

考虑跨区数据交互安全性的电子操作票系统设计

纪青春, 陈亮, 杨鹏云, 史雷, 许文

(国网甘肃省电力公司 甘肃 兰州 730000)

摘要: 针对跨区域电力调度操作, 设计了考虑跨区数据交互的电子操作票系统。首先分析了区域互联电网对电力调度操作的要求; 其次分析了电力跨区域交互的核心技术, 包括数据交互的安全机制、异构数据共享互融处理技术及基于物联网的智能操作终端和边缘数字化电子操作票技术; 然后设计了分区分层控制和纵深防御的安全策略, 并将其应用于跨区域数据交互的电子操作票系统, 同时提出了系统构架以及关键技术, 并对其具体功能进行了分析; 最后对电子操作票系统应用情况进行了分析。

关键词: 跨区数据交互; 安全防护; 电子操作票; 系统设计

Design of electronic operation ticket system considering the security of cross-region data interaction

Ji Qingchun, CHEN Liang, YANG Pengyun, SHI Lei, XU Wen

(State Grid Gansu Electric Power Company, Lanzhou 730000, China)

Abstract: For cross-regional power dispatch operations, an electronic operation ticket system considering cross-regional data interaction is designed. First, the requirements of regional interconnected power grids for power dispatch operations are analyzed. The core technology of power cross-regional interaction is analyzed, including the security mechanism of data interaction, heterogeneous data sharing and fusion processing technology, intelligent operation terminal based on the Internet of things and edge digital electronic operation ticket technology. The security strategy of zoned and hierarchical control and defense in depth is designed and applied to the electronic operation ticket system of cross-regional data interaction. The system architecture and key technologies are proposed, and its specific functions are analyzed. Finally, the application situation of the electronic operation ticket system is analyzed.

Key words: cross-regional data interaction; security defense; electronic operation ticket; system design

0 引言

现阶段, 电网调度任务在移动互联等电子化技术不断应用到电力网络的背景下呈现出数字化的发展趋势。推动实施电力操作票网络化发令业务, 包括网络化布置预令和网络化下发正令, 都有助于提高电力调度质量和效率, 提升电网运行

管理水平。但是电网的互联导致电力调度指令出现跨区交互的情况, 需要确保调度指令下发过程中的安全性。

目前针对跨区域数据交互的电力操作票系统研究不足, 文献[1]提出了配电网分布式电源“源—网”调度数据交互技术。文献[2]针对面向调控业务的多级一体化数据交换系统进行了研

究。文献[3]针对配电网智能操作票生成方法进行了研究。文献[4]设计了一种电力调度操作票系统。文献[5]提出了一种配电主站数据流跨区交互通道实现方法。文献[6]研究了电力公司电网调度智能操作票系统。可以看出,目前针对智能交互平台的研究和应用还没有与电力操作票生成管理协调。

本文针对跨区域数据交互的电子操作票系统进行了剖析。首先分析了跨区域数据交换的核心技术,同时分析了以交互机制、数据共享以及智能终端操作为特点的技术,说明了跨区域数据交互的安全策略设计。其次以分区分层策略、纵深防御策略和攻击面最小化策略对电子操作票数据交互进行了系统设计,并且对电子操作票安全管理措施进行了分析,提出了基于角色的访问控制模式。最后针对电子操作票的实际应用进行了案例分析。

1 跨区数据交换的核心技术

1.1 数据交互的安全机制

项目在通信协议代理、基于XML的数据统一平台、穿越隔离装置技术和数据管理技术等方面都采用了自主研发的新技术,从系统数据使用进行权限的管理,并对数据的访问进行了限制;在数据传输的交互过程中,利用数据封装的方式对跨安全区和系统数据进行了加密及封装,保证了传输过程的数据安全性;制定了统一的基于XML的存储和展现方式,由于XML文件是基于全文本的解释型数据文件,满足了对于隔离装置的数据传输规定。在硬件网络隔离装置的基础上对数据进行安全处理,大大满足了电力生产的要求。

1.2 异构数据共享互融处理技术

系统采用了异构数据共享互融处理技术,对工作票、操作票的数据进行集中管理,建立以两票管理后台为核心的多层次系统架构,实现各种异构数据的兼容、转换、存储、读取和分析功能,将计划任务、操作票和工作票联系起来,实现信息统一管理,统一维护。

1.3 基于物联网的智能操作终端

系统利用先进的物联网技术进行两票电子化管理,实现与风控计划的关联,在现场作业时,需要按照智能操作终端的电子工作票、操作票顺序依次执行,提高现场作业的安全性和可靠性。

