2019 电力行业信息化年会论文集

会议主题：生态互联 数字电力

● 中国电机工程学会电力信息化专业委员会　主编

人 民 邮 电 出 版 社
北　京

内 容 提 要

本论文集收录了中国电机工程学会电力信息化专业委员会 2019 电力行业信息化年会论文 108 篇，内容涵盖全业务电力物联网、智能制造、电力大数据、工业互联网、信息系统安全运维等诸多领域，全面反映电力行业信息化领域的热点、最新技术、研究进展和应用前景等，充分体现了我国电力产业链各方在这些领域的积极创新和深入实践。

本论文集可供高等院校相关专业的师生、电力信息化行业中的工程技术人员、全国信息通信网络技术管理领域的工程技术人员参考。

人民邮电出版社

◆ 主　　编　中国电机工程学会电力信息化专业委员会
责任编辑　李彩珊

◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路 11 号
邮编　100164　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京时捷印刷有限公司印刷

◆ 开本：800×1230　1/16
印张：27　　2019 年 9 月第 1 版
字数：850 千字　　2019 年 9 月北京第 1 次印刷

定价：180.00 元

读者服务热线：（010）81055488　印装质量热线：（010）81055316
反盗版热线：（010）81055315
广告经营许可证：京东工商广字第 8032 号

2019 电力行业信息化年会论文集

专家委员会

主 任 委 员： 李建成

副主任委员： 王继业　刘建明　胡红升　王志英　吕庭彦
杨富春　王聪生　吴张建　沈　亮

委　　员：（按姓氏笔画排序）

丁　涛　王　建　王少杰　王东方　王健斌
方　翎　曲朝阳　吕　韬　朱晓东　朱朝阳
齐　峰　江　华　许凌峰　孙从海　孙丕石
孙靖初　杜永胜　李建华　李美平　李继红
杨建军　吴文炤　邹来龙　张　利　张大国
林　峰　林为民　罗念华　金和平　庞松涛
郑贵德　房　方　赵　威　赵永柱　赵现军
赵建保　胡　曙　贺玉彬　钱天林　高昆仑
郭　浩　曹军威　崔恒志　曾　楠　董　杰

编辑委员会

欧阳述嘉　胡　威　王思宁　靳　莉　古　巍
蒋　月　李　颖　杨　菲　蒋　妍　张竞文
刘　攀　柳　絮　马　娜　杨　莹　王大垒
张志宏　宋亚琼

人民邮电出版社

人民邮电出版社

目 录

“国网+智慧农业”生态圈建设在四川省落地实践…… 余梦佳，尧　广，刘　利，罗　新，施崇智，高　畅（1）
IT 共享服务中心建设方案 …… 程华福，郑越峰，吕新丽（4）
LTE-230 MHz 电力无线专网在泛在电力物联网建设中的应用与实践 …… 韩冰洋，宋继高，王炫中（11）
SPI 通信方式在智能电表安全芯片中的应用 …… 张彦荣（18）
TD-LTE230 电力无线专网研究与应用 …… 齐悦言，孔祥余（22）
大数据在电力行业的应用 …… 任惠姣（30）
大型企业端到端流程系统的设计与实现 …… 丁彩云，胡　劼，孙婷婷（33）
大型企业信息通信智慧客服一体化解决方案 …… 刘娇丽，李雅西，沈雪晴，邹晓颖，李　枫（37）
电力大数据下的电动汽车充放电隐私数据保护 …… 王　帅，周　晶，孙喜民，张　宾（42）
电力行业数字证书互信互认体系的研究 …… 廖会敏，玄佳兴，李丽丽（47）
电力行业智慧物联体系研究与设计 …… 葛冰玉，冯志鹏，韩　璐，黄文雯，安培秀，李丹丹（52）
电力企业网络安全方案设计与优化 …… 李　斌，伍泽军，邓文杰（55）
电力通信运行支撑系统不中断迁移上云方案 …… 杨志敏，洪丹轲，谢俊毅（59）
电力系统 IMS 话务预测模型研究 …… 王晓东，范秉旭，叶　欣，苑晓东（67）
电力信息通信网络安全防护研究综述 …… 杨　珂，陈绍真（73）
电网生产业务工单分类的文本挖掘方法应用 …… 陈小峰，齐晓明，赵雅迪，张利鹏（76）
电网信息安全防护的现状及思考 …… 郑子洵，朱　峰，齐晓明（82）
泛在电力物联网标识管理服务平台建设研究 …… 杨　珂，王焕娟，秦日臻，赵丽花（85）
泛在电力物联网技术的应用研究——以“光–车”互联系统为例 …… 陈绍真，王俊生，伍　燕，吕梓童（89）
泛在电力物联网通信方式 …… 李　明，汪俊洋（93）
泛在电力物联网战略部署实践 …… 赵　威，孙绍辉（97）
泛在物联网终端设备安全威胁与防护技术 …… 郭永和，闫龙川，何永远，赵子岩，朱　京（100）

人民邮电出版社

分布式数据库跨数据中心同步数据研究与设计……张　亮，周　晶，孙喜民，张　宾（103）
公有云承载的多种网络场景下的专属云网络接入模型……董　铮，陈　思，吴　琦，孙智强，桑晓宇（106）
核电厂电力监控系统网络安全态势感知平台研究……张士帅，付振旭，舒　超（110）
核电容器设备力学分析标准化研究与应用……赵　栋，景晓冬，赵继成（113）
核电站电气协同设计的研究与应用……张　宇，杨　东，许心炜，刘　森（118）
基于 EMD-LSTM 的短期负荷预测模型……刘月灿，孙建刚，周　逸，张晓亮，丁雪伟，李伟良（121）
基于 EMS 系统区域备自投在湛江电网中的应用……付振宇（124）
基于 FCME 检测的脉冲干扰抑制方法……余梦佳，尧　广，罗　新，刘　利，施崇智，高　畅（129）
基于 *k*-means 算法的 ECC 巨网分割研究……苏　鹏，陈　曦，孟　宇，黎　洋（135）
基于边缘计算的配网状态监测……刘　冲，魏　鑫，李　迪，赵　钊（140）
基于边缘计算的智慧用电生态场景……张林锋，欧阳述嘉，贾　涛（144）
基于大数据分析的核电工程预见性设备管理系统研发与应用……
……腾　飞，黄光明，侯新宝，黎艺华，李　霞（147）
基于泛在电力物联技术的大型供电企业无人值守智能选购仓店应用研究……
……王　超，张晓枫，陈　曦，王　颖（153）
基于泛在物联网的智慧城市应用……寇立冬，周　晶，孙喜民，张　宾（158）
基于机器学习的水电站水库水位预测应用……林文孝，郑贵德（162）
基于加权 Apriori 算法的电力光传输网故障诊断……吴宜聪，彭　蔚，黄一双，黄舒畅（169）
基于开源平台的 Docker 安全性分析……徐孝晋，伍泽军，邓文杰，陈霄楚（173）
基于“零信任”的工业信息安全防护研究……向人鹏（177）
基于流程匹配技术的库房管理调度系统……帅　率，尹　飞，宋　煜，陈　佐（181）
基于区块链的电力数据共享机制……李　旭，王合建（186）
基于区块链和泛在电力物联网的安全体系……王　丹，赵训威，王文华（190）
基于区块链技术的电力系统信息交换平台……袁　野，李向阳（194）
基于区块链与第三方的混合智能合同应用……边新宁，周　晶，孙喜民，张　宾（197）
基于人工智能的输电线路鸟害检测方法……孙建刚，刘月灿，张晓亮，董耀众，贾　真，李伟良（201）
基于深度学习的高效实时性 *M*:*N* 模式人脸识别方法……郑开发，李宏伟（206）
基于数据中台的电力企业统一数据模型优化完善方法……王家凯，冯定东（211）
基于物联网标识的物资安全电子追溯……崔九鑫，吕梓童（214）
基于物联网标识技术的智慧供应链管理……王焕娟，秦日臻（219）
基于物联网的智慧小区综合能源管理系统……王卫卫（223）

人民邮电出版社

基于物联网的智能电网信息化建设研究 ……石孟磊，周　军，杨志强（228）
基于物联网与人工智能技术的工程现场安全风险智能预警算法……
……黄文雯，冯志鹏，韩　璐，葛冰玉，安培秀，李丹丹（231）
基于现代（智慧）供应链的重大电网工程智慧供应平台研究……马　敏，王　平，李梦渔（236）
基于知识图谱的电力通信网智慧大脑技术研究……周　晶，孙喜民，张　宾（242）
基于智能合约的 IBC 密钥更新方案……甄　平，史　睿，陈绍真，杨　珂（248）
可穿戴 AR 单兵系统在电力检修工作现场的应用……刘启才，陈　兵，吕小锋（253）
密码技术在能源互联网中的应用及展望 ……王　栋，薛　真，廖会敏（257）
面向 6G 的高阶 APSK 软解调及简化 ……张长青（265）
面向电网巡检的点云高精度配准算法研究 ……吴新桥，王　昊，杨家慧（273）
某企业园区网改造工程规划设计与实施 ……谢金友，王燕杰（277）
企业“中台”战略研究——以国家电网公司为例……杜　栋，杨莉媛，谢　炯（284）
企业混合云环境数据级容灾的研究与应用 ……邵腾刚，卓弋凌，李丙超（288）
企业能力开放平台的研究与应用 ……马　兴，闪　烁（292）
前景理论下分布式发电市场化交易卖方市场行为的预测……那峙雄，王晓岚，马大燕，沈文涛，孟凡腾（296）
轻量级自动化巡检系统开发和实践 ……曹小明（301）
区块链技术在电子数据存证取证中的应用 ……朱兴雄（307）
区块链加密算法研究 ……朱兴雄（311）
全业务数据中心运维探讨 ……崔乃栋，潘　磊，冯志鹏（315）
适用于输变电工程造价管理的智能化应用平台……叶宝玉，王雁宇，师潇然，梁雯艳，衣丰超（318）
输变电工程造价分析与成果应用 ……叶宝玉，王雁宇，师潇然，梁雯艳，衣丰超（323）
数字化审计体系在电力行业的实践 ……赵恩来，陈　曦，崔　颢（327）
通信机楼动力母线供电方案 ……邵正忠（331）
通信系统集中监控平台建设方案 ……叶敏倩，詹　望（338）
新能源城配物流充电站运营服务平台建设与服务……李　迪，高立忠，刘　冲，马　娜（342）
新一代国家级电力交易平台微服务架构设计 ……詹卫许，张志翔，杜　龙，胡学强（345）
信息化技术在绿色供应商评价管理中的应用 ……潘晓婷，王俊生（349）
一种基于遗传算法的数据脱敏方法 ……李　澜，杨　华，马维青（353）
应用软件自动化变更的方法与实践 ……卓林贵，李胜德，朱晓玲（357）
园区级泛在电力物联网——局域能源互联网研究及应用……寇建涛，贾少堃，白　洁，魏建丰（362）
园区级供电服务中心用能策略 ……魏　鑫，刘　冲，黄嘉浩，张治刚（369）

人民邮电出版社

针对终端通信接入网及管理系统的集成优化建设……李文清，赵　甦，张　立，陈　鹤，肖云杰（373）
智慧安防监控系统与综合管理平台在抽水蓄能电站的设计与实现……郑凤柱，马明明，刘　宗，王艳如（378）
智慧变电站设备状态识别技术……程华福，闫蓓蕾，马洪波，刘　奔，王　鹏（382）
智慧物联电动自行车充电系统……孙胜宇，蒋　月，李　琳，庄　斌（386）
智慧园区综合能源智能调控算法实现与综合能源用能策略管理……赵鲲鹏，保　拉，胡　剑（390）
智能电网与泛在电力物联网的边界互联信息安全防护……曹　洋，范　义（395）
智能化语音监控系统在群堆电厂的应用……邝　豪，高小岩（400）
基于改进蚁群算法的云计算用户任务调度算法……罗斯宁，王化龙，李弘宇，彭　蔚（404）
5G 技术在配电网电流差动保护业务中的应用……吕玉祥，杨　阳，董亚文，汪玉成（405）
电力潜在敏感客户预测的大数据方法应用……陈小峰，赵雅迪，张利鹏，朱　峰（406）
基于回归分析的迎峰度夏用电量分析方法……
……陈雨泽，李　磊，方学民，刘　建，赵加奎，刘玉玺，左松林（407）
基于调度自动化系统的低压分布式光伏电站接入估算模型……
……马大燕，谢祥颖，那峙雄，沈文涛，孟凡腾（408）
基于多模型融合的电网故障抢修时长预测……潘坚跃，吴懿臻，徐汉麟（409）
基于知识图谱的泛在电力物联网安全可视化技术……余　洋，朱少敏，卞超轶（410）
电力企业基于 RPA 技术助力财务智能化应用实践……全文举（411）
泛在电力物联网无线网络规划……马　跃，李炳森，胡全贵（412）
基于国网商旅大数据融合背景的用户画像构建框架……张长浩，余志勇，周　振，石瑞杰，王新勇（413）
风电场电力监控系统网络安全威胁防控体系……丁　伟（414）
无实时网络下约定式运算的控制研究和应用……张正峰（415）
基于量子通信的电力业务调度算法……于卓智，张叶峰，韩冰洋，陈文伟，王　栋（416）
基于组合密钥的智能电网多源数据安全保护……高　建，王立城，余梦月，庞建民，宋国瑞（417）
基于电力大数据的经济景气指数分析……刘玉娇，宋坤煌，王　向（418）
电力大数据安全治理体系……朱洪斌，安　龙，杨铭辰（419）
电网机巡图像分析框架与深度学习方法……李远宁，宁柏锋，董召杰（420）
电力通信网省地集约化监控运行支撑系统架构及关键技术……杨志敏，洪丹轲，黄　昱（421）
230 MHz 电力无线通信技术的优化研究……赵训威，白　杰，丁高泉，相里瑜（422）
一种可量化的云计算平台安全评估模型……许　剑，靳　莉（424）

人民邮电出版社

“国网+智慧农业”生态圈建设在四川省落地实践

余梦佳[1]，尧广[1]，刘利[1]，罗新[1]，施崇智[1]，高畅[2]
（1. 国网泸州供电公司，四川 泸州 646000;
2. 国家电网四川省电力公司检修公司，四川 成都 610000）

摘　要：泛在电力物联网立足于现有电网实体与通信技术，将不同能源系统物理互联、时空信息互联、商业互联等相融合，具有全息感知、泛在连接、开放共享、融合创新的特征。依托泛在电力物联网建设，充分利用四川省农业优势，深入研究建设“国网+智慧农业”生态圈的思路，对生态圈中的两大构成：清洁能源圈和生态农业圈中各环节的工作模式及特点进行探索，该项目在四川省电力公司青年创新创意大赛中斩获铜奖。

关键词：泛在电力物联网；融合创新；“国网+智慧农业”生态圈

1　引言

新时期国网公司面临新的机遇与挑战，一是电力体制改革、售电侧放开、输配电价核准，对国网的盈利造成了巨大的冲击；二是工商业电价连续两次下调，大大压缩了电网利润[1]；三是2019年国网两会报告显示，国网780亿元利润中，超过一半的利润来自产业和金融服务，根据国资委最新要求，国网2019年利润要同比增长15%，压力空前巨大。为实现转型升级和新的利润增长点，2019年国网公司提出了建设平台型、共享型企业，通过电力的枢纽型作用，力争把更多的客户、商家吸引到国网生态圈，实现合作、共享、共赢[2-3]。

从国家政策方面来看，当前正大力推进乡村振兴、精准扶贫等一系列政策，鼓励地方结合实际发展现代农业[4-6]。四川作为农业大省，存在产业落后、交易环节长、成本高以及有机垃圾再利用困难等客观实际，现代信息技术在农业各环节也应用不足，发展数字乡村和智慧农业大有可为[7-8]。

基于此，本项目便应运而生，以泸州董允坝农业示范区为试点，依托泛在电力物联网建设，开发综合能源管控系统，打通上下游产业链，构建“国网+智慧农业”生态圈。

2　校企结合，打造生态圈

依托泛在电力物联网建设，本项目拟利用四川省水电优势，结合光伏、沼气发电等能源开发及储能系统搭建综合能源管控系统，并以董允坝农业示范区为落地试点基地，构建“国网+智慧农业”生态圈，如图1所示。

在清洁能源圈，搭建水电、沼气、光伏、低谷储能互补互换用电的综合能源管控系统，实现用能动态调节、循环利用、摊低成本；进行供暖锅炉气改电、光伏路灯基站新建。

在生态农业圈，依托国网数据中心，智能管控农产品从选种、种植、成品、市场的生命周期全过程[9]。

选种阶段：依托数据中心获取的市场反馈数据对农作物的种植类别及规模制定合理的购种方案，增加农业企业的收入，实现农业生产资料（种子、化肥等）供应商零库存。

种植阶段：进行传感器部署及监控大屏改造等，并通过智能传感终端对农业生产过程数据进行全方位采集，对大棚用电、用水、用气、采光等多种形式能源的利用进行智能监测、调度，全方位提高能源使用效率，保障能源安全、稳定、高效供应；结合农业负荷特点以及农作物生长周期规律等，运用四川大学农作物智能管控模型，制定适合农作物全天候、全季节生长的最佳管控方案，并打造种植基地观光旅游项目，振兴数字乡村经济。

成品阶段：对于成熟的农产品，将依托数据中心，科学分类、筛选品质，并积极与政府和科研机构合作，出具相应农产品的检测及营养分析报告，努力为客户提供放心、优质的农产品。

水电电出版社

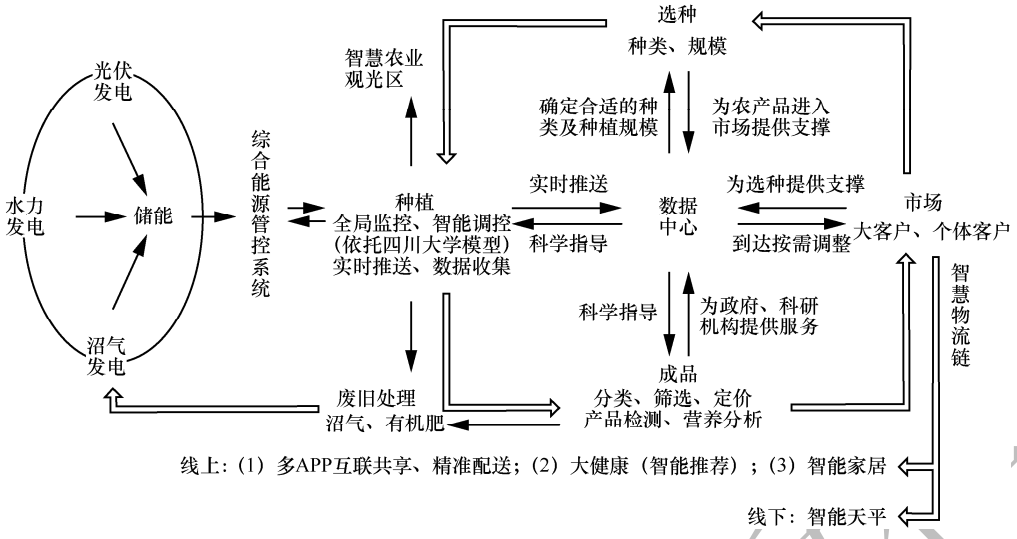


图 1 “国网+智慧农业”生态圈

市场阶段：通过大数据分析引导农业企业建立以市场需求为导向、以销定产的生产经营模式，培育“叫得响、质量优、特色显”的农村电商品牌，形成乡村智慧物流体系，建立线上与线下 2 种销售模式。

（1）线下

在景点、农贸市场、超市定点投放具有智能感知功能的电子天平进行产品销售，将农产品种类、数量等销售数据实时上传至数据中心，动态分析了解地区客户偏好，为后期的农产品选种及种植规模确定提供数据支撑。

（2）线上

对于大客户，通过智慧农业（来源可追溯、生长可视化、健康有保障）的优势，积极与企/事业单位、学校、政府等机构建立深度合作，打造健康食堂；对于个体客户，加强国网电商 APP 与“下厨房”“美食杰”等美食 APP 的合作，实现资源共享共赢，客户可根据喜好在电商 APP 中下单买菜，实现精准配送；引入大健康理念，分期出具客户饮食结构报告及配餐建议，进一步提升客户粘性；与智能家居（如智能冰箱、智能橱柜等）厂商合作，实现智能配送。

3 项目计划与商业价值

本项目计划分为 3 个阶段实施。第一阶段：研究作物全天候进行生产的最佳能源管控方案，研发综合能源管控系统；第二阶段：建设数据中心，研发智能感知天平，打通农产品-物流-农贸市场/超市-企/事业单位-小区居民的全过程产业链；第三阶段：通过示范企业的辐射效应，规模化推广，实现国网新的利润增长。

经济效益分析：农产品产量增长直接收益。根据相关资料，2018 年董允坝年收入 2.5 亿元，其中农产品收益 1.7 亿元、旅游观光及其他收益 0.8 亿元。由此计算本项目实施后农产品年产量增长 30%，旅游观光增加 25%，预计增长 7 000 万元利润。

沼气发电相关收益：结合本项目，以装机容量 100 kW 的沼气池为例，总投资 540 万元（其中 180 万元为中央财政拨款，自筹资金 360 万元，含发酵池、沼气净化系统和利用系统，沼渣用于制作有机肥），估算如下：

收入=售电收入+燃气取暖费+环保补贴+有机肥=36+30+10+120=196 万元；

成本=机组成本+沼气池成本+有机肥处理成本+（人工成本+设备维护成本）=36+10+60=106 万元。

综上可知每年净利润为 90 万元，预计 4 年收回投资（含政府补贴）。假设发电天数为 300 天，全年发电 72 万 kWh，按照 0.5 元/kWh 计算，每年节约电费 36 万元。此外每年节约燃料费 30 万元，节约污水处理费 10 万元，产生有机肥净利润 60 万元。扣除每年维护成本 10 万元。

除了上述的具体利润分析外，生态圈打造成功后，利用海量的用户，将为国网公司增加平台服务费、广告费、咨询费、金融服务费等收益，这部分才是未来主要的利润增长点。

4 结束语

“泛在电力物联网建设”是一项系统工程，是国网

公司落实党中央、国务院关于国企改革重要战略部署的一项关键举措，也是推动中国经济高质量发展的一项重要措施，需要长期的具体实践。国网泸州供电公司将利用这一难得的发展机遇，加强与政府部门、社会团体以及广大电力客户沟通协作，通过泛在电力物联网实现平台共享、合作共赢。本项目与四川大学电气学院深度合作，在建设生态圈的同时，解决弃水、弃光、弃垃圾问题，于客户更环保、节能、成本更低，于电网削峰填谷，提高负荷率，降低损耗，减少高峰期的低电压台区，并极大助力数字乡村建设和智慧农业战略。

参考文献：

[1] 顾志伟，杨威. 泛在电力物联网在地级供电企业的建设思考[J]. 中国电力企业管理. 2019(10)：70-71.

[2] 陈麒宇. 泛在电力物联网实施策略研究[J]. 发电技术. 2019(2): 99-106.

[3] 国网互联网部. 泛在电力物联网建设大纲[R]. 2019.

[4] 吴永华. 以科学规划引领乡村振兴[J]. 浙江经济, 2018(17): 35-37.

[5] 段鹏. 实施数字乡村战略 助推智慧农业发展[J]. 湖北政协, 2019(5): 20.

[6] 范秉衡. 加快数字乡村建设助力乡村振兴[J]. 中国合作经济. 2018(3): 11.

[7] 郎慧, 肖诗顺, 王艳. 四川省农业碳排放与经济增长的脱钩效应分析[J]. 山东农业大学学报(社会科学版)，2019，21(2): 69-78+158.

[8] 叶霄, 曾静, 杨晓, 等. “互联网+”环境下智慧农业发展策略研究——以四川省为例[J]. 云南农业大学学报(社会科学)，2019, 13(3): 12-16.

[9] 四川移动. 5G+智慧农业亮相海峡两岸电子信息产业对接交流会[J]. 通信与信息技术, 2019(3): 13.

人民邮电出版社

IT 共享服务中心建设方案

程华福，郑越峰，吕新丽
（国网信通产业集团北京分公司，北京 100032）

摘　要：直属单位 IT 共享服务中心整合国网信通产业集团内部优势资源，面向国网直属单位提供统一客服服务、统一运维服务、统一基础设施服务、统一安全服务。以“四统一”的服务方式承接了多家国网公司直属单位的运维业务，覆盖数据中心基础设备托管和云资源租赁服务、基础软硬件安装调试和系统应用层的运维保障服务以及信息系统安全防护服务。为国网直属单位开展了预防性诊断、隐患排查与治理等全面“健康检查”工作，为托管单位提供专业化的“管家式”服务。实现数据中心、人力、技术等资源的共享服务，有效降低资源投入成本，提升信息化水平。

关键词：IT 共享服务；IT 共享服务中心；“四统一”服务

1　引言

国家电网公司信息化于“十一五”期间开展，全面推进信息化建设，信息化工作取得显著成效。现阶段信息化推进到“十三五”期间，建设步伐明显加快，基础得到进一步夯实，信息安全保障体系取得长足进展，信息化对业务和管理的支持在深度、广度和协同度上得以全面提升。省市公司信息化取得了很大成效，但是大部分直属单位存在着信息化管理队伍人员少，运维队伍组织分散，服务质量有差距，运维体系不健全，运维标准不统一，基础设施条件无法匹配信息化发展要求，信息化安全风险缺乏有效控制手段等问题。

2018 年国家电网公司提出针对“加强直属单位信息化管理和运维机构建设，针对薄弱单位建立 IT 共享中心”的工作要求。国网信通产业集团（以下简称“集团”）在国网信通部指导下，以资源“共享、集约”为理念，成立直属单位 IT 共享服务中心（以下简称“IT 共享服务中心”）解决直属单位信息化的现存问题。

IT 共享服务中心针对国网直属单位的信息化运维业务，提供统一客户服务、统一运维服务、统一基础设施服务、统一安全服务。统筹协调集团各单位及外部供应商的 IT 服务资源，构建统一的服务体系、服务标准和服务目录，实现 IT 共享服务中心一体化运作，由综合管控整体对中心下设各部门提供的服务进行绩效考核和客户沟通评价等管理工作。

IT 共享服务中心成为直属单位客户服务的统一渠道，打破资源壁垒，实现人力资源、基础设施、新技术等资源共享，规避直属单位的运维人员架构重复建设问题，节省大量基础设施建设投入，有效控制成本；同时解决信息化投入分散，运维机构不规范，技术支撑单薄、安全防护薄弱等问题，补齐信息化短板，有效地提升效率、提高水平。

2　共享服务的概念及发展现状

共享服务是在具有多个运营单元的公司中组织管理功能的一种方式，它指企业将原来分散在不同业务单元进行的财务、人力资源管理、IT 技术等事务性或者需要充分发挥专业技能的活动，从原来的业务单元中分离出来，由专门成立的独立实体提供统一的服务。

共享服务起源于 20 世纪 80 年代末的美国，以其能够帮助大型企业降低成本、提高服务质量、提升企业战略管理水平和技术运用水平等优势，在西方得以快速发展，并成长为一种较为重要的管理模式和组织形式。罗伯特等人在 1993 年最早提出共享服务这个词汇[1]，他们认为共享服务是一种管理模式，企业利用这种模式对现有分散管理方式进行改进，使其逐步发展成集中管理模式，进而赢得竞争优势。学者朱先军等人[2]在 2009 年所发表的有关论述中表示，对于规模比较大的企业来说，IT 共享服务模式要更为适用，企业可以通过共享实现资源整合，能够有效提升企业

人民邮电出版社

解决问题的效率。学者何英[2]在 2010 年对 IT 共享中心提出新的定义，指出企业利用 IT 共享服务对资源、业务等进行整合，可有效降低企业的人力成本，工作效率能够得到大幅度提升。学者侯锐[2]对 IT 共享模式进行了深入的分析，这种模式能够提升企业业务流程操作的规范性，能够强化企业风险管理。

近几十年来，全球经济与技术飞跃性的发展，推动了技术、资金、人员等资源在全球范围内的流动，在这样的环境下，全世界的公司都在不断寻求资源高效利用法，共享成为一种比较可行的方式。现在，越来越多的公司进行区域或者全球共享服务中心的建立工作，坚持以客户需求为导向，能够基于市场价格与服务水平协议为企业业务单位提供专业化的服务，让企业能够把更多的精力与资源放在自身核心业务的发展上。共享服务的意义体现在：企业整体成本效率最大化；组织协同能力增强，效益增大；为企业其他业务部门提供有力的支撑服务;企业投资的灵活性增加，保障了长期的竞争优势[3]。

最早使用共享服务中心这一管理模式的是美国福特公司。20 世纪 80 年代初，福特就在欧洲成立了财务服务共享中心。随后，杜邦和通用电气在 80 年代后期也建立了相似的机构。90 年代初期，惠普、道尔和 IBM 也相继做出这样的决定。国内企业海尔集团、新奥集团、中国联通也正使用共享服务中心管理模式。2017 年 11 月 8 日，中国石化共享服务有限公司成立，实现财务、HR、IT 一体化共享，推动资源优化配置，促进职能部门转型，提高经营管理效率，节约管理运行成本。国网信通产业集团在 2016 年开展财务共享服务中心试点工作，将财务管理人员从繁杂的非核心业务工作中解放出来。目前全球在财务、人力资源、市场营销、IT 管理等业务都有不同程度的共享服务业务，但是 IT 共享服务与其他有一定的区别，不仅在建立的标准上要求较高，同时面临 IT 资源调配、项目管理以及各种外包管理等问题。

3 建设 IT 共享服务中心的必要性和可行性

3.1 IT 共享服务中心建设的理论基础

3.1.1 规模经济效应

共享服务模式通过对多个职能相同的独立部门进行整合的方式来达到规模的扩大和生产成本的降低，所以适用于规模经济理论，具体可以从以下几方面进行。

• 组织重复建设情况被最大化避免，进而减少企业相关成本支出。

• 通过资源的整合可以实现效率的最大化，进而增强企业的融资能力。

• 通过资源整合来实现业务操作的标准化，进而有效降低成本。

规模效应产生的基础为现代科学技术的进步，随着科学技术的不断发展，相同投入获得的产出不断提升，所以共享服务模式要想获得同样的成本优势，对于技术发展的关注以及技术成果的运用都是十分必要的。

3.1.2 资源配置理论

共享服务非常显著的两个特征即共享和集中，其中共享的为资源，通过将企业有效资源合理分配至企业各部门并实现资源配置的最优化，可以促使企业资源效用得到最大程度的发挥,进而获得最大化的利益。共享服务模式在企业中的运用使得资源配置的要求很好地得到了实现。

• 企业通过共享服务模式的构建，不仅可以实现资源的集约配置和集中共享，还可以使资源的利用效率最大化。

• 从企业层面来看，共享服务模式实现了将企业的人力和资源集中到企业核心业务方面，使企业竞争力得以大幅提升。

• 通过共享模式的构建，企业规模经济效应可以最大化发挥，进而促使资源利用效率进一步提升。

3.1.3 虚拟团队

虚拟团队是基于现代信息技术发展而出现的一种团队形式，团队成员多为跨组织以及跨地区的人员，通过现代通信信息技术的运用和工作的协作来达成企业或者是组织的发展目标。与传统的团队相比较，其具有以下几方面的优势：组织更具灵活性；可以实现人力资源的整合，并充分利用共享中心的理论基础。

由此可见，资源配置理论、规模经济效益以及虚拟团队等理论为共享服务模式的发展提供了坚实的基础。

3.2 IT 共享服务中心建设的必要性

国家电网公司在 2019 年指出基于能源互联网的功能特点和国家电网公司的责任使命，建设的能源互联网企业必然是具有枢纽型、平台型、共享型特征的现代企业。树立“开放、合作、共赢”的理念，积极有序地推进投资和市场开放，吸引更多社会资本和各

人民邮电出版社

类市场主体参与能源互联网建设和价值挖掘，带动产业链上下游共同发展，打造共建共治共赢的能源互联网生态圈，与全社会共享发展成果。

“共享服务”作为一种比较成熟的商业模式，可以通过建立共享服务中心，为公司提供 IT 和业务等方面的标准化服务，有效降低运营总成本，为公司打造“三型两网”企业提供有力支持。因此，在经济全球一体化进程日益加快的大背景下，建设 IT 共享服务中心尤为必要。

国网公司信息化发展规划经历了“十一五”“十二五”、“十三五”3 个阶段，国网的运维业务总体经历了从粗放式到标准化再到向智能化发展的三大历程，在这个过程中国网公司内部信息化企业对国网不断变化的信息化要求应是创新，紧跟总部的步伐，持续推进自身服务产品的演进发展。“十一五”初期为 SG186 的规划建设时期，信息化业务都重在研发、建设，运维的业务规模相对较小，没有一个大的业务范围的领域产出，整个运维为粗放的、被动式的。“十一五”末期“十二五”初期，大量的系统上线了，开始进入建转运期，运维业务出现分散式、爆炸式增长，运维业务主要为被动救火的形式，总部为了改变运维业务的现状，提出了“两极三线”和调研体系，由被动式、救火式的运维业务向主动式运维发展。经过“十二五”期间的信息化建设，坚持“统一管理、统一规划设计、统一标准、统一建设”的原则，实现了多专业数据的集成共享，但实现系统用好、用深还面临着诸多挑战。企业级信息系统庞大而复杂，系统运维面临挑战。“十三五”初期，国网公司内部部分单位在参观了互联网公司企业后，提出运维业务向自动化方向发展，随后公司提出全面建设全新“SG-ITOM3.0”运维架构，新的运维体系、新的运行标准、紧缩的运维费用、更高的效率要求，目标直指智能化运维。随着信息化的不断发展，国网部分直属单位的信息化水平与省市公司开始显现出一定的差距，公司对此很重视，提出“加强直属单位信息化管理和运维机构建设，针对薄弱单位建设 IT 共享服务中心”，IT 共享服务中心是应势而生。对 IT 服务进行统一协调和整合，通过共享 IT 服务，实现业务需求快速响应，IT 资源集约化配置及管理效益稳步提升。

3.3 建设 IT 共享服务中心的可行性

作为一种比较成熟的商业模式，“共享服务”已在国内外大型企业，尤其是跨国大公司中广泛应用。据了解，目前已有超过 50%的《财富》500 强企业建立了共享服务中心。1999 年，摩托罗拉公司在天津成立亚洲财务结算中心，2006 年更名为摩托罗拉全球会计服务中心；2003 年，埃森哲在上海成立亚太共享服务中心，为在 10 个亚太国家 19 个工作地点的 1.4 万多名埃森哲员工提供支持服务；2004 年，惠普公司在大连成立共享服务中心，为北亚区的日本、韩国和中国等国家提供共享服务。近几年来，中国平安保险、中国保险集团、海尔集团、四川长虹等一批国内大型公司也先行建立了共享服务中心，并已经取得实效。到 2010 年年底，中国境内已有超过 450 家共享服务中心，100 人以上的共享服务中心达到 340 多家，共享服务业务领域涵盖了各行各业。

国网公司在 2018 年提出加强直属单位信息化管理和运维机构建设，针对薄弱单位建立 IT 共享中心。完善地市公司信通组织机构，优化相关专业工作界面。国网信通产业集团在总部的指导下，对 24 家直属单位的信息化现状进行了调研。调研发现大部分直属单位存在着信息化管理队伍人员少，运维队伍组织分散，运维体系不健全，运维标准不统一，基础设施条件无法匹配信息化发展要求，信息化安全风险缺乏有效控制手段，信息化水平与国网公司整体信息化水平存在一定差距等问题。以资源“共享、集约”为理念，通过建设 IT 共享服务中心全面提升直属单位的信息化水平。

国网信通产业集团，有充足资源作保证，备足软硬件资源，并建立了一支信息化人才梯队，这些能为 IT 共享服务提供有效的资源支撑。IT 共享服务的流程和组织模式可采用建运一体模式。建运一体是一整套流程、技术方法和工具的统称，用于促进开发、技术运营和质量保障部门之间的沟通、协作与整合。通过采用建运一体模式，能将开发、测试、发布过程高度集成管控，确保运维团队和开发团队之间的协作，大大提升 IT 共享服务的质量和效率。IT 共享服务在管控模式上可引入分系统模块的责任制模式。为实现 IT 共享服务过程灵活化、服务内容个性化，真正做到以客户为导向，可在每个系统模块下设立相应的责任人，该责任人负责其系统从问题与需求收集分析至服务交付的全过程管理。

4 国网公司直属单位 IT 共享服务中心的建设

4.1 坚持国网特色的共享服务建设思路及目标

IT 共享服务中心为各直属单位提供“统一客户服

人民邮电出版社

务、统一运维服务、统一基础设施共享服务、统一安全服务”，通过建立统一的组织体系、服务标准，强化服务管理、考核评价和资源协调，实现“资源共享、控制成本、补齐短板、提升效率、提高水平”的工作目标。

IT 共享中心通过统一管理，打破资源壁垒，实现人力资源、基础设施、新技术等“资源共享”。通过人力资源、基础设施资源共享，规避各直属单位的人员架构和基础环境的重复建设，节省大量的基础设施建设投入，有效“控制成本”。建立统一渠道、统一制度、统一标准的组织机构，定期开展全面的安全隐患排查及修复、技术业务培训、经验共享、知识库学习，实现各直属单位信息化“补齐短板”。实现客户服务和基础设施地理上的集中，调、运、检工作在工作内容和工作团队上集中。IT 共享服务中心将化被动运维服务为主动运维服务，达到了“提高质量”。IT 共享服务中心在集团统一的规范和标准管控体系下，整体在给直属单位提供的 “四统一”服务方面“提升水平”。

以“集约、共享”的建设思路，共享服务中心建设要紧紧围绕国网公司的大战略，共享服务范围应全面配合推进战略的发展。按照“统一规划、统一标准、统一设计、统一投资、统一建设、统一管理”的六统一原则，统一制定共享服务体系规划，统一制定共享服务体系架构、信息化标准和服务标准，统一设计和建设共享服务信息化平台，统一管理共享服务中心运营和开展绩效考核。对重点业务及无人问津、多人管理等业务开展共享服务，从提高资源利用率、降低总运营成本、提升经营管理水平的角度出发，充分利用信息化手段，提供全方位、一体化的保姆式服务。

4.2 建设直属单位 IT 共享服务体系

国网信通产业集团根据国网内部实际情况，按照“试点先行、分步推广”的原则，先期以北七家园区单位为试点，整合国网信通产业集团内部信息基础设施资源、信息技术资源和信息化队伍资源，建设 IT 共享服务信息化平台，在试点建设过程中总结经验，设立标杆，逐步扩大服务覆盖范围，最终实现业务覆盖全部直属单位的 IT 共享服务中心。

IT 共享服务中心引入（信息客服）ISC 工具和 ITSS/ISO20000 等 IT 服务管理标准，并建立起相关的服务标准、管理标准以及绩效评价指标体系。

4.3 直属单位 IT 共享服务中心建设

自 2018 年以来，国网总部领导和组织，走访多家直属单位进行全面调研和研究，确定建设直属单位 IT 共享服务中心，主要针对国网直属单位信息化运维业务，提供统一客户服务、统一运维服务、统一基础设施共享服务、统一安全服务的“四统一”服务。2018 年 7 月前，先后完成方案制定、人员、场地等各项准备工作，成立了直属单位 IT 共享服务中心，与 8 家直属单位签署了合作备忘录，逐步完成了人员选拔和培训，制订了业务流程、制度、考核等管理办法。中心下设客服中心、运维中心、基础设施中心、安全中心、综合管控部、调控中心、技术支持服务中心，如图 1 所示。

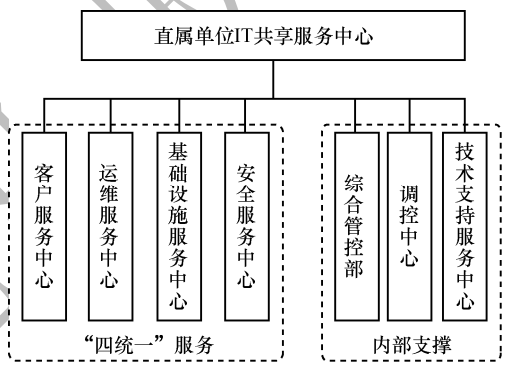


图 1 IT 共享服务中心组织机构

4.3.1 组织架构

• 客户中心

负责制定统一的客户服务规范和服务流程，实现直属单位信息通信服务请求的统一入口，受理统一客服 1186 服务热线，包括服务请求受理、问题受理、信息发布、投诉受理、客户回访、业务需求收集和统计分析等。

• 运维中心

以驻场、现场及远程支持形式为各直属单位提供硬件设备、基础软件、应用系统的安装调试、故障受理、升级维护、升级扩容、环境迁移、系统迁移、特殊保障等多项信息系统运维服务内容。

• 基础设施中心

基于北七家数据中心提供机房租赁、服务器租赁托管、机柜租赁、网络通信以及云资源服务，包括云弹性计算、云存储、系统迁移上云等服务。

• 安全中心

安全服务囊括技防体系建设、高级监测分析、安

全专项以及红蓝队服务，也从实体安全、运行安全、信息安全、安全管理方面提供全面的信息化安防解决方案。

• 综合管控部

制定 IT 共享服务中心的配套管控、运行、考核等机制流程，开展日常管理、评价考核等工作。负责中心发展战略规划以及统筹协调所需人、财、物等相关资源、中心市场的拓展和合同签署以及 IT 共享品牌宣传、策划、培训等事项。

• 监控中心

负责制定调控服务流程及管控机制，实现对直属单位信息网络系统的 7×24 h 监控，主要工作职责包括信息通信调度值班、检修计划管理、方式资源管理、故障处置协调指挥、应急管理和统计分析等。

• 技术支持服务中心

响应与处置直属单位包括业务应用、系统平台、安全防护、基础设施、高级巡检等方面的重大服务请求。

4.3.2 运行机制建设

IT 共享服务中心根据各直属单位“四统一”服务购买情况，基于项目合同额及人员能力设置相应业务的项目经理，项目经理负责汇总、收集所服务直属单位的信息化系统阶段性运行报告，将该报告提交至综合管控部及相应中心领导。同时项目经理根据实际运行情况将直属单位的需求意向推送至“一对一”大客户经理，由“一对一”大客户经理根据相应的意向，与直属单位开展下阶段工作。

IT 共享服务中心内部参照国网公司信息系统调运检体系的相关规范，形成以调控中心为核心、以客户服务中心为入口，“纵向联动、横向协同”的格局。

IT 共享服务中心运行流程如图 2 所示。

调控中心与国网信通调度形成纵向联动机制，通过 I6000 及综合网管等系统，实现对直属单位信息网络系统的 7×24 h 监控。根据告警类型通知运维服务中心、基础设施服务中心、安全服务中心进行处置。处置中如需其他中心协作，需向调控中心提出联合处置需求，由调控中心协调资源解决问题。

客户服务中心受理直属单位用户的请求、咨询、问题等服务请求，将无法处理的请求通过 ICS 系统工单，辅以电话、邮件等形式派送到运维服务中心、基础设施服务中心和安全服务中心的相关人员处，并及时跟踪反馈结果；客户服务中心派发的问题如需联合处置，则由调控中心协调资源。

4.3.3 需要处理好人力资源方面问题

共享服务体系建设不能一蹴而就，也不会一帆风顺，要充分考虑到建设过程可能会遇到的问题与困难，资源整合是共享服务中心建设的基础。在共享服务体系的建设过程中，必然会涉及到信息基础设施的整合和人员队伍的整合等。直属单位 IT 共享服务中心主要涉及人员队伍的整合和未来 IT 共享服务平台整体信息化技术架构的规划。在资源整合中，人员的整合是最难的，因为涉及到个人的工作环境变化、工资待遇调整和个人成长规划实现等各方面问题。

5 直属单位 IT 共享服务中心践行信通“三型”生态

直属单位 IT 共享服务中心自 2018 年 7 月成立后，

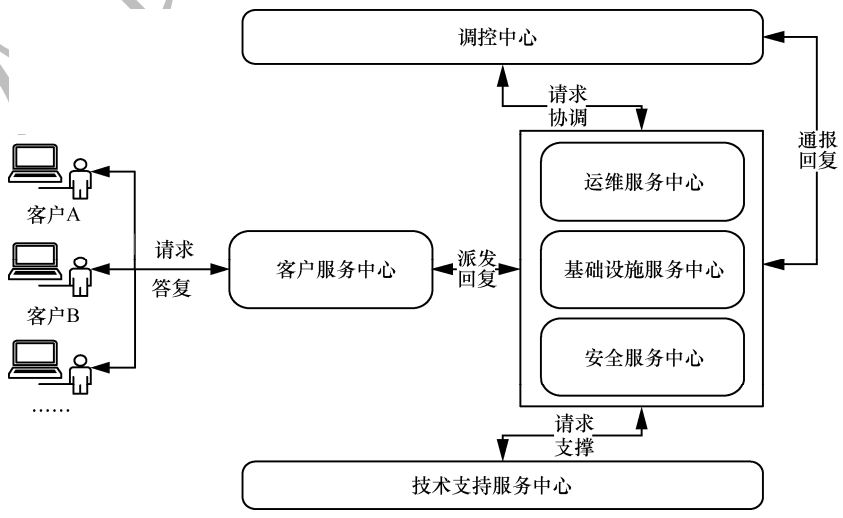


图 2 IT 共享服务中心运行流程

以“四统一”服务方式承接了 16 家直属单位的运维业务，整合了国网信通产业集团内部的优势资源，为托管单位提供专业化的“管家式”服务，截至目前，各单位信息系统可用率为 99.96%，信息网络可用率为 99.99%，设备可靠率为 99.99%，未发生信息系统故障和非计划停运问题，未发生网络安全运行事件。

5.1 增强了试点单位整体网络安全保障能力

针对直属单位信息化人员不足，运维资源分散，运维服务管理薄弱，网络安全水平低等现状，一是从信息系统基础环境、软硬件平台、业务应用、安全防护层面开展常态化检查和运行监控，开展了预防性诊断、隐患排查与治理等全面的“健康检查”工作，共检查 18 套自建业务系统，涉及服务器主机 297 台；核查防火墙、IPS、WAF 设备 16 台，各类交换机设备 50 余台；检查办公内网 5 个 C 段超 600 台办公终端；共查出设备配置不规范、弱口令、系统及应用层漏洞等六大类共 116 个问题，并完成漏洞整改消缺工作，有效提高了试点单位的安全防护能力，逐步实现了“补齐短板”。二是建设了安全等级高、服务全面的基础设施共享中心，完成了机房的安全加固、T3+等保及安全和性能测评工作，确保了基础设施环境的安全防护能力和服务质量，为直属单位提供安全可靠的运行环境。三是与直属单位共建红蓝督联队，开展常态化漏扫、整改和演练工作，形成信息共享、资源共享、情报共享、工具共享等工作机制。以攻促防，增强实战能力，提升信息系统的安全防护能力。四是与英大金融单位共建网络预警与通报中心，统筹资源，强化协调指挥，加强网络安全分析、监控、稽查力量建设，增强了金融单位的安全预警能力。五是全面加强开展重大活动以及节假日期间的保障工作，完成 2019 年全国“两会”（XT19001）保电期间被服务单位的信息通信及网络安全保障工作；完成了第二届“一带一路”国际合作高峰论坛及 2019 年中国北京世界园艺博览会期间的信息通信系统保障工作，针对 IT 共享服务中心的消防安全进行了检查和整改，开展“防风险保平安迎大庆”消防安全隐患排查治理专项行动，承担国家网络安全专项演习（XT19003）保障工作。

5.2 强化了信通生产调度运行体系建设，充分实现公司内部资源共享

一是建立了 IT 共享服务中心的运营协调机制、管理机制、考核机制、营销机制及分配机制，编制并下发了统一调度、运行、检修、客户服务指导手册，完善了试点运维单位的业务流程；二是通过对客服、运维、安全和调控等核心岗位的梳理，不断优化运维队伍结构、共享人力资源；三是组织开展软硬件平台、业务系统、安全技能等专项技能培训，通过共享培训资源，逐步实现核心业务运维人员 100%持证上岗。明确 IT 共享服务中心承接信息通信系统在设备巡检、上下线、系统检修、定级评测、资料存档等业务方面的操作规范和标准；进一步完善 IT 共享服务中心管理办法、考核细则，落实信息安规“三种人”制度在直属单位的应用。充分共享资源，统一开展直属单位应急演练工作，将园区单位的应急演练规划好、开展好。

5.3 提升了直属单位运维能力，支撑其聚焦核心业务

针对直属单位人员信息化力量不足、管控能力弱等问题，IT 共享服务中心整合国网信通产业集团优势资源，并为其提供专业化的“管家式”服务。引进“互联网+”理念，采用先进的智能化运维管控平台。从信息系统运行环境、软硬件平台、业务应用、安全防护层面开展常态化检查和运行监控，提升服务响应速度，对隐患实施预防性诊断以及排查与治理，贯彻落实国网信通部相关信息化专项工作，全面承担各单位核心系统的安全运行，解决试点单位网络安全运行“散、乱、人少”等突出问题，迅速为其补齐短板，提升运维服务水平，保障试点单位生产经营业务正常开展，支撑其聚焦核心业务。截至目前，统一客服创建工单 2.5 万余张，一线解决率达 78.4%，同比提高 14%；统一运维解决率达 96.8%，同比提高 12%，工单平均处理时长由原来的 118 min 缩短至 87 min；试点单位信息系统可用率达 99.96%，信息网络可用率达 99.99%，设备可靠率达 99.99%，监测告警 1 156 次，未发生信息系统故障和非计划停运，未发生网络安全运行事件，全面保障了试点单位的生产经营工作。

5.4 打造了信息通信产业新模式新业态

国网信通产业集团不断聚焦信息通信运维业务，将 IT 共享服务中心作为集团运维品牌。一是积极与公司 25 家直属单位（安全运行 B、C 类直属单位）进行交流沟通，以“四统一”服务模式承接运维业务，与国网英大集团共建 IT 共享服务中心金融分中心，IT 共享服务品牌效应初显；二是通过日常运维工作，积累大量系统运行数据和用户需求，成为集团信息系统研发和创新需求来源的重要战略高地，是集团发展运营产业生态建设的重要平台；三是作为集团核心业务

之一，不断加大投入力度，2018 年已投资 7000 余万元用于基础设施扩建和安全防护加固、运营管理系统和自动化运维工具，以及办公场地配套设施等项目建设，为直属单位信息系统的托管和运行提供全面的安全防护与运行支撑；四是按照公司要求，多措并举，不断提高核心岗位、核心人员的自主化水平，组建安全共享服务团队，实现安全资源共享、技术共享、情报共享及工具共享的专业红蓝督团队。

5.5 安全工具共享平台建设

当下中国的网络安全被纳入国家战略规划，国网公司作为中国重要的基础设施建设和支撑单位，网络安全管理形势尤为严峻，目前直属单位及集团内部安全力量总体偏弱。IT 共享服务中心致力于为用户提供更好、更安全的服务，努力降本增效、促进安全工具共享，筹备规划了 IT 共享服务中心安全工具共享平台建设，解决传统安全设备数量少、设备老旧、缺乏高端监测工具、台账缺乏记录、工具无共享等问题，初期先提供本单位所需的安全工具包括硬件安全设备、软件安全系统、人工渗透测试支持、安全培训服务等，逐步过渡到实现安全工具在线的 SaaS 服务。后期实现安全工具等对集团内部及直属单位等外部公司的在线运营，实现集团对总部相关单位的安全工具使用趋势、安全问题发展态势等进行精准预测，实现安全工具的全面共享和针对性的安全管理。

5.6 拓展服务范围，创新服务模式，加强品牌建设

针对公司直属单位总体信息化安全和运维态势，在充分总结试点经验的基础上，适度扩大试点范围，承担更多职责。一是持续优化内部建设，夯实北七家运维班组能力，开展客服、调控中心 7×24 h 服务体系建设，提升运维服务水平，加大运维模式创新力度，利用管理手段和新技术应用，降低属地运维人员比例，适应直属单位点多面广及外地分支机构的服务需求，在金融分中心、清河区域、都城区域扩大试点，延伸“四统一”服务覆盖范围；二是拓展服务模式，加大业务创新模式，通过多种模式服务直属单位，采用经营性租赁方式，快速开展信息系统的完善提升工作，针对直属单位的共性需求，采用集中建设、服务租赁方式开展运营；三是加快金融分中心的建设，面向国网金融单位统一提供安全高效的金融信息化服务支撑，于 2 月底组织召开试点运行工作总结座谈会暨金融分中心建设推进会，邀请公司相关领导、国网信通部领导和相关直属单位领导参加，年内完成金融分中心试运行。

6 结束语

国网公司于 2019 年提出要建设世界一流的能源互联网企业就要打造“三型两网”企业的目标追求。以能源互联网为支撑，以公司品牌信誉为保障，汇聚各类资源，促进供需对接、要素重组、融通创新，打造能源配置平台、综合服务平台和新业务、新业态、新模式发展平台，打造共建共治共赢的能源互联网生态圈，与全社会共享发展成果。IT 共享中心力争建成国内一流的共享服务平台，在做好直属单位信息化服务的同时，要把集团先进的成果及服务能力向其他央企输出。通过管理创新、技术创新和能力提升，实现集团业务运营，加快推进枢纽型、共享型、平台型企业建设。

参考文献：

[1] 文必龙, 赵晶浩, 张璇, 等. IT 系统运维管理研究[J].计算机系统应用, 2018(3): 44-46.

[2] 李宝玲, 曹宝香. 基于 ITIL 的安全管理平台流程响应机制设计[J]. 计算机安全, 2017(3): 12-13.

[3] 屠正. A 集团中国区 IT 共享服务中心费用分摊管理办法的研究[D]. 南京: 东南大学, 2018.

[4] 王景涛. 以信息化建设为平台构建石化特色共享服务体系[J]. 信息系统工程, 2012(9): 114-117.

[5] 刘森, 余芸, 赵武清. 南方电网 IT 共享服务模式的研究与探索[J]. 企业管理, 2016(S2): 530-532.

人民邮电出版社

LTE-230 MHz 电力无线专网在泛在电力物联网建设中的应用与实践

韩冰洋，宋继高，王炫中
（北京中电飞华通信股份有限公司，北京 100071）

摘　要：在建设泛在电力物联网的背景下，LTE-230 MHz 电力无线专网以其广覆盖、低时延、高可靠的优点可作为解决海量终端“最后一公里”接入难题的重要手段。基于此，国家电网有限公司在嘉兴建成了地市级全覆盖的电力无线专网。首先介绍了 LTE-230 MHz 电力无线专网的关键技术方案、系统性能、安全架构，接着介绍了嘉兴电力无线专网的建设和应用情况，最后通过 LTE-230 MHz 电力无线专网对现网业务承载的通信性能和安全性测试分析，表明 LTE-230 MHz 系统在通信和安全方面均满足电力业务需求。

关键词：LTE-230 MHz；电力无线专网；性能测试；应用实践

1　引言

随着国家电网有限公司（以下简称国网公司）全面部署“三型两网，世界一流”战略，泛在电力物联网作为与能源互联网同等重要的“第二张网”首次被公众聚焦。两网相辅相成，能源互联网是泛在电力物联网的必要基础，而泛在电力物联网是建设能源流、业务流、数据流“三流合一”能源互联网的核心任务。

目前，国网公司物联网建设和应用已具有一定规模，覆盖电力生产经营各个环节，已接入智能电表、输变电监测装置、配电自动化装置、摄像头等终端 5 亿余台（套），采集数据日增量达 TB（2^{40} byte）级，支撑了当前各专业自身的管理和应用需求。然而，面对泛在电力物联网海量终端接入需求和爆发式增长的业务数据，现有光纤专网/无线公网的建设模式已经无法满足业务接入需求。此外，光纤建设难度大、成本高，而公网存在安全隐患、可靠性低、容量受限、运维不便等缺点，无法满足泛在电力物联网终端“最后一公里”的接入需要[1]。

电力无线专网具有“安全、可靠、经济、泛在、灵活”等优点，能够弥补光纤建设成本高、施工难度大且接入受限的不足，有效破解电力业务接入受限的局面，是构建泛在电力物联网的关键一环[2]。

国网公司在嘉兴开展电力无线专网试点建设，于 2018 年建成了首个地市级全覆盖的 LTE-230 MHz 电力无线专网，是覆盖面积最广、规模最大、接入终端数量最多的电力无线专网，为泛在电力物联网建设奠定坚实的通信网络基础。

2　LTE-230 MHz 电力无线专网

2.1　频率资源

LTE-230 MHz 电力无线专网工作频段为 223～235 MHz。根据国家无线电管理委员会在 1991 年印发的《关于印发民用超短波遥测、遥控、数据传输业务频段规划的通知》（国无管[1991]5 号），230 MHz 频段共 12 MHz 作为遥测、遥控、数据传输等业务使用的频段，分配给电力、地震局、天文、建设部、军队、气象局、轻工业部、水利部等 8 个行业。其中分配用于电力行业有 40 个离散频点，共 1 MHz 频率[3]。国家无线电管理委员会于 2018 年批准 223~226 MHz 和 229~233 MHz 共 7 MHz 频率资源作为电力、燃气、人防、水务等行业数据传输共享频段[4]。

230 MHz 属于低频段，具备较强的穿透、绕射、衍射能力，与高频段无线通信系统相比，LTE-230 MHz 电力无线专网能实现无线信号的广、深覆盖，既能满足电力行业深度覆盖需求，又能减少基站建设数量，

基金项目：国家电网公司科技项目（No.5700-201941234A-0-0-00）

人民邮电出版社

节约成本，还能充分利用电力自有物业，满足无线专网建设站址选择的要求[5]。

2.2 技术体制

LTE-230 MHz 电力无线专网采用基于 25 kHz 离散载波聚合的时分双工 LTE-230 MHz 电力无线通信系统[6]。

LTE-230 MHz 电力无线专网通过采用载波聚合技术将离散的频谱资源整合为适合电力行业的宽带资源，并重新设计帧结构，调整上下行子帧配比以适应电力业务数据传输特点[7]。采用频谱感知、干扰协调技术提高系统抗干扰能力，提升电力无线专网在频谱资源多行业共用条件下的可靠性和可用性。同时采用 OFDM、高阶调制、高效编码等技术，提升数据传输速率，并采用扁平化的系统结构降低数据传输时延[2, 8]。LTE-230 MHz 系统的高带宽、低时延、高安全性等优点能有效满足电网各类业务的安全接入需求。

2.2.1 载波聚合

载波聚合技术（carrier aggregation，CA）通过将多个成员载波（component carrier，CC）聚合在一起，实现宽带传输，提升传输速率。由于电力无线专网使用的是离散频点，通过载波聚合能产生几倍于单子带系统的传输带宽，达到宽带传输的效果[9]。目前 LTE-230 MHz 电力无线专网通信终端可以实现 200 个离散载波聚合达到 5 MHz 带宽。

2.2.2 OFDM

正交频分复用（orthogonal frequency division multiplexing，OFDM）技术是将高速串行数据流转换为低速并行数据流，通过相互正交的子载波调制后传输[10]，并通过增加循环前缀（cyclic prefix，CP），可以抗多径衰落和符号间干扰（inter symbol interference，ISI）。由于电力行业使用的是离散频点，每个频带带宽为 25 kHz，因此 LTE-230 MHz 电力无线专网子载波间隔设置为 2 kHz，每个频点的 25 kHz 信道带宽内部署 11 个子载波[6]。

2.2.3 调制与编码

LTE-230 MHz 电力无线专网物理层调制方案采用 BIT/SK、QPSK、16QAM 和 64QAM，信道编码方案采用（3，1，7）咬尾卷积编码和 Turbo 编码[6]。通过采用自适应重传（hybrid automatic repeat request，HARQ）、自适应调制编码（adaptive modulation and coding，AMC）技术保障系统 QoS。

2.2.4 帧结构设计

LTE-230 MHz 电力无线专网采用时分双工（time sivision duplexing，TDD）的通信模式，上下行数据使用不同的时隙传输，可以根据业务需要灵活配置上下行信道资源[11]。对于电力行业“上行数据大而下行数据小”的情况，LTE-230MHz 电力无线专网采用 3：1 的上下行配比，即一个无线帧由 5 个长度为 5 ms 的子帧组成，包含一个特殊子帧、3 个上行子帧和 1 个下行子帧[6]。

2.2.5 资源调度机制

LTE-230 MHz 电力无线专网通过动态调度、干扰规避机制，保证传输可靠性。基于测量—反馈的频率选择性调度机制，使高可靠性要求的业务工作在信道质量较好的子带上，不仅有效规避受严重干扰的子带，确保高优先级业务的传输要求，使系统整体性能最优，还降低了对异系统的干扰。

2.3 系统组成与性能指标

LTE-230 MHz 电力无线专网由核心网（evolved packet core，EPC）、基站（evolved node B，eNB）、通信终端（user equipment，UE）、网管系统（operation and maintenance center，OMC）构成[5]，其系统架构如图 1 所示。

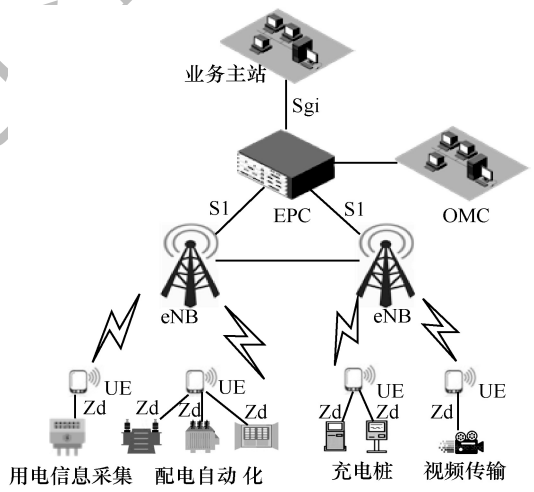


图 1 LTE-230MHz 电力无线专网系统架构

2.3.1 UE

UE 与电力业务终端通过 Zd 接口实现数据交互[6]，二者可以实现无缝连接，即插即用。UE 能支持电力采集类业务数据的汇聚和上传、控制信息的下发等功能。UE 形态分为独立式终端和嵌入式终端，支持 25 kHz 离散载波聚合，目前最多可支持 200 个子带载波聚合。UE 传输能力见表 1[6]。

2.3.2 eNB

eNB 是 LTE-230 MHz 电力无线专网的核心网元，包括天线、射频拉远单元（remote radio unit，RRU）

表 1　UE 峰值速率

信噪比	最大速率/kbit/s	子带数 1	子带数 4	子带数 8	子带数 16	子带数 40	子带数 80	子带数 140	子带数 200
信噪比≥20 dB（64QAM）	上行	50.9	208.8	417.8	840.9	2107.8	4215.6	7377.3	10539
	下行	21.9	76.5	177.8	385.9	1 009.7	2 019.4	3 533.9	5 048.5
信噪比 8~15 dB（16QAM）	上行	27	110.6	221.3	447.8	1 122.5	2245	3 928.8	5 612.5
	下行	11.5	40.3	107.8	218.4	550	1 100	1 925	2 750
信噪比-3~3 dB（QPSK）	上行	6	12	24	48	128	256	448	640
	下行	2	4.1	11.2	22.4	60	120	210	300

和基带处理单元（baseband unite，BBU），提供有线/无线协议转换、无线资源管理分配、终端接入与控制等功能，通过S1接口接入电力SDH回传网实现与EPC之间的数据传输[5]。其工作带宽为 25 kHz×N(N=1～280），典型工作带宽包括 500 kHz、1 MHz、3.5 MHz、5 MHz、7 MHz。其传输性能见表 2 [6]。

2.3.3　EPC

EPC 负责终端鉴权认证、数据加密、IP 地址管理、移动性管理等，通过 Sgi 接口接入电力骨干通信网与业务主站通信[5]。核心网按性能可分为Ⅰ、Ⅱ、Ⅲ、Ⅳ、Ⅴ 5 类，系统容量指标见表 3 [6]。

2.3.4　OMC

OMC 可管理的网元对象包括 EPC、eNB、UE，能够实现配置管理、性能管理、故障管理、软件管理等，并提供 GIS 功能[7]，并通过北向接口接入电力终端通信接入网管理系统。

OMC 系统按性能分为Ⅰ、Ⅱ、Ⅲ、Ⅳ 4 类，其系统容量指标见表 4 [6]。

2.4　安全防护

根据电力安全防护要求，生产控制类大区与管理信息化大区的业务需要实现物理隔离，且生产类和控制类业务需要实现通道的逻辑隔离。因此 LTE-230 MHz 电力无线专网通过空口不同物理资源（频率隔离）[12]、双基站传输板/端口、双核心网/板卡和 SDH 通道或综合数据网为不同业务提供通道，通过 APN/VPN 实现管理信息大区内业务之间的逻辑隔离[13-14]。电力无线

表 2　eNB 峰值速率

带宽	500 kHz	1 MHz	3.5 MHz	5 MHz	7 MHz
上行峰值速率	1 Mbit/s	2.1 Mbit/s	7.2 Mbit/s	10.3 Mbit/s	14.4 Mbit/s
下行峰值速率	0.5 Mbit/s	1 Mbit/s	3.5 Mbit/s	5 Mbit/s	7 Mbit/s

表 3　核心网设备主要系统容量指标

分类	单设备可接入基站数量 A	单设备可承载终端数量 B
Ⅰ	A≥400	B≥20 万
Ⅱ	200≤A＜400	10 万≤B＜20 万
Ⅲ	100≤A＜200	5 万≤B＜10 万
Ⅳ	30≤A＜100	1 万≤B＜5 万
Ⅴ	1	B≥1 000

表 4　OMC 系统容量指标

分类	可管理核心网数量 A	可管理基站数量 B	可管理用户数量 C
Ⅰ	A≥10	B≥4 000	C≥200 万
Ⅱ	5≤A＜10	2 000≤B＜4 000	100 万≤C＜200 万
Ⅲ	1≤A＜5	400≤B＜2 000	20 万≤C＜100 万
Ⅳ	1	1≤B＜400	1≤C＜20 万

水电出版社

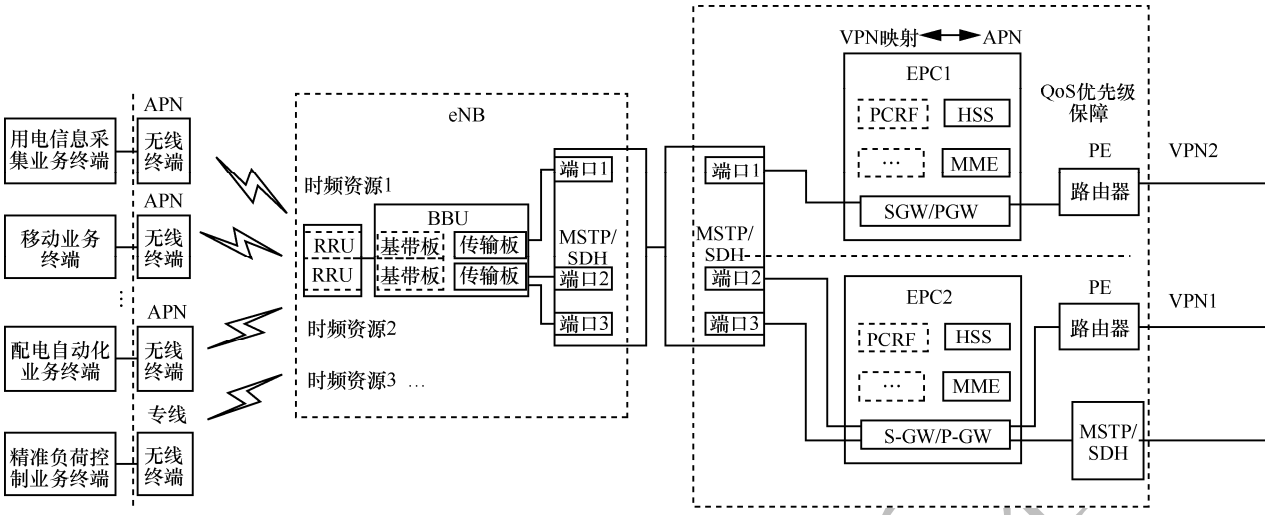


图 2　电力无线专网安全架构

专网安全架构如图 2 所示[6]。

对于内部网络边界，采用安全接入区和电力纵向加密认证措施实现边界隔离和安全防护。对于终端接入的安全性，在无线通信终端和基站之间采用基于四元组鉴权的双向认证方式，实现终端用户与无线网络的双方向的身份认证。

3　应用与实践

3.1　建设情况

基于国网公司“推进电力无线专网扩大试点及业务应用”的要求，在海盐电力无线专网试点建设的基础上，扩大试点规模，建设了嘉兴电力无线专网。嘉兴电力无线专网覆盖嘉兴 A、B、C 3 类供电区域 3 915 km^2，建设范围包括核心网、网管、基站、光缆线路等，能够承载嘉兴 90%的电力业务终端。目前已接入了配电自动化、用电信息采集、配变监测、视频传输等 12 类业务。

3.2　业务接入方案

根据《电力监控系统安全防护规定》“安全分区、网络专用、横向隔离、纵向认证”的原则，生产控制大区和管理信息大区通过双核心网实现物理隔离，两套核心网分别承载生产控制类业务和管理信息类业务。生产控制大区遵循“安全分区、网络专用、横向隔离、纵向认证”原则，采用加密、认证、边界防护等措施进行安全防护，在业务主站部署防火墙，并设置安全接入网关，通过正反向隔离装置接入主站；管理信息大区遵循“双网双机、分区分域”原则，内网边界设置安全接入平台。系统架构如图 3 所示。

3.2.1　配电自动化

配电自动化业务通过无线专网承载，并经过配电自动化主站侧安全接入区接入业务主站。其中，安全接入区包含正反向隔离、采集服务器、电力专用纵向加密认证装置及无线专网采集交换机。如图 3 所示，配电终端与无线通信终端连接，经过空中接口接入基站，基站将数据通过地市传输网回传至核心网，核心网与配电自动化采集交换机相连，以此接入配电自动化业务主站。

3.2.2　用电信息采集

用电信息采集业务通过无线专网承载可实现单表、多表的采集信号传输，如图 3 所示，用电信息采集业务数据通过管理信息大区安全接入平台接入采集主站系统。

3.2.3　配变监测

配变监测是配网掌握线损、变损、负荷率、电能质量等一系列重要运行参数的重要业务，监测配电变压器的运行情况、配电网的整体状况及线路当前运行状况，提升管理效率。配变监测属于采集类业务，其无线专网接入方案与用电信息采集业务类似，通过管理信息大区安全接入平台接入配变监测主站。

3.2.4　视频传输

基于 IP 摄像头和 CPE 通信终端，LTE-230 MHz 电力无线专网可支持视频通信业务，LTE-230 MHz CPE 通信终端可以支持 720P 视频、1080P@H.265 视频。视频业务通过管理信息大区安全接入平台接入视频监控主站。

人民邮电出版社

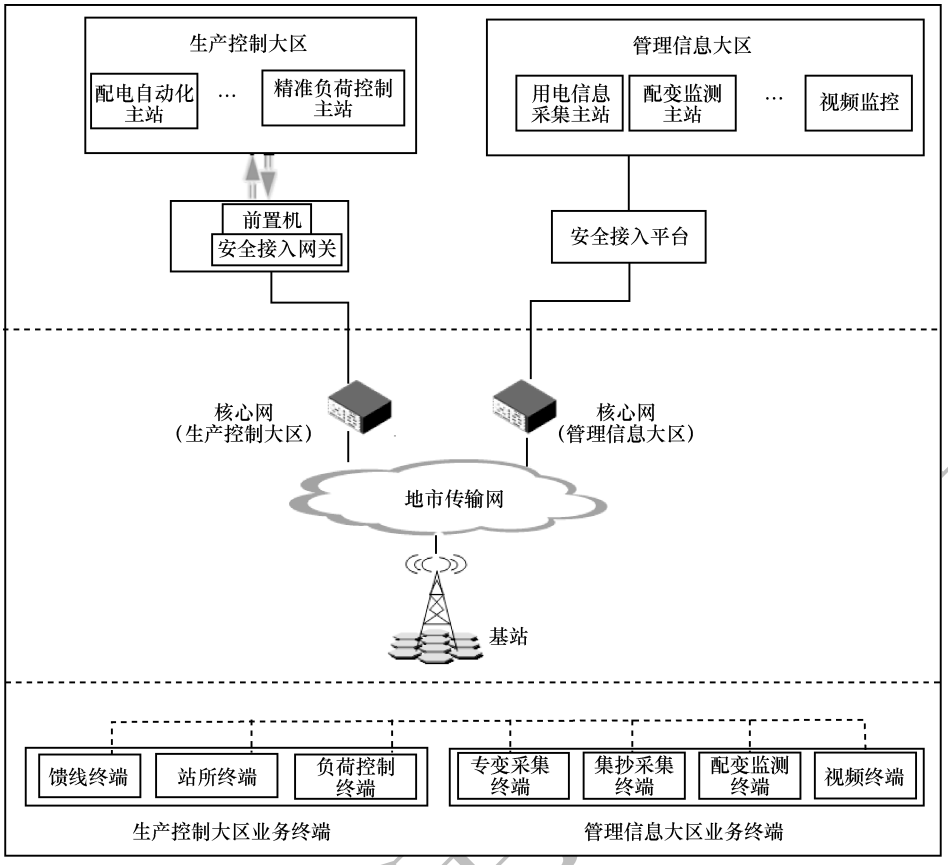


图 3　电力无线专网业务接入方案

4　业务承载性能测试

通过对嘉兴 LTE-230 MHz 电力无线专网开展现网覆盖测试、性能测试和安全测试，验证了 LTE-230 MHz 电力无线专网在覆盖能力、传输能力和安全性方面对于电力业务适用性。

4.1　覆盖测试

通过在规划覆盖区域内遍历测试，统计 RSRP≥−115 且 SINR≥−3 的采样点比例作为覆盖率。

测试结果见表 5，其中覆盖率大于 99%的站点比例为 45.4%，覆盖率 98%～99%站点比例为 36.5%，覆盖率 97%～98%的站点比例为 13.6%，覆盖率 96%～97%的站点比例为 4.5%，所有站点覆盖率均大于 95%。根据《电力无线专网规划设计技术导则》的要求，在 A+、A 类地区规划目标覆盖区域内无线网络总体覆盖率应满足≥−115 dBm 且 RS SINR≥−3 dB 的位置不低于 95%，在 B、C 类地区不低于 90%，因此覆盖率指标满足电力行业需求。

选取位于不同类型覆盖区域的基站进行覆盖范围测试，其覆盖半径与理论值对比见表 6。根据测试结果，LTE-230 MHz 电力无线专网在密集城区最远覆盖半径为 4.1 km，一般城区为 3.7 km，郊区为 7.6 km，基本符合理论覆盖半径，充分验证了 LTE-230 MHz 电力无线专网广覆盖能力。

表 5　站点覆盖率分布

序号	覆盖率	站点比例
1	99%～100%	45.40%
2	98%～99%	36.50%
3	97%～98%	13.60%
4	96%～97%	4.50%

4.2　通信性能测试

开展网络性能测试，包含基本性能测试、时延测试、分组丢失率测试。通过与系统标准要求对比，验证了 LTE-230 MHz 电力无线专网传输能力。

4.2.1　基本性能测试

基本性能测试结果见表 7。LTE-230MHz 电力无

表 6　嘉兴 LTE-230MHz 电力无线专网覆盖半径

覆盖类型	理论覆盖半径/km	最远测试点距离/km	最远测试点对应 RSRP/km
密集城区	3.5	4.1	−109
一般城区	2.7	3.7	−92
郊区	4.18	7.6	−110
农村	7	4.4	−112

表 7　基本性能测试

测试项目	指标	标准要求	结论
接入成功率	100%	≥95%	√
下行速率测试	449.59 kbit/s		√
上行速率测试	1 889.72 kbit/s		√
边缘 RSRP、SINR 测试	边缘 RSRP 均值为−115.25 dBm；边缘 SINR 均值为−3.33 dB	RSRP≤−115 dBm 且 SINR≤−3 dB	√

线专网终端接入成功率为 100%。通过选择 RSRP≥−85 dBm，SINR≥15 dB 的环境进行上行、下行速率测试，测得单个 UE 实测上行速率为 1 889.72 kbit/s，下行速率为 449.59 kbit/s。根据测试结果，小区边缘 RSRP 均值为−115.25 dBm、边缘 SINR 均值为−3.33 dB。

4.2.2　时延和分组丢失率测试

选择在 RSRP 为−90±5 dBm 且 SINR 值为 20±1 dB 的环境下分别测试配电自动化、用电信息采集、精准负荷控制业务数据传输时延和分组丢失率。测试结果见表 8，根据测试结果可知，LTE-230 MHz 电力无线专网满足电力业务传输要求。

4.3　安全性测试

通过对基站以及核心网、网管服务器，通信终端开展安全测试，测试结果如下：

（1）终端认证安全

选取分布式基站进行测试，将合法 USIM 卡插入非法终端中，业务主站无法召测业务终端数据，验证了终端接入的安全性。

（2）渗透测试

现场测试环境部署防火墙无法进行有效攻击。

（3）隔离测试

选取分布式基站进行测试，通过不同板卡和端口实现物理隔离，不同业务主站、终端之间不能互相通信，符合物理隔离和业务隔离要求。

5　结束语

电力无线专网是泛在电力物联网建设的重要一环。嘉兴已建成地市级全覆盖的 LTE-230 MHz 电力无线专网，并承载了用电信息采集、配变监测、配电自动化等业务，有效解决配用电业务信息的可靠、稳定传输问题。通过测试验证了 LTE-230 MHz 电力无线专网的可靠性和安全性，具备电力主要业务承载能力。未来还可以扩展无线专网的移动应用业务，提高泛在电力物联网的管理水平和工作效率。

参考文献：

[1] 闫淑辉, 冯世英. 电力无线专网在配用电自动化中的应用[J]. 电子技术应用, 2015(Z1): 4.

[2] 徐光年. 230MHz 电力无线宽带通信系统的建设与应用[J]. 电力系统通信, 2012, 33(7): 58-62.

[3] 国家无线电管理委员会. 关于印发民用超短波遥测、遥控、数据传输业务频段规划的通知[Z]. 1991.

[4] 工业和信息化部. 工业和信息化部关于调整 223-235MHz 频段无线数据传输系统频率使用规划的通知 [Z]. 2018.

[5] 周浩, 吴国庆, 陆竑, 等. TD-LTE 230 无线专网在嘉兴电力通信的应用 [J]. 浙江电力, 2018, 37(5): 16-21.

表 8　时延和分组丢失率测试

数据类型	平均时延/ms	标准要求[16]/ms	分组丢失率	标准要求	结论
配电自动化	47	6 000	0%	0.01%	√
用电信息采集	88	6 000	0%	0.01%	√
精准负荷控制	39	50	0%	0.01%	√

人民邮电出版社

[6] 国家电网有限公司. 230 MHz 离散多载波电力无线通信系统第 2 部分：LTE-G 230 MHz 技术规范[S]. 2018.

[7] 李金友, 闫磊, 齐欢, 等. 基于 LTE-230 MHz 系统的电力无线通信专网研究与实践 [J]. 电气技术, 2014, 15(1): 132-4.

[8] 易浩勇, 张京娜, 汤琰君. 基于电力无线专网的用电信息采集通信系统 [J]. 电力系统通信, 2013, 34(2): 30-4.

[9] 毛永泉, 周子冠, 宋彦斌, 等. 基于 LTE-230 MHz 无线专网的用电信息采集技术研究 [J]. 供用电, 2015, 32(12): 1-7.

[10] 邵炜平, 陆阳, 李建岐, 等. 面向电力业务接入的跨频段融合与宽窄一体无线专网 [J]. 电信科学, 2018(8): 167-76.

[11] 周建勇, 田志峰, 李艳, 等. 广覆盖 LTE-230 MHz 系统在电力配用电应用中的研究与实践[J]. 电信科学, 2014, 30(3): 168-72.

[12] 韦磊, 耿铨, 过烽, 等. 基于频率隔离的无线专网多业务承载关键技术研究 [J]. 电力信息与通信技术, 2016(11): 87-92.

[13] 徐志强, 马平, 邵炜平, 等. 基于 230 MHz 频段的新型电力无线专网安全性研究 [J]. 电力信息与通信技术, 2016, (1): 74-9.

