标及键盘的每一个动作,可按关键字、时间段等多条件进行检索和展示
带宽、Ukey支持	调度终端延伸带宽 ≥30 MB KVM 调控中心本部, <1 km D5000数字证书Ukey识别率低<70%	任意距离支持窄带宽≥2 M,数据实时刷新、图形和模型加载快、多屏操作流畅 D5000数字证书Ukey识别率>98%
调度主站系统数据加载	县供对历史库数据查询时耗时超过2 min 数据更新下发时远程工作站通道阻塞,无法操作	县供电公司对历史库数据查询时耗时约30 s 虚拟工作站与主站系统同处控制大区,数据更新不影响前端正常操作
数据传输安全	不支持	管控平台与终端之间证书认证和通道国密算法加密,可结合网络边界纵向加密装置多重网络安全保护
工作站集中运维	成本高,专业要求高	地调平台集中创建、维护和管理工作站,无需进站维护
投入资源	图形工作站、KVM矩阵、运维审计系统、代理服务器、代理软件	调控终端集中管控平台、基础服务器和精简安全终端
主站系统结构影响	较大,需新增代理服务器和代理软件并改造人机软件	无需对D5000进行改造
机房空间	114台工作站,占用15个机柜	大量节省机房空间,2个机柜

桌面放置的小型化、精简的安全终端设备经网络接入终端管控系统,获取相应的虚拟机资源和交互画面并对其进行操作,使用体验与使用物理工作站无差别。

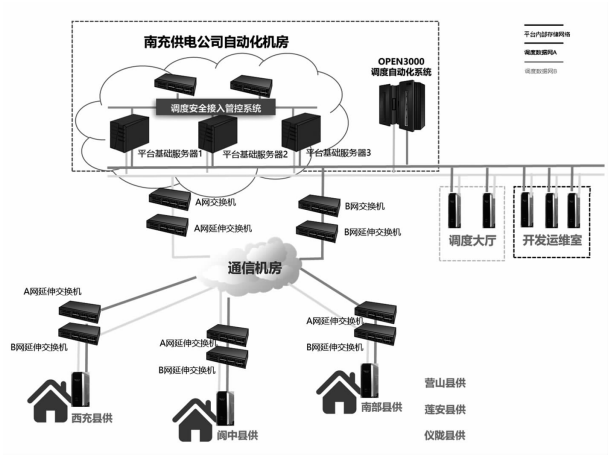

图 5　示范应用拓扑

特别是在西充(距地调 40 km)和阆中(距地调 80 km)两个县供电公司远程部署的场景下,终端管控系统优化了自身传输协议,对于网络带宽的需求降至 10 M 以下,满足窄带宽工作要求,相较传统物理工作站 30 M 以上的带宽需求,明显降低了对于网络带宽的消耗。同时对于所穿透的纵向加密设备,也减轻了其加密负载。数据实时刷新、场站图形和模型加载、历史库数据查询速度较传统工作站提升 60% 以上。

8　结　语

所提出的调控终端安全管控系统极大提高了日常对工作站的管理和维护效率,结合终端管控系统的安全审计、认证管理、授权管理等运维安全管理功能,可对调控终端进行统一管理和集中调配,实现了对调度员和维护人员使用调控终端的安全审计、风险防范,加强了调度工作站使用的机密性和规范性,满足等保要求。

项目试运行以后运行良好、稳定、可靠,达到了项目预期效果,可以推广应用。

参考文献

[1] 殷自力, 钱静, 陈宇星,等. 基于 D5000 平台的调配一体技术方案[J]. 电力系统自动化, 2016, 40(18): 162 – 167.

[2] 李敏子. 电力调度自动化中的一体化技术[J]. 电子技术与软件工程, 2018(10):123 – 123.

[3] 邱丽娜. 电力调度自动化系统中一体化技术的应用[J]. 现代信息科技, 2017,1(6):28 – 29.

[4] 余时强,张为华. GPU 虚拟化相关技术研究综述[J]. 计算机系统应用,2017,26(12):25 – 31.

[5] 仝伯兵,杨昕吉,谢振平,等. GPU 虚拟化技术及应用研究[J]. 软件导刊,2015,14(6):153 – 156.

[6] 陈钢,吴百锋. 面向 OpenCL 模型的 GPU 性能优化[J]. 计算机辅助设计与图形学学报,2011(4):571 – 581.

[7] 卢风顺,宋君强,银福康,等. CPU/GPU 协同并行计算研究综述[J]. 计算机科学,2011,38(3):5 – 9.

作者简介:

王先强(1979),男,高级工程师,从事电网及二次系统管理工作;

张　睿(1982),男,硕士,高级工程师,从事电网及二次系统管理工作;

张　华(1985),男,硕士,高级工程师,从事调度自动化管理工作。

(收稿日期:2020 – 01 – 17)

(上接第 19 页)

[12] 卜云,高传海,李文芳,等. 大数据架构下电力系统风险评估[J]. 电网与清洁能源,2021,37(1):77 – 83.

[13] 田园,原野. 基于改进 K – means 算法的电力大数据系统研究[J]. 电子设计工程,2021,29(2):76 – 80.

作者简介:

靳文星(1996),男,在读硕士,研究方向为电力信息化及自动化;

王电钢(1973),男,教授级高级工程师,研究方向为电力信息化;

张哲敏(1997),男,在读硕士,研究方向为电力信息化及自动化。

(收稿日期:2021 – 03 – 01)