1.4 边缘数字化电子操作票技术

智能操作终端将操作票的各类关键信息数字化、结构化,通过边缘计算与后台系统进行关联互动,现场操作全程录音,否则无法继续开展工作。给不同人员分配不同的权限,不在系统的人员无法进行操作,执行完成后可汇报风控平台,大大提高操作票执行的安全性和作业全流程的管控能力。

2 跨区数据交换的安全策略设计

电力系统中各应用系统为克服各自系统信息孤岛问题,方便信息高效便利地互联互通,采用信息总线技术。按电力系统安全规范要求,信息总线必须分别部署在生产区、管理区两个安全分区中,之间用物理装置隔离,形成了两条跨区的信息交互总线,各应用系统之间既存在同安全分区的数据交互需求,也存在跨区的数据交互需求。因此,在跨区数据交互过程中,应重点考虑安全策略问题。

2.1 分区分层策略

系统分区是为了保证相互操作不会产生干扰,需要采取有效设计对系统以及系统数据进行解耦,同时进行必要的隔离。

系统分层是为了建立系统的整体纵深层次,在各个不同层次上添加不同的安全措施,使得同一个威胁有多个安全防护措施,同时进行针对性防御。

2.2 纵深防御策略

单一安全防护措施经常因为设计不当、维护不当及硬件失效等原因无法永久有效地应对某类网络威胁,这种情况需要针对某类危险具有多层次的防御措施,比如防SQL注入攻击和程序自动报警等。调度纵深防御机制示意图如图1所示。

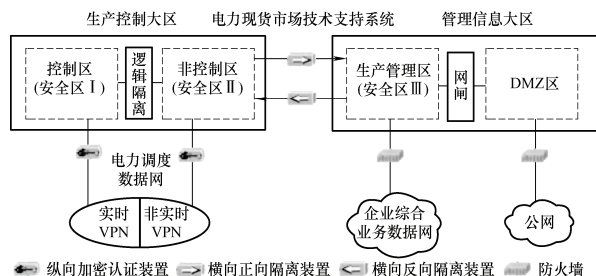


图1 纵深防御机制

Fig. 1 Defense in depth mechanism

2.3 攻击面最小化策略

系统包含了不同安全级别的数据，从安全角度出发，需要对接入方式和访问方式进行限制。为了保证总体的安全性，并减少总体安全成本，总体设计要求用户管理和授权管理等操作需要VPN接入到内网进行操作，而那些不敏感的查阅操作或影响较小的操作可以提供其他访问方式。

3 考虑跨区数据交互的电子操作票系统

3.1 电子操作票特点

现阶段调度运行工作受到电网规模不断扩大、可再生能源渗透率不断增加的影响，存在工作强度高、多线程处理及过程易中断的问题，传统电话调度指挥，在调度发令和下令过程中都存在一定被干扰的几率。利用电子操作票以及网络下令等方式，能够提升厂网交互效率和准确率。网络化发令过程按照调度下令、厂站复诵、调度确认、厂站回令、调度收令和厂站确认的方法和流程进行开展，保证调度与场站指令信息可靠交互。受令人员在复诵和回令前需要通过人脸识别以及电子登录等方式对身份进行验证识别，能够准确识别受令人身份，拒绝冒名顶替操作等。利用区块链加密技术、非对称密钥算法实现网络法令过程中的数据加密和解密，保证指令信息的完整度，防止外部黑客对数据进行盗取和篡改。

电子操作票利用网络化手段下发指令，是一种厂网双赢的交互模式。在指令信息交互过程中，能够实现数据的安全可靠，操作指令通过文字传输，内容清晰明确，每项指令由监护人审批后执行，解决了电话发令中存在的错误记录、谐音误

扰等问题。发令过程能够通过网络化实现高效便捷的传输。通过鼠标单击代替电话拨号交互，能够自动记录受令人、发令时间等关键信息，从而在时间上缩短发令过程，还能够实现多任务并行处理。调度员被动“串行”工作能够转变为由网络化执行任务的主动“并行”工作，减少现场汇报排队以及操作等待时间，能够大幅提升操作票的执行效率。

3.2 电子操作票系统构架

将移动互联应用至电力调度电子化发令过程中，能够依托调控云、数据中心资源建立设备台账数据库和电网实时运行数据库，实现对设备和设备运行状态的动态管理。依托OMS能够建立相应的生产信息数据库，将操作票系统、调度日志系统和检修申请单系统等融合，实现数据的多维度应用。在调度指令下发阶段，还需要依托管理系统，建立受令单位、受令人等用户数据库。同时建立业务前台、管理后台与数据中台的数据调用接口，能够满足上下层调度业务，灵活调用数据中台中的数据、服务和组件。电子操作票系统架构如图2所示。