人民邮电出版社

SPI 通信方式在智能电表安全芯片中的应用

张彦荣
（北京智芯微电子科技有限公司，北京 100083）

摘　要：针对传统 ISO/IEC7816 通信方式在智能电表安全芯片通信中传输效率较低的问题，提出了一种将 SPI 接口应用在智能电表安全芯片中的方法。SPI 是一种同步串行通信方式，相比传统 ISO/IEC 7816 异步半双工的通信方式具有传输效率高、结构简单和传输稳定等优点，尤其是大数据量传输时，基于 SPI 通信方式的智能电表安全芯片其传输速率更具优势。详细分析了 SPI 接口在智能电表安全芯片中实际应用，并且详细描述了一主一从和一主多从的 SPI 通信方式。

关键词：SPI；智能电表安全芯片；ISO/IEC 7816；COS

1　引言

随着智能电网的完善和智能电表的普及，智能安全芯片也被广泛应用在电力行业，智能电表在用户和电网公司之间进行实时的数据交互。为了保证数据传输的安全性和完整性，将智能安全芯片嵌入在智能电表中来实现电表数据的安全存储、数据加解密、身份认证、线路加密传输校验等安全控制功能。

智能安全芯片是指一个支持数据存储、传输、加解密的装置，内部拥有独立的处理器、存储单元、通信接口和算法模块，可以抵御硬件攻击、实现密码运算、密钥的安全存储和使用。它由硬件平台和芯片操作系统两部分构成。其中，硬件平台包括 CPU、协处理器、程序和数据存储器、定时器、随机数发生器、算法模块、通信接口、电压和频率保护机制等。芯片操作系统（chip operating system，COS）是业务流程得以实现的基础。COS 主要功能是控制智能卡和外界的信息交换，管理智能卡内的存储器并在卡内部完成各种命令的处理。其中，与外界进行信息交换是 COS 最基本的要求。

传统的智能电表安全芯片与智能电表的通信方式采用 ISO/IEC7816 的 T=0 协议，此种通信方式的缺点是传输效率低、速度慢。在小数据量传输时，通信速率对接收方和发送方的数据传输效率影响不大，但当大数据量传输时，此缺点尤为明显。

随着智能电表安全芯片功能的增强，对于数据传输量较大时，这种协议将不再适用。针对这些问题，提出了在智能电表安全芯片中应用新型 SPI 通信方式来取代 ISO/IEC7816 的通信方式。SPI 是一种高速、全双工、同步串行的通信方式，具备通信效率高、硬件结构和驱动程序简单及传输稳定等优点。

2　传统智能电表安全芯片的通信方式

传统智能电表安全芯片与智能电表的通信方式采用 ISO/IEC7816 的 T=0 协议，是一种接触式、异步半双工、字符传输的方式。

主要使用 3 条数据线和 1 条控制线，分别是复位线 RST、时钟线 CLK、数据线 I/O。ISO/IEC 7816 DIP 8 封装管脚排布如图 1 所示，其中，VCC 表示电源，GND 表示接地，NC 表示保留。

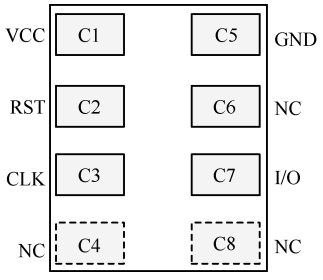


图 1　ISO/IEC 7816 DIP 8 封装管脚排布

此种通信方式的缺点是传输效率低、速度慢。在小数据量传输时，传输速率对接收方和发送方的数据传输效率影响不大，但当大数据量传输时，此缺点尤为明显。

人民邮电出版社

另外，对于智能电表和安全芯片通信时发送和响应都有数据域的情形，T=0 协议不能用一条命令实现，必须分为两步实现，第一步用一条命令为智能芯片提供数据，第二步用另外一条指令来取回数据。这样给芯片编程带来很大麻烦，同时卡片内存必须保留上一次操作需要返回的

数据。若不及时取回，可能会造成敏感信息泄露并产其他安全问题。

将 SPI 通信方式应用在智能电表安全芯片中会解决上述问题，SPI 通信方式传输效率高，而且只用一条命令来实现数据交互，通信安全、操作简单。

3 基于 SPI 的智能安全芯片通信方式

3.1 SPI 介绍

SPI 是 Serial Peripheral Interface 的缩写，即串行外围设备接口，是 Motorola 首先在 MC68HCXX 系列处理器上定义的，主要应用在 EEPROM、FLASH、实时时钟、AD 转换器及 MCU，还有数字信号处理器和数字信号解码器之间等。

它是一种高速、全双工、同步串行的通信方式，并且在芯片的管脚上只占用 4 根线，节约了芯片的管脚，同时为 PCB 的布局上节省空间，提供方便，正是出于这种简单易用的特性，现在越来越多的芯片集成了这种通信协议，比如 AT91RM9200。

SPI 采用主从模式架构，支持多个从设备应用。时钟由主设备控制，数据在时钟脉冲下按位传输，高位在前。

（1）引脚

SPI 共 4 个引脚，包括 2 条数据线、1 条时钟线和 1 条控制线，分别是主设备输出从设备输入线 MOSI、主设备输入从设备输出线 MISO、串行时钟线 SCK、从设备选择线 SSN。

本文中，SPI 通信接口智能电表安全芯片的引脚分配如图 2 所示。

- MOSI：主设备数据输出，从设备数据输入。
- MISO：主设备数据输入，从设备数据输出。
- SCK：时钟信号，由主设备控制发出。
- SSN：从设备选择信号，由主设备控制。根据此信号可以决定能连接到总线上从设备的数量。

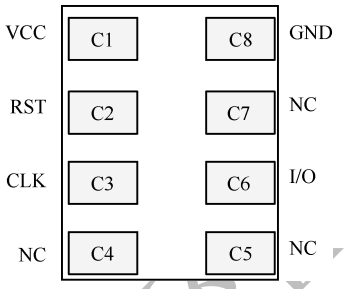


图 2 SPI DIP 8 封装管脚排布

主设备：也称为主机，是指带有 SPI 主模式接口的芯片，能主动控制 SPI 总线动作的机制。

从设备：也称为从机，是指带有 SPI 从模式接口的芯片，不能掌控 SPI 总线的动作而是被动与从芯片进行互动。

（2）工作模式

根据时钟极性（CPOL）及相位（CPHA）不同，SPI 可以组合成 4 种传输时序分别为 SPI0，SPI1，SPI2，SPI3，见表 1。

时钟极性（CPOL）用来决定时钟信号（SCK）空闲时的电平，CPOL = 0 时，空闲电平为低电平；CPOL = 1 时，空闲电平为高电平。

时钟相位（CPHA）用来决定数据的采样时刻，CPHA = 0 时，在每个周期的第一个时钟沿采样；CPHA = 1 时，在每个周期的第二个时钟沿采样。

其中，时序 3 比较常用，即 CPOL = 1、CPHA = 1。

3.2 SPI 在智能电表安全芯片中的应用

智能电表安全芯片的通信接口与存储器、算法模块等是分离的，将传统 ISO/IEC 7816 协议替换为 SPI 接口与其他 SPI 设备进行数据交互。SPI 主设备和从设备只要数据线连接正确，并且具有相同的通信协议，即可进行数据通信。

表 1 SPI 时序

时序	极性（CPOL）	相位（CPHA）	时钟空闲电平	采样沿
时序 0	0	0	低电平	第一个时钟沿
时序 1	0	1	低电平	第二个时钟沿
时序 2	1	0	高电平	第一个时钟沿
时序 3	1	1	高电平	第二个时钟沿

人民邮电出版社

智能电表安全芯片通过 SPI 接口与接口设备连接时，其本身作为从设备，接口设备作为主设备。SPI 不仅支持一主一从还支持一主多从的通信模式。

一个主设备与一个安全芯片的连线示意图如图 3 所示。

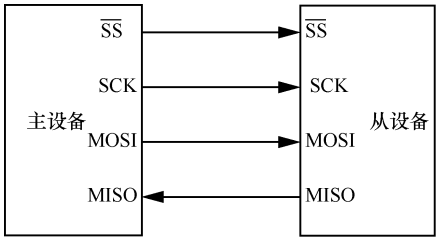


图 3　SPI 主设备和一个从设备连线

一个主设备与多个安全芯片的连线示意图如图 4 所示。

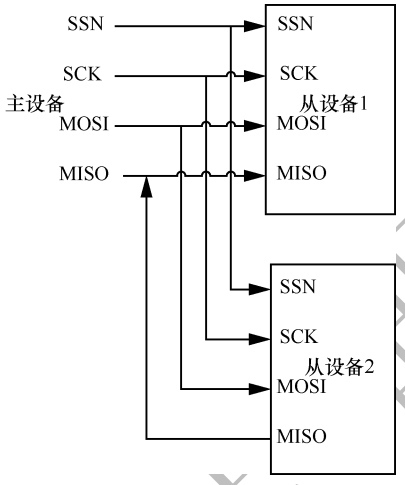


图 4　SPI 主设备和多个从设备连线

除 SPI 数据线连接正确外，SPI 主设备和从设备通信的另一个要素是具备相同的通信协议。一种 SPI 通信协议的流程图如图 5 所示，具体解析如下。

（1）主设备发送请求数据 0x55 CLA INS P1 P2 Len1 Len2 DATA LRC1，其中：

- 55 为发送命令结构的命令头；
- CLA 是命令类别；
- INS 是命令类别中的指令代码；
- P1、P2 是一个完成指令代码的参考符号；
- Len1 Len2 是后续 DATA 的长度，不包含 LRC1，由 2 个字节表示；
- DATA 是由 T-ESAM 来处理的数据输入；
- LRC1 是发送数据的校验值。

（2）智能电表安全芯片发送响应数据 SW1 SW2 Len1 Len2 DATA LRC2，其中：

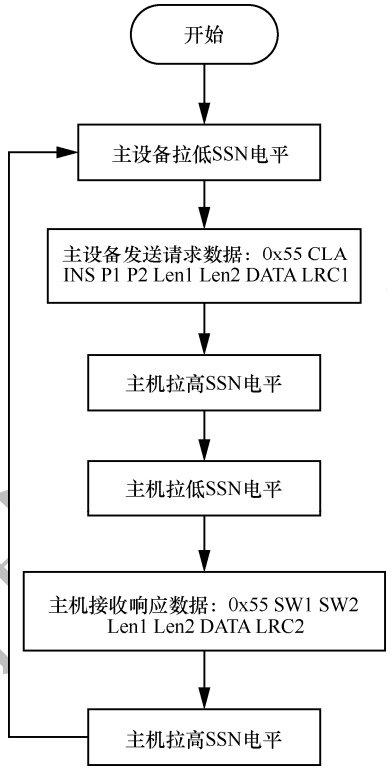


图 5　智能电表安全芯片 SPI 通信协议流程

- SW1 SW2 是指令执行完毕后，从设备返回的状态字；
- Len1 Len2 是后续 DATA 的长度，不包含 LRC2，由 2 个字节表示；
- DATA 是 T-ESAM 处理数据完毕后，返回的输出数据；
- LRC2 是接收数据的校验值；

经过测试，以上通信协议的数据传输速率为 3.8 Mbit/s，并可以稳定通信，极大满足了实际智能电表安全芯片的通信要求。

3.3　与传统通信模式优势比较

基于 SPI 的智能电表安全芯片与采用传统 ISO/IEC 7816 T=0 的协议的智能电表安全芯片相比，具备以下优势。

（1）相对抗干扰能力强，传输稳定。

（2）只用一条命令来实现数据交互，通信简单更为安全可靠。

（3）高效的传输速率，具体如下：

- ISO/IEC7816 缺省通信模式下，有效数据的传输速率为 9.6 Kbit/s，一般最高可达 100 Kbit/s；
- SPI 当其稳定通信时钟为 5 MHz，字节间隔为 500 ns 的情形下，有效数据传输速率可达到 3.8 Mbit/s，当时钟 CLK 为 10 MHz 的情形下，传输速率会更快；
- 对比得出，SPI 通信模式下有效数据的传输速率是传统 ISO/IEC 7816 T=0 通信模式下传输速率的 30 倍左右。

由以上可以看出，将 SPI 通信模式应用在智能电表安全芯片中具有更高的安全性与适用性。

4 结束语

通过 SPI 接口在智能电表安全芯片上的应用，使得智能电表安全芯片的传输速率比传统 ISO/IEC 7816 T=0 通信模式下的传输速率有了极大的提高，有效改变了智能电表大数据量传输耗时长的现状。经过严密测试，SPI 通信方式应用在智能电表安全芯片上是可行的，能够大规模使用。SPI 因其硬件结构和驱动程序简单、通信效率高、连线简单及传输稳定等诸多优点，其应用会越来越广泛，并取代传统的通信方式。

参考文献：

[1] 王爱英. 智能卡技术[M]. 北京: 清华大学出版社, 2009.
[2] 韦小刚, 黄益彬, 杨维永. 智能电网终端安全芯片中 COS 系统的设计[C]// 中国电机程学会年会. 2011.
[3] Freescale Semiconductor. SPI Block Guide V04.01[EB]. 2004.
[4] ISO/IEC 7816-2. Information technology-Identification cards-Integrated circuit(s) cards with contacts[S]. 1999.
[5] ISO/IEC 7816-3. Identification cards-Integrated circuit cards[S]. 2006.
[6] ISO/IEC 7816-4. Identification cards-Integrated circuit cards[S]. 2005.

人民邮电出版社

TD-LTE230 电力无线专网研究与应用

齐悦言，孔祥余
（北京中电飞华通信股份有限公司，北京 100071）

摘　要：随着全球能源互联网与智能电网的快速发展，“互联网＋”、大数据、云计算、物联网等新技术开始应用，各种业务终端不断增加，单一依靠 EPON 等有线通信方式已经不能满足快速增长的业务对终端通信接入网的要求，这对电力终端通信接入网的支撑提出越来越高的要求。无线通信作为电力终端通信接入网的主要技术手段之一，对于提高电力终端通信接入网覆盖面积、通信质量都起到非常重要的作用。首先深入分析研究了电力业务的应用需求、电力无线业务种类，业务特点及对通信技术要求。其次，对电力 230 MHz 频谱资源与政策、电力无线专网技术发展方向进行了分析，同时对 TD-LTE 230 电力无线专网的概念以及应用现状进行了深入剖析。详细阐述了 OFDM、HARQ、频率聚合、动态资源分配、干扰协调、全 IP 等 TD-LTE 230 关键技术。最后，结合智能电网业务应用需求对 TD-LTE 230 电力无线专网网络架构、安全防护、技术参数、支持的业务类型进行了详细的阐述。

关键词：TD-LTE230；智能电网；电力无线专网；电力业务应用；关键技术

1　引言

随着全球能源互联网与智能电网的快速发展,“互联网＋”、大数据、云计算、物联网等新技术开始应用，无线通信作为电力终端通信接入网的主要技术手段之一，对于提高电力终端通信接入网覆盖面积、通信质量都起到非常重要的作用[1]。

“十二五”至今，依托配电自动化、用电信息采集等项目建设，初步形成了以光纤网络为主，无线公网、宽带载波、无线专网等多种技术体制为补充的电力终端通信接入网。“十三五”期间，国家将进一步加大配电网建设改造力度,配电自动化覆盖率将在 2020 年达到 90%。结合电网发展的新形势，应当全面提升电力终端通信接入网对生产运行、经营管理等业务的支撑服务水平,而电力无线专网作为光纤网络的有力补充，也将有更大的发展。

TD-LTE230 电力无线通信系统部署灵活安全，可解决有线通信网络建设与部署中存在的接入层情况复杂、地理环境、施工条件、功能需求、资金投入等多方面的困难和问题。通过研究 TD-LTE230 无线通信技术，实现 TD-LTE230 电力无线专网网络与光纤有线通信网络的相互补充、互为备份，有助于提高传输通道安全可靠性，满足智能电网与全球能源互联网现有业务、未来扩展业务的应用。有效扩大无线网络的覆盖范围，缩小覆盖盲区、增强网络可扩展性。满足配电自动化、用电信息采集、语音集群、视频监控业务以及分布式电源、移动充电桩（站）等新业务的承载，保障电网安全稳定运行、支撑企业高效运营、服务产业融合创新,有利于提升电力行业的服务水平。

2　TD-LTE230 电力应用需求

2.1　电力无线业务应用分析

近年来，随着无线通信技术和智能电网的快速发展，电力业务种类和终端数量也有较大的增长，截至 2015 年年底，国网公司共计有 1 225 万个业务终端，主要有配电自动化、用电信息采集、电动充电站、充电桩四大类基本业务。从电力专业来看，电力无线通信业务主要集中在营销、运行检修、物资、生产基建等环节，见表 1。

营销环节最主要的应用是用电信息采集。截至 2015 年年底，国家电网公司已经部署用电信息采集系统接入的集中器（含专变采集终端）约 1 200 万个，覆盖智能电表超过 2 亿只。其中，98%以上的集中器采用了运营商的 GPRS、CDMA 无线网络接入，可见租用运营商提供的 GPRS、CDMA 业务作为用电信息采集等业务的主要无线通信手段。

运行检修无线业务种类最多，终端类型多样化，主要有在线监测、移动巡检、移动作业、应急抢修等。截至

人民邮电出版社

表 1　电力无线业务[2]

分类	应用业务	终端类型
营销	用电信息采集、负荷管理、配电自动化、移动缴费	集中器、负荷控制终端、专变终端、电力 POS 缴费（售电）移动终端等
运行检修	生产管理、移动作业与检修、电能质量在线监测、电力线路移动巡检、配电自动化系统、输变电在线监测、配网终端数据采集、应急抢修现场作业、车载 GPS 监控管理等	PDA、笔记本、手持终端、数据采集装置、电能质量检测终端、输电线路在线监测装置等
物资管理	仓库管理、物资管理、现场收发货管理、物资调配等	PDA
基建	生产管理信息系统、工程指挥、基建项目管理、移动监控、基建管理信息等	集中器、笔记本电脑，平板电脑、无线终端

2015 年年底，配电自动化终端达到 21.2 万个，光纤覆盖占 16.6%，无线公网占 82%，载波占 1%，无线专网占 0.4%。

基建环节采用移动终端采集现场的图片、数据和视频，实现远程工程指挥。此外，移动办公的需求也日渐强烈。

2.2　电力无线业务应用需求

智能电网无线业务需要具备双向性、实时性、可靠性、安全性等特征。电力无线专网应该能承载智能电网现有业务和未来扩展业务，如配电自动化、用电信息采集、电动充电站、充电桩等基本业务，移动作业、移动巡检、视频监控、应急抢修等扩展业务，同时需要组网灵活、便于施工、专网专用、高可靠性、高安全性、扩容升级便利、多业务承载等特点。表 2 将电力无线业务从数据流量、QoS、安全性、移动性、终端数量几个方面进行分析。

3　TD-LTE230 电力无线专网简介

3.1　230 MHz 频谱分析

3.1.1　频率政策

国家无线电管理委员会发布的《关于印发民用超短波遥测、遥控、数据传输业务频段规划的通知》[3]（国无管[1991] 5 号）中规定，将 223～235 MHz 作为遥测、遥控、数据传输等业务使用的频段。该频谱资源被划分为 480 个 25 kHz 的离散频点，分配给能源、军队、气象、地震、水利、地矿、轻工、建设等行业使用。其中，电力行业拥有 40 个授权频点[4]，共计 1 MHz。为进一步提升频段的使用效率，工业和信息化部于 2018 年 8 月 31 日又出台了《工业和信息化部关于调整 223～235 MHz 频段无线数据传输系统频率使用规划的通知》[5]（工信部无 2018 165 号），鼓励相关行业部门采用共网模式使用 223～226 MHz 和 229～233 MHz 频段。建网单位应按照公平合理负担和节约资源的原则，为共网部门、单位提供可靠、高质量的业务和应用服务，并确保部署的无线电数据传输系统安全运行和高效应用。因此，TD-LTE230 系统利用其在频率使用政策上的优势在电力行业得到广泛应用。

3.1.2　技术发展方向

现有的电力无线专网主要有 TD-LTE230、TD-LTE1800、230 数传电台 3 种主要技术体制。

230 数传电台覆盖能力与 TD-LTE230 虽然基本相当，但是数传电台数据无线传输网络独占一个频率资源，在同一频点（25 kHz）上同时只能有一个设备发

表 2　电力无线业务需求分析

典型业务	数据流量	QoS	安全	移动性要求	终端数量
用电信息采集	上行流量小；下行流量几乎没有	较高	较高	低	众多
负荷控制	上行流量几乎没有；下行流量小	高	高	低	少
配电自动化	上行流量小；下行流量小	高	高	低	多
电动充电站	上行流量小；下行流量小	较高	较高	低	众多
充电桩	上行流量小；下行流量小	低	较高	低	少
移动作业	上行流量大；下行流量几乎没有	较高	较高	高	少
移动巡检	上行流量较大；下行流量小	较高	较高	高	少
视频监控	上行流量大；下行流量几乎没有	低	较高	低	少
应急抢修	上行流量大；下行流量小	较高	较高	高	少

人民邮电出版社

送数据，采用一个中心对远端多点的通信分配方式，采用轮询方式进行数据传输。由于数传电台技术的传输速率低（最高 19.2 kbit/s）、频谱利用率低等先天缺陷，不能满足智能电网发展所需的大带宽、高速率的业务需要[6]，近年来已经逐渐被 TD-LTE 技术所取代。

TD-LTE1800 工作频段为 1 800 MHz，虽然数据传输能力较强，但覆盖半径仅为 TD-LTE230 的 1/3～1/5，因此在建网、运维成本方面也不占优势，且 1 800 MHz 频段目前批复权在各省无线电管理局，各行业纷纷抢占频谱资源，频率申请困难，因此 TD-LTE230 已经逐渐成为电力无线专网主力技术[7-8]。

3.2 TD-LTE230 电力无线专网

3.2.1 TD-LTE230 电力无线通信系统简介[9]

TD-LTE 是 3G 标准 TD-SCDMA 的长期演进版本，由 3GPP 组织涵盖的全球各大企业及运营商共同制定，采用 OFDM、MIMO 等技术，使系统性能上有很大提升。

TD-LTE230 系统是基于 230 MHz 频段的无线频谱，利用 TD-LTE 先进无线通信技术、采用国际通用的 LTE 标准，采用了 OFDM、频域多址、HARQ、载波聚合、动态资源分配、干扰抑制、全 IP 等关键技术，为电力行业用户开发的电力无线通信系统，该系统具有覆盖广、海量用户、高可靠性、实时性强、安全性强、频谱适应性强等特点，可实现数据、语音、视频的双向传输[9]。

3.2.2 TD-LTE230 电力无线专网简介

TD-LTE230 电力无线专网是指利用 TD-LTE230 电力无线通信系统建设的电力终端接入网络，该网络具有广域覆盖、绕射能力强、布网灵活、扩容升级便利、专网专用、安全可靠等优点。

3.2.3 TD-LTE230 电力无线专网应用现状

自 2010 年以来，国家电网公司先后在浙江海盐、河北平山、内蒙巴林左旗、河北大厂、湖南京山、重庆武隆、江苏昆山、福建晋江等地市县开展试点验证工作，主要用于用电信息采集、配电自动化、负荷控制、配变监测、集群通信等业务。

经过多年的试点验证、技术提升和经验积累，TD-LTE230 电力无线专网运行稳定可靠、专网专用、安全可靠，能够大幅提升电力各种业务运行指标。“十三五”期间，国家电网公司将在其供电服务区域内开展 TD-LTE230 电力无线专网推广建设。

4 TD-LTE230 电力无线专网关键技术

4.1 频域多址技术

频域多址技术，即正交频分复用技术（orthogonal frequency division multiplexing，OFDM）[10]，具有复杂度低、应用广泛的多载波传输特点。在现有信息传输通信系统中，业务量日益增多，传输信号带宽势必会提升，码分多址（code division multiple access，CDMA）技术性能将因多径因素的影响而受到一定限制，而 OFDMA（orthogonal frequency division multiple access，正交频分多址）信号保持正交特性不变，因此使用 OFDMA 可以更好的设计应对增加带宽的需求。OFDMA 采用扁平化结构设计，分组调度在其基站实现时，可以采用快速调度、包含频域调度的办法来增加网络带宽。频域调度可通过 OFDMA 实现，而 CDMA 无法实现。另外，为了实现上行功放的需求，SC-FDMA 比 OFDMA 能够获得更低的峰均比，大大提高了终端利用上行功放的效率，下行多址技术系统如图 1 所示。

OFDMA 与普通的 FDMA、TDMA、CDMA 相比具有频谱效率高、抗频率选择性衰落的能力比较强、通过频域均衡可以实现低复杂度的接收机等优点，是 4G 的主要调制方式。

4.2 HARQ 技术

由于信息在发送端经过信道传输到接收端的过称中，容易数据丢失而导致信息的不吻合，务必需要重

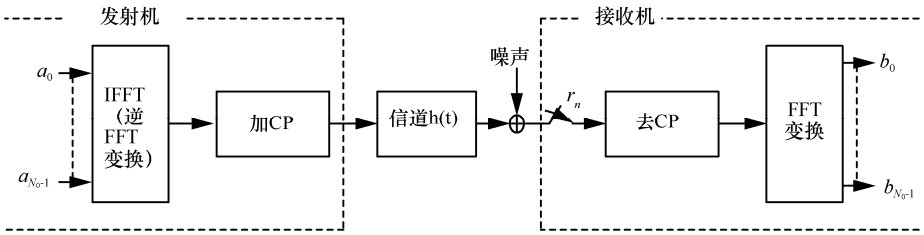


图 1 OFDM 系统框图

传至所有的信息都接收完整为止。混合自动重传请求（hybrid automatic repeat request，HARQ）[11]指的是将需要发送的物理层信息数据按照约定协议组合成协议帧，编码形成可替代性很强的 4 个数据子分组。基站一次仅仅发送一个数据信息子分组，接收端只要收到数据信息子分组立刻进行译码。当破解重组成功，则立刻向基站返回一个确认应答信号；当破解重组失败，则立刻向基站返回一个失败应答信号，此时基站响应接着发送数据子分组，直到接收端解析出正确的数据分组为止。

由于信号从移动台到基站的物理通道很不简单，因此 LTE 上行链路系统使用同步非自适应的 HARQ 技术[11]来设计，还有其他设备系统辐射的随机性干扰源的影响，从而基站不能很好的预测各个接入设备的信干比（SINR）值，接下来重点分析下行信道采用的异步自适应的 HARQ，下行 HARQ 时序如图 2 所示。

下行传输发送端使用 PDSCH 来调度，PDSCH 相应的 ACK 或者 NACK 在 PUCCH 或者 PUSCH 上发送；下行传输接收端通过 PDCCH 来调度。TX 代表发送端，RX 代表接收端，一般情况下在数据传输之前，常使用跟踪等方法来整合所有的数据。如果需要传输的数据量过大时，要增加一个递增冗余为了降低重传时流量的消耗，仅仅再上传没有收到的数据。

4.3 载波聚合技术

随着无线技术的大量应用，连续频谱越来越难以得到，这为大带宽无线传输带来了困难，3GPP 载波聚合技术[12-13]的提出为解决这一问题奠定了基础。载波聚合技术是指某一个 UE 通过基站的调度，为其分配多个离散的载波，用于信息的传输。3GPP 提出的载波聚合技术，可以根据不同的用户需求和网络规划，将现有的 LTE 的多个不同的分量载波（component carrier，CC）整合使用，能够灵活地将频谱带宽扩展到 LTE-advanced 所要求的最多 100 MHz 的带宽。

模拟数传电台技术，无线信道分配的带宽通常比较窄，而且相邻信道之间还要保留一定的间隔。与大带宽连续频谱分配相比，这种离散的窄带频谱很难进行高速率大带宽数据传输。而面对日益增长的电力业务高速无线通信的需求，必须对这种频谱进行整合，从而提高传输速率。而在现阶段，模拟电台大量存在的情况下，很难对已分配的频谱资源进行重新划分，只能考虑通过某种处理方法来实现频谱合并的效果，载波聚合技术是其理想的选择。

载波聚合技术非常适合解决离散频谱的高速传输问题，非常适合应用到 TD-LTE230 系统中来以提高数据传输。而且载波聚合技术的引入可以根据用户的不同需求为其分配不同的带宽，提高频率的利用效率，增加用户的上、下行数据传输速率，减少传输时延，增强用户的体验。具体来说，可以将不同离散的窄带频点看作是不同的成员载波，利用载波聚合技术将这些离散的窄带频点进行聚合。

4.4 动态资源分配技术

TD-LTE230 系统采用正交频分多址技术，无线资源可以灵活地在频域上划分为多个子带（一个子带由多个子载波构成），再从时域上划分为多个时隙，这样构成的时频二维无线资源有利于根据用户的信道状况、数据量大小、时延要求、QoS 等级等因素进行动态调度，以实现频率分集。

TD-LTE230 系统小区内的用户之间的资源使用是

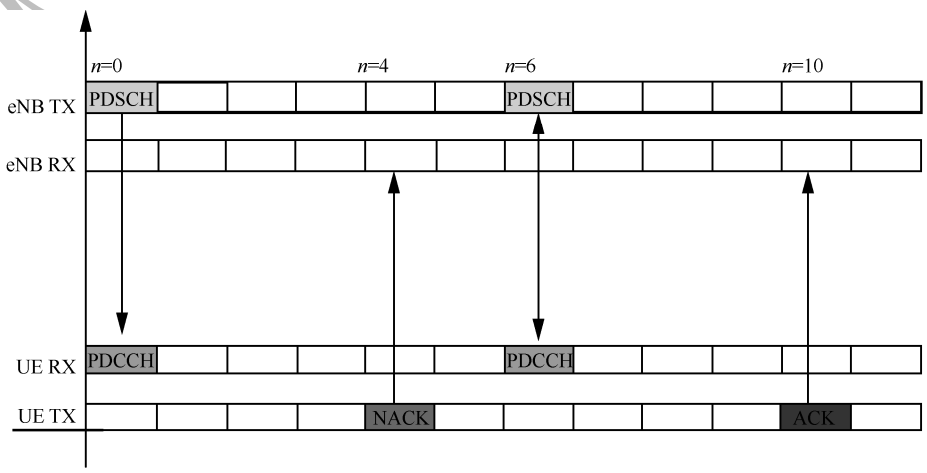


图 2　下行 HARQ 时序

完全正交的，因此小区内用户之间没有干扰。除了时频无线资源的分配，TD-LTE230 系统还通过动态功率分配降低小区间用户同频资源干扰，进一步提高系统性能。

4.5 干扰抑制技术

为了提高传输速率引进载波聚合技术虽然可以增加系统以及终端的吞吐量，但是由于离散的子带间的空隙并不是完全干净的，可能存在其他干扰信号，甚至可能这种干扰非常大。如果接发射机和接收机采用相同的结构，则很有可能造成 AD 饱和甚至烧毁[7]。

为了解决上述问题，就是对电力的 40 个子带分别接收，用 40 个模拟电路去接收 40 个子带，每个子带在中频做 25 kHz 的模拟滤波，这样便可以完全将高功率的干扰信号滤除。

4.6 全 IP 技术

TD-LTE230 系统采用全 IP 网络架构，如图 3 所示。

全 IP 网络架构是系统不仅能够适用现有业务的承载，而且方便将来新业务的扩展应用。

5 TD-LTE230 电力无线专网在智能电网中的应用

5.1 TD-LTE230 电力无线专网网络架构[14]

TD-LTE230 电力无线通信专网的作用就是在远端监控模块与后台主站之间提供安全、可靠的数据传输通道，并提供对网络设备和远端通信模块的配置和管理功能。TD-LTE230 电力无线通信专网采用全 IP 网络构建，组网灵活，TD-LTE230 电力无线专网通信系统由核心网 EPC、基站、网管中心、终端四大部分组成，其网络架构如图 4 所示。

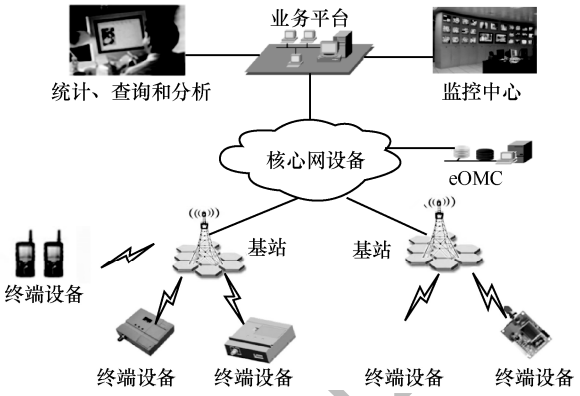


图 4 TD-LTE230 网络架构

5.1.1 核心网 EPC

TD-LTE230 电力无线通信专网基础网络由演进型无线接入网络（E-UTRAN）和演进型核心网络（EPC230）构成。在 3GPP 的体系架构中，演进后的系统仅存在分组交换域。每个 eNode B 和 EPC230 通过 S1 接口连接，S1 接口在 EPC230 内部的用户面和控制面均终止在 EPC 上，控制面和用户面的另一端终止在 eNode B 上。

TD-LTE230 的核心网 EPC 逻辑功能模块包括为移动管理实体（mobile management entity，MME）和 Serving-Gataway 等构成。其中 MME 负责网络的漫游管理，提供与其他通信网络的接口（如 GPRS）。Serving-Gataway 提供对应用业务平台的接口，可以与数据采集主站之间进行数据交互， TD-LTE230 核心网逻辑实体如图 5 所示。

5.1.2 基站

基站（eNode B）由 BBU 和 RRU 两部分构成，为光纤拉远基站。作为 TD-LTE230 接入网中仅有的一个节点类型，设计的思想就是尽量简化网络结构，

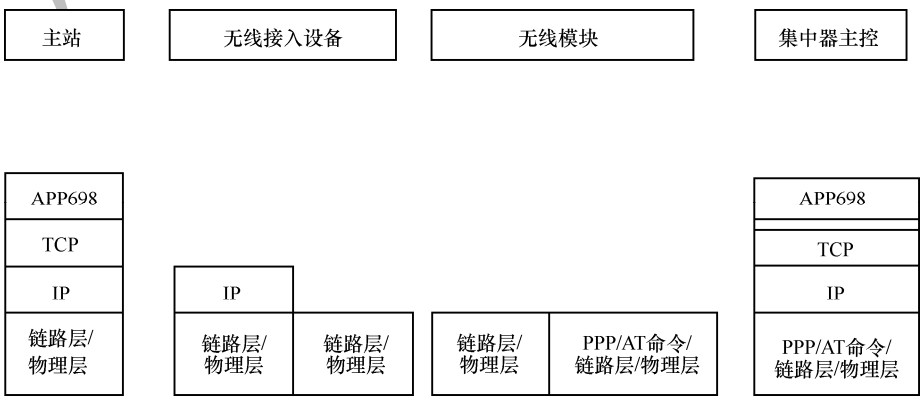


图 3 全 IP 技术架构

人民邮电出版社

便于无线网络的规划和应用。

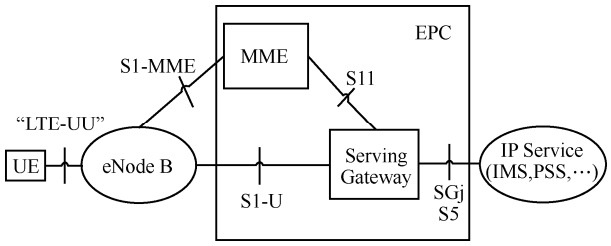


图 5　TD-LTE230 核心网逻辑实体

eBBU230 是一种针对 230 MHz 频段开展宽带无线传输的设备，系统容量大、频谱利用率高。eBBU230 是宽带无线接入通信系统的重要组成单元，eBBU230 采用了 OFDM、载波聚合、AMC 等关键技术，可以满足用户对于覆盖和容量的双重要求。

eBBU230 是根据宽带无线接入通信系统协议研发的 eNode B230 分布式基站基带单元设备，简称 eBBU230。eRRU230 是 eNode B 分布式基站射频远端设备。其中 eRRU230 通过 Ir 接口与 eBBU230 相连，eBBU230 与 eRRU230 共同配合实现一个完整的 eNode B 逻辑功能。eBBU230 产品与 eRRU230 设备配合工作。

eBBU230 支持数据采集、负荷控制、视频传输等多种业务，单机柜最大可支持 6 载扇。eBBU230 与 eRRU230 通过光纤连接，组网灵活，可以为运营商提供低成本、广覆盖的建网解决方案。eBBU230 具有架构先进、可靠性高、安装方便等特点，适合对城市、农村进行广覆盖。

5.1.3　网管中心

为了提高在电网中的应用网络运维效率，最大程度地降低网络运营维护成本，网管系统是基于智能综合网管平台技术，采用组件式扩展应用研发，具备有配置管理、故障管理、性能管理、日志、安全及其扩展功能，网管系统整体架构如图 6 所示。

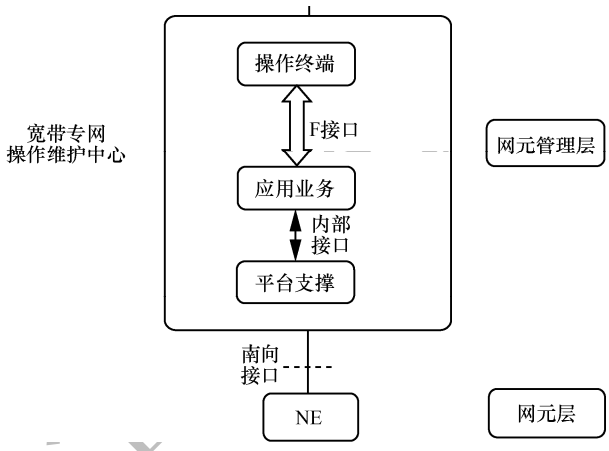


图 6　网管系统整体架构

整个系统基于分布式架构设计，具有高扩展性、高安全性、高可靠性和良好的跨平台性，操作便捷，依据网络规模可以灵活部署和扩裁，同时，遵循国际、国内通信网管标准，兼容行业通行的协议接口，如 SNMP、FTP 等，便于与第三方系统对接融合，其物理部署示意图如图 7 所示。

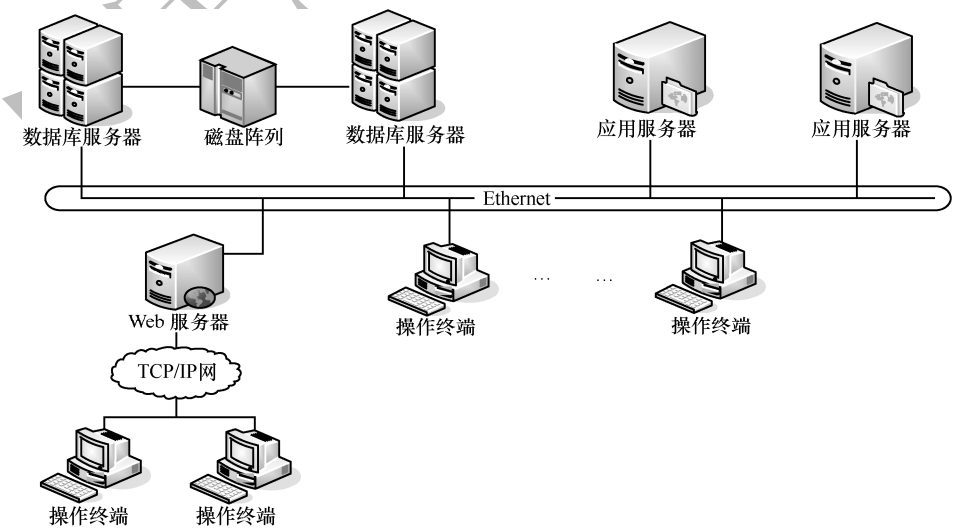


图 7　网管系统物理部署

5.1.4 终端

TD-LTE230 系统终端有两种产品形态，分别是客户终端设备（customer premise equipment，CPE）、远程通信模块（嵌入式）。CPE 为通用通信设备，拥有标准网口，可与计算机或其他设备终端连接等设备连接。远程通信模块主要对接集中器、故障指示器等业务终端，采集数据并且上传到主站。

CPE 是一种针对 230 MHz 频段开发的多子带无线接入通信系统终端设备，数据传输高速稳定、频谱利用率高，该产品物理层采用了 OFDM、载波聚合、AMC 等关键技术，协议标准采用 LTE230 协议规范，可以满足各行业通信系统中数据传输、负荷控制、视频传输的实时性、高效性、稳定性和可靠性。CPE 在 LTE230 无线通信系统中的位置如图 8 所示。

5.2 TD-LTE230 电力无线专网安全防护[15-18]

TD-LTE230 系统为用户提供鉴权、空口保密等安全技术，满足无线通信系统安全传输的需要，同时系统支持用户端到端密码设备，保障用电信息的端到端加密传输。

TD-LTE230 系统的认证体制是用户终端和通信网络之间的双向认证，采用扩展的 UMTS AKA 可信协议信令流程，通过存储在用户终端和归属网中的鉴权中心的唯一的秘密密钥 *K* 来认证，同时采用一种序列号机制，保证认证密钥的“一次一密”，支持 128 bit 的认证密钥，杜绝了类似 GSM 的 SIM 卡被破解和复制情况的发生。基于 IP 地址与内容的过滤、基于电力规约的安全过滤、完全私有协议规避攻击，TD-LTE230 系统安全构架如图 9 所示。

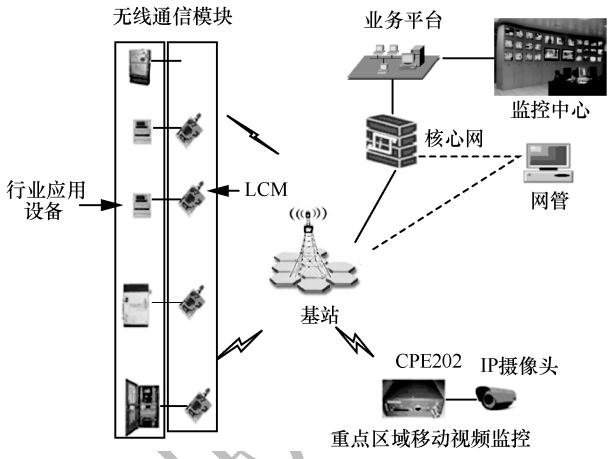


图 8 CPE 在 LTE230 宽带无线通信系统中的位置

5.3 TD-LTE230 电力无线专网通信系统技术参数

TD-LTE230 电力无线专网通信系统采用电力行业专用的 40 个离散频点，工作于 223～235MHz 频段，采用 OFDMA、频谱聚合、频谱感知等技术，具体技术参数见表 3。

5.4 TD-LTE230 电力无线专网支持业务类型

TD-LTE230 电力无线专网面向智能电网通信网的应用，主要支撑配用电侧的用电信息采集、配网自动化、负荷管理、应急抢修、移动巡检与检修、移动作业、数字集群及移动资产可视化管理、智能用电服务以及电力物联网的其他业务。

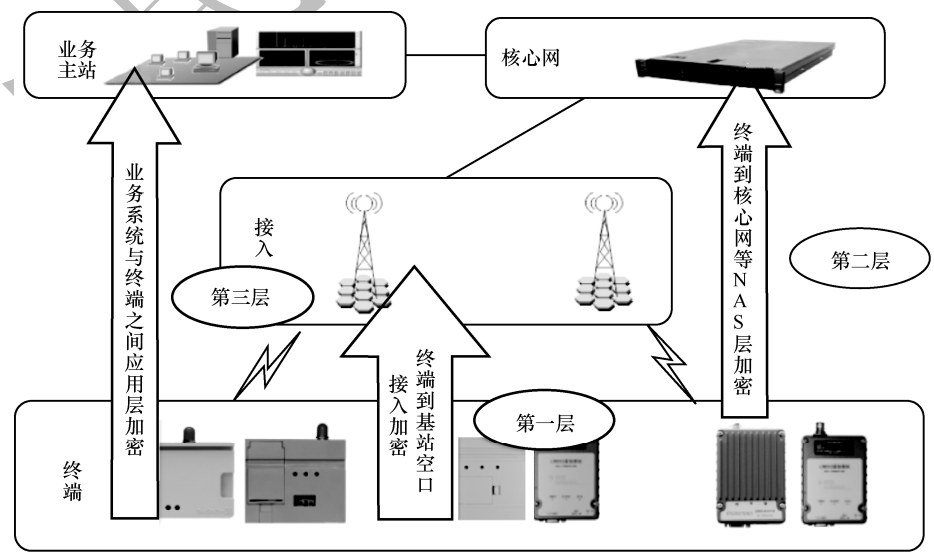


图 9 TD-LTE230 系统安全构架

表 3　TD-LTE230 系统技术参数

TD-LTE230 系统技术指标	
工作频段/MHz	223.025～235.000
多址方式	OFDM 多址方式
双工方式	TDD 双工方式
调制方式	QPSK、16QAM 和 64QAM
基站系统射频信道带宽	离散 8.5 MHz
单小区吞吐量	上行峰值速率 14.96 Mbit/s， 下行峰值速率 7 Mbit/s
单小区支持在线用户数	2 000/MHz
终端峰值速率	上行峰值速率 1.76 Mbit/s, 下行峰值速率 0.7 Mbit/s
覆盖半径	密集城区 3 km，郊区 10 km，农村 30 km
接收灵敏度	−120 dBm

6　结束语

随着计算机应用、通信、传感、嵌入式、大数据、云计算等技术的日益发展和成熟，逐渐地被应用到生产生活中去，很大程度地改善了我国传统工业设备的水准，显著提高了设备自动化数字化生产运行层次。针对我国电力工业设备与管理水平的现况，提出了 TD-LTE230 电力无线专网研究与应用的研究目标，对电力业务的应用需求、TD-LTE230 电力无线专网、关键技术支撑业务等进行了研究分析，本文从系统网络架构、智能电网电力业务应用、TD-LTE230 系统 3 个方面加以详细阐述，以解决如今存在的各种问题。

我国电力无线专网的研究起步相对比较晚，但是随着新兴技术的突飞猛进，最近几年发展的十分迅速。互联网和传统工业的有机融合，必然引起工业自动化发展的大潮，加快数传电台等传统制造业升级换代的步伐，提高电力系统生产生活智能化信息化环保化的进程，进而增强中国制造向中国创造的驱动转型能力。

参考文献：

[1] 孙圣武, 程远. 面向业务覆盖的 LTE 电力无线专网研究[J]. 电力信息与通信技术, 2015, 13(4): 6-10.

[2] 王一蓉, 佟大力, 邓伟. 电力无线虚拟专网应用分析及网络设计[J]. 电力信息与通信技术, 2013, 11(12): 49-53.

[3] 国家无线电管理委员会. 关于印发民用超短波遥测、遥控、数据传输业务频段规划的通知(国无管[1991]5 号)[EB]. 1991.

[4] 国家无线电管理委员会. 工业和信息化部关于同意国家电网公司使用电力负荷监控系统频率的批复[EB]. 2013.

[5] 工业和信息化部. 工业和信息化部关于调整 223~235 MHz 频段无线数据传输系统频率使用规划的通知(工信部无[2018] 165 号) [EB]. 2018.

[6] 陈靓. 基于 230 MHz 宽带数传系统干扰共存研究[D]. 北京: 北京交通大学, 2016.

[7] 于佳, 马平, 刘锐, 等. 电力无线专网业务支撑能力研究[J]. 广东电力, 2018, 31(12): 49-56.

[8] 李金友, 闫磊, 齐欢, 等. 基于 230 系统的电力无线通信专网研究与实践[J]. 电气技术, 2014(1): 132-134.

[9] 周浩, 吴国庆, 陆竑, 等. TD-LTE230 无线专网在嘉兴电力通信的应用[J]. 浙江电力, 2018, 37(5): 16-21.

[10] 吕卓. 宽带无线通信中 OFDM 关键技术的研究[D]. 西安: 西安电子科技大学, 2005.

[11] LU J, WU C K, XIAO S, et al. A network coding based hybrid ARQ algorithm for wireless video broadcast[J]. Science China(Information Sciences), 2011.

[12] 马晓勇. 230 MHz 频段使用载波聚合技术在县域配电网数据监控及配电自动化的应用与分析[J]. 通讯世界, 2017(21): 129-130.

[13] 徐光年, 王奇褚, 褚建新, 等. 载波聚合技术在电力无线通信系统中的应用[J]. 电气应用, 2016(S2): 718-721.

[14] 张瀚峰, 闫淑辉, 冯世英. LTE230 系统在智能电网中的应用[J]. 电信网技术, 2015 (1): 22-25.

[15] 刘功杰. TD-LTE 技术在电力无线通信系统中的应用分析[J]. 通讯世界, 2017(21): 208-209.

[16] 朱凌廷, 何剑, 黄爽. 电力无线专网信息安全思考与建议[J]. 中国新通信, 2018, 2018(13): 127.

[17] 杨艳辉. 浅析电力企业网络信息安全管理[J]. 工程建设与设计, 2016(14): 170-171.

[18] 张恩超. 智能电网信息安全防御体系架构与关键技术研究[D]. 北京: 华北电力大学, 2016.

人民邮电出版社

大数据在电力行业的应用

任惠姣 [1,2]

（1. 北京航空航天大学，北京 100191;
2. 北京中电飞华通信股份有限公司，北京 100070）

摘　要：随着时代的发展变化，科技的进步日新月异，大数据也越来越广泛地应用于人们的生产生活中。依托互联网，大数据给很多行业的发展提供了便利。对于电力行业来说，大数据的应用给这个传统行业的发展提供了新的动力。但是对于大数据在电力行业的使用，也存在着一定的风险。如何更好地规避风险，使大数据在电力行业的应用变得更加的高效，也是需要不断探索的。重点论述了大数据的特点优势及其在电力行业中的具体应用，并且在此基础上，针对大数据目前在电力行业的应用现状提出了相应的发展建议。

关键词：大数据；电力；互联网

1　引言

电力行业是我国非常重要的一个行业，它与人们的生活息息相关。电力行业的发展离不开对出现问题的不断改进和完善，所以如何更好地收集信息从而更好地了解当前我国电力行业的发展现状十分关键。目前我们国家的电网建设在不断地完善，但是在这个过程中由于信息匮乏造成了一些问题，针对这个情况，大数据可以更好地搜集整理相关的数据，为电力行业的发展提供相应的数据支撑。针对电力行业的大数据收集，称之为电力大数据。电力大数据的应用很好地顺应了时代的发展潮流。但目前来看，大数据在电力行业的应用既是机遇，又是挑战。如何将大数据更好地应用于电力行业，使其促进电力行业的发展，是本文要探讨的最为关键的问题。

2　大数据相关概念

2.1　大数据概念

大数据主要指的是无法使用常规的手段获取的信息资源，这种信息资源对于各行业的发展都是有很重要的作用和影响的，对于大数据的掌握关键不在于学习的收集，而是在于对信息的使用和归纳总结。

2.2　电力大数据概念

电力大数据主要指的是关于电力生产、输送电力以及进行调度各个环节中的设备检测、企业营销与管理的相关数据。这类数据对于电力行业的发展有着不可替代的作用，通过对于相关数据的采集以及归纳，在处理分析后可针对电网的使用现状进行优化和升级，从而更好地为电网高效可靠的运行提供相应的保障。

电力大数据的来源很多，主要来自于各个运行系统，如专业的数据采集系统、数据管理系统和配电管理系统等，这些系统都是根据配电的步骤环节进行具体划分的。因而，各个数据来源相对比较孤立，信息较为单一，信息质量参差不齐，这是电力大数据今后需要完善的地方。

3　电力大数据应用现状

根据我国现阶段的发展，大数据对于电力行业能源的影响巨大。电力能源问题和公共事业是人们所关注的问题，大数据时代的到来可以很好地帮助国家电网公司对有效信息进行挖掘和获取，并且在此基础上将大数据应用于推进智能电网并进行适当的转型。针对一些分布式可再生的发电资源来说，大数据的应用可以帮助其进行预报或者调度，使国家电力行业的发电效率得到很大程度的提高。电网互联不仅是电力体系的具体要求，更是为了发展的客观需要，所以需要得到重视。用电是人们工作生活都离不开的，对于电力技术的安全性以及完善的体系都是在发展过程中需要重点关注的对象，而对于智能电网中的大数据进行

人民电力出版社

收集于研究分析，可以更好地预测电能流的情况，及时地发现和解决存在的问题，最后实现发电的清洁化和高效化。

信息化和企业的管理良好的结合也很关键。很多企业为了响应中国共产党第十八次全国代表大会提出的“推动信息化与工业化深度融合”的理念，进行了自身管理和运作模式的完善与丰富。电力企业都是慢慢地趋于一体化的发展，这种一体化是基于大数据背景之下的，这些大数据的内容分析和使用，对推动我国电力企业的进步和发展起到至关重要的作用。

大数据在电力行业的应用也分为很多层面，首先大数据可以用来分析电力行业的发展现状、我国现阶段的人口状况以及我国的政策情况，在新政策制定的过程中提供相应的参考。因而国家电网公司也开始使用大数据分析作为政策制定的参考。

比如用电量和人口之间有着的密切关系。人口的增加和减少对于国家电力的使用有着很大的影响，所以说通过大数据分析近些年我国的人口变动以及用电量的变动，可以很好地发现二者之间的关系，根据人口的增减以及分布情况，为电力的提供进行了良好的预测。

其次，商店中的消费情况和经济环境有着密切的关系。随着社会的进步，人们生活生产中用电的地方越来也多，经济的发达某种程度上也是意味着用电量的增加，所以可以通过大数据的分析来挖掘电力消费与人均收入以及国民生产总值之间的关系。

我国对大数据在电力行业的应用相对比较晚，但在普及的过程中取得了不错的成绩，各地纷纷响应号召，建立电网数据搜集平台，从而更好地进行电力大数据的收集和利用。综上所述，目前大数据在我国电力行业的应用比较普遍，并且给我国电力行业的发展带来了新的方向。

对电力大数据的合理运用可以给行业内外都提供很高附加值的增值服务，特别是对电力企业的盈利及控制水平的提升都有很高的价值，之前有电网方面的专家做过调查研究，表示每当数据利用率提高 10%，电网的利润随之提高 20%～49%，可见数据的利用率和电网的利润成正相关。

另外，大数据分析也可以让电力企业的运营效率得到很大的提高，包括提升客户体验。在运营效率上，可以提高需求的预测准确性和产品管理的高效性；在改善用户体验上，可以优化客户关系，进行互动营销，针对性地进行优惠的定制与服务，从而更好地提升客户的体验感。

4 电力大数据应用风险

尽管大数据的应用给电力行业的发展带来了很多便利，提高了工作的效率，但也存在一定的风险，这些风险可以在未来进行合理有效的规避。由于大数据的来源主要依托于互联网和计算机云端等，数据的真实性和可靠性都有待商榷，包括可能遇到黑客的攻击从而造成隐私泄露。所以大数据的应用需要采取一定的科学的手法进行管理，将大数据分析中的风险降到最低。由于来源不同，大数据信息的质量也存在参差不齐的情况，在进行分析前还应进行适当的筛选，留下高价值信息以提高大数据分析的效率和准确度。

再者，对于数据内容的真实性、准确性以及管控力度的大小，都是会在一定程度上影响到大数据的分析成果。不过目前来看电网数据相对比较杂乱，这之中沟通较少的原因也会导致整个电力行业的数据集成度大幅度降低，很难将大数据的优势发挥出来。针对这些问题，需要构建相应的数据模型，统一数据规范，以扩展数据的复用性，增强数据处理以及交互能力，从而完善建立电网数据的基础构建。

5 结束语

新时期下任何行业的发展也都需要顺应时代的发展需求。互联网科技的发展势头下，大数据应用是新时代发展的潮流和必然趋势，针对电力行业覆盖面积大、涉及人群广等特点，大数据的采集分析和利用可以很好地解决电力行业发展中存在的问题。不过目前我国对于电力大数据的应用还是不够深入，需要花费时间研究才能将电力大数据的价值最大程度地挖掘出来。大数据对于电力行业的发展，既是机遇也是挑战。大数据与电力资源信息的结合过程暴露出了很多的问题，信息的准确性、安全性都会影响到相应电力政策的实施，如何解决这些问题也是需要在今后的实践中不断探索和学习的。

参考文献：

[1] 吕敬尤, 胡梁, 林海, 等. 基于大数据的电力行业指标体系的建立

与应用[J]. 机电信息, 2019(8): 62-63.

[2] 赵颖. 分析电力行业大数据应用建设及配网停电优化[C]//中国电力科学研究院 2018 智能电网信息化建设研讨会论文集. 2018: 2.

[3] 李志勇, 郭一通. 大数据背景下电力行业数据应用研究[J]. 自动化技术与应用, 2018, 37(9): 156-158.

[4] 汪俊洋. 电力大数据的未来发展趋势[C]//中国电机工程学会电力信息化专业委员会 2018 电力行业信息化年会论文集. 北京: 人民邮电出版社, 2018.

[5] 秦小强, 尚宝. 浅谈大数据在电力行业中的应用[J]. 信息系统工程, 2018(8): 111.

[6] 廖继军. 大数据在电力系统中的应用现状及发展前景研究[J]. 通讯世界, 2018(6): 141-142.

人民邮电出版社

大型企业端到端流程系统的设计与实现

丁彩云，胡劼，孙婷婷
（中国广核电力股份有限公司信息技术中心，广东 深圳 518124）

摘　要：集团公司以“管理四化”为目标推动流程管理，在建立分级业务流程体系的基础上，对流程进行信息化实施。通过集团流程体系信息化建设项目，实现线上工作流、线下业务以及非工作流应用的全面串接，并对流程运行情况进行监控评估，以便持续改进。主要阐述了集团流程体系信息化建设项目中，如何进行系统设计及技术实现，包括流程平台设计、监控平台设计、主子流程串接等。该系统完善了集团流程管理四大工具平台，实现了9 条端到端流程从业务需求提出到任务完成全线贯通，提高了各业务领域办公效率，也确保了核心业务流程的合规运行，大幅提升了集团公司流程管理水平。

关键词：端到端流程；流程平台；流程监控

1　引言

集团在全面深化改革过程中，借鉴台塑等企业的精益化管理经验，结合集团发展历程，将管理活动制度化，建立分级业务流程体系，以“管理制度化、制度流程化、流程表单化、表单信息化”为目标推动流程管理。集团公司已通过流程体系建立项目建立了集成的、可视化的流程管理体系，建立了集团公司业务流程架构、编制业务流程清单、业务流程文件，并以流程门户的形式发布。

现需启动集团流程体系信息化建设项目，对流程体系已梳理优化并出版的流程进行信息化实施，实现业务流转、跟踪记录、信息反馈、数据统计等。同时，设计端到端流程监控指标，并对指标进行监控和评估，以便持续改进。

2　项目目标

在满足整体 IT 架构的前提下，采用业界成熟稳定的工作流引擎，快速建立面向全集团核心业务流程和管理流程的统一流程平台，设计并完成流程门户、流程设计、流程应用、流程监控。通过流程平台进行流程编辑、发布、上线，制定端到端流程的监控指标，并进行流程监控。

- 流程平台方面，主要达成以下目标：可视化表单设计、图形化流程设计、模块化应用组件、参数化数据建模，支持复杂的业务工作流，支持图形化流程运行监控和分析，支持强大的组织机构和权限以及强大的扩展和集成能力。
- 流程信息化方面，搭建 EPM 端到端流程管理系统、EMS 端到端流程监控系统，实现 9 个端到端流程和 16 个核心职能流程的信息化运行和在线监控。

3　流程平台设计

流程平台是业务流程体系落地的 IT 支撑中心，要满足业务端到端的管理和业务过程监控要求。作为企业基础服务类应用，要为上层业务提供支撑服务，降低业务应用对业务流程支撑的技术依赖，要提升对业务流程支撑的能力与效率，提高业务流程支撑规范度，打通应用间流程堡垒，实现端到端流程贯通。流程平台设计具体如下。

- 流程设计平台，用于流程设计和维护管理，对流程、制度、风险、组织与岗位等流程全要素进行建模管理，是管理体系融合的载体；
- 流程展示平台，用于建模后模型库的前端展示，是集成流程体系的知识库；
- 流程运行平台，是电子化流程运行的核心平台；
- 流程监控平台，是流程运行监控平台，为流程优化提供运行数据。

其中，流程运行平台和流程监控平台是本次集团流程体系信息化建设项目的重点建设内容。流程运行平台需将流程能力封装成界面级、应用级的技术服务，通过服务开放对外发布，各类业务应用通过服务调用实现流程能力的集成，主要流程服务见表 1。

人民邮电出版社

表 1　主要流程服务

序号	功能	功能描述
1	流程发起	通过该接口并传入参数产生一条流程实例，发起的同时进行流程的提交
2	任务提交	通过任务提交达到流程正常流转的目的
3	任务退回	可将任务退回到指定历史步骤的实际处理人进行任务重办
4	任务撤回	当已处理的任务到达目标环节还未办理时，处理人可将任务撤回到当前环节
5	流程作废	业务流程可中途作废
6	任务调度	一般拥有特殊权限的用户可根据实际情况将流程调度到任务环节
7	任务抄送	任务可抄送给其他人待阅，可在流程处理时进行抄送，也可以单独抄送
8	待办、待阅	可获取我的待办、待阅记录以及流程相关数据信息
9	已办、已阅	可获取已经办理和已经批阅的处理记录
10	代理、委托	可实现流程代理和流程委托，代理是将某一范围内的流程授权给其他人处理
11	邮件提醒	流程处理时刻邮件通知进行提醒
12	流程跟踪	丰富的流程跟踪接口以及图形化流程跟踪，方便直观
13	流程统计	提供了大量的流程统计接口，可综合分析业务进展状况
14	性能监控	系统记录大量的数据处理性能日志，为性能分析提供数据保障

由于业务流程种类繁多，特点差异大，对于一些在统一流程平台不能完全支撑的特殊流程，业务应用可以通过业务流程适配的方式，基于统一流程平台的能力进行一定程度的扩展支撑。

4　EPM 系统设计与实现

EPM 端到端流程管理系统是全流程视角业务化的统一流程管理系统，实现了线上工作流、线下业务以及非工作流应用的全面串接。以全流程的视角展示状态，而不仅是片段；以业务化的方式展示流程图，而不是显示流程的技术视图。

4.1　主子流程串接

端到端流程审批过程中，各个审批环节可能会触发子流程。主流程当前环节调用子流程时，只有子流程审批完成后，主流程当前环节才能审批。如子流程未完成，则主流程为挂起状态。通过流程图可以查看到主子流程间的关系和流程状态。流程串接走向示意图如图 1 所示。

4.2　运转功能设计

端到端流程处理过程中，环节处理人（发起人）因业务需要，向运转对象（接收人）发起运转，运转对象按需进行回复。运转对象收到待办后，只能填写处理意见、修改附件以及再次发起运转，不能修改表

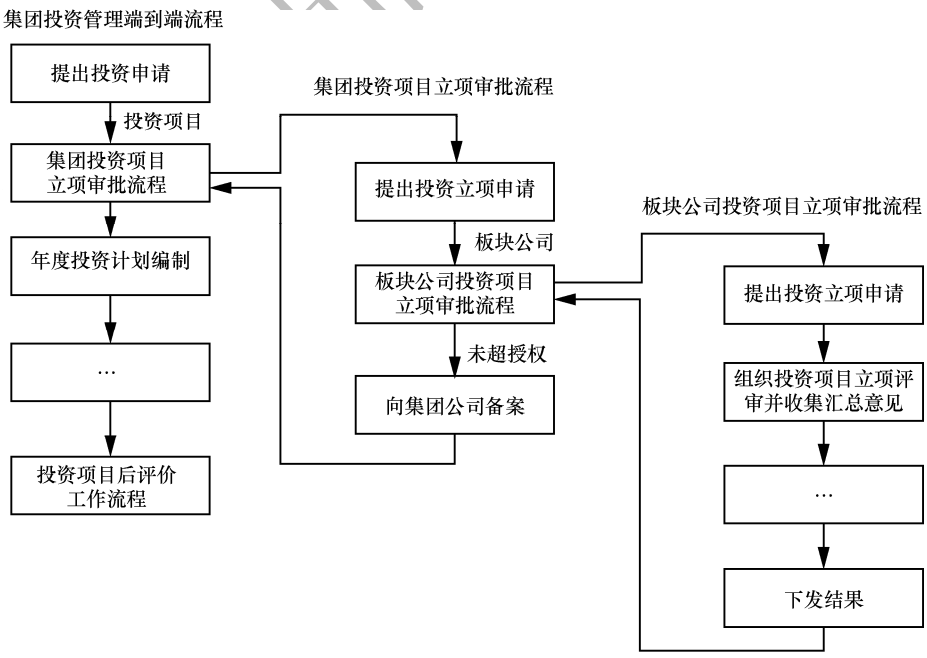


图 1　流程串接走向示意图

单信息及其他操作。

运转功能拆分出 3 个功能项：部门内处理、协办、澄清。部门内处理用于环节内的内部处理，支持部门内工作的任意分派、多次审核、审批。协办是环节内的跨部门办理，一般应用于主办部门审批时，需要其他职能部门协助办理；主办部门可以向一个或多个职能部门发起协办，系统自动带出协办部门接收人；协办部门由部门总或授权部门副总签发本部门意见，回复主办部门。澄清是环节内的处理人点对点的沟通澄清操作；可以向一人或多人发起澄清操作；接收人收到待办后必须对需要澄清的问题进行回复。

5 EMS 系统设计与实现

EMS 端到端流程监控系统，与 EPM 系统同步建设，集成多个流程系统的数据源，对流程运行数据予以监控分析，通过图形化图表与报表进行展现，并支持逐级钻取。监控指标包括流程状态监控、流程效率监控、流程质量监控、流程合规性监控等。

5.1 监控平台设计

EMS 系统涉及监控平台、报表统计、阈值管理三大方面，其中监控平台分为流程状态监控、流程效率监控、流程质量监控、流程合规性监控。系统主要功能如下。

- 流程状态监控包括已完成、进行中、已作废。对流程状态为已完成、运行中、已作废的端到端流程实例统计。
- 流程效率监控包括正常、超时、严重超时。超时是流程环节审批时效超过系统设定正常的阈值，严重超时是流程审批时效超过系统设定的严重超时的阈值。
- 流程质量监控包括澄清、退回。澄清指流程环节处理人需要点对点的沟通，退回是指流程审核不符合接受的条件，退回至指定环节修改后再次审批。
- 流程合规性监控包括跳转、转办。跳转是指从流程当前处理环节跳到其他环节，EMS 只监控因流程无法正常流转或路由流转错误时，由系统管理员在后台干预的跳转；转办是指委托他人代表自己审批流程，EMS 只监控因审批人无法自己进行转办操作，由系统管理员在后台干预的转办。

端到端监控分为 4 层监控，逐层钻取，每个层级都能显示监控的指标。单击流程名称，向下一级钻取，展开所有流程场景监控数据；单击流程场景名称，展示该流程场景下的所有流程实例列表；单击监控统计数据，跳转到流程实例列表；单击流程实例列表的流程主题，可以查看表单详情和流程图。

5.2 超时监控设计

为优化和完善流程监控功能，进一步提升办公效率和质量，EMS 系统在实现全流程监控的基础上，实现了流程的分级提醒功能。

纳入 EMS 监控流程的各个环节，根据要求都设置 KPI。当前处理人待办审批时间超时，则系统会发送邮件提醒用户。流程环节超时提醒分为“普通超时提醒”和“分级超时报警”。如为普通超时提醒只给超时环节的处理人发送邮件提醒；如为分级超时报警，提醒规则如下，待办超时后，系统给提醒对象每天发送提醒邮件。

- 当环节处理时间 T 超过 KPI 时，即环节超时，此时触发第 1 级报警，提醒对象为经办人。
- 第 1 级预警：若此后经过 ΔT 时间，环节仍未处理，则报警等级上升到 2 级，除提醒经办人外，同时提醒经办人的上级领导（提醒对象由系统根据提醒规则自动确定）。
- 第 2~5 级预警：以此类推，此后若环节一直未处理，则每过 ΔT 时间，报警等级提升 1 级，提醒对象行政级别逐级提高。报警等级共分 5 级，最高可提醒到集团公司总经理。

6 结束语

通过搭建 EPM 端到端流程管理系统和 EMS 端到端流程监控系统，完善了集团流程管理四大工具平台：流程设计平台、流程展示平台、流程运行平台、流程监控平台。四大工具平台的有机融合，为“管理四化”从设计到运行的落地提供了技术保障。

项目实现了 9 条端到端流程和 16 条核心职能流程信息化和监控，实现流程落地、过程可控、管理可视。端到端流程信息化实现了从业务需求提出到任务完成全线贯通，打破传统职能管理产生的“部门墙”，填补了部分业务流程的空白，内部审批流程更加清晰，提高了各业务领域办公效率；集团公司管理者可通过监控平台实时监控各业务领域流程运行情况，随时掌握业务动态和流程异常，做到全流程可视，确保了核心业务流程

人民邮电出版社

的合规运行，大幅提升了集团公司流程管理水平。

参考文献：

[1] 王磊. 流程管理风暴: EBPM 方法论及其应用[M]. 北京: 机械工业出版社, 2019.

[2] 国网天津市电力公司.“五位一体”协同机制理论与实践[M]. 北京: 中国电力出版社, 2017.

[3] 王玉荣，葛新红. 流程管理[M].北京: 北京大学出版社, 2016.

人民邮电出版社

大型企业信息通信智慧客服一体化解决方案

刘娇丽，李雅西，沈雪晴，邹晓颖，李枫
（国家电网有限公司信息通信分公司，北京 100761）

摘　要：目前大型企业信息化发展迅速，导致信息通信客户服务的人工成本的压力随着服务质量要求的不断提升而逐年提高。而企业传统信息通信客户服务模式存在运维智能化水平低、人力成本效益偏低、缺乏精益管理手段、客户体验有待提升四大痛点。针对此现状，提出了一种基于“AI+大数据”分析的企业信息通信智慧客服一体化解决方案，包括在线客服机器人、语音导航、语音外呼机器人、智慧工单、智能分析等五项微服务，并基于微服务，开发客户侧 App、运维侧 App 以及管理侧后台，从而拓展业务受理渠道，节约人力资源，全面提高运维效率，创新客户体验。

关键字：大型企业；人工智能；信息通信智慧客户；在线客服机器人，智慧工单

1　引言

互联网时代改变了人们的办公方式和生产工具。计算机已经成为了现代公司的主要生产工具，目前国家电网信息化发展迅速，电力生产、营销、人财物管理等多专业都积极推行信息化以提高工作效率，员工办公过程遇到的诸如网络不通、软件兼容性等信息通信难题也随之而来，为解决上述问题的客户服务工作应运而生。但是，企业传统的信息通信客户服务模式[1-2]存在运维智能化水平低、人力成本效益偏低、缺乏精益管理手段、客户体验有待提升[3-4]四大痛点。

提出了一种基于“AI+大数据”分析的企业信息通信智慧客服一体化解决方案，包括在线客服机器人、语音导航、语音外呼机器人、智慧工单、智能分析等 5 项微服务，并基于微服务，开发客户侧 App、运维侧 App 以及管理侧后台，从而拓展业务受理渠道，节约人力资源，全面提高运维效率，创新客户体验。通过该解决方案，最终实现客户侧一站式智能服务，运维侧智能接单、远程协作、后台管理侧智能决策、质量管控。

2　总体设计思路

信息通信智能客服一体化解决方案设计思路为：围绕人工客服坐席工作全流程，提供全链路 AI 能力辅助，智能应答过程采用先机后人、基于漏斗服务模式、人机无缝结合方式，并为人工客服服务全流程工作环节提供 AI 辅助，全面提升客服坐席服务效率，提升咨询用户服务体验。解决方案示意图如图 1 所示。

具体应用如下。

（1）客户侧一站式智能服务

基于人脸识别、智能流程机器人、智能工单调度等技术，实现用户申请的自动审批和办理。用户可通过人脸识别、指纹识别等方式一键登陆 App，在线进行业务咨询、资源申请或故障报修。智能工单调度可根据客户标签画像与客服能力画像的匹配程度，将用户的申请智能分流至相关的人工坐席或在线客服机器人。在线客服机器人采用多模态人机对话模式，精准识别用户需求，为用户智能推荐解决方案，智能预判客户情感及潜在问题，辅助精准服务，全面提升客户满意度。

App 具有良好的交互方式与交互体验，用户可在 App 上实时查询在办业务进展情况及反馈结果，App 也可主动为用户进行业务进展情况推送。此外，可通过 App 主动推送各类公告信息及增值服务信息，用户可在线参与调查问卷、反馈意见等，加强与用户互动交流，提升交互体验，进一步提供个性化增值服务。

（2）运维侧智能接单、远程协作

智能派接单：App 自动关联台账生成用户工单，通过智能派单自动派发至匹配工程师，工程师可在

人民邮电出版社

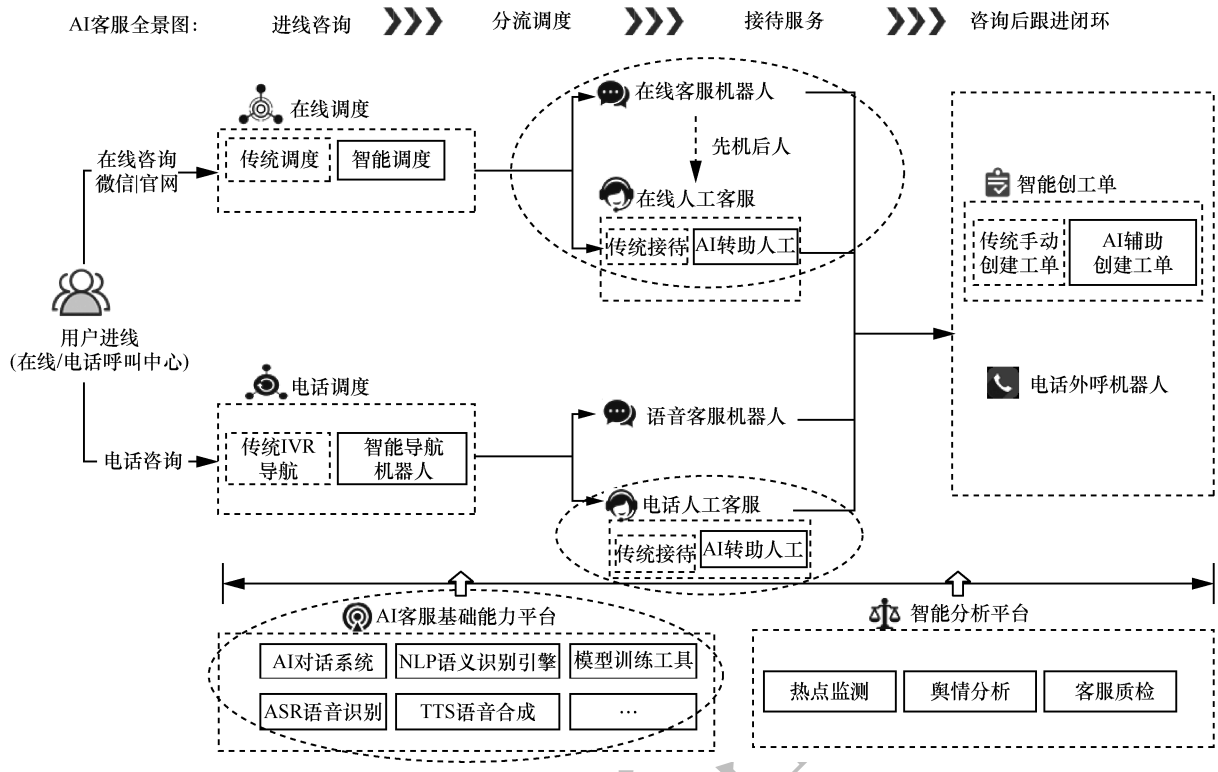


图1　信息通信智能客服一体化解决方案示意图

App 上在线接单，服务完成后，相关数据自动归档分析，实现工单与出入库及台账数据的自动关联与管理。

智能巡检：实现调度台、配线间等的智能巡检，实现表单在线填写、设备历史故障查询，历史巡检结果查询，巡检结果自动上传与统计。

远程协作：针对现场运维与后台专家协同处理的工作，可通过视频开展远程协作。

（3）管理侧智能决策、质量管控

基于“AI+大数据”实现智能分析决策，实时监控客户反馈、检查运营异常。提供多维度、多形式的数据分析与管理机制，深度挖掘运维数据价值，挖掘客户痛点问题，为各业务信息系统优化提供有力支撑。实现各类运维业务数据、资产设备、安全数据等的整体分析及可视化展示，对工程师服务质量进行分析评价，基于语音识别及自然语言处理等技术实现客户服务的全量质检，辅助运营管理。

3　智能客服机器人

在线智能服务机器人采用多模态人机对话模式，提供 7×24 小时智能应答服务。支持纯文本、图文、折叠、富媒体等多种消息展示模式，支持网站、App、微信、微博等多种渠道接入；支持用户文本与语音信息输入、支持情绪识别、复杂上下文理解与多轮对话能力、支持先机后人、智能转人工客服策略。

智能客服机器人接入如下，智能客服提供一个 https/URL 的链接地址，使直接嵌入到微信公众号/App、企业管网的菜单即可使用。工作示意图如图 2 所示。

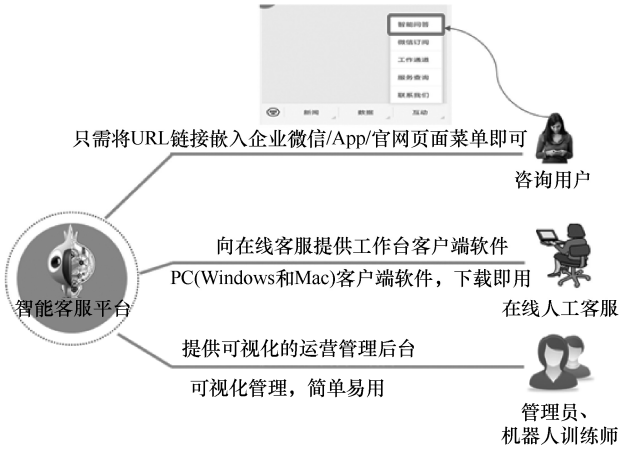


图2　智能客服机器人接入示意图

按照先机后人的漏斗服务模式，当智能客服机

器人无法回答时，无缝转到人工客服，人工客服通过该工作台与用户进行交流沟通。在线客服工作台软件直接安装在 Windows/Mac 电脑，人工客服登录后即可使用。

4 语音导航机器人

传统企业服务热线大多采用交互式IVR菜单按键方式进行坐席转接，这种方式菜单按键繁琐、聆听时间长，另一方面，随着企业业务不断发展以及业务分支机构的壮大，会导致企业热线 IVR 菜单设置的层级较多，进一步增加 IVR 菜单按键繁琐层度，导致用户拨打热线相当不便。

通过引入 AI 技术，用语音交互替代掉传统的IVR，就能够实现语音导航进行的效果，引导用户说出所反映问题的类型，根据问题类型，机器人会自动引导到专业坐席提供专业服务，提升问题的解决效率。对于不能明确定位专业坐席的用户，将引入到综合坐席进行处理。

智能语音导航机器人应用场景如图 3 所示。

5 语音外呼机器人

智能客服通过外呼的方式对用户进行跟踪回访、问卷调查等，按照预设多轮对话交互服务，自动识别用户的关键答复，从中提取用户回访或问卷调查场景中的关键信息，智能语音导航需切合企业具体业务场景进行定制，构建满足企业业务需要的智能外呼能力。

智能语音外呼功能主要有以下几个部分。

（1）数据获取

回访功能模块从工单系统中获取待回访工单，获取的模式包括实时获取与批量获取。

1）实时获取模式：回访处理人员在对已回复工单进行审核时，可以直接调取回访功能，实时对用户进行回访，并实时获取回访结果。

2）批量回访功能：回访处理人员可对所有待回访用户进行审核后，批量将待回访工单传递到回访系统，进行智能客服自助回访。

（2）数据清理

对待回访工单中的异常数据进行处理。根据业务规则，对回访工单中匿名用户、多联系电话用户进行数据规范，避免在呼叫用户时产生争议。

（3）数据统计

对所有智能客服自助回访结果，按照统一维度进行统计分析，包括按照处理单位维度、回访结果维度

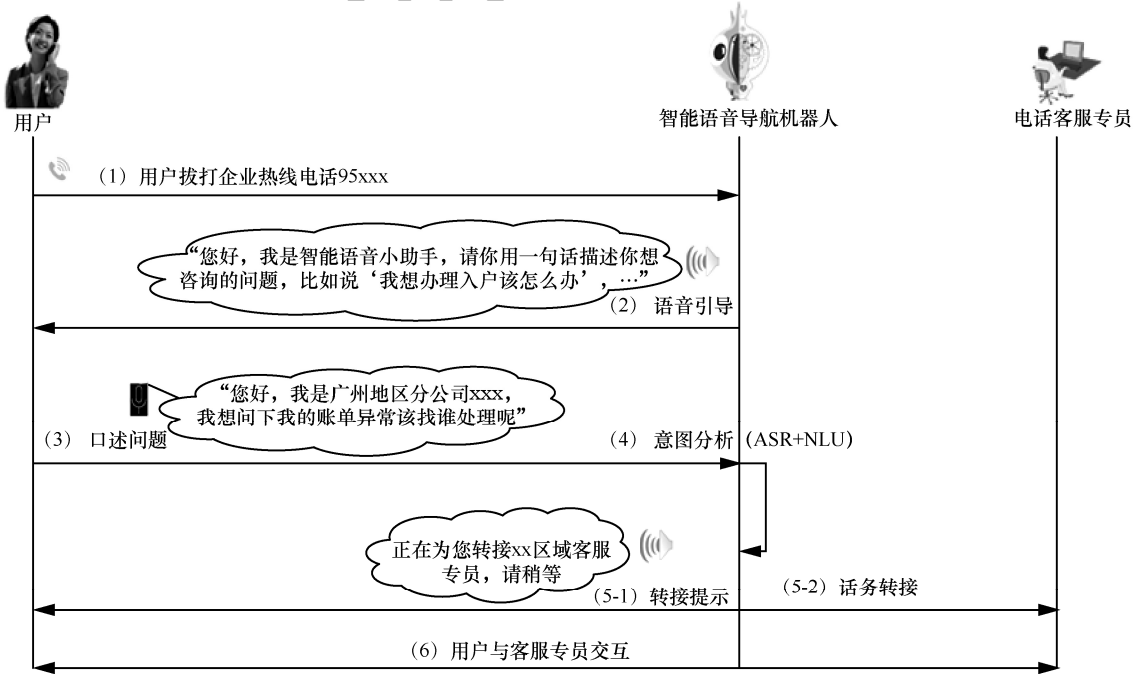


图 3 智能语音导航机器人应用场景示意图

印电出版社

等。同时对不满意工单进行清单展示，可方便回访人员进行二次人工处理。

（4）录音管理

针对所有智能客服自助回访工单，系统将全程实现录音管理，并可针对不满意原因进行语音转写，方便提供工单处理人员进行二次处理。

（5）流程开发

通过对历史回访记录的分析，建立全场景智能客服自助回访流程，自助回访服务的业务实现流程如下。

步骤 1 智能客服对需回访用户进行自动外呼回访。

步骤 2 智能客服通过语音识别、意图识别、对话管理等过程分析用户的响应率、解决率、满意率。

步骤 3 针对用户不满意的回复，分析用户留言，并将语音自动转换成文字，提供回访审核人员进行二次处理。

6 智慧工单

智慧工单系统是根据工程师实时状态，依据工程师的评价、工作状态、限制因素等选择要出勤的工程师。后期再利用深度学习算法，不断优化各项指标的权重，优化结果。

为了合理公平的分配任务，系统挑选影响任务分配的影响因子。

（1）忙闲状态

该项指标是指当前工程师工作状态，有工作中、空闲中、休息中 3 种状态。

（2）当日已工作时长

工程师当日已经完成工单的累计时长，该指标主要衡量了工作量，参考此指标是为了保障公平原则。

（3）工单剩余时长

当前工单预计剩余时长，这项指标主要考虑的是当前全部运维工程师都在工作状态，需要从中选择一个即将最快结束任务的工程师。

（4）距离远近

当前任务地点距离工程师当前地点的距离。当运维工程师在办公区域服务过程中，系统需要根据他们当前所处的楼层，选择距离客户最近的工程师。

（5）负效应因子

工程师被当前客户投诉次数。在选择运维工程师的过程中，还需要考虑用户满意度，即尽量避免工程师服务于投诉过他的用户。

然后制定影响工单调度分配的原则，梳理如下。

（1）用户等待服务时间不得大于 1 h。

（2）一个工程师同时接受工单数不得大于 5。

（3）不同工程师工作量的差距不得大于阈值（阈值会根据深度学习算法进行优化调整）。

（4）工单难度不得大于工程师能力水平。

最后根据指定的调度原则，将工单调度问题转化为多目标优化问题，再利用深度学习算法，不断优化各项指标的权重，得到系统最优解，为用户分配最合适的工程师。

7 智能分析

智能分析平台是面向企业业务系统或工单系统的历史，集热点趋势预测、舆情风险跟踪和服务质量管控于一体的高效运营平台，通过全链条大数据挖掘，提供精准实时和清晰可视化的服务。以大数据、语义分析技术为基础集数据管理、挖掘、分析于一体的业务智能分析系统。通过本系统应用可以深入挖掘数据中心的数据价值，有效支持数据中心构建智能化的数据分析体系，及时深度洞察运营中的短板，设定改进策略和优化流程，提供多维分析和报表展现，提升运营效率、降低风险，最终提升综合绩效。

从用户行为数据的采集、建模、挖掘到效果分析，实现对用户“千人千面”的个性化内容推荐，为人工客服提供应答辅助推荐，改善用户体验，持续提升客服服务核心业务指标。对在线客服的场景进行服务流程的实时监控质检，提升客服标准操作流程的执行率，降低质检的人力成本。对业务重点关注的热点异常问题事件进行监控分析和预警，帮助热点管控团队及时跟踪干预、处理热点异常问题、提升端用户体验。在线与语音咨询范围的全量质检；在线风险模型复用于语音转写后实现文本风险抓取，支持系统跟进闭环处理语音风险。实时根据业务和指标需求强相关点，抓取分类场景下员工的方案、话术等服务内容执行情况，根据执行准确率提高员工方案执行准确率、服务质量和客户满意度。

8 结束语

本文通过对大型企业信息通信客户服务工作现状进行分析，提出了一种基于“AI+大数据”分析的企业信息通信智慧客服一体化解决方案，包括在线客服机器人、语音导航、语音外呼机器人、智慧工单、智

人民邮电出版社

能分析等 5 项微服务，从而拓展业务受理渠道，节约人力资源，全面提高运维效率，创新客户体验。为企业日常信息化工作的开展保驾护航。

参考文献：

[1] 黄翊. 基于智能语音分析的客服智慧运营管理系统解决方案[J]. 科技传播, 2018(3): 121-123, 161.