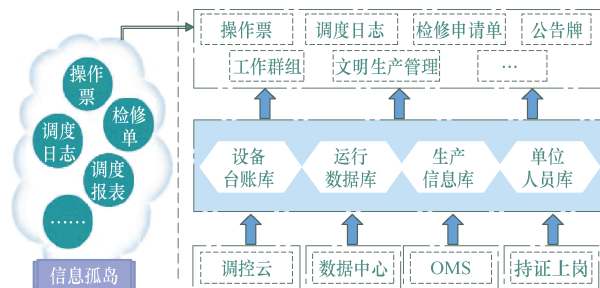


图2 电子操作票系统架构

Fig. 2 Architecture of electronic operation ticket system

3.3 系统功能

电力调度操作票网络化下发系统能够将传统的分散性业务集中到统一平台，实现电力调度操作票各模块之间的数据交互和业务协同共享，并根据调度的实际需求丰富调度业务场景，形成网络化管理。

电力调度操作票下发系统是集成生产管理、调度指挥和数据分析的多业务平台，主要包括操作票、网络化发令、调度日志、应急检修申请、故障异常汇报、调度任务下发和电子公告牌等生产指挥类业务，还包括电网运行精益化评估、生产报表分析等数据类业务。

平台能够根据移动互联数据的信息,判断并分析所需电力操作票种类、下发流程和所需时间等,将分析得到的结果传输至调度中心,并且进行多级调度系统同时传递信息,满足不同的调度级别需求。

由于电力调度需要实时掌控现场设备的信息,利用移动互联技术能够打通设备与操作票系统之间的界限,实现调度员对设备信息和调度信息的同时掌控,以高效协同的调度、日常工作生态为目标,促进调度日常工作提质减负。

该系统能够实现调度业务的深度贯通,通过线上协同、数据交互等手段,促进上下级调度间、各类调度业务流程线上贯通,实现并行处理,减少传统电力调度操作票下发等待时间。

4 电子操作票安全控制措施

4.1 RBAC 权限管理模型

系统将会采取 RBAC 权限管理模型进行灵活授权。RBAC 权限管理模型具有适用范围广、高扩展及可以大幅降低权限管理工作量的特点。

RBAC 权限管理能够识别访问地址和生物特征信息,保障用户认证安全可靠。设置 IP 地址访问白名单,IP 地址与受令单位绑定,实现“IP 地址-受令单位-用户”的一一对应,确保用户在指定变电站只具备该站的网络化业务权限。在系统登录、预令签收、正令复诵和正令回令等环节设置人脸识别认证,解决受令人身份识别问题。

4.2 基于角色的访问控制

系统将会基于用户的角色进行访问控制,访问控制将从 Web 服务器层、应用服务器层和数据层依次开展工作。

针对电力调度操作票过程中的数据加密,采用流量清洗、流量控制等手段防范域名注入攻击,并采用 UKey 认证、https 安全协议和 Web 应用防火墙等保障措施来提高安全防护性能。在内部安全防护方面,通过对调度指令的敏感数据进行加密、基于角色的访问控制和安全监控等措施,提高数据安全性。以调度数据安全为例,包括检修数据、倒闸操作等,在传输及存储过程中面临泄露风险的数据,可通过数字证书、数字加密、权

限制和数据脱敏等一系列措施,保障数据的安全性。在场站对电子操作票的指令进行确认时,先通过私钥进行身份确认,再通过公钥将电子信息进行加密和签名,以加密的方法是发送至安全 II 区,并通过多重解密后得到明文,用于进一步电子操作票的流转。数据加密流程如图 3 所示。

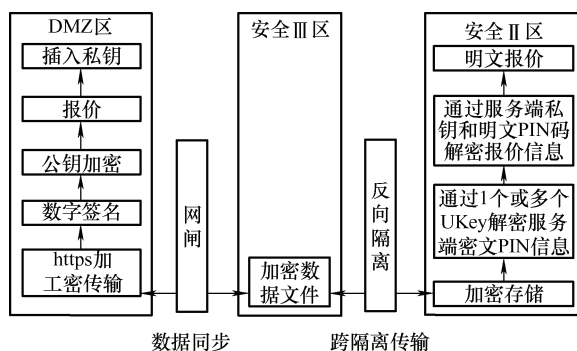


图 3 数据加密流程

Fig. 3 Data encryption process

4.3 应用抗抵赖技术

通过建立有效的责任机制,使管理人员或运维人员对自己的操作行为负责,包括对应用日志记录和数字签名等技术手段进行抗抵赖设计。

(1) 日志记录

通过对用户行为记录日志,并采取措施保障日志信息的完整性。

(2) 数字签名

对用户的所有操作行为进行数字签名,记录操作行为及操作时间。

4.4 系统完整性防护

为了保证信息系统的完整性,主要是防止系统被篡改,注入病毒木马或者恶意调整系统结构。

还可以应用区块链和数据加密技术,保障数据传输的安全完整性。提升纵向数据网络化交互的安全级别,应用区块链、非对称密钥算法等先进数据加密算法,防止数据篡改,兼顾数据传输过程的完整性和保密性。

4.5 安全基础设施设计

统一用户管理和身份认证、RBAC 授权管理与访问控制、统一加解密,跨区数据交互的主要安全基础设施如下:① 身份管理与身份认证基础设施;② 授权管理和访问控制基础设施;③ 加密解密基

基础设施；④ 系统安全管理、监控与审计基础设施。

5 电子操作票应用效果分析

为验证网络化交互方式的安全可靠性，某地区调控中心选定“批复计划检修申请单”作为网络化交互试点。主要基于以下考虑：一是业务相对简单，仅需要核对检修申请单中工作单位、停电设备及状态、工作内容、工作要求及工作时间等信息准确无误即可；二是受令对象相对单一，受令对象仅包括调度中心和直属电厂；三是业务容错率相对较高，若网络化批复过程出现问题，后续存在主值拟票、值长审核及申请单开工等多环节发现问题的缓冲机制；四是基础条件成熟，调度中心及直属电厂均配置与各级分调度中心互联互通的三区网络；五是技术实施简单，仅涉及申请单系统的简单改造，即可建立上下级网络协同及相互确认机制。

另外，网络化发令还能够实现调度员多任务并行的处理方式，实现多个调度任务的并行处理，避免正常工作被中断，提升效率的同时使工作流程更加合理化。与网络化发令相比，调度电话由原先的 49 322 个，减少至 33 757 个，调度电话数量减少高达 30%，随着电子化操作票发令逐步推广，预计调度电话将比去年降低 45%以上。

与传统电话下发操作指令对比，优势如下表所示。

表 操作票下发形式对比

Tab. Comparison of issuing forms of operation ticket

下令环节	传统操作票	电子操作票
拟票	手动拟写	常规操作自动拟写，减少手 写错误
审票	人工审票	人工审票，并进行自动拓扑 校核，减少人工遗漏
身份认证	调度电话 听音识人	人脸识别，安全可靠 性高
预发	传真预发	网络下发，提高效率
复诵	口头复诵	关键词选择或填写复诵，加 深受令人印象
正令	口头通知，可能信 息遗漏	网络化流转，信息唯一，而 且效率高
回令	人工核对状态	自动比对 SCADA 状态核 实，安全性高

对比了电力操作票网络化下令和调度电话下令两种方式，调度电话下令中各项环节的安全保

障手段在网络化下令过程中均有采用或有提升，网络化下令安全性可以得到保障。

6 结束语

通过本文对跨区域数据交互电子操作票的设计，提升了跨区与数据交互过程中的信息安全性，能够利用现阶段较为成熟的数字边缘化技术、物联网技术和数据共享技术等对数据加密信息进行处理。通过分区分层策略、纵深防御策略和攻击面最小化策略，能够实现电子操作票的安全控制，形成系统性的防护。本文设计的电子操作票安全控制措施能够应用于电网各级调度电子化操作过程，具有较强的实用性。EA

参考文献

[1] 田赟，冯李军. 配电网分布式电源“源—网”调度数据交互技术研究[J]. 山西电力，2019(6)：23-26.

[2] 陈郑平，梅峥，林静怀，等. 面向调控业务的多级一体化数据交换系统设计与实现[J]. 电力系统自动化，2020，44(4)：195-204.

[3] 郝方舟，罗林欢，孙奇珍. 配网智能操作票生成方法研究与应用[J]. 无线互联科技，2019，16(17)：123-124.

[4] 姜宁浩. 电力调度操作票系统的设计与实现[D]. 成都：电子科技大学，2019.

[5] 曹寅翔，李俊达. 配电主站数据流跨区交互通道的设计与实现[J]. 华电技术，2019，41(4)：10-13.

[6] 曹冬梅. 电力公司电网调度智能操作票系统的研究与应用[J]. 电气时代，2019(2)：69-71.

作者简介：



纪青春

纪青春，(1973—) 男，高级工程师，研究方向：安全生产管理、设备运维管理。

(收稿日期：2020-12-20)