[2] 李博, 高志远. 人工智能技术在智能电网中的应用分析和展望[J]. 中国电力, 2017, 50(12): 136-140.

[3] 高庆辉, 刘佳, 李玮, 等. “互联网+95598 供电服务”模式探索与实践[J]. 电气技术, 2017, 18(12): 134-137.

[4] 姜冬. 基于客户体验的 95598 新型服务模式[J]. 电气技术, 2018, 19(9): 111-114.

人民邮电出版社

~

电力大数据下的电动汽车充放电隐私数据保护

王帅，周晶，孙喜民，张宾
（国网电子商务有限公司，北京 100053）

摘　要：针对电动汽车充放电阶段各实体的通信要求，设计了一种实用的通信网络体系结构，分析了各实体信息交互过程中存在的隐私泄露问题。针对电动汽车充电/放电阶段用户、用户车辆信息及充电数据的隐私保护问题，提出了一种基于无证书环签密方法的电动汽车充放电阶段的隐私保护方案，设计了方案的系统建立、环签密、验证和账单生成时的伪身份核实等 4 个算法，给出了隐私保护方案的实现流程，从身份信息和数据信息两个方面解决对电动汽车充放电的隐私保护问题。为了提高方案的执行效率，将环签密算法中耗时较长的双线性对运算和指数运算，改进为开销相对较小的乘法运算，并尽可能减少乘法运算数量。理论证明了方案的正确性、不可伪造性、匿名性和保密性，相关实验表明该方案实现隐私保护时效率较高，从而表明该方案的有效性和可行性，可以用于大规模电动汽车接入电网进行充放电操作的场景。

关键词：电动汽车；隐私保护；无证书；环签密

1　引言

随着能源与环境问题日趋严峻，电动汽车作为缓解此问题的重要技术逐渐成为全球研究和应用的热点。电动汽车通过接入电网（vehicle to grid，V2G）实现电动车辆（electric vehicle，EV）在受控状态下与电网之间进行双向能量交换，它是智能电网的重要组成部分[1]。根据既定的充电/放电策略，在满足电动汽车正常行驶需求的前提下，可将剩余电能可控地回馈给电网。从而不仅可作为新能源供电不稳定问题的缓冲，还可为电网起到“削峰填谷”的作用[2]，同时由于峰谷电价差可为电动汽车用户带来额外的收益。

为了保证电动汽车在充放电过程中通信信息的保密性、可用性、完整性、不可否认性和不可抵赖性，需要从充电/放电隐私保护问题涉及的两个方面，基于身份信息的隐私保护以及基于数据信息的隐私保护[3]进行研究。基于身份信息的隐私保护方案[4]的主要思想是将用户身份匿名化，使充电服务运营平台收到的细粒度数据无法与实际用户关联，从而达到隐私保护的目的，主要采用盲签名、假名技术、群/环签名、零知识证明等技术。基于数据信息的隐私保护方案的主要思想是利用数据聚合[5,6]的方式，使得攻击者即使在得知用户身份的前提下也不能关联到具体用户的数据。

Saxena N 和 Mahmoud M 分别提出了基于双线性对技术的方案[7,8]，Saxena N 提出的方案能满足通信双方的相互认证，以及对 EV 信息的隐私保护，如身份、电池状态、位置、充电/放电持续时间等。可抵御各种各样的安全攻击，包括中间人攻击、重播攻击、模拟攻击、重定向攻击和拒绝攻击。但基于双线性对的方法在计算开销方面相对较高。

近几年，无证书环签密以其具有无证书公钥密码体制以及环签密二者特有的优势被用在隐私保护上[9-11]。既解决了密钥的托管问题，又实现了在需要验证方验证身份时能保证在匿名条件下通过验证，同时又能够对信息进行加密传输。

在已有研究的基础[9]之上，针对电动汽车充放电阶段的隐私问题，本文提出了一种无证书环签密方案。在该方案中优化了无证书环签密的运算步骤，提高匿名认证的效率，降低计算的开销，以解决电动车用户在充放电费用结算和认证过程中可能带来的用户个人隐私信息、充电与缴费[12]数据隐私信息、EV 隐私信息泄露的问题，同时避免以往方法在认证和加密过程中开销较大的不足。

2　电动汽车充放电阶段用户身份及数据隐私保护方案的设计

2.1　电动汽车充放电数据通信网络体系结构设计

电动汽车充放电数据通信网络体系结构包括可信

人民邮电出版社

中心（central authority，CA）、充电服务运营平台（charging pile operation platform，COP）、汇聚单元（aggregation，AGG）、充电站（charging station，CS）和电动汽车（electric vehicle，EV）5 个实体。

电动汽车充放电数据通信网络体系结构如图 1 所示。

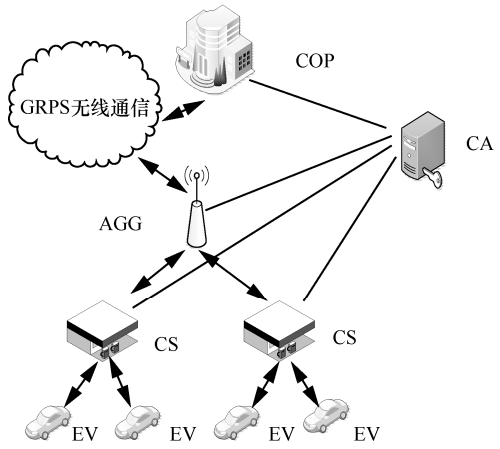


图 1　电动汽车充放电数据通信网络体系结构

2.2　电动汽车充放电时需要保护的用户身份和数据隐私

V2G 作为智能电网配电端的一个重要应用，在用户与电网进行双向的信息交流时，其隐私信息就完全暴露给了非授权者，EV 充电/放电的隐私主要包括身份信息和数据信息两大部分，针对这两方面的 EV 充电/放电隐私信息见表 1。

3　电动汽车充放电隐私保护设计与实现

3.1　充放电隐私保护方案的实现

V2G 充放电隐私保护方案由 4 个算法组成。基于无证书环签密的电动汽车充放电隐私保护方案的实现流程如图 2 所示。

3.2　系统建立算法

（1）建立 CA 并初始化

选取两个素数 p 和 q，p、q 需满足关系 $q|p-1$，设 g 为循环群 G 中一个阶数为 q 的生成元。CA 随机选取一个系统主密钥 z，且 $z\in Zq^*$，其中 $Zq^*=\{1,2,\ldots,q-1\}$。计算系统公钥 y，且 $y=z^*g$。选取适当哈希函数 H1、H2、H3、H4，其中 H1 为 $\{0,1\}^*\times Zp^*\times Zp^*\rightarrow Zq^*$，H2 为 $Zp^*\rightarrow Zq^*$，H3 为 $\{0,1\}^*\rightarrow Zq^*$，H4 为 $Zp^*\rightarrow\{0,1\}n$。公开系统参数为{G, p, q, g, y, H1, H2, H3, H4}。

（2）EV 注册

① CA 为用户 EV 随机选取身份标识 ID$i\in\{0,1\}^*$，$i=\{1,2,\ldots,n\}$，其中 n 为电动汽车接入环的数量。随机选取 CS 的身份标识 IDC，IDC$\in\{0,1\}^*$；AGG 的身份标识 IDA，IDA$\in\{0,1\}^*$；COP 的身份标识 IDG，IDG$\in\{0,1\}^*$。

② EV 用户随机选取 Zq^* 中的元素 X_i，即 $X_i\in Zq^*$，计算 $b_i=X_i^*g$ 用作部分公钥，并将 bi 发送给 CA。

③ CA 随机选取 Zq^*中的元素 S_i，即 $S_i\in Zq^*$，然后计算部分公钥 $w_i=S_i^*g$，$t_i=S_i+z^*$H1（ID_i，w_i，b_i），并将 w_i 和 t_i 发送给 EV 用户，其中 t_i 将被作为新的 EV 标识被使用。

④ EV 用户收到 w_i 和 t_i 后进行验证，w_i+y^*H1（ID_i，w_i，b_i）$=t_i^*g$，若等式成立，计算 $z_i=t_i+$H2（X_iy），得到部分私钥 z_i。

⑤ 得到 EV 用户的公钥对（w_i，b_i）。

表 1　EV 充电/放电隐私信息

隐私信息	描述	
用户姓名	账户的所有者	身份信息隐私
充电服务提供商	提供服务方的身份	
账户 ID	账户的唯一识别 ID	
EV 的身份	EV 的车辆信息（EV 的型号、车辆识别号码 VIN、车牌号码等）	
用户权限数据	用户的个人密码	
电池状态	EV 电池的运作状态，净流入或流出电网的电量，用电模式等充放电设备的实时状态数据，电池温度	数据信息隐私
负荷数据	EV 电池的最大容电量以及充放电电压、功率等	
计量计费数据	充放电前后账户上的数据记录，充放电持续时间及电量，用户以往的账单（包括迟付或未付的账单记录）	
EV 的位置	EV 进行充放电活动的地点	
电机参数	电机的功率、最大扭矩、温度等	

人民邮电出版社

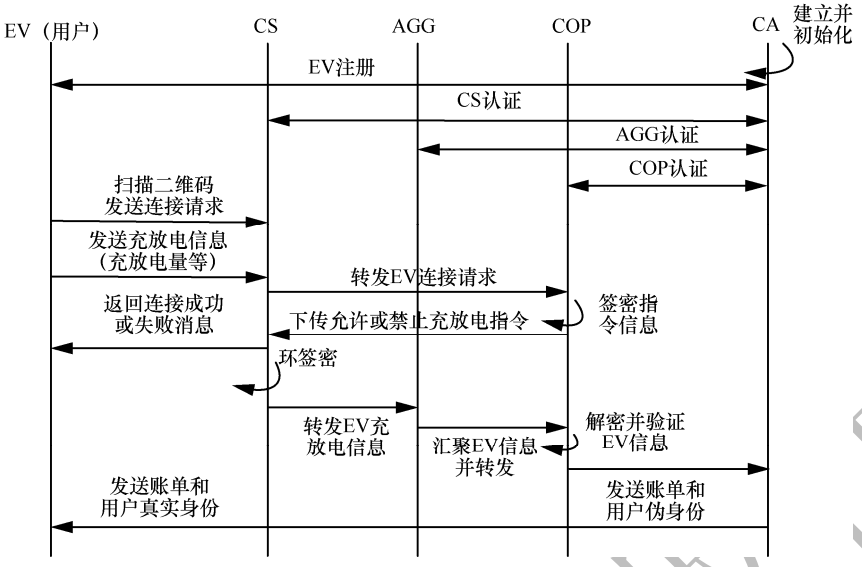


图 2　设计方案的实现流程

⑥ 得到 EV 用户的私钥对（z_i，X_i）。

（3）CS 认证

CS 认证过程类似于 EV 的注册过程，最终可得到 CS 的身份标识 IDC，公钥对（wC，bC），私钥对（zC，xC）。

（4）AGG 认证

AGG 认证过程类似于 EV 的注册过程，最终可得到 AGG 的身份标识 IDA，公钥对（wA，bA），私钥对（zA，xA）。

（5）COP 认证

COP 认证过程类似于 EV 的注册过程，最终可得到 COP 的身份标识 IDG，公钥对（wG，bG），私钥对（zG，xG）。

3.3　签密算法

在与 EV 建立连接时，CS 首先要选出某一个用户 EVs 代表环成员对消息 m 进行签密，其身份标识为 IDs，公钥为{ws，bs}，私钥为{zs，xs}，假设该环中有 n 个成员，EV={EV1,EV2,…,EVn}。充电站 CS 的身份标识为 IDC，公钥为（wC，bC），私钥为（zC，xC）。用户 EVs 要执行如下操作。

- 首先随机选择 $r1\in Zq^*$，然后计算 $B=g^*r1$。
- 生成可验证 EV 身份的信息：代表签密的 EV 用户 EVs 随机选取 $r2\in Zq^*$，然后计算 $A=r2^*g$（$zs+xs$），式中 zs、xs 为签密者 EVs 的私钥。
- 对任意 $i\neq s$，选择 $a_i\in Zq^*$，$EV_i=a_i^*p$，然后计算 $h0$=H1（IDC，wC，bC），h_i=H3（m，EV_i，A，EV，wC），式中 bC、wC 为消息接收者的部分公钥，m 为 EV 用户充电/放电信息和用户伪通信身份的级联 $m=m_i||t_i$，m_i 为 EV 用户 i 的充电/放电信息，ti 为 EV 用户 i 的通信伪身份，$i\in\{1,2,\cdots,n\}$。
- 当 $i=s$ 时，CS 随机选择 $as\in Zq^*$，然后计算 $EVs=as^*ws-\sum_{i=1,\ i\neq s}^{n}(EV_i+h_i*w_i)$，$hs$=H3（$m$，EV$s$，$A$，EV，$wC$），$v=hs^*y$，$h0$=H1（$ID_i$，$w_i$，$b_i$），$f=\frac{d}{y*h_0+v}$，$d=r2^*(zs+xs)$。式中 EV$s$ 为环成员中消息发送者的签名，ws 为发送者的部分公钥，w_i 为除发送者外其他环成员的部分公钥。
- 计算密文 C。

C=H4{（$wC+bC+y^*h0$）$r2$（$zs+xs$）A}⊕m，式中⊕为异或运算。

- IDc（充电站 CS）输出环签密信息。

σ={A, C, f, v, d, EV, EV1, EV2,⋯, EVn}

3.4　验证算法

- 转发

CS 转发 EV 用户的信息给 AGG。AGG 汇聚 EV 用户信息并转发给 COP。

- COP 验证签密消息

COP 收到环签密信息 σ={A, C, f, v, d, EV, EV1, EV2, ⋯, EVn}后，执行的操作如下。

步骤 1　计算 $h0$=H1（ID_i，w_i，b_i），l=[zC-H2（xC^*y）+xC]$^*d^*A^*g$，m'=H4（1）⊕C，$D=d^*g$。恢

复出解密消息 m'，若 $m'=m$，则说明收到了正确的消息。

步骤 2 验证下式是否成立，其中 $i\in(1, 2,\cdots, n)$。若成立则接收方接收 m'，否则丢弃收到的签密信息。

$$H3\{m', EV_i, D, EV, wC\}=h_i$$

3.5 账单生成时伪身份核实算法

COP 收到来自 AGG 的签密消息，进行解密并验证，获得 EV 用户的充电/放电信息 m，根据级联 $m=m_i\|t_i$，找出对应的（m_i，t_i），根据该对应信息生成 EV 用户 i 的账单 T_i，之后 COP 将用户伪身份 t_i 和账单 T_i 通过安全信道发送到 CA，CA 收到消息后通过计算 $t_i=S_i+z*H1\{ID_i,w_i,b_i\}$ 找到用户的真实身份，并将账单 T_i 发送给 EV 用户，用户即可通过账户密码进行充电/放电费用的缴纳和收取。

4 所设计方案的安全性理论证明与效率分析

4.1 所设计方案的安全性证明

（1）方案的正确性验证

① 消息的正确性验证

当 COP 接收到环签密信息 $\sigma=\{A, C, f, v, d, EV, EV1, EV2, \cdots, EVn\}$ 后，执行如下操作，首先计算 m'，恢复出经过加密的明文消息。

m'=H4（1）$\oplus C$

=H4{[zc-H2（$xc*y$）+xc]*d*A*g}$\oplus C$

=H4{[sc+z*H1（IDC，wC，bC）+xc]*d*A*g}$\oplus C$

=H4{[$sc*g$+$z*g$*H1（IDC，wC，bC）+$xc*g$]*d*A}$\oplus C$

=H4{（wC+bC+$y*h0$）*d*A}$\oplus C$

=H4{（wC+bC+$y*h0$）*$r2$*（zs+xs）*A}$\oplus C$

而由上节中环签密算法的设计可知，m=H4{（wC+bC+$y*h0$）*$r2$*（zs+xs）*A}$\oplus C$，对比经解密恢复出的明文消息 m' 和加密前的明文消息 m 可知，m'=H4{（wC+bC+$y*h0$）*$r2$*（zs+xs）*A}$\oplus C=m$ 成立，故消息正确。

② 身份的合法性验证

验证下式是否成立，其中 $i\in$（1, 2, …, n）。若成立则接收方接收 m'，否则丢弃收到的签密信息。

$$H3（m', EV_i, D, EV, wC）=h_i$$

其中，$D=d*g=r2*（zs+xs）*g=A$。

若 $D=A$，则身份正确，除 EVs 以外的任何攻击者在不知道 EVs 的私钥的情况下计算出与 D 相对应的 A 是不可能的。

（2）不可伪造性

① CA 是可信的：当外部攻击者想要充当环中的某一成员去构造并发送 CS 能够识别的签名 IDs 时，他必须清楚真实的发送者 EVs 的私钥（zs，xs），然而攻击者并不知道环中任何一位成员的私钥，而求解私钥将面临椭圆曲线上的离散对数问题（ECDLP）。

② CA 是不可信的：若 CA 将签密者 EVs 的伪身份 ts 泄露给攻击者，但因为 $zs=ts+H2（Xs*y）$，也无法求解 EVs 的私钥（zs，xs），进而无法构造出签名 IDs。若 CA 将 bs 泄露给攻击者，攻击者通过 $bs=xs*g$ 计算 xs 也属于 ECDLP 困难性问题，因此也无法构造签名 IDs。

（3）匿名性

由于本方案是完全对称的，从密文的角度出发，环中的任何成员之间是无差异的，都可能代表整个环中的所有成员去充当签密者，即便做最坏的假设，环中所有 EV 成员的私钥都遭到泄露，攻击者从中猜对签密者的概率也不大于 $\frac{1}{n}$，而如果攻击者来自环的内部，其成功猜中的概率也不会超过 $\frac{1}{n-1}$，所以本方案满足无条件匿名性。

（4）保密性

无证书环签密方案存在两类攻击者[12]，第一类攻击者不能获知系统主秘钥，但可以在公钥空间任意取值来篡改任意用户的公钥；第二类攻击者可以获知系统主密钥，但不能篡改目标用户公钥。在本方案中，假设攻击者取得了发往 CS 的密文 $\sigma=\{A, C, f, v, d, EV, EV1, EV2,\cdots, EVn\}$，而要想从密文中取得原始消息 m，则需要知道 l，而 l=[zC-H2（$xC*y$）+xC]*d*A*g，在不清楚 CS 私钥的前提下，上述两类攻击中的任何一个都无法还原出消息 m，所以本方案满足保密性。

4.2 方案效率分析

在主频为 3 GHz 的 CPU 上，计算中国剩余定理需要耗费的时长为 5.6 ms，计算双线性运算需要耗费的时长为 4.5 ms，计算模指数运算需要耗费的时长为 2.4 ms，而计算乘法运算只需要耗时 0.6 ms[2]。所以各方案的耗费总时长计算如下。

当参与认证进行充放电的电动汽车数量为 n 时：

参考文献[6]方案的耗时 $T1$=（3×2.4+2×4.5+9×0.6）n=21.6n（ms）；

人民邮电出版社

参考文献[2]方案的耗时 $T2=(6\times2.4+5.6)n=20n$（ms）；

本文方案的耗时 $T3=(n+7+4)\times0.6=(0.6n+6.6)$(ms)。

3 种方案计算耗时比较如图 3 所示。

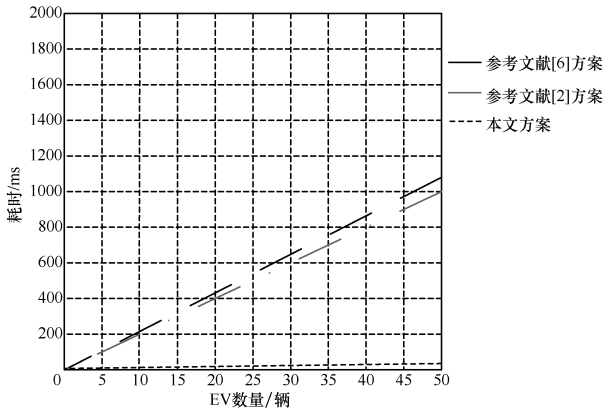


图 3　三种方案计算耗时比较

由图 3 可以看出，本文方案耗时随 EV 数量增加，变化最小。因为参考文献[6]、参考文献[2]中的方案还未计算 AGG 和 COP 的数据汇聚时延，所以其时间上的开销要远远大于本方案。

4　结束语

针对电动汽车充电/放电阶段用户、用户车辆信息及充电数据的隐私保护问题，本文提出了一种基于无证书环签密方法的电动汽车充放电阶段的隐私保护方案，设计了方案的实现算法及实现流程，从身份信息和数据信息两个方面解决了对电动汽车充放电的隐私保护问题。理论证明了该方案具有正确性、不可伪造性、匿名性和保密性。通过对方案的性能进行实验，结果表明其有耗时少和计算效率高的特点。本方案适用于大规模的电动汽车接入电网进行充电/放电操作。而如何保证行驶当中的电动汽车能够在享受电网个性化服务的同时，用户的隐私信息不被泄露是下一步研究的目标。

参考文献

[1] YONG J Y, RAMACHANDARAMURTHY V K, TAN K M, et al. A review on the state-of-the-art technologies of electric vehicle, its impacts and prospects[J]. Renewable & Sustainable Energy Reviews, 2015, 49: 365-385.

[2] 闫文肖. 电动汽车接入电网的用户隐私保护研究[D]. 北京:华北电力大学, 2015.

[3] ABDALLAH A, SHEN X S. Lightweight authentication and privacy-preserving scheme for V2G connections[J]. IEEE Transactions on Vehicular Technology, 2017, 66(3):2615-2629.

[4] HE D, KUMAR N, ZEADALLY S, et al. Efficient and privacy-preserving data aggregation scheme for smart grid against internal adversaries[J]. IEEE Transactions on Smart Grid, 2017, PP(99):1-1.

[5] LIU H, NING H, ZHANG Y, et al. Aggregated-proofs based privacy-preserving authentication for V2G networks in the smart grid[J]. IEEE Transactions on Smart Grid, 2012, 3(4):1722-1733.

[6] LIU H, NING H, ZHANG Y, et al. Battery status-aware authentication scheme for V2G networks in smart grid[J]. IEEE Transactions on Smart Grid, 2013, 4(1): 99-110.

[7] MAHMOUD M, SAPUTRO N, AKULA P, et al. Privacy-preserving power injection over a hybrid AMI/LTE smart grid network[J]. IEEE Internet of Things Journal, 2016 (99):1-1.

[8] SAXENA N, CHOI B J. Authentication scheme for flexible charging and discharging of mobile vehicles in the V2G networks[J]. IEEE Transactions on Information Forensics & Security, 2017, 11(7): 1438-1452.

[9] 张少敏, 赵乙桥, 王保义. 智能电网下保护用户隐私的无证书环签密方案[J]. 电力系统自动化, 2018(3): 1-7.

[10] YEH K H. A Secure transaction scheme with certificateless cryptographic primitives for IoT-based mobile payments[J]. IEEE Systems Journal, 2017 (99): 1-12.

[11] SHEN H, CHEN J, HE D, et al. Insecurity of a pairing-free certificateless ring signcryption scheme[J]. Wireless Personal Communications, 2017, 96(4): 1-7.

[12] MOON S K , KIM J O . Balanced charging strategies for electric vehicles on power systems[J]. Applied Energy, 2017(189): 44-54.

人民邮电出版社

电力行业数字证书互信互认体系的研究

廖会敏[1,2]，玄佳兴[1,2]，李丽丽[1,2]
（1. 国网电子商务有限公司（国网雄安金融科技集团有限公司），北京 100053;
2. 国家电网有限公司电力金融与电子商务实验室，北京 100053)

摘　要：电力网络安全是电力信息安全的重要组成部分，是电力信息化发展的重要保障和重要建设内容。以密码技术为核心的数字证书在身份认证、数据真实性、完整性和不可抵赖性等方面发挥了重要作用，是网络安全的核心基础，也是促进电力信息系统安全运行和可控的基础。近年来，基于数字证书的电子认证服务在电力行业的各类信息系统中得到了广泛的应用，但由于各电子认证服务机构相对独立、数字证书中间件不一致等因素的影响，提供的数字证书无法互认互通，给新一代电力系统的广泛互联、开放共享带来了一定的阻碍。

关键词：电力行业；数字证书；电子认证；互认互通

1　引言

近年来，电力企业大力开展信息化建设，已建成覆盖办公管理、业务经营、招投标等领域的多套应用系统，满足了企业各专业信息管理和网上办公的需求，支撑了企业的高效运营。以密码技术为核心的数字证书是众多系统中身份认证、授权管理、责任认定等网络安全的核心技术，大量企业已经开始采用数字证书完成信息系统的建设和运行，但是普遍存在当一个企业或一个应用采用一套证书信任体系，进行跨企业、跨应用流转时，面临多个数字证书互认互通互相信任的问题。

2　电力行业数字证书现状和存在的问题

2.1　电力行业数字证书现状

电力行业系统庞大、分布较广，在各省各市都有自己的电力企业，基于数字证书的 PKI/CA 认证技术在各电力企业的信息化建设过程中得到了广泛的应用。

（1）PC 端用户身份认证应用

在企业员工登录其个人电脑时，由于传统的“用户名+口令”的方式安全强度不够，采用以数字证书为载体的 UKey。员工插入 UKey 并输入正确的 U 盾口令后，便可安全的登录到个人电脑，拔掉 UKey 电脑自动锁屏，有效地保证了个人电脑登录环节的安全性。

（2）电子邮件应用

数字证书可以解决电子邮件的安全问题。企业用户通过 PKI/CA 平台申请安全电子邮件证书，使用数字证书来发送加密和签名邮件，保证邮件的内容在传输过程中是加密的，非法用户无法获得邮件的明文。

（3）网上申报与审批系统应用

用户持有的数字证书作为访问网上申报与审批的唯一身份，使用数字证书对申报与审批的数据进行加密、签名。实现了网上申报与审批的访问控制以及数据传输的机密性、完整性和不可抵赖性需求。

（4）电力行业电子政务应用

在电力行业的不同电子政务应用系统中（如网上办公、政务公文流转、网上年检等），用户登录系统时，验证用户的数字证书身份，根据用户的身份授予相应的权利，实现访问控制；在用户提交办公室数据等保密信息时，使用用户数字证书对数据签名，并通过安全通道对数据加密传输。

（5）电子商务交易应用

对于网上电子交易的企业和个人，在进行电子交

基金项目：国网电子商务有限公司（国网雄安金融科技集团有限公司）科技项目（No.5100/2019-72007B）；
国网电子商务有限公司（国网雄安金融科技集团有限公司）科技项目（No.5100/2019-72006B）

人民邮电出版社

易时通过数字证书确认其真实身份，确保网上交易平台发布信息的真实、完整和可靠；建立一个可信的网络环境，确保客户重要数据的安全性，通过数字签名技术有效地防止了用户抵赖行为的发生。

2.2 存在的突出问题

由于给电力行业提供 PKI 服务的电子认证服务机构（CA）不尽相同，缺乏完善的管理、法规和标准、技术，使得这些 CA 机构建立的 PKI 体系基本处于互相分割、互不关联的信任“孤岛”，因而无法在同一业务系统中兼容多家 CA 数字证书，一张数字证书也无法在多个系统中使用。其存在的问题有以下几点。

（1）数字证书格式不统一

不同的 CA 机构对数字证书标准规范的理解不同，采用的证书模版证书项定义不尽相同，各 CA 机构为了各自业务和客户的需求，在相关标准规范基础上，又增加了自定义的扩展项，导致该证书仅能在单个业务场景中使用，为了办理不同的业务，用户需要办理多张数字证书。

（2）介质驱动各有不同

目前国内生产安全介质的厂商有数十家，各家介质理论上都需要按照国产密码算法（即国密）的要求，实现国密和国际相关标准接口（如国密 SKF 标准接口和微软 CSP 标准接口）。但各家对标准的理解各有不同，而且即使同一厂商同一型号的介质，其不同批次在生产的细节上也可能有所不同。另外介质厂商必须满足 CA 机构定制化接口的需求，导致一个应用系统往往只能使用一家或者几家的安全介质。

（3）数字证书中间件不统一

数字证书在应用系统中的使用，所涉及的业务大致上有数据加密、数据解密、PKCS1#/PKCS7#签名及验签、时间戳签名及验签等。根据应用系统架构方式的不同（B/S，C/S），各 CA 机构会提供相应的服务端和客户端中间件以及签名验签服务器和时间戳服务器等。从客户端软件讲，各 CA 机构所提供的中间件通常包含私有定制化的接口，仅能配合自己 CA 签发的数字证书使用，更有甚者其中间件仅能在某个项目中使用。

（4）算法问题

在推进国密算法的背景下，国内已有的 RSA 算法的数字证书要逐步过渡到 SM2 算法的数字证书。现阶段，很大一部分电力行业的 PKI 体系已经完成了国密算法的改造，已完全使用国密算法或兼容国际国密算法两种模式，但由于一些历史原因，部分业务系统还没有进行国密算法的改造。

（5）数字证书策略分级的问题

目前国际上普遍对证书策略分级，但是国内数字证书目前没有统一的分级定义。根据不同的证书用途、证书安全保障级别（私钥存储介质、证书申请实体鉴别方式等），部分 CA 机构在其 CPS 中约定了不同场景下的鉴证要求，但没有统一的标准。

2.3 互认互通的需求

2017 年 6 月，《网络安全法》正式施行，网络安全法第二十四条指出：“国家实施网络可信身份战略，支持研究开发安全、方便的电子身份认证技术，推动不同电子身份认证之间的互认。”这对电子认证的互信互认指明了方向。

随着信息化的不断推进和发展，电力行业提出了构建广泛互联、开放共享的新一代电力系统，这对数字证书的互联互通提出了新的需求。但由于历史原因或者技术限制，一张数字证书往往仅能在一个应用或者平台中使用，无法在其他应用或者平台中使用，即无法实现数字证书多证书融合。

3 互认互通可行性分析

3.1 PKI 信任模式

目前在国际上被普遍使用的 PKI/CA 信任模式可以分为 4 种：根 CA 信任模式、桥交叉信任模式、CA 信任模式和信任列表信任模式。

（1）根 CA 信任模式

根 CA 信任模式，也称层次信任模式。在该信任模式下，CA 中心可以分为多级，用户证书由 CA 中心签发，各级 CA 中心之间呈现层次关系。最上级 CA 中心只有一个，称作根 CA，其他 CA 称作子 CA。根 CA 的数字证书由自己签发，属于自签名证书，子 CA 的数字证书由上级 CA 签发。

（2）交叉信任模式

该信任模式下，根 CA 之间可以相互签发交叉认证证书，该交叉认证证书等同于子 CA 证书，网状结构中包含多个 CA，提供 PKI 服务，每个使用者仅信任其证书发放 CA 发放的证书；这些 CA 以点对点（peer-to-peer）模式，也就是互相发给证书方式，达成双向的信任关系。

人民邮电出版社

（3）桥 CA 信任模式

该信任模式下，引入独立的桥 CA 中心，等同于虚拟的根 CA。所有根 CA 与桥 CA 之间相互签发交叉认证证书，实现 CA 之间的互操作，建立互信的环境。其中，桥证书机构（BCA）技术是实现混合体系的一种有效手段。

（4）信任列表信任模式

该信任模式下，用户可以拥有多个信任锚，信任列表结构是一份被认证机构数字签名后包含“所信认证机构根证书”列表的数据结构。因为使用了数字签名技术，因此信任列表模式具有一定的抗篡改能力。使用者可以通过该数据结构中的一大串认证机构的数字证书遴选出其所信任的认证机构， 同时也可以获得其所信任的认证机构的政策依据，是一个既简单又实用的手段。

3.2 信任机制的可行性分析

4 种信任模式在我国都有不少实践案例。

根 CA 信任模式在我国的即有实践案例，国家电子认证根 CA 项目是我国建设统一根信任体系的重要工程，项目由国家密码管理局负责建设。由于受限于基础软件，SM2 证书还未能实现普及，大量的非同根 RSA 证书还在继续使用。从现实情况看，由于存在行业、部门间的协调问题，短期内实现全国统一根还有相当的难度。

交叉信任模式实现较为简单，应用也较为灵活，但由于缺乏统一的管理中心，扩展后的认证路径复杂度难以控制，加之现实中也缺乏推动此认证模式的应用需求，因此网状结构认证模式实际上一直停留在技术层面。

桥 CA 信任模式在我国开始的较早，在 2004 年，为解决各 CA 机构互联互通的问题，国家信息中心提出建设一个“桥证书机构”的 CA 互联互通示范工程项目，作为各个 CA 机构互联互通的桥梁。该项目通过桥证书机构与国内已经建立的 6 家不同行业、不同区域的 CA 机构，经过系统的改造和建设，实现了证书的互联互通和信任域的扩展，为建设我国电子认证服务体系的互联互通做出了示范。

信任列表结构是最为常见且应用最为广泛的交叉认证模式，Windows 系统内预置根证书信任列表就是典型的信任列表模式应用。卫生部、深圳市政府、贵州省公共资源交易中心等应用部门在不自建 CA 的情况下，利用信任列表模式实现了多家第三方 CA 交叉认证。

4 互认互通应用研究实现

4.1 标准支持

互信互认，标准先行。标准规范是技术框架的重要组成部分，国家密码管理局作为电子认证服务机构的主导单位，发布了诸多的和数字证书、电子认证相关的标准规范，主要有《GM/T 0014 数字证书认证系统密码协议规范》《GM/T 0015 基于 SM2 密码算法的数字证书格式规范》《GM/T 0018 密码设备应用接口规范》《GM/T 0027 智能密码钥匙技术规范》《GM/T0033 时间戳接口规范》《GM/T 0043 数字证书互操作检测规范》等。

其中《GM/T 0043 数字证书互操作检测规范》为数字证书的互信互认提供了有力的依据。电力行业在这些标准规范的基础上，结合电力行业电子认证服务的监管思想和市场准入机制，对现有标准规范进行了补充和完善。

4.2 互认互通技术支撑

在数字证书互联互通信任体系下，一个应用系统中使用的数字证书可能由不同的认证机构颁发，不同的数字证书对应的发证体系、信任根、密码算法、设备驱动、应用接口、安全中间件等都存在不同。在解决证书的交叉信任问题后，还需要解决设备驱动、密码算法、应用接口等一系列兼容性技术问题。

数字证书互联互通信任技术框架设计需要面对下列两个方面的问题。

一方面，应用场景较为复杂，大致总结为下列 3 种情况。

（1）在一个应用中支持多家 CA 颁发的数字证书。如网上报税，税务总局要求网上报税系统支持税务证书及其他第三方 CA 证书。

（2）在多个同类型应用系统中实现数字证书互联互通。如不同厂商开发的电子招投标系统，要求系统支持多种证书登入，互认签名数据和文件。

（3）不同类型应用系统实现数字证书互联互通。如电子证照跨省应用、电子口岸互通应用等要求电子证照、电子文件互联互通。

另一方面，不同 CA 颁发的数字证书还存在许多差异，现行的技术和应用管理规范还不能满足应用系统要求数字证书实现互联互通的需求。

建立一套强大的中间件系统同时配套相应的技术及应用管理规范应该是现阶段行之有效的解决方案，

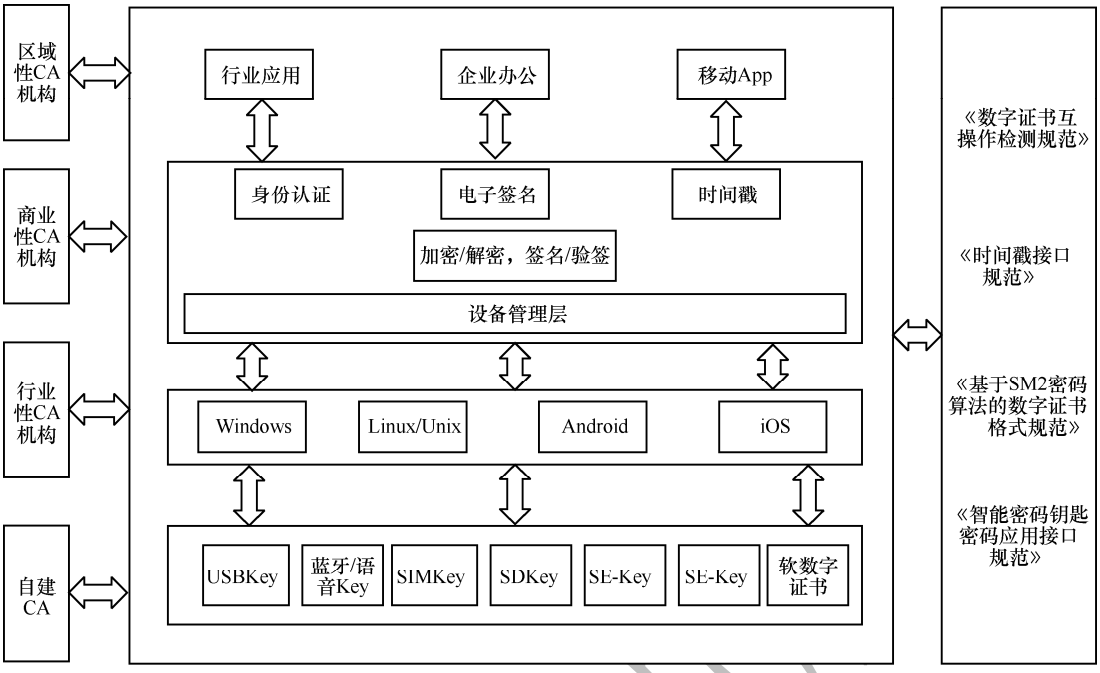


图 1　数字证书互联互通信任体系技术框架

技术框架如图 1 所示。

技术框架的核心是经过抽象的签名、验签、加密及解密等中间件，中间件给上层应用提供了统一的数字证书应用接口。该中间件包含 Windows 系统、Unix 系统、Linux 系统、Android 系统和 iOS 系统的多个版本，涵盖服务端、PC 客户端和移动客户端的应用需求；支持各个 CA 颁发的多种接口类型的数字证书；支持不同算法的数字证书；支持数字证书 CRL 及 OCSP 验证；支持可自主管理的分类信任域。中间件除了面向应用系统提供文件数据签名验签、加解密接口外，还向应用提供电子签章及时间戳等安全应用组件，从而保障使用统一中间件的各业务系统中的文件数据保持兼容性。

4.3　数字证书分类管理机制

在数字证书策略分类分级规范未能完全贯彻执行的情况下，应用系统各参与方直接依赖证书策略规避应用风险的方法并不可行。应用系统建设方对证书信任列表进行分类管理是确定数字证书安全类别的有效手段。

证书信任列表分类管理的方法，即对信任域中不同机构证书设定相应的信任类别，并进行分类管理，为不同机构证书设定不同的权限，提高业务系统自主可控能力及其安全性。

在电力行业应用中，特别是在电力外网应用中，业务系统可能涉及政府机关单位、事业单位、公务员个人、中介机构、本地区企业个人、外地企业个人等众多角色，各类角色由于各种安全要求，都需要使用数字证书。在多种不同安全类别的数字证书混用时，信任域的划分和辨识就显得特别重要。

5　结束语

对电力行业提出“广泛互联、开放共享”要求的新一代电力系统的背景下，各电力企业中使用的数字证书由于提供服务的电子认证机构不同、标准不统一、数字证书中间件不统一、服务标准不尽相同等情况，给电力系统数字证书的“互联互通，互相信任”的发展带来了一定的困难。笔者从电力系统数字证书的现状、互联互通可行性作了分析，并提出了互联互通互相信任的实现方案，供电力企业、各 CA 机构和相关服务商参考。

参考文献：

[1]　王静. 统一身份认证和用户管理平台在集团型电力企业的应用[J]. 信息网络安全, 2016 (12): 81-85.

[2]　赵保华, 王志皓, 王树才. 电力终端可信身份认证技术研究与应用[J]. 网络空间安全, 2018, 9(7): 15-18.

[3]　李玮. 长三角电子认证服务体系互联互通平台的研究与设计[D]. 杭州: 浙江工业大学, 2014.

[4]　贵州公共资源交易互联互通服务平台数字证书和电子印章交叉互

认系统通过专家初验[J]. 建筑市场与招标投标, 2016(5): 22.
[5] 郭亓元, 沈宇超, 岑荣伟. 电子政务数字证书互认平台的研究与设计[J]. 信息安全研究, 2017, 3(6): 548-553.
[6] 曹炀. 建设行业电子认证互联互通的探索[J]. 中国建设信息化, 2016(20): 76-77.
[7] 侯瑞. 电子认证服务的新探索——长三角地区开通数字证书应用交叉互认平台[J]. 信息化建设, 2011(1): 28-29.
[8] 陈广涛. 多 CA 互认互通让网上招投标更便捷[N]. 中国建设报, 2016-10-18(012).
[9] 李琳. 电子招投标系统数字证书兼容互认的探索与研究[J]. 建筑市场与招标投标, 2018(2): 54-56.
[10] 艾瑞咨询. 中国第三方电子签名行业研究报告 2018 年[R]. 2018.
[11] 梁达, 邓家红. 数字证书应用安全中间件的研究与实现[J]. 企业科技与发展, 2014(19): 17-18, 22.

人民邮电出版社

电力行业智慧物联体系研究与设计

葛冰玉，冯志鹏，韩璐，黄文雯，安培秀，李丹丹
（国家电网有限公司信息通信分公司，北京 100761）

摘　要：目前，电力行业信息化已具备一定基础，但仍存在信息感知深度广度不足，各专业感知信息共享、资源复用及新兴业务支撑能力不足等问题。因此，智慧物联体系的研究是必然趋势。目前，多家互联网公司已经开始了智慧物联体系的研究，但缺乏对电力行业智慧物联体系的整体设计。为弥补这一空白，梳理了电力行业智慧物联体系的建设原则，构建了智慧物联体系的整体架构，明确了智慧物联体系的建设重点，设计了物联管理平台的基本功能。同时，也对物联平台的测试方法进行研究，从而保障技术架构的科学合理以及适用性，为电力行业智慧物联体系的研发提供借鉴。

关键词：信息感知；资源复用；智慧物联

1　引言

随着电力行业信息化建设的深入，已基本建成了覆盖各专业的信息系统，支撑了企业管理、生产控制、客户服务等工作的正常开展。但物联网整体建设与应用仍存在不足。（1）感知深度广度不足，用户用能信息感知不及时、配电信息覆盖面不全、新兴业务感知未充分共享。（2）各专业感知信息共享不足、资源复用不足。各专业系统自成体系，存在传感设备重复部署，未实现一次采集、共享共用；感知体系智能化水平不足，无法动态变更应用需求，难以集中统一管控。（3）新兴业务支撑能力不足，在互联网侧缺少感知来源，网络部署结构无法支撑综合能源服务、数据运营等新业态发展[1]。因此，结合泛在物联技术将现有电力系统建成智慧物联网是未来电力能源体系的发展趋势。

2　研究背景与意义

2.1　背景现状

近年来，电力行业不断加强业务各环节信息采集和感知的建设，在发电环节通过部署测控装置实现对电源侧运行状态数据的采集，在输/变/配电环节通过部署运行控制终端、监测终端、巡检机器人、智能巡检设备等实现对输/变/配电设备和运行检修工作的信息采集和控制，在用电环节通过部署智能电表、采集器、自助终端、采集监控设备、专变终端等实现对用电信息采集计量、营销业务支持、信息采集和控制，同时也不断拓展其他业务环节和领域的感知设备应用。电力行业物联网建设在核心业务各环节开展了大量工作，已具备一定应用基础，但仍在感知层建设、数据和业务贯通、体系标准化、新技术应用、网络和安全支撑方面存在不足[2]。

2.2　研究意义

目前，多家互联网公司开展了云物联网的研究，但仍缺乏对电力行业智慧物联体系的研究，为了弥补这一研究的空白，　立足现有实体设备与信息通信技术，建设电力行业智慧物联体系，是电力行业发展的必然趋势[3]。通过建设物联管理平台和边缘物联代理，实现各业务采集终端、传感器、智能终端的数据统一采集、处处使用，同时，向企业中台、业务系统提供标准化数据与服务。协同输变电、配用电等相关专业建设任务，联合打造全面感知、高效处理、应用灵活的企业级智慧物联体系，实现统一物联管理、终端标准化接入和数据共享共用[4]。

3　研究内容

3.1　建设原则

智慧物联体系建设总体技术原则为“边缘智能、统一物联、共享共用、能力开放”。

- 边缘智能

基于硬件平台化、软件可扩展、计算智能化、形

人民邮电出版社

态多样化的原则实现边缘智能。硬件装置遵循通用化、平台化、可扩展，通过 App 平滑升级实现软件功能扩展，基于边缘计算实现就地集成和区域自治，结合具体业务场景建设边端分离或合一的多形态边缘物联代理。

• 统一物联

按照统一的接入标准、通信规约和接口，实现各类终端的统一物联和在线管控；兼顾各专业、各单位的现状与发展，支持多种形式的接入。

• 共享共用

遵循终端、通信、计算、数据等各类资源共享共用的原则，构建跨专业共享的边和端，从源头实现业务融合，基于统一物联模型实现跨专业数据共享和业务流程贯通。

• 能力开放

基于边缘计算框架、接口规范和 App 应用商店，打造开放合作、共建共享、安全可控的国网智慧物联应用生态和产业生态。

3.2 架构设计

智慧物联体系重点建设物联管理平台和边缘物联代理，对下实现各业务采集终端、传感器、智能终端的数据统一采集、处处使用，对上向企业中台、业务系统提供标准化数据与服务。总体架构设计如图 1 所示。

3.3 功能设计

本文构建的物联管理平台包括总部物联管理平台和省级物联管理平台，按照总部—省公司两级部署。其中，总部和省公司物联管理平台通用功能包括连接管理、消息处理、设备管理、应用管理、边缘计算管理、模型管理、标识管理、安全管理、平台管理、运行监控、远程运维管理等功能[5]；总部专有功能包括全网物联调控、全网物模型管理、全网物联应用管理功能。

总部、省公司两级物联管理平台之间通过远程调用、消息总线和文件复制等方式实现物联管理数据传输和协同计算[6]。对于终端设备采集数据，省公司侧由物联管理平台传输至省公司数据中台，再由省公司数据中台上传至总部数据中台。总部物联管理平台实现对物联数据的全网感知，对各省公司物联管理平台“监而不控”。物联管理平台功能设计如图 2 所示。

3.4 测试方法

在测试过程中，从安装部署、能力覆盖、用户体验方面验证物联管理平台的能力。

• 安装部署

验证物联管理平台是否支持自动化部署的方式，是否能够通过部署工具快速将平台进行部署，是否支持与多种边缘物联代理的接入与使用。

• 能力覆盖

一是对物联管理平台本身的功能、性能进行测试，如物模型定义及下发功能、设备接入能力、设备管理能力、固件升级能力等；二是进行非功能性测试，包括可维护性、可管理性、可配置性、松耦合性、可靠性、开放性、安全性等角度对产品进行全面的评估；三是典型应用场景测试，包括电表数据上报、电表数据召测、电表控制指令下发、配电检测数据上报、断路器远程调试等典型场景的测试。

• 用户体验

验证操作界面是否简洁易懂，功能分区是否合理，关键核心内容是否均可直观显示，并有相应的消息提示[7]。

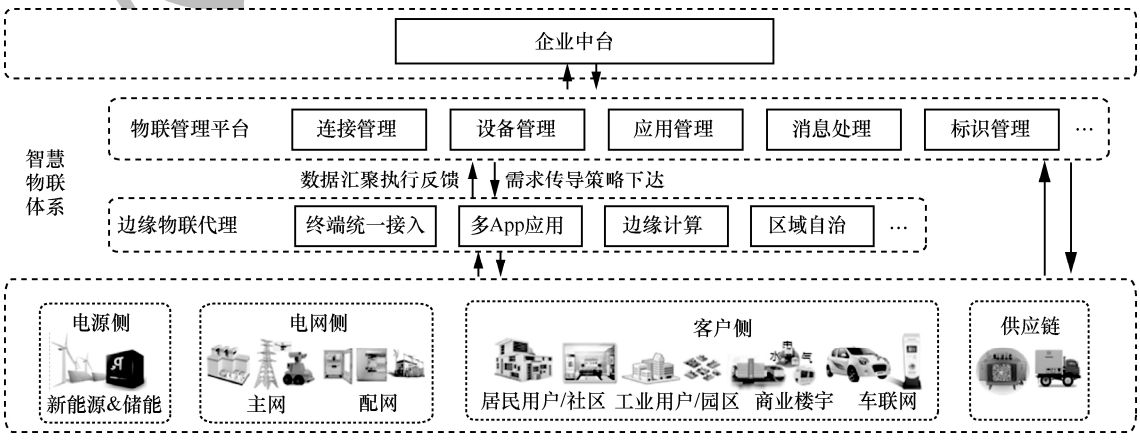


图 1　智慧物联体系总体架构设计

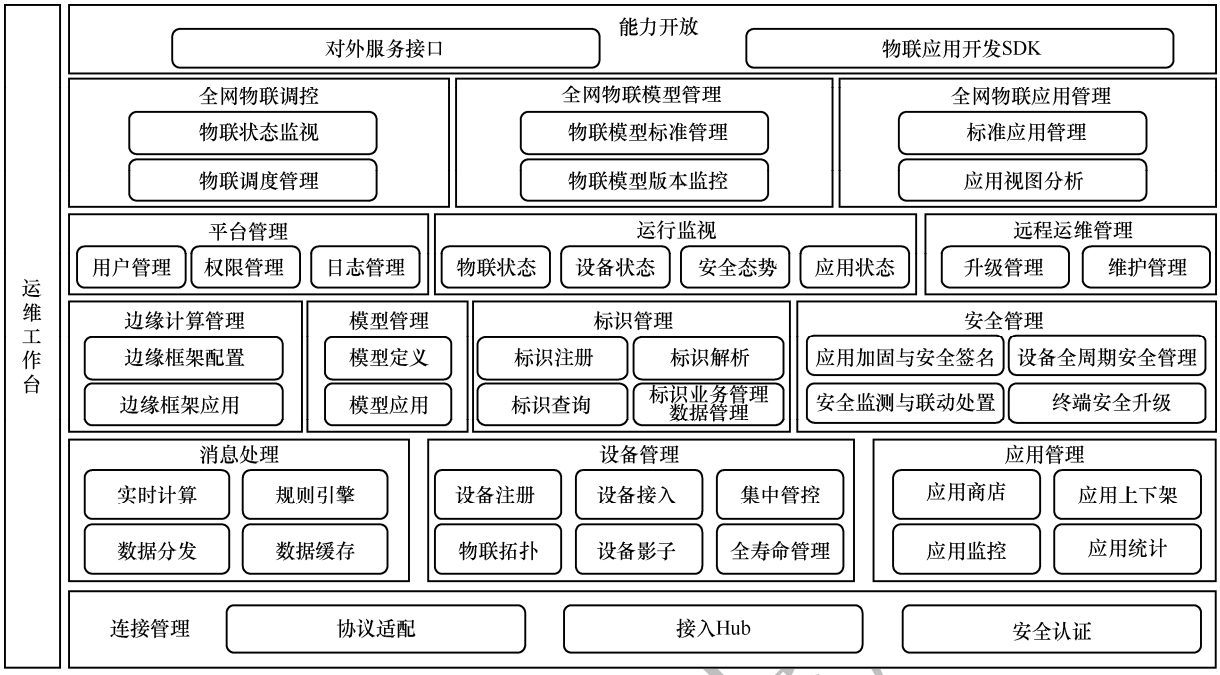


图 2　物联管理平台功能设计

4　结束语

本文在现有实体设备与信息通信技术基础上，梳理了电力行业智慧物联管理体系的建设原则，构建了智慧物联体系的整体架构，并明确了智慧物联体系的建设重点，设计了物联管理平台的基本功能。同时，对物联管理平台的测试方法进行研究，保障技术架构的科学合理以及适用性，通过智慧物联体系的建设，实现各业务采集终端、传感器、智能终端的数据统一采集、数据共享，实现向企业中台、业务系统提供标准化数据与服务。为建设电力行业具有泛在连接、开放共享、融合创新特征的智慧物联体系提供借鉴。

参考文献：

[1]　袁帅. 物联产品应用场景研究[D].黑龙江：东北石油大学, 2018.

[2]　张翠. 基于物联技术的企业电力能效管理方法研究[D].陕西：西安理工大学, 2019.

[3]　BALAJJI S, KATAN N, SANTHAKUMAR R. IoT technology, applications and challenges: a contemporary survey[J]. Wireless Personal Communications, 2019, 108(1): 363-388.

[4]　MEHDI G, GUO J. A context-aware privacy-preserving method for IoT-based smart city using software defined networking[J]. Computers & Security, 2019.

[5]　YASMINE H, ZIBOUDA A, SAAD H. A review of security in internet of things[J]. Wireless Personal Communications, 2019, 108(1).

[6]　FADI A T, MOHAMMED Z H, HUSSAIN A R. Task scheduling in cloud‐based survivability applications using swarm optimization in IoT[J]. Transactions on Emerging Telecommunications Technologies, 2019, 30(8).

[7]　陈博. 物联网运营商的客户忠诚影响因素及作用机理研究[D].北京：北京邮电大学, 2019.

人民邮电出版

电力企业网络安全方案设计与优化

李斌，伍泽军，邓文杰
（中国广核电力股份有限公司信息技术中心，福建 宁德 352000）

摘　要：随着互联网的发展和普及，企业分部与企业总部、企业内部与企业外部之间使用网络互联，更能方便数据的传递、资源的共享，提高企业的工作效率、降低企业的运维成本。然而现在多数企业在架设好企业网络后，没有足够重视网络安全的重要性及企业网络被攻击后可能带来的不良后果。从某电力企业的网络现状出发，指出当前该电力企业网络中存在的安全问题，论述了边界防护对网络安全的重要性，并提出一个合理可靠的网络安全建设方案，确保网络架构的稳定可靠，为该电力企业提供一个良好健康的网络运行平台。

关键词：企业网；网络安全；边界防护；网络架构

1　引言

随着互联网的发展和普及、网络信息技术的发展，社会各行各业对网络的依赖性逐渐增强，网络信息技术的发展正逐步改善人类的工作生活方式，信息安全的重要性不言而喻。网络所面临的安全威胁正在急速增长，如饱和攻击、Web 攻击威胁、蠕虫病毒等。网络病毒的防治已经从“杀”时代进入“防”时代。只有拒病毒于企业网络之外，才能真正地保证企业数据安全。

2　电力企业网络系统概述

电力企业网络系统按区域一般可分为广域网出口区域、本地局域网业务安全隔离区域、数据中心安全防护区域及承包商专网区域。广域网出口区域由电力企业外部网络系统组成，通过运营商广域网专线连接本地局域网业务安全隔离区域；本地局域网业务安全隔离区域由各种通信设备、终端设备互联而成；数据中心安全防护区域包含本地所有系统服务器、数据库；承包商专网区域由各承包商网络系统组成，通过防火墙接入本地局域网。电力企业网络系统如图 1 所示。

3　电力企业网络系统中存在的安全问题

（1）广域网边界安全防护问题

广域网边界作为企业本地局域网与企业外部网络的分界线，是网络的重要组成部分，负责对网络流量进行最初及最后的过滤，因此广域网边界安全的有效部署对整个网络安全意义重大。

企业核心交换机直接通过网线与运营商设备互联，并没有在广域网边界上建立可靠的安全防御体系，外部的安全威胁问题将直接导致企业网络系统的脆弱性。

（2）数据中心安全防护问题

数据中心承载保存着用户的核心业务数据，为企业内部及外部用户提供业务服务和数据交换，因此在数据中心建设过程中，安全体系建设成为一个不可或缺的主题，只有规划设计合理的网络安全方案，设计提供持续的安全加固，才可以保证企业网络平台的安全可靠。

目前该电力企业数据中心汇聚交换机直连核心交换机接入网络系统，没有采取任何必要的安全防护措施，网络中存在的非法访问以及恶性攻击入侵和破坏等问题，对网络数据的安全性构成直接威胁。

（3）承包商网络安全访问问题

目前该电力企业工程承包商通过防火墙直接访问电力企业内部业务系统，防火墙可对网络进行隔离控制，通过设置安全策略实现严格的访问控制，只允许必要的流量通过防火墙，阻止其他未授权的访问。然而工程承包商终端设备不同于企业内部终端设备，没有要求安装企业规定的安全防护软件，未加以控制可随意访问互联网，极易被植入病毒、木马、蠕虫等。

人民邮电出版社

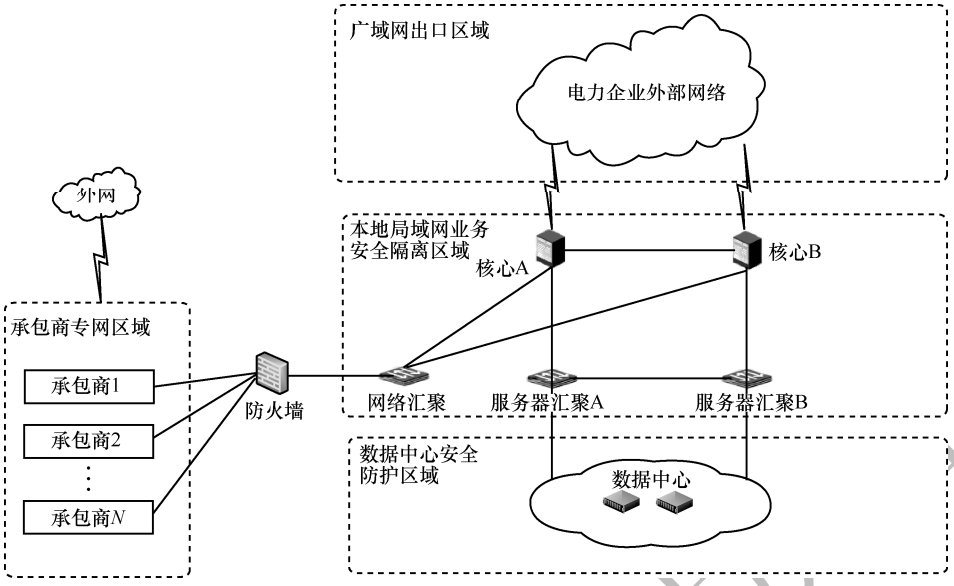


图 1　电力企业网络系统

工程承包商终端通过防火墙直接访问企业内部资源，使企业内部网络系统存在被病毒、木马、蠕虫等入侵攻击而造成传播破坏的危险。通过公共网络访问还存在数据信息泄露风险。

（4）运维管理及日志审计问题

目前该电力企业没有运维审计机制，无法实现集中有序的运维操作管理，从而防止非法、越权访问事件发生，给企业信息系统安全运行带来较大的潜在人为安全风险。随着企业资产数量日趋增多，大量网络设备、应用系统等每天会产生大量不同格式的日志，且分散存储在不同的位置，企业无法通过人工去分析管理日志，无法及时识别针对信息系统的入侵攻击、内部违规等信息，存在事后取证难等问题。

（5）电力企业内部安全防护问题

除了做好网络边界安全防护外，还需防范其他未知内部威胁，例如加密和非加密黑客远程通信控制、钓鱼邮件、攻击渗透、后门通信、黑客入侵攻击、用户内部违规行为等。提升未知威胁发现能力，构建内部已知及未知威胁和网络边界纵深防御体系迫在眉睫。

4　网络架构设计注意事项

企业网络系统的组网方案主要要素包括局域网、广域网连接、网络管理、安全性等。具体来说，企业组网方案设计时的注意事项如图 2 所示。

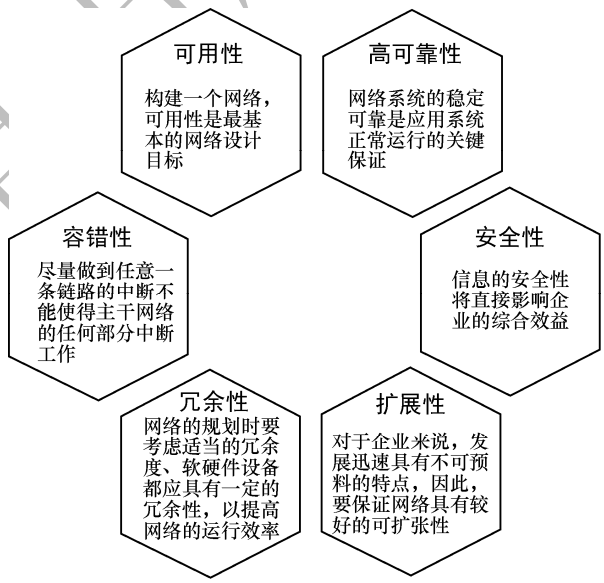


图 2　网络组网方案设计注意事项

5　网络安全方案设计要点

电力企业网络安全方案在设计过程中要注意保持整体性原则。网络从被攻击到恢复一般需要经过 5 个阶段：预警阶段、攻击防范阶段、攻击检测阶段、响应阶段和恢复阶段。这些都是网络安全系统的组成部分，因此提高企业网络安全管理能力可以从以下几个方面考虑。

（1）提高员工自身的网络安全意识

大部分网络安全漏洞问题是员工的疏忽和渎职而

直接或间接造成的，因此提高员工自身的网络安全意识，加强员工的信息安全管理是实现信息安全的根本。

（2）用户访问控制

企业可以通过部署专业防火墙对用户访问实施精确控制，防火墙部署于企业内部网络和外部网络、企业内部网络各区域之间，可以对流量进行监控、过滤，可依照特定的源地址、目的地址、服务端口等规则对数据流进行限制。部署防火墙后，入侵者首先需通过防火墙后才能进入目标设备。防火墙大体可分为网络层防火墙和应用层防火墙，网络层防火墙是对 OSI 三层及以下的防护，针对特定的端口、特定的源和目的地址设置安全防护策略；应用层防火墙可以对 OSI 七层进行防护，功能接近于入侵保护系统。

（3）使用 VPN 技术

VPN 全程虚拟私有网络，主要采用 4 项技术来保证安全，分别是隧道技术、加/解密技术、密钥管理技术及身份认证技术。VPN 可在公共网络之上为企业构筑安全可靠、方便快捷的私有网络，例如，出差员工可以通过使用 VPN 提供安全的远程接入，访问企业内部网络。

（4）使用入侵检测防御、防病毒技术

入侵检测防御系统能够对网络、数据造成危害的恶意行为进行检测和防御，及时识别攻击程序或有害代码及其克隆和变种，采取预防措施，先期阻止其入侵，防患于未然。防病毒系统可对病毒等恶意软件进行防御，可以防护各类病毒和恶意软件，对其进行隔离和清除，降低因恶意软件传播带来的安全威胁，及时发现并限制网络病毒爆发疫情。

6 电力企业网络安全优化实例

6.1 优化方案

优化企业各区域边界，加强网络边界安全防护。在企业连接承包商专网区域边界增加部署入侵防御系统、防病毒网关等网络安全设备，防止企业内部网络系统被病毒、木马、蠕虫等入侵攻击。使用上网行为管理规范承包商用户访问外网行为，上网行为管理融合了应用控制、行为审计、网络业务优化等功能，为承包商用户提供一个综合完整的企业务应用场景解决方案。

在企业广域网出口区域与本地局域网业务安全隔离区域边界以及本地局域网业务安全隔离区域与数据中心安全防护区域边界旁挂 4 套防火墙、入侵防御系统、防病毒网关等网络安全设备，加强区域间访问控制，防护各类病毒和恶意软件，对其进行隔离和清除，及时识别攻击程序或有害代码及其克隆和变种，防止被恶性攻击入侵和破坏，防患于未然。

在网络系统中增加部署堡垒机、日志审计系统、安全态势感知平台等设备，加强运维管理、日志审计分析，直观、准确地对网络安全事件进行发现、预测和反向追踪，找到攻击源。电力企业网络安全优化方案如图 3 所示。

6.2 价值点

工程承包商用户使用 SSL VPN 通信方式通过防

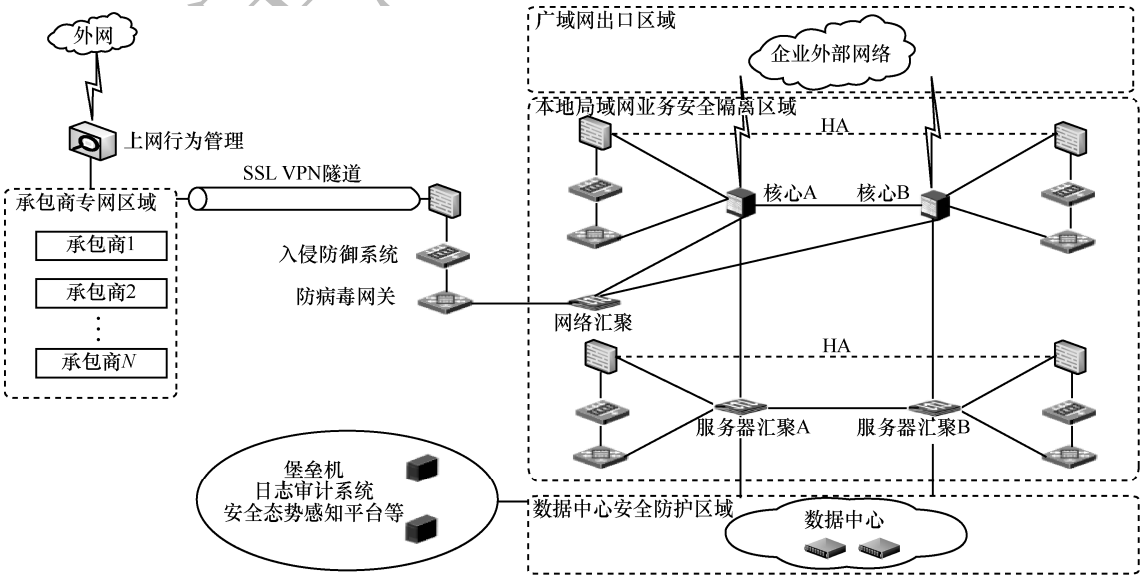


图 3　电力企业网络安全优化方案示意图

火墙代理访问企业指定内部服务器，SSL 是一个安全协议，数据是全程加密传输的，SSL 网关隔离了内网服务器和客户端，只留下一个 Web 浏览接口，客户端大多数木马病毒感染不到内网服务器，为工程承包商用户访问内部资源提供了一种安全可靠的连接方式。

防火墙、入侵防御系统、防病毒网关等网络安全设备通过旁挂方式增加部署在核心或服务器交换机上，通过心跳线互联做主备。旁挂部署可采用二层模式旁挂部署，或交换机使用 VRF 虚拟化技术采用三层模式旁挂部署。不改变企业原有网络结构，网络安全设备出现硬件故障、掉电等意外情况时可远程快速恢复网络。

7 结束语

随着计算机网络信息技术的发展，影响计算机网络安全的因素也必然增多，网络安全解决方案也要与时俱进。首先要遵循相关的网络安全管理法规和制度，制定实施企业内部信息安全管理规定，然后要加强用户的安全意识，最后可以定期对终端进行扫描杀毒，依靠防火墙、入侵检测等硬件设备来进行安全防护，利用身份认证、数据加密、访问控制等软件技术来解决网络安全隐患，不断探索、维护网络安全的有效措施，设计合理稳定的解决方案，提高网络的安全性。

参考文献：

[1] 朱海虹. 浅谈网络安全技术[J]. 科技创新导报, 2007(32): 32.
[2] 肖军模, 刘军, 周海刚. 网络信息安全[M]. 北京: 机械工业出版社, 2006.
[3] 王瑞梁. 新时期企业网络管理的现状及对策研究[J]. 电脑知识与技术, 2017, 13(2): 47-48.
[4] 李艺文. 计算机网络安全现状分析与防御技术探讨[J]. 信息系统工程, 2018(3).

人民邮电出版社

电力通信运行支撑系统不中断迁移上云方案

杨志敏，洪丹轲，谢俊毅
（中国南方电网电力调度控制中心，广东 广州 510525）

摘　要：云计算技术被广泛应用于改造和新建新一代信息通信系统。对电力通信网运行技术支撑系统迁移上云工作开展了研究，提出了一种确保系统不中断地迁移上云的方案，并介绍了其在电力企业的实践情况。迁云后的系统充分应用了云平台的优势，提升了系统可靠性、显著改善了用户体验，为通信网运行工作提供了不间断、高性能、高可靠的技术支撑。同时最大程度利用了存量的软件资产，实现了资产保值。

关键词：电力通信网；运行支持系统；云平台；高可用

1　引言

电力通信网是电力行业通信专网，是电力系统的重要组成部分[1]，是保障电网安全稳定运行的基础性资源[2]。保障通信网安全可靠运行是保障电网安全稳定运行的内在要求。

随着电网安全生产对通信可靠性要求的不断提高，保障通信网安全可靠运行的难度也明显增加；随着通信网规模扩大，运行工作量增加明显；随着通信网新技术的发展与应用，通信网的驾驭难度显著增加。为此，通信运行工作必须依靠科技进步。

通信网运行的技术支持系统，为通信网安全可靠运行提供智慧的技术支撑，主要包括通信网资源管理、综合监视、运行控制、统计分析等功能，也为通信网运行监控、资源调度、运行工作管控和专业管理工作提供先进的技术支撑[3]。

国内的电力通信运行技术支撑系统建成于2010 年左右，基于当时成熟和先进的技术，硬件平台基于小型机物理服务器搭建[3]，数据管理采用Oracle 关系型商业数据库。系统应用软件定制化开发并逐年迭代更新，能较好地支撑通信运行工作。当前系统存在的主要问题是硬件平台面临超期服役问题，亟需更换。继续沿用原来的独立物理服务器组网还是迁移至云平台[4]，是硬件更新可选的两种技术路线。

随着信息通信技术的发展，云计算产业已经高度成熟，云平台具有业务上线周期短、运维自动化程度高、系统高可用性、云组件功能丰富、技术经济性好等优点，参考文献[5]-[8]介绍了云计算的技术、应用及发展情况。云计算已被各行业广泛用于建设和改造信息通信系统，参考文献[9][10]介绍了云计算平台在电力信息化、电力调度方面的应用。中国南方电网有限责任公司已经建设完成了调度云平台，因此，将通信运行管控系统迁移至云平台是安全和技术经济综合最优的方式。

鉴于电力通信网运行支持系统的技术特性和网络复杂性，一方面系统逻辑关系复杂，关系型数据库脚本数量多且相互依赖关系强；另一方面，系统部署在安全 III 区和安全 II 区，与通信网管有数据交互需求，系统应用功能主要部署在安全 III 区。因此现有的研究成果均以全系统整体迁云为主，难以直接应用，且尚未查阅到基于云平台的电力通信网运行技术支撑系统迁移方法方面公开发表的研究成果。

本文介绍了一种将通信网运行支撑系统不中断业务迁移上云的方案和具体实践，支持基于小型机物理服务器的硬件平台向云平台平滑演进、不中断业务，充分利用原有软件和中间件资产，实现迁移期间对通信运行支撑工作不中断、随时可回退的高可靠、技术经济最优的迁云解决方案。

2　系统迁云的基础条件及约束

2.1　基于小型机的系统现状

基于小型机物理服务器的通信运行管控系统现状如图 1 所示，主要特性如下。

（1）硬件系统主要包括 5 部分，分别为：安全 II 区采集网管数据的采集服务器及其网络、安全 III 区的

人民邮电出版社

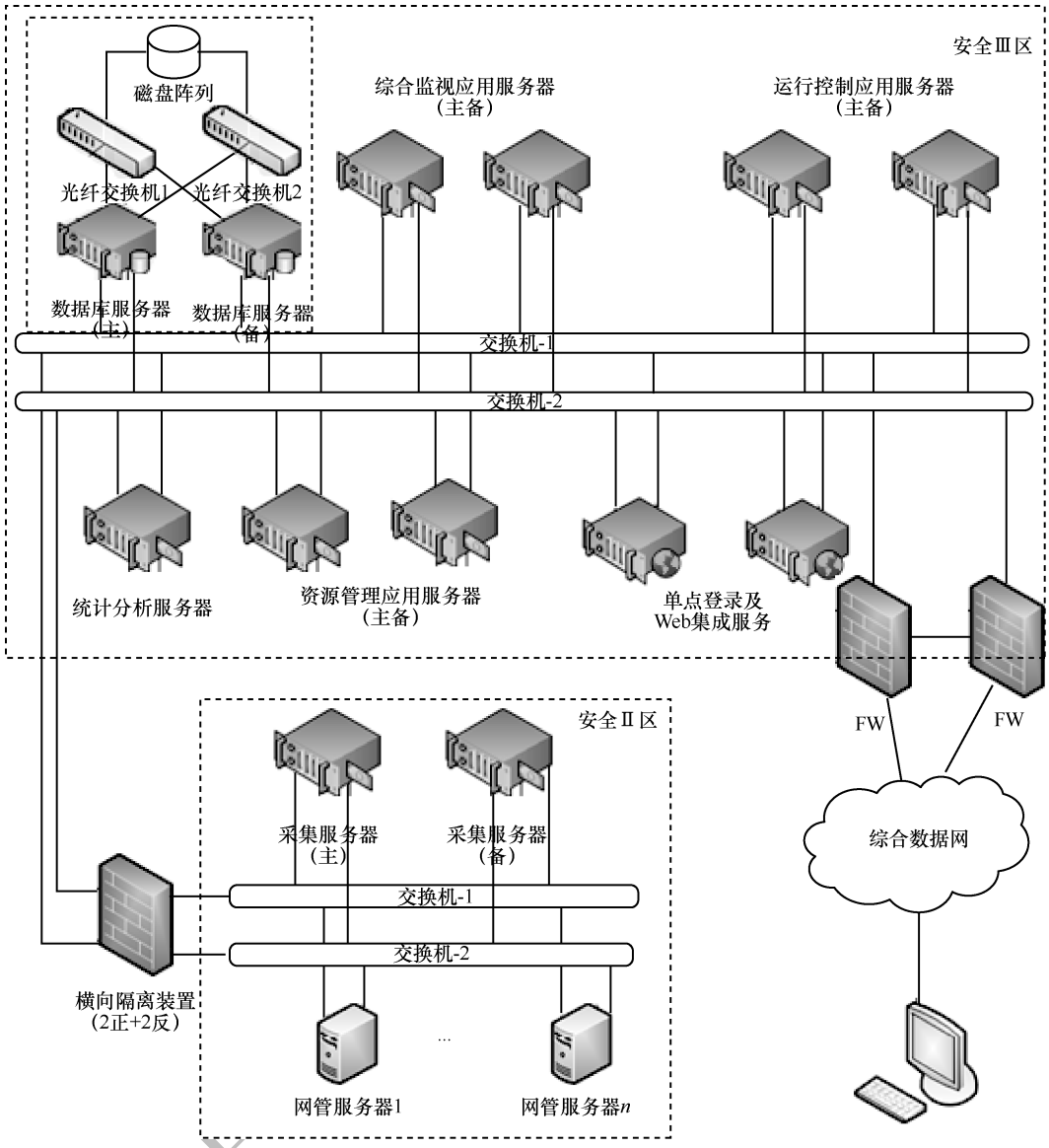


图 1　基于小型机物理服务器的系统现状

数据库服务集群、安全 III 区的应用系统及其网络、安全 II 区与 III 区边界的横向安全隔离装置以及安全 III 区与用户边界的安全防护设备。

（2）数据库及数据管理方面，使用 Oracle 关系型数据库软件管理和存储结构化数据，数据库设备为光纤磁盘阵列。非结构化数据（如附件等）存储在各应用系统服务器的本地磁盘中。

（3）应用系统功能主要包括五大块业务，分别为资源管理、综合监视、运行控制、统计分析、单点登录。

2.2　云平台基本情况

为迁云后的通信运行管控系统提供计算服务的云平台基本情况如下。

• 部署于安全 III 区。

• 提供的云计算基础资源包括云主机（虚拟服务器）、云存储、云网络、云安全防护等。

• 提供的关系型云数据库为 MySQL。

• 其他相关云组件。

2.3　系统迁云应遵循的原则与约束条件

根据保障电网安全生产工作要求和资产保值要求，结合通信运行管控系统现状，本次系统迁云改造工作应遵循的原则与约束条件如下。

（1）软件资产最大化利用。

（2）系统可靠性更高，用户体验更佳。

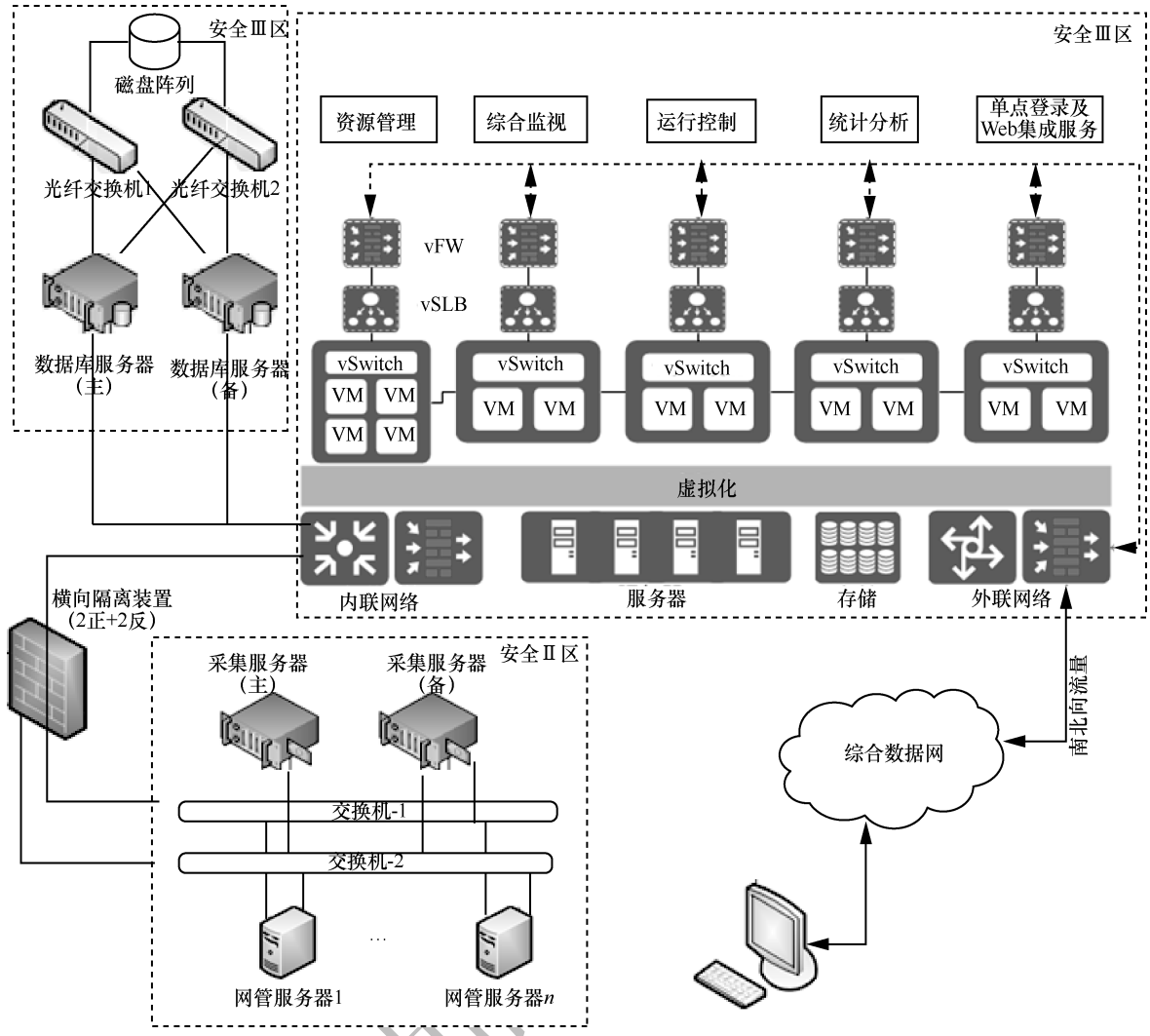


图 2　基于云平台的目标系统架构

（3）可不涉及新功能开发，但要求系统原有功能不删减、数据不丢失。

（4）改造过程中，始终保持通信运行管控系统的运行不中断，为通信运行工作提供随时可用的技术支撑，以保障通信网安全可靠运行。

一方面，云平台相对物理服务器而言，天然具有更高的可靠性，且云平台的计算能力显著优于 10 年前的小型机；另一方面，把现行物理服务器上运行同版本、同配置参数的应用系统部署到云主机上，把系统切换前的数据库拷贝到云系统，可实现迁云前后功能一致、数据一致。

因此系统从基于小型机物理服务器的硬件平台迁移至云平台后，天然可满足条件（2）和条件（3）。而如何满足条件（4）实现全程不中断平滑迁云是最具技术挑战性的工作，也是迁云工作的难点。

3　系统不中断迁云方案

3.1　总体方案及系统架构

迁云前的云下系统硬件共包括 5 个部分，逐个分析其局部方案。

（1）安全 II 区采集服务器及其网络，考虑到采集功能单一、采集服务器数量少、网络安全管控要求网络专用等因素，综合技术经济分析，该部分不适合迁云，依然保留其网络结构和系统结构。

（2）数据库方面，考虑到本系统使用的关系型数据库是 Oracle 数据库，而云平台提供的关系型数据库是 MySQL 数据库，两者存在部分底层代码不兼容的问题，若数据库需要从 Oracle 迁至 MySQL，则需对不兼容的数据库语句（脚本）进行逐条修改和测试。经统计，本系统共有数据库语句（脚本）数量超过 10

万条，且语句（脚本）之间的依赖、关联关系复杂，单一语句的问题可能导致大面积的报错，修改和测试工作量巨大并且难以在短时间内完成、系统出错宕机的风险大，因此数据库短期内不适合迁至 MySQL。另一种方法是购买云平台的 Oracle 数据库授权，但需要一笔费用不低的新投资，且原 Oracle 数据库资产无法再利用，不满足软件资产最大化利用的迁云原则。因此数据库暂不迁云。

（3）安全 III 区的应用系统及其网络，该部分应用系统服务器多、变化快、对运维自动化需求高、应用需求和部署要求多变，正适合迁云至云平台，应充分运用云平台的优点来改进系统，整体迁移至云平台。

（4）安全 III 区与用户边界安全防护设备，因安全 III 区系统已全部迁移至云平台，可充分利用云平台提供的安全防护设施，因此该部分的边界安全防护设备可取消。

（5）安全 II 区至 III 区隔离装置，因安全 III 区系统已经迁移至云平台，因此隔离装置的外网侧需要调整运行方式，实现与云平台安全对接。

根据上述总体方案分析，通信运行管控系统迁移至云平台后的目标系统整体架构如图 2 所示。

主要特性如下。

（1）安全 III 区业务系统全部迁移至云平台，5 个业务系统全部配置主备双虚拟机服务器，主备服务器部署相同版本的应用程序，通过虚拟防火墙进行安全加固，通过虚拟负载均衡实现主备双机实时热备和负载均衡。

（2）鉴于安全 III 区云平台未采购商业化的关系型数据库，为实现原有 IT 资产的利用效率并兼顾系统应用程序的数据库兼容性，仍然将安全 III 区数据库放在云下单独运行，应用小型机物理服务器组成集群，数据库运行在实时热备状态，通过浮动 IP 地址为安全 III 区云平台及安全 II 区采集系统提供关系型数据库服务。

3.2 迁云实施方案

为确保通信运行管控系统在业务不中断情况下实现图 2 所示迁云目标，系统迁云实施方案包括 5 个阶段，如图 3 所示，主要过程如下。

（1）S0 准备阶段

主要完成云平台资源分配、地址规划等各项准备工作。

（2）S1 云系统部署与测试阶段

主要实现安全 III 区业务系统的上云部署并完成闭环测试。为实现完整运行测试，需要部署一台线下的 Oracle 数据库，用于云上系统的功能验证测试。云上系统各个业务均主备部署应用服务，软件版本及参数与云下当前运行的系统一致。

（3）S2 云系统并网阶段

云系统通过闭环测试后，接入云下生产运行环境的数据库，并与安全 II 区的网管采集系统打通数据，开展并网测试。

（4）S3 云上/云下系统双轨运行阶段

云系统通过并网测试后，对生产用户群开放，实

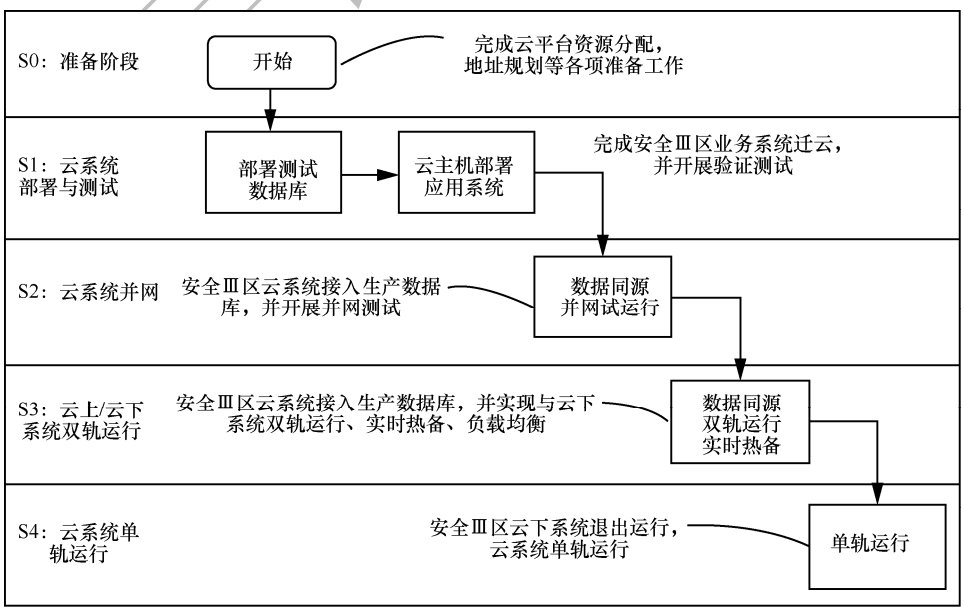


图 3　系统迁云实施方案流程

现与云下系统双轨运行、实时互为热备和负载均衡。

（5）S4 云上系统单轨运行阶段

双轨运行完成，并充分验证云系统的可靠性之后，将云下系统退运，实现云上系统单轨运行。

4 系统不中断迁云实践

4.1 S1 云系统部署与测试实施

完成 S0 准备阶段工作之后，开始 S1 云系统的部署与测试工作，主要包括云下测试数据库（临时）搭建、5 个业务系统云上部署、系统闭环测试 3 部分工作。

测试用的临时数据库使用 Oracle 数据库，与生产运行数据库版本一致。云上系统的 5 个业务均主备部署应用服务，软件版本及参数与云下当前运行的系统一致。系统通过虚拟防火墙进行安全加固，通过虚拟负载均衡实现主备双机实时热备和负载均衡。

该阶段工作期间，当前运行的云下生产系统不做任何调整，维持原方式运行，继续为通信运行工作提供技术支撑。该阶段工作完成后，云上测试系统作为施工调试区域，与云下生产运行系统的对比如图 4 所示，云上系统与当前运行系统完全独立、互不干扰，测试用户通过综合数据网访问测试云上系统。

4.2 S2 云系统并网实施

完成 S1 云系统部署与测试工作后，开始 S2 云系统并网运行工作。该阶段，云系统会断开测试用的临时数据库，改为接入云下生产运行环境的数据库，并与安全 II 区网管采集系统打通数据，开展并网测试。该阶段的云上、云下系统运行方式如图 5 所示。

该阶段，云下生产系统继续按照原来的方式对通信运行工作提供技术支撑。云上、云下系统使用相同的数据、相同的功能，但云系统仅做并网测试，针对试运行用户发布使用。该阶段，云下系统开展的业务，也可在云上系统开展。

4.3 S3 云上云下系统双轨运行

完成 S2 云系统并网运行工作后，开始 S3 云上、云下系统双轨运行阶段工作。该阶段的运行方式如图 6 所示，系统硬件连接方式和数据流方面与图 5 基本一致。双轨运行阶段，云上系统和云下系统同时对生产用户群开放，并实现实时互为热备、负载均衡，共同为通信运行工作提供技术支撑。

为减少双轨运行对用户使用的干扰，同时为实现系统平滑切换，利用云下系统的单点登录主备服务器，部署了基于 Nginx+keepalived 方案[11]的双轨运行架构，如图 7 所示，实现反向代理和云上云下负载均衡，主要特性如下。

（1）反向代理功能

对外向用户公布双轨运行系统的访问地址为浮动 IP 地址，该 IP 地址为虚拟 IP 地址，其不属于具体的主机。用户访问系统时，该浮动 IP 地址根据既定的策

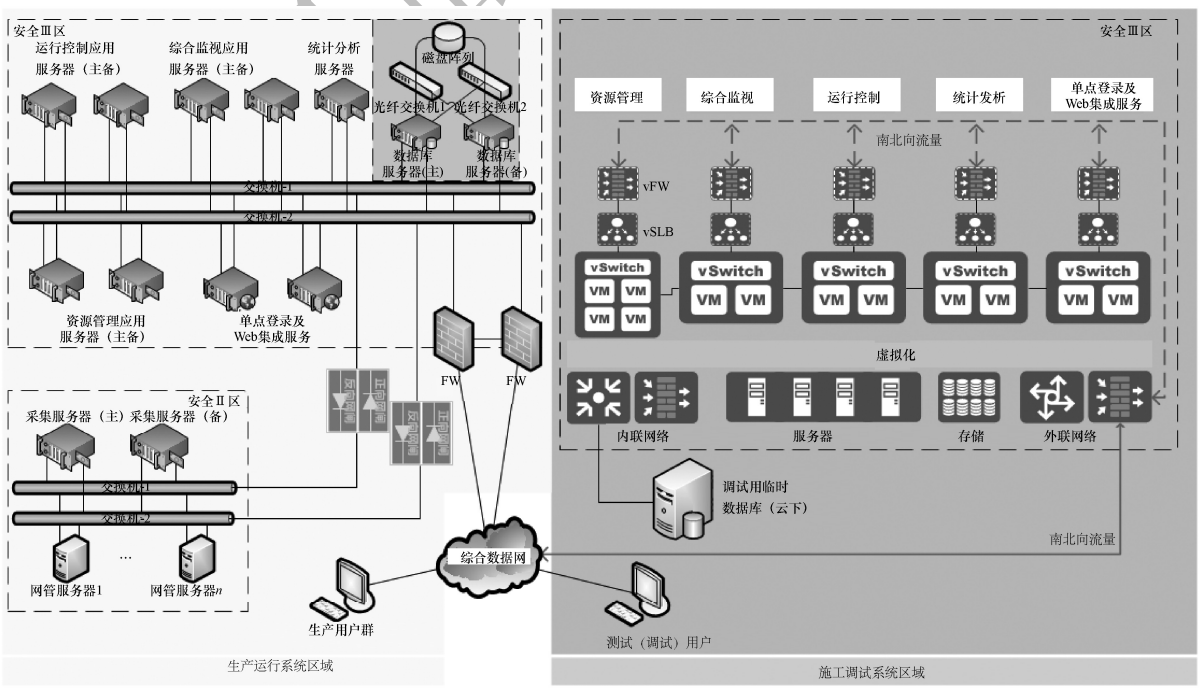


图 4 S1 云系统部署与测试阶段成果

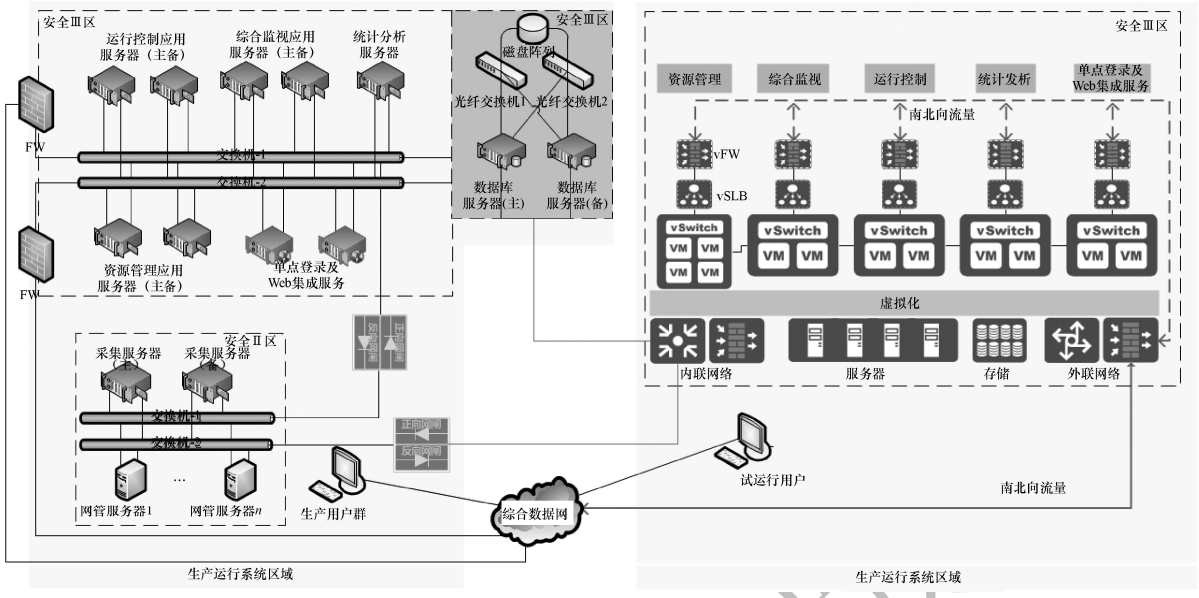


图 5　云系统并网运行方式

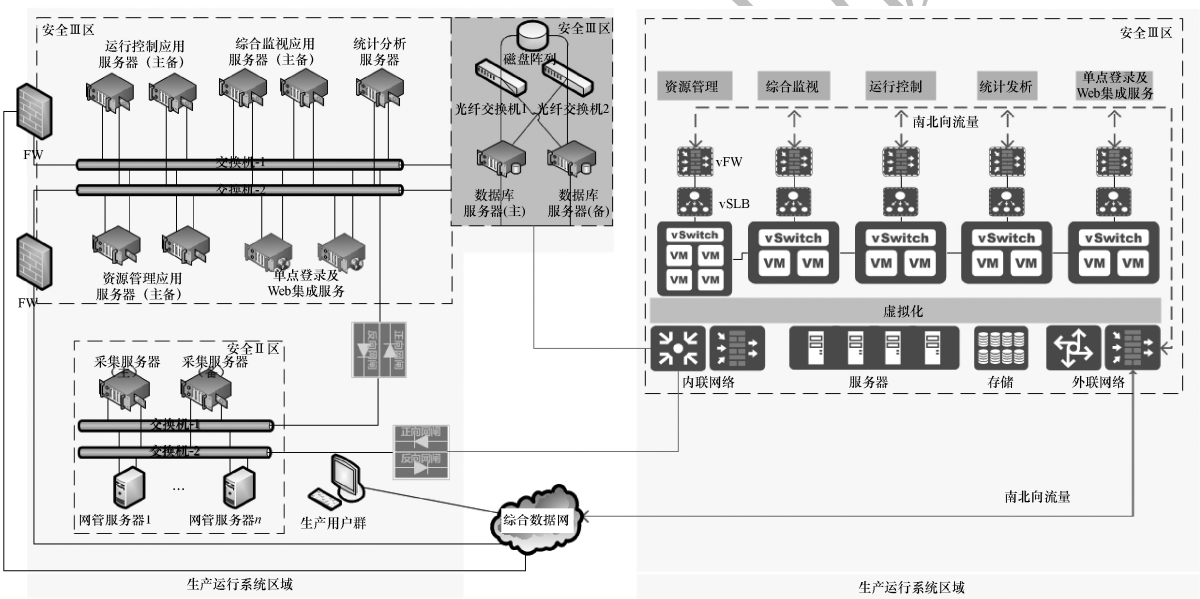


图 6　云上云下系统双轨运行方式

略将用户的访问连接指向云上系统或云下系统对应的主机。云上和云下业务系统主机的实际 IP 地址无需对外公布，既有利于网络安全防护工作，也免去了用户要记录多个 IP 地址并选择访问哪个系统的问题。

（2）双轨系统实时热备和负载均衡功能

Nginx+keepalived 方案可设定多种负载均衡策略，实现云上系统和云下系统的负载均衡[12,13]。双轨运行初期，设置云下业务系统权重较高、云上业务系统权重较低，将用户访问更多地导入到云下系统处理。随着双轨运行工作的不断推进，逐步增加云上系统的权重、降低云下系统的权重，逐步将用户访问导入云上系统处理。这种通过设置双轨系统权重的方式实现负载均衡的策略，实现了系统由云下平滑地向云上切换运行，任何时候任一系统出现故障，均不会中断系统，对用户而言不会有知觉、也不会造成任何影响，同时留给管理员足够的时间处理缺陷。

（3）双重化

Nginx+keepalived 软件双机部署，通过心跳线协同工作，不会发生因 *N*-1 问题导致系统对外服务中断的问题。

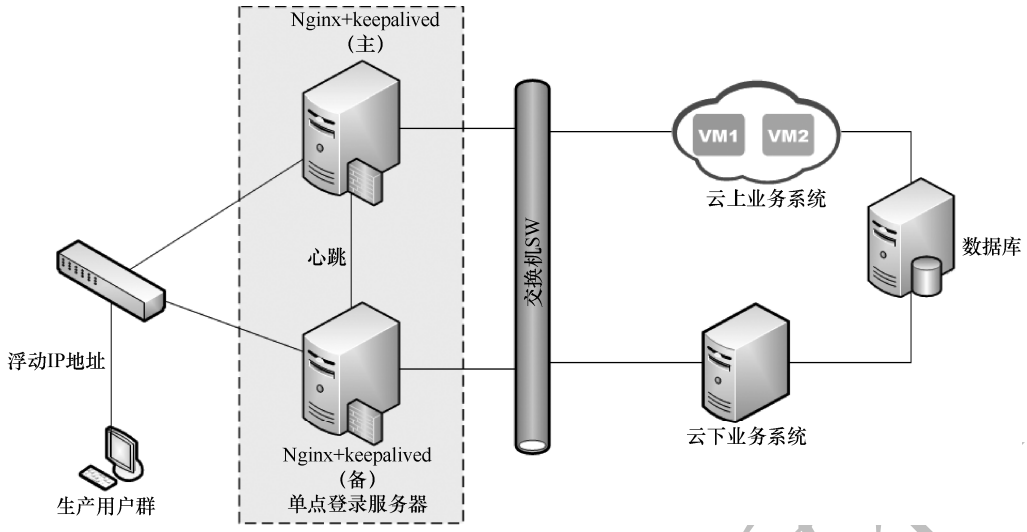


图 7　基于 Nginx+keepalived 方案的双轨运行架构

4.4　S4 云系统单轨运行

完成 S3 云上云下系统双轨运行期后，开始 S4 云上系统单轨运行阶段工作。在图 7 所示的双轨架构中，在运行后期将云下系统的权重设置为 0、云上系统权重设置为 100%，便实现了系统从双轨运行向单轨运行切换，观察系统单轨运行一个周期后，若遇到问题，可随时通过调整负载均衡权重的方式回滚到双轨运行方式。

确认云上系统具备单轨运行条件后，将对外向用户公布的系统访问地址设置为云上系统业务主机对应的虚拟负载均衡的浮动 IP 地址，并同时可将安全 III 区的云下系统应用服务器退出服务，实现图 2 所示的通信运行管控系统迁云后的目标系统架构单轨运行。

5　应用成效

本文所述的通信运行管控系统不中断迁移上云的方案在电网公司总部系统中进行了实践应用。云平台采用公司统一的调度云，基于 x86 服务器，云平台使用飞天操作系统。

目前已经完成系统不中断迁移上云工作，处在双轨运行阶段，并完成了从双轨向单轨运行的切换试验，云上系统具备了单轨运行的条件。因双轨运行观察周期尚未完成，双轨运行向单轨运行切换试验完成后，重新切换回到双轨运行阶段，当前云上系统和云下系统的权重均为 0.5，下一步将逐步加大云上系统的权重，平滑过渡至云上系统单轨运行。

方案实施期间，云下系统安全、平稳、有序运行，未出现因迁云工作导致的系统中断故障，为通信运行工作提供了不间断的技术支持，实现了系统不中断迁移上云的目标。

经过不断调优和迭代改进，云上系统运行稳定，系统可抗任意 *N*-1 故障，系统可靠性明显提升。相对云下 10 年前的运算资源，云上系统的运算能力进步明显，系统响应用户操作请求的时间明显缩短，用户体验改善明显。以通信资源管理模块传输网链路 *N*-1 分析功能为例，某 10 Gbit/s 光纤链路承载各类通信通道 854 条，对该链路做 *N*-1 故障分析测试。系统测试工作均在系统启动后立刻开展，取 3 次测试平均值，云下系统耗时为 32.4 s，云上系统耗时 12.9 s，响应速度提升约 60.2%，效果明显。

云上系统与云下系统的软件版本和配置完全一致，确保了系统功能不删减。云上系统使用原数据库，确保了数据不丢失，也实现了软件资产的最大化利用目标。

6　结束语

本文在分析电力通信网运行支持系统的技术特性和网络复杂性的基础上，研究了系统迁移上云的若干问题，提出了一种确保系统不中断迁移上云的方案，并完成了实施工作，验证了方案的可行性，实现了系统迁云工作安全、有序、平稳开展和云下系统平滑切换至云上运行。

系统迁移到云平台后，运行稳定，可靠性提升，用户体验改善，为通信网运行工作提供了不间断、高

人民邮电出版社

性能、高可靠的技术支撑。同时最大程度上利用了存量的软件资产，实现了资产保值。

该方法还可以被应用到对数据物理安全敏感的系统迁移至公有云的实施工作中，保留数据库不迁云，应用系统迁至公有云。既利用了云计算的优点，同时也消除了数据物理安全的担忧，确保数据存储和管理均本地可控。

下一步，针对云平台提供的丰富组件，如大数据组件、人工智能组件等，可开展云组件应用于通信运行技术支持系统的新功能研发工作。

参考文献:

[1] 汤涌. 电力系统安全稳定综合防御体系框架[J]. 电网技术, 2012, 36(8):1-5.

[2] 郝福忠. 电力系统现代通信技术[M]. 郑州：郑州大学出版社, 2012.

[3] Q/CSG 1204019-2016, 南方电网通信运行管控系统技术规范[S].

[4] 刘沛东, 安博, 钟业弘, 等. 私有云环境下基于虚拟集群的资源共享方法[J]. 计算机科学与探索, 2017, 11(8):1204-1213.

[5] 罗军舟, 金嘉晖, 宋爱波, 等. 云计算：体系架构与关键技术[J]. 通信学报, 2011, 32(7):3-21.

[6] 张建勋, 古志民, 郑超. 云计算研究进展综述[J]. 计算机应用研究, 2010, 27(2): 429-433.

[7] SINGH B, DHAWAN S, ARORA A, et al. A View of Cloud Computing[J]. International Journal of Computers & Technology, 2013, 4(2b1):50-58.

[8] 武志学. 云计算虚拟化技术的发展与趋势[J]. 计算机应用, 2017, 37(4): 915-923.

[9] 李如初, 沈名龙, 彭海棠. 大数据、云计算在电力工业中的应用[J]. 电信科学, 2018, 34(4): 151-155.

[10] 王桂风, 耿向华. 云技术在电网资源调度系统中的应用研究[J]. 电源技术, 2017(11): 146-147.

[11] 肖佳, 王古城, 杨旭,等.双机热备与负载均衡的设计与实现[J]. 电子设计工程, 2015, (18): 176-179.

[12] 陈沛, 马卫东. 一种基于 Nginx 的负载均衡算法实现[J].电子设计工程, 2017, (19): 19-22.

[13] 戴伟, 马明栋, 王得玉. 基于 Nginx 的负载均衡技术研究与优化[J]. 计算机技术与发展, 2019(3): 77-80.

人民邮电出版社

电力系统 IMS 话务预测模型研究

王晓东[1]，范秉旭[2]，叶欣[1]，苑晓东[1]
（1.中国电力工程顾问集团东北电力设计院有限公司，吉林 长春 130021；
2.国家电网内蒙古东部电力有限公司，内蒙古 呼和浩特 010000）

摘　要：随着程控交换设备逐渐淡出市场，电力系统开始引入 IMS（IP multimedia subsystem，IP 多媒体子系统）技术体制作为电力行政交换网的演进方向。IMS 技术与传统程控交换技术有着本质的技术体制区别，电力系统行政交换网相对于公网也存在独有的企业网特点。对电力系统 IMS 行政交换网的各类话务特点进行分析，并对 IMS 排队系统进行研究，提出 2 种适用于电力系统的 IMS 话务预测模型算法，为电力系统 IMS 核心网建设提供合理性指导。

关键词：话务模型；排队系统；指数平滑预测法；BP 神经网络预测法

1　引言

行政交换系统是电力系统日常办公的重要手段，同时也是调度交换系统的备用保障。随着电路交换退出历史舞台，IMS（IP multimedia subsystem，IP 多媒体子系统）将成为电力系行政交换网的发展方向，并成为数字电力建设的重要环节。目前，国家电网公司正在利用 IMS 技术体制进行行政交换网的升级改造，最终实现电力系统行政交换网的技术体制变革。

业务话务量预测是 IMS 工程设计的重要组成部分，是确定核心网建设方案的前提和基础。电力行政交换网作为电力系统企业专网有别于公网，而 IMS 与电路交换又有着本质的技术体制区别。因此，需要一种适用于电力系统 IMS 行政交换网的话务量预测方法，以真实地反映客观需要，科学准确地对网络建设规模进行判断。

文中结合电力系统的话务特点和规律。通过对 IMS 排队模型的分析，提出指数平滑预测法和 BP（back propagation，反向传播）神经网络预测法 2 种 IMS 话务预测模型算法，并对模型算法进行仿真验证。

2　电力系统话务特点分析

话务量的波动性以及波动的随机性和周期性是研究电话网内业务流量各种问题的出发点。而电力系统行政交换网有自身的特点。为此，文中首先对电力系统行政交换网的话务量的波动性和周期性进行研究。

2.1　呼叫量特点分析

研究选取国家电网公司某 4 省的 IMS 行政交换网网管数据，采用概率学数理理论将某 4 省省级话务量近半年的数据进行统计，运用大数据技术分析并取均值进行计算（法定节假日话务量较小，故未计入统计），利用计算机进行仿真。工作日 24 h 内呼叫量统计见表 1，计算机仿真结果如图 1 所示。

表 1　工作日呼叫量统计/次

时刻	0:00	1:00	2:00	3:00	4:00	5:00	6:00	7:00
呼叫次数	38	20	8	16	16	50	40	200
时刻	8:00	9:00	10:00	11:00	12:00	13:00	14:00	15:00
呼叫次数	2 216	3 512	3 392	2 036	264	232	2 180	3 376
时刻	16:00	17:00	18:00	19:00	20:00	21:00	22:00	23:00
呼叫次数	3 116	2 124	668	388	312	180	48	20

2.2　话务量特点分析

话务量用来反映通信网中用户的通话频繁程度和通话时间的长短，用户进行通话时，必然要占用核心网元，通话的次数多少和每次通话时间的长短反映了占用核心设备的程度，同时也反映了用户对核心设备的需求，从数量上表示这种程度或需求的参数就是话务量 Y，它可以表示为

$$Y = \lambda ST \tag{1}$$

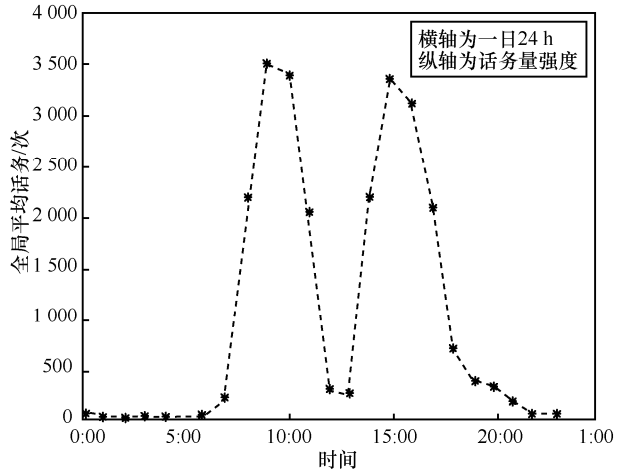


图 1　工作日呼叫量仿真

其中，λ 为单位时间内的呼叫次数，即呼叫强度（次/h）；S 为一次呼叫的平均占用时长（h/次）；T 表示计算话务量的时间范围（h）。

定义单位时间的话务量为话务量强度 a（即通信网中的呼叫量），即

$$a = \lambda S \tag{2}$$

单位为“erl”。话务量强度 a 既反映了用户的通话程度，也反映了用户对核心设备的需求程度。对于电力系统行政交换网，以国家电网某 4 省全局话务量的统计数据为基础，根据 4 省平均话务通话时长，可得工作日 24 h 内话务量强度计算机仿真如图 2 所示。

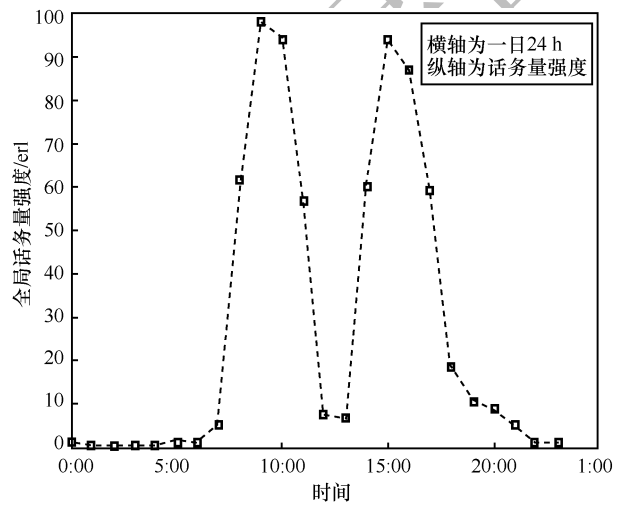


图 2　工作日话务量强度仿真

通过仿真，分析可知我国某 4 省电网一日（0:00-24:00）内话务流量在时域上存在着规律性差异，话务量呈现“M 型潮汐效应”，即 0:00-6:00、12:00-14:00、17:00-24:00 电网内通信网话务量较低，即“汐”，而在 7:00-12:00 话务量、14:00-17:00 话务量较高，并在 9:00-10:00、15:00-16:00 到达一日话务量顶峰，即“潮”。

3　电力系统话务模型

电力系统行政交换网的主要用途是行政办公通话，作为企业专网通信话务模型有别于公网运营商。话务模型是IMS核心网元配置以及网络带宽流量测算的重要依据。

3.1　话务比例模型

选取国网某 4 省 IMS 网管话单数据，对 IMS 系统各项通话比例进行统计，得到电力系统话务比例模型，具体见表 2，分布图图 3 所示。

表 2　电力系统话务比例模型

项目	比例
IMS 用户主叫	51%
IMS 用户被叫	49%
IMS 用户域内呼叫	51%
IMS 用户呼叫电路交换及软交换网用户	17%
IMS 用户呼叫公网用户	32%
IMS 用户本地呼叫	83%
IMS 用户长途呼叫	17%

3.2　基本话务模型

基本话务模型可采用“忙时每用户话务量”和“忙时每呼叫平均占用时长”进行衡量。文中结合电力系统行政交换网的特点，利用某 4 省电网公司实际话务数据，对电力系统基本话务模型进行推算。

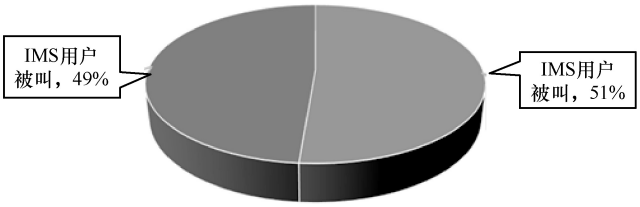
由于目前电力系统各省割接至IMS系统的用户数量存在较大差异，用户数量较小的省份，其各种特征数据普遍适用性相对较差。因此文中运用概率学理论进行分析时，采用加权平均的方法计算话务量，具体方法如下。

加权忙时话务量为：

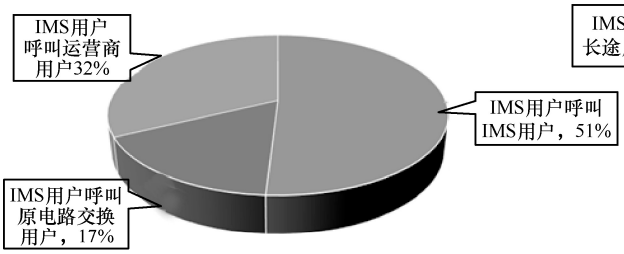
$$S = \sum_{i=1}^{4} B_i \times H_i \tag{3}$$

其中，B_i 为某 4 省在网比例，H_i 为某 4 省忙时话务总量。

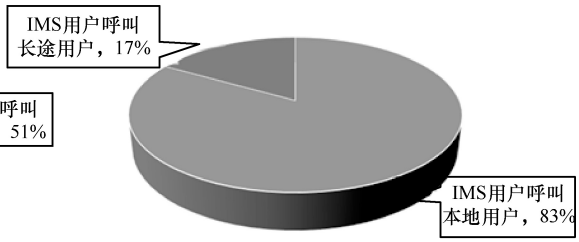
加权忙时通话时长为：



(a) IMS用户主叫、被叫比例分布



(b) IMS用户呼叫各类用户比例分布



(c) IMS用户本地、长途呼叫比例分布

图 3　电力系统话务比例分布

$$T=\sum_{i=1}^{4}B_i\times W_i \tag{4}$$

其中，B_i 为某 4 省在网比例，W_i 为某 4 省忙时通话平均时长。

忙时每用户音频呼叫话务量为：

$$a=S/R \tag{5}$$

其中，R 表示加权平均人数。

忙时每用户平均占用时长为：

$$\lambda=T/R \tag{6}$$

文中根据国网某 4 省一个月内的 IMS 网管数据（非节假日）所有忙时通话数据作为样本，根据上述加权计算方法，可得电力系统基本话务模型见表 3。

表 3　电力系统基本话务模型

项目	数值
忙时每用户音频话务量/erl	0.016
忙时每音频呼叫平均占用时长/s	90

目前，由于电力系统多数省份尚未开通视频通话业务，缺乏网管数据支撑，视频通话等话务量统计缺乏数据支撑。但其确定方法应与音频通话的话务量模型基本一致。

4　IMS 话务量预测模型

话务量预测是 IMS 工程设计的重要组成部分，是确定项目建设规模的重要依据。通过对数据多维度的挖掘分析，基于对历史记录数据挖掘分析后建立的概率统计模型，提取数据中蕴含的多种影响因素并寻找出其特有的变化规律，建立准确的话务量预测模型对项目工程具有重大意义。

本研究根据目前国家电网内部存在的IMS话务量变化的规律，运用了 2 种话务量预测的模型。

（1）采用时间序列预测方法，将话务量的历史数据定义为时间序列，采用加权平均的方法对时间序列进行平滑修匀，通过数理统计方法进行回归处理，建立数学模型，进而预测未来话务量；

（2）采用数据挖掘技术，利用 BP 神经网络中前向传播和误差的反向传播 2 个过程，以国网真实有效的话务数据作为神经网络的训练集，拟合数据最终预测未来的话务量。

4.1　话务量预测的总体方法

话务量某一时刻的数值是由时刻变化受各种因素影响综合而成的结果，一个典型的话务量可以采用如下形式表达：

$$Y(t)=N(t)+W(t)+S(t)+R(t) \tag{7}$$

其中，$Y(t)$为 t 时刻的话务总量，$N(t)$为 t 时刻的基本

人民邮电出版

话务量分量值，$R(t)$ 为 t 时刻的随机话务量分量值，$S(t)$ 为 t 时刻的特殊事件话务量分量值，$W(t)$为 t 时刻的敏感话务量分量值。

由于话务量模型基本满足时间序列的基础特性，因此总话务量总体上可以由基本规律和周期规律数据 2 类数据组成，基本规律是指正常时间的话务量，周期性是指节假日话务量。为了提高模型的预测精度，文中将总话务量分成工作日的话务量和节假日的话务量 2 类，并将节假日的话务量从时间序列中剔除。

4.2 平滑预测法

指数平滑法认为时间序列的态势具有规则性或稳定性，该方法认为最近的过去态势，在某种程度上会持续到未来，即时间序列可被合理地顺势推延，且越近的数据拥有越大的权重。

4.2.1 基本原理

指数平滑方法根据时间序列的上期历史数和预测值，用指数加权的方法进行预测。该方法的优点是只需要存贮少量的历史数据，同时又因前序的数据依时间远近都会对预测数值产生影响，可认为全部历史资料。常见的平滑预测法有一次指数预测、二次指数预测、三次指数预测，分别对应时间序列的总体状态为稳定、线性增长、加速增长 3 种情况。

根据现有话务量没有呈现直线变化或二次曲线变化的趋势特点，文中预测话务量采用一次指数平滑法。

4.2.2 一次指数平滑模型预测法

一次指数平滑模型预测法的计算公式为

$$Y_{t+1}=\alpha X_t+(1-\partial\alpha)Y_t \quad (8)$$

$$Y_{t+1}=Y_t+\alpha(X_t-Y_t) \quad (9)$$

由上式可知，一次指数平滑模型预测法提供的预测值是前一期预测值加上前期预测值中产生的误差修正值。式中 t 和 Y_{t+1} 分别为时刻 t 和时刻 t+1 的预测值，X_t 为时刻 t 的原始值，α 为加权系数，0<α<1。

从以上两式可推出

$$Y_{t+1}=\alpha X_t+\alpha(1-\alpha)X_{t-1}+\cdots+\alpha(1-\alpha)^{t-1}X_1 \quad (10)$$

加权系数 α, $\alpha(1+\alpha)$,$\alpha(1+\alpha)^2$...呈几何级数衰减，越近的数据对预测结果影响越大，远期数据影响较小。话务预测具体流程如图 4 所示。

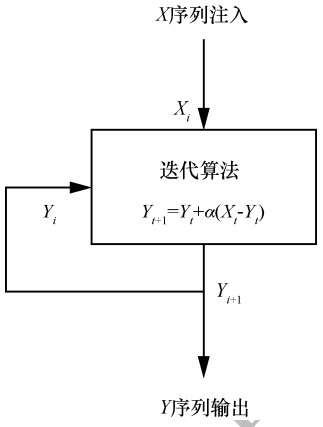


图 4 话务预测流程

4.2.3 预测模型仿真试验

根据上节提出的预测模型对话务量进行预测，并采用工作日的话务量数据作为历史数据训练集。

（1）仿真条件

- 硬件设备：CPU：Intel i5；内存：RAM 8G；硬盘：1 TG。
- 软件平台：仿真在 Matlab R2018a 平台进行。
- 实验数据：国网某省的 IMS 网管话务量通信数据（不包括周末节假日）。

（2）试验方法

本试验采用某省某月（除去节假日）加权话务量作为训练集，来预测话务量。

（3）仿真结果

本实验采用某省某月（除去节假日）加权话务量作为训练集，实验中对于每个时间段采用多个阻尼系数模拟来预测的话务量，阻尼系数分别取 0.4、0.6、0.8。

通过不同阻尼系数的预测值与实际值的比较，利用上述仿真条件，利用 Matlab 计算机软件进行仿真建模，如图 5 所示，测试的目的在于测试指数平滑预测方法的准确性。

由仿真结果可知，阻尼系数 c=0.6 时，预测偏差率为 8.62%，话务模型预测工作日话务量可很好地反映话务量变化规律，可满足日常话务预测的精度要求。

IMS 话务量具有时变性、随机性、周期性等特点，传统线性预测模型很难得到高精度的预测结果。针对话务量变化特点，文中应用一次指数平滑模型预测法预测模型。通过仿真结果验证，一次指数平滑模型预测法具有较高的话务量预测精度，可很好地反映话务量变化规律，可用于 IMS 话务量预测的实际应用。

人民邮电出版社

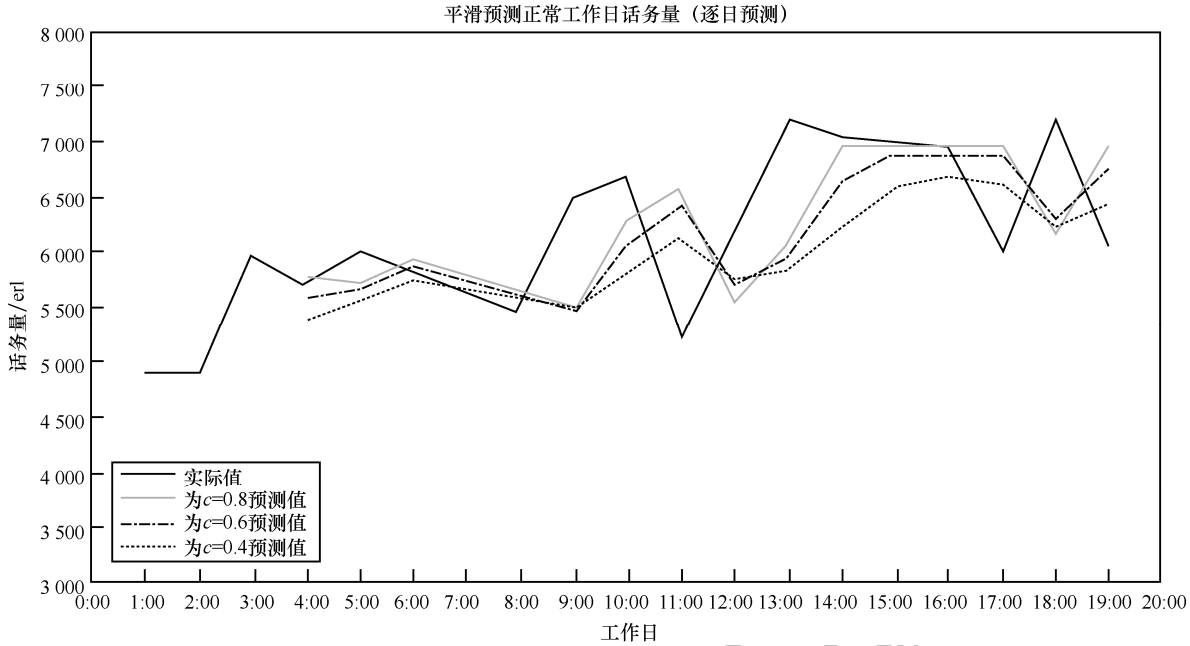


图 5　IMS 话务预测仿真

4.3　BP 神经网络预测法

4.3.1　基本原理

人工神经网络是由大量具有信息处理功能的网络节点即神经元构成的非线性、自适应的信息处理模型，常见的神经网络有前馈神经网络、循环神经网络、卷积神经网络、长短记忆神经网络、递归神经网络等。

采用 BP 算法（误差反向传播算法）的并由一个输入层、一个或多个隐藏层和一个输出层组成的前馈神经网络被称为 BP 神经网络，如图 6 所示。

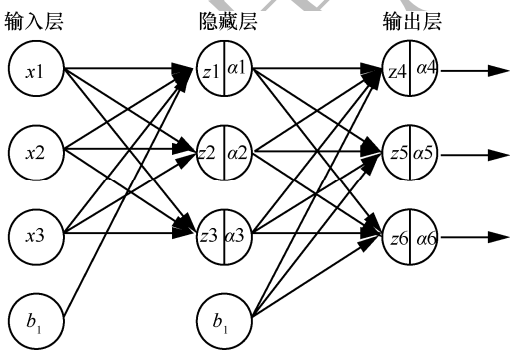


图 6　BP 神经网络结构示意

4.3.2　BP 算法

误差反向传播算法（error back propagation TRaining），简称 BP 算法。

BP 算法的基本原理是通过学习训练，利用输出结果和期望输出的误差来间接调整隐层的权值方法。学习训练过程由信号的正向传播（求损失）与误差的反向传播（误差回传）2 个过程组成。这 2 个过程的核心思想是梯度下降，利用梯度搜索技术实现快速的梯度下降从而降低实际输出值和期望输出值间的误差。

4.3.3　预测模型仿真实验

根据上节提出的预测模型对话务量进行预测，并采用工作日的话务量数据作为历史数据训练集。

（1）仿真条件

- 硬件设备：CPU：Intel i5；内存：RAM 8G；硬盘：1 TG。
- 软件平台：仿真在 Matlab R2018a 平台进行。
- 实验数据：国网某省的 IMS 网管话务量通信数据（不包括节假日）。

（2）试验方法

本试验采用某省某月（除去节假日）加权话务量作为训练集，来预测话务量。

（3）仿真过程

创建 BP 神经网络，隐含层设置 5 个神经元，输出层为 1 个神经元，通过调用函数进行训练并对话务量进行仿真预测，输出结果。

（4）仿真结果

利用上述仿真条件，用 Matlab 计算机软件进行仿真建模，测试的目的在于测试 BP 神经网络预测话务量方

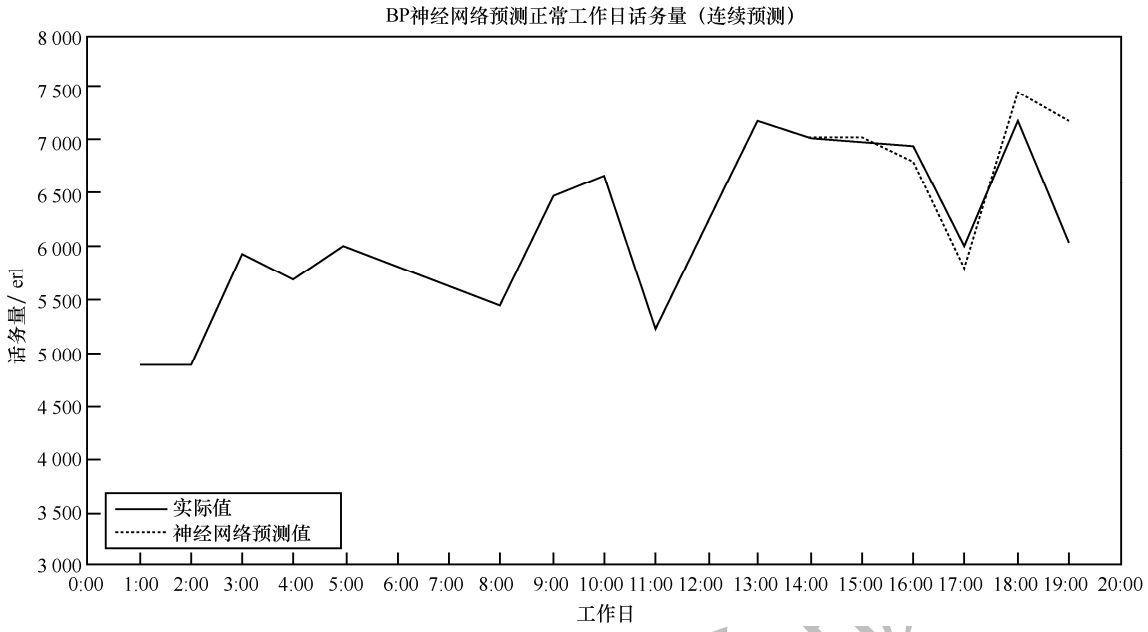


图 7　BP 神经网络话务预测仿真

法的准确性。神经网络话务预测仿真结果如图 7 所示。

由仿真结果可知，通过建立 BP 神经网络模型并进行仿真预测，在进行上百次的迭代后，虽然支持 IMS 的话务训练数据较少，无法形成较大的训练集，但均方差仍低于 70。BP 神经网络模型对历史话务数据、预测数据具有较好的拟合度，预测结果与实际值偏差不大，可应用于中长期的话务模型预测。

5　结束语

IMS 话务量具有时变性、随机性、周期性等特点，文中分析了电力系统 IMS 行政交换网话务的各种特点，并应用两种预测模型对电力系统 IMS 行政交换网话务量进行预测。通过仿真验证，一次指数平滑模型预测法可很好地反映话务量变化规律，可应用于预测短期内的 IMS 话务量变化规律；采用 BP 神经网络模型预测话务量的方法，其话务量预测精度较高，且能预测未来较长一段时间内 IMS 话务量的变化规律，但 BP 神经网络需要训练集数据量较大。根据不同的外界条件，2 种话务量预测方法均可在实际工程中运用，对指导 IMS 核心网建设具有重要的指导意义。

参考文献：

[1] 艾勇. 电力呼叫中心话务量的指数平滑预测方法[J]. 中南民族大学学报（自然科学版）, 2012, 31(3): 81-84.

[2] 牟颖， 王俊峰， 谢传柳，等. 大型呼叫中心话务量预测[J]. 计算机工程与设计， 2010， 31(21): 4686-4689.

[3] 曾俊.话务量预测模型的建立与仿真研究[J]. 计算机仿真, 2012, 29(2): 116-119.

[4] 刘润杰, 杨放春. 软交换系统话务量模型研究[J]. 通信学报, 2004, 25(8):9-13.

[5] 康巧燕, 孟相如, 王建峰. 软交换系统一般话务量模型的研究[J]. 空军工程大学学报(自然科学版), 2005, 6(5): 46-49.

[6] 王少军, 刘琦, 彭喜元, 等. 移动通信话务量多步预测的 LS-SVM 方法研究[J]. 仪器仪表学报, 2011, 32(6): 1258-1264.

[7] 任君明. 基于数据挖掘技术的移动通信话务预测模型[J]. 电信工程技术与标准化， 2015(28): 79-82.

电力信息通信网络安全防护研究综述

杨珂[1,2]，陈绍真[1,2]
(1. 国网电子商务有限公司(国网雄安金融科技集团有限公司)，北京 100053;
2. 国家电网有限公司电力金融与电子商务实验室，北京 100053)

摘　要：随着电网向信息化、自动化和互动化方向发展，电力信息通信网络发挥着日益重要的作用，与此同时，也正面临着更加多样和复杂的网络安全威胁。近年来，电力系统信息通信的网络安全问题成为研究热点，并取得了丰富的成果，但依然远远不能满足建设坚强智能电网和泛在电力物联网的需求。分析电力信息通信网络面临的网络安全风险，从电力信息通信网络的脆弱性及风险评估、可靠性分析及关键节点识别、访问控制及隐私保护等方面综述现有的研究方法及成果，为更深入的研究提供借鉴。

关键词：电力信息通信；网络安全；风险评估；访问控制；隐私保护

1　引言

电力信息通信网络主要有 3 方面的功能：信息传递、提供子系统接入与信息交互服务以及对设备状态和电网调度等实施监控，应用于发电、输电、变电、配电和用电等各个环节，是实现智能电网的基础[1]。电网信息通信网络安全不仅包括通信网络自身的可靠性和生存性，还包括信息传递过程中信息的完整性、机密性和不可否认性以及网络服务的可用性和可控性[2]。

随着电网向信息化、自动化和交互化方向发展，电力信息通信网络发挥着日益重要的作用，与此同时，也正面临着更加多样和复杂的网络安全威胁。近年来，针对电力系统的网络攻击时有发生，愈演愈烈。2015 年乌克兰电力部门遭到恶意代码网络攻击，导致 8 万用户断电[3]；2016 年以色列国家电网遭到勒索软件攻击，是其有史以来遭受的最大规模的网络攻击；2019 年委内瑞拉国家电力系统遭受大规模网络攻击，导致全国性大面积停电。电力系统信息通信的网络安全问题引起了世界各国的高度重视，成为研究热点，并取得了一定的进展。本文首先梳理了电力信息通信网络面临的网络安全风险，然后从电力信息通信网络的脆弱性及风险评估、可靠性分析及关键节点识别、访问控制及隐私保护等方面综述现有的研究方法及成果，为更深入的研究提供借鉴。

2　电力信息通信网络面临的网络安全风险

电力信息通信网络是电力系统的基础设施，是实现电网调度自动化和管理现代化的基础，是确保电网安全、稳定、经济运行的重要手段，由骨干网和接入网组成，其中骨干网又可分为传输网、数据网和支撑网[4]。电力信息通信网络安全具有自身的特点，第一，其发生网络安全事件会对国计民生产生极大的破坏，事关国家安全，因此需要超高的可靠性和较强的实时性；第二，其使用专用的软件、网络设备和通信协议，公网防护方案无法照搬；第三，电力信息通信网络结构复杂，点分散，业务量少[2]。

电力信息通信网络面临的网络安全风险主要包括系统外部的安全风险、系统内部的安全风险、系统基础平台网络安全风险和自然灾害引起的安全风险。系统外部的网络安全风险包括病毒、黑客针对电网监控系统和调度数据网络等发起的攻击、未授权用户非法访问系统或获取系统数据等。系统内部的网络安全风险包括系统内的操作人员无意识或有意地破坏，窃取关键业务系统数据等。系统基础平台网络安全风险包括平台中软件和网络设备存在的漏洞或后门、功能冗余等带来的安全风险。

3　电力系统信息通信网络安全防护研究

电力系统信息通信网络安全是保障智能电网安

基金项目：国家电网公司 2019 年科技项目（No.5700-201972227A-0-0-00）

全、稳定运行的先决条件。针对智能电网通信系统面临的层层网络安全威胁，必须开展体系化的防护措施，研究热点主要包括以下几个方面：电力信息通信网络脆弱性及风险评估、可靠性分析及关键节点识别、访问控制及隐私保护等[5]。

（1）电力信息通信网络脆弱性及风险评估研究

电力信息通信网络脆弱性和风险评估贯穿于系统设计、开发、测试、运维等各个环节，是从根本上保证电力通信系统安全必不可少的关键环节，为网络安全策略的制定、系统开发和运行方式及系统优化方向的确定提供依据。定期开展电力信息通信网络脆弱性和风险评估，并制定改进措施，是网络安全防护的重要一环。

参考文献[1]基于信息价值评估各个电力通信设备受到网络攻击的可能性，进而量化评估电力信息通信系统的脆弱性；参考文献[6]将电力信息通信系统建模为复杂网络，采用度数和介数指标评估节点脆弱性，通过效能函数确定网络脆弱点并分析了异构网络脆弱性的本质原因；参考文献[7]基于模糊层次分析法构建了电力信息通信系统网络安全指标体系，解决了当前指标冗余且难以量化的问题，提高了对安全风险评估的准确性；参考文献[8]从电力信息通信系统风险三要素：资产、威胁和脆弱性的风险值计算入手，对比分析了现有的风险计算方法，最终提出一种考虑三要素相互关联性的电力通信系统风险计算模型；参考文献[9]针对光纤通信网通过构建资产、威胁、脆弱性和安全措施之间的树状图模型建立了安全风险量化模型。

（2）电力信息通信网络可靠性分析及关键节点识别研究

电力信息通信网络承载着电网各类业务，网络的可靠性对于保障电力生产至关重要。电力信息通信系统中节点的重要性越高，其在受到网络攻击的情况下对网络性能的影响越大，因此，识别出电力信息通信系统中的重要节点，并加以严密保护，对提升电力信息通信网络的可靠运行能力有着重要作用。

参考文献[10]结合电力信息通信网络的管理特点以及电力通信安全性行业评价办法，确定了可靠性分层，提出了一种基于改进模糊层次法的电力信息通信网络综合可靠性评价方法；参考文献[11]将电力信息通信网络的业务特点和分布考虑在内，基于业务重要度，提出了一种可有效反映当前网络的业务可用性状况的网络可靠性量化评估方法；参考文献[12]基于节点分类、负荷大小和拓扑位置构建了电力信息通信网络节点重要性评价体系，进而基于层次分析法和熵权法为指标赋权，通过多属性决策的 TOPSIS 算法确定节点重要度；参考文献[13]对参考文献[12]进行了改进，将电网关联度因素考虑在内，从信息通信系统自身的重要性以及其与电网的关联程度两个方面综合评估节点重要性。

（3）电力信息通信网络访问控制及隐私保护研究

用户侧用电信息记录了用户的用电行为，一方面用户数据为优化电网运行提供决策支撑，另一方面信息泄露将会严重侵犯用户的隐私权，甚至危及国家安全。因此需防止未授权用户访问系统数据，保障用户数据的安全性和完整性。隐私保护成为电力信息通信系统网络安全防护的重中之重。

参考文献[14]指出配电端大数据具有双刃剑效应，在增强了配电端与能源端、用户端的互动能力的同时，由于数据集中引发了严重的网络安全问题；参考文献[15]采用隐私同态聚合、签名批验证和基于属性的加密算法，实现了一种具有隐私保护功能的电力信息通信网络多维数据归集和访问控制方法；参考文献[16]基于智能配电网信息通信系统的层次化结构设计了一种基于身份密码体制的访问控制方法；参考文献[17]提出了一种带屏蔽参数的 Merkle 树认证协议，既保证了接收数据的完整性，又实现了数据隐私保护。

此外，网络流量识别技术和网络安全管理等对于电力信息通信网络安全来说也必不可少。网络流量识别技术用来分析网络流量的来源以及目的，对于加强网络的可控性至关重要，可以有效地识别和防御大多数网络安全威胁。参考文献[18]针对电力信息通信系统网络流对比分析了基于主机行为特征、基于有效负载、基于端口映射和基于机器学习的 4 种流量分类方法，得出基于机器学习的流量分类方法最适用于电力通信系统并深入探究了 C4.5 决策树算法和神经网络算法的性能。网络安全技术和管理措施相辅相成，据统计，90%以上的网络攻击事件是由管理措施不当造成的。参考文献[19]指出电力信息通信系统网络安全防护还必须从网络设备国产化、采购安全管控、上线安全管控、运行监控安全管控和下线安全管控等管理措施方面推进。

4 结束语

本文分析了电力信息通信网络面临的网络安全风险，从脆弱性及风险评估、可靠性分析及关键点识别、

人民邮电出版社

访问控制及隐私保护等方面总结了当前的主要研究方法和成果，为今后的相关研究提供借鉴。考虑到未来智能坚强电网和泛在电力物联网的发展需求，尽快制定出符合电力信息通信网络业务特点的、综合的网络安全防护策略体系是当务之急。

参考文献：

[1] 叶夏明. 电力信息物理系统通信网络性能分析及网络安全评估[D]. 杭州: 浙江大学,2015.

[2] 高会生. 电力系统通信的网络安全问题[J]. 电力信息与通信技术, 2013, 11(1): 16-17.

[3] 童晓阳, 王晓茹. 乌克兰停电事件引起的网络攻击与电网信息安全防范思考[J]. 电力系统自动化, 2016(7): 144-148.

[4] 朱斌. 未来坚强智能电网的电力通信网络[J]. 电力系统通信, 2011, 32(4): 71-73.

[5] 马韬韬, 李珂, 朱少华,等. 智能电网信息和通信技术关键问题探讨[J]. 电力自动化设备, 2010, 30(5): 87-91.

[6] 郭静, 王东蕊. 基于复杂网络理论的电力通信网脆弱性分析[J]. 电力系统通信, 2009, 30(9): 6-10.

[7] 王庭钧, 马庆峰, 刘雪冰, 等. 基于模糊层次分析的电力通信系统网络安全评估指标体系构建[J]. 科学技术创新, 2018(13): 30-31.

[8] 高会生, 李聪聪. 电力通信网安全风险计算模型[J]. 电力系统保护与控制, 2007, 35(14): 50-53.

[9] 高会生, 李聪聪, 朱静. 基于树状图的电力光纤通信网安全风险模型[J]. 光通信研究, 2008, 34(3): 19-21.

[10] 高会生. 电力通信网可靠性研究[D]. 保定:华北电力大学, 2009.

[11] 刘俊毅, 何明甫, 范超,等. 基于业务可用性的电力通信网可靠性量化评估方法[J]. 浙江电力, 2015(10): 40-43.

[12] 耿子惠, 崔力民, 舒勤, 等. 基于 TOPSIS 算法的电力通信网关键节点识别[J]. 电力系统保护与控制, 2018(1): 78-86.

[13] 崔力民, 耿子惠, 舒勤, 等. 考虑电网关联度的电力通信网关键环节识别[J]. 电力建设, 2017(5): 134-142.

[14] 苗新, 张东霞, 孙德栋. 在配电网中应用大数据的机遇与挑战[J]. 电网技术, 2015, 39(11): 3122-3127.

[15] 刘雪艳, 张强, 李战明,等. 面向智能电网通信系统的数据聚合和访问控制方法[J]. 电力系统自动化, 2016, 40(14): 135-144.

[16] 孙中伟, 张荣刚. 智能配电网通信系统访问控制研究[J]. 电力系统保护与控制, 2010, 38(21): 118-121.

[17] 徐琳, 温蜜, 李晋国. 智能配电网中具有隐私保护的数据安全认证方案[J]. 电子技术应用, 2015, 41(12): 98-101.

[18] 姜羽, 华俊, 胡静, 等. 电力信息通信网络流量识别技术研究[J]. 信息化研究, 2015(1): 10-14.

[19] 高鹏, 李尼格, 范杰. 电力系统信息通信网络安全及防护研究[J]. 现代电子技术, 2014(18): 146-148.

人民邮电出版社

电网生产业务工单分类的文本挖掘方法应用

陈小峰，齐晓明，赵雅迪，张利鹏
（北京国网信通埃森哲信息技术有限公司，北京 100032）

摘　要：文本挖掘技术作为描述性数据分析的重要手段，在电网业务中发挥着愈加重要的作用。创建了电网生产工单文本分析系统，利用结巴分词技术处理工单中文本内容，基于 TF-IDF 算法计算关键词重要性权重值，构建电力关键词库。通过构建贝叶斯文本分类模型，对工单内容完成缺陷部位、类别、原因的自动分类，提升数据质量和系统自动化水平，助力业务部门提高工作效率，为电网业务分析及未来发展方向提供依据。

关键词：电网生产业务工单；文本挖掘；结巴分词；贝叶斯分类

1　引言

在现代化企业发展和宏观经济的影响下，电网企业作为主营电网业务的运营商和区域电力市场交易的主体，对企业管理和经营数据及时有效统计的需求越来越高[1-2]。随着网络技术和信息技术的不断发展，电网企业的信息化程度逐步提高，在信息系统不断增加的同时，企业数据也呈海量增长趋势[3-4]。我国电网企业的业务数据报送多数还采用人工方式，这种方式很容易受到人员素质和部门管理方式的影响，使得数据在创建过程中可能出现不一致或不准确等质量问题。随着电力企业的不断发展，资产积累、部门增加以及专业分工更为细化，企业内部的业务数据分类越来越多，导致数据交叉和冗余情况严重，数据难以维护、质量难以保证[5]。

国家电网公司提出构建泛在电力物联网，更大发挥公司数据价值，实现大数据智能分析、多源大数据治理与跨领域智能分析，主动培育大数据运营、大数据征信等新兴业务[6]。大数据方法作为实现泛在电力物联网的重要基础，已经被应用到电工领域的许多专业中去解决一些重要问题，以提升数据质量、实现数据科学合理的运营[7-8]。张志亮等[9]通过大数据规则进行数据质量校验处理研究，实现基于 Hadoop 并行化数据质量校验技术，利用 Hadoop 平台，实现针对数据校验的索引数据存储管理方法。电力设备缺陷方面，陈拥军[10]对电网运行分析决策支持系统缺陷数据进行了整理分析，提出了一种基于时间序列法的电力系统设备缺陷预测方法，同时使用时间序列法对某单位某型开关设备缺陷进行了预测，取得了较好的效果。张延旭等[11]为提升电力系统二次设备的运维和管控水平，从二次设备的缺陷数据出发，提出了基于 Apriori 算法的二次设备缺陷数据挖掘与分析方法，该方法能够有效分析二次设备的薄弱环节，并能够找到诱发薄弱环节的原因，给二次设备运维和管控提供参考依据。但由于文章主要采用人工数据清理的方式，生产系统中存在着海量的设备缺陷信息，数据清理效率低，一定程度上限制了对于海量缺陷数据的分析能力。

基于数据清理效率低、数据不完整的情况，对于描述性文本数据，可以运用文本挖掘方法对数据进行整理与固化，为更好地进行数据分析与决策工作提供优质数据基础[12-14]。本文针对电力企业生产业务数据，构建了电网生产工单文本分析系统，该系统以自然语言处理方法为主要技术[15]，利用结巴分词和 TF-IDF 算法分析生产受理工单中数据内容，创建电力关键词库，基于关键词库中的分类规则，运用朴素贝叶斯分类算法通过挖掘规则和标签进行训练，形成工单录入后的自动分类，更加准确、高效地为电网业务分析及未来发展方向提供依据。

2　理论方法

2.1　文本分词算法

现代分词都是基于统计的分词，而统计的样本内容来自一些标准的语料库。如果有一个句子 M，它有 m

人民邮电出版社

种分词选项 $\{A_{11},A_{12},\cdots,A_{1n_1},A_{21}A_{22}\cdots A_{2n_2},\cdots,A_{m1}$，$A_{m2},\cdots,A_{mn_m}\}$，其中下标 n_i 代表第 i 种分词的词个数。如果从中选择了最优的第 r 种分词方法，那么这种分词方法对应的统计分布概率应该最大，即有 $r=\arg\max_i P\left(A_{i1},A_{i2},\cdots,A_{in_i}\right)$。为了简化计算，通常使用马尔可夫假设，即每个分词出现的概率只和前一个分词有关，可以写为：

$$P\left(A_{ij}\middle|A_{i1},A_{i2},\cdots,A_{i(j-1)}\right)=P\left(A_{ij}\middle|A_{i(j-1)}\right) \quad (1)$$

则联合分布可为：

$$\begin{aligned}&P\left(A_{i1},A_{i2},\cdots,A_{in_i}\right)=P\left(A_{i1}\right)P\left(A_{i2}\middle|A_{i1}\right)\\&P\left(A_{i3}\middle|A_{i2}\right),\cdots,P\left(A_{in_i}\middle|A_{i(n_i-1)}\right)\end{aligned} \quad (2)$$

同时，通过软件中的标准语料库，可以近似计算出任意两个分词间的二元条件概率，比如任意两个词 a_1,a_2，它们的条件概率分布可以近似表示为：

$$P\left(a_2|a_1\right)=\frac{P\left(a_1,a_2\right)}{P\left(a_1\right)}\approx\frac{\mathrm{freq}\left(a_1,a_2\right)}{\mathrm{freq}\left(a_1\right)} \quad (3)$$

$$P\left(a_1|a_2\right)=\frac{P\left(a_2,a_1\right)}{P\left(a_2\right)}\approx\frac{\mathrm{freq}\left(a_1,a_2\right)}{\mathrm{freq}\left(a_2\right)} \quad (4)$$

其中，$\mathrm{freq}\left(a_1,a_2\right)$ 表示两个词在语料库中相邻一起出现的次数，$\mathrm{freq}\left(a_1\right)$、$\mathrm{freq}\left(a_2\right)$ 分别表示各个词在语料库中出现的统计次数。利用语料库建立的统计概率，对于一个新的句子，就可以通过计算各种分词方法对应的联合分布概率，找到最大概率对应的分词方法，即为最优分词。本文用到的分词方法为结巴分词，一是该算法包在对语料库精心选择的情况下，通过数据结构中的前缀树或字典树算法对词语进行了高效的分类，便于查找；同时结合有向无环图（DAG），解决了双重理解词语组合的问题。二是对于未登录词，采用了基于汉字成词能力的 HMM 模型，并使用了 Viterbi 算法，将词语分为开始、中间、结束和单独成词 4 种分类来自动分词，解决了因没有录入字典导致的词汇无法找到的问题。

2.2 TF-IDF 关键词挖掘算法

词频-逆文档频率方法（term frequency-inverse document frequency，TF-IDF）的主要思想是：如果某个词或短语在某分类中出现的频率 TF 高，并且在其他分类中很少出现，则认为此词或者短语具有很好的类别区分能力，适合用来分类，可以标记为关键词汇。设 d 是分类类别，f 是基于工单内容细分的特征词，词频标准化的计算方法如下：

$$\begin{aligned}&\text{词频}(TF_{f,d})=\text{词汇在所属}\\&\text{类别中的出现次数/词汇在样本集合的总次数}\end{aligned} \quad (5)$$

式（5）表示某一个给定的词语在所属类别中出现的次数。文档频率用 DF 表示样本集中包含某个词汇的所有类别数目，DF 通常比较大，将其映射到一个较小的取值范围，用逆文档频率（Inverse document frequency,IDF）表示如下：

$$\begin{aligned}&\text{逆文档频率}(\mathrm{IDF}_f)=\log(\text{数据集总的样本个数/}\\&(\text{包含某个词汇的样本数}+1))=\\&\log(N/(\mathrm{DF}_f+1))\end{aligned} \quad (6)$$

式（6）的意义在于，如果包含该词汇的样本数越少，IDF 越大，则说明该词汇具有很好的类别区分能力。词项的权重用 TF – IDF 来表示，计算式如下：

$$\mathrm{TF-IDF}=\text{词频}\left(\mathrm{TF}_{f,d}\right)\cdot\text{逆文档频率}\left(\mathrm{IDF}_f\right) \quad (7)$$

使用 TF – IDF 可以计算某个词汇在某个分类中的重要性，因而识别出该词汇是否是关键词汇，实现分类规则的构建，精准定位文字描述的基本内容，为后续分类分析工作提供精准数据。

2.3 朴素贝叶斯分类算法

在朴素贝叶斯分类器中，根据每个特征来确定哪个标签应该被分配到给定的输入值中。为输入值选择标签，朴素贝叶斯分类器以计算每个标签的先验概率开始，它通过检查训练集上的每个标签频率来确定。同时每个特征的贡献与它的先验概率相结合，可以得到每个标签的似然估计，似然得分结果可以认为是从给定的标签和特征集的训练集中随机选取出来的值的概率估计，似然估计最高的标签会分配给输入值，分类原理如图 1 所示。

以 label 表示输出标签，features 表示输入的 n 个特征值，算法的计算过程如下：

（1）计算

$$P\left(\text{features}\right)=\sum_{\text{label}\in\text{labels}}P\left(\text{features,label}\right)$$

（2）似然标签可以展开为标签的概率乘给定标签特征的概率，在特征独立的情况下，有：

$$\begin{aligned}P\left(\text{features,label}\right)&=P\left(\text{label}\right)\times P\left(\text{features}\middle|\text{label}\right)\\&=P\left(\text{label}\right)\times\prod_{f\in\text{features}}P\left(f\middle|\text{label}\right)\end{aligned} \quad (8)$$

其中，$P\left(\text{label}\right)$ 是一个给定标签的先验概率，每个

人民邮电出版社

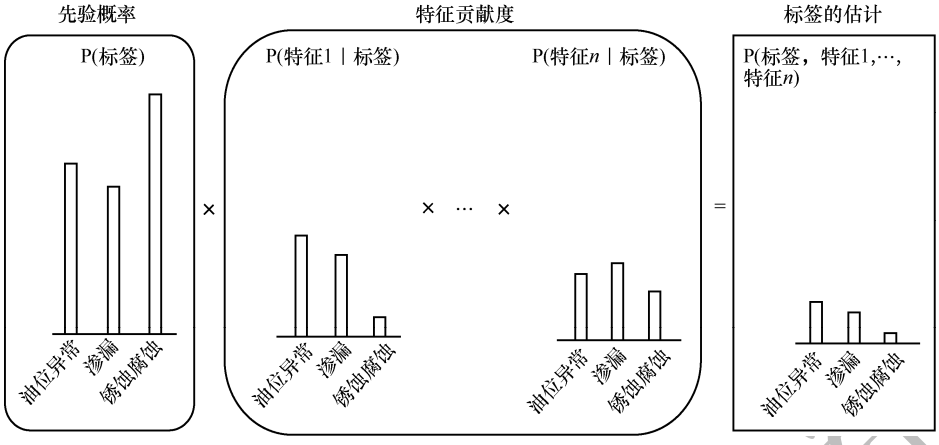


图 1　分类原理说明

$P(f|\text{label})$ 是单个特征对标签可能性的贡献，是取得具有给定特征和给定标签的训练实例百分比，可表示为：

$$P(f|\text{label}) = \text{count}(f,\text{label}) / \text{count}(\text{label}) \quad (9)$$

（3）当训练集中存在从来没有和给定标签一起出现的特征时，$P(f|\text{label})$ 的计算值为 0，这将导致给定标签的标签可能性为 0，从而输入将永远不会被分配给这个标签，导致分类准确度降低。为了避免其他属性携带的信息被训练集中未出现的属性值“抹去”，在估计概率值时通常要进行“平滑”处理，常用“拉普拉斯修正”。令 N 表示训练集 D 中可能的类别数，N_i 表示第 i 个属性可能的取值数，D_c 表示训练集 D 中第 c 类样本组成的集合，$D_{c_i x_i}$ 表示 D_c 中在第 i 个属性上取值为 x_i 的样本组成的集合，则有如下计算式：

$$\text{count}(\text{label}) = \frac{|D_c|+1}{|D|+N} \quad (10)$$

$$\text{count}(f,\text{label}) = \frac{|D_{c_i x_i}|+1}{|D_c|+N_i} \quad (11)$$

（4）计算 $P(\text{label}|\text{features}) = P(\text{features},\text{label}) / P(\text{features})$，并选择最大概率所对应的标签作为新输入特征值的标签结果。

3　场景应用

将主要分类算法运用在电网生产工单文本分析系统的建设中，其功能框架如图 2 所示。关键词库管理模块结合缺陷定级标准提取生产关键词，实现原始关键词的挖掘功能，同时提供关键词查询。基础数据分类标准库和原始工单库以关键词库作为基础，由关键词组成分类规则，基于规则和标签进行训练，形成了工单录入后的自动分类。分类知识库和统计分析报表功能为在关键词提取和分类功能的基础上，建立分类规则与各类生产业务关系，支撑更多的业务应用。以分类后的工单作为基础数据，根据不同业务进行报表统计，实现基于电网业务下的不同功能应用。

作为电力设备运行维护的重要内容之一，缺陷管理一直是电力企业管理人员、生产维修人员高度关注的工作。而在现实工作中，缺陷管理存在不规范的现象，特别是缺陷描述、处理等的不标准，影响了缺陷管理的水平。设备缺陷的描述内容与现场情况最为贴近，能反映现场具体情况，因此对缺陷描述文本进行分词处理，可以得到现场具体情况的关键词。基于处理得到的关键词及分类标准进行词频分析，运用 TF-IDF 算法计算词汇在本类中出现的词频及在其他类中的词频，生成工单关键词，构建关键词库，原理如图 3 所示。以关键词库作为基础，建立分类规则样本数据集，采用机器学习的手段并应用贝叶斯模型训练得出分类规则。

基于缺陷数据，分别进行了缺陷部位、缺陷类别、缺陷原因的分类，这里缺陷部位分为一级、二级、三级，缺陷原因分为一级和二级，可以运用算法进行迭代计算。自动分类全过程示例如图 4 所示，以缺陷类型作为目标分类内容，输入值为“2 号主变有载调压呼吸器油杯油位低”，输出类型值为“油位异常”。

人民邮电出版社

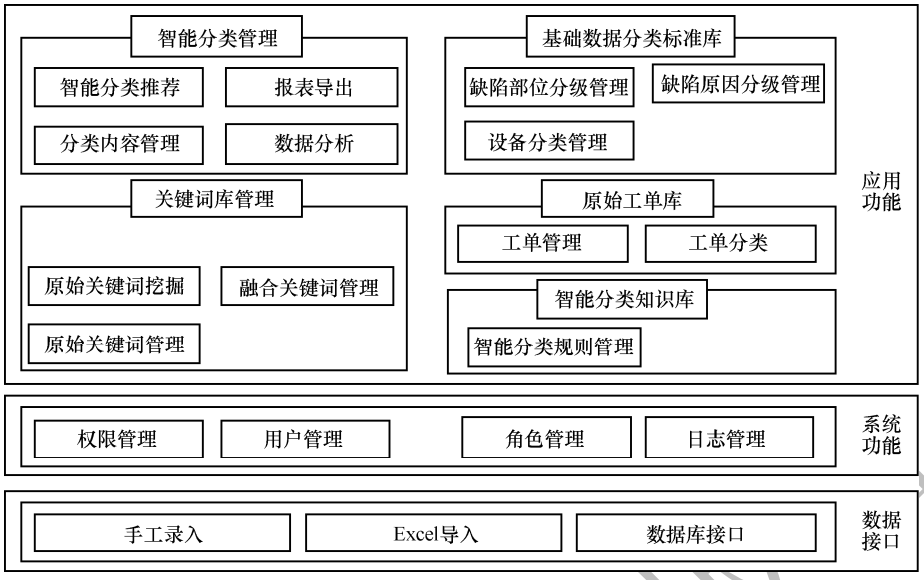


图 2　电网生产工单文本分析系统功能框架

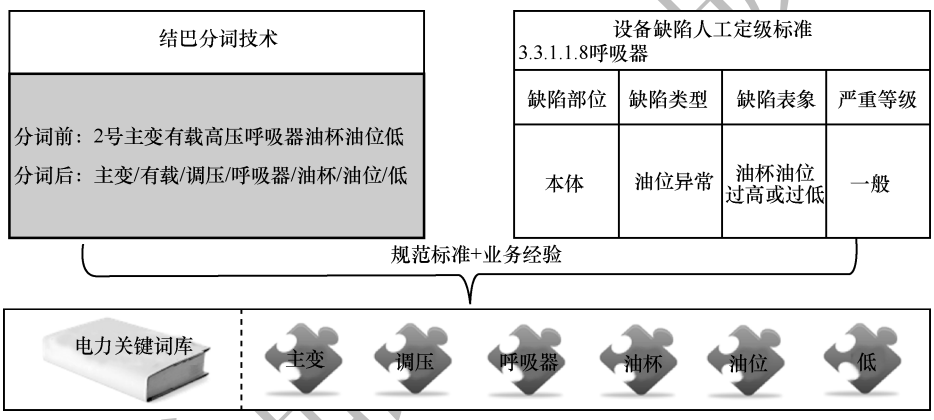


图 3　关键词库构建原理

智能分类结果展示见表 1，该模块通过录入一条或者多条缺陷描述（或者从数据库、Excel 中批量导入），选择分类内容后，平台调用规则自动显示其推荐的缺陷类别、缺陷部位、缺陷原因等结果。

4　结束语

电网生产工单文本分析系统通过将文本分词、关键词挖掘、自动分类技术应用到各个模块，对电网变电一次设备生产数据清洗的关键词库及清洗规则起到了固化作用。将该方法运用到某电网企业近 7 年变电一次生产设备数据清理工作中，清理电压 110 kV 或以上的设备缺陷数据总数 36 255 条，分类结果见表 1。其中矫正缺陷类别错误数据 21 220 条，占比 58.52%；矫正缺陷部位错误数据 31 857 条，占比 87.87%；数据矫正准确率均在 93%~95%，达到了良好的效果。

电网生产工单文本分析系统从一般数据质量管理平台的只能发现问题到该系统从发现到解决问题的一站式贯通，将分类规则固化与规范标准制定相结合，提供数据问题解决方案。如图 5 所示，将原平台分析情况与本系统分析结果做比较可以看到，新系统在对缺陷工单自动分类的基础上，可以直观地看到问题数据情况，完成数据校验、数据质量问题报表导出和分析等工作，提高数据质量，辅助数据治理工作的开展。

目前，电力行业还没有建立规范的电力词库，处于刚起步阶段。因此该系统的建立为电网企业未来建立一套规范的电力词库提供了依据和发展方向。该系统在实现了数据自动清洗功能的基础上，提高了数据质量和清晰效率，具有工单智能分类、关键词库建设

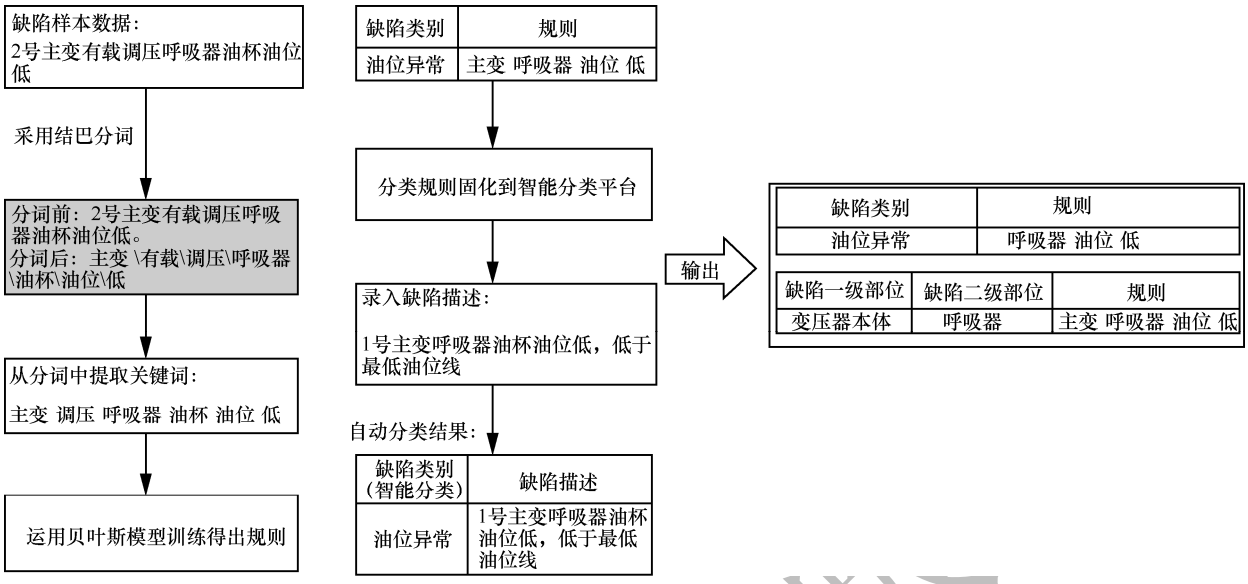


图 4　分类全过程示例

表 1　智能分类结果展示

缺陷类型（智能推荐）	缺陷一级原因（智能推荐）	缺陷二级原因（智能推荐）	缺陷一级部位（智能推荐）	缺陷二级部位（智能推荐）	缺陷三级部位（智能推荐）	缺陷描述	设备类别
机械损伤	产品质量	产品生产原材料（零部件）质量不合格	非电量保护装置	瓦斯继电器	控制回路	2 主变C相分控箱相序继电器损坏	变压器
拒动/误动	设备老化	接触不良：	冷却系统			1号主变2号风机切至运行集团时，风机不转，工作灯不亮。	变压器
锈蚀腐蚀	外部影响	自然环境—高温、高湿、高盐	本体	其他	其他	1号主变A相分控箱锁芯生锈脱落无法打开	变压器
指示异常	设备老化	过负荷	本体	表计	控制回路	温度指示异常（主变油温现场为49度，监控中及后台监控电脑均显示-50度）。	变压器
密封不良	设计质量	不满足典型设计要求	调压开关	绝缘油	其他	2号主变分接开关油箱油枕表计内有水珠。	变压器
拒动/误动	外部影响	自然环境—高温、高湿、高盐	冷却系统			1号主变5号、6号、12号、13号冷却风扇停转	变压器
	外部影响	自然环境—高温、高湿、高盐	冷却系统	端子箱类设备	控制回路	2号主变第一段风冷控制电源故障，检查发现风冷管制箱内交流接触器无法吸合，是缺相保护器坏导致。	变压器
油位异常	外部影响	自然环境—高温、高湿、高盐	本体	呼吸器	其他	2号主变有载调压呼吸器油杯油位低。	变压器
渗漏	外部影响	自然环境—高温、高湿、高盐	冷却系统			2号主变1、2号组冷却器流量指示器前放油阀渗油	变压器
渗漏	外部影响	自然环境—高温、高湿、高盐	冷却系统			1号主变6号散热器下阀门渗油，每分钟约4滴。	变压器
拒动/误动	外部影响	自然环境—高温、高湿、高盐	冷却系统			2号主变压器第一组风机第二个风扇不转	变压器

表 2　智能分类效果

	矫正前个数/条	准确率	矫正后个数/条	准确率
缺陷部位	4 398	12.13%	31 857	93.53%
缺陷类别	15 035	41.48%	21 220	94.61%

及优化、统计分析辅助等功能，可供系统应用建设部门、设备管理部门、各业务研究部门使用。下一步，计划将更多算法运用至该系统，实现对各模块功能的优化，同时增加应用部分的业务拓展，如增加对配网数据的研究、对设备事故事件数据智能的分类等，支

缺陷类型	缺陷描述
元器件故障	风机不能转动
漏水(油)	2号主变本体严重渗漏油
密封不良	1号主变有载调压呼吸器硅胶受潮变色超过2/3
拒动/误动	2号主变9号风机、3号主变11号风机交流接触器异响
闭锁装置异常	#1主变压器有载开关油枕呼吸器硅胶变色达二分之一缺陷表象：硅胶变色（超过2/3）
闭锁装置异常	#1主变硅胶变色已达2/3缺陷表象：硅胶变色（超过2/3）
冷却风机故障	#1主变#5风机合闸即跳开空气开关
风机不转	220 kV岗华变电站#2主变的#6风机不能转动
	110 kV1号主变有载调压在线滤油装置面板黑屏，启动不了
	110 kV新华变110 kV1号主变油温变送器显示温度过高，与本体温度指示温度不符
密封不良	1号主变压器端子箱底座锈蚀严重（老生产管理系统于2015年09月11日已报缺）
震动及异响	500 kV#3主变A相第3组冷却器组上部风扇电机出现异响
装置故障	#3主变本体绕组温度显示异常（绕组温度低于油温表温度）
封堵异常	#2主变A、B、C三相本体呼吸器油封杯内油面偏低

一般数据质量平台

缺陷类型	缺陷类型（是否正确）	缺陷描述
元器件故障	正确	风机不能转动
漏水（油）	错误	2号主变本体严重渗漏油
密封不良	正确	1号主变有载调压呼吸器硅胶受潮变色超过2/3
拒动/误动	正确	2号主变9号风机、3号主变11号风机交流接触器异响
闭锁装置异常	正确	#1主变压器有载开关油枕呼吸器硅胶变色达二分之一缺陷表象：硅胶变色（超过2/3）
闭锁装置异常	正确	#1主变硅胶变色已达2/3缺陷表象：硅胶变色（超过2/3）
冷却风机故障	错误	#1主变#5风机合闸即跳开空气开关
风机不转	错误	220 kV岗华变电站#2主变的#6风机不能转运
	错误	110 kV1号主变有载调压在线滤油装置面板黑屏，启动不了
	错误	110 kV新华变110 kV1号主变油温变送器显示温度过高，与本体温度指示温度不符
密封不良	正确	1号主变压器端子箱底座锈蚀严重（老生产管理系统于2015年09月11日已报缺）
震动及异响	错误	500 kV#3主变A相第3组冷却器组上部风扇电机出现异响。
装置故障	正确	#3主变本体绕组温度显示异常（绕组温度低于油温表温度）
封堵异常	正确	#2主变A、B、C三相本体呼吸器没封杯内油面偏低

工单文本分析系统

缺陷类型	缺陷类型（智能分类推荐）	缺陷描述
元器件故障	拒动/误动	风机不能转动
漏水（油）	渗漏	2号主变本体严重渗漏油
密封不良	颜色异常	1号主变有载调压呼吸器硅胶受潮变色超过2/3
拒动/误动	声音异常	2号主变9号风机、3号主变11号风机交流接触器异响
闭锁装置异常	颜色异常	#1主变压器有载开关油枕呼吸器硅胶变色达二分之一缺陷表象：硅胶变色（超过2/3）
闭锁装置异常	颜色异常	#1主变硅胶变色已达2/3缺陷表象：硅胶变色（超过2/3）
冷却风机故障	拒动/误动	#1主变#5风机合闸即跳开空气开关
风机不转	拒动/误动	220 kV岗华变电站#2主变的#6风机不能转运
	拒动/误动	110 kV1号主变有载调压在线滤油装置面板黑屏，启动不了
	指示异常	110 kV新华变110 kV1号主变油温变送器显示温度过高，与本体温度指示温度不符
密封不良	锈蚀腐蚀	1号主变压器端子箱底座锈蚀严重（老生产管理系统于2015年09月11日已报缺）
震动及异响	声音异常	500 kV#3主变A相第3组冷却器组上部风扇电机出现异响
装置故障	指示异常	#3主变本体绕组温度显示异常（绕组温度低于油温表温度）
封堵异常	油位异常	#2主变A、B、C三相本体呼吸器油封杯内油面偏低

图 5　系统分析结果比较

撑更多、更高的电网业务分析，推动泛在电力物联网业务高质量发展。

参考文献：

[1] 邹保平, 周亮. 电网企业数据服务研究[J]. 电力信息与通信技术, 2010(9): 30-32.

[2] 黄武锋, 郑华. 面向企业信息化的数据质量评估研究[J]. 计算机技术与发展, 2011(1): 185-188.

[3] 鞠小丽. 基于数据仓库技术的电力营销分析系统[J]. 数字技术与应用, 2012(3): 68-69.

[4] 朱义军, 王乘. 应用在电力系统中的数据仓库及其设计[J]. 浙江电力, 2003, 22(4): 146-148.

[5] 党芳芳. 电网企业业务数据质量管控技术的研究[D]. 北京：华北电力大学, 2014.

[6] 汪兴. 面向智能电网建设的电力物联网架构研究[J]. 电力大数据, 2018, 21(10): 34-37.

[7] 李昀昊, 王建学, 王秀丽. 基于混合聚类分析的电力系统网损评估方法[J]. 电力系统自动化, 2016(1): 60-65.

[8] 马瑞, 周谢, 彭舟, 等. 考虑气温因素的负荷特性统计指标关联特征数据挖掘[J]. 中国电机工程学报, 2015(1).

[9] 张志亮, 孙煜华, 陈承志, 等. 基于 Hadoop 的电网数据质量校验方法与验证系统[J]. 计算机研究与发展, 2014(S2): 134-144.

[10] 陈拥军. 电力系统设备缺陷预测[D]. 杭州：浙江大学, 2003.

[11] 张延旭, 胡春潮, 黄曙, 等. 基于 Apriori 算法的二次设备缺陷数据挖掘与分析方法[J]. 电力系统自动化, 2017(19).

[12] 吴刚勇, 张千斌, 吴恒超, 等. 基于自然语言处理技术的电力客户投诉工单文本挖掘分析[J]. 电力大数据, 2018(10).

[13] 杜修明, 秦佳峰, 郭诗瑶, 等. 电力设备典型故障案例的文本挖掘[J]. 高电压技术, 2018, 44(4): 1078-1084.

[14] 邹云峰, 何维民, 赵洪莹, 等. 文本挖掘技术在电力工单数据分析中的应用[J]. 现代电子技术, 2016, 39(17): 149-152.

[15] STEVEN B. Python 自然语言处理[M]. 北京: 人民邮电出版社, 2014.

电网信息安全防护的现状及思考

郑子洵，朱峰，齐晓明
（北京国网信通埃森哲信息技术有限公司，北京 100032）

摘　要：随着泛在电力物联网的不断发展，电网信息安全防护存在信息系统组成复杂、安全管理待规范、操作人员专业素养待提高等问题，采取引入风险评估、网络隔离和信息加密等先进技术以及统一安全标准、完善管理制度和增加培训机制等管理方法，提高电网信息安全防护水平，保障电网安全稳定运行。

关键词：电网信息；信息安全防护；物联网

1　引言

电力行业中的互联网络具有标准化、保密性、完整性和迅速性等特点，其中的信息数据与电力系统的安全稳定运行息息相关。因此，信息安全对于电力行业十分重要。电网信息安全包含的主要内容有信息的保密性、完整性和可用性。对于电力行业而言，信息安全不仅涉及规划发展、财务状况、商业模式等一般行业的问题，更会牵涉到社会稳定、居民生活等方面。其中，信息的保密性指公司内部人员均会根据其职位、阶层拥有相应的权限，不同权限的人员获取的信息种类和数量均存在差异；信息的完整性包括信息数据的内容、数据格式等的完整性，而且包括信息处理方式、传输转换的完整性；可用性指可以及时提供给已被授权用户所需信息的能力。

2　现状及发展需求

2.1　现状

随着计算机网络技术、大数据技术的不断发展，电力信息系统逐步向智能化、信息化转变。实际中，电力行业信息系统采用统一部署、分散控制、联合运行的方式运行，系统中各线路、设备、通信装置通过互联网互联、完成数据共享与信息交换，将发电、输电、配电和售电系统一体化。然而，存在信息系统组成成分比较复杂、各单位设备不统一且无统一操作标准和规范制度以及电力信息系统难易度不统一等情况，这些会导致一些电力系统信息安全防护问题。

2.2　存在的问题

当今，在泛在电力物联网建设不断推进的情况下，电力行业也开始从传统电力相关业务向新兴业务拓展，大量外部信息的汇入和内外部数据的交换导致电力信息系统更加复杂，相应的信息安全防护也出现了新的问题。

（1）信息系统组成复杂化，由原本营销、运检、调度等电力相关业务信息系统向联合外部新能源、电商、金融等综合信息系统转变，信息种类、数量以及相应的传输方式和处理方式的增加，加大了信息存储、传输过程中的安全隐患，需要采用更先进的技术提高安全管理的效率和可靠性。

（2）信息安全管理待规范，泛在电力物联网处于建设阶段，信息的多样性、复杂性导致还没有总结出一套高效可行的信息安全管理规范，故在实际操作过程中，存在各单位规范不一致、标准不统一的情况，导致效果不尽如人意。

（3）信息专业跨度大，当今信息多样性强，涉及电力、热动、通信、网络、计算机等多种专业，对于操作人员专业素养要求较高，非专业操作人员可能由于专业知识不足出现信息的错误录入等问题，极大地影响了信息安全的防护。

2.3　建设必要性

电力系统作为支柱型能源产业，关系着国计民生、社会稳定。伴随着泛在电力物联网的建设，电力行业不仅具有海量的电力相关数据信息，而且纳入越来越多的外部多领域、多元数据。重要信息的丢失，不仅会导致电力以及相关合作企业蒙受巨大的经济损失，

人民邮电出版社

而且会影响供电质量，从而影响人民的正常生产生活，不利于社会和谐稳定发展。因此，电力系统信息安全防护愈加重要。

3 改善措施

3.1 技术层面

3.1.1 风险评估技术

为了降低电力系统互联网遭到侵袭的概率，采用风险评估相关技术对电力心态的信息安全进行评估，提高信息安全水平，主要采用威胁分析技术、资产管理技术和脆弱性识别技术。

（1）威胁分析技术，主要以环境因素与人为因素，通过识别威胁和评估威胁来总结出信息遭遇威胁的种类及可能性。

（2）资产管理技术，主要用于具备高价值的信息资产（如文档、硬件等），通过划分资产类别和资产赋值，划分出不同信息的重要程度，制定相应的安全防护机制。

（3）脆弱性识别技术，主要用于潜在威胁、漏洞的发现，通过扫描软件或测试机制，判断出电力设备、系统是否存在信息安全隐患，为进一步制定对策提供支撑。

3.1.2 网络隔离技术

网络隔离技术是指两个或两个以上的计算机或网络在断开连接的基础上，实现信息交换和资源共享，即通过某种技术将多个计算机或网络实现物理上隔离的同时，可以完成安全的数据信息交换共享，其中包括物理隔离、硬件隔离、数据隔离和安全通道隔离。目前网络隔离仍以物理隔离为主，针对电力系统内部敏感网络进行物理隔离。安全隔离网闸作为比较常用的物理隔离装置，通过对数据进行病毒检测、防火墙、入侵防护等安全监测以及对用户的身份认证、权限判别，达到不同安全等级网络的有效隔离，并可根据职能和业务进行不同场景的应用。

3.1.3 电力系统信息加密技术

为应对信息传输过程中存在的信息丢失、信息失真等问题以及易受到网络攻击等威胁，采用信息加密技术对传输信息进行处理，对其传输途中的安全威胁起到防范作用，包括私钥加密算法和公钥加密算法。

（1）私钥加密算法

收发双方持有相同的密钥，基于硬件的特点增加了该算法的安全性，但是对密钥的管理成本较高，其中主要有数据加密标准（DES）算法和高级加密标准（AES）算法。

（2）公钥加密算法

收发双方使用的密钥不同，且几乎不可能通过加密密钥推导解得解密密钥，其可适应网络的开放性要求，大大降低了密钥的管理和分发成本，但是算法复杂、加密解密速率较低，其中最为著名的是数字签名技术（RSA），它能抵抗目前几乎所有的已知密码攻击。

3.2 管理层面

3.2.1 制定统一信息管理规范

信息管理规范仪旨在为信息存储、传输、操作、处理等各个环节提供规范标准，以减少因标准不同而导致的信息不完整、数据不准确的情况，主要包括信息存储标准、信息传输标准和信息处理规范。信息存储标准规定不同类型信息的存储格式与存储区域，支撑数据库信息安全管理方案的建立。信息传输标准规定不同格式信息的传输标准和传输信道要求，对不同信道实施不同级别的保护措施，保证信息传输的完整性、准确性。信息处理规范主要用于指导操作人员对不同类型、不同专业的信息进行处理，以免因操作原因导致数据丢失、失真。

3.2.2 完善管理制度

在电网公司内部成立信息安全防护小组，加强信息安全防护管理，小组主要包括信息管理员、操作审核员和网络监测员。信息管理员主要负责对操作系统、数据库等进行维护管理，在保障其不受病毒、黑客攻击的同时，做好系统信息、人员信息等更新维护，保证人员账户信息的唯一性、正确性和实时性。操作审核员主要负责对数据操作人员的操作进行审核，并在一定时间内备份其操作记录，以保障对突发状况的应急响应能力。网络监测员主要负责对信息传输网络状况的实时监测，运用风险评估技术及相应软件对传输网络的潜在威胁进行实时评估，并提出相应的解决方案，以降低网络遭遇病毒、黑客攻击等威胁的概率。

3.2.3 完善信息安全培训机制

在现有电力行业员工培训机制的基础上，强调信息安全的重要性，完善信息安全培训机制。其中，培训内容方面，每类信息安全培训内容由该信息数据所涉及的操作系统、传输网络、业务部门和信息安全防护部门相关人员共同编写，以保证各类信息的安全性

人民邮电出版社

和可用性；组织管理方面，针对信息安全防护内容的变化频率，由各职能部门与业务部门配合制定适当的培训、考核制度；经验交流方面，定期组织各部门对近期遇到的信息安全防护问题交流、讨论，从中总结经验、吸取教训，并依此更新培训内容，以提高培训质量和信息安全防护效率。

4 结束语

信息安全作为电网在互联网浪潮中保障稳定安全运行的关键，正在被越来越多的电网公司重视。随着泛在电力物联网的建设，越来越多的信息汇入电网系统，电网信息安全防护工作亟需建立高效可行的信息安全防护标准，并通过人员培训、组织管理的改革，向新一代电网信息安全防护体系转型。

参考文献：

[1] 张星.电力信息安全防护体系研究分析[J]. 科技创新与应用, 2018(14): 57-58, 60.

[2] 许魏. 电力系统信息安全防护关键技术研究[J]. 技术与市场, 2012(10): 67-67.

[3] 程帅. 电力生产应用中的信息安全及其防护[J]. 电子技术与软件工程, 2018, 134(12): 238.

[4] 孙宏意, 许轲. 电力系统计算机网络信息安全防护问题分析[J]. 中国标准化, 2019(6): 227-228.

[5] 王洁民. 风险评估在信息安全中的有效运用及关键技术[J]. 电子技术与软件工程, 2018(4): 225.

[6] 薛彩楼.基于电力行业的终端信息安全防护研究[J]. 科技风, 2018(28): 167.

[7] 李志红. 计算机网络隔离技术浅析[J]. 数字技术与应用, 2012(11): 194.

人民邮电出版社

泛在电力物联网标识管理服务平台建设研究

杨珂[1,2]，王焕娟[1,2]，秦日臻[1,2]，赵丽花[1,2]
（1. 国网电子商务有限公司（国网雄安金融科技集团有限公司），北京 100053;
2. 国家电网有限公司电力金融与电子商务实验室，北京 100053）

摘　要: 物联网标识是物的“身份证号码”，是实现物与物之间精准交互的核心技术，是推动物联网产业化发展的关键要素。目前电力行业面临着标识体系杂、信息融通难、感知能力弱等发展困境，构建泛在电力物联网标识管理服务平台，为电力行业的企业和用户提供灵活的标识编码注册和解析服务，破解企业间互联互通障碍，大幅降低上下游企业互联成本，全面提升电力系统各环节连接和智能感知能力，并打造基于标识码流量入口的物联网商业模式。

关键词：物联网标识；感知连接；编码体系；异构标识解析；营销

1　引言

以数据运算为基础的万物互联的前提，必须为物联网中的每一个物品、工序、资源和服务等编制唯一的数据标识。物联网标识是物的“身份证号码”，是实现物与物之间精准交互的核心技术，是推动物联网产业化发展的关键要素。2013 年，国家发展与改革委员会《物联网发展专项行动计划》提出“着力解决我国物联网应用的互联互通问题”，支持建成了我国物联网标识领域唯一的国家级平台——国家物联网标识管理公共服务平台[1]。2017 年，国务院印发了《关于深化“互联网+先进制造业”发展工业互联网的指导意见》，“推进标识解析体系建设”是主要任务之一。2018 年，工业和信息化部发布了《工业互联网发展行动计划（2018-2020 年）》，发起“标识解析体系构建行动”。物联网标识技术已在智能家具、智能环保、商品溯源、科学数据管理、数字权益管理等领域获得了广泛应用，并取得了良好的效益[2-3]。参考文献[4]将物联网标识技术与区块链技术融合，生成基于区块链的物联网标识编码，并用于智慧家庭场景中。

电力行业作为资产信息和数据信息“种类多、数量大、范围广”的典型能源行业，目前信息化程度较高，广泛使用 RFID 标签、条码、实物 ID 等标识对各类物资、人员、数据进行管理，支撑企业管理、生产控制、客户服务等工作。随着国家电网公司泛在电力物联网建设的推进，全息感知、泛在连接、开放共享等能力严重不足已成为制约公司发展的瓶颈，其根源在如下几个方面。一是标识体系杂，电力行业业务面广、上下游企业众多，不同企业采用的标识编码不统一，导致产品流通过程中，往往需要多次编码和贴标签，既降低工作效率，又难以实现信息的准确关联和自动获取。二是信息融通难，电力行业各专业系统自成体系，存在传感设备重复部署，未实现一次采集、共享共用；产业链上下游信息“孤岛”严重，产品售后失联，无法实现产品闭环优化设计等。三是感知能力弱，在物联网侧缺少感知来源，数据和信息的实时传输和共享难以实现，用户用能信息感知不及时、配电信息覆盖面不全，无法支撑综合能源服务、数据运营等新业态发展。

实现电力系统各环节万物互联是公司“三型两网”战略的迫切需求。泛在电力物联网标识管理服务平台为电力行业的企业和用户提供统一的标识编码注册和解析服务，高效、廉价地实现物联网信息获取、处理、传送与交换，支持商品条码、实物 ID 等国内外主流及企业自建标识体系接入，破解企业间互联互通障碍，大幅降低上下游企业互联成本，全面提升电力系统各环节连接和智能感知能力。平台为解决电力行业跨企业、跨平台甚至于跨国界的数据互通共享等痛点问题以及融入国家标识体系，实现全行业信息化、数字化、智能化升级改造，打造电力行业先进生产力，提供了一种先进可靠可行的解决方案。

基金项目：国网电子商务有限公司科技项目（No.5100/2019-72002B）

2 泛在电力物联网标识管理服务平台架构设计

面向电力行业，建设物联网标识节点及应用服务平台，实现标识注册、标识解析、标识代理服务、数据同步、业务综合管理等二级节点的基础服务能力[5]。同时面向电力行业的生产、制造、运行、服务特点，建设电力设备全生命周期管理、分布式能源数据共享支撑、智慧供应链管理等应用能力，打造功能和应用平台。

2.1 部署架构

泛在电力物联网标识管理服务平台作为统一智慧物联体系的基础设施，为智慧物联平台提供标识注册、标注解析及标识管理等功能支撑等功能，实现数据的统一编码和查询，如图 1 所示。平台采用二级部署架构，包括电力行业节点和企业节点。其中，行业节点是行业级物联网标识管理服务系统，同时是国网统一智慧物联管理平台的重要组成部分，由国网总部部署；企业节点部署于各网省公司、直属单位及供应商等企业，是企业级物联网标识管理服务系统，企业节点在技术架构上与国网节点兼容，向上对接国网节点的数据定义、标识解析等接口，也可根据应用需求开展本地化服务。

2.2 功能架构

泛在电力物联网标识管理服务平台从功能划分上主要包括企业服务层、公共基础层、应用支撑层和应用层，如图 2 所示。

（1）企业服务层

企业服务层对应企业节点，企业节点对接各单位自有业务系统及下游供应商业务系统，为各企业提供标识注册、元数据定义等服务，各业务系统在企业节点注册对外共享的数据并设置访问权限，企业节点返回注册数据的唯一标识编码信息。用户对标识编码进行查询时，企业节点通过标识解析功能，为用户提供权限范围内的相关信息。

（2）公共基础层

行业节点公共基础层具备以下基础功能：前缀分发管理、运行状态监控、标识解析、客户端 App、基础应用平台、安全控制、业务管理、连通体系等。行业节点接收企业节点的节点注册信息，审核通过后为其分配企业节点编码前缀，保证每一个企业节点有且仅有一个唯一的前缀，监测企业节点的运行状况，为企业节点提交的查询请求提供解析服务。行业节点具有扫码客户端等 App，并面向中小微企业提供“一站式”物联网标识解决方案。行业节点支持基于国产密码的公共密码基础设施，能够自主管理数据、访问权限和用户身份等，保证信息安全可控。行业节点向上对接国家顶级节点，向下对接企业节点，处于标识体系的关键位置。

（3）应用支撑层

应用支撑层用于支持电力行业各种应用的开发和

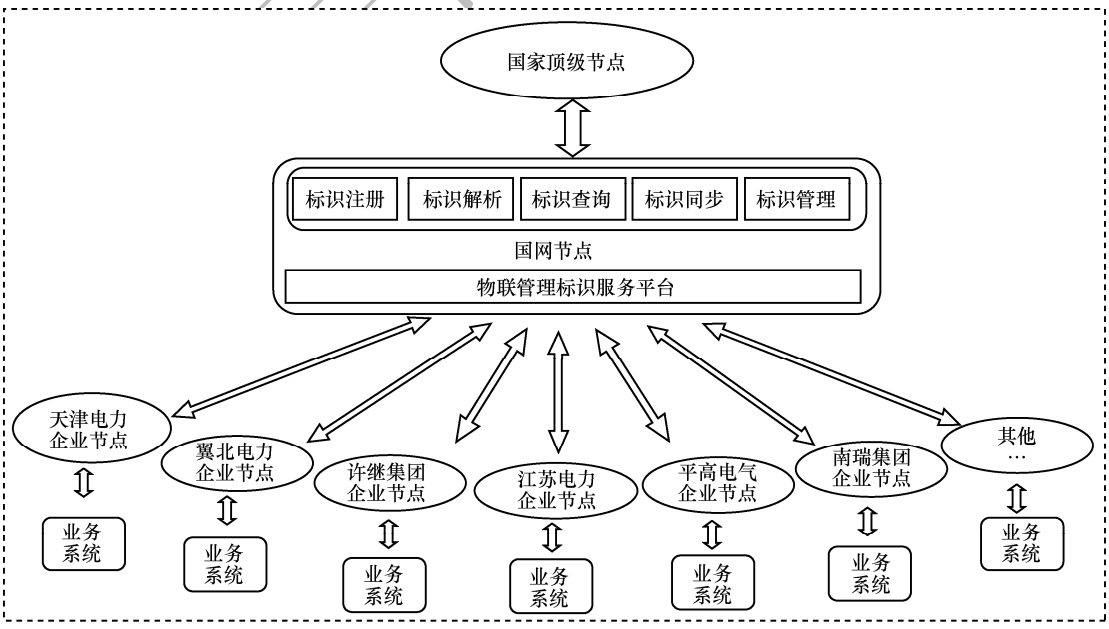


图 1 泛在电力物联网标识管理服务平台部署架构

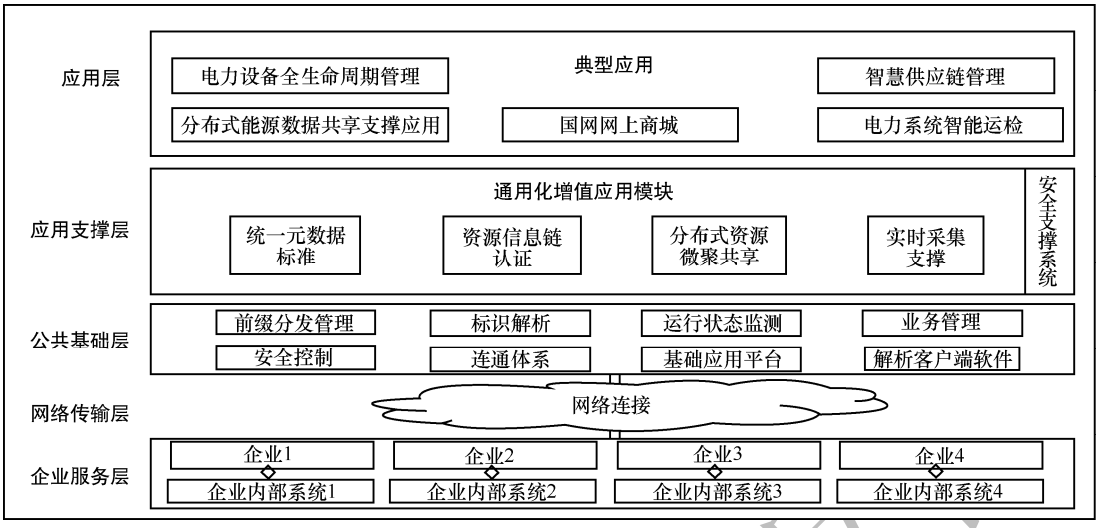


图 2　泛在电力物联网标识管理服务平台功能架构

运营，为应用开发者提供封装好的管理功能和开发接口，应用开发者可直接调用应用支撑模块的开发接口，快速有效地开发应用系统。所有的应用支撑模块都得到安全支撑系统的支持。统一元数据标准模块可让不同企业节点共享相同的元数据标准；资源信息链认证模块提供信息关联和信息链条双向链接功能；分布式资源微聚共享模块提供去中心化的数据共享机制，一次注册，共享共用；实时采集支撑模块实现实时采集和传输传感器数据功能。

（4）应用层

应用层基于公共基础层和应用支撑层，打造面向通用应用及企业特色应用的综合性应用服务平台，并对外提供通用化、基础化公共服务及特色化、增值化的电力行业专属公共服务体系，如电力设备全生命周期管理、供应链管理等。行业节点也可以结合电力行业的需求和特点，在公共基础层和应用支撑层之上开发行业所需要的其他应用系统，不断扩展和完善行业节点的功能。

3　泛在电力物联网标识管理服务平台应用场景

泛在电力物联网标识管理服务平台，为电力行业的企业和用户提供统一的标识编码注册及解析服务，促进电力行业的电力设备全生命周期管理、分布式能源数据共享、国网网上商城运营、智慧供应链管理、电力系统智能运检等应用，并打造基于标识码流量入口的物联网商业模式。

3.1　应用能力

（1）电力设备全生命周期管理应用能力

平台为电力行业的设备和设施等提供唯一的标识编码，支持电力行业设备的全生命周期数据（包含生产、销售、使用、检修、报废全过程的状态变化数据信息）的实时采集、追踪、查询与管理，建成开放、可控、可信的设备状态数据分发共享能力，实现来源可查、去向可追和责任可究。

（2）分布式能源数据共享支撑能力

平台为分布式能源参与方提供传感器等感知设备互联支撑，支持分布式能源生产和消费数据的采集、存证、共享、公证等，实现一次采集、多方共享，提升分布式能源生产和消费的透明度，维护电站用户的合法经济效益，加强政府监管力度，促进分布式能源数据流、价值流、能源流的多方流动。

（3）国网网上商城运营支撑能力

平台为国网网上商城的商户提供物联网标识服务，为每一件售出商品颁发唯一的标识二维码，消费者通过扫码能够全面了解商品详细信息、查验商品的真伪以及寻求售后服务等，同时商户基于标识二维码进行用户大数据搜集实现精准营销、个性化推荐和促销等。商城管理者通过信息共享、数据互通，加强商城商品的质量监控、服务监管，促进供应商商品品质及服务水平提升。

（4）智慧供应链管理应用能力

人民邮电出版

平台为车间中的零部件、设备、工序等提供标识服务，实现全维度信息采集支撑、全寿命周期质量信息归集与问题精准溯源等，通过与感知系统、定位系统、信息系统结合实现产品数据的全方位感知、采集、关联、处理，从而实现生产控制与仓储调度自动化智控。

（5）电力系统智能运检应用能力

平台解决目前运检工作中数据种类复杂、结构化/非结构化数据并存、各个业务系统数据割裂、数据标准不一、数据质量参差不齐等问题，建成具有自我及环境感知、主动预测预警、辅助诊断决策及集约管控功能，支撑运检业务管理信息化、自动化、智能化。

3.2 盈利模式

平台为电力企业和上下游供应链公司提供商品或设备物联网标识码及信息管理服务，按年或按标识码的个数收取服务费。

平台建设基于标识的供应商管理系统，客户通过扫码实现产品质量溯源，提升供应商的知名度以及信誉，从而提升其竞争力，带动销量，按年向供应商收费。

平台依托海量标识注册信息，建立电力设备全生命周期管理等应用系统，按次收取信息查询费。还可以为金融、保险、征信等业务提供企业分析报告，收取大数据服务费。

4 结束语

泛在电力物联网标识管理服务平台作为电力行业级标识节点，采用两级部署，向上对接国家顶级节点，向下联通所有电力企业节点，提供公共基础服务以及行业典型应用服务。平台加速传统产业转型升级，加快新兴产业发展壮大，推动能源行业数据共享融通，壮大能源大数据产业规模，带动能源装备技术创新，推动工业级芯片产业自主化发展，助推能源供应链智能化提升，优化上下游企业的营商环境。

在充分保证数据主权的情况下，实现跨企业信息互通共享及交易，是平台必须具备的核心功能。异构标识解析技术、多信息节点关联的标识发现技术、标识服务隐私保护及信息安全技术等都是值得研究的重要课题。

参考文献：

[1] 广州中国科学院计算机网络信息中心. 国家物联网标识管理公共服务平台白皮书[R]. 2019.

[2] 田野, 刘佳, 申杰. 物联网标识技术发展与趋势[J]. 物联网学报, 2018, 5(2): 12-21.

[3] 郭晓峰, 孙洵. Handle 系统的发展及应用[J]. 数字图书馆论坛, 2013(8): 18-24.

[4] 陈美娟, 朱晓荣. 基于区块链的物联网设备标识研究[J]. 物联网学报, 2018, 5(2): 22-30.

[5] 工业互联网产业联盟. 工业互联网标识解析二级节点建设导则(试行版)[R]. 2019.

人民邮电出版社

泛在电力物联网技术的应用研究

——以“光–车”互联系统为例

陈绍真[1,2,3]，王俊生[1,2,3]，伍燕[1,2,3]，吕梓童[1,2,3]

（1. 国网雄安金融科技集团，河北 雄安 071600;
2. 国网电子商务有限公司，北京 100053;
3. 国网电力金融与电力商务实验室，北京 100053）

摘　要：通过分布式光伏、“云储能”技术、区块链及物联网技术相结合，不但可以提升充电桩布设的合理性与易获取性，还可以切实减少碳排放和减少“弃光”现象。借助物联网技术将分布式新能源电站、储能装置、充电桩、新能源汽车等终端联结为一个有机整体，实现新能源的“产、配、消”等环节的智能服务，提高新能源、公共充电桩的使用效率。

关键词：电力物联网；区块链；共享充电桩；分布式光伏发电

1　引言

近年来，世界各国都在大力推广新能源汽车。我国也不遗余力，综合采取了多种措施促进新能源汽车的推广使用。在基础设施建设上，修建了智能充电高速公路，同时不断扩大公用充电桩的建设；在经济支持方面，国家财政对新能源汽车的产销环节都进行了有力的资金支持，以促进新能源汽车的研发、生产与销售。然而，当前新能源车在使用的过程之中，仍然存在充电不便利的问题，换句话说，现有的充电设施在数量或者布设的地理位置方面远远不能满足新能源汽车数量增加所产生的需求。另一方面，随着新能源汽车的不断推广普及，交通运输对动力能源的需求将逐渐从以汽油、柴油为代表的化石能源向电力进行转移，从表观上看，新能源汽车的大力推广将减少交通出行对化石燃料的需求，能够减少因使用石化燃料所产生的污染物，有利于改善人们的生活环境。但实际上，从我国电源的组成结构不难得知，火力发电仍然是我国电力生产的主要手段，其当前占比为 60%以上，尽管呈逐年下降趋势。因而，如若不改变新能源汽车的电力来源，推广新能源汽车只能是将污染从汽车运行城市转移到发电站所在地而已，与国家减少污染排放的初衷相悖。光伏发电为解决这一问题提供了可能，通过分布式光伏、“云储能”技术、区块链及物联网技术相结合，不但可以提升充电桩布设的合理性与易获取性，还可以切实减少碳排放和减少“弃光”现象，能够借助物联网技术将分布式新能源电站、储能装置、充电桩、新能源汽车等终端联结为一个有机整体，实现新能源的“产、配、消”等环节的智能服务，提高新能源、公共充电桩的使用效率。

2　现状分析及关键技术

2.1　新能源与新能源汽车现状

自 2016 年以来，新能源汽车的产销呈现出快速增长的趋势。据汽车资源网的研究数据显示，新能源汽车的市场规模有望达万亿，预计至 2020 年，我国新能源汽车产销量将达到 200 万辆；到 2030 年，我国新能源乘用车年销量将突破 1 300 万辆。其中，新能源大中型客车将成为客车销售主力军。2018 年至 2030 年间，新能源乘用车与大中型新能源客车的市场空间有望攀至 13.9 万亿元。在重要的基础设施——充电桩方面，截至 2017 年年底，中国充电桩数量达 45 万个，公共充电桩为 21 万个，按 172 万辆的新能源汽车保有量计算，新能源汽车的车桩比约在 3.8:1。充电桩基础设备仍然是新能源汽车发展的一块短板。为了跟上新能源汽车发展的步伐，在 2030 年新能源乘用车

人民邮电出版社

保有量接近 7 000 万辆的估计下，充电服务对应的市场规模将不低于 5 100 亿元。

最近的数据显示，2018 年全国光伏发电弃光电量达 54.9 亿千瓦时，按照每千瓦时电能 0.5 元的价格计量，全国整个年度因光伏发电“弃光”所导致的直接经济损失就达 27.45 亿元之多。而另一方面，我国光伏新增装机容量逐年增大，其中，分布式光伏电站新增装机容量增速呈上升趋势。国家在多年前为了支持光伏发电产业的发展，对该产业实施财政补贴，但近年来随着光伏装机容量的迅速扩大，光伏补贴支出对国家的财政造成了较大的压力，截至 2017 年年底，光伏补贴缺口就高达 455 亿元之多。未来，国家对光伏产业的补贴完全取消是必然趋势。因此，光伏发电产业未来的盈利主要将取决于：（1）光伏发电设备成本的下降；（2）光伏电力在差异化市场进行交易，通过满足特定电能需求进行差异化定价而实现盈利。

新能源汽车保有数量的不断攀升为分布式光伏电能的消纳提供了一个潜在市场。新能源汽车，尤其是纯电动汽车，在使用过程之中，需要补充电力的地点更为随机，这与分布式光伏发电站在地域分布上的广泛性极为契合。

通过区块链技术、物联网技术能够实现分布式光伏发电的实时感知与实时结算，分布式光伏电站的所有者的发电权益账户可以将其发电权益用来消费电力能源（比如用于支付新能源汽车使用公用充电桩充用的费用）。为了更好地理解区块链技术与物联网技术如何用于分布式光伏发电的结算，下文将分别对区块链和物联网技术的基本原理做简要介绍。

2.2 区块链技术

区块链本质上是一个对等网络（P2P）的分布式账本数据库。区块链是一串链接的数据区块，其链接指针是采用密码学 Hash 算法对区块头进行处理所产生的区块头 Hash 值。每一个数据块中记录了一组采用 Hash 算法组成的树状交易状态信息，保证了每个数据区块内的交易数据的几乎不可篡改，区块链里链接的区块也几乎不可篡改。区块链技术不是一个单项的技术，而是一个集成了多方面研究成果基础之上的综合性技术系统。其中，有 3 项必不可缺的核心技术，分别是共识机制、密码学原理和分布式数据存储。

第一，共识机制。所谓共识，是指多方参与的节点在预设规则下，通过多个节点交互对某些数据、行为或流程达成一致的过程。共识机制是指定义共识过程的算法、协议和规则。区块链的共识机制具备“少数服从多数”以及“人人平等”的特点，其中“少数服从多数”并不完全指节点个数，也可以是计算能力、股权数或者其他的计算机可以比较的特征量。“人人平等”是当节点满足条件时，所有节点都有权优先提出共识结果，直接被其他节点认同后，有可能成为最终共识结果。

第二，密码学原理。在区块链中，信息的传播按照公钥、私钥这种非对称数字加密技术实现交易双方的互相信任。在具体实现过程中，通过公/私密钥对中的一个密钥对信息加密后，只有用另一个密钥才能解开。并且将其中一个秘钥公开后（即为公开的公钥），根据公开的公钥无法测算出另一个不公开的密钥（即为私钥）。

第三，分布式存储。区块链中的分布式存储是参与的节点各自都有独立的、完整的数据存储。跟传统的分布式存储有所不同，区块链的分布式存储的独特性主要体现在两个方面：一是区块链每个节点都按照块链式结构存储完整的数据，传统分布式存储一般是将数据按照一定的规则分成多份进行存储；二是区块链每个节点存储都是独立的、地位等同的，依靠共识机制保证存储的一致性，而传统分布式存储一般是通过中心节点往其他备份节点同步数据。数据节点可以是不同的物理机器，也可以是云端不同的实例。区块链用于存储分布式光伏电站的发电权益，区块链智能合约能可以实现分布式光伏发电收益的实时智能结算。

2.3 物联网技术

物联网是借助互联网技术与信息传感设备将所有的物理设备以及人相互联结起来，实现信息的交换和通信的网络。围绕电力系统各环节，应用先进的通信技术与现代信息技术，实现电力系统各环节万物互联、人机交互，达到状态全面感知、信息高效处理、应用便捷灵活特征的智能服务系统，即为泛在电力物联网系统。物联网系统通过感知层、网络层、平台层、应用层分别进行信息的采集、传输、处理和应用。在感知层，通过各类传感器设备，可以自动采集到被监控设备的运行数据，如通过各设备中的传感器分别感知到光伏电站的上网电量数据、感知充电桩联接的储能设备电量数据、感知新能源汽车的位置信息以及汽车剩余电量数据等。这些数据借助信息通信网络传输到平台层，平台层实现对数据的清洗、建模与运算，最

人民邮电出版社

后输出处理结果，应用层则将平台层的输出结果转化为对应的服务或者指令信息。

3 “光–车”互联系统构成与功能

“光–车”互联平台通过通信网络将分布式光伏电站、云储能装置、充电桩、光伏发电结算系统和新能源汽车连接（如图 1 所示），实现这些装置或系统的相互感知，形成一个新能源电力物联网生态系统。整个系统按照架构可以分成感知层、网络层、平台层及应用层（如图 2 所示）。

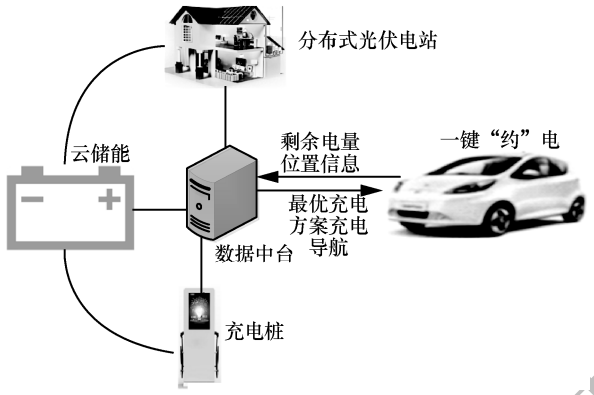


图 1 “光–车”互联系统

（1）感知层

感知层负责数据的采集和物物之间的数据传输，数据采集的技术包括传感器、条形码、二维码、RFID 射频技术等多媒体数据；数据的传输包含远近距离数据传输技术、自组织组网技术、协同信息处理技术、数据采集中间件技术等传感网络。感知层是实现物联网全面感知的核心。

在“光–车”互联体系中，分布式光伏电站的电力不并入传统的电力网络之中，而是利用“云储能”装置进行存储，充电桩与“云储能”装置相连，为新能源汽车提供充电服务。在所述“光–车”互联体系中，需要借助传感设备实现对分布式光伏电站向“云储能”装置供能数量的感知、对“云储能”设备电量信息的感知以及有充电需求的汽车的位置信息和剩余电量的感知。下文将提及的充电支付及充电线上预约服务中，还涉及用户身份、与支付账户信息的感知，此处，将主要通过二维码技术实现。

（2）网络层

网络层利用无线或有线网络对采集的数据进行编码、认证和传输，广泛覆盖的移动通信网络是实现物联网的重要基础设施，是物联网 4 层中标准化程度最好、产业化能力最强、最成熟的部分，其作为物联网协同感知的网络。



图 2 “光–车”互联系统功能架构

（3）平台层

平台层实现对终端设备和资产的“管、控、营”一体化服务。主要满足设备、数据和运营 3 个方面。既能向下连接和管理感知层，又向上提供开发能力和统一接口。

在本文所述的“光–车”物联系统中，从感知层采集到的数据，通过网络层传输至平台层，平台层通过内嵌的算法程序对输入数据进行处理（如清洗、规则化、归一化、主因子提取等）。根据平台最终所需要提供的服务，采用机器学习算法，构建分类预测、回归模型，实现预测结果的输出，并将结果或传输至本系统内接入的相关设备以使设备做出恰当响应的目的，或传入至应用层。

（4）应用层

应用层，通过计算技术和算法处理数据并提供服务，是物联网的最终目标。将物联网技术和行业信息化需求结合，是实现广泛智能化应用的解决方案集。其关键在于行业融合、数据资源的开发利用、数据安全保障等。

此层是物联网中极为重要的一层，是实现对接入网中的设备进行智能控制、向接入网中的人提供服务的关键所在。在“光–车”互联系统的应用层中，提供光伏发电自动结算、实现“云储能”设备的远程监测与控制、根据接入网中的新能源汽车的剩余电量和位置信息向汽车使用者推介最佳充电桩位置及所需等待时间等信息。

在光伏发电自动结算方面，传感设备每天指定时间节点（比如每日零时）采集一次电表的示数，平台根据过去 24 小时电站向外输送的电量，向电站受益人权益账户增加对应的权益数量，权益可以流通交易，

人民邮电出版社

亦可以用于消费（比如用于支付新能源汽车充电费用），接入网中的所有参与人交易信息均记录在区块链之中。

针对“云储能”与充电桩等设备的管理与控制，内嵌算法可以根据储能设备的储能情况判断设备的状态，当储能设备电量不足时或者目标充电桩的预约充电用户达到预设阀值时，充电桩电源从储能设备切换到传统电网供能，以提高充电效率满足需求。因为新能源汽车用电市场属于一个细分市场，使用公用充电桩的消费者对电力的需求弹性比较小，所以在该市场中可以进行差别定价，定价可以略高于民用电力市场中的电力价格。在该市场中，使用分布式光伏电站的电力作为供给来源，这一细分市场的特征使得电价定在光伏发电成本之上具有较高的可行性。尤其是针对某些充电需求旺盛的充电桩群，可以采用竞价的方式进行充电预购预约，如此可使加入其中的光伏发电站在脱离发电补贴的情况下实现盈利，从而达到减少碳排放的目的。此处提及的电力竞价交易应用是“光−车”互联系统发挥作用的关键之一。

应用层中很重要的一个组成就是新能源车用户应用，该应用根据用户的授权连接汽车内的系统，获取汽车的电池信息与位置信息，采用智能模型根据用户的行车习惯计算出需要补充电能的时间节点，并依据汽车所处地理位置与公用充电桩的位置信息以及被使用/预约信息，向用户推荐最优的备选充电方案（包括最优行车路线、等待时间最少的充电桩、最优充电价格等）。

4 结束语

本文阐述了基于物联网的“光−车”互联系统，该系统将分布式光伏电站、“云储能”设备、新能源汽车、光伏电站受益人、汽车用户联为一体，使系统的组成部分之间实现智能响应，或者向汽车用户提供最优的服务方案。该系统不仅提高了分布式光伏的结算效率，还使分布式光伏电站项目摆脱补贴实现盈利成为可能，更能够在便利新能源汽车充电的同时促进清洁能源的推广使用，达到减少碳排放改善环境的目的。为了使“光−车”互联系统未来能够给用户提供更加丰富的服务体验，后续在应用层将继续深入创新研究，特别在电力竞价交易应用领域，使之适应新的市场形势。

参考文献：

[1] 傅质馨, 李潇逸, 袁越. 泛在电力物联网关键技术探讨[J]. 电力建设, 2019(40).

[2] 李向阳, 喇果彦, 向项. 大云物移智等新技术在电网应用的研究[J]. 电力信息与通信技术, 2019, 17(1).

[3] 陈绍真, 王俊生, 伍燕. 基于古诺模型的能源互联网电能产品定价与交易模型研究[C]//2018 年电力行业信息化年会论文集. 北京: 人民邮电出版, 2018.

[4] MONTEIRO V, FERREIRA J, MELÉNDEZ A A N, et al. Electric vehicles on-board battery charger for the future smart grids[C]//2013 Technological Innovation for the Internet of Things: 4th IFIP WG 5.5/SOCOLNET Doctoral Conference on Computing, Electrical and Industrial Systems(DoCEIS 2013), April 15-17, 2013, Costa de Caparica, Portugal. Heidelberg: Springer, 351-358.

[5] SALEEM Y , CRESPI N, REHMANI M H, et al. Internet of things-aided smart grid: technologies, architectures, applications, prototypes, and future research directions[J]. Networking and Internet Architecture, 2017.

[6] SUN Y C, SONG H B, JARA A J, et al. Internet of things and big data analytics for smart and connected communities[J]. IEEE Access, 2016(12): 766-773.

人民邮电出版社

泛在电力物联网通信方式

李明[1]，汪俊洋[2]
（1. 国家电网黄冈供电公司，湖北 黄冈 438000;
2. 国家电网鄂州供电公司，湖北 鄂州 436000）

摘 要：第一届中国无线电大会在北京召开，标志着电力无线专网进入发展快车道，同时为泛在电力物联网提供了新的通信方式。随着时代的高速发展，电力企业输电、变电、营销等各专业的业务需求爆发增长，由于微波、载波通信已经逐步退出历史舞台，光缆建设成本过高、无线公网安全性有待增强、各专业通信需求分散等原因，如何实现电力系统各环节的万物互联、打造状态全面感知、信息高效处理、应用便捷灵活的泛在电力物联网成为了电力通信专业的新课题。首先介绍了各类电力通信方式，然后就主流电力通信方式运用进行分析，最后对泛在电力物联网的通信方式开展了探析。

关键词：泛在电力物联网；电力通信；无线网；发展应用

1 引言

随着经济的发展、社会的进步、科技和信息化水平的提高以及全球资源和环境问题的日益突出，电网发展面临新的课题和新挑战，依靠现代信息、通信和控制技术积极推动泛在电力物联网建设，适应未来可持续发展的要求，已成为电力企业积极应对未来挑战，建设具有卓越竞争力的世界一流能源互联网企业的重要举措。通信从广义上指需要信息的双方或多方在不违背各自意愿的情况下采用任意方法、任意媒质将信息从某方准确安全地传送到另一方。在电力行业中通信方式在几十年的发展中已经走过了载波通信、微波通信，正处于光纤通信和无线通信的黄金时期，而推动通信方式变革的根本动力就是日益增长的数据信息需求和科技的进步。

2 电力通信方式

2.1 载波通信

电力载波通信是指利用已有电力线，通过载波方式将模拟或数字信号进行高速传输的技术，它最大特点是不需要重新架设网络，通过电线就能进行数据传递，据统计在“八五”初期，全国 110 kV 及以上电力线载波话路公里数已达 26 万，到“十一五”期间话路公里数超过 65 万，电力载波通信存在通道干扰大、信息量小，再加上设备技术、管理维护等因素造成的设备稳定性差、故障率高等问题,电力载波通信已经难以适应现代电网对通信质量的要求。

2.2 微波通信

微波通信是利用微波频段（波长为 l m~1 mm 或频率为 300 MHz~300 GHz 范围的电磁波）的无线电波把待传递的信息从一地传送到另一地的一种电信方式，微波通信的主要方式是视距通信，易被反射和阻断。随着智能电网的建设，发电站、变电站、电力线路的数量呈几何倍数增长，大数据即巨量数据集合的提出，电力微波通信已经难以满足电力行业通信的现实需求。

2.3 光纤通信

光纤是光导纤维的简写，是一种由玻璃或塑料制成的纤维，光纤通信以光波作为信息载体，以光纤作为传输媒介利用光的全反射原理实现信息的传递，1966 年，由英籍华人高锟（Charles Kao）发表的论文提出用石英制作玻璃丝（光纤），其损耗可达 20 dB/km，可实现大容量的光纤通信，引发了通信技术的一场革命。光纤通信容量大、传输距离远、信号干扰小、保密性能好等优点使光纤通信迅猛发展，在电力行业已然成为主要通信手段之一。

2.4 无线通信

无线通信是利用电磁波信号可以在自由空间中传播的特性进行信息交换的一种通信方式，这一技术已深入到人们生活和工作的各个方面，已知在国家电网

人民邮电出版社

公司无线通信逐步在配电自动化、用电信息采集、精准负荷控制等电网业务使用，无线通信具有建造成本低、不依靠物理线路、不受工业环境的限制、故障诊断容易、便捷、扩展性强等优点，在电力线路末端使用空间广泛。

3 基层电力企业通信现状

3.1 地市电力企业层面光纤线路现状

3.1.1 光缆网络现状

以湖北省某地市为例，截至 2016 年 12 月该市拥有通信站点（变电站、直调电厂、用户变、二级单位）约 250 个，光纤覆盖率达到 100%，全区光缆总长度超过 5 300 km，其中 OPGW 光缆约占 50%，ADSS 光缆约占 10%，普缆约占 40%，全区各县（市）供电公司均已建成相对完善的光纤通信网络。目前，该市电力通信电路运行方式为资源共享、电路互为备用。电路分配原则采取互为备用的电路应尽量做到完全独立，网内站点将国网一级骨干电路或省网三级电路、地网四级电路混合互为备用，环型、链型结构光路在正常运行时光缆路由满足 *N*−1 原则；在光路故障、检修情况下，光缆路由满足 *N*−1 原则。

3.1.2 光缆运行存在问题

以该市 2016 年光缆运行情况为例，该地区 2016 年光缆总故障 83 次，总故障时间超过 14 万 min，平均单次故障时长约为 28 h。光缆故障分别有以下几种：外力破坏 70 次，光纤老化 11 次，其他 2 次；在外力破坏故障中，被车挂断 29 次，市政建设及施工损坏 18 次，鼠咬 12 次，倒杆拉断 4 次，着火致损 2 次，天灾 5 次。另外，随着地市电力企业管理工作的开展，由于 35 kV 多采用 110 kV 变电站作为汇聚点附挂，受多方面因素制约光缆无法实现双路由覆盖，一旦光路中断会导致多个变电站业务全停，站所合一的 35 kV 站点营销业务也将受到影响。可见，地市电力企业面临的光缆网络风险点主要有光缆路由单一和光缆纤芯资源紧张两大问题。

3.2 地市电力企业层面无线网络现状

3.2.1 无线公网

（1）近年来，配电自动化工程在湖北省各地市逐步开展，武汉、鄂州、宜昌、荆州公司配网自动化试点区域内通信接入网已建成投运，设备覆盖率 100%，配网自动化通信主要是采用光纤专网由 EPON（由 ONU、OLT 组成）设备组成，目前，全省 EPON 设备投运约 1 000 套。在设计、建设过程中光缆建设成本高、部分地点不具备光缆建设条件的问题日益突出，而采用无线公网的数据传输方式则可以圆满地解决成本高、建设难的问题，有利于解决“最后一公里”接入难题，目前，湖北地区配电自动化工程通信方式逐步采取光纤通信和无线公网结合的方法。

（2）“十九大”确立了清洁能源优先发展战略，湖北地区分布式光伏发电、风电发电项目逐渐增多，国家电网公司发布的《分布式电源接入电网技术规定》（Q / GDW 1480 — 2015）第 11.1.3 条指出“通过 380 V 电压等级并网的分布式电源，以及通过 10（6）kV 电压等级并网的分布式光伏发电、风电、海洋能发电项目，可采用无线公网通信方式（光纤到户的可采用光纤通信方式），但应采取信息通信安全防护措施。”该文件为分布式电源通信采用无线公网的方式提供了依据和指导，目前，湖北省 10 kV 及以下电压等级并网的分布式新能源基本以无线公网方式并网。

（3）长期以来如何提升电力用户用电信息采集效率这一难题始终困扰电力营销人员，用电信息采集始终找不到合适的通信手段，光纤 EPON 通信技术建设成本过高，难以实现全面覆盖；电力线载波与微功耗无线（ZigBee、Wi-Fi 等）技术抄收存在一定失败率，可靠性难以得到保证；无线宽带方式使用 2.4 Gbit/s 和 1 800 Mbit/s 的频段，需要使用部门向无线电管委会申请该频段的使用权，具有较大困难，因此，无线公网成为提升电力用户用电信息采集效率的最佳方式，初步统计湖北省无线公网约共有节点 24 万个，其中地市公司约 18 万个，县（市）公司约 6 万个，无线公网租用由市县公司各业务部门自行管理。

3.2.2 无线专网

2018 年 9 月 19 日，在北京举办的第一届中国无线电大会上，国家电网信息通信部副主任王磊分享了“电力无线专网建设与应用”的思考，他提出电力行业需要和通信行业合作共同开展电力专网的建设。根据国网公司各项业务需求和技术经济分析，国家电网有限责任公司在已授权 1 MHz 带宽的基础上向工信部申请增补 7 MHz 频率资源，同年 9 月上旬获批增补 6.25 MHz 频率资源，目前，国家电网已拥有 230 MHz 频段的 7.25 MHz 带宽用于建设电力无线专网。电力专网试点工作——LTE 电力无线专网，自 2009 年开始研发，有 11 个省（市）公司（北京、天津、冀北、江苏、浙江、福建、湖南、江西、重庆、辽宁、蒙东）

已经建设成具有一定规模的 LTE 电力无线专网。

目前，地市电力企业层面无线专网尚处于空白，按国网公司最新规划 2019—2020 年将建设无线专网基站 2 500 余座，接入终端数十万个，至“十三五”末初步建成有效覆盖全网范围 C 类及以上供电区域的无线电力专网。

3.3 地市电力企业层面其他通信方式现状

湖北省内电力载波通信基本退出运行；微波通信基本停用，大部分微波铁塔已拆除，少数几条国家电网管理微波设备尚处于热备用状态；各地市公司均配备有应急单兵卫星通信设备，每年开展地市公司应急演练中均有使用。

4 泛在电力物联网通信方式分析

4.1 骨干网络

自 1966 年，英籍华人高锟就光纤传输的前景发表了具有历史意义的论文，该文分析了造成光纤传输损耗的主要原因，从理论上阐述了有可能把损耗降低到 20 dB/km 的见解。4 年后，美国康宁公司研制出衰耗 20 dB/km 的光纤，证明光纤作为通信介质的可能性。至此，光纤才真正开始应用于光纤通信。光纤通信较之于其他方式具有无可比拟的优势：（1）通信容量大、传输距离远；（2）信号串扰小、保密性能好；（3）抗电磁干扰、传输质量佳；（4）光纤尺寸小、重量轻、便于敷设和运输等优点。进入 21 世纪以来，中国的光纤通信以日新月异的姿态快速成长，截至目前，我国已累计铺设光缆超过 400 万 km，光纤用量约 8 000 万 km，随着互联网的发展、大数据的提出，用户对光纤通信网的传输速度和容量需求不断增长。

电力行业已经建成以光纤通信为骨干网络的通信方式，以湖北省电力通信网为例，目前已实现全区 220 kV 以上站点双光缆覆盖率 100%，110 kV、35 kV 站点和供电所（营业厅）自建光纤覆盖率均达到 100%。建成大容量骨干传输网和地县通信传输双网络，省、地县传输带宽分别提升 40 倍、5 倍，实现双万兆到市、双千兆到县、千兆到站（变电站）所（供电所、营业厅）。由于无线网的传输容量限制和保密性等因素制约，在骨干传输网和各站所之间尚不具备无线网的使用条件。因此，可以预见在泛在电力物联网建设期间光纤通信将成为骨干网络的主要方式。

4.2 终端通信接入网

“三型两网”在国家电网公司的提出，有力推动供电企业率先实现通信方式的多样性结构形成，为构建全球能源互联网打下坚实基础，实现国家电网公司数字化智慧运营，建设具有卓越竞争力的世界一流能源互联网企业。同时，也对电力通信网提出了新的挑战，终端通信接入网“最后一公里”的通信方式至关重要。光纤通信在终端接入网的运用建设成本较之骨干网络中的建设大幅提升，主要是终端节点数量庞大、建设环境复杂等因素制约，因此，无线网的使用在电力终端接入更具优势。

电力无线专网作为行业性网络，已陆续启动了电力无线专网技术研究、标准制定、频谱资源申请、产品研发定制等相关工作，并初步形成阶段性成果。当前无线公网尚处于 4G 大规模商用阶段，5G 将是产业未来的发展重点，由于电力无线专网尚未具备投运条件，无线公网的使用已然成为当下终端通信接入网的最佳选择，无线公网接入具有如下优势：（1）建设成本低，充分利用通信商在运设备，节约资源；（2）建设工程周期短、适应性强；（3）扩展性好，可以根据电力终端个体要求制定通信容量、速率需求；（4）设备维护方便。

4.3 电力无线专网在泛在电力物联网中的应用

4.3.1 电力无线专网的摸索

早在 2009 年基于 LTE 的电力无线专网就开始在北京、天津、冀北、江苏、浙江、福建、湖南、江西、重庆、辽宁、蒙东，共 11 个省市公司开始研发建设，目前已形成一定规模的 LTE 电力无线专网，从应用效果来看，已经完成 22 类业务的接入，业务支撑效果良好，供电可靠性得到有效提升，11 家省市公司优质服务水平显著增强，电网运维效率较之以前大幅提高，智能电表集采周期从原来的一天缩短至 15 min，电力无线专网已实现数据、语音、图像、视频等业务的泛在接入和可靠承载，基本满足电力系统发输配变用环节的业务通信需求。

4.3.2 电力无线专网的春天

随着国家能源局发布《配电网建设改造计划(2015—2020 年)》后，全国范围内配电网改造升级加速明显，对通信网络的需求进一步提升，如何打通“最后一公里”成为电力终端接入网的重中之重，而电力无线专网因其安全可靠、泛在灵活的优势，成为支撑电力终端通信接入网建设的重要选择。2018 年 9 月，工信部批准对国网公司增补 6.25 MHz 频率资源，至此，国网公司已拥有 230 MHz 频段的 7.25 MHz 带宽

人民邮电出版社

用于建设电力无线专网，基本满足电力业务需求。同年，第一届中国无线电大会在京召开，电力无线专网产业联盟成立，电力无线专网技术研究、标准制定、频谱资源申请、产品研发定制等工作相继启动或已形成阶段性成果。本次电力无线专网产业联盟凝聚了科研机构、通信设备生产商、系统集成商、通信服务商等产业骨干力量，旨在加强以 LTE 230 为主、涵盖 LTE 1800、NB-IoT、LoRa 等技术体制的无线专网技术研发应用，重点在于制定、推广电力无线专网标准体系，构建完善的电力无线专网产业生态，促进电力无线专网产业发展，满足智能电网多业务承载需求，增强电网综合服务水平。

5 结束语

通信技术已成为建设泛在电力物联网的关键一环，实现全息感知、泛在连接、开放共享、融合创新对电力通信的传输速率、覆盖范围、信息安全提出了全新的挑战，可以预见电力通信在未来将呈现出以电力光纤专网为骨干网络、电力无线专网终端通信接入的多样性通信方式。

参考文献：

[1] 王辉. 浅谈光纤通信技术在我国的应用[J]. 电子世界, 2014(12): 166.

[2] 姜有泉, 汤亚芳, 黄良, 等. 智能配电网无线通信系统可靠性研究[J]. 电力大数据, 2017(12):52-55.

[3] 徐玉蓉, 陈田. 探究光纤技术发展及其在电力通信中的应用[J]. 信息系统工程, 2018(1):166.

[4] 刘伟. 光纤技术发展及其在电力通信中的应用[J]. 电子技术与软件工程, 2017(23):46.

[5] 徐婧婧. 无线通信技术及在电力通信专网中的应用研究[J]. 企业技术开发, 2016(12):77-78.

人民邮电出版社

泛在电力物联网战略部署实践

赵威，孙绍辉
（国网黑龙江省电力有限公司信息通信公司，黑龙江 哈尔滨 150000）

摘　要：为全面推进国家电网有限公司“三型两网”建设，泛在电力物联网的建设已成为当下工作的重中之重。国网黑龙江电力信通公司充分利用现有技术储备落地项目，紧紧围绕“三型两网世界一流”能源互联网企业建设要求，积极开展泛在电力物联网建设切入点探索研究。介绍了我国 IDC 建设现状，详细阐述了国网黑龙江电力信通公司“多站融合”项目建设的思路、目标及实施情况。

关键词：泛在电力物理网；多站融合；数据中心站

1　引言

目前，国家电网有限公司已全面推进“三型两网”建设，加快建设具有全球竞争力的世界一流能源互联网企业。作为“三型两网”建设的重要内容和关键环节，建设泛在电力物联网为电网运行更安全、管理更精益、投资更精准、服务更优质开辟了一条新路，同时也可以充分发挥电网独特优势，开拓数字经济这一巨大蓝海市场。建设泛在电力物联网是落实“三型两网、世界一流”战略目标的核心任务。

近年来，随着国网黑龙江电力大力推进全业务统一数据中心、多维精益管理体系变革、同期线损监测治理、电网资产统一身份编码等重点项目建设，数据共享和业务融合逐步向纵深推进，为企业和电网高效运营提供信息数据支撑，为泛在电力物联网建设提供丰富的数据资源。

作为泛在电力物联网建设的重要组成部分，国网黑龙江电力信通公司承接了“多站融合”建设工作。公司经过充分调研论证，按照泛在电力物联网战略要求，结合互联网思维，深入挖掘用户痛点，攻坚克难；在经营上，采用了适配的组织架构、商业和运营模式；在内部，构建与各专业部门沟通渠道，在外部，打造共建共治共赢的能源互联网生态圈，与全社会共享发展成果。

2　我国 IDC 建设现状

2.1　IDC 行业发展现状

由于互联网技术飞速发展，当今社会已步入日新月异的智能化时代。海量数据被物联网设备采集、传输并存储于云平台中，人工智能技术利用高性能定制芯片，对历史数据进行分析形成“经验”，利用实时数据和“经验”进行快速决策。数据的采集、传输、存储、分析、共享构成了未来社会的数据化形态。人们也已经习惯于通过抖音、快手等短视频、直播类软件获得快乐，VR/AR 技术在游戏、电影领域迅速普及，2017 年泛娱乐产业规模达 5 484 亿元，占数据经济 20%，大数据量应用发展迅猛。

IDC 作为数据和计算的基础载体之一，市场规模增速显著。2017—2018 年，中国 IDC 市场总规模分别为 946.1 亿元、1 228 亿元，同比增长分别为 32.4%、29.8%，预计 2020 年，市场规模将超 2 000 亿元。

2.2　传统 IDC 行业发展及存在的问题

传统 IDC 的典型特征为集中、大规模部署，综合土地建设成本、能源政策、自然环境等因素限制，一般建设在偏远地区。随着人工智能、边缘计算等技术的兴起，传统数据中心与用户需求存在以下的矛盾。

（1）大数据量应用企业发展与租用 IDC 高昂成本之间的矛盾

建设 IDC 的成本受场地、土建、市政、电源等因素影响，整体投资周期长、用户租赁价格高。2018 年，虎牙公开总营收为 46.63 亿元，净利润为 4.61 亿元，IDC 成本高达 6.527 亿元。2019 年年初，直播平台三巨头之一熊猫直播宣布破产，逐年增加的高昂 IDC 租赁费用是其破产的重要原因之一，IDC 租用成本已经成为企业发展的负担。

人民邮电出版社

（2）集中式数据中心架构与物联网发展之间的矛盾

集中式数据中心将难以满足万物互联时代下高频、高交互的 M2M 需求，联网设备几何级的增长以及交互式的高频化，带来了海量数据的实时传输需求。从互联网到物联网的演进，需要进行数据中心和网络架构创新。

（3）新兴技术与 IDC“完美”运行环境之间的矛盾

区块链、机器学习等新技术在部分业务应用上，对机房环境、网络带宽及延迟、设备稳定性的依赖度大大降低，IDC 提供的“完美”运行环境将会造成资源的浪费。

3 “多站融合”数据中心站建设

国网黑龙江电力信通公司经过充分调研论证，凭借在信息通信软硬件开发运维方面雄厚的技术和人才储备，以“整合资源、专业运营、比特储能、实现盈利”为目标，在如何实现数据中心站、储能站、北斗卫星地面基准站、5G 基站在电力领域有效融合、高效应用的课题上持续进行探索，适用于“多站融合”的高密度集装箱式数据中心逐步从蓝图变为现实。“多站融合”数据中心站未来发展潜力巨大，尤其分布式特点能够解决政府、大型央企和互联网企业的行业痛点。公司不断完善“多站融合”运营模式、改进加强多站融合运营工作，在黑龙江省全面部署分布式数据中心站，站站互通互联，相互感知、相互协同，形成去中心化的雾计算网格，实现数据中心站、储能站、北斗卫星地面基准站、5G 基站对泛在电力物联网建设的强力支撑。

3.1 建设思路

（1）合理利用投资，引入社会资本

在“多站融合”建设初期，以低投入做好商业模式验证和技术验证；在业务扩张期间，利用资源优势，引入社会资本实现共赢。

（2）谨慎投资，用户定位精准

杜绝盲目大面积推广建设，坚持以用户需求为导向，利用建设较快的优势，快速落实资源。

（3）由简单到复杂，逐渐实现高回报率

先期开展机柜出租、共建 5G 基站等简单盈利模式，实现资金快速回流与业务验证；后续提供高附加值的信息通信服务，提升资源价值回报率。

3.2 建设目标

利用互联网思维，针对已识别痛点，充分利用国网公司资源优势，梳理出目标用户，注重精准投资，充分考虑对内实用性、经济性和基层应用的便捷性，对外广泛连接内外部服务资源和服务需求，打造能源互联网生态和新的利润增长点。

3.3 建设情况

国网黑龙江电力信通公司充分利用自身在信息通信方面的技术优势，生产符合龙江低温特色的集装箱式数据中心，参照国际集装箱通用标准分为小型集装箱数据中心和大型集装箱数据中心。

小型集装箱数据中心 20 尺长内径：5 898 mm × 2 352 mm×2 390 mm，单模块设计总功率 80 kW，制冷总量 50 kW，可容纳 6 个机柜（75 台 2U 服务器），单柜满配总重量 11 t。

大型集装箱数据中心 40 尺长内径：12 024 mm× 2 352 mm×2 390 mm，单模块设计总功率 225 kW，制冷总量 120 kW，可容纳 15 个机柜（210 台 2U 服务器），单柜满配总重量 21 t。

相比传统数据中心较大的空间占用，集装箱数据中心可利用变电站内电源、网络和部分闲置土地等资源，通过高密度、模块化建设，不仅提高了数据中心的运行健康性，而且实现了对北方高寒气候的良好适应性。高密度集装箱式数据中心可承载大计算量业务，通过自主研发的雾平台组建“电力盒子”进行统筹管理，形成分布式数据中心，实现内外部数据就近接入、存储和分析。建成后，集装箱数据中心可长期稳定运行，支持通过网络对集装箱本身和内部安装设备进行远程管理和操作，提供机房所有动环要素，可以采集分析箱内设备运行参数，提高自动化运维能力。

随着泛在电力物联网建设工作持续深入开展，电网内部运维对象数量急剧增加、范围不断扩大、运维难度持续升高。国网黑龙江电力信通公司将充分利用技术储备和应用经验，打造“多站融合”的同时，建设高度灵活、一键式操作的微工具等自动化运维利器，借助自动化运维平台的高效性、开放性、扩展性，不断实现技术突破，持续提升自动化运维水平，充分发挥“多站融合”突出优势，为国家电网有限公司实现“三型两网”战略目标提供强有力支撑。

国网黑龙江电力信通公司不仅实现“多站融合”项目的技术创新，而且探索、验证以低投入实现多站融合有效产出的商业模式。开展主机托管、带宽出租

人民邮电出版社

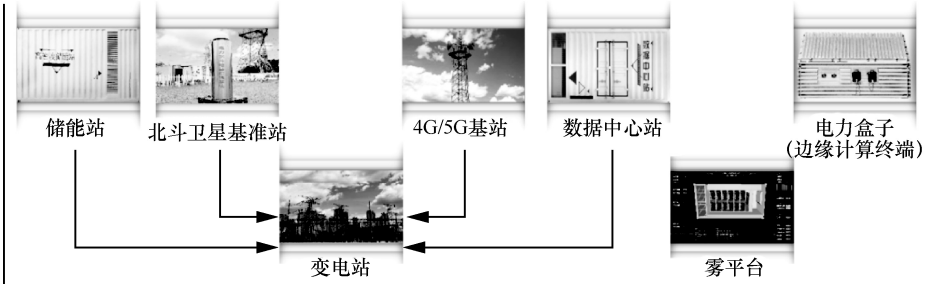


图 1 “多站融合”架构

等对外租赁业务，提供 IT 资源私有云、边缘计算等增值服务，拓展新的效益增长点。通过搭建“多站融合”统一资源服务平台，如图 1 所示，科学调配空间资源，存储、整合、分析内外部数据资源信息，在实现资源高效管控与运营的道路上走在前列。

4 “多站融合”数据中心站未来发展方向

随着“多站融合”工作深入开展，国网黑龙江电力信通公司积极学习其他行业相关知识，关注大众的生活需求，寻找“多站融合”未来发展的途径和空间，主要包括以下两方面。

（1）在发展中形成行业标杆，再寻找新的业务增长点

公司应深入挖掘、稳健自身的业务，在发展中总结自身优势，结合行业的痛点，在社会上进行推广并实现盈利。

（2）优化组织机构，突破人才壁垒

在“多站融合”的建设与运营过程中，深刻体会到了在没有资源优势情况下开展运营工作的难度。以往国有企业的良好运营依赖于资源的垄断，在激烈的市场竞争下，公司需要依靠产品质量、性价比和优质服务进行竞争，归根结底就是人的竞争。在此次试点中的参与人员具有敢拼、敢闯的素质，确保能够短期见成效，但是从长期考虑，需要完善现有人员进出、奖励等制度，提升竞争能力。

5 结束语

本文介绍了国网黑龙江电力信通公司“多站融合”项目建设的思路、目标及实施情况。公司未来将结合“三型两网”建设，通过省内 13 家地市供电公司多站融合建设以及 73 家县级供电企业泛在电力物联网络节点加固改造，实现基础设施标准化、泛在物联应用平台化、信息运维自动化。一方面解决国网黑龙江电力新上划农网单位信息化建设基础薄弱的问题，另一方面，建成泛在电力物联网的区域枢纽型节点，初步形成泛在电力物联网网架结构，为实现国网公司建设世界一流能源互联网企业的战略目标做出有力支撑。

参考文献：

[1] 陈麒宇. 泛在电力物联网实施策略研究[J]. 发电技术, 2019, 40(2): 99-106.

[2] KARMAKAR A, DESAI R. 能量收集技术为物联网设备供电的发展现状与未来趋势[J]. 中国集成电路, 2017(8): 24-27.

[3] 蔡泽祥, 孙宇嫣, 郭采珊. 面向泛在电力物联网的支撑平台与行业生态构建[J]. 机电工程技术, 2019 (6): 1-4.

[4] WANG W L , WANG D , JIA H J , et al. Review of steady-state analysis of typical regional integrated energy system under the background of energy internet[J]. Proceedings of the CSEE, 2016, 36 (12): 3292- 3305.

[5] 汪洋, 苏斌, 赵宏波. 电力物联网的理念和发展趋势[J]. 电信科学, 2010(Z2): 9- 14.

人民邮电出版社

泛在物联网终端设备安全威胁与防护技术

郭永和，闫龙川，何永远，赵子岩，朱京
（国家电网有限公司信息通信分公司，北京 100761）

摘　要：物联网终端设备安全是泛在电力物联网建设过程中需要解决的重要问题。随着海量物联网终端接入，传统的以边界隔离为主的信息安全防御手段难以适应新形势下安全防护的需求。就泛在物联环境下终端设备所面临的安全威胁和防护技术进行探讨。

关键词：物联网；终端；信息安全

1　引言

随着国网公司建设泛在电力物联网战略的出台，物联网技术又一次成为了资本市场的新热点。从发展前景来看，物联网技术可以深刻改变传统产业形态，开拓产业、经济和社会发展的新潮流。全球联网设备数量高速增长，“万物互联”成为全球网络未来发展的重要方向。据 GSMA 预测，到 2025 年，工业物联网设备数量将达到 138 亿。物联网设备的安全问题日益成为人们关注的焦点。可以预见的是，在不远的未来。物联网安全事件频发，全球物联网安全支出将不断增加。文中就物联网终端设备存在的安全风险及安全防护技术发展进行介绍。

2　物联网终端类型

物联网终端系统的主要功能是数据采集和设备控制。按照功能特点分类，物联网终端系统包含终端和物联网网关两大类设备[1]。

（1）物联网终端

物联网终端是感知层的基本单元，是数据信息的采集者和控制命令的执行者。按照功能和技术的复杂程度，物联网终端可以分为轻型终端和复杂终端。轻型终端结构简单、功能单一、成本较低，通信方式以低功耗近场通信体制为主，需通过物联网网关与物联网服务器端通信。此类终端的典型设备包括智能门锁、智能温控、烟雾报警器、门禁、智能开关、射频标签等；而复杂终端通常内置处理器和操作系统，具备一定的计算处理能力可以实现更多功能，可通过移动通信网络（2G/3G/4G/5G）或 Wi-Fi、以太网与物联网服务端进行数据交互，典型的复杂终端包括监控摄像头、智能家电、工业控制设备等。

（2）物联网网关

物联网网关的主要作用是网络的汇聚接入，一个网关通常支持多种通信方式，如蜂窝移动通信、ZigBee、NB-IoT、LoRa、Wi-Fi、以太网等。一方面，物联网网关将终端采集到的数据进行处理聚合后，发送给服务端；另一方面，它接收服务端系统发出的控制命令，并以此控制终端执行相应的动作。随着技术的发展，物联网终端数量不断增加，物联网网关的计算处理能力不断增强，相应出现了边缘计算的概念。一些具备较强处理能力的物联网网关可以作为边缘计算设备，替服务端承担一部分实时性强的物联网数据处理工作。

3　物联网终端安全风险

泛在物联网终端侧具有设备类型多、分布范围广、无人值守、不能或者难以安装终端管控软件的特点。这些特点使得物联网终端系统的安全风险很容易暴露出来。典型的物联网终端安全风险包括如下几种。

（1）终端软件漏洞

受其自身成本所限，大量的物联网终端没有包含提供信息安全防护功能的模块，同时缺乏定期安全更新的能力。如果其存在软件漏洞，极易被恶意攻击者利用获取终端的控制权限。攻击者可以窃取存储在这些终端里的敏感信息，如用户的身份信息、日常行为等，或者将这些设备用于恶意目的，如作为挖矿节点、

人民邮电出版社

作为其他攻击的肉鸡、进行恶意操作等。如曾经导致美国大面积网站访问瘫痪的域名解析服务商 DDoS 攻击事件，就是由 Mirai 病毒大面积感染物联网设备引发的。根据绿盟公司的研究报告，2018 年在所有设备和出现过异常行为的设备中，路由器和摄像头比例均为最高，异常设备的行为主要以 DDoS 攻击、僵尸网络通信和扫描探测为主。典型的物联网设备病毒包括 BASHLITE、Mirai、Lizkebab、Gafgyt、Torlus 等。研究指出，大量的 UPnP 服务暴露在互联网上，面临着被利用发起 DDoS 攻击的风险。其中很大一部分设备开启了缺乏鉴权的 UPnP SOAP 服务，极有可能被恶意控制，成为攻击内网信息系统的跳板[2]。

（2）网络通信安全

目前对于通用的计算设备构成的信息系统，存在着较为完善的防护设备和机制，如防火墙、入侵防护系统、Web 应用防火墙、网闸、加密机等。然而，出于系统类别、计算资源和成本的限制，许多安全防护功能很难在物联网上实现，导致物联网通信机制存在较大的安全风险。例如，大量的物联网设备缺乏加密通信机制，导致数据明文传输或者加密通信机制使用不合理，如使用固化的对称加密密钥进行数据加密；许多物联网缺乏鉴权认证机制，使得终端面临被恶意攻击者未授权访问的风险，典型的案例有窃取、替换智能摄像头的监控画面；此外，物联网终端网络缺乏分域隔离和安全防护机制，无法有效阻止病毒传播和阻断攻击。

（3）数据泄露风险

物联网系统存在着较高的用户隐私泄露的风险，一方面是物联网终端或云端数据存储存在安全漏洞，导致数据被恶意攻击者非法访问造成的泄露；另一方面是随着大数据分析和机器学习技术的发展，攻击者可以通过关联分析和侧信道分析发现用户的隐藏数据，如用户的活动习惯、行为特征等。

4 物联网终端固件脆弱性挖掘技术

物联网终端的软件系统与传统的通用计算机有所不同，被称为固件（firmware）。固件指的是烧录在可编程只读存储器中的软件程序。一个功能完整的固件通常包含固件头、Bootloader、操作系统内核、根文件系统和附加数据等部分。各部分的功能如下：

- 固件头用来存储该固件的标识信息，如厂商名称、设备型号、固件版本号、数字签名、固件哈希等；
- Bootloader 用于引导设备启动，作用类似于传统 PC 机上的 BIOS 系统。其主要功能是在设备上电后对嵌入式处理器和相关外设硬件进行初始化设置，如构建堆栈、设置网卡、配置内存管理单元寻址方式等，之后将操作系统内核加载到内存中，启动操作系统运行；
- 操作系统内核在设备启动之后接管设备的控制权，主要功能是管理调度系统进程、分配系统内存、加载设备驱动程序、加载文件系统等；
- 根文件系统包含了操作系统其他重要的系统代码、所有的应用程序代码和配置文件，是固件的重要组成部分。

需要指出的是，并非所有物联网终端固件都包含上面所述全部模块，有些功能简单的物联网设备，如射频标识、智能开关等，其固件只包含一些简单的功能代码。

大部分物联网系统存在的安全风险来源于物联网终端固件存在的安全脆弱性，即软件漏洞。常见的漏洞类型包括缓冲区溢出、整数溢出、命令注入、弱口令、明文传输、认证绕过等，而其中缓冲区溢出和命令注入这两类漏洞对系统的危害最大，因为攻击者借助这两类漏洞可以获得设备的完全控制权。对物联网终端固件脆弱性进行分析的技术包括静态分析技术和动态模糊测试技术[3]。

程序静态分析技术利用了控制流和数据流分析、符号执行及污点分析等理论。其核心思想是构建程序的控制流图（control flow graph）和数据依赖图（data dependency graph），在此基础上通过符号执行或污点分析的方法寻找一条从输入到不安全系统函数（如 strcpy、sprintf）的路径，从而发现可能的漏洞隐患[4-7]。

动态模糊测试技术是一种通过构造生成特定的随机数据发送给目标软件，使得目标软件崩溃，从而发现系统中存在缺陷的安全测试方法。该方法通常被用来检测网络协议、文件、驱动程序等的漏洞，模糊测试具有自动化程度高、适应性广、扩展性强等特点，使其成为漏洞挖掘领域中比较有效的方法之一。Jonas Zaddach 、 Luca Bruno 、 AurelienFrancillon 、 DavideBalzarotti 等人于 2014 年提出了一个嵌入式系统漏洞挖掘框架—Avatar[8]。Avatar 运用了动态分析的方法对嵌入式系统进行漏洞挖掘，通过软件仿真硬件，并采用模糊测试方法对嵌入式系统进行漏洞挖掘。

通过对物联网终端固件进行脆弱性分析，及时发现其中隐藏的安全漏洞，及时进行更新修复，是保护物联网终端安全的重要手段。

5 物联网终端安全防护

物联网中的终端设备种类繁多，系统架构复杂多样，功能多变。大量的物联网终端缺乏合理的安全防护手段，导致其容易成为黑客利用的对象。对物联网终端进行安全防护，要综合考虑其自身和所面临的安全威胁特点，制定合理的安全防护策略。构建一个完整的物联网终端防护体系，需从软件、硬件、通信协议、业务应用等多方面入手。硬件方面，需要引入加密芯片、安全模块，实现物联网终端芯片的安全访问，抵御攻击者或者恶意程序对芯片内系统程序和数据的非法访问和篡改；软件方面，在固件开发阶段就引入安全开发的规范，尽量减少高危漏洞的出现几率，同时确保可控的更新机制，防御固件更新过程中的恶意篡改；通信协议方面，确保应用正确的加密机制，通过引入轻量级的证书系统，实现强制认证机制，抵御重放攻击和中间人攻击。

面对海量的物联网终端，传统的以边界隔离为主的信息网络防御手段变得不再有效。零信任网络安全模型由 Forrester 研究所于 2010 年提出。其核心思想是不信任任何的实体，无论它来自网络内部还是外部，每一次对服务的访问都需要经过认证授权，而访问控制是以身份为基础的。零信任网络模型实践的技术基础包括多因子身份认证、身份与访问管理、加密、安全评级和文件系统权限等。要实现零信任网络模型并不容易，但是可以从根本上改变物联网安全现状。

6 结束语

泛在电力物联网为众多新能源企业、互联网企业、信息和通信技术企业提供了无限可能。在能源结构转型和低碳化发展的大势下，互联网、大数据、物联网等技术的发展以及与能源行业的融合，将打破长久以来传统能源体系封闭的垄断结构，为能源和信息行业带来新的活力。然而，“万物互联”的网络，模糊了传统信息系统的边界，为信息安全防护提出了新的挑战。而物联网设备自身存在的脆弱性是物联网威胁的一大重要来源。如何做好物联网系统的信息安全防护，是泛在电力物联网建设中的重要课题。

参考文献：

[1] 中国信通院. 物联网安全白皮书（2018）[EB/OL].

[2] 2017 绿盟科技物联网安全年报[EB/OL].

[3] 李登, 尹青, 林键, 等. 基于同源性分析的嵌入式设备固件漏洞检测[J]. 计算机工程, 2017, 43(1): 72-78.

[4] 孙力行. 网络安全漏洞分析知识库系统的设计与实现[D]. 成都：电子科技大学, 2011.

[5] 代子营. 面向符号执行的内存模型研究[D]. 长沙：国防科学技术大学, 2009.

[6] 辛伟, 时志伟, 郝永乐, 等. 基于污点分析和符号执行的漏洞签名生成方法[J]. 清华大学学报(自然科学版), 2016(1): 28-34.

[7] 潘璠. 基于高阶属性文法的协议逆向关键技术研究[D]. 南京: 解放军理工大学, 2013.

[8] Zaddach, Jonas, Bruno, et al. AVATAR: A framework to support dynamic security analysis of embedded systems' firmwares[M]. Avatar: A Framework to Support Dynamic Security Analysis of Embedded Systems’ Firmwares. 2015.

人民邮电出版社

分布式数据库跨数据中心同步数据研究与设计

张亮，周晶，孙喜民，张宾
（国网电子商务有限公司，北京 100053）

摘　要：提出分布式数据库跨数据中心的同步涉及到的数据结构、数据一致性级别、数据一致性策略以及跨数据中心的同步机制设计原理、组网原理和高可用机制设计原理。

关键词：分布式数据库；跨数据中心同步；数据同步

1　引言

大数据时代的来临对数据的存储、查询和分析提出了新的挑战。各种不同类型、不同特征、动辄以 PB 甚至 EB 计的数据，以及几十、上百万的并发 IO，都让传统关系数据库无从招架。分布式数据库是数据库的集合，在分布式数据库系统中，数据库存储在一定数量的计算机上。分布式系统中的计算机通过高速网络彼此通信。分布式数据库提供了良好的扩展能力、对高并发请求的响应能力，以及数据安全性、可靠性的保证，这都是在大数据时代必不可少的。然而在一个分布式数据库的环境中，跨数据中心的数据副本同步写入将会带来较大的延迟，从而影响到系统的整体性能。本文站在数据的视角，描述跨数据中心同步主要涉及到的数据结构定义、数据一致性级别及策略，以及关键处理流程的设计原理和组网原理。

2　数据模型

2.1　数据复制及数据一致性策略

需要复制的数据如下。

• 资源数据：包括容器、对象、ACL，资源数据存放在对象存储引擎中。

• 账号数据：账号注册信息、密钥信息、账号统计结果等，账号数据存放在 RDBMS（PostgreSQL 或 MySQL）中。

数据复制手段如下。

• 资源数据：通过对象存储数据复制工具完成跨数据中心的异步复制。

• 账号数据：通过 RDBMS 自带的 Replication 工具完成跨数据中心的同步或异步复制。

跨数据中心的数据一致性级别如下。

• 强一致性：要求 $R + W > N$。以两个数据中心为例，读取时，只要保证每次从两个数据中心读取数据，则可以保证强一致，即保证了 $R(2) + W(1) > N(2)$。两份副本版本不一致时，依靠数据生成时间解决版本冲突，数据生成时间由对象存储服务生成，并保存在数据元中。另外，对于 W=1 且 N=2 的情况，当发现读数据的数据中心为数据所属地（当 W=1 时，整个系统只有唯一写者，Write Preference List 中只包含一个数据中心）时，可以只从本地读取，这也可保证强一致。

• 最终一致：$R + W \leqslant N$。以两个数据中心为例，为 $R(1) + W(1) = N(2)$，当在非所属地读取时可能会读到旧版本（当数据尚未完成异地复制时）。

一致性级别的选择策略如下。

• 请求路由（request router）根据 Consistency Strategy 组件判断应使用哪种一致性级别。对于两个数据中心的情况，设定 W=1（即数据有唯一写者），此时实际选择的是，在读取时的 R 值。

• Consistency Strategy 组件在实现时，可根据不同的 API，返回不同的一致性级别（两个数据中心的情况，即返回不同的 R 值）。例如，对于“公开 URL 下载”API，返回强一致性策略（R=2，同时从本地和远程读，确保读到新版本，当读请求发生在数据所属地时，可优化为只从本地读）；对于“GET Object”API，返回最终一致性策略（R=1，本地读，有可能读到旧版本）。

2.2　关键数据结构

（1）Event

① 作用：分布式对象存储引擎发送给对象存储数据同步实体的数据变更事件。

② 字段

人民邮电出版社

slot_id：数据所属的 Slot ID。

event_id：一个 Slot 内部的 Event ID，一个单调连续递增的整数。

storage_id：数据所属的 Storage ID。

operation：操作（PUT, DELETE, TRUNCATE, …），所有操作要求是幂等的。

source_id：数据主键（在 Storage 内唯一）。

param：其他额外参数，如描述 File Slice 的<pos, len>。

（2）Checkpoint

① 作用：对象存储数据同步实体用于标记已完成数据复制的 Event ID，所有小于等于 Committed Event ID 的数据说明已经成功复制至远程对象存储引擎；当对象存储数据同步实体恢复重启后，在追赶更新事件时，只需要从本数据中心对象存储引擎中得到（Commiited Event ID, Current Eevent ID]范围内的更新事件列表。

② 字段

storage_id：事件所属的 Storage ID。

slot_id：事件所属的 Slot ID。

committed_event_id：该 Storage 的 Slot 当前已处理完成的事件 ID。

Checkpoint 示例见表 1。

表 1　Checkpoint 示例

storage_id	slot_id	committed_event_id
fs	0	130
fs	1	24
…	…	…
obj	127	101
…	…	…

（3）Routing Table

①作用：访问路由利用 Routing Table 决定读写请求的首选集群列表。

②字段

account_id：账号 ID。

read_preference_list：读优先列表，记录每个数据中心的逻辑访问地址。

write_preference_list：写优先列表，记录每个数据中心的逻辑访问地址。

Routing Table 示例见表 2。

表 2　Routing Table 示例

account_id	read_preference_list	write_preference_list
Account_1	DC-1, DC-2	DC-1
Account_2	DC-2, DC-1	DC-2
…	…	…
Account_*N*	DC-2, DC-1	DC-2

3　关键质量属性的设计原理

（1）关系型数据库跨数据中心同步机制设计原理

账号按照所属地做 sharding，每个账号都会对应一个主数据中心和一个从数据中心。两个数据中心的数据互相部署成 Master/Slave 的主备模式。在数据中心之间互相做复制的过程中，利用 REQUEST_ROUTING 库表筛选要复制的数据，保证数据的单一复制流向（Master→Slave）。

（2）跨数据中心组网设计原理

首先要选择两个数据中心是否应组成一个逻辑上互通的集群。理论上，可以通过 Rendezvous 发现机制实现两个数据中心中的两个子网形成一个逻辑上互通的通信集群。这样，两个远程的数据中心在逻辑上成为了一个通信集群，每个节点都可以通过 pub/sub 与其他节点（同数据中心或跨数据中心）发送消息。但由于跨数据中心的网络情况比较复杂，相比于同一机房的不断网段间的通信而言，网络层不稳定的因素会加倍。这种情况下，Rendezvous 发现机制可能会出现由于网络情况不良造成的错误判断或状态判断震荡。另外，就跨数据中心的同步以及访问的需求而言，将两个数据中心在逻辑上连成一个通信集群也不是必须的。因此不建议使用这种组网方式。

推荐保持两个数据中心的网络彼此隔离，每个数据中心内部分别通过 Broadcast 发现机制维护节点列表。当进程需要跨数据中心访问时，通过 Message-Routing 机制将消息发送给远程数据中心的 Routing 节点，进而通过 Routing 节点转发消息。同时，通过配置 Fault-Tolerance，可保证当主 Routing 节点宕掉后，能自动选择其他的备 Routing 节点。

（3）高可用机制设计原理

对象存储数据同步工具的高可用机制分为两个层面。

进程级高可用机制：利用操作系统 crontab 机制定期检测数据同步进程状态，如果进程死掉，则执行重

人邮电出版社

启脚本，进入恢复流程（后面详细介绍）。

集群级高可用机制：部署多个数据同步节点。数据同步节点加入到群组通信 GroupComm 组（guardian failover group）中；节点启动后进入 INIT_MODE 状态，此模式下节点不接收本数据中心对象存储引擎的事件更新消息；节点成功加入组后，根据 GroupComm 提供的 Rank ID 确定自己是否为主节点。如果是主节点，则进入 LEADER_ROLE 角色，否则进入 FOLLOWER_ROLE 角色；此后节点进入 RUNNING_MODE 状态，节点判断自己的角色，如果是 LEADER_ROLE，则开启 Messaging Thread 监听本数据中心对象存储引擎的事件更新消息，并进入到前面提到的数据复制的各个流程中；每当 Membership 变更事件到来后，节点根据最新的 Rank ID 判断是否发生从 FOLLOWER_ROLE 到 LEADER_ROLE 的角色切换。如果发生，则说明该节点是当前集群中的新 Leader，这时节点应从 RUNNING_MODE 切换到 RECOVERY_MODE 状态，进入 Guardian 恢复流程。

数据同步进程的恢复流程如下：

①进入恢复流程前，节点状态为 RECOVERY_MODE；

②节点从本数据中心对象存储引擎中获取 Checkpoint 信息，根据每个 Slot 的当前 Event ID，向本数据中心 DataCell 获取漏掉的 Event List，并根据 Slot Partitioner 分别放入合适的 SlotQueue 中；

③节点将自己切换回 RUNNING_MODE 状态，进入正常工作流程。

数据同步扩展机制的设计原理如下。

总体思路：按照 Slot 做 partition，每个 Guardian 承担部分 Slot 的复制工作。

静态扩展方式：数据同步节点与 Slot list 的映射保存在配置文件中，数据同步进程启动后读取配置文件，并据此选择其所负责的部分 Slot 进行复制；增加或减少数据同步节点时，首先修改每个节点的 Slot List 映射配置文件，然后重启每个数据同步进程程序（重启后，可先执行恢复流程，追赶更新）。

动态扩展方式：每个同步进程加入到 GroupComm 群组中，并通过 Rank ID 判断自己是否为 Leader，由 Leader 维护更新所有数据同步进程与 Slot List 的映射关系。当增加或减少 Guardian 节点时，由 Leader 更新映射，并同步广播给所有成员。

对于异地数据中心的数据复制而言，最可能出现的潜在性能瓶颈在异地机房间的网络带宽以及由于网络不稳定造成的传输延时上，考虑到系统潜在的瓶颈点并不在 Guardian 节点本身的处理能力上，因此真正需要动态扩展的场景应该不多。考虑到静态扩展方式在实现难度上远低于动态扩展方式，因此建议优先实现静态扩展方式。

4 结束语

本文提出了分布式数据库跨数据中心的数据同步涉及到的数据结构、数据一致性级别、数据一致性策略以及跨数据中心的同步机制设计原理、组网原理和高可用机制设计原理。解决了跨数据中心的数据副本同步写入的问题，本系统的简单原型实现证明了该设计方案的可实施性。

参考文献：

[1] MARZIEH K, FARAMARZ S E, NASIM N. Improving response time of Web service composition based on QoS properties[J]. Indian Journal of Science and Technology, 2015,8(16).

[2] TANUJA S, RADHA K R. Perfect commit protocol for distributed database system: analysis review[J]. International Journal of Advanced Research in Computer Science and Software Engineering, 2015,5(11).

[3] PARUL T M. An overview of distributed databases[J]. Information and Computation Technology, 2014, 4(2): 207-214.

[4] PRAKASH C J, ROHINI P M, B GANESH R, et al. Hybrid reliability model to enhance the efficiency of composite Web services[C]//IEEE International Conference on Emerging Trends in Computing. Communication and Nanotechnology(ICECCN 2013), 2013.

[5] SUNIL K, SEETHA J, VINOTHA S R. Security implication of distributed database management system models[J].International Journal of Soft Computing and Software Engineering, 2012, 2(11).

人民邮电出版社

公有云承载的多种网络场景下的专属云网络接入模型

董铮，陈思，吴琦，孙智强，桑晓宇
（中国电信股份有限公司南京分公司，江苏 南京 210008）

摘　要：讨论了 3 种接入方式下 IPSec VPN、EPON（ethernet passive optical network，以太网无源光网络）及 IP-RAN（IP radio access network，IP 化无线接入网）专属云网络的接入模型，比较三 3 种模式各自的优缺点，并对未来可能的专属云接入方式做了分析和展望。

关键词：公有云；专属云；云专线；VPLS；VPDN

1　引言

公有云业务因具有灵活、成本低、安全性高、可扩展性强和容量大等优势，具有很广泛的应用前景。相对于公有云业务，私有云业务可以提供更大的控制权和隐私权，但成本很高。专属云业务基于公有云业务实现，但又与其他公共租户物理隔离，越来越受到需要专属服务的企业、政府、金融等用户的青睐。专属云业务的网络接入模型成为了云业务发展的一个重要方向。

2　背景技术

2.1　IPSec VPN

IPSec（internet protocol security）VPN 是一种基于互联网的采用 IPSec 协议来实现远程接入的 VPN 技术。IPSec 协议是一种开发标准的框架结构，特定的通信方之间在 IP 层通过加密和数据摘要（Hash）等手段，来保证数据分组在互联网上传输时的私密性（confidentiality）、完整性（data integrity）和真实性（origin authentication），IPSec 协议通过加密算法实现数据分组的私密性，通过 Hash 算法实现数据分组的完整性，通过身份验证保证数据的真实性。IPSec 安全协议描述了如何利用加密算法和 Hash 算法来保护数据安全，包含加密、数据摘要和对称密钥交换三部分。IPSec 安全协议框架结构具体如图 1 所示。

IPSec 协议常用的身份认证算法有预共享密钥（pre-shared key）和数字签名（RSA signature）2 种，预共享密钥是指通信双方在配置时手工输入相同的密钥，数字签名是指通过公钥+私钥的方式来加密和解密，数字证书中存储了公钥信息，私钥用户自己保留，公钥加密过的数据只有对应的私钥才能解开。

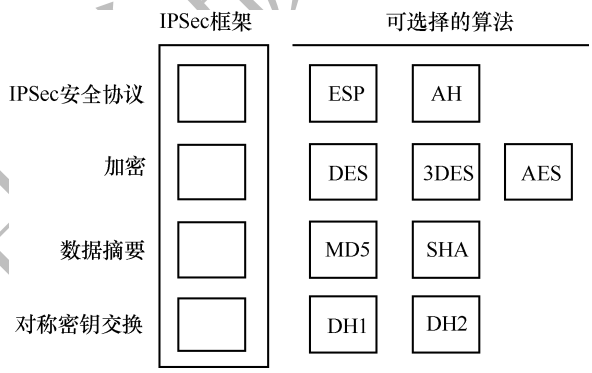


图 1　IPSec 安全协议框架结构

2.2　VPLS

VPLS（virtual private LAN service，虚拟专用局域网业务），是一种基于 MPLS 的二层 VPN 技术，VPLS 技术属于二层分组承载技术，本质上是一种基于 IP/MPLS 和以太网技术的 L2VPN（二层虚拟专用网）技术。其核心思想是利用信令协议在 VPLS 实例中的 PE（运营商边缘路由器）节点之间建立及维护 PW（伪线），将二层协议帧封装后在 PW 上传输、交换，使广域范围内多个局域网在数据链路层面被整合为一张网络，向用户提供虚拟的以太网服务。VPLS 技术有效地结合了 IP/MPLS、L2VPN 以太网交换等多种技术的特点，支持点到点、点到多点、多点到多点的业务类型，能够在较大网络规模下支持电信级以太网服务。

2.3　EPON

EPON（ethernet passive optical network，以太网无源光网络）采用点到多点结构、无源光纤传输，在以太网

之上提供多种业务。在该标准中将以太网和 PON 技术结合，在物理层采用 PON 技术，在数据链路层使用以太网协议，利用 PON 的拓扑结构实现以太网接入。因此，它综合了 PON 技术和以太网技术的优点：低成本、高带宽、强扩展性、与现有以太网兼容、方便管理等。

2.4 IP-RAN

IP-RAN（IP radio access network，IP 化无线接入网）是针对 IP 化基站回传应用场景进行优化定制的路由器/交换机整体解决方案。在城域汇聚/核心层采用 IP/MPLS 技术，接入层主要采用二层增强以太技术，或采用二层增强以太与三层 IP/MPLS 相结合的技术方案。相对于传统分组网，IP-RAN 中引入 BFD（bidirectional forwarding detection，双向转发检测）、FRR（fast reroute，快速重路由）、隧道保护、路由快速收敛等技术保证网络毫秒级可靠性，支持 1588、同步以太网，满足基站、TDM（time division multiplexing，时分复用）业务时钟同步要求，通过 E2E 图形化网管简化业务部署，保证大规模组网能力，降低运维成本。

3 多种网络场景下的接入模型

3.1 IPSec 云专线

IPSec 云专线是基于 IPsec VPN 连接的、低成本的企业云业务，在运营商终端综合管理系统 ITMS（integrated terminal management system），平台和云侧管理平台的配合下，用户可以通过云 Portal 实现 IPsec VPN 参数在政企网关侧和云侧的自动配置，简单快捷地建立政企网关与云服务商的云侧网关的 IPSEC VPN 连接，从而实现中小企业云资源池的安全访问以及云资源池侧网络与企单侧网络的安全互通。具体 IPSec 云专线网络拓扑如图 2 所示。

该种方式的云专线基于互联网（Internet）实现，具备实现快速、成本低、安全性高的特点，只需要在客户原有的政企网关上开启 IPSec VPN 功能即可。用户端通过基于 IPSec tunnel 隧道的私网地址，安全地访问云侧 VPC（virtual private cloud，虚拟私有云）内的云主机。

具体实现时，通过 ITMS 系统下发具体的 IPSec 网络配置到用户端的政企网关（部署前需要先对政企网关做软件升级），通过云侧 Portal 页面配置该政企客户的终端信息（如终端信息、密钥信息等），从而在云侧和用户端之间建立起端到端的 IPSec 安全连接。整体网络基于互联网实现，互联网的网络性能参数（带宽、时延、抖动等）情况将直接决定 IPSec 云专线的网络性能和使用感知。

3.2 EPON 云专线

EPON 云专线通过 e8-c 设备接入 ODN（optical distribution network，光分配网络），再接入 OLT（optical line terminal，光线路终端），之后通过 IP 城域网接入地市城域网的 CR 设备，再通过传输系统从各地市 CR 直拉到云侧核心 ASBR（autonomous system border router，自治系统边界路由器）设备。具体 EPON 云专线网络拓扑如图 3 所示。

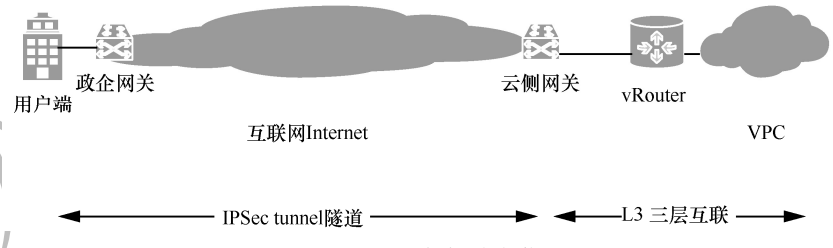


图 2 IPSec 云专线网络拓扑

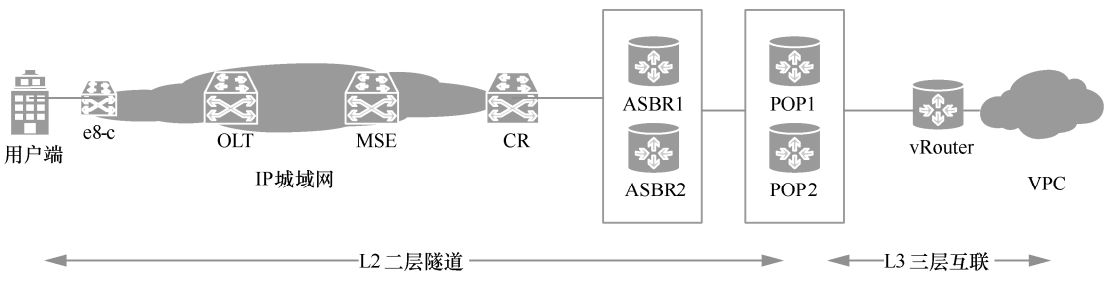


图 3 EPON 云专线网络拓扑

在数据层面，在城域网络通过 VPLS 承载，最终实现从用户端到云侧 POP 交换机的 L2 二层隧道。在云侧 VPC 内通过 NFV 实现的虚拟化的 vRouter 实现与用户端地址段的三层互联。

具体实现时，如果用户侧 e8-c 设备作为二层桥接使用，则需要在用户侧的出口路由器设备上配置指向云侧的静态路由；如果用户侧 e8-c 设备作为三层路由使用，则需要在 e8-c 设备上配置指向云侧的静态路由。在云侧 POP 交换机上配置指向用户侧内网网段的静态路由以及指向云主机网段的静态路由，在云侧 vRouter 设备上配置用户侧内网网段以及用户侧和 POP 交换机互联网段作为远端子网。由于用户侧的出口路由器和云侧 POP 交换机之间为通过城域网络的 VPLS 和从各地市 CR 直拉到云侧核心 ASBR 设备的传输系统承载，为以太网二层网络连接，基于 MAC 地址转发数据，故无需新增三层路由配置。

3.3 IP-RAN 云专线

IP-RAN 云专线通过客户端 U 设备接入到局端 A 设备，再接入 B 设备，之后通过 IP-RAN 接入地市的 ER 设备，之后通过 CN2 网络连到云侧核心 ASBR 设备。具体 IP-RAN 云专线网络拓扑如图 4 所示。

在数据层面，在城域网络通过 IP-RAN 的 PW（伪线）承载，在 CN2 层面通过 VPLS 承载，最终实现从用户端到云侧 POP 交换机的 L2 二层隧道。在云侧 VPC 内通过 NFV 实现的虚拟化的 vRouter 实现与用户端地址段的三层互联。

具体实现时，需要在用户侧的出口路由器设备上配置指向云侧的静态路由，在云侧 POP 交换机上配置指向用户侧内网网段的静态路由以及指向云主机网段的静态路由，在云侧 vRouter 设备上配置用户侧内网网段以及用户侧和 POP 交换机互联网段作为远端子网。由于用户侧的出口路由器和云侧 POP 交换机之间通过 IP-RAN 的 PW（伪线）和 CN2 网络的 VPLS 技术承载，为以太网二层网络连接，基于 MAC 地址转发数据，故无需新增三层路由配置。

4 专属云网络接入模型对比分析

从应用范围和互联网（Internet）隔离情况、带宽、上下行是否对等、双向时延情况和故障响应时间这几个维度，分别对 IPSec 云专线、IP-RAN 云专线和 PON 云专线的特点进行了总结和比较，具体见表 1。

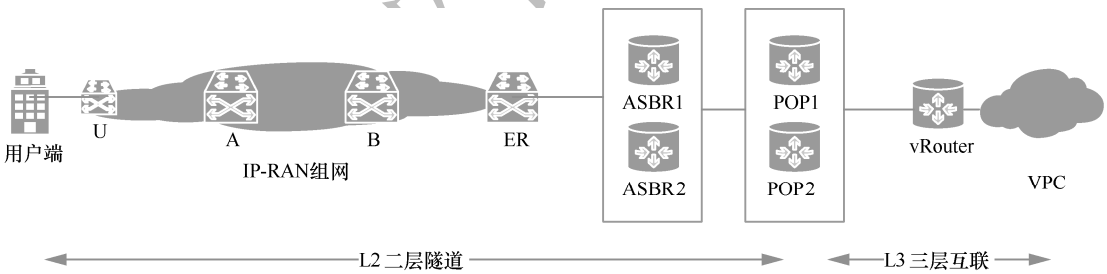


图 4 IP-RAN 云专线网络拓扑

表 1 专属云网络接入模型对比分析

特性	IPSec 云专线	IP-RAN 云专线	EPON 云专线
应用场景	低成本的云专线	高保障的云专线	广覆盖的云专线
隔离	应用层与 Internet 隔离	IP-RAN 传输网络与 Internet 隔离	数据链路层与 Internet 隔离
带宽	取决于互联网宽带情况	10 MHz、20 MHz、50 MHz、100 MHz、200 MHz…1 000 MHz	10 MHz、20 MHz、50 MHz、100 MHz
上下行对等	取决于互联网宽带情况	上下行确保对等	上下行可达对等
双向时延	取决于互联网宽带情况	双向时延≤ 19 ms	双向时延≤19 ms
故障响应时间	取决于互联网宽带情况	故障响应时间≤ 4 h	故障响应时间≤24 h

5 结束语

文中提出的 3 种网络场景的专属云网络接入模型，均基于运营上的公用数据网络实现集中式的虚拟专用网络与云端云主机网络的连接，IPSec 云专线由政企网关、互联网（Internet）和云侧网关组成，具有成本低和便于部署的特点；EPON 云专线由用户侧终端、IP 城域网、长途传输系统、ASBR、云侧 POP 交换机和 vRouter 虚拟路由器组成，具有广覆盖、快部署和高性价比的特点；IP-RAN 云专线由客户端 U 设备、IP-RAN、ASBR、云侧 POP 交换机和 vRouter 虚拟路由器组成，具有高保障、物理隔离和高性能的特点。

随着物联网和未来 5G 业务的快速发展，未来的专属云接入方式将会向着移动化、无线化和大容量接入的方向发展。在万物互联的网络场景下，由于未来众多的物联网终端也需要和云侧的服务器、软件平台等互联，预计基于 5G 的大容量、低时延和高带宽的专属云接入方式也会不断涌现。

参考文献：

[1] 邵翀. IP-RAN 关键技术浅析和应用展望[J]. 电信快报, 2012(6).

人民邮电出版社

核电厂电力监控系统网络安全态势感知平台研究

张士帅，付振旭，舒超
(中国广核电力股份有限公司，广东 深圳 518026)

摘　要：在网络安全严峻形势的背景下，网络安全态势感知的研究和应用也备受关注，电力监控系统网络是未来电网的发展基础，核电厂电力监控系统的网络安全甚至关乎核安全，结合工程实例论述了态势感知平台在核电厂电力监控系统中的应用，阐述了态势感知在提升核电厂电力监控系统网络安全防护水平的必要性，解决了核电厂电力监控系统风险监视以及管理主要依靠人工日常运维、缺乏自动化的风险发现以及监视措施等问题。

关键词：态势感知；网络安全；核电厂；电力监控

1　态势感知概念

态势感知的概念最早在军事领域被提出，是为了分析空战环境信息、快速判断当前及未来形势，以做出正确反应进而提升空战能力而进行的研究。

态势感知的正式定义为“一定时间和空间环境中元素的感知，以及对它们含义的理解，并对它们稍后状态的投影”，是一种基于环境的，动态、整体地洞悉安全风险的能力，是以安全大数据为基础，从全局视角提升对安全威胁的发现识别、理解分析、响应处置能力的一种方式，最终是为了决策与行动，是安全能力的落地。

态势感知一般覆盖感知、理解和预测 3 个层次，如图 1 所示，是一种感知外界信息到分析理解信息，最后对信息未来变化趋势预测的过程。如从字面上分析，“态”即当前的状态，“势”指未来的趋势，“感”即探测与发现，“知”指理解与掌握。通过相互组合，又形成“感态”“感势”“知势”“知态”，即对象的采集、分析，行为的监视及未来预测 4 个具体方面。

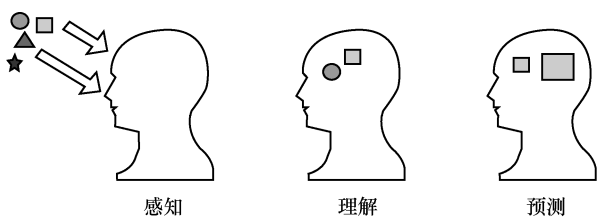


图 1　态势感知概念的 3 个层次

2　网络安全态势感知

20 世纪 90 年代态势感知的概念被引入信息安全领域，并随着网络的兴起而升级为“网络态势感知”，指在大规模网络环境中对能够引起网络态势发生变化的安全要素进行获取、理解、显示以及最近发展趋势的顺延性预测，最终目的是要进行网络安全方面的决策与防护行动。

2.1　网络安全态势要素的提取

网络安全态势要素主要包括静态的配置信息、动态的运行信息以及网络的流量信息。静态的配置信息一般包含网络的拓扑信息、设备硬件信息和状态信息等基本配置信息；动态的运行信息一般指从各种防护措施的日志采集和分析技术获取的威胁信息等；网络流量信息方面通常关注瞬时的爆发性流量监控及网络闲时出现的异常流量增长或访问事件。

2.2　网络安全态势的评估

在获取海量网络安全信息的基础上，解析信息之间的关联性，对其进行融合，获取宏观的网络安全态势，称为态势评估，数据融合算法是态势评估的核心。应用于态势评估的数据融合算法一般分为基于逻辑关系的融合方法、基于数学模型的融合方法、基于概率统计的融合方法、基于规则推理的融合方法等。

2.3　网络安全态势的预测

网络安全态势的预测是指根据网络安全态势的历史信息和当前状态对网络未来一段时间的发展趋势进行预测。通过这项工作能够帮助用户确定网络中存在

人民邮电出版社

的问题，结合问题实质进一步分析出根本原因，在这个过程中找出能够反映网络安全问题的信息内容，结合数学模型预测相关的网络安全问题和发展态势，为计算机网络安全的发展提供可参考的信息，保证网络环境的安全发展。

3 核电厂电力监控系统基本组成

电力监控系统作为专用网络中的一员，是电力行业的重要生产控制系统，指在电力生产过程中用于监视和控制电力生产和供应过程的、基于计算机及网络技术的业务系统及智能设以及作为基础支撑的通信及数据网络等。电力监控系统以计算机、通信设备、测控单元为基本工具，为变配电系统的实时数据采集、开关状态检测及远程控制提供了基础平台，它可以和检测、控制设备构成任意复杂的监控系统，在变配电监控中发挥核心作用，帮助发电企业消除“孤岛”、降低运作成本、提高生产效率，加快变配电过程中异常的反应速度。

根据核电厂电力监控系统的特点、现状和安全要求，核电厂电力监控系统一般分为两个工作区：生产控制区和管理信息大区，其中生产控制区又分为安全Ⅰ区和安全Ⅱ区。控制区中的业务系统或其功能模块（或子系统）的典型特征为：是电力生产的重要环节，直接实现对电力一次系统的实时监控，是安全防护的重点和核心。非控制区中的业务系统或其功能模块的典型特征为：是电力生产必要环节，在线运行但不具备控制功能，与控制区中的业务系统或其功能模块联系紧密。管理信息大区是指生产控制大区以外的电力企业管理业务系统的集合。管理信息大区的传统典型业务系统包括调度生产管理系统、行政电话网管系统等。

4 态势感知在电力监控系统中的应用

4.1 总体构架

电力监控系统网络安全态势感知在核电厂各分区内部署厂站装置，厂站装置作为态势感知系统的重要组成部分，实现电力监控系统网络安全态势在变电站的数据采集以及变电站网络安全数据的分析功能。厂站安全监控终端与态势感知平台主站采用统一架构，以实现相关网络安全数据的采集以及在线辨识及告警功能。能够实现电力监控系统现有主机设备、网络安全、安全设备等的状态采集、配置信息采集、日志信息、流量数据的采集，并通过专网上传至电网主站，为上级网络安全分析提供数据支持。电力监控系统态势感知构架如图 2 所示。

4.2 数据采集

电力监控系统态势感知采集对象包括通用主机、工控设备、网络设备、安全防护设备等。采集方式一般包括 SNMP、Syslog 等方式。采集数据内容包括通用主机服务器、工作站的采集数据（状态类、日志类）、工控装置的采集数据（状态类、日志类）、网络设备的采集数据（状态类、日志类、流量类）、安全设备采集数据（状态类、日志类）。通过对上述设备及参数的大数据采集，实现底层设备运行状态收集。

4.3 资产信息生成

态势感知厂站装置支持电力监控系统资产信息的

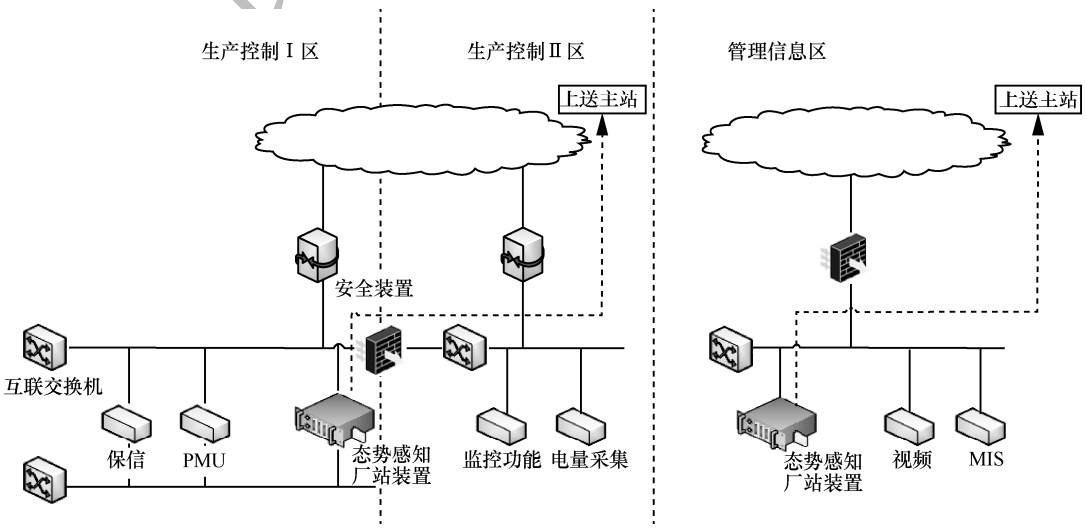


图 2 电力监控系统态势感知构架

自动扫描及匹配，并通过主站子站联通，实现统一维护，具体包括：支持网络扫描功能，支持全协议扫描、流量镜像方式等，自动发现在线的 IP 地址资产；支持全站多源在线 IP 地址资产信息的比对、去重和拼接，实现厂站资产信息的建模；支持与态势感知主站系统联动，实现厂站资产的主动上送、合法注册和实时同步，实现厂站资产的主站统一维护。

4.4 拓扑信息生成

支持自动生成全厂站逻辑拓扑连接关系表，逻辑拓扑连接关系表包含：序号、调度分区、IP 子网、VLAN 号、设备名称、IP 地址、设备全局唯一标识（GUID）；支持逻辑拓扑连接关系表动态全量上送主站；支持逻辑拓扑连接关系表的本地查询，提供按 IP 地址、设备名称进行检索，并支持逻辑拓扑连接关系数据的本地导出。

4.5 告警信息上送

支持事件告警信息上送，包括：告警级别、告警时间、厂站装置唯一标识、告警设备类型、告警内容等信息。告警内容包括：开始日期时间、告警设备唯一标识、告警设备类型、告警类型、告警子类型、重复次数、内容描述等内容。支持事件告警生成后实时主动上送主站，事件告警类型包含安全事件类、人员操作类、设备故障类和运行异常类；支持事件告警类型信息与设备相关联。系统日志（登录、操作、维护日志）以列表形式展示厂站装置的操作日志，可以通过条件查询、关键字查询等方式，实现对厂站装置操作日志的查询。

4.6 系统管理及升级

态势感知厂站装置支持系统升级功能，分为本地升级（用户通过本地管理界面上传补丁包进行软件升级）和远程升级（主站对厂站装置软件进行远程升级）。支持如下功能：支持软件升级包的数据校验，确保升级包的完整性和安全性；支持升级过程对装置配置文件和数据文件的保护不丢失；升级后如需要重启，重启后能自动恢复业务。

4.7 系统日志记录

系统日志（登录、操作、维护日志）以列表形式展示厂站装置的操作日志，可以通过条件查询、关键字查询等方式，实现对厂站装置操作日志的查询：支持按照时间顺序排序展示当天的设备日志，可以查看每条日志的详情；条件查询包括用户账户、用户类型、开始时间和结束时间；列表字段包括用户账户、用户类型、操作类型、操作时间、操作内容等；设备日志历史数据保留 6 个月；时间范围查询时，时间跨度不超过 3 个月；支持导出 Excel 格式文件。

5 态势感知应用的必要性

当前，网络安全问题作为国家基础设施本质安全的重要组成部分，得到了各行业各领域的广泛重视。国家提出加快构建关键信息基础设施安全保障体系、全天候全方位感知网络安全态势等具体要求。网络安全法也对关键信息基础设施的运营者提出了具体的网络安全防护的义务，要求建立网络安全监测预警和信息通报机制。

电厂端电力监控系统的网络安全风险主要依靠传统的等级保护测评以及风险评估来发现，系统的网络安全风险监视以及管理主要依靠人工日常运维，缺乏自动化的风险发现以及监视措施，电力监控系统网络安全态势感知技术的应用，能够及时发现各类网络安全风险以及非法访问事件，同时国内电力行业态势感知技术也已成熟并广泛开展实用，为态势感知技术的推广落地打下了基础。

6 结束语

核电厂作为电力行业关键信息基础设施，作为电网重要的电源点，因其特殊性往往面临着更加复杂严峻的网络安全威胁，对于核电厂各类网络设备繁多分散的情况，如何采用网络信息化新技术来解决核电发展中遇到的网络安全问题是运维人员面对的重要问题，随着态势感知技术在核电厂电力监控系统中的研究及应用，对加快实现电力监控系统网络安全风险可发现、可控制、可溯源的目标，实现电力监控系统网络安全的闭环管理，全面提高电力系统电力监控系统网络安全防护的整体水平起到积极作用。目前态势感知技术在国内仍处于快速发展阶段，本文通过结合态势感知应用的实际案例，简要阐述了态势感知的作用，同时也为网络安全向“智能化”发展奠定一定的基础。

参考文献：

[1] 管晓娟, 张涛, 马媛媛. 网络安全态势感知研究综述[J]. 计算机安全, 2014(5): 1-4.

[2] 李刚, 唐正鑫, 李纪锋. 智能电网安全态势感知与组合预测[J]. 电力信息与通信技术, 2016(11): 1-7.

[3] 徐成, 梁睿, 程真何. 面向能源互联网的智能配电网安全态势感知[J]. 电力自动化设备, 2016(6): 13-18.

人民邮电出版社

核电容器设备力学分析标准化研究与应用

赵栋，景晓冬，赵继成
(中广核工程有限公司核电安全监控技术与装备国家重点实验室，广东 深圳 518031)

摘　要：核电设备设计中，计算机辅助工程（CAE）技术可以节省设计开发时间和设计成本，缩短设计周期，预先发现并修正潜在的设计缺陷。作为现代产品设计中的高级 CAE 工具，ANSYS 软件功能强大，但使用复杂、入门难、且输入菜单多、不够直观、对设计人员的要求高，使分析耗费大量的人力和时间，而且 70%工作量花费在有限元模型的建立上。针对以上问题，深入研究 ANSYS 开发技术，以核电卧式容器为示范，开展有限元分析流程总结和整理，梳理分析过程中所需要的参数、关系、条件等，研发出一套能够快速实现几何建模、材料设置、截面设置、网格划分等功能的系统，实现容器的精细化设计，将容器力学分析模块化、流程化和标准化，降低设计人员劳动量，提升工作效率。

关键词：核电；容器设备；力学分析；ANSYS

1　引言

高质量的设计是核电设备加工制造质量以及核电机组投产以后高安全性的重要前提。当前，采用计算机辅助工程（computer aided engineering，CAE）技术，在设备设计过程中，根据提出的设备原型建立相应的计算机仿真模型和虚拟环境，并对设备进行力学分析已越来越得到认可。采用 CAE 技术进行分析不但可以节省设计开发时间和设计成本，缩短设计周期和分析周期，预先发现并修正潜在的设计缺陷，并且可以通过模拟多种实验方案和优化设计方法获得产品设计的更优方案，预测产品的可靠性，是一种行之有效的分析方法。核电容器设备作为核电设备的重要组成部分，具有一般复杂工业产品设计制造技术复杂的特点，还具有对安全性和可靠性要求高、技术等级高、质量要求高等鲜明行业特点，这也对核电容器设备的研发和设计提出了更高的要求。因此，在核电容器设备的设计中，通过对设计出的部件进行结构、流体等方面的分析来确定所设计的容器设备是否符合标准是十分重要的。CAE 技术有助于提高核电容器设备的安全性和经济性。

作为现代产品设计中的高级 CAE 工具，ANSYS 软件是第一个通过 ISO9001 质量认证的大型分析设计类软件，是美国机械工程师协会（ASME）、美国核安全局（NQA）及近 20 种专业技术协会认证的标准分析软件，并是国内第一个通过了中国压力容器标准化技术委员会认证（1995 年）并被国务院 17 个部委推广使用[1]。

目前中广核设计院设计人员采用 ANSYS 进行核电容器设备有限元分析，具有丰富的 ANSYS 的使用经验，积累了大量的 ANSYS APDL 命令流文件和经验数据。但是鉴于 ANSYS 使用较为复杂，入门相对困难，学习周期较长且输入菜单多，对设计人员的要求较高，使设备分析耗费大量的人力和时间，尤其有限元模型创建阶段是整个有限元分析过程中最耗费时间、最易出错的阶段。在此需求上，本文选择卧式容器的有限元模型建立过程作为研究对象，研发出卧式容器力学分析辅助设计系统，探索核电容器设备力学分析标准的应用实践。

本文所研发的系统通过清晰标准的分析流程、规范的参数输入和简单按钮式操作，快速高效地实现卧式容器有限元建模，促进了力学分析工具的自主化，提高了核电技术的安全性和经济性，提高了设备设计的自动化和效率，加快设备设计中迭代的速度，减少了迭代时间，减少了人因失误，节约人力，同时规范容器设备力学分析的流程，加强分析数据的管理，给设计和力学分析带来方便，充分体现了专业化、用户化、便捷化的特点。

水电部电出版社

2 关键技术研究

作为优秀的大型通用有限元分析软件，ANSYS 不仅功能强大，而且为用户提供了良好的开发工具[2]，有 APDL[3]（ANSYS 参数化设计语言）、UPFs[4]（用户可编程特性）、UIDL[5]（用户界面设计语言）及 Tcl/Tk[2,6]（工具命令语言）。4 种开发工具相互联系、协同工作、密不可分，但它们的侧重点有所不同[2]。UPFs 主要通过编写底层源代码程序实现 ANSYS 所不具有的功能，完成复杂的开发工作；APDL 主要和 ANSYS 的分析部分频繁交互，对 ANSYS 的命令进行重新组合，以完成一系列分析任务；UIDL 主要控制 GUI 界面；Tcl/Tk 用于创建更高级的界面。

通过对 ANSYS 开发技术的对比研究，本文采用 Tcl 语言和 APDL 语言实现系统的逻辑控制和业务执行，使用 Tk 语言实现系统的界面开发，另外，由 XML 文件作为系统的数据存储。通过 ANSYS 内嵌的方式运行，保证系统操作与 ANSYS 界面显示同步。

2.1 系统入口技术

该系统通过 ANSYS 内嵌的方式运行，因此，在 ANSYS 菜单中设置系统访问入口。修改 ANSYS 配置文件，实现 ANSYS 新建菜单的添加。

ANSYS 菜单文件为 ANSYS121_DIR\gui\scripts\AnsysMenu.eui。该文件中，在数组 ansMenuNames 添加新建项 AnalysisPackage，新建数组 ansChineseMenuNames 以建立菜单的中文名称。在菜单名与软件界面映射过程中，对新数组名进行替换。新建菜单通过函数关联到用户界面，实现菜单响应。菜单文件修改后，重启 ANSYS 软件，新建菜单即可出现在菜单栏中。

2.2 用户界面技术

（1）顶层窗口的建立

系统界面以对话框的形式显示，Tk 语言遵循层次结构。对话框是一个窗口，应首先建立它的窗口才能放置各种组件。使用 Tk 的命令 toplevel 创建一个顶层窗口的框架，如：

```
toplevel .topWin -width 150 -height 50
#创建一个名为 topWin，尺寸为 150×50 的窗口
wm title .topWin “卧式容器力学分析辅助设计系统”
#使用窗口管理器设定 topWin 的标题为“卧式容器力学分析辅助设计系统”
```

需注意的是，“#”字符是注释的标志，它后面的语句不会被执行。

（2）组件的添加

Tk 提供了多种界面中添加组件的命令，常见的有：Button（按钮）、Entry（单行文本输入框）、Checkbutton（多选框）、Label（文本）、Feedback（进度条）等，以及 tk_getOpenFile 命令调用“打开文件”标准对话框等。每个组件都有很多属性，在定义时，指定其属性值，如：

```
button $matS_frame.sayOK -text "确定"  -font 18 -command vesselPenetration::sayOKMaterial
```

该命令表示创建变量名为 matS_frame.sayOK 的按钮，该按钮显示的中文名为“确定”，字体大小为 18，单击该按钮执行 sayOKMaterial 过程段。

（3）组件的布局

组件在窗口中的布局由布局管理器来安排。Tcl/Tk 中包含有 3 种管理器：打包摆放管理器（pack）、栅格摆放管理器（grid）、定位摆放管理器（place）。以本系统中常用的打包摆放管理器为例，它不确切指定每个组件的摆放位置，而是由打包器根据设置实施具体的操作，如：

```
pack $matComp_frame.sayOK -side bottom -ipadx 50 -pady 10
```

将已定义按钮 matComp_frame.sayOK 以左边距 50，上边距 10 放在当前界面的下方。

（4）过程的编写

将具有特定功能的命令集合放在一起，作为特定事件的命令，需要调用的地方仅通过过程名即可调用该功能段。

2.3 ANSYS 通信技术

对话框与 ANSYS 的通信包括两种情况：用户输入对话框中的数据传递到 ANSYS 中；系统获取 ANSYS 计算结果。对于这两种情况，通过调用 ANSYS API 函数来实现。如：

```
ans_sendcommand)str_component1='$str_component1'
# 将 str_component1='$str_component1' 发送到 ANSYS 解释器中
set numberOfNode [ans_getvalue  node,,count]
# 获取 node,,count 对应的值并赋给变量 numberOfNode
```

2.4 XML 文件存储技术

界面数据保存在 XML 文件中，Tcl 语言通过

documentElement 方法，可以获取顶级标签<SimProject>，进而得到其子标签列表，获取或存储相应数据。

3 核电容器设备力学分析标准化应用实例

3.1 核电容器设备力学分析流程

核电容设备该系统根据核电卧式容器力学分析流程而设计，从几何模型创建到最后有限元模型生成是串行完成的，各步骤之间的数据流如图 1 所示。

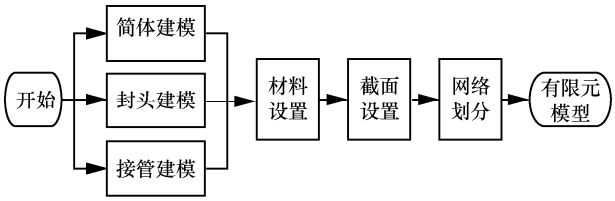
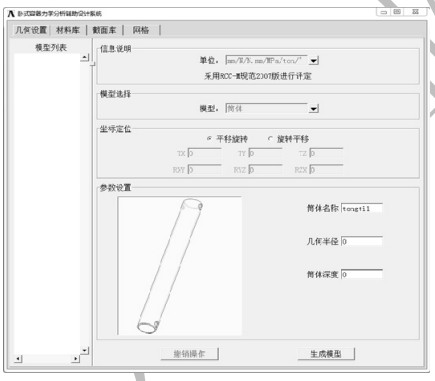


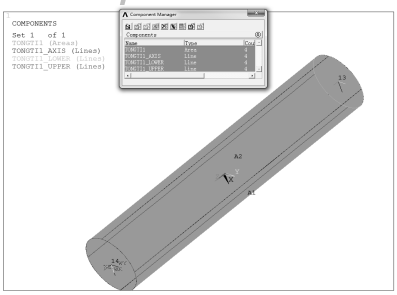
图 1 核电卧式容器力学分析流程

3.2 几何建模模块

几何建模过程是首先确定模型类型，根据模型类型确定是否需要指定坐标定位，输入相应模型特征参数，生成模型。在几何建模过程中，要求首先建立筒体，然后建立封头，最后建立接管。坐标定位是为定义接管位置而设定的，分为平移旋转和旋转平移两种。几何建模界面及筒体模型如图 2 所示。



（a）几何建模界面



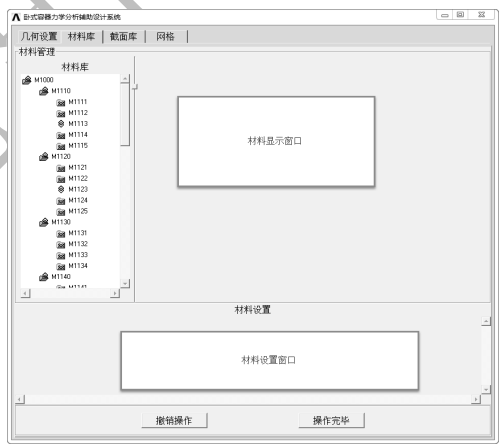
（b）筒体模型

图 2 几何建模界面及筒体模型

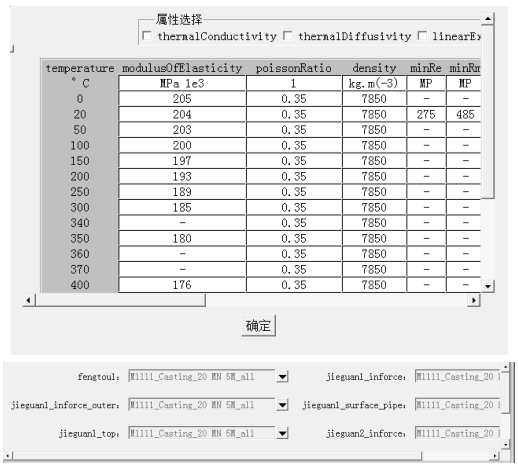
根据模型类型，参数设置分为筒体、封头、接管 3 类。各模型参数种类均不相同，根据自身特点设置，如筒体的输入参数为筒体名称、几何半径和筒体深度，封头的输入参数为封头类型、封头名称、封头半径等，接管的输入参数为接管类型、参考名称、接管名称等。设置参数完成之后，生成几何模型。

3.3 材料设置模块

材料设置模块旨在完成材料的选择和设置，如图 3 所示。材料管理根据 RCCM（2007 版）材料属性，按照 TPS、Product Form、AFNOR Grade、Dimension 4 个等级组织材料，包含了规范中所有的 TPS 牌号、制造类型和尺寸类型。其中，材料显示窗口显示当前选择材料的材料属性（modulusOfElasticity、poissonRatio 等）。选中材料，单击“确定”，在材料设置中可以被使用。材料设置窗口在材料被选中后，显示出所有的面组件，在面组件后给出允许被使用材料，给各面组件设置对应材料。



（a）界面 1



（b）界面 2

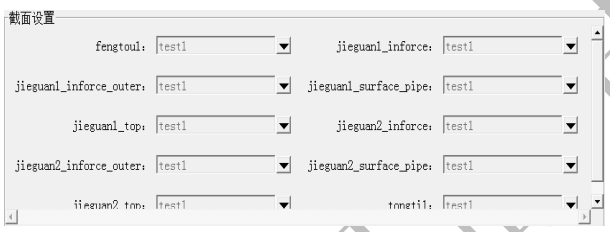
图 3 材料设置相关界面

3.4 截面设置模块

截面设置模块包括截面类型显示、截面设置等功能，截面类型显示系统中支持的截面类型，选择截面名称，在截面属性窗口显示该截面类型的属性数据，同时支持截面自定义。截面设置窗口显示需要设置截面的面组件，每一个面组件的多择框中包含已定义的截面，如图 4 所示。



（a）界面 1



（b）界面 2

图 4　截面设置相关界面

3.5 网格划分模块

网格划分模块分为单元设置、全局网格设置、网格设置、组件导入、网格生成等功能。单元设置在单元类型输入框中输入单元编号（如 solid45，输入 45），建立单元类型。单元类型将在网格设置中使用。全局网格设置中，用户输入全局网格尺寸。组件导入可以导入已经建立的线组件和面组件，更新网格设置界面中的线组件窗口和面组件窗口。网格设置界面中，用户输入线组件应该划分的份数，选择面组件网格划分方法和单元类型，如图 5 所示。面组件的网格划分方法为映射划分和自由划分两种，单元类型为用户建立的单元类型。

网格生成将生成系统最终的成果，即有限元模型，如图 6 所示。



（a）界面 1



（b）界面 2

图 5　网格划分相关界面

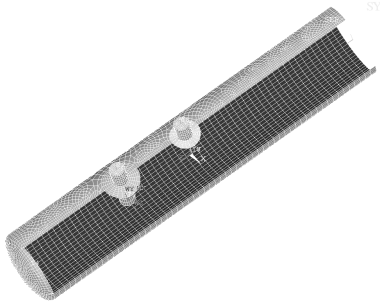


图 6　有限元模型

4　结束语

本文所研究系统基于 ANSYS 开发技术，以安全友好的界面，快速高效地实现卧式容器在 ANSYS 软件中的有限元建模，包括：快速建立几何模型；建立单元、截面形状、材料数据库，并实现自动调用属性；自定义网格尺寸、自动建立规则网格、并能够根据用户需要进行调整；建立软件人机交互界面方便用户使用。通过该系统的研发，实现了卧式容器有限元分析的流程化、模块化，提高有限元模型建立的效率，进而缩短整个有限元分析的周期。该系统将有限元分析

专业经验和流程进行了固化，提升了仿真分析的质量和效率，降低了基于 ANSYS 进行有限元分析人员的门槛，该系统的开发技术和应用可以拓展至其他设备的仿真分析过程，进一步提升力学分析水平和能力。

参考文献：

[1] 博弈创作室. ANSYS 7.0 基础教程与实例详解[M]. 北京: 中国水利水电出版社, 2004.

[2] 师访. ANSYS 二次开发及应用实例详解[M]. 北京: 中国水利水电出版社, 2012.

[3] ANSYS Inc. ANSYS APDL programmer's guide[R]. 2002.

[4] ANSYS Inc. Guide to ANSYS user programmable features[R]. 2001.

[5] 曾红, 吴鹏, 张旭. ANSYS 二次开发技术及叉车门架 CAE 系统的实现[J]. 工程机械, 2005, 36(7): 36-39.

[6] 张朋. ANSYS 二次开发及其在地下洞室分析中的应用[D]. 兰州: 兰州交通大学, 2013

人民邮电出版社

核电站电气协同设计的研究与应用

张宇，杨东，许心炜，刘森
（中广核工程设计有限公司，广东 深圳 518172）

摘　要：电气设计是核电站设计的重要组成部分，经过数十年的发展，电气设计方法和理论已经非常成熟，但传统的电气设计仍然主要以离散的图纸设计为主，数字化设计功能弱，数据和知识的协同性和共享性差；电气设计缺陷排查和设计验证主要依靠传统的设计审查、人工经验和少量的理论计算方式进行，重复工作量大，效率低。针对该现状进行深入研究，依托信息化技术手段，以设计数据为核心，研发了电气设计平台，实现电气在线协同设计，以实现有效节约人力成本，提升工作效率的目标。

关键词：协同设计；信息化；核电

1　引言

电气设计是核电站设计的重要组成部分，包括核电站输变电，所有电气设备供电、布置、保护、通信和火警的设计，设计任务重、数据量大，对核电站建设、运行和安全有至关重要的影响。经过数十年的发展，电气设计方法和理论已经非常成熟，但传统的电气设计仍然主要以离散的图纸设计为主，数字化设计功能弱，数据和知识的协同性和共享性差；电气设计缺陷排查和设计验证主要依靠传统的设计审查、人工经验和少量的理论计算方式进行，重复工作量大，管理难度大，效率低。数字化的精细协同设计和管理是未来核电站设计发展必然趋势。

核电站电气设计协同，是指核电电气设计各相关专业（包括高压设计、中低压设计、电气二次设计、平面设计等电气子专业，也包括电气设计上下游如工艺系统、仪控等）对同一个设计对象进行协同作业，达到各专业数据实时联动互通的目的。电气设计平台的研发，目标在于提高数据流通的效率，减少人工提资、收资工作，降低项目管理难度，从而提高项目管理水平。

2　协同设计方案

设计 C/S 架构，进行用户角色权限分配，实现设计用户的在线协同设计。服务器对设计的基础数据和设计对象进行统一存储和管理。设计用户通过客户端连接至服务器，对平台采用 C/S 体系架构，在服务器端统一管理平台及工程数据，在客户端实现业务功能。以工程数据库为核心，将电气系统模型与布置模型相融合，满足电气设计系统性与逻辑性的特点，同时兼顾三维工厂设计模型信息的协同和共享，通过数据驱动实现设计过程的自动化，一处修改，多处联动，构建基于电厂设计一体化的数字化设计体系，如图 1 所示。

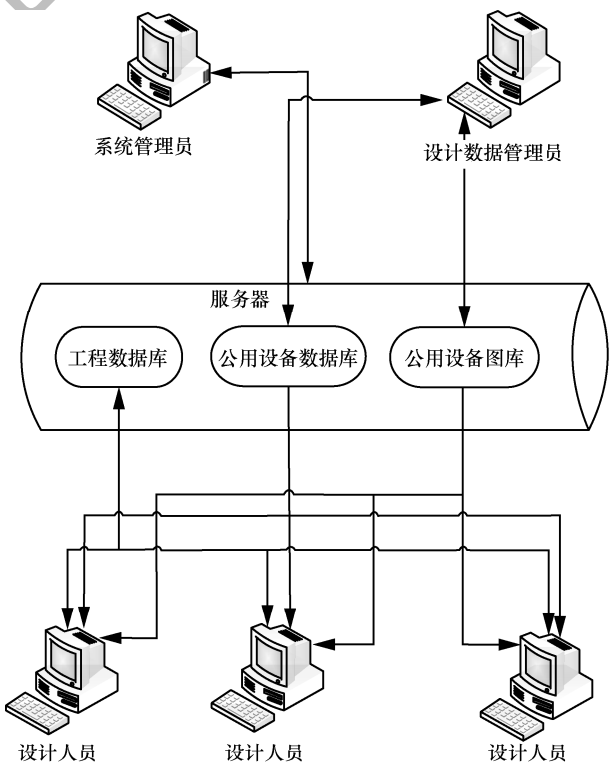


图 1　协同设计架构

核电出版社

2.1 数据统一存储和管理

基础数据包含电气设备制造厂商的设备材料型号数据和电气设计基础图符、控制回路的图形图例基础数据。其中设备材料数据使用 SQL Server 数据库平台进行统一存储和管理，图形数据采用 MongoDB 分布式文件存储技术，将图形数据存储在服务器中。设备材料库管理主要在平台中独立使用，通过权限控制，具备权限的用户才可以进行管理操作，主要管理平台中各个专业的各类设备分类及设备详细参数，所有元件数据统一在该模块下进行维护。图形图例库管理主要在 AutoCAD 软件环境下嵌入使用，通过权限控制，具备权限的用户才可以进行管理操作。AutoCAD 下的平台所用的图形图例通过该模块进行管理，例如元件符号、典型图例符号、典型图纸等。图例符号库按照专业需求，采用树形结构展示，方便用户分层浏览与查阅，同时支持用户对图例符号库结构进行编辑。

2.2 设计规则配置化和数字化

设计规则主要包含电气编码规则、选型规则、制图样式、技术条件 4 个部分。编码规则管理用于存储与管理所用的多套典型编码方案，在工程中可根据实际需要具体选择，待选基本配置内容包含机组号、系统号、设备类型码、流水号、固定文本，适应于设备、母线、柜子、回路、电缆等电气设计对象的编码应用；选型规则管理是根据电气设计法规、标准和设计经验，封装成适用不同项目/子项的选型规则集合，将经验、设计方法、相关参考在相对应的流程中存储，实现知识的共享和管理；制图样式管理主要包括对工程制图中的文字样式、线型样式和图层配置按照元件类型、设计专业等进行精细化设置，以满足制图设计需求；技术条件管理是对工程的系统分类、计算参数、防护等级、算法配置等一系列技术条件进行预设，实现设计顶层管理。设计规则可灵活配置，实现多种规则共存，用以满足不同工程条件下的设计活动。

3 应用效果

以电气在线协同设计理念进行方法研究和平台研发，在研发阶段和正式应用阶段，均使用中国自主第三代核电技术项目的项目工程数据进行测试和正式投用。

3.1 设备材料库和图形图例库

基础数据包含电气设备制造厂商的设备材料型号数据和电气设计基础图符、控制回路的图形图例基础数据。电气设计平台分别搭建了设备材料数据库和图形图例数据库，作为底层的数据支撑电气设计元件选型和自动绘图任务。

设备材料库作为支撑整个电气设计活动的厂商产品信息数据库，目前收录了 10 万条电气产品数据。设备材料库具备批量添加、删除、修改等维护工具，极大地方便了平台用户对数据进行维护，满足了电气产品的更新换代，保障了项目与市场的实时接轨。同时，设备材料库拥有多种配置模式，使不同项目、技术路线、采购包从源头上对设备材料数据进行筛选，提升了自动选型的效率。设备材料管理如图 2 所示。



图 2 设备材料管理

图例符号既是电气各种设计图的最基本单元，也是元件选型的根本依据。图例符号管理采用先进的图形存储与管理技术，将电气制图中的各种基本单元进行预先绘制，通过标签关联手段，进行统一存储和管理。

图形由基本图例符号加上连接线绘制而成，电气回路是最典型的图形代表。在高压主接线设计、中低压系统设计以及照明系统设计中，大量用到回路来完成自动绘图工作。图形管理如图 3 所示。

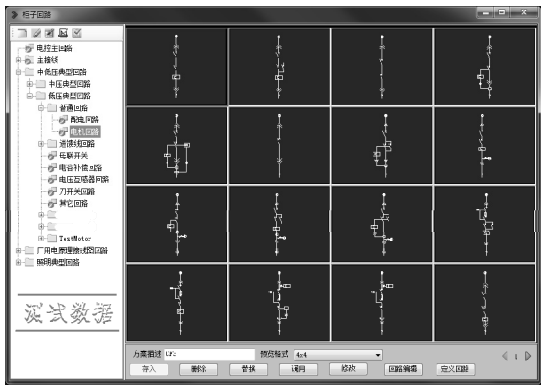


图 3 图形管理

3.2 设计规则集成和应用

平台采用“规则集成”的理念，将电气设计的设计经验、算法经验、行业规定、国家标准等作为可配置和调整的数字化规则集合，并且规则集合可多套并存，用于不同项目和子项。

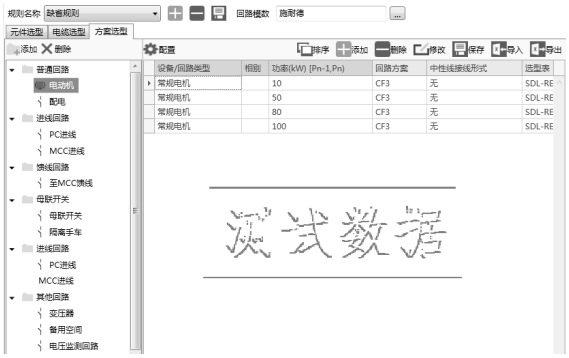


图 4　选型规则管理

每套选型规则包含一套元件选型、电缆选型和方案选型。元件选型是定义每种设备类型（如电机、加热器等）回路中各种元器件电气参数和型号，如断路器的型号、壳架电流、脱扣器额定电流、电流互感器、接触器、漏电互感器等元件及参数；电缆选型是定义每种设备类型所需连接的电缆的选型规则，如导体类型、计算系数、相截面规则、芯数形式等；方案选型是针对每种电气回路（如电机回路、配电回路、进线回路等），根据其设备/回路类型和功率/电流，配置相应的回路方案、接线形式、选型表等，通过配置的方案选型，中低压系统设计能自动根据负荷的电气参数，自动计算并选择适合的回路形式和型号参数。选型规则管理如图 4 所示。

制图样式是针对于 AutoCAD 二维出图的设置集合，包括文字、线型、图层以及各专业特定例图的绘制样式等。在设计过程中的自动绘图或者手动绘图时，平台根据当前设计模块和专业分类，自动采用预设的制图样式，使全项目的成果图纸要求和风格始终统一。

4　结束语

电气设计平台集成了数字化、智能化的电气设计工具和在线协同设计的方法，以数据驱动设计协同，使整个项目基于唯一的数据源头，项目中的不同设计角色共同参与协同设计，传统的单机离散设计状态变为在线协同，提高了信息沟通效率，提升了项目管理成效，降低了管理成本。除了在核电领域，火电、水电、新能源等领域的电气设计方法和管理方法也基本相通，该平台可以针对各领域的电气设计进行个性化的改造，具有良好的应用前景和推广意义。

参考文献：

[1] CORMEN T H, LEISERSON C E, RIVEST R L, 等. 算法导论[M]. 殷建平, 徐云, 王刚, 译. 北京: 机械工业出版社, 2013.

[2] 中国电力工程顾问集团有限公司. 电力工程设计手册[M]. 北京: 中国电力出版社, 2018.

[3] MARTIN R C. 敏捷软件开发[M]. 邓辉, 译. 北京: 清华大学出版社, 2003.

人民邮电出版社

基于 EMD-LSTM 的短期负荷预测模型

刘月灿，孙建刚，周逸，张晓亮，丁雪伟，李伟良
（国家电网有限公司信息通信分公司，北京 100761）

摘　要：为适应泛在电力物联网建设的需要，数据的深度感知成为当前亟需解决的问题。负荷预测作为电网企业的基础问题，对负荷进行精准预测成为建设泛在电力物联网的依托。随着现代电力设备的普及和深度学习算法的研究深入，电网对于负荷相关数据的获取和掌握更加方便，可借助深度学习算法进行更加准确的预测。提出采用经验模态分解算法对负荷数据进行分解，随后基于长短期记忆神经网络对分解后的各分量进行预测并加和，最后对提出的模型进行了实验验证。

关键词：经验模态分解；长短期记忆神经网络；负荷预测

1　引言

电力负荷预测对电网公司的运营和规划至关重要，随着电力市场化改革的深入以及“三型两网”建设的提出，原有的负荷预测手段已不能满足精度的需要。传统的负荷预测方法多采用时间序列预测、回归分析、人工神经网络等方法，这些方法具有一定的精度和准确度，但由于电力设备的普及，对于用户用电数据的抓取呈现多维度化，面对用电数据的复杂化和海量化，传统方法无法展现其优势。因此，为了实现对负荷数据的深度感知，对负荷数据进行多维度分析，并采用先进的算法对负荷进行预测。

本文提出采用经验模态分解（empirical mode decomposition，EMD）算法对负荷数据进行消噪和多维度分解，采用对时间序列具有良好预测性能的深度学习算法长短期记忆（long short term memory，LSTM）神经网络对各维度序列进行预测，将各维度序列预测结果相加得到最终预测结果。最后通过实验证明了本文提出的模型具有较高的精度。

2　相关算法介绍

2.1　EMD 算法原理

EMD 方法在理论上可以应用于任何类型的时间序列的分解，尤其在处理非平稳及非线性数据上，比之前的平稳化的方法更具有优势。不同于傅里叶变换和小波变化，其不需要事先确定基函数，实质上是局部的平稳化[1]。EMD 可将时间序列分解为本质模态函数（IMF）和残波，IMF 分量反映了原始时间序列的不同时间尺度的振荡特性，而残波反映了原始序列的长期趋势。然而，上述 IMF 分量包含两个约束：一是零交叉和极值点的数量需要相同，二是 IMF 信号应该是零均值。EMD 的分解过程[2-3]是：找出原数据序列 X_t 所有的极大值点，并用 3 次样条插值函数拟合形成原数据的上包络线；然后找出所有的极小值点，并将所有的极小值点通过 3 次样条插值拟合形成数据的下包络线，上包络线和下包络线的均值记为 m_t，将原数据序列，减去该平均值，得到一个新的数据序列：

$$h_t = X_t - m_t, t = 1,2,\ldots \tag{1}$$

其中，t 代表筛选次数，如果 h_t 满足 IMF 的两个条件，则 h_t 是滤波的 IMF 分量，若不满足，则需要重复上述步骤继续进行筛选，直到满足条件。

本文采用阈值 λ 表示筛选过程的停止条件：

$$\lambda = \sum_t \frac{|h_{t-1} - h_t|^2}{h_{t-1}^{\ 2}} \tag{2}$$

λ 的值由经验确定，在重复实验的过程中，当 λ 的值连续 5 次在设定的阈值之下，可以停止筛选并将此时的数据序列 h_t 选为 IMF 组分。对于生序序列：

$$r_t = X_t - h_t \tag{3}$$

对 r_t 重复以上的 IMF 筛选步骤，直到趋势项 r_t 变为单调函数时，IMF 组分不能从新序列中筛选出来，则整个 EMD 分解过程结束。以下是整个 EMD 分解表达式：

人民邮电出版社

$$X_t = \sum_t h_t + R_n \tag{4}$$

其中，R_n 为残波，代表序列长期趋势。

2.2 LSTM 算法原理

LSTM 是深度学习中非常适合用于时间序列预测的一个算法，它在 RNN 的基础上增加了一个参数，用来保存长期的状态[4]，因此对于像负荷数据这种具有明显季节性趋势的数据，具有良好的预测能力。LSTM 示意如图 1 所示。

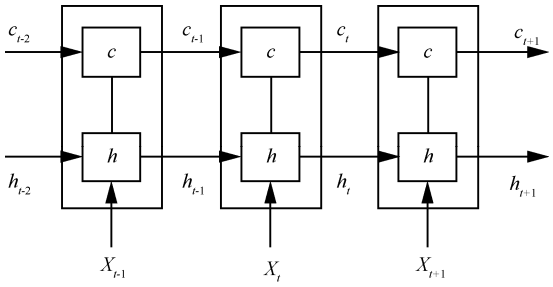


图 1　LSTM 示意

其中，h 为 RNN 中的状态，c 为新增加的状态，称为单元状态，t 代表当前时刻，x 为当前时刻输入值。在 t 时刻，LSTM 的输入有 3 个：当前时刻网络的输入值、上一时刻 LSTM 的输出值以及上一时刻的单元状态；输出有两个：当前时刻的输出值和当前时刻的单元状态[5]。

3　模型构建

通过对 EMD 和 LSTM 算法的研究，本文构建了基于 EMD-LSTM 的预测模型，用以实现以小时为单位的短期负荷预测。本文提出的预测模型流程如图 2 所示。

由于采集到的负荷数据中夹杂着大量的噪声，并且负荷会受多维度的因素影响，为了进行数据消噪并提取负荷的多维度信息，本文采用 EMD 进行模态分解，根据经验设定阈值，得到多个本质模态函数序列和残波。得到的各序列可视为受不同因素影响的负荷振荡特征和趋势特征，随后将各序列输入 LSTM 网络分别进行预测，最后将各序列的预测结果相加即为最终的预测序列。

4　实验分析

实验数据为某市 2018 年 3 月 1 日—2018 年 9 月 1 日以小时为单位的负荷数据。

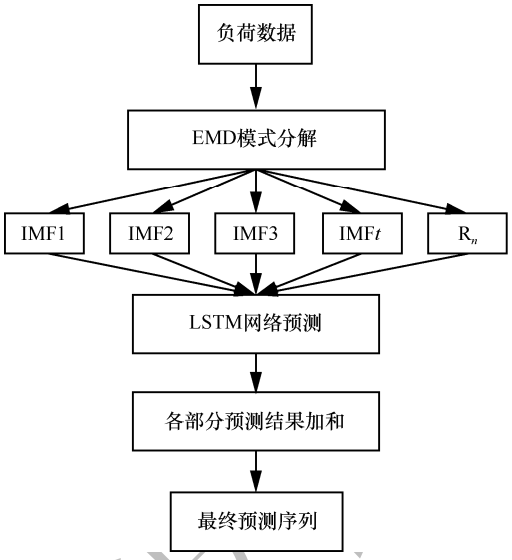


图 2　预测模型流程图

在做 EMD 模态分解时，选择的阈值为 $\lambda = 0.5$，最终得到了 5 个 IMF 成分（编号为 1~5）和一个残波。对于本文所用 LSTM 算法，用 Python 语言实现，将数据集随机分配比例为 0.75、0.1、0.15 分别作为训练集、验证集和测试集。隐层的维度设置为 100，迭代 100 次。本文实现的是短期预测，预测其中 3 天 72 个点的负荷值与真实值的结果对比如图 3 所示。

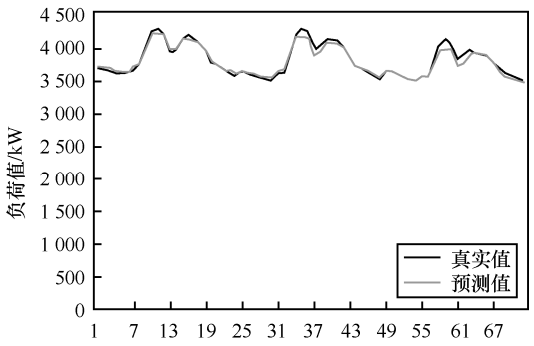


图 3　预测值与真实值对比

本文将传统的用于时间序列预测的算法（ARIMA 和 ANN）用来做同样的预测，计算本文提出的方法与传统方法预测结果的均方根误差以及误差率，所用计算式如下：

$$\text{RMSE}=\sqrt{\frac{\sum_{i=1}^{n}\left(x_{\text{actual}}-x_{\text{forecasting}}\right)^2}{n}} \tag{5}$$

$$\text{error rate}=\frac{\left|x_{\text{actual}}-x_{\text{forecasting}}\right|}{x_{\text{actual}}}\cdot 100\% \tag{6}$$

人民邮电出版社

其中，x_{actual} 代表真实值，$x_{forecasting}$ 代表预测值，n 为预测值和真实值的个数。对于 3 种方法，均方根误差和误差率的比较见表 1。

表 1　3 种模型的比较结果

模型	RMSE	误差率
ARIMA	381.931 1	24.421%
ANN	289.345 6	20.257%
EMD-LSTM	172.350 5	10.934%

实验证明，本文提出的基于 EMD-LSTM 的短期负荷预测模型可提高负荷预测精度，以辅助电网公司制定决策。

5　结束语

本文提出的基于 EMD-LSTM 的短期负荷预测模型首先对负荷数据进行 EMD 模态分解，然后对各分解序列分别采用 LSTM 网络进行预测，最后将各序列预测结果相加得到最终预测结果。实验证明，本文提出的方法与传统方法相比具有更高的精度，能够辅助电网公司相关工作人员制定决策，在一定程度上为负荷数据的深度感知做出了贡献。

参考文献：

[1] 孙巍伟, 黄民, 高延. 基于 EMD-HMM 的机床刀具磨损故障诊断[J]. 机床与液压, 2017, 45(13): 178-181.

[2] 高波, 张钦宇, 梁永生, 等. 基于 EMD 及 ARMA 的自相似网络流量预测[J]. 通信学报, 2011, 32(4): 47-56.

[3] 王文波, 费浦生, 羿旭明. 基于 EMD 与神经网络的中国股票市场预测[J]. 系统工程理论与实践, 2010, 30(6): 1027-1033.

[4] 陆泽楠, 商玉林. 基于 LSTM 神经网络模型的钢铁价格预测[J]. 科技视界, 2017(13): 116-117.

[5] 陈卓, 孙龙祥. 基于深度学习 LSTM 网络的短期电力负荷预测方法[J]. 电子技术, 2018, 47(1): 39-41.

人民邮电出版社

基于 EMS 系统区域备自投在湛江电网中的应用

付振宇
（广东电网有限责任公司湛江供电局，广东 湛江 524000）

摘　要：湛江地区地处雷州半岛、广东电网西端边界处，网架薄弱，夏秋季又多台风暴雨，电网运行风险较多。通过完善网络结构及站内标准备自投建设，消除部分基准风险，但较多基准风险及基于问题风险还未得到解决，因此在网架允许的情况下通过基于 EMS（energy management system，能量管理系统）区域备自投解决基于基准风险及基于问题风险。

关键词：电网风险；EMS；区域备自投

1　引言

湛江电网网架相对薄弱，运行风险较多。正常运行方式或检修方式存在单一故障发生变电站失压的风险，通过站内标准备自投无法消除的风险，在网架允许的情况下通过基于 EMS（energy management system，能量管理系统）系统区域备自投能有效解决该类风险。

2　区域备自投逻辑

区域备自投作为单独的功能模块嵌入 EMS，采用跨厂站遥控实现区域备自投，适用范围广，现已应用于线路检修状态下提高供电可靠性，探索出补充及代替站内备自投新途径，同时适用于带小电源厂站。区域备自投的实时数据和模型都来源于 EMS，通过对 EMS 模型和实时数据的处理，做出相应判断，在符合备自投动作的全部条件时，进行遥控操作，完成备自投功能。区域备自投读取 EMS 网络模型，通过区域备自投建模工具，把区域备自投的充/放电、闭锁、触发、动作条件及遥控操作编辑为一个固定模型。备自投程序根据已有模型读取 SCADA（supervisory control and data acquisition，数据采集与监视控制系统）的遥信遥测量，对备自投串实时状态进行判断，当满足动作条件时，向 EMS 下发遥控指令，由 SCADA 完成遥控操作，实现备自投功能。为了防止模型及动作逻辑的错误，增加了逻辑校正功能。区域备自投功能框架如图 1 所示。

区域备自投一个站串建立完成，在人工投运和解闭锁后进入工作状态，在区域备自投工作的任何状态都可以人工闭锁和停运。区域备自投工作状态分为放电状态、充电状态、触发等待动作、动作等待触发判断状态、遥控状态。进入充电状态后，区域备自投程序持续检测闭锁条件、触发条件和动作条件，满足闭锁条件并在整区域备自投解锁后，读取 EMS 实时数据，先进行充放电状态判断，放电时持续等待，直到满足充电条件并在整定时间内持续满足，区域备自投

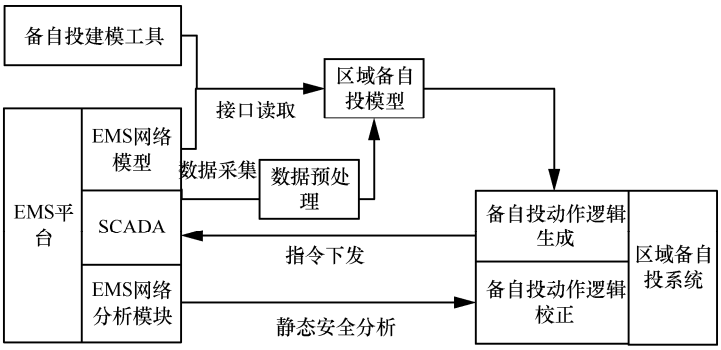


图 1　区域备自投功能框架

人民邮电出版社

进入充电状态。区域备自投充电时，在连续不满足充电条件 40 s 后，进入放电状态持续等待。整定时间内持续满足时，根据中断触发条件和动作条件判断，进入闭锁状态，直到人工解闭锁。区域备自投与传统站内备自投一个重要的不同是增加了触发条件。传统站内备自投误动可能性很低，在二次回路上也容易引入保护信号和手动跳闸闭锁，而 EMS 由于经过站内转发，还受通道、前置等影响，存在信号误发的可能。为此，区域备自投把动作条件拆分为触发条件和动作条件，以保护信号为核心组成触发判据，以遥测量为核心组成动作判据，相互结合，减少误信号带来的影响，同时方便分类管理。当触发或动作条件任一满足时，等待另一条件是否满足，当两组条件都满足后进入校验遥控阶段；当触发和动作条件未能在整定时间内满足时，备自投进入闭锁状态。区域备自投进入校验遥控阶段后，会根据设定的操作顺序操作开关。每次操作前检测上一操作是否完成，操作完成后检查操作过程是否正确；当校验不通过时，中断遥控操作。操作结束后进入闭锁状态。区域备自投工作过程如图 2 所示。

3 区域备自投实际应用场景

（1）正常运行情况下提高供电可靠性

由于传统站内备自投的局限性，无法实现跨厂站遥控，而在特定的运行方式下，部分厂站虽有主备供电线路却无法自动实现备自投功能。为了解决这种运

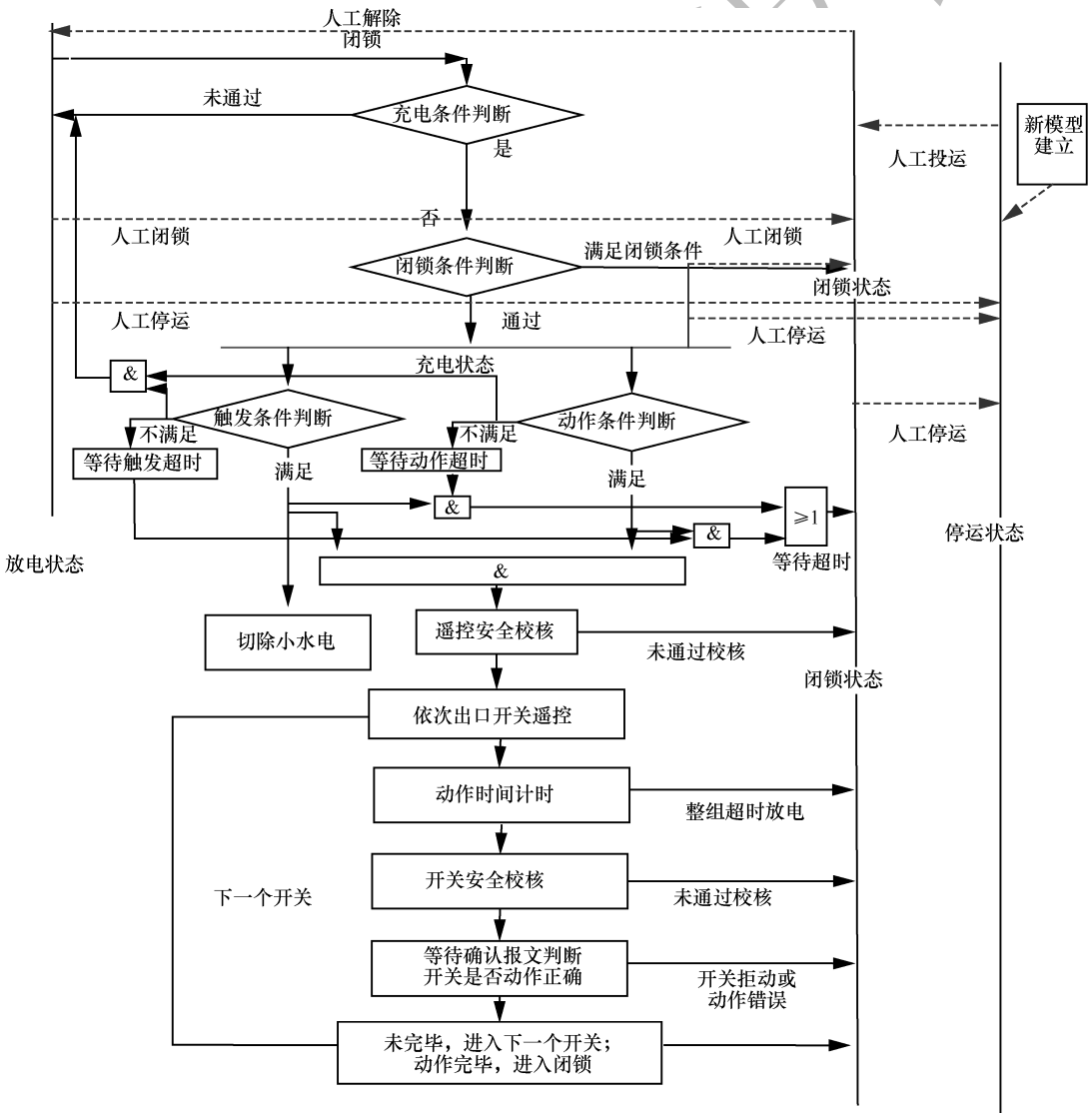


图 2　区域备自投工作过程

行方式下的供电可靠性问题，使用基于 EMS 的区域备自投系统来实现备自投功能。由于 EMS 能可靠实现遥控功能，难点在于区域备自投的逻辑设置。雷龙乌串运行方式如图 3 所示。

在图 3 的运行方式中龙门站面临失压而不具备备自投功能的风险，继保专业详细分析该运行方式下的特点，给出详细的充电条件，并根据备自投使用的基本原则设置闭锁条件。在制定区域备自投逻辑时，继保专业人员先采用穷举法，列举出该运行方式下所有可能出现的故障情况，对所有故障情况下的电气特征进行分析总结，得出该运行方式下的各个故障方案，确定备自投运行的各项参数。自动化根据故障方案对区域内各个厂站进行建模，并配合继保专业进行厂站测试，实际模拟出故障情况，进一步检验区域备自投的性能。在现场测试中，区域备自投经过各个故障方案测试，能根据预先设定的逻辑，做出正确的判断，自动实现区域备自投功能。

（2）线路检修状态下提高供电可靠性

赤沙金串运行方式如图 4 所示，当赤沙甲乙线中有一回线路检修的情况下，沙郭站供电可靠性变低。由于检修持续时间不长，在检修期间不会增加设备进行保护，导致沙郭站停电风险高。

而区域备自投具有快速投运等特点，在这种特殊的运行方式下发挥作用，能有效降低线路检修停电期间的风险。在回路检修期间，使用区域备自投可以给沙郭站配置备自投功能；在回路检修结束后，退出区域备自投恢复原有站内备自投，确保了线路检修期间的供电可靠性。

（3）作为站内备自投的补充

通过宝满霞山串单站区域备自投的现场测试，证明区域备自投能实现站内备自投的功能，拓大了备自投的使用范围，能应用于大部分需要备自投功能的场合。

（4）适用于带小电源的厂站

在带小电源的厂站发生失压而该站不能孤网运行时，由于小电源供电母线仍有压，站内备自投无法动作，将导致更大的损失。霞太良串运行方式如图 5 所示，当太平站因霞太线故障失压时，备自投可以切除小电源太鸣甲乙线路，同时切断霞山主供电源，投入良丰站备用电源，避免存在小电源、不能孤网运

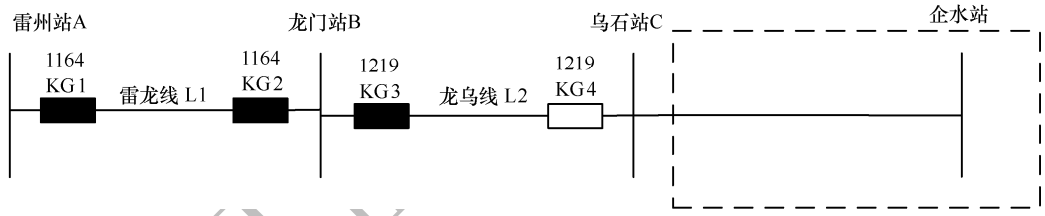


图 3　雷龙乌串运行方式

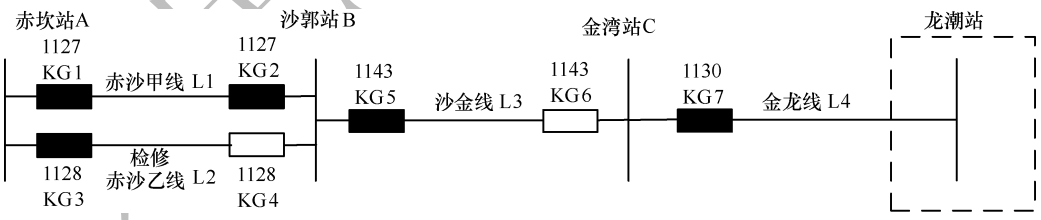


图 4　赤沙金串运行方式

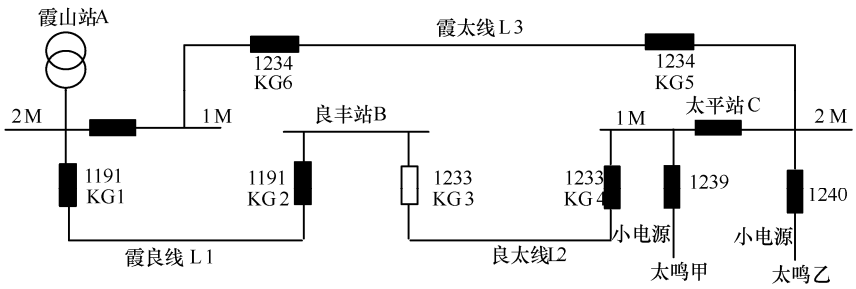


图 5　霞太良串运行方式

行的情况下，太平站无法实现备自投的情况。

4 区域备自投现场调试

区域备自投在主站端经过软件模型自行调试后，在通过相应站端现场带测控装置调试后，才能闭环投入运行。现场测试主要通过采用模拟断路器来模拟相应串的需要遥控的开关；通过继电保护测试仪来模拟厂站的遥信遥测信号，并采用 GPS 时钟定时触发方式使多台继电保护测试仪同时启动，以此模拟故障时各开关分、合及相应的电流、电压变化过程，达到模拟现场故障动作相应各类遥信遥测量传送到主站侧的效果。测试前编制相应模拟各类故障的现场测试表单，主站及现场测试人员按表单进行测试，现场测试模型如图 6 所示，现场测试记录表单见表 1。

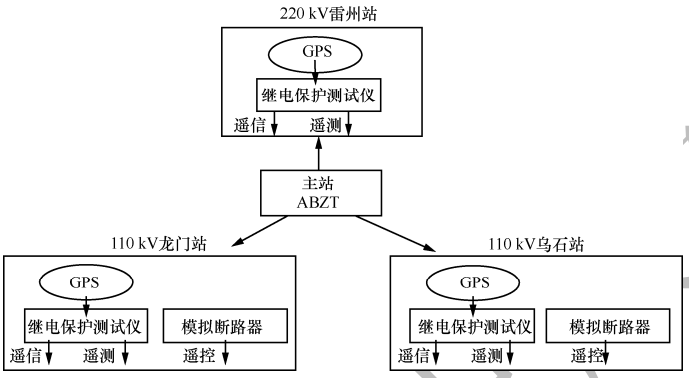


图 6　现场测试模型

表 1　现场测试记录表单

雷龙乌串区备现场测试记录							
方式1 第1组	模型一	雷州站A　龙门站B　乌石站C　企水站 1164 KG1　雷龙线 L1　1164 KG2　1219 KG3　龙乌线 L2　1219 KG4					
	变电站	220 kV雷州站			开关间隔	110 kV雷龙线开关	
	模型间隔	KG1			测试人		
	故障编号	GZ-1101			测试日期		
	故障名称	方式一：L1永久性故障					
	策略类型	正常状态					
	模拟开关初始状态	信号	KG1 ABC相	1 G	2 G	3 G	其他遥信	现场确认
		状态	合位					
		信号	线路电压	母线电压	线路电流			
		状态		ON	ON			
	模拟开关动作策略	顺序	信号/模拟量		状态	时间	核对确认	备注
		1	保护动作		ON	0		
		2	KG1 ABC相		分位	80		
		3	线路电流I		OFF	80		
		4	KG1 ABC相		合位	1 080		
		5	线路电流I		ON	1 080		
		6	保护动作		ON	1 180		
		7	KG1 ABC相		分位	1 260		
		8	线路电流I		OFF	1 260		
		9						
		10						
		11						
		12						
		13						
		14						
		15						
		16						
		17						
		18						
		19						
		20						
		21						
		22						
		23						
		24						
	现场动作情况记录	策略触发过程无误，开关无动作					现场确认	
	备注	区域备自投动作						
	结论	正确						

5 结束语

（1）节约成本，提高效率

新增区域备自投只需要继保方式专业给出区域备自投逻辑及各项参数，在自动化机房即可完成建设，无需增加投资、安装及维护，节省设备费用；通过优化区域备自投逻辑，从保护动作情况分析转为采集信号结果分析，优化测试逻辑，并利用现有继保测试仪及模拟开关断路器自主调试，无需新增资金投入，缩短建设周期，使区域备自投得到较为广泛的应用。

（2）管理维护便捷

作为嵌入 EMS 的软件模块，区域备自投比站内备自投更便捷。调度员可以通过区域备自投运行界面进行区域备自投的投退操作，无需安排人员到站，节省人力物力。通过区域备自投监视界面，能方便地对各个备自投情况进行监视，还能结合区域备自投发出的告警，第一时间发现电网异常情况。在发生变电站失压时，区域备自投能自动投切电源或切换至半自动模式辅助调度员迅速恢复供电。

参考文献:

[1] 邹德虎, 王仲达, 徐柳飞, 等. 网络备自投系统在地调 EMS 中的应用[J]. 电力系统自动化, 2003, 37(17): 106-111.

人民邮电出版社

基于 FCME 检测的脉冲干扰抑制方法

余梦佳[1]，尧广[1]，罗新[1]，刘利[1]，施崇智[1]，高畅[2]
（1. 国网泸州供电公司，四川 泸州 646000;
2. 国网四川省电力公司检修公司，四川 成都 610000）

摘　要：针对 FCME（forward consecutive mean excision，前向连续均值去除）算法检测时间过长，且常规干扰处理方法抑制干扰后出现数据缺损的不足，研究一种基于改进 FCME 检测的 FBMC（filter banks multi-carrier，滤波器组多载波）脉冲干扰抑制方法。该方法包括干扰检测和干扰消除两方面：干扰检测是对 FCME 检测算法中的初始门限计算进行改进，以误符号率最低的样本计算初始门限；干扰消除则是根据检测结果，结合压缩感知技术提纯脉冲干扰，再将原接收信号与脉冲干扰作差实现。仿真结果验证改进的干扰检测方法在保证 FCME 检测性能的同时缩短了检测时间，且干扰抑制效果优于常规方法，提高了 FBMC 数据传输的可靠性。

关键词：压缩感知；FCME；干扰抑制；误符号率

1　引言

泛在电力物联网是覆盖电力“云、网、端”，与智能电网“同生共存”的国网公司第二张网，是新时代国网信息化发展的新战略。滤波器组多载波（filter banks multi-carrier，FBMC）作为泛在电力物联网建设的候选技术，相较于正交频分复用（orthogonal frequency division multiplexing，OFDM）[1-2]具有无需循环前缀、频谱利用率较高等优势[3-4]。在多种 FBMC 调制中，基于余弦调制滤波器组（cosine modulation filter-banks，CMFB）的 FBMC 因抗干扰能力强得到广泛研究[5-6]。然而不可避免的是 FBMC 存在对外界干扰敏感的问题，其中较为敏感的是时域脉冲干扰（time domain pulse interference，TDPI）。TDPI 的特点是幅值大、持续时间短，通过时频变换后，对整个频谱都会产生影响，使得 FBMC 系统误符号率（symbol error rate，SER）增加。

FBMC 干扰抑制算法相继提出，主要分为干扰检测和干扰处理 2 个步骤[7-13]。干扰检测时通常采用能量检测法，该方法无需干扰信号先验信息，通过计算设定时间内接收到信号的能量，将其与事先设定的阈值（门限制）进行比较，以此判断该接收信号中是否存在干扰[7-8]。参考文献[9-10]分别提出了双门限检测和最小值检测算法，均能够有效提高检测精度，前者存在的问题是难以判断能量处于两门限间的信号是否存在干扰，而后者的问题则是检测概率与虚警概率难以平衡。由此，频域前向连续均值去除（forward consecutive mean excision，FCME）检测算法被提出[11]，该方法是对连续均值去除(consecutive mean excision，CME)算法的改进，可以对干扰有效地进行检测，存在的问题是检测时间过长且常规干扰处理方法抑制干扰后出现数据缺损。

干扰处理常用门限归零法及修剪法[12]。门限归零法实现简单，但容易出现数据信号丢失。门限修剪法在检测出干扰后，将门限值赋予干扰点，一定程度上减少了信号损伤，但也引入了一定误差，参考文献[13]利用压缩感知和预留子载波技术预判干扰，通过原信号与干扰作差的方法消除干扰，无需检测，该方法能有效降低系统误符号率，但其预判干扰过程没有检测，可能造成误判产生新干扰。

针对以上问题，文中将 FCME 应用于基于 CMFB 的 FBMC 系统，给出了一种基于改进 FCME 检测的 FBMC 脉冲干扰抑制方法：首先 FBMC 系统接收端利用改进的 FCME 算法对干扰位置进行检测；再根据预留子载波上的信息，通过压缩感知贪婪基追踪算法重建干扰，最后结合检测信息，在混合干扰中提取纯净的 TDPI 并消除。

2　基于 CMFB 的 FBMC 系统模型

基于 CMFB 的 FBMC 系统框图如图 1 所示。为

基金项目：重庆市教育科学“十三五”规划课题（No.2018-GX-384）；重庆电子工程职业学院自然科学类项目（No.XJZK201807）

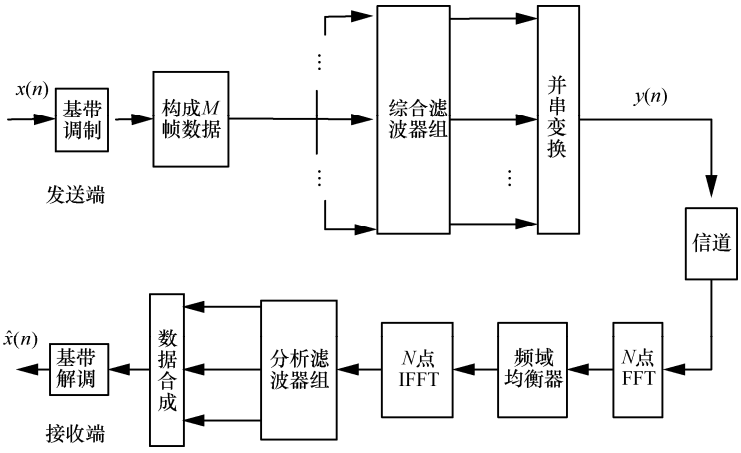


图 1　基于 CMFB 的 FBMC 系统框图

使信号压缩更为醒目，更好地与 GBP 算法结合[14]，文中的 FBMC 综合滤波器组（synthesis filter banks，SFB）与分析滤波器组（analysis filter bank，AFB）均采用 DCT-4 变换矩阵。发送端输入信号首先通过基带调制、信号映射，变换为 M 个并行子带信号，再经 SFB 调制和并串转换发送出去。在接收端，信号先经过频域均衡、AFB 解调，再通过合成与基带解调得到原始信号。

当信号在信道中传播受到时域脉冲干扰时，脉冲干扰经过 AFB 后反变换到频域中，使其能量被分配到各个频点，严重影响信号后续处理。

3　干扰分析

3.1　压缩感知 GBP 算法估计混合干扰

在多载波通信中，不承载信号的子载波被称为预留子载波。文中就是用其估计干扰，设 FBMC 系统接收到的信号为

$$\begin{aligned} \boldsymbol{y} &= \boldsymbol{\Psi W x} + \boldsymbol{w} + \boldsymbol{e} \\ &= \boldsymbol{s} + \boldsymbol{w} + \boldsymbol{e} \end{aligned} \tag{1}$$

其中，$\boldsymbol{s}$ 为 FBMC 发送信号，$\boldsymbol{w}$ 为高斯噪声，$\boldsymbol{e}$ 为时域脉冲干扰，子载波个数为 M，$\boldsymbol{\Psi}$ 为 DCT-4 变换矩阵，$\boldsymbol{x}$ 为输入信号，可以将 $\boldsymbol{x}$ 看作一个$(M\text{-}m)\times 1$ 的向量，m 为预留出的不承载信号的子载波的个数，$\boldsymbol{W}$ 为一个扩展矩阵，该矩阵可将 $\boldsymbol{x}$ 扩展为一个 $M\times 1$ 的向量，可以等价认为是在向量 $\boldsymbol{x}$ 中插入了 m 个零。再将 FBMC 调制信号发送到高斯信道中，为简化论述，只在 $\boldsymbol{s}$ 中叠加 $\boldsymbol{e}$ 和 $\boldsymbol{w}$，且单个脉冲干扰时间宽度一个时隙。由于时域脉冲干扰的稀疏特性，可将 k 个不同位置表示为形如 $\boldsymbol{e}=[e_1,0,e_2,...,e_k,0]^T$ 的 $M\times 1$ 向量。当多个脉冲作用在同一时隙时，可视为该处仅有一个脉冲，其幅度为这几个脉冲的叠加。信号在干扰抑制模块中经过 AFB 后的信号为

$$\boldsymbol{Y} = \boldsymbol{\Psi}^{-1}(\boldsymbol{s}+\boldsymbol{e}+\boldsymbol{w}) \tag{2}$$

其中，$\boldsymbol{\Psi}^{-1}$ 为一个 $\boldsymbol{\Psi}$ 的逆矩阵。在对 $\boldsymbol{Y}$ 完成解调之后，提取预留子载波中的信号为

$$\begin{aligned} \tilde{\boldsymbol{E}} &= \overline{\boldsymbol{W}}\boldsymbol{Y} \\ &= \overline{\boldsymbol{W}}\boldsymbol{\Psi}^{-1}(\boldsymbol{y}+\boldsymbol{e}+\boldsymbol{w}) \\ &= \overline{\boldsymbol{W}}\boldsymbol{\Psi}^{-1}(\boldsymbol{e}+\boldsymbol{w}) \end{aligned} \tag{3}$$

其中，$\overline{\boldsymbol{W}}$ 为抽取矩阵，可以提取预留子载波上的信号。由于信道中只有高斯噪声，预留子载波上的信息应全部是 $\boldsymbol{e}$ 和 $\boldsymbol{w}$ 留下的，因此 $\tilde{\boldsymbol{E}}$ 是在 DCT-4 变换基上对 $\boldsymbol{e}$ 和 $\boldsymbol{w}$ 的观测值。

可以将 GBP 算法建模为

$$f(\boldsymbol{\Phi},\boldsymbol{D},\boldsymbol{r}) = \boldsymbol{u} \tag{4}$$

其中，$\boldsymbol{\Phi}$，$\boldsymbol{D}$，$\boldsymbol{r}$ 分别为随机高斯矩阵、基矩阵以及观测值，$\boldsymbol{u}$ 为重构信号，$\boldsymbol{f}$ 为实现信号重构的函数。在 CS 框架下，为了更精确地重构出信号，应根据信号自身的特点，寻找最适合其特征的正交基 $\boldsymbol{D}$。在 CMFB 中，显然 DCT-4 基相较于其他基更加匹配。将 $\tilde{\boldsymbol{E}}$ 代入 GBP 函数得到

$$f(\boldsymbol{\Phi},\boldsymbol{\Psi},\tilde{\boldsymbol{E}}) = \Delta(\boldsymbol{e}+\boldsymbol{w}) \tag{5}$$

比较常见的方法是将估计出的信号与 $\boldsymbol{y}$ 直接作差，再通过 AFB 解调得到

$$\begin{aligned} \tilde{\boldsymbol{Y}} &= \boldsymbol{\Psi}^{-1}[\boldsymbol{s}+\boldsymbol{e}+\boldsymbol{w}-\Delta(\boldsymbol{e}+\boldsymbol{w})] \\ &= \boldsymbol{\Psi}^{-1}(\boldsymbol{s}+\Delta) \end{aligned} \tag{6}$$

人民邮电出版社

通过 $\tilde{\boldsymbol{Y}}$，只要提取出数据子载波上的信息，经并串变换、解调等信号处理过程即可得到原信号。

但在式（6）的恢复过程中，由于 $\boldsymbol{w}$ 的影响，仿真结果表明：相较于 $\Delta(\boldsymbol{e}+\boldsymbol{w})$ 作为干扰估计，用纯净的时域脉冲干扰 $\Delta\boldsymbol{e}$，会使解调信号的 SER 更加理想。因此为进一步精确地恢复信号，在 $\Delta(\boldsymbol{e}+\boldsymbol{w})$ 中提取 $\Delta\boldsymbol{e}$ 是必要的。

3.2 基于最低误码率的 FCME 干扰检测

信号的频域能量检测原理如图 2 所示。信号经过 FFT 运算后，在若干个频点上取平均，获得系统频域范围内的干扰功率，然后进行干扰判决，给出判决结果。

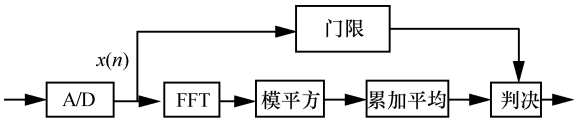


图 2　频域能量检测原理

频域能量检测利用多音干扰的能量集中在有限个频点的特点，有效检测信号受干扰的频点。由于 $\boldsymbol{e}$ 的能量集中在有限时域，可以将能量检测算法原理应用到 $\boldsymbol{e}$ 的时域检测中。

FCME 是一种能量检测方法[15]，它的初始门限的均值因子选取接收信号谱线中最小的一部分，认为它们没有受到干扰，用其估计均值，然后以此均值设置初始门限，将频点分成两部分：噪声频点集合和被干扰频点集合。通过迭代运算不断地从噪声频点集合中去除大于门限的频点，加到被干扰频点集合，再计算门限来进行去除操作，直到没有频点被去除为止[16]。

由于 FCME 设置的初始门限通常较低，在数据较大时迭代次数的增加，将导致运算时间增大。基于此，文中在将其应用于时域检测时做出了改进，研究了一种改进的 FCME 算法，伪代码见表 1。

表 1　改进 FCME 算法伪代码

改进的 FCME 算法：

初始化发送端发送 V 组数据的向量集合 $D=\{\boldsymbol{D}_1,...,\boldsymbol{D}_V\}$，其中 $\boldsymbol{D}_V=[a_1^V,...a_M^V]$，$a_M^V$ 的上标表示第 V 组，下标对应该组数据长度 M，空集 R；

计算每组数据相对应的误符号率，构成集合 $P=\{P_1,...,P_V\}$；

P 中最小 N 个数构成集合 P'，$P'=\{P_1',P_2',...,P_N'\}$，对应向量集合 $D'=\{\boldsymbol{D}_1',...,\boldsymbol{D}_N'\}$；

for i=1 to N

　$x_i=0$；

　for j=1:M

　　$p_j=\left|a_j^L\right|^2$；

　end for

　$\overline{p}_i=\dfrac{\sum_{i=0}^{L}p_i}{M}$；

end for

$t=\dfrac{\sum_{j=1}^{N}\left|\overline{p}_j\right|^2}{N}$；

根据式 13 确定 k；

根据 k 初始门限 $T=kt$；

重复以下步骤，直至 R 中的数据不变为止；

接收一组数据 $y_1,y_2,...,y_M$；

for i=1 to M

　Q=0；

　if $|y_i|^2\le kt$

　　$y_i\in$R，$Q=Q+1$；

　end if

end for

计算 $t_1=\dfrac{\sum_{i=1}^{Q}|y_i|^2}{Q}$；

更新 $t=t_1$；

3.3 检测性能

高斯噪声概率密度为

$$P(x)=\frac{1}{\sqrt{2\pi}\sigma}\mathrm{e}^{-\frac{x}{2\sigma^2}} \tag{7}$$

文中干扰点的检测模型为

$$\begin{cases}H_0:\boldsymbol{i}=\boldsymbol{s}+\boldsymbol{w}\\ H_1:\boldsymbol{i}=\boldsymbol{s}+\boldsymbol{w}+\boldsymbol{e}\end{cases} \tag{8}$$

其中，H_1、H_0 分别为 $\boldsymbol{e}$ 存在和不存在 2 种状态。当 $\boldsymbol{e}$ 与 $\boldsymbol{w}$ 均为高斯分布的平稳随机过程时，信号模型简化为高斯背景下高斯信号的最佳检测问题，则检测统计量近似服从高斯分布[17]，可以表示为

$$H_0:Y\sim N(\sigma_{\boldsymbol{s}}^2+\sigma_{\boldsymbol{w}}^2,\frac{2}{M}(\sigma_{\boldsymbol{s}}^2+\sigma_{\boldsymbol{w}}^2)^2) \tag{9}$$

$$H_1:Y\sim N(\sigma_{\boldsymbol{s}}^2+\sigma_{\boldsymbol{w}}^2+\sigma_{\boldsymbol{e}}^2,\frac{2}{M}(\sigma_{\boldsymbol{s}}^2+\sigma_{\boldsymbol{w}}^2+\sigma_{\boldsymbol{e}}^2)^2) \tag{10}$$

其中，$\sigma_{\boldsymbol{s}}^2$、$\sigma_{\boldsymbol{w}}^2$、$\sigma_{\boldsymbol{e}}^2$ 分别为 $\boldsymbol{s}$、$\boldsymbol{w}$、$\boldsymbol{e}$ 的平均功率。检测概率 P_d 和虚警概率 P_f 为

$$\begin{aligned}P_d&=P\{Y>kt\,|\,H_1\}\\&=Q\left(\frac{kt-(\sigma_{\boldsymbol{s}}^2+\sigma_{\boldsymbol{w}}^2+\sigma_{\boldsymbol{e}}^2)}{(\sigma_{\boldsymbol{s}}^2+\sigma_{\boldsymbol{w}}^2+\sigma_{\boldsymbol{e}}^2)\sqrt{2/M}}\right)\end{aligned} \tag{11}$$

$$P_f\{Y>kt\,|\,H_0\}=Q\left(\frac{kt-\sigma_{\boldsymbol{s}}^2-\sigma_{\boldsymbol{w}}^2}{(\sigma_{\boldsymbol{s}}^2+\sigma_{\boldsymbol{w}}^2)\sqrt{2/M}}\right) \tag{12}$$

其中，$Q(x)=\dfrac{2}{\sqrt{\pi}}\int_x^{\infty}\mathrm{e}^{-t^2}dt$，$P_d$ 为 $\boldsymbol{e}$ 存在时，判定 H_1

人民邮电出版社

的概率，P_f 为 $\boldsymbol{e}$ 不存在时，判定为 H_1 的概率，可得到判决门限为

$$kt=\sigma_w^2+\sigma_s^2+\sqrt{\frac{2}{M}}Q^{-1}(P_f) \tag{13}$$

代入上式可得

$$P_f\{Y>kt/H_0\}=Q(\frac{Q^{-1}P(f)}{\sigma_s^2+\sigma_w^2}) \tag{14}$$

$$P_d\{Y>kt/H_1\}=Q(\frac{\sqrt{M/2}\sigma_e^2}{(\sigma_s^2+\sigma_w^2+\sigma_e^2)}) \tag{15}$$

3.4 干扰的消除

检测到干扰后，处理干扰点的常见方法是门限归零法[18]和门限修剪法[19]。文中干扰的消除处理如图 3 所示。

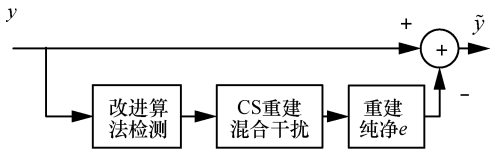


图 3　干扰消除原理

由 CS 技术估计出的混合干扰信号为 $\tilde{e}$，将 $\tilde{e}$ 中除干扰时隙点外的其他点置零得 $\hat{e}$，此时的 $\hat{e}$ 是重建的脉冲干扰，将接收信号与 $\hat{e}$ 作差，得

$$\begin{aligned}\tilde{y}&=s+e+w-\hat{e}\\&=s+e+w-\hat{e}\\&=s+w+\Delta e\end{aligned} \tag{16}$$

将干扰消除后的信号进行均衡、AFB 解调以及基带解调等操作即可恢复出原始信号。

4　仿真验证

为了验证本方法对FBMC信号检测脉冲干扰的有效性，设计了如下几组实验。

2 种算法运行时间比较如图 4 所示，分别取 FBMC 信号长度 M 为 8、16、32、64、128 点（这里对应的 DCT 矩阵阶数与 IFFT/FFT 点数均为 M），对比了文中改进检测算法与 FCME 算法的运行时间，其中 FCME 算法中 k 取 M 的 5%且向上取整。可以看到，改进检测算法所用时间较少。这是因为 FCME 算法初始门限设置取决于当前数据的最小值，而改进的检测算法取决于最低误符号率的训练序列整体平均值，改进算法门限合理且高于 FCME 算法，减少了迭代过程，使得运算时间更短。

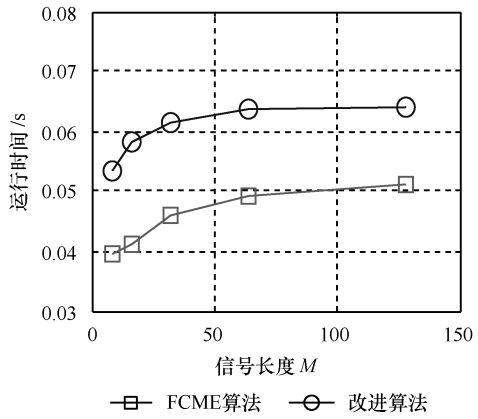


图 4　2 种算法运行时间比较

改进前后的 FCME 检测方法对随机脉冲干扰的检测概率对比如图 5 所示。可以看到，改进前后的检测概率曲线几乎重合，说明两者检测性能几乎一致。这是由于改进算法与 FCME 算法均是基于迭代的检测方法，具有较强的检测性能，同时改进前后只是门限初始值的取值不同，经过迭代运算后，最终更新的门限趋于一致。

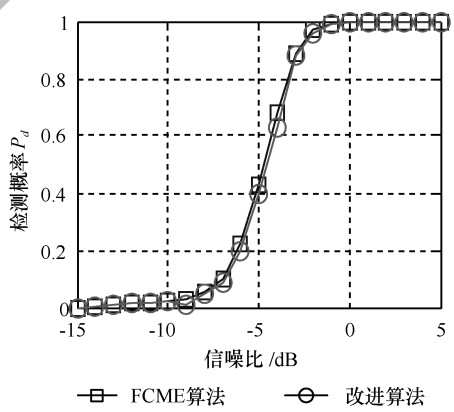


图 5　改进前后 FCME 算法 P_d 比较

改进算法检测概率和虚警概率的关系如图 6 所示。可以看到，当信噪比一定时，P_f 越低，P_d 就越低。这是由于 P_f 决定了门限权值因子 k，较低的 P_f 决定了较高的检测门限，导致 P_d 降低，反之亦然。而当 P_f 恒定时，P_d 与信噪比呈现正相关变化关系。故要保证检测性能，应根据实际情况合理设置 P_f。

人民邮电出版社

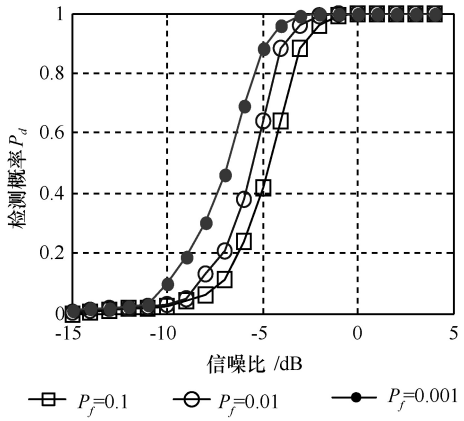


图 6　P_f 与 P_d 关系

FBMC 脉冲干扰处理时，参数设置见表 2。

表 2　仿真参数

参数名称	参数确定
调制方式	QPSK
DCT 矩阵阶数	128
IFFT/FFT 点数	128
原型滤波器	矩形窗
预留子载波数	32
脉冲干扰数	3
均衡方式	迫零均衡 MMSE

分别以误符号率和运行时间为指标将改进干扰抑制方法与门限归零法、门限修剪法进行对比如图 7、图 8 所示。

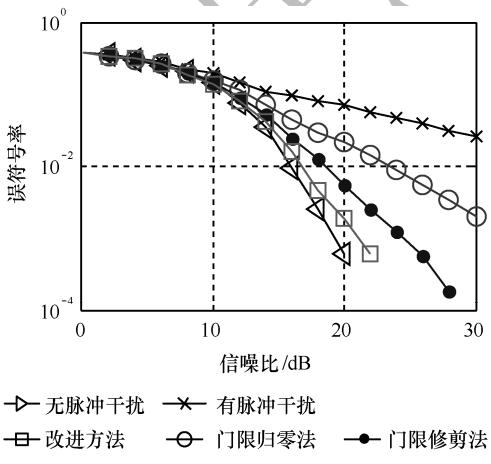


图 7 不同场景下 FBMC 的误符号率

从图 7 可以看到，在误符号率这个指标上，改进方法性能优于门限修剪法和门限归零法，而门限修剪法略优于门限归零法。这是因为门限归零法将干扰点置零，丢失干扰点原有的信息数据，影响了后续解调等信号处理过程；门限修剪法将门限值赋予干扰点，虽然相对门限归零法减少了信号损伤，但仍存在较大误差；而改进方法通过 CS 算法估计干扰点的数据信息，通过作差处理保证了原有信息不被丢失，对干扰点的赋值较门限修剪法更为精确。

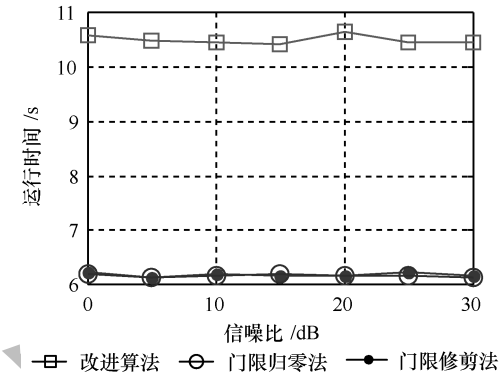


图 8　3 种干扰消除方案的运行时间

从图 8 可以看出在运行时间上，门限归零法和门限修剪法性能几乎一致，都优于改进方法。这是因为门限归零法和修剪法在检测到干扰点后直接对干扰点赋值，方法简单易行，改进方法结合了干扰估计，增加了运行时间。

5　结束语

文中研究了一种基于改进 FCME 检测的 FBMC 时域脉冲干扰抑制方法，可以对时域随机脉冲干扰进行盲检测与消除。该方法在干扰检测时规避了信道估计和导频自适应盲检测，简单可靠，具有检测时间短、准确率高、漏检率低的特点，在保证传统 FCME 检测性能的同时缩短了检测时间；在对干扰点进行处理时则结合了压缩感知与预留子载波技术的优势，使得 FBMC 系统的误符号率降低，保证了 FBMC 传输可靠性，为实际信号处理提供参考。

参考文献

[1] HU W W. SLM-based ACO-OFDM VLC system with low complexity minimum amplitude difference decoder[J]. Electronics Letters, 2018(54): 144-146.

[2] XIAO Y, WANG Z, CAO J, et al. Time-Frequency Domain Encryption With SLM Scheme for Physical-Layer Security in an OFDM-PON System[J]. Journal of Optical Communications and Networking,

2018(10): 46-51.

[3] NISSEL R, SCHWARZ S, RUPP M. Filter bank multicarrier modulation schemes for future mobile communications[J]. IEEE Journal on Selected Areas in Communications, 2017(35): 1768-782.

[4] MESTRE X, KOFIDIS E. Pilot-based channel estimation for FBMC-OQAM systems under strong frequency selectivity[C]// IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). Piscataway: IEEE Press, 2016: 3696-3700.

[5] LIU H, YANG Z, CAO Z. Design perfect reconstruction cosine-modulated filter bank by variable neighborhood search-least-mean-square error[J]. IET Signal Processing, 2012, 6(3): 273-280.

[6] EGHBALI A, JOHANSSON H. On efficient design of high-order filters with applications to filter banks and transmultiplexers with large number of channels[J]. Signal Processing, 2014, 62(5): 1198-1209.

[7] 马伯乐, 朱世强, 孙贵青. 基于特征值的单矢量水听器目标检测算法[J]. 国防科技大学学报, 2019(1): 95-100.

[8] 郭婷莺, 陈永锋, 刘凯. 非合作通信下弱突发信号的双重检测算法[J]. 电讯技术. 2018(11): 1290-1295.

[9] 杨铁军, 司春丽. 基于混合加权的双门限能量协作检测算法研究[J]. 计算机仿真, 2012, 29(7): 179-183.

[10] 吕再兴. 通信对抗中的干扰检测算法研究[D]. 成都: 电子科技大学, 2011.

[11] 徐兵政, 任清华, 孟庆微, 等. 小波变换域通信系统中连续均值剔除算法. 空军工程大学学报（自然科学版）, 2018(4): 93-98.

[12] 关清三. 数字调制解调基础[M]. 北京: 科学出版社, 2002.

[13] 杨静, 余梦佳, 李健波. 改进的 CMFB 多载波通信系统脉冲干扰抑制方法[J]. 重庆邮电大学学报（自然科学版）, 2015, 27(5): 583-588.

[14] BAI H H, WANG A H, ZHANG M M. Compressive sensing for DCT image[C]// 2010 International Conference on Computational Aspects of Social Networks (CASoN), Piscataway: IEEE Press, 2010: 378-381.

[15] 樊明, 魏泽鼎, 郭艺. DSSS 频域干扰检测方法研究[J]. 现代电子技术, 2007, 30(13): 15-17.

[16] 孙志国, 李立金, 郭黎利. 基于 RIE 和 IS-DT-FCME 的直扩系统窄带干扰抑制方法[J]. 电路与系统学报, 2012, 17(1): 111-115.

[17] CHEN J, GIBSON A, ZAFAR J. Cyclostationary spectrum detection in cognitive radios[C]// IET Seminar on Cognitive Radio and Software Defined Radios: Technologies and Techniques. 2008: 1-5.

[18] 王卓刚. 基于改进的 SCR 算法的 NBI 抑制技术研究[D]. 哈尔滨: 哈尔滨工程大学, 2010.

[19] 杨凯, 邹耘, 尹路明. 重叠加窗 FFT 频域抗干扰算法设计[J]. 测绘科学技术学报, 2013, 30(3): 228-231.

人民邮电出版社

基于 *k*-means 算法的 ECC 巨网分割研究

苏鹏，陈曦，孟宇，黎洋
（国网四川省电力公司德阳供电公司，四川 德阳 618000）

摘　要：随着智能电网的飞速发展， 同步数字体系（synchronous digital hierarchy，SDH）网络规模不断扩大。目前嵌入控制通道（embedded control channel，ECC）巨网分割大都基于可靠性、保证性能以及分层、分域管理等原则进行划分，该方法侧重经验积累，较难形成通用的科学划分方法。将巨网分割问题考虑为划分聚类问题，通过结合 *k*-means 聚类算法进行求解，得出最优的子网划分方案。该方法在德阳供电公司 ECC 巨网分割应用中取得较好的成效，成功解决了网元大面积频繁脱管、告警信息丢失等问题。

关键词：SDH；ECC；巨网分割；*k*-means 算法；子网划分

1　引言

随着智能电网的飞速发展，同步数字体系（synchronous digital hierarchy，SDH）网络规模不断扩大。大规模 SDH 网络中单个网关网元管理的网元数目为 100 个以上，传统的 ECC 巨网因依靠经验积累的方式进行划分，出现网元设备大面积脱管等网络管理性能较差的现象，影响了正常生产和业务监控。科学合理的 ECC 子网划分方法，将有效保障 SDH 网络的稳定运行。

2　光传输网络与 ECC 巨网现状

2.1　德阳供电公司光传输网络现状

目前，德阳供电公司华为光传输网络采用传统 SDH 网络与自动交换光网络（automatically switched optical network，ASON）网络混合方式组网。传统 SDH 网络以环形、链型结构组建，ASON 网络以 Mesh 结构组建。光传输网络划分为 3 个层次：以德阳地调为核心节点的核心层，以 220 kV 变电站、各县公司局点为汇聚节点的汇聚层，以 110 kV 及以下变电站为接入节点的接入层。德阳供电公司光传输网络现状如图 1 所示。

核心节点与汇聚节点主要以华为设备 OptiX OSN 3500 为主，接入节点以华为设备 OptiX Metro 1000 为主，部分新建节点采用 OptiX OSN 2500。公司光传输设备详细情况见表 1。

2.2　ECC 巨网现状分析

DCN（data communication network）即数据通信网，它为集中管理网元提供通信通道，从而实现对网元的远程管理与维护。德阳供电公司光传输网络已经发展为包含 118 个网元的巨型网络，网管服务器通过网线连接至德阳地调 1（OptiX OSN 3500）网关网元，从而实现对所有网元设备的管理与维护。德阳供电公司 DCN 组网示意如图 2 所示。

DCN 网络可以划分外部 DCN 和内部 DCN。外部 DCN 实现网管与网关网元之间的通信，德阳供电公司光传输系统的外部 DCN 采用 TCP/IP 协议实现。内部 DCN 实现网关网元与非网关网元网元之间的通信，主要基于 HWECC 协议栈实现。目前，德阳供电公司光传输网络由 118 个网元组成，严重超出 ECC 网络建议的网络规模，是一个典型的 ECC 巨网。

2.3　ECC 巨网存在的隐患

ECC 组网规模过大，存在以下几个隐患。

- 网元脱管
  组网规模过大，使得路由计算量增加，造成路由表收敛时间过长。当网络拓扑结构发生变化时，出现 ECC 振荡，导致网元脱管，严重影响网络的监控、维护与管理。
- ECC 通道拥塞
  若 ECC 网络规模过大，当出现故障而产生大量突发数据时，ECC 通道拥塞，进而出现告警信息时延上报或丢失。
- 主机异常复位
  组网规模过大，使得路由表刷新、接收到的

仅供电力出版社

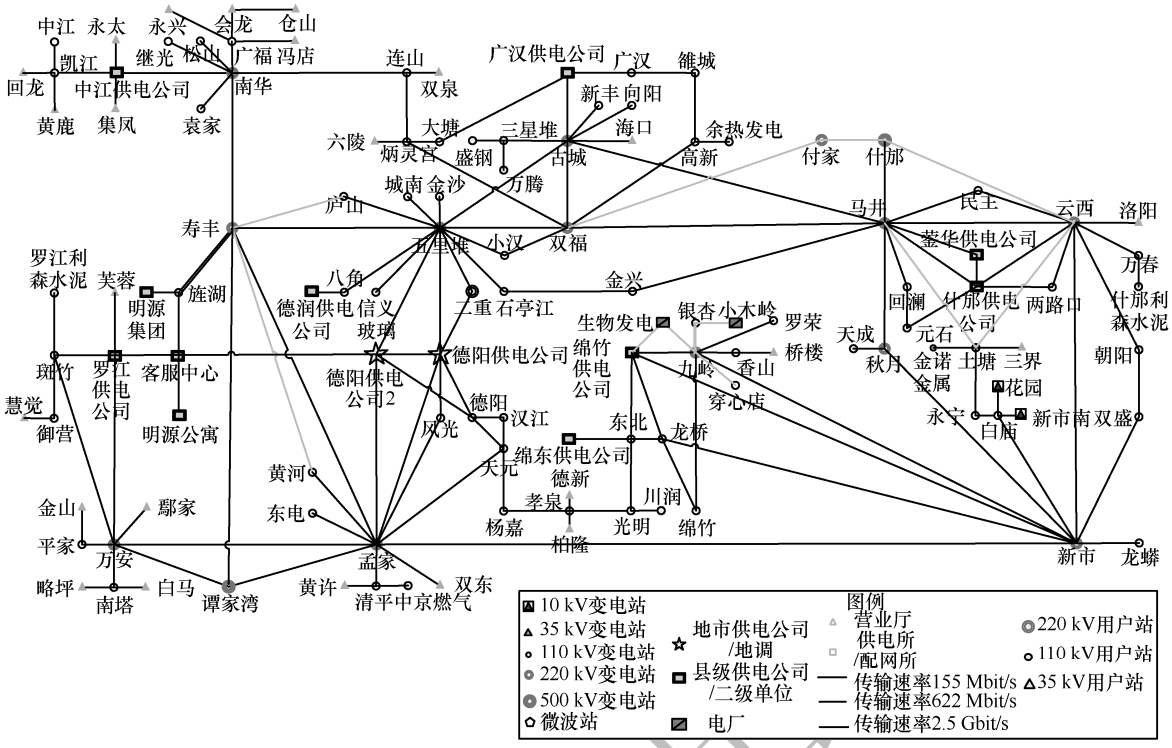


图 1　2018 年德阳供电公司光传输网络拓扑

数据分组流量过大，导致内存溢出，产生的中断过于频繁，进而导致主机异常复位。

表 1　2018 年德阳供电公司华为光传输设备统计

设备类型	数量（台）	用途
OptiX OSN 7500	1	汇聚层
OptiX OSN 3500	25	核心层、汇聚层
OptiX OSN 2500	17	汇聚层、接入层
OptiX Metro 1000（v3）	63	接入层
OptiX Metro 500	12	接入层
合计	118	

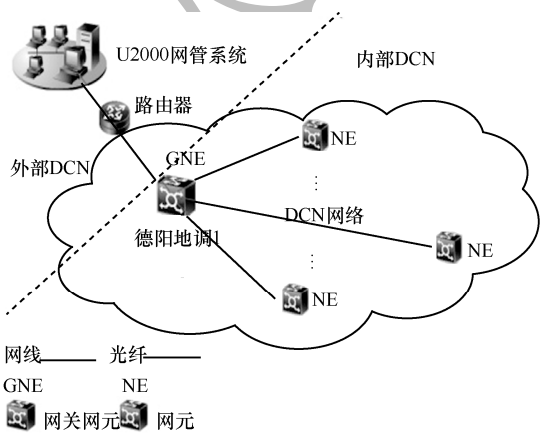


图 2　德阳供电公司 DCN 组网示意

3　ECC 巨网分割方案

对于 ECC 巨网问题，目前通用的方法是将其划分为若干个子网，在各个子网中设置网关网元，从而实现网管对各个子网内网元的管理。为防止子网内 ECC 通道拥塞，各非网关网元与网关网元之间的距离应最近，从而减少非网关网元的 ECC 通信负载。因此，聚类算法是与巨网分割较为契合的方法。

3.1　*k*-means 聚类算法简介

k-means 算法是经典的聚类算法，其时间复杂度与空间复杂度均较低。该算法原理如下：在包含 *n* 个对象的集合 A 中，随机选取 *k* 个对象作为初始的聚类中心，计算其余 *n-k* 个对象与各个聚类中心间的相似值，根据该相似值将 *n-k* 个对象分配到与其最相似的聚类中，然后计算聚类的新质心，重复上述过程，直到约束函数收敛。

3.2　算法设计

ECC 巨网划分问题结合 *k*-means 聚类算法，可描述如下：给定网元个数、各个网元之间的距离（本文的距离定义为路由跳数）以及子网划分个数，划分目标即将各个网元根据就近原则划分到各个子网，使得各个非网关网元至网关网元的距离最短。

令集合 U={A_1, A_2,…, A_n}表示 n 个网元，A_i 表示第 i 个网元，d_{ij} 表示网元 A_i 与 A_j 之间的距离，K 为网元集合 U 需划分的子集（即子网）个数，各个子网聚类中心（即网关网元）集合 S={s_1, s_2, …, s_k}，算法描述如下。

步骤 1 从集合 U 中随机选取 K 个样本作为初始聚类中心，即 S。

步骤 2 针对网元集合 U 中的每个网元 Ai，计算它到 K 个聚类中心的距离 d_{ik}，并将其分到 min（d_{ik}）的聚类中心所对应的类中。

步骤 3 针对每个类别 s_i，重新计算它的聚类中心 $s_i = \frac{1}{|s_i|}\sum_{A \in s_i} A$。

步骤 4 重复步骤 2 及步骤 3 直到 s_i 不变或达到最大迭代次数。

为降低算法收敛时间，考虑选取入口光纤数较多的汇聚节点网元作为初始聚类中心，再根据德阳县级行政区域数目设定 K=6。汇聚节点入路光纤数统计见表 2。

表 2 汇聚节点入路光纤数统计

节点名称	入路光纤数目（个）	所属区域
万安	7	中江
南华	7	罗江
九岭	9	绵竹
新市	9	绵竹
云西	10	什邡
马井	11	什邡
古城	8	广汉
双福	7	广汉
五里堆	15	旌阳
孟家	10	旌阳

按照片区划分原则，选取各片区内光方向密集的站点，S={万安，南华，新市，马井，古城，五里堆}作为初始聚类中心，通过 MATLAB 平台仿真计算，最终子网划分结果如图 3、图 4 所示。具体结果表 3。

3.3 技术方案

对于表 3 中的仿真结果，各个子网均为单网关网元配置，若该网关网元出现故障，将导致该子网内所有网元脱管。为了提升各 ECC 子网的健壮性，考虑在各个 ECC 子网设置备用网关网元。备用网关的选取情况见表 4。

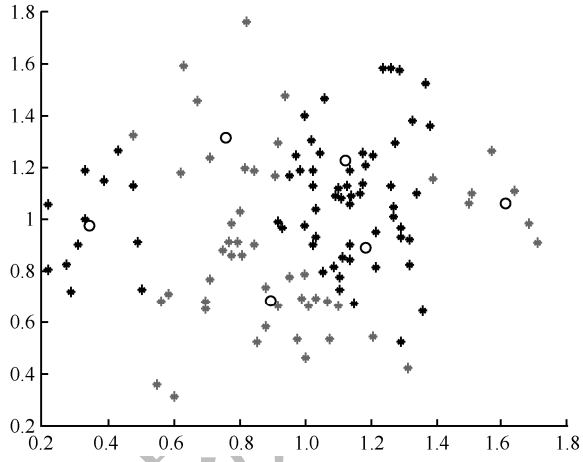


图 3 k-means 算法仿真结果

各个 ECC 子网内的非网关网元在设定其网关网元时，可将其分为两部分，且分别从属不同的网关网元。如此不仅使得两个网关网元互为主备，而且备用网关网元还能承载部分 DCN 通信负荷，使得该子网的 DCN 网络的安全性与通信性能均得到显著提高。ECC 子网划分性能结果对比如图 5 所示。

子网划分后，不仅减少了网元与网关网元之间的平均路由跳数，也减少了末端节点与网关网元之间的路由条数，如图 6 所示。

网关网元与网管服务器之间的通信通过带内 DCN 进行传输，在德阳地调 2 配置到各个子网网关网元共享 Port 的 EVPL（VLAN）业务，且各业务通道需配置 SNCP 保护，从而保证外部 DCN 通道的安全、可靠。

4 结束语

本文提出的新型 ECC 巨网分割方法，基于 k-means 聚类算法对 ECC 子网进行划分，根据路由距离最短原则实现网关网元与该子网内成员的平均路由距离最短，从而实现子网划分结果达到条件最优。通过在德阳供电公司 ECC 巨网分割进行验证，该方法切实有效，成功解决了网络运维中网元大面积脱管、告警信息上报延迟（丢失）等问题，进一步提高了 SDH 网络管理的高效性、实时性。

本文所提出的算法目前还存在两个问题：一是算法中初始条件的设定比较随机；二是聚类相似衡量的

人民邮电出版

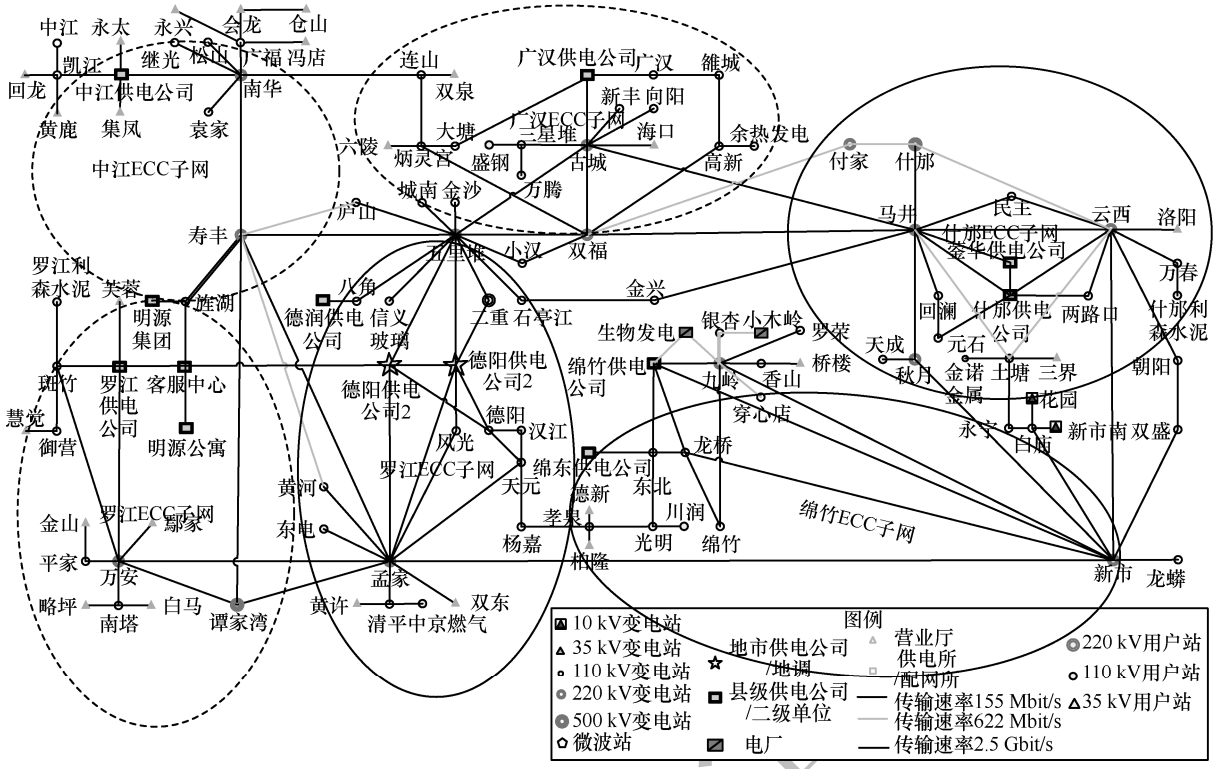


图 4　基于 K-MEANS 算法子网划分

表 3　基于 *k*-means 算法子网划分结果

子网序号	网元数量/个	网关网元	所含网元
1	33	网关网元：五里堆	德阳供电公司，孟家，黄河，黄许，清平，中金燃气，双东，东电，风光，德阳，天元，杨嘉，孝泉，德新，柏隆，寿丰，庐山，明源集团，旌湖，客服中心，明源公寓，秋月，天成，德阳供电公司 2，孟家，二重，德润，八角，城南，金沙，信义玻璃，石亭江，付家
2	14	网关网元：万安	罗江供电公司，谭家湾，万安，芙蓉，斑竹，利森水泥，御营，慧觉，平家，鄢家，金山，南塔，白马，略平
3	16	网关网元：南华	中江供电公司，南华，中江，回龙，黄鹿，凯江，永太，集凤，袁家，松山，继光，广福，永兴，会龙，仓山，冯店
4	17	网关网元：古城	广汉供电公司，古城，双福，双泉，连山，六陵，炳灵宫，大塘，广汉，雒城，高新，新丰，海口，三星堆，向阳，盛钢，小汉
5	20	网关网元：马井	什邡供电公司，什邡，云西，马井，蓥华供电公司，金兴，回澜，元石，金诺金属，土塘 1，土塘 2，三界，两路口，民主，洛阳，朝阳，万春，什邡利森，双盛，永宁
6	18	网关网元：新市	绵竹供电公司，九岭，新市，白庙，龙蟒，龙桥，绵竹，东北，绵竹实业，光明，川润，罗荣，银杏，小木岭，穿心店，香山，桥楼，生物发电

表 4　备用网关网元统计

子网序号	网元数量/个	网关网元
1	34	主用网关网元：德阳供电公司 1；备用网关网元：五里堆
2	14	主用网关网元：万安；备用网关网元：罗江供电公司
3	16	主用网关网元：南华；备用网关网元：中江供电公司
4	19	主用网关网元：古城；备用网关网元：双福
5	20	主用网关网元：马井；备用网关网元：云西
6	20	主用网关网元：新市；备用网关网元：九岭

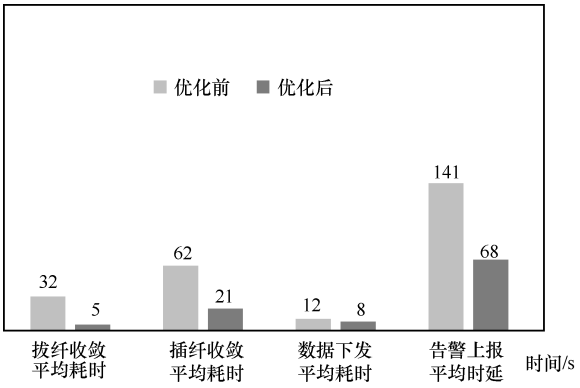


图 5　子网划分性能对比

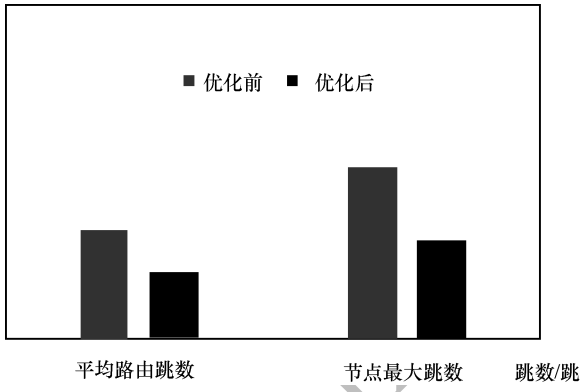


图 6　路由距离优化结果对比

变量选取单一。后续，将从 K 值的选取优化以及综合衡量聚类相似度两个方向进一步深入研究。

参考文献：

[1] 赖玉霞, 刘建平, 杨国兴. 基于遗传算法的 K 均值聚类分析[J]. 计算机工程, 2008(20): 200-202.

[2] 韩萌, 丁剑. 基于交叉验证的 BP 算法的改进与实现[J]. 计算机工程与设计, 2008(14): 3738-3739, 3742.

[3] 唐勇智, 葛洪伟. 基于聚类的 RBF-LBF 串联神经网络学习算法[J]. 计算机应用, 2007(12): 2916-2918.

[4] 陈燕俐, 洪龙, 金达文, 等. 一种简单有效的基于密度的聚类分析算法[J]. 南京邮电学院学报, 2005(4): 24-29.

[5] 谷淑化, 吕维先, 马于涛. 关于数据挖掘中聚类分析算法的比较[J]. 现代计算机(专业版), 2005(3): 26-29.

[6] 陈灿. 大容量骨干光传输网技术及运维案例解析[J]. 电力信息与通信技术, 2013(12): 71-76.

[7] 李擘, 莎沙, 李博, 等. 基于 RPR 的传输 ECC 通信管理方案[J].湖南文理学院学报(自然科学版), 2011(1): 77-80.

[8] 薛珊珊, 李俊, 金涛. 基于 SNMP 的链路层拓扑发现算法[J]. 计算机工程, 2009(14): 120-121, 124.

人民邮电出版社

基于边缘计算的配网状态监测

刘冲，魏鑫，李迪，赵钊
（国网信息通信产业集团北京国电通网络技术有限公司，北京 100070）

摘　要：目前配网状态监测业务快速发展，国网两会重点提出大力发展泛在电力物联网，作为电力重点供电环节的配网，将引入大量智能终端。现阶段大部分配网状态监测数据，都上传至云端进行集中式管理，随着终端数量和数据的不断增加，给云端计算、存储带来很大的挑战。提出了采用边缘计算框架，在智能终端中集成边缘计算网关，应用于配网状态监测，实现本地化的数据采集、存储和分析。

关键词：泛在电力物联网；边缘计算；配电网；状态监测

1　引言

随着我国智能电网建设的日趋成熟，大数据和物联网技术深入发展，广泛应用到配网日常监测和维护中，配网监测终端数量和采集数据急剧增加，给云数据中心的网络带宽、云存储和计算能力带来很大挑战[1]。由于缺少有针对性的故障处理策略、运维人员个人素质不同等问题[2]，无法有效判断安全隐患、发现运行问题和处理问题不及时给配网安全运行带来很大的影响[3]。同时受制于网络运行情况，当网络延时过高或无网络时无法及时发现和处理问题和故障点，影响配网安全运行。

边缘计算将网络边缘上的计算、存储等资源进行有机融合，按就近服务原则对网络边缘节点任务请求及时响应并有效处理[4]。边缘计算技术发展受到广泛关注，通过在网络边缘进行处理，降低云端核心节点的压力，这种工作模式，是未来大规模终端实现自动需求响应的理想解决方案[5]。

基于边缘计算在配网状态监测的研究和应用，以配电室状态为例，利用边缘计算的前置设备，有效解决物联网与云计算结合引起的终端节点请求延时、云服务存储和计算负担过重、网络传输带宽压力过大等问题。同时增加物联网传感器，全面采集配网运行中的动力环境、电气参数等数据，实现对配电室运行情况的全面掌控，提高本地化问题和故障及时发现、及时上报、及时处理的能力[6]。

2　边缘计算

2.1　边缘计算的发展

边缘计算是指在物理上靠近数据源头的网络边缘侧，融合网络、计算、存储、应用核心能力的开放平台，就近提供边缘智能服务的计算模式[7]。满足行业数字化在敏捷联接、实时业务、数据优化、应用智能、安全与隐私保护等方面的关键需求[8]。2016 年 11 月 30 日，由华为技术有限公司、中国科学院沈阳自动化研究所、中国信息通信研究院、英特尔公司、ARM 和软通动力信息技术（集团）有限公司联合倡议发起的边缘计算联盟（edge computing consortium，ECC）在北京正式成立。该联盟旨在搭建边缘计算产业合作平台，推动 OT（operation technology）和 ICT（information and communication technology）产业开放协作，孵化行业应用最佳实践，促进边缘计算产业健康与可持续发展。国家电网在 2019 年度工作会议上指出，充分应用移动互联、人工智能等现代信息技术和先进通信技术，打造状态全面感知、信息高效处理、应用便捷灵活的泛在电力物联网，边缘计算的应用在泛在电力物联网建设中占据十分重要的地位[9]。

2.2　边缘计算优点

（1）实时性

随着物联网时代的到来，相关传感器的使用不断增多，数据量传输呈几何递增，对数据的快速传输和快速处理提出了更高的要求。传统的数据传输和处理方式中，数据在到达目的地之前通过本地网络连接路

人民邮电出版社

由器，会增加 10～65 ms 的延时；数据到达云端后，由于大量数据需要云端处理，并将处理结果反馈到数据采集端，使数据采集端需要更多的相应时间。边缘计算通过将处理源与数据源缩短物理距离，减少延时，边缘计算数据中心针对数据源进行定制化设定，能够快速完成数据分析和处理，整个数据传输和处理过程能够提高至微秒级，有效解决数据延时、减少云端运算负荷。

（2）安全性

物联网设备的激增，增加了网络攻击的选择性和概率。对于传统的云计算架构来讲，也提供了一些重要的安全措施，但其本质是集中式的，使它容易受到分布式拒绝服务和断电的影响。物联网设备的每个节点都可以被用作网络攻击的入口，从单个软件入侵感染网络。边缘计算是在接近数据侧进行数据的采集、存储和分析，这种只服务于数据侧的边缘计算很难受到任何中断的影响，其分布式的架构特性更容易实现安全协议，可以在不关闭整个网络的情况下封锁受损部分。

传统的数据处理是将用户的一切数据上传至云端处理，再将处理结果反馈到控制中心或采集设备端，在数据传输的整个过程中都有数据泄露的风险。边缘计算是将大部分数据在本地实现存储和处理，减少传输过程中存在的泄露风险。

（3）可扩展性

边缘计算数据中心可以针对云端大数据和用户需求，增加相关传感器和采集设备，实现对数据的补充。云端利用大数据分析结果，通过自主学习能力，完成新增数据和动态数据的处理逻辑更新，并将新的程序传输至边缘计算数据中心，实现远程升级。这种利用物联网传感器、边缘计算数据中心、云端数据中心的组合扩展能力，可以有效降低成本，同时提高数据处理能力。

（4）可靠性

由于物联网设备和边缘数据中心更靠近终端用户侧，所以网络问题影响本地前置设备的难度很大。即使在附近数据中心终端的情况下，物联网设备也可以继续有效运行。由于各边缘计算中心是独立运行的，一个边缘计算中心出现故障，不会影响其他的在线运行设备，确保用户保持对所需产品和信息的访问。

2.3 边缘计算架构

边缘计算架构在每层提供模型化的开放接口，实现了架构的全层次开放，如图 1 所示。通过纵向管理服务、数据全生命周期服务、安全服务，实现业务的全流程、全生命周期的智能服务。通过开发服务框架和部署运营服务框架在统一的模型驱动服务框架下，实现开发和部署的智能协同，实现软件开发接口的一致性和部署运营的自动化。智能业务编排通过业务 Fabric 定义端到端业务流，实现业务敏捷。联接计算 Fabric 实现架构极简，简化业务边缘智能分布式架构，实现基础设施部署运营自动化和可视化，支撑边缘计算资源服务与行业业务需求的智能协同。

3 边缘计算在配网状态监测的应用

边缘计算指在靠近物或数据源头的网络边缘侧，融合网络、计算、存储、应用核心能力的开放平台，

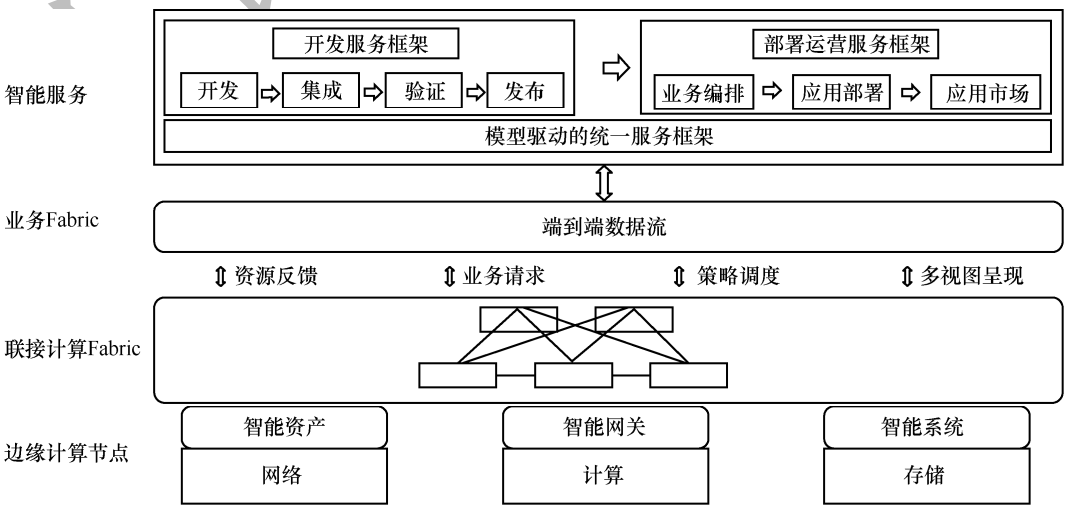


图 1　边缘计算架构

就近提供边缘智能服务，满足行业数字化在敏捷连接、实时业务、数据优化、应用智能、安全与隐私保护等方面的关键需求。具备边缘计算能力的前置设备，采用自主研发芯片，基于开放边缘计算架构，利用网络远程连接，灵活升级、增加功能和提升识别率，使配网运维具备更强的资源配置能力和更快的需求响应速度。

3.1 边缘计算前置设备

本设备采用双核 CPU，具有低功耗、处理速度快、安全等特点，适配工业级场景，适应配网复杂运行环境，同时集成国网安全芯片，支持双通道身份认证和数据加密传输，满足主站与终端交互协议的转换和安全防护的要求。可提供多种业务接口，如 RJ45、RS485、RS433、LoRa 等，如图 2 所示。

本设备功能支持智能环网柜运行监控、高压开关柜带点显示、电流电压等符合运行监控、母线测温检测、电缆测温监控、环境监控、安防监控、采暖通风、灯光、风机、除湿机控制等功能，并可以实时监测 SF_6、H_2S、O_3 等有害气体和门禁的功能。可实现本地化图像和数据采集、存储和处理，大大缩短数据传输和处理时间，提高设备处理效率。

3.2 业务架构

采用边缘计算前端设备实时监测配网运行，集成采集层各物联网传感器，通过本地边缘计算，完成数据的采集、存储、分析和处理，实现视频监控、环境监测、设备在线监测、安全防范、智能控制、智能联动和能源管理等功能，业务架构如图 3 所示。



图 2 边缘计算前置设备

3.3 功能实现

（1）视频监控

视频监控通过安装摄像头实现实时监控一次、二次设备运行状态和运行环境以及场地、蓄电池室、继保室、主变的运行情况。摄像头将模拟视频、音频信号，通过压缩编码后上传至边缘计算前置设备，前置设备将采集数据进行存储，自动识别断路器状态、隔离开关状态、接地刀闸状态、PT、CT 外观状态等电气设备运行状态，还可以进行入侵监视以及工作人员佩戴安全帽、穿着工作服等安全规范是否符合标准。

（2）环境监测

通过安装温/湿度传感器、微气象设备、水浸探针等，实时监测配电室内环境情况。边缘计算前置设备采集相关环境传感器设备，工作人员可以通过前置设备对配电室环境进行告警设置，设定正常运行范围，



图 3 业务架构

当采集数据处于正常范围以外时，前置设备通过边缘计算自动判断告警类型，通知工作人员，并采取相应的措施。

（3）设备在线监测

通过安装 CT、PT、电力传感器等设备，对绝缘油中溶解气体、放电量、放电电位、变压器铁心接地电流等参数的实时监测，边缘计算前置设备通过上述参数的模数转换、分析，显示目前电气设备运行状态，并向工作人员和云端推送显示信息和告警信息。

（4）安全防范

通过安装红外对射、电子围栏、红外双鉴、门禁等设备，实现配电室的安全防范功能。当有异物或人员入侵时，边缘计算前置设备第一时间检测入侵位置，锁定入侵区域，通知工作人员，并启动智能联动功能，进行语音警告，实现对入侵人员的实时视频跟踪。

（5）智能控制

工作人员可以通过云端，远程向边缘计算前置设备下发控制命令，实现对灯光、风机、水泵、门禁、空调等设备的控制，并将上述设备的运行状态上传至云端。

（6）智能联动

边缘计算前置设备能够对配电室内环境、电气运行参数进行实时监测，并不间断的对采集数据进行分析和对比，比如检测到人员入侵时，启动视频跟踪和声光告警；检测到水位超过告警值时，启动水泵进行抽水；检测到温度越过告警温度时，启动空调进行降温等。

（7）能源管理

边缘计算前置设备通过智能电表等设备，实现电气参数趋势曲线分析，通过梳理用电类型、用电区域、用电部门并与公共建筑管理商业模式、运营模式、温度、人流量等数据相结合，做到智能识别“异常负荷”、“恶性负荷”、“偷、窃、漏电”等问题。

4 结束语

边缘计算具有分布式计算的特征，支持分布式计算与存储、实现分布式资源的动态调整与统一管理，同时更靠近终端侧，具有广阔的应用前景。配网状态在线监测方面，利用边缘计算能力，减少数据通信压力、降低云端运算和存储负荷，同时可以提高事件处理的响应速度。与传统的在线监测的数据孤岛形式相比，具备边缘计算能力的在线监测技术，能够促进数据的共享和融合、与云端实现边云协同、全方位立体的实现配网状态实时监测。

参考文献：

[1] 夏星.智能配网运维一体化建设[J].科技创新与应用，2019(13): 191-192.

[2] 阿布都艾尼·阿布都克力木. 10 kV 配网运维现状和管理模式的思考[J]. 中国新通信, 2019, 21(4): 145.

[3] 邹宇, 谢振俊, 陈恒龙, 等. 面向配网运行状态在线监测的 VCO 设计[J]. 信息技术, 2019, 43(4): 47-51.

[4] 彭晓晖, 徐志伟. 基于边缘计算的物端系统挑战与愿景[EB]. 中兴通讯技术, 2019.

[5] 刘铎, 杨涓, 谭玉娟. 边缘存储的发展现状与挑战[EB]. 中兴通讯技术, 2019.

[6] 黄宸希. 配网故障定位在线监测管理系统的设计与实现[D]. 北京：北京交通大学, 2017.

[7] 朱友康, 乐光学, 杨晓慧, 等. 边缘计算迁移研究综述[J]. 电信科学, 2019(4): 74-94.

[8] 丁春涛, 曹建农, 杨磊, 等. 边缘计算综述: 应用、现状及挑战[J]. 中兴通讯技术, 2019(3): 2-7.

[9] 高志鹏, 尧聪聪, 肖楷乐. 移动边缘计算: 架构、应用和挑战[J]. 中兴通讯技术, 2019(3): 23-30.

人民邮电出版社

基于边缘计算的智慧用电生态场景

张林锋，欧阳述嘉，贾涛
（国家电网有限公司信息通信分公司，北京 100761）

摘　要：随着社会发展的不断深入，新时代特征的现代化、智能化和智慧化已逐渐成为人们热议的焦点话题。电力作为支撑这“三化”的关键元素，扮演着不可替代的角色，已渗透到生产生活的方方面面。近些年来，由电气故障引发的火灾起数逐年攀升，严重威胁到人们的生产和生活安全。基于边缘计算的智慧用电技术及平台，有效地解决了传统电气火灾监测系统技术落后、高误报率、时延长等问题，具有十分广泛的应用基础和前景。

关键字：智慧化；智慧用电；电气火灾；监测系统；边缘计算

1　引言

电力的使用涉及每一个行业、每个家庭、每一个人，对于用电安全和用电效率问题引起了社会的极大的关注。根据公安部消防局火灾统计年鉴，十几年来，我国平均每年由于电气故障引发的火灾起数，占总火灾起数的比例在 30%左右，占重特大火灾起数的比例在 40%～50%[1]，电气火灾情况严峻。而欧、美、日等发达国家和地区，相同的数据基本为 4%～12%。我国的电气火灾形势比发达国家和地区要严峻。2018 年，我国《建筑设计防火规范》（GB50016-2018）建议安装剩余电流火灾报警装置，并被要求强制安装在老年人服务设施。但是，电气设备质量参差不齐、用电环境复杂，传统的剩余电流火灾技术存在的问题。

（1）传统剩余电流火灾报警系统无法排除容感性干扰和谐波类干扰，据电气协会公布的最新调查，传统的剩余电流火灾技术误报率达到 53%，同时还有 8%的漏报率。导致上线的剩余电流火灾报警系统闲置弃用率超过 50%，无法达到预期效果。

（2）传统剩余电流火灾报警系统预警周期短，不能在早期发现电气火灾隐患。早期隐患具有信号微弱、变化缓慢、数据量大的特征，隐患数值一般远低于报警阈值，传统技术对早期隐患“视而不见”。

（3）传统剩余电流火灾报警系统缺乏对电气线路和用电设备绝缘水平的绝缘水平监测手段。据统计，我国现阶段绝大部分电气火灾都是长期使用过程中电气老化导致，电气老化也是形成易发热的阻性剩余电流的主要原因。

目前，我国能源使用总量跃居世界前列，我国发电还是以燃煤为主，对大气污染形成很大压力，因此开展节能降耗是全社会普遍关注的话题。此外，在经济下行压力增加，中国企业转型大背景下，如何降低企业成本（特别是用能成本）、提升能源使用效率，已成为企业重点关注对象，其中的关键是具有完善的数据采集与监测体系。缺乏各行各业有效、高效、用能大数据平台，开展综合能源服务缺乏有力支撑工具。

综上，迫切建立低成本高效的智慧用电平台，为提高全社会用电安全，提高用电效率。

2　基于边缘计算的智慧用电技术

基于边缘计算的电气安全监测和大数据分析，在用户用电设备终端部署智慧电气终端，采用用电设备开关电压、电流、温湿度等参数，在边缘侧进行计算，降低对云平台计算力的要求，减少网络延时，如图 1 所示。边缘计算保留底层模拟信号的真实性，如剩余电流的矢量特征如果直接上传会部分丢失，在边缘侧做数据分析是对策。海量数据边缘侧运算，只提取特征值上传，降低对带宽的要求；传统技术放弃全过程的参数分析，只周期性上传暂态值，解决传统技术精度差问题。新技术采用全时域动态分析（FTDA）、基于底层终端的多层次大数据处理、大数据显微功能模块（big data micro）等创新技术，构成了全新的、基于传感器硬件层的边缘计算型数据处理模型。

人民邮电出版社

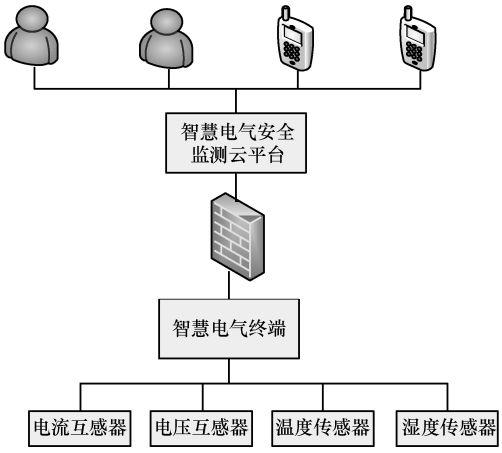


图 1 基于边缘计算的电气安全监测

相比传统技术，基于边缘计算的电气安全系统主要特点包括以下。

（1）实现了电气火灾监测技术从“报警”到“预警”的飞跃。精度实现 100 万至 93 亿倍的提升，将预警的时间提前量从“秒”级提升到“月”级；误报率从 53%以上降为 0，彻底解决了传统电气火灾报警设备误报率过高、闲置弃用率等问题。

（2）除传统剩余电流监测功能外，新增“电气绝缘和老化在线监测”功能，实现电气绝缘和老化全时、量化描述，突破了长久以来难以对电气设备绝缘水平实时监测的技术难题。

（3）新系统集成了能耗监测功能，能实时监测用户用能数据，为用户实施节能减排提供了有效工具，同时避免了用户的重复投资。

3 智慧用电生态场景

智慧用电安全监控平台是智慧城市[3]的核心之一，其应用场景十分广阔，可广泛应用于智慧小区、智慧工业园区等安全用电场景。为智慧用电安全监控平台架构如图 2 所示。用户侧电表、断路器终端以及线路监测采集信息经边缘代理做初步数据处理，将有效数据发送至监控平台。完成数据的采集、分析预处理、传输、存储及应用，最终得到有效数据经过平台做展示分析。

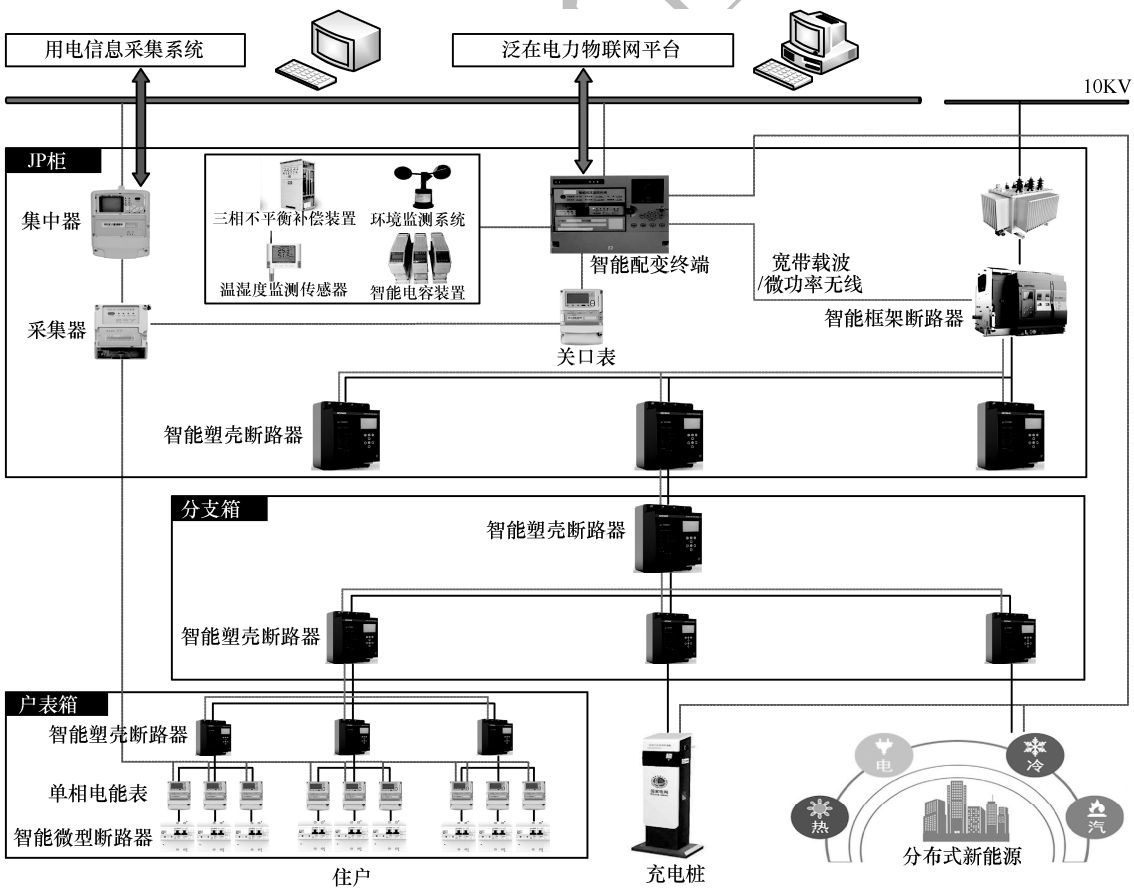


图 2　智慧用电安全监控平台架构

4 智慧用电应用案例

2016 年在省级某文物总店安装监测预警系统后，发现严重电气绝缘隐患，省文物局拨专款进行电气线路改造后电气绝缘状况良好。该文物总店的六楼（文物库房）一个非工作日（2018 年 5 月 1 日）的监测预警云平台展示情况如图 3 所示，可以看到一个与绝缘隐患高度相关的小时级过程参数在凌晨 4 点和 7 点明显有几倍的突变。后经过现场排查，该楼层库房存在鼠患，室内裸露的电缆成为“跑道”，凌晨这些时间段数据突变与老鼠的生物钟特征相关。



图 3 某文物店电气监测预警云平台

通过实际运行，新一代电气安全（含电气火灾超前预警物联网系统）不仅能够清楚展示监测对象是否存在相关安全隐患，也能清楚展示隐患处于极早期、早期或中/后期等具体阶段；该系统已经能够具体识别相关隐患是产生在电气线路或具体用电设备，并进一步向隐患行为识别、设备行为识别等人工智能方向发展。

5 结束语

电力是未来支撑智慧城市运行的重要因素，而用电安全则是保障，基于边缘计算的电气安全监测系统通过精准全面的大数据分析和低延时的网络传输，实现了传统火灾监测系统无法实现的精确“预警”，有效地解决了传统电气火灾监测系统技术落后、高误报率、时延长等问题，具有十分广泛的应用基础和前景。

参考文献:

[1] 吴荡儒, 康文彬. 智慧用电安全管理服务平台[J]. 新品导览, 201(1): 132-134.

[2] 陆云杰. 基于大数据的智慧用电监管平台的设计与研究[D]. 杭州: 浙江工业大学, 2017.

[3] 孙厚涛. 智能用电技术在智慧城市中的应用[J]. 电气自动化, 2019, 41(4): 1-4.

人民邮电出版社

基于大数据分析的核电工程预见性设备管理系统研发与应用

腾飞，黄光明，侯新宝，黎艺华，李霞
（中广核工程有限公司，广东 深圳 518031）

摘　要：对核电设备管理全过程产生的海量数据进行系统性分析，并以对应的数学模型进行归纳，以此对批量化建设的核电机组进行预见性设备管理，提前识别、预判设备管理风险点，并对这些风险进行针对性的提醒与预防。中广核工程有限公司在 4 个核电项目 16 台机组中的应用结果表明，该方法能够有效提高后续机组建设过程中设备问题的处理效率，使得同类型机组建设过程中，设备管理在质量、成本、效率、进度等方面的提升具有可预见、可评价、可控制的系统化手段。

关键词：大数据；设备管理；预见性；核电

1　引言

在核电工程建设中，设备采购是核电厂建设成本中最重要的部分，其投资占比在 40%以上；同时，在核电站建设和运行的整个寿命周期内，设备质量、可靠性及寿命管理是核电管理的核心对象和核安全保障的关键。

根据统计，CPR1000 型机组单台机组涉及的设备数量超过 8 万台（套），产生和处理的各类设备问题高达 40 万条，这些问题对核电建设周期、关键节点进度和安全运行均带来不同程度的影响。

本文通过使用大数据方法，对核电工程阶段设备管理数据进行建模分析，得出指导后续机组设备管理的一般规律，把应用这些规律开展的带有预防性质的准备工作称为预见性设备管理。

2　核电工程阶段设备管理现状与需求

核电行业安全要求极高，单台核电机组设备的总量极大，类型很多。核电工程设备管理复杂程度远远超出一般工程项目。在复杂背景下，必须找到设备管理的趋势和规律，并对其加以利用，才能有效降低成本，减小进度波动的影响，提高设备的管理成效。

3　核电设备管理类数据特征与分析方法

3.1　数据准备的方法

（1）明确要解决的问题[1]

对问题的界定始于提出关键性的问题，明确目标和需求是数据分析的关键所在。数据分析问题的种类一般分为推理性问题、预测性问题、描述性问题、探索性问题、因果问题、相关性问题。

（2）数据准备

数据准备是关于数据获取、数据清洗、数据标准化并实现将数据转化为最优数据集过程的环节。本文在系统平台开发时主要使用 Openrefine 工具进行数据处理。

（3）预测建模

预测建模是采用数据分析的方法生成或者选择一个统计模型，目的在于使模型输出的可能结果成为最优预测值。本文及所介绍的系统，输出的数据模型分为 3 个种类：分类结果、数值型结果、描述性建模。

（4）结果可视化

结果可视化是分析处理过程的最后环节，根据核电常用报表规范了多种数据的展示方法。这些展示方法被应用于建设设备管理系统中。

3.2　数据的来源

核电设备管理数据的来源见表 1。

这些数据涵盖了开源数据、文本文件、Excel 文件、SQL 数据库、NoSQL 数据库、多媒体数据、网页检索等多种数据形式。这些数据分别存储于中国广核集团位于深圳的数据大楼中，此前一直没有统一的检索端口。

3.3　数据的清洗

数据清洗是对数据集中错误、不精确、不完整、格式错误的一级重复的数据进行修正、移除的过程。

人民邮电出版社

表 1　核电设备管理数据来源

表格类型	产生阶段
GVN 单	物资到场验收阶段的验收问题单
NCR	设备制造、开箱验收、安装阶段的不符合项问题单
UES	设备调试、试运行阶段的意外事件问题单
DCR	设备/系统设计、调试阶段的设计澄清类问题单
CR	设备安装、调试阶段的各类问题清单
EESR 尾项	设备在安装竣工验收阶段的偏差问题记录
BHO 尾项	设备厂房移交过程中的偏差问题记录单
FW 尾项	系统安装完工阶段遗留问题记录单
DCK	设备移交运行阶段质保期内设计变更记录单
DCL	设备移交运行阶段质保期内工程生产联络单
经验反馈系统	设备在全周期内的已发生、已解决问题的过程记录
人力配备 A（工程人员）	工程建造阶段全周期内工程方人力投入情况记录
人力配备 B（供应商代表）	工程建造阶段全周期内制造厂人员投入人力情况记录

通过数据清洗，提高数据本身的质量，从而提高数据分析的准确性。为了避免数据集中存在脏数据，需要对数据进行如下特征检查：正确性、完整性、精确性、一致性、统一性。在实际工作中，使用了简单的统计学检验方法及 python 工具进行文本解析，剔除了重复项和杂质[2]。

3.4　数学建模及结果输出

描述性需求模型见表 2。

输出类别对应使用的数据加工算法及所引用的数据源见表 3。

3.4.1　标准双堆全周期数据期望模型

本模型使用了 16 台机组全部问题量数据累加折算的标准双堆全周期（“CFT-45M”至“商运+12M”）数据量趋势图，如图 1 和图 2 所示。该模型作为“标尺”，用于衡量实际工程建设过程中，设备管理情况与理论工期的偏差。模型算法亦可作为核电设备管理中每一类数据单独监控的模型算法。

表 2　描述性需求模型

输入	加工	输出类别
核电设备管理数据	分析算法	（1）预判可能会发生的故障及设备可能发生的故障类型，提前做好预检查
		（2）根据可能会发生故障的设备及故障类型，提前采购长周期备件
		（3）预判下游施工安装需求计划、制造厂排产时间、设备质保维护周期、库存指数、运输资源情况，制定合理的设备制造开工时间
		（4）根据设计变更、安装进度变更、调试意外时间对进度的综合影响，调整设备制造资源的分配策略，使供货适应现场变化
		（5）根据现场各类设备问题数据，评价设备管理健康情况，预判设备管理风险趋势及对后续工程大节点影响
		（6）建立标准的设备管理方法，使缺乏经验的工程技术人员在计算机系统的辅助下进行决策
		（7）建立经验数据反馈方法，滚动更新计算机系统的人工智能学习数据库，为本计算机系统的学习扩充资源
		（8）建议标准机组的设备管理类人力需求模型，含考勤 A 和考勤 B

昆明电力出版社

表 3　输出类别对应的数据加工算法工具及所引用的数据源

输出类别	数据加工算法	引用数据源
A/B/G	概率统计&随机游走算法中的无规则分类算法	UES/NCR/CR/DCR/各类尾项
C/D	自然语言工具包	各类尾项、经验反馈、变更
E	朴素贝叶斯算法&权重分析	UES/NCR/CR/DCR/各类尾项、经验反馈、变更
F/H	D3.js 可视化数据模型	UES/NCR/CR/DCR/DCK/DCL、各类尾项、经验反馈、变更、工程图片、考勤 A、考勤 B

图 1 和图 2 中的数据量均值能够同时兼顾进度控制、仓储压力、人力投入、供货匹配度、安装负荷、调试负荷等多方需求的最优解。根据进一步分析，放任数据向上限偏离，会明显影响机组的建造进度；如果将数据进一步向均值下方调整，所付出的成本和投入的资源会导致机组建设成本增加[3]。

3.4.2　标准双堆机组全周期设备类问题颗粒度细化方法模型

本文使用“TOP 排序原则”来对数据量最大一些系统或设备进行统计。

（1）对标准双堆问题发生数量统计 Top10，求平均数后排序。找到了机组设备问题出现最多的前 10

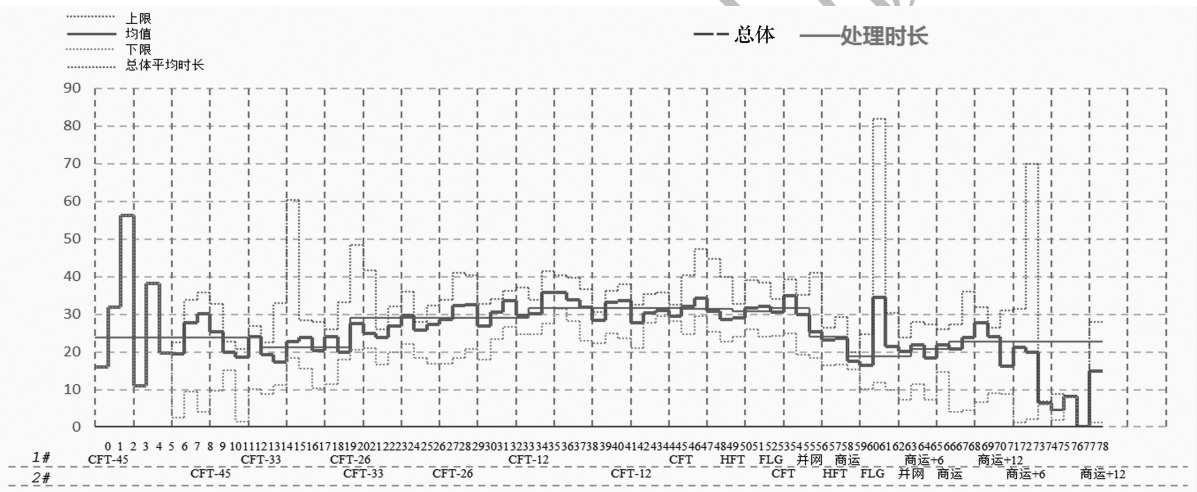


图 1　标准双堆设备问题数量期望分布

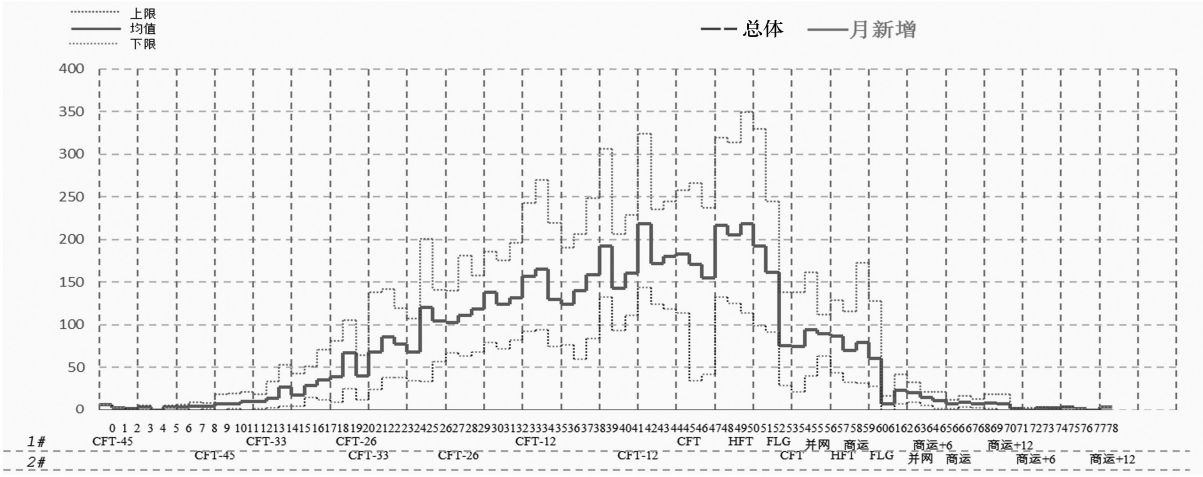


图 2　标准双堆设备问题处理效率期望分布

个系统或设备类别，见表 4。

（2）对 Top10 排序，进行全周期时间节点分布分析，得出设备问题最多的 Top10 系统或设备发生问题的时间节点分布情况，见表 5。

表 4　标准双堆 Top10 系统/设备的故障数量排序

设备类别	故障数量/个
汽轮机	1 546
压力仪表	779
消防	653
核岛容器	587
核岛吊车	515
封闭母线	498
压力容器	477
小三箱	264
照明/通信系统	237
大宗材料	186

（3）对单一系统的单一节点问题单数量进行细化分类分析，可以找到某一工艺系统或设备的问题类别，如图 3 所示。

（4）设备管理健康指数模型

a_{11} 列为机组的 m 个系统中 GVN（差异项）单的数量，a_{21} 列为 m 个系统的 NCR 量，a_{115} 列代表人力配备数据 $\boldsymbol{B}$。矩阵 $\boldsymbol{A}$ 表示非权重分配下的单机组健康指数，该指数配以节点权重矩阵 $\boldsymbol{B}$，即可计算任意节点时单机组在系统权重条件下的实时健康指数。

$$\boldsymbol{A}=\begin{vmatrix} a_{11} & a_{12} & a_{115} \\ a_{21} & a_{22} & a_{215} \\ a_{31} & a_{32} & a_{315} \\ \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & a_{m15} \end{vmatrix} \quad B=\begin{vmatrix} x_{11} & x_{12} & x_{115} \\ x_{21} & x_{22} & x_{215} \\ x_{31} & x_{32} & x_{315} \\ \vdots & \vdots & \vdots \\ x_{m1} & x_{m2} & x_{m15} \end{vmatrix}$$

根据核电工程不同节点，代入不同的系统及权重数据，可以计算出当前节点下健康指数。本文计算的

表 5　双堆机组 Top10 设备问题时间节点与问题数量统计

设备采购合同	-45	-33	-26	-12	冷试	热试	装料	并网	商运	"+6"	"+12"	之后	总计
汽轮机		3	16	271	826	259	160	163	132	1	2		1 833
柴油机			8	222	556	151	132	47	39	1	5	3	1 164
压力仪表		7	10	159	260	106	98	29	37	3			709
VELAN 核岛阀门		2	19	150	210	94	120	23	38	6	2	1	665
消防		3	6	167	247	74		31	25				626
装卸料机		9	41	193	208	61	53	20	9				594
核岛容器	26	54	81	173	143	25	22	9	1	1	2		537
温度仪表		3	151	195	64	75	23	17	2	1			531
核岛吊车		39	99	258	58	17	32	10	9	1			523
常规岛主给水泵				53	207	124	63	17	36				500

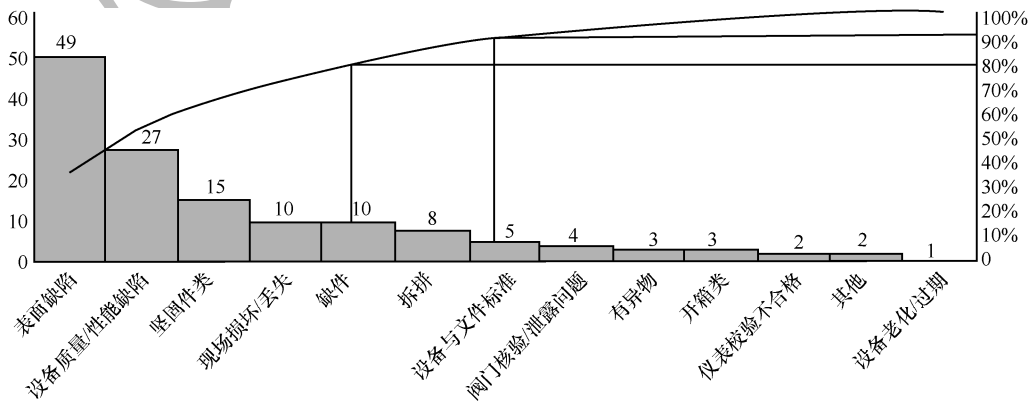


图 3　核岛主泵质量分析

人民邮电出版社

全部 24 台在建及已建成机组设备健康指数曲线如图 4 所示。

4 基于大数据的预见性设备管理平台研发及应用

使用上述算法/模型对数据进行分类梳理后，本文开发了设备管理平台。

4.1 设备管理平台的原理与构架

设备管理平台的架构分为数据的收集与录入、数据加工、AI 算法处理数据结果及 AI 算法生成并推送数据，具体见表 6。

4.2 应用场景及功能介绍

当前系统已经实现的功能简要介绍如下。

- 按照设定的提醒算法，系统能够在节点到来之前的特定时间段，提醒负责某个工艺系统或设备的工程师，预检查哪些环节，注意哪些风险，核实哪些信息，落实哪些经验反馈。
- 实现全平台的实时的集中数据监控，对全部在建核电工程的设备，进行全周期全范围的数据监控。并参照标准双堆模型，对不同层级的人员发出有针对性的辅助工作信息，例如可以提醒设备经理目前 NCR 处理效率的偏差，并依据系统、设备的权重，给出处理优先级和关注事项。
- 基于细化颗粒度模型算法，能够给出从全部在建项目总数据到个人数据统计。
- 其他辅助统计与演示功能。

4.3 应用效果的评价

自本系统于 2018 年 5 月上线试运行以来，以当前收集到的效率维度进行评价，得出初步评价效果如下。设备管理类问题单处理效率较系统运行前整体提升了 23.3%；设备管理类人力实际投入量，较标准双堆机组人力投入量下降 33.3%；设备类经验反馈落实数量达到 1 100 余项，同类设备问题重发率下降 71%。

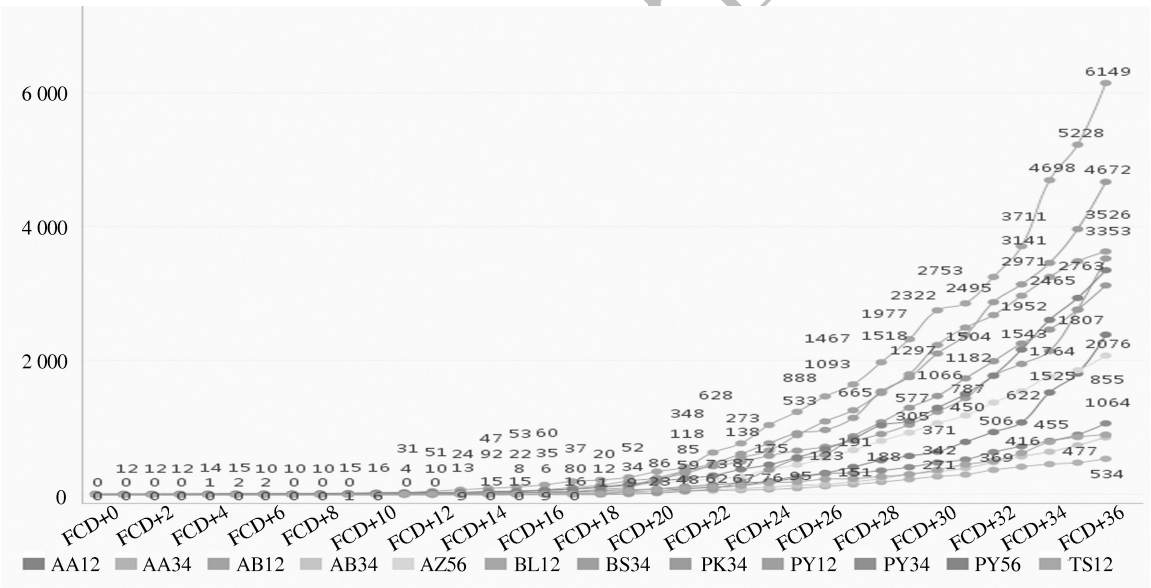


图 4 24 台机组设备健康指数曲线

表 6 设备管理平台的架构

数据录入/收集		安装、配置、授权和访问控制				
数据加工		数据仓库		数据流处理		数据训练库
输出值与标准数据对比	自我	分布式数据库		分布式计算框架		
导入专家系统	学习	CASP	IMSESP	IMSCA	IMSSU	PRAN2.0
	算法	（设计管理平台）	（采购管理平台）	（施工管理平台）	（调试管理平台）	（项目管理平台）
生成推送或提醒信息		多维度数据输出		多维度图表输出		信息提醒、预警、推送

5 结束语

在成熟的数学分析方法、信息化管理手段的条件下，在成本、进度、政策等方面的压力推动下，“大数据+核电”模式的预见性设备管理工具是当前智能化核电建设的发展方向。可以确信，大数据能够为超大型能源工程建设提供辅助决策和管理支持，经过人工智能算法训练过的数据分析平台，能够实现贴近工程实际的设备管理服务。

基于大数据的核电工程预见性设备管理系统，通过打通核电业务多种数据库壁垒，使得各个信息“孤岛”被有效地整合起来，通过多种维度描述核电项目建设的实时状态，为设备管理提供决策依据。

参考文献：

[1] GUESTAH, KUMARS. 实用数据分析[M]. 北京: 机械工业出版社, 2014: 46-56.

[2] 李友俊, 李丽萍, 孙菲. 统计学[M]. 北京:石油工业出版社, 2013: 177-198.

[3] 阿利斯泰尔·克罗尔, 本杰明·尤科维奇. 精益数据分析[M]. 韩知白, 王鹤达, 译. 北京: 人民邮电出版社, 2015: 153-172.

人民邮电出版社

基于泛在电力物联技术的大型供电企业无人值守智能选购仓店应用研究

王超，张晓枫，陈曦，王颖

（国网信通产业集团北京国电通网络技术有限公司，北京 100085）

摘　要：依托国网公司当前泛在电力物联网体系建设，推进大型电网企业智慧无人值守仓店的建设，全面推广物联感知和智能识别技术，应用人脸识别等智能物联技术，打造基于智能物联网的电力无人值守智慧仓店，实现大型电网企业办公用品、零星物资、配网协议物资、电商化物资“智能选购、即采即用、无感支付、便捷舒适、智能物联”的选购需求，为大型电网企业开创一种全新的物资选购管理模式。

关键词：电力物联网；无人值守；人脸识别；智慧选购；无感支付

1　引言

2018 年，国家电网有限公司（以下简称公司）贯彻落实国务院推进供应链创新与应用的指导意见，打造现代（智慧）供应链管理体系。公司紧紧围绕建设“三型两网”的战略目标，推动泛在电力物联网建设，开创“供应链+互联网”新模式。公司当前全力建设的智慧供应链体系，为实现“智慧选购、无人运营、高效供应”的电力打下了良好的基础，但公司目前办公类物资、零星物资、配网协议库存等具有特定电力属性的物资在物资业务管理创新方面仍有较大提升空间。

（1）公司办公用品、零星物资、协议储备物资等对时效性要求极高的物资，目前的常规招标采购模式无法立即满足用户的“即采即用”需求；

（2）公司配网日常运维、应急抢修物资需求具有偶发性、紧急性、响应要求迅速等特点，夜间或紧急抢修事发地处偏远时则无法立即满足抢险需求，延误正常生产；

（3）目前公司电网物资的采购业务流程逐渐表现出耗时长、节点多、工作量大、智能化程度有待提升等管理短板，亟待通过管理模式的创新提升大型电网企业物资采购供应的整体效率和用户体验。

综上，公司针对以上亟待解决问题，紧抓当前泛在电力物联网建设契机，积极推进公司办公用品物资、零购物资、协议库存物资无人值守仓店（打造国网体系内电力物资无人选购商超，对传统无人仓库进行颠覆革新）的试点建设，大胆尝试对具有特定属性的电力物资选购流程进行变革，改进电力物资选购方法，创新选购模式。

2　研究思路

本研究总体设计思路如下：从公司物资业务需求出发，按照泛在电力物联管理理念，全面应用物联感知和智能识别技术建设基于物联网的无人值守智慧仓店。智能物联电力物资无人仓店选址于人流量密集的陕西省电力公司大楼主门附近，方便省公司职工随时选购所需物资，店内配备智能货架和物联网识别、采集设备，智能货架上存放具有特定属性（办公用品、零购、配网协议库存等）的日常必需且消耗量大的电力物资。

进行物资选购时人员只需刷脸入店—选购所需物资—刷脸离店 3 步即完成物资采购，电网公司无人值守仓店的正常运转由电网企业自主研发的“泛在电力物联管控运营平台”进行统一管理，订单的自动生成及推送、电子发票生成及校验、电e宝自动支付等业务环节均通过智能物联平台和移动应用技术后台集成实现，全程无需现金及手机电子支付，电力智能物联管控平台感知终端实现物、人、设备的原始信息采集，实现“物的互联”；网络及平台层实现无人选购业务全程在线记录，永久追溯，实现人机无接触交互，信息化协同与融合；电力物联管控运营管理平台还可以通过挖掘选购数据资产价值，掌控全供应链运营情况，为电力用户提供更优质的选购、结算体验。泛在电力物联技术正逐步变革着目前烦琐冗长的采购业务流

人民邮电出版社

程，是大型电网企业物资部在全面创新泛在电力物联网物资管理业务上的重要里程碑。

大型电网企业智能物联物资无人仓店研究技术路线如图 1 所示。

3 主要研究内容

针对大型电网企业采购频繁、消耗快、需求及时、单品价值低等特性的电网物资，通过组建泛在电力物联网，应用智能终端和移动应用新技术，实现感知层与应用层的互联，实现了电力物资“即采即用、无感支付”这一重大技术突破。

3.1 智能物联无人仓店整体架构

大型电网企业电力物资无人值守仓店研究在国网 SG-ERP3.0 顶层设计和智能物联技术路线的基础上，采用多场景、微服务物联设计，全面推广物联感知和智能识别管理模式，文中主要研究内容如下。

（1）智能物联感知层

感知层作为整个研究最核心、最前端的采集技术，通过人脸识别、电子标签、智能货架、动态视频、物联网基站、有源标签等实现智能无人值守仓店内所有物资的物联网，将以前手工提报、审核的业务通过信息、数据进行流转实现。

（2）智能物联网络层

物联网通信网络实现了大区域、长距离、低成本物联全覆盖，其网络部署轻便、架构优、速度快、连接多、覆盖广、运营商网络成熟，是目前电力物联网应用的核心，网络层接入国网安全认证的物联网络是实现感知层与应用层互联的关键。

（3）智能物联应用层

应用层主要为部署在内外网的物联应用，包含刷脸入店、动态视频监控、即时交互APP、供应商星级评价、库存联动等。物联网应用部署在大型电网企业全业务统一数据中心，开展具体业务应用，对物联业务信息进行处理和展示。

大型电网企业基于智能物联的电力无人仓店整体架构如图 2 所示。

3.2 智能物联无人仓店业务实践

（1）刷脸入店

大型电网企业各单位根据实际业务需求完成本单位实际负责无人选购的人员账号权限分配，首次入店选购需完成选购人员人脸信息采集，通过“物联管控平台”实现注册人员所在单位、ERP账号、利润中心等关键信息绑定，便于后续系统选购、结算业务管理。

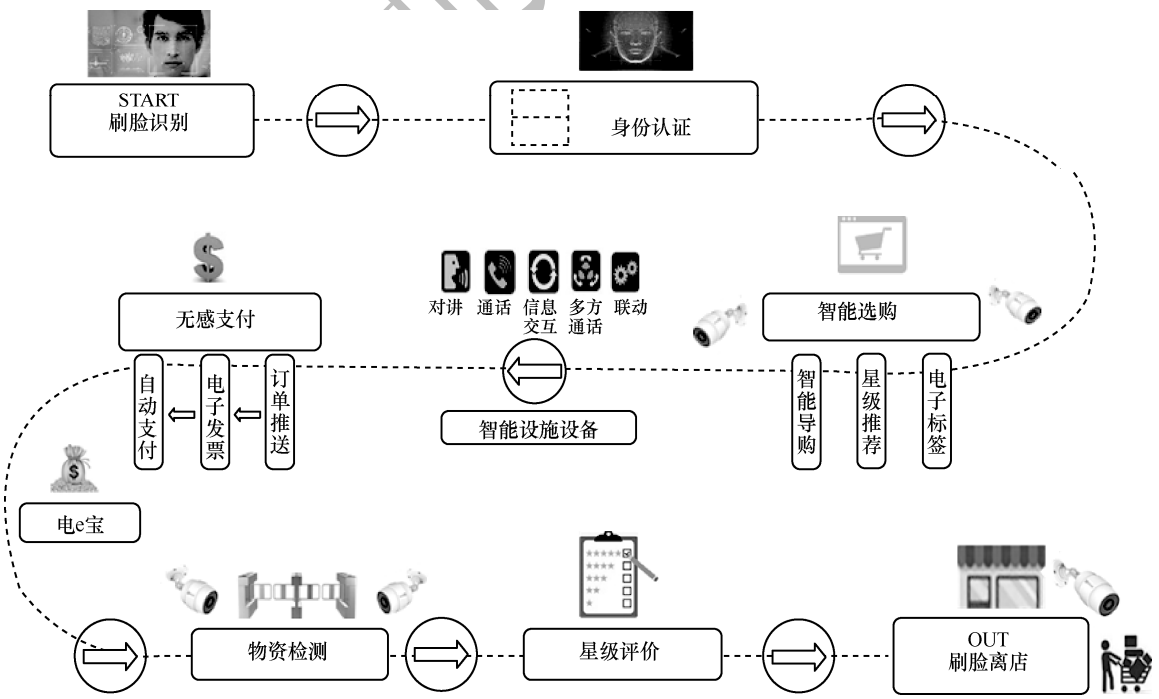


图 1　大型电网企业智能物联物资无人仓店研究技术路线

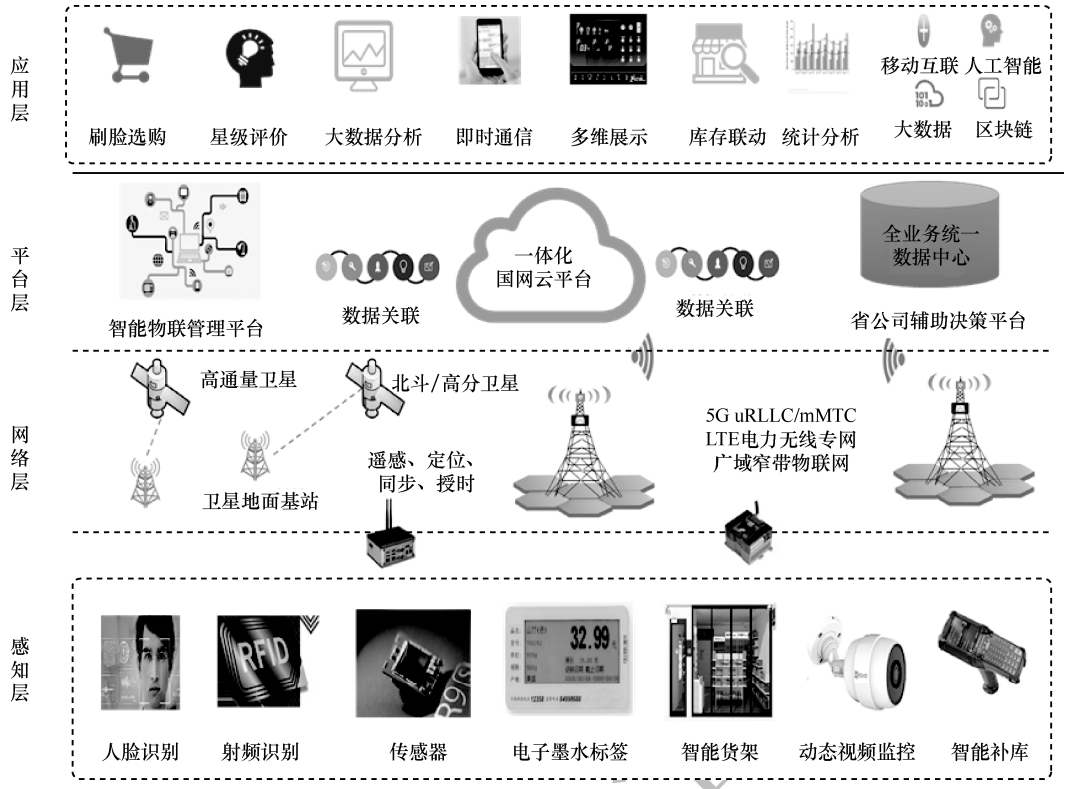


图 2　大型电网企业智能物联物资无人仓店整体架构

（2）智选导购

物资选购人员根据自身权限和物资需求挑选所需物资，当选购人员从智能货架上选取所需物资时大屏会显示价格、数量、供应商、入店时间等物资详细信息，并高亮显示该物资的历史累计星级评分（星级评分为 1～5 星），供物资选购人员对比不同供应商产品时提供决策依据。

（3）无感支付

当选购人员选定所需物资，进入结算区时，智能无人仓店结算系统自动扫描结算区内所有待结算物资，大屏上自动显示本次选购物资数量、选购人、总价等详细物料信息，自动生成选购订单，管控系统后台自动将订单信息推送至ERP财务和财务管控系统，完成电子发票生成、校验，待完成电子支付结算后同步将电子订单、电子发票、结算信息推送至选购人员手机。

（4）刷脸离店

智能无人仓店通道设有物资自动识别设备及防盗感应监测门禁，当物资选购人员完成物资选购并完成后台无感支付后，抬头正视门禁上的人脸识别设备完成身份校验，打开通道门禁，实现闭环防盗验证，既让电力公司员工享受物资选购的便捷、高效，也保证无人仓店的安全。

（5）自动补库

智能物联无人仓店物联管控系统根据历史物资选购大数据分析各物资的未来消耗趋势，各仓店可科学设置各品类物资的安全库存并进行预警，供应商在最短时间内响应缺货仓店的补货需求，及时进行补货。用户可在手机端实时查询无人仓店当前物品数量，确保“即采即用”。

（6）智慧评价

无人仓店智能物联管控系统为物资选购人员提供便捷的商品评价渠道，在无人仓店内的智能货架上配备电子墨水标签，高亮显示历史用户累计评价星级，直观呈现各供应商产品的质量评价信息，为后续选购用户提供科学参考，同时也为省公司在年度供应商招标过程中提供客观的评分依据，优选供应商。

大型电网企业智能物联物资无人仓店业务模式如图 3 所示。

4　创新点及成效

基于智能物联技术的电力无人值守智慧仓店应用

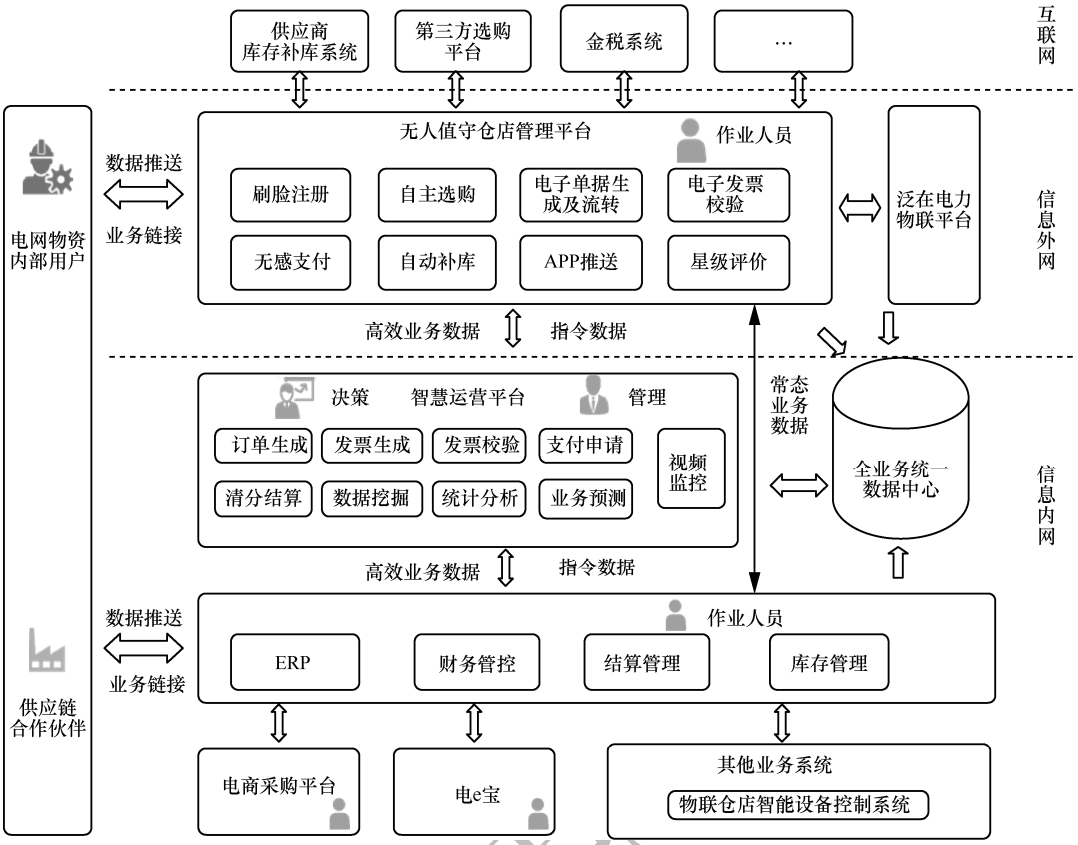


图 3 大型电网企业智能物联物资无人仓店业务模式

创新性地实现了电网企业在办公类物资、零星购置物资、配网协议物资、电商化选购物资领域“智能选购、即采即用、无感支付、舒适体验”的物资选购需求，为大型电网企业开创了一种全新的物资选购管理模式。

（1）全息感知实现智能物联

智能物联无人仓店依托泛在电力物联管理理念，运用传感器、人脸识别、智能货架、电子标签等技术实现物与物、物与人的泛在连接。

（2）业态变革推动智慧选购

智能物联无人仓店打造无人值守、自动结算、全天候选购的物资采购管理新模式，这种新业态可随时满足大型电网企业职能部门办公用品、运维抢修物资等的“即时领用”，是顺应国网公司泛在电力物联发展的坚强推手，有利于大型电网企业培育物资采购新业态。

（3）智能集成实现无感支付

物资选购人员刷脸入店后所有结算流程均通过系统后台无缝集成，真正实现物资选购全程“无感支付”体验。智能物联无人仓店的应用正式催生出一种“解放采购人员双手，活动选购人员双脚”的新管理模式，为电力用户打造“五分钟”电力物资选购生活圈。

（4）全程参与实现智慧评价

智能物联无人仓店为电力物资选购人员在选购过程中提供便捷的评价渠道，选购人员可通过手机进行星级评价并同步至物联管控平台为后续用户选购该商品提供直观、科学的参考，同时为大型电网企业在供应商年度入围框架，招标过程中提供更客观真实的打分依据，优选出更合适的供应商。

（5）即领即用实现自动补库

智能物联无人仓店实现与供应商系统的无缝集成，智能物联管控平台根据历史物资消耗大数据，得出各物资的消耗趋势，科学设置各物资安全库存并实时预警，当物资消耗接近安全库存时智能物联管控系统自动生成补货订单推送至供应商库存系统，供应商在最短时间进行补货上架。

5 结束语

大型电网企业智能无人仓店依托泛在电力物联管

理理念创新物资采购模式，有效地解放了传统物资采购、履约、供应等环节现场工作，提高了物资管理的高效性、即时性，建设以智能物联的电力无人值守仓店为代表的新业态管理模式在电力物资采购业务中的应用具有划时代意义，是全面创新泛在电力物联网物资管理领域质的突破。

在不久的未来，电力物资采购及供应管理人员可通过智能穿戴设备，利用增强现实技术，实现物资和系统数据的叠加展示，减轻物资采购供应作业的负担，提升作业的效率，进而打造大型电网企业全新一代泛在电力物联网物资采购智慧力。

参考文献

[1] 姚志强, 朱恒军, 都文和. 基于物联网的智能仓库监控系统设计与实现[J]. 河北工程大学学报, 2014(2): 86-88+97.
[2] 任芳. 无人仓需求在望技术有待突破[J]. 物流技术与应用, 2017(1): 58-61.
[3] 刘化君. 物联网关键技术研究[J]. 计算机时代, 20l0(7).
[4] 陈明, 刘翔. 电力 EPC 在物联网的应用研究[J]. 电力信息化, 2011(12): 53-56.
[5] 王浩宇. “无人超市”自动识别技术[J]. 电子技术与软件工程, 2017(19): 80.
[6] 胡永利, 孙艳丰, 尹宝才. 物联网信息感知与交互技术[J]. 计算机学报, 2012(6): 1147-1163.
[7] CONTIP N. The internet of things[J]. Communications Engineer, 2016, 4(6).

人民邮电出版社

基于泛在物联网的智慧城市应用

寇立冬，周晶，孙喜民，张宾
（国家电网电子商务有限公司，北京 100053）

摘　要：物联网（internet of things，IoT）应能透明和无缝地整合大量不同的终端系统，同时为开发大量数字服务提供对指定数据内容的公开访问。因此，为物联网构建通用架构是一项非常复杂的任务，这主要是因为在这样一个系统中可能涉及到各种设备、链路层技术和服务。特别关注一个城市物联网系统，该系统虽然仍然是一个相当广义的范畴，但却有其特定的应用领域。事实上，城市物联网旨在支撑智慧城市建设，其目的是利用最先进的通信技术，为城市管理和公民提供增值服务。因此，对城市物联网的技术应用、协议和体系结构进行了全面的介绍。

关键词：网络体系结构；传感器系统集成；智慧城市

1　引言

本文旨在研究城市物联网设计的一般参考框架。首先，描述了城市物联网的具体特征，以及可能推动地方政府采用城市物联网的服务。然后，概述了基于Web 的物联网服务设计方法，以及相关的协议和技术，讨论了它们对智慧城市环境的适用性。最后，通过报告“智慧城市”项目中的经验来证实论文观点。

2　智慧城市的定义与服务

智慧城市市场源于关键行业和服务部门的协同互联，如智能治理、智能交通、智能公用事业、智能建筑和智能环境。表 1 中报告了服务的概要视图，包括拟部署的网络的建议类型、服务产生的预期流量、可容忍的最大延迟、设备供电以及对当前可用技术的每个服务的可行性估计。从表 1 中可以清晰地看出，一

表 1　智慧城市服务统计

服务类型	网络类型	数据传输率	允许延时	供电方式	可行性等级
建筑健康监测	802.15.4、Wi-Fi、以太网	10 min/次	数据：30 min 报警：10 s	电池供电	1：容易实现，但振弦传感器不易安装
废物管理	Wi-Fi、3G 和 4G	1 h/次	数据：30 min	电池或太阳能板	2：容易实现，但需要安装智能垃圾桶
空气质量监测	802.15.4、蓝牙、Wi-Fi	30 min/次	数据：5 min	太阳能板	1：容易实现，但二氧化碳传感器比较贵
噪声监测	802.15.4、以太网	10 min/次	数据：5 min 报警：10 s	电池或太阳能板	2：固定设备噪声检测有困难
交通拥堵	802.15.4、蓝牙、Wi-Fi、以太网	10 min/次	数据：5 min	电池或太阳能板	3：根据空气质量和噪声情况判断
城市能耗	PLC、以太网	10 min/次	数据：5 min	交流 220 V	2：容易实现，但需要供电方授权
智能停车场	802.15.4、以太网	按需求发送	1 min	太阳能板	1：智能停车场已经应用于大型超市
智能照明	802.15.4、Wi-Fi、以太网	按需求发送	1 min	交流 220 V	2：没有难度，但要进行基础设施改造
公共楼宇自动化与安全	802.15.4、Wi-Fi、以太网	10 min/次	5 min	交流 220 V 或电池供电	2：没有难度，但要进行基础设施改造

人民邮电出版社

般来说，大多数此类服务的实际实现并不受技术问题的阻碍，而是受限于缺乏广泛接受的通信和服务架构，该架构可以从单一技术的具体特征中抽象出来并提供统一的服务支持。

3 智慧城市物联网架构

大多数智慧城市服务都基于一种集中的体系结构，其中部署在城市地区的一组密集和异构的外围设备会生成不同类型的数据，通过适当的通信技术将其传送到控制中心，在控制中心进行数据存储和处理。

因此，城市物联网基础设施的一个主要特点是有能力将不同的技术与现有的通信基础设施结合起来，以支持物联网的逐步发展，并实现其他设备的互联以及新功能和服务的实现。另一个基本方面是，必须使城市物联网收集的部分数据便于当局和公民查看，提高政府对城市问题的反应能力，并提高公民对公共事务的认识和参与[1]。基于 Web 服务方法的城市物联网概念示意如图 1 所示。

（1）物联网服务体系结构的 Web 服务方法

物联网的 IETF 标准采用了物联网服务的 Web 服务体系结构，作为一种非常有前景和灵活的方法，该结构已经被广泛地记录在文献中。事实上，Web 服务允许通过采用被称为代表性状态传输（REST）的基于 Web 的模式，实现灵活和可互操作的系统，可以扩展到物联网节点。按照 REST 规范设计的物联网服务与传统的 Web 服务具有很强的相似性，极大地方便了终端用户和服务开发人员对物联网的采用和使用，使其能够方便地重用从传统 Web 技术中获得的大量技术，为包含智能对象的网络开发服务。IETF、ETSI 和 W3C 等国际标准化机构以及欧洲关于物联网的研究项目（如 SESEI、物联网和 SmartSantander）也推广了 Web 服务方法。

图 2 显示了城市物联网系统的参考协议架构，其中包括不受限协议栈和受限协议栈。第一个协议由当前 Internet 通信的实际标准组成，通常由常规 internet 主机（如 XML、HTTP 和 IPv4）使用。这些协议由它们的低复杂度代换（即有效 XML 交换（EXI）、受限应用协议（CoAP）和 6LoWPAN）镜像在受限协议堆栈中，它们适用于非常受限的设备。图 1 中左右侧堆栈协议之间的代码转换操作，可以以标准且低复杂度的方式执行，从而保证物联网节点与互联网的易接入性和互操作性。值得指出的是，不采用

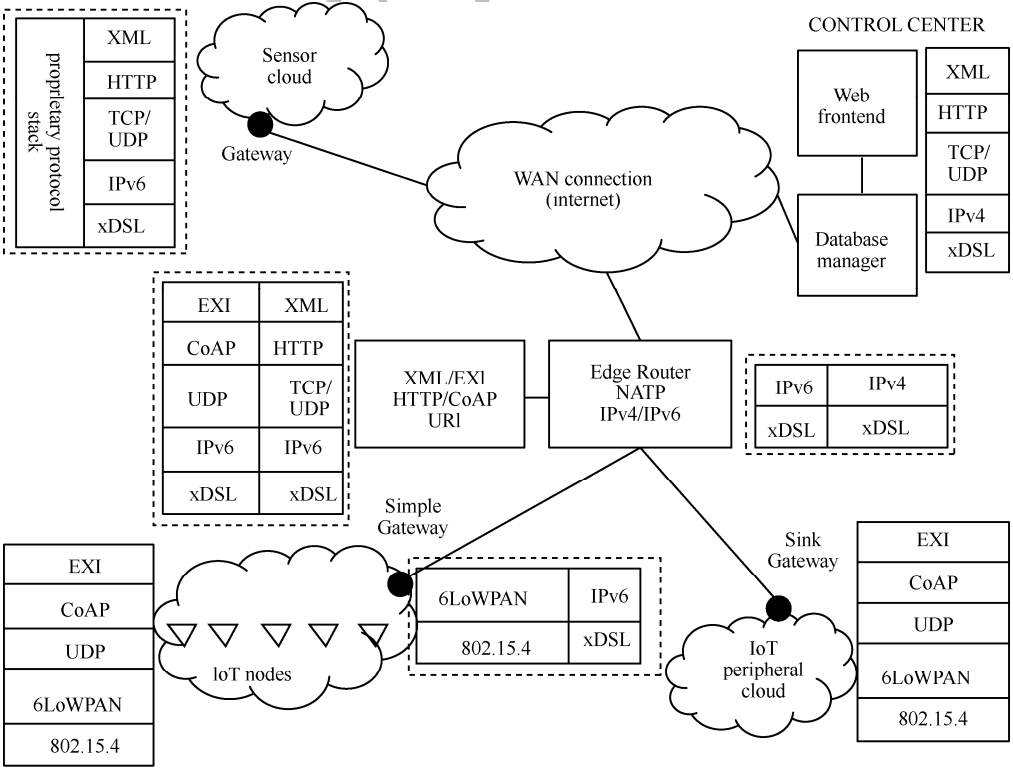


图 1　基于 Web 服务方法的城市物联网概念示意

EXI/CoAP/6LoWPAN 协议栈的系统仍可无缝包含在城市物联网系统中，前提是它们能够与图 2 中协议架构左侧的所有层进行接口。

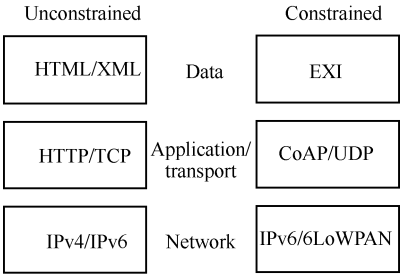


图 2　物联网节点不受限协议栈和受限协议栈

在图 2 所示的协议体系结构中，可以区分为 3 个不同的功能层，即数据、应用/传输和网络，它们需要专门的实体来操作受限和不受限的格式和协议之间的转码。

• 数据格式

万维网联合会（W3C）的工作组提出了 EXI 格式[2]，这使得非常受限的设备也能够使用与 XML 兼容的开放的数据格式在本地支持和生成消息。

通过使用由高级应用程序创建和维护的数据库，可以将多个 XML/EXI 数据源集成到一个物联网系统中。实际上，物联网应用程序通常会建立一个由应用程序控制的节点的数据库，以及通常由这些节点生成的数据库。数据库使集成任何物联网设备接收的数据成为可能，以提供构建应用程序的特定服务。

• 应用和传输层

CoAP 协议[3]提出通过 UDP 传输的二进制格式来克服这些困难，只处理提供可靠服务所严格要求的重传。此外，CoAP 可以很容易地与 HTTP 进行互操作，因为：它支持 HTTP 的 REST 架构（GET、PUT、POST 和 DELETE）；两个协议的响应代码之间存在一对一的对应关系；CoAP 选项可以支持广泛的 HTTP 使用场景。

尽管常规 Internet 主机可以在本机支持 CoAP 直接与 IoT 设备对话，但最通用且易于互操作的解决方案需要部署 HTTP-CoAP 中介，也称为网关，可在两个协议之间直接进行转换请求/响应，从而实现与本机 HTTP 设备和应用程序的透明互操作[4]。

• 网络层

V4/V6 端口地址转换（V4/V6 PAT）。该方法将任意一对 IPv4 地址和 TCP/UDP 端口映射到 IPv6 地址和 TCP/UDP 端口。它类似于许多局域网目前支持的经典网络地址和端口转换（NAPT）服务，通过共享公共 IPv4 地址（用于在公共 Internet 上对数据包进行寻址）来向专用网络中的多个主机提供 Internet 访问。当分组返回到 IPv4 公共地址时，支持 NATP 服务的边界路由器将拦截该分组并用预期接收器的（私有）地址替换公共 IPv4 目的地址，该地址是通过在 NATP 表中查找与该分组所携带的特定目的端口相关联的主机地址来确定的。同样的技术可以用于将多个 IPv6 地址映射到一个单独的 IPv4 公共地址，从而允许在 IPv4 网络中转发数据报及其在仅使用 IPv4 的主机上的正确管理。该技术的应用需要较低的复杂度，实际上，端口映射是 V4/V6 转换的一种既定技术。另一方面，这种方法带来了可伸缩性问题，因为可以多路复用到一个 IPv4 地址的 IPv6 主机的数量受到可用的 TCP/UDP 端口数（65 535）的限制。此外，这种方法要求连接由 IPv6 节点发起，以便在 NATP 查找表中创建正确的条目。从 IPv4 云开始的连接也可以实现，但这需要更复杂的体系结构，本地 DNS 位于 IPv6 网络中，并静态地关联到 NATP 转换表中的公共 IPv4 地址上。

通过利用 HTTP 主机头中包含的信息来标识用户请求的特定网站，支持同一 Web 服务器上的多个网站，共享相同的 IPv4 地址。类似地，可以编程 DNS 服务器，以便在 DNS 请求到物联网 Web 服务的域名时，DNS 返回 HTTP-CoAP 交叉代理的 IPv4 地址，以便与之联系及访问物联网节点。一旦通过 HTTP 请求来处理，代理就需要将 HTTP 主机头中包含的域名解析到 IPv6 DNS 服务器中，后者使用标识请求中涉及的最终物联网节点的 IPv6 地址进行应答。然后，代理可以通过 CoAP 将 HTTP 消息转发到预期的物联网中。

URI 映射[5]还描述了通用资源标识符（URI）映射技术。该技术涉及一种特定类型的 HTTP-CoAP 交叉代理，即反向交叉代理。此代理充当 HTTP/IPv4 客户端的最终 Web 服务器和 CoAP/IPv6 Web 服务器的原始客户端。由于这台机器需要放置在存在 IPv6 连接以允许直接访问最终物联网节点的部分网络中，因此 IPv4/IPv6 转换由应用的 URI 映射函数在内部解决。

（2）链路层技术

受限物理层和链路层技术的特点是能量消耗低，传输速率相对较低，通常小于 1 Mbit/s。这类技术中比较突出的解决方案是 IEEE802.15.4[6]、蓝牙和蓝牙低能量、8 IEEE 802.11 低功耗、PLC[7]、NFC 和 RFID[8]。

人民邮电出版社

这些链路具有较长的延迟性，主要有两个因素：一是物理层传输速率低；二是节点实施节能策略，这通常涉及工作周期较短的任务循环。

（3）设备

• 后端服务器

位于控制中心的后端服务器，在那里收集、存储和处理数据，以产生增值服务。

• 网关

向物联网的“边缘”移动，网关的作用是将终端设备与系统的主要通信基础设施互连。参照图 2 中描述的协议体系结构，网关需要提供不受限协议与其受限对应方之间的协议转换和功能映射，即 XML-EXI、HTTP-CoAP、IPv4/v6-6LoWPAN。

• 物联网外围节点

在物联网系统的外围，负责将数据传送到控制中心的设备，通常称为物联网节点。物联网节点可以根据多种特性进行分类，如供电方式、网络角色（中继或终端）、传感器/执行器设备以及支持的链路层技术。

4 结束语

本文分析了目前城市物联网实施的解决方案。所讨论的技术已接近标准化，业界参与者已经在积极生产利用这些技术实现的应用设备。虽然物联网系统的设计选择范围相当广泛，但开放和标准化的协议集却很少。此外，相关技术已经达到了成熟的程度，能够实现物联网解决方案和服务，智慧城市部署的具体案例实施正是将物联网模式应用于智慧城市的可行性案例。

参考文献：

[1] MULLIGAN C E A, OLSSON M. Architectural implications of smart city business models: anevolutionary perspective[J]. IEEE Communications Magazine, 2013, 51(6): 80-85.

[2] FIELDING R T. Architectural styles and the design of network-based software architectures (the representational state transfer (REST)).[J] Dissertation UCI, 200, 65(3): 303.

[3] SCHNEIDER J, KAMIYA T, PEINTNER D, et al. Efficient XML interchange (EXI) format 1.0. eds., 2nd ed. world wide Web Consortium, [Z]. 2014.

[4] SHELBY Z, HARTKE K, BORMANN C, et al. Constrained applica-tion protocol (CoAP), draft-ietf-core-coap-18 (work in progress)[Z]. 2013.

[5] CASTELLANI A, LORETO S, RAHMAN A, et al. Best practices for HTTP-CoAP mapping implementation, draft-castellani-core- http-mapping-07 (work in progress)[Z]. 2013.

[6] IEEE standard for local and metropolitan area networks—part 15.4: low-rate wireless personal area networks (LR-WPANs)[S]. 2011.

[7] IEEE communications society, P1901.2-2013—standard for low fre-quency (less than 500 kHz) narrow band power line communications for smart grid applications[S]. 2013.

[8] ISO/IEC 14443-1:2008, identification cards—contactless integrated circuit cards—proximity cards—part 1: physical characteristics[Z]. 2008.

人民邮电出版社

基于机器学习的水电站水库水位预测应用

林文孝，郑贵德
（中国电机工程学会，北京 100761）

摘　要：水电是清洁能源，日益受到重视。水电水情主要受到天气影响，水库水位短期预测可以借助天气预报预测，但中长期预测仍然是个问题，预测准确度无法达到预期。一种常用的水库水位预测方法是根据水库水位监测的历史数据做统计分析，虽然水库水位本身已经隐含了天气等因素，但仅依据水位自身数据预测还是无法满足预测准确度的需要，从目前已有的预测效果来看，最上游水库水位预测相对稳定，但对下游水库来说，由于水库水流之间相互影响，水库水位预测比较复杂，预测稳定度不好。提出一种对水库水位预测的方法，该方法的特点是能够客观考虑各水库的上下游关联及影响，并利用大数据、机器学习技术，包括关联分析及基于神经网络的多特征及记忆能力预测分析技术，更加准确地预测水库水位，为中长期发电计划提供有效辅助。

关键词：水库水位预测；机器学习；水库水位关联分析

1　引言

我国一些地区，特别是西南地区，水资源非常丰富，随着国家对清洁能源利用的政策导向，优先充分利用水电资源成为重要举措，所以，水电站发电预测十分重要[1-2]。然而，多年来，水电站发电能力预测不能满足实际期望，其中重要原因之一就是中长期的天气难以把握。

由于中长期天气难以预测[3-5]，本文对水电站本身历史水库水位的数据进行预测，与传统方法的不同表现在：其一是能获得的历史数据比以往完整且数据量比较大，能够反映一定的历史趋势；其二是考虑水位变化的环境影响，特别是水库之间错综复杂的相互影响；其三就是综合应用大数据技术及多种机器学习算法[6-7]，实现预测的创新应用。

目前使用水电站水库水位历史监测数据的预测分析，对于最上游的水库，通过数据本身水位反映的趋势。其预测基本可以满足要求，但对于下游的水库，由于水库之间的上下游流动，相互影响，通过水位直接预测的稳定度、准确度明显差于最上游水电站，预测结果的准确性还需要提升。本文是在传统监测水位分析的基础上，改进预测模型，增加各水库的上下游关联及其他特征，作为影响水位的因素，再根据时间序列的神经网络，对水位进行预测，该预测方法的稳定度、准确度比传统方法有明显提升，可以为中长期水电发电计划提供有效辅助。

2　研究路线

水位趋势符合季节规律，而且越是近期的水位对未来趋势判断影响越大，这种分析方法如果采用 Holt-winters 的 3 次指数平滑或 ARIMA 差分自回归移动平均方法[8-12]也能预测，但是，这种方法高度依赖单一数据指标，特别是其他影响特征没有得到有效考虑，所以预测准确度不够。本文采用了具备多特征的神经网络时间序列算法。综合考虑了历史趋势、时间权重以及环境特征影响因素，分析效果明显改进。

关于水库水位预测分析的步骤如下。

（1）获取数据源及数据清洗

包括各水电站水库的历史水位、天气状态、日水流量等。由于无论是下雨，还是储放水，都会反映到邻近几天的水位。故此，可重点采用基于密度的离群点检测方法[13-15]，对异常数据校正。基于密度的观点来看，离群点是在低密度区域中的对象。基于密度的离群点检测给出了对象是离群点程度的定量度量，并且即使数据具有不同密度的区域也能够很好地处理。对于缺失值，也可以用以上方法处理，把缺失值当作异常处理。

（2）水位关联影响特征

上下游水库水位关联指的是水库受到上游或同一流域水位变动的影响，这个影响程度多大，人工很难

人民邮电出版社

估计，但通过机器学习就可以自动识别，而且更加客观，甚至还可能有意外收获。在大部分日期中，如果几个水库水位波存在一定的因果概率，那么这些水库是有相互关联的，把这些高度相互关联的水库水位变化作为预测分析的影响因素。

（3）基于时间序列模型算法的预测

水电站水库水位本身是有一定规律的，随着季节年复一年，经历了汛期、平水期、枯水期等。所以对于中长期水位预测，可以应用历史数据使用时间序列的算法拟合出水位的变动规律。但增加除水位以外的特征，可以使预测更加精确，本文在水位本身数据的基础上增加天气状态、日水流量上下游水库关联等特征。

3 水库关联分析方法

水电站的上下游水库水位是相互影响的。尽管人工可以标记上下游水库，但由于流域影响的复杂性，这种主观很难反映真实情况。本文借用 Apriori 算法思路[16-17]，通过频繁项挖掘发现关联关联程度及关系。Apriori 算法的主要概念如下。

- 项与项集：设 itemset={item1, item_2, …, item_m}是所有项的集合，其中，item_k(k=1,2,…,m)称为项。项的集合称为项集（itemset），包含 k 个项的项集称为 k 项集（k-itemset）。
- 关联规则：关联规则是形如 A=>B 的蕴涵式，其中 A、B 均为 itemset 的子集且均不为空集。
- 支持度（support）：反映数据集的频繁程度，关联规则的支持度定义如下：

$$\text{support}(A \Rightarrow B) = P(A \cup B) \tag{1}$$

- 置信度：确定 A 在包含 B 的记录项中出现的频繁程度，关联规则的置信度定义如下：

$$\text{confidence}(A \Rightarrow B) = P(B \mid A) = \frac{\text{support}(A \cup B)}{\text{support}(A \cup B)} = \frac{\text{support\_count}(A \cup B)}{\text{support\_count}(A)} \tag{2}$$

频繁集挖掘步骤如下。

输入：数据集合 D，支持度阈值 α；

输出：最大的频繁 k 项集；

（1）扫描整个数据集，得到所有出现过的数据，作为候选频繁 1 项集。k=1，频繁 0 项集为空集。

（2）挖掘频繁 k 项集：扫描数据计算候选频繁 k 项集的支持度；去除候选频繁 k 项集中支持度低于阈值的数据集，得到频繁 k 项集。如果得到的频繁 k 项集为空，则直接返回频繁 k−1 项集的集合作为算法结果，算法结束。如果得到的频繁 k 项集只有一项，则直接返回频繁 k 项集的集合作为算法结果，算法结束。基于频繁 k 项集，连接生成候选频繁 k+1 项集。

（3）令 k=k+1，转入步骤（2）。一旦找出了频繁项集，就可以直接由它们产生强关联规则。产生步骤是：

对于每个频繁项集 itemset，产生 itemset 的所有非空子集（这些非空子集一定是频繁项集）。

对于 itemset 的每个非空子集 s，如果存在：

$$\frac{\text{support\_count}(l)}{\text{support\_count}(s)} \geqslant \text{min\_conf} \tag{3}$$

则输出：

$$s \Rightarrow (l - s) \tag{4}$$

其中，min_conf 是最小置信度阈值，l 是项集中的一项。

由于各水库水位涨跌影响有点时间滞后，所以以周为单位。累计水库周水位涨幅变化率达到指定阈值的水库名字才能出现在数据集中。

假设 a、b、c、d、e 是 5 个水库名称。按时间顺序，周水位波动达到 10%的水库数据集见表 1。

表 1 潜在关联水库数据集

周标志	水库名称
W1	a、c 、e
W2	b、d
W3	b、c
W4	a、b、c、d
W5	a、b
W6	b、c
W7	a、b
W8	a、b、c、e
W9	a、b、c
W10	a、c、e

频繁集生成过程如图 1 所示。

从以上输出可以看出，水库 a 对水库 b 和水库 c 的水位有影响。也就是说，水库 a 的水位变化，可以作为水库 b、c 的影响特征。至于支持度、置信度大小，可以根据实际情况设定。

人民邮电出版社

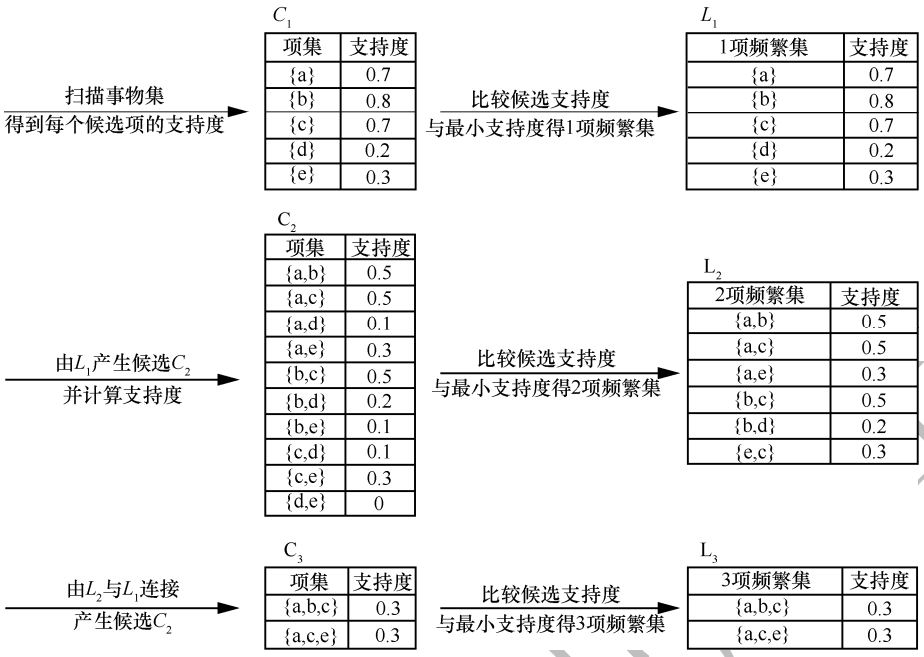


图 1　水库频繁集生成过程

输出结果见表 2。

表 2　水库关联的支持度及置信度输出

规则	（支持度，置信度）
a→b	(50%,71.428 6%)
b→a	(50%,62.5%)
a→c	(50%,71.428 6%)
c→a	(30%,71.428 6%)
b→c	(50%,62.5%)
c→b	(50%,71.428 6%)
e→a	(30%,100%)
e→c	(30%,100%)
a,b→c	(30%,60%)
a,c→b	(30%,60%)
b,c→a	(30%,60%)
e→a,c	(30%,100%)
a,c→e	(30%,60%)
a,e→c	(30%,100%)
c,e→a	(30%,100%)
d→b	(20%,100%)

4　水库水位预测算法模型

水库水位趋势，具有明显的季节波动规律，可以用时间序列分析算法。传统方法一般可以用指数平滑、自回归移动平均等，但这些算法往往只局限于本身数据，对其他影响因素考虑不够。如果用浅层神经网络或 SVM 算法进行回归分析，虽然可以分析水位受环境变量的影响，但对水位的历史规律把握不好。

LSTM（long-short term memory）[6,18-20]，是一种时间递归神经网络（RNN），适合被用于处理和预测时间序列中间隔和延迟较长的重要事件，经实验证实，在时间序列应用上，它通常比 RNN 和 HMM 效果更好，LSTM 神经元在其管道中可以保持记忆，以允许解决顺序和长时间问题，而不会出现影响其性能的消失梯度问题，同时，相对传统时间序列算法，LSTM 还能够考虑多个特征的综合影响。

基本的 LSTM 的结构如图 2 所示，图 2 中隐藏状态 h_t 是当前学习的输出，由本次输入序列数 x_t 和上次输出 h_t−1 得到。得到 h_t 后，一方面用于当前层的模型损失计算，另一方面用于计算下一层的 h_{t+1}。

对水位这种有一定季节规律性趋势的预测，不仅需要最新的时间序列数据，还需要有能力学习参考历史规律，为此，还需要学习系统能够对历史规律的记忆。LSTM 是典型具有记忆的递归神经网络。LSTM 的特色是引入了细胞状态及门控结构，其神经网络结构如图 3 所示。

人民邮电出版社

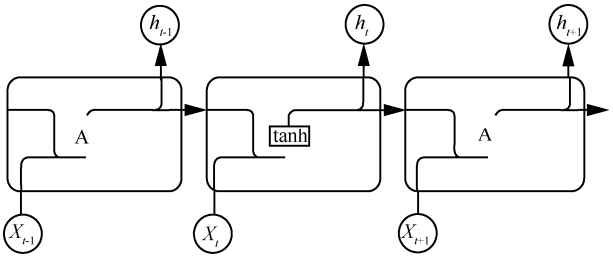


图 2　LSTM 神经网络基本结构

图 3 中 σ 为 sigmoid 激活函数。

每层 LSTM 内部结构如图 4 所示。

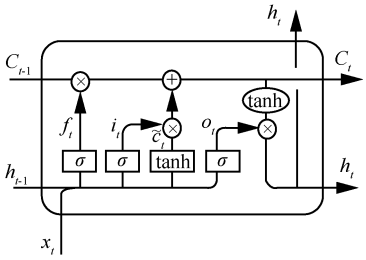


图 4　LSTM 细胞单元及内部结构

其中，细胞状态是使 LSTM 具备记忆能力的重要体现，即图 4 中上方的水平线。

细胞状态贯穿整个链条。针对水库水位变化趋势来说，由于水位变化趋势具有季节规律，但也有噪音。通过的细胞状态是 LSTM 需要记忆的信息，比如近期的信息需要多记，远期的信息需要少记住一些，甚至遗忘一些噪声信息，这就需要通过 LSTM 的几个门来控制，LSTM 的门包括遗忘门、输入门和输出门 3 种。

LSTM 的第一步决定从细胞状态中舍弃哪些信息。这一决定由“遗忘门”层的 S 形网络层做出。它接收 h_t−1 和 x_t，并且对细胞状态 C_{t-1} 中的每一个数来说输出值都介于 0 和 1 之间。1 表示“完全接受这个”，0 表示“完全忽略这个”。遗忘门及遗忘算式如图 5 所示。

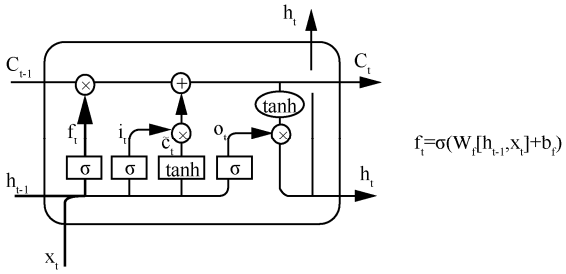


图 5　LSTM 遗忘门及计算函数

第二步要确定需要在细胞状态中保存哪些新信息。这里分成两部分：第一部分，一个“输入门”层的 S 形网络层确定哪些信息需要更新；第二部分，一个 tanh 形网络层创建一个新的备选值向量 $\tilde{C}_t$，用来添加到细胞状态。输入门及算式如图 6 所示。

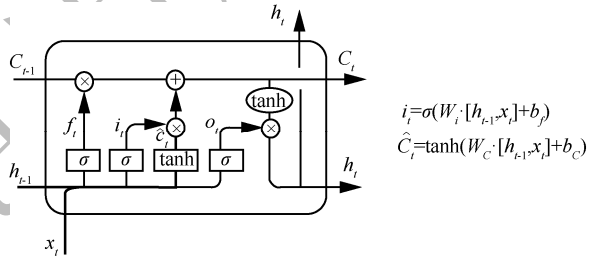


图 6　LSTM 输入门及计算函数

第三步将上面的两步结合起来，产生对状态的更新。把旧的细胞状态 C_{t-1} 更新到 C_t。对旧的状态乘以 f_t，用来忘记决定忘记的事。然后加上 $i_t\cdot\tilde{C}_t$，这是新的候选值，根据对每个状态决定的更新值按比例进行缩放。对状态的更新逻辑及算式如图 7 所示。

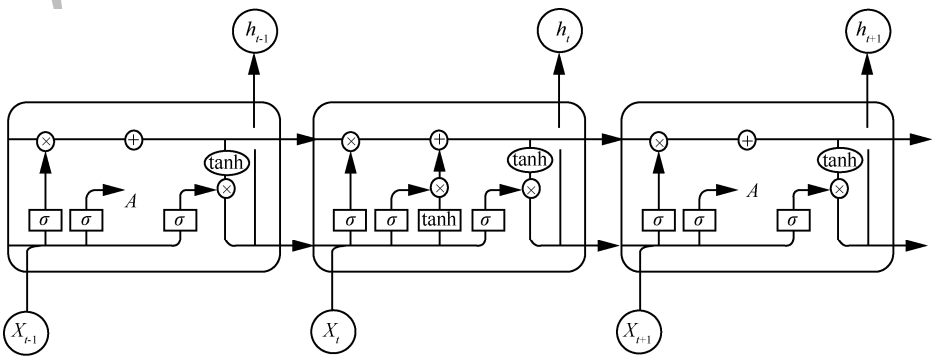


图 3　LSTM 神经网络及门控结构

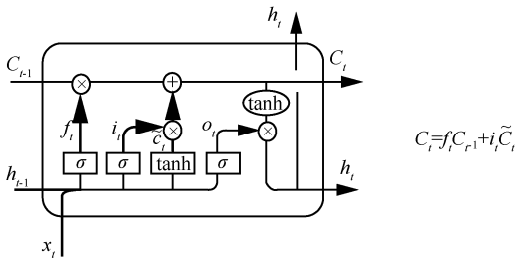


图 7　LSTM 状态更新逻辑及计算函数

最后，确定输出值。输出依赖于细胞状态，但会是一个“过滤”的版本。先通过运行 S 形网络层，确定细胞状态中的哪些部分可以输出。然后，把细胞状态输入 tanh 再和 S 形网络层的输出值相乘，输出需要的部分。输出门及计算式如图 8 所示。

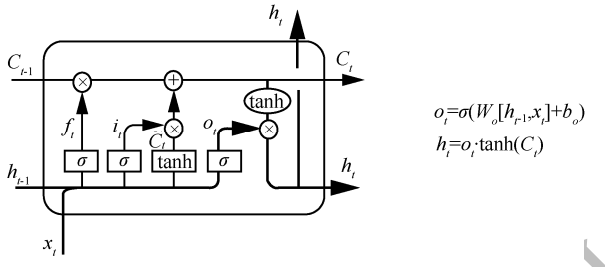


图 8　LSTM 输出门及计算函数

准备了十几年各水库每天水位记录，以一周为单位，通过历史数据预测下周水位。由于水位基本波动有明显的“月”周期性，把时间跨度设为一个月，让 LSTM 记住一个月的周期信息。

图 9 是某 3 个水电站的实际水位波动图。

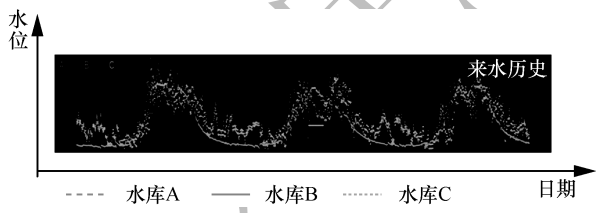


图 9　3 个水电站水库水位散点

LSTM 层的工作方式是采用 3 维（N，W，F）的 numpy 数组，其中 N 是训练序列的数量，W 是序列长度，F 是每个序列的特征数。选择使用一个月的序列长度（读取窗口大小），因此可以在每个序列中看到周期波的形状，并建立基于序列的序列模式。

使用机器学习工具建模训练测试和预测，数据集至少分为训练样本和测试样本，并依据损失图，调整 LSTM 参数，使训练和测试的损失函数结果的差异稳定并最小化。

通过训练验证并逐步调优过程如下。直到训练误差与测试误差趋于稳定并接近，同时误差相对最小化。LSTM 训练及测试的损失函数逼近图如图 10 所示。

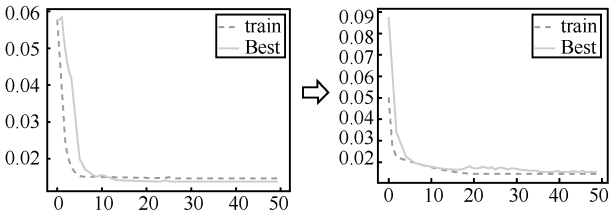


图 10　LSTM 训练及测试的损失函数

最后应用训练模型预测，预测效果如图 11 所示。

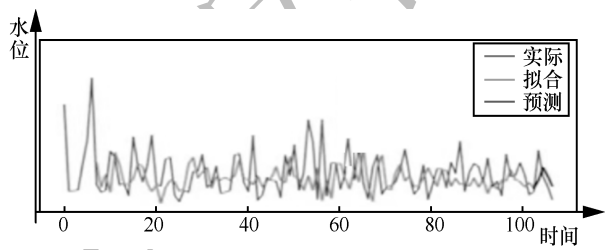


图 11　基于 LSTM 的水位预测

5　结束语

水电站水情预测长期以来一直都在进行中，中小型水电站都具备一定的水位监测点能力。水库水位短期内的波动，基本可以依靠天气预报以及水库现有水位、日来水量、各季节的日蒸发、渗透、畜放水计划等统计分析得到比较准确预测。

随着清洁能源重视度提高，中长期的水情预测变得更加重要。水电站经过多年的数据采集，已经积累了大量数据，这为基于大数据/机器学习的水库水位预测提供了基础，实践证明，目前基于新技术的中/长期预测已经成为可能，是在传统预测建立的基础上的创新与突破。

本应用研究主要创新点如下：

- 利用十几年的海量数据挖掘分析，而不只是传统的基于小数据的数理统计分析方法，同时数据模型是动态的，可根据实际数据学习更新；
- 模型算法分析的特征变量具有多个，除了水位本身，还增加了多个影响水位的特征变量，包括日流水量、天气主要状态、关联水库水位等，根据隐马尔可夫理论，天气状态的转换应该和

降雨存在一定概率的依存关系；

- 水库水位关联分析，各水库水位是有关联的，通过历史数据探索，最上游水库规律明显比较好把握，而下游水库水位受其他水库影响，这种影响很难通过主观挖掘，通过机器学习的关联分析可以很客观反映水库之间水位的关联影响；
- 采用具有记忆能力的神经网络算法模型，LSTM 可以实现具有一定周期规律的多特征变量预测分析，相比传统的指数平滑等预测分析可以考虑更多的特征变量影响，同时比普通神经网络有长期记忆能力，相对 RNN 来说，由于 LSTM 通过门机制使用激活函数，使梯度能够更好地在 LSTM 中传递，很大程度上减轻了梯度消失发生的概率。

总之，中/长期水电预测十分重要，但目前采用的传统方法预测准确是不尽如人意。通过本文方法，可以显著提升预测准确度和稳定度。这对于发电调度，特别是对清洁能源的利用具有极其重要的意义，也就是说，如果预测不准确，对于拥有水电资源丰富的地区，很可能就会造成弃水发电的问题，同时也不利于清洁能源的利用与环境的保护。

以下是在某省级试点城市，用一组数据进行预测，算法采用传统的 Holt-winters 指数平滑方法和本文方法对水位进行预测比较，分别比较两个纬度：一是模型的稳定程度；二是实际预测的准确程度。比较结果如图 12 所示。稳定度指使用模型分别用训练数据和测试数据进行预测的结果是否接近，如果接近，模型是稳定的，反之，模型是不稳定的。衡量方法可以用预测的损失或代价函数的百分比差异计算，即 100%减去损失函数差异比例率。预测准确度，这里指拟合结果，即实际与预测各时间点的平均绝对百分误差。从以上试验结果看，本方法效果明显优于传统方法。

本文应用研究后续需要进一步改进提高，后续主要关注以下问题。

- 数据源缺失或异常的填补或纠正，因为数据源的问题对预测影响比较大，目前历史数据缺失和异常还存在问题，补缺或纠正方法很多。有一种方法是利用历史实际发电与水位、来水对比，该方法更结合实际业务，其准确度有待验证。
- 特征变量提取，实际上，水位本身已经反映天气及季节变化，但更多的特征可以更好地反映水位的变化，今后，可以在此基础上研究其他环境影响变量，比如水库的渗水、不同季节的水蒸发以及其他地理地质影响，甚至灌溉等影响因素特征，并可进一步使用主成分 PCA 方法，选取合理特征及权重。
- 预测算法模型及参数调优，使用机器学习有许多算法，最近几年，神经网络独占鳌头，其中 LSTM 具有长时间记忆能力，对时间序列关系的分析具有一定优势，目前发展 LSTM 的变种也不少，但如何把控神经元个数、隐含层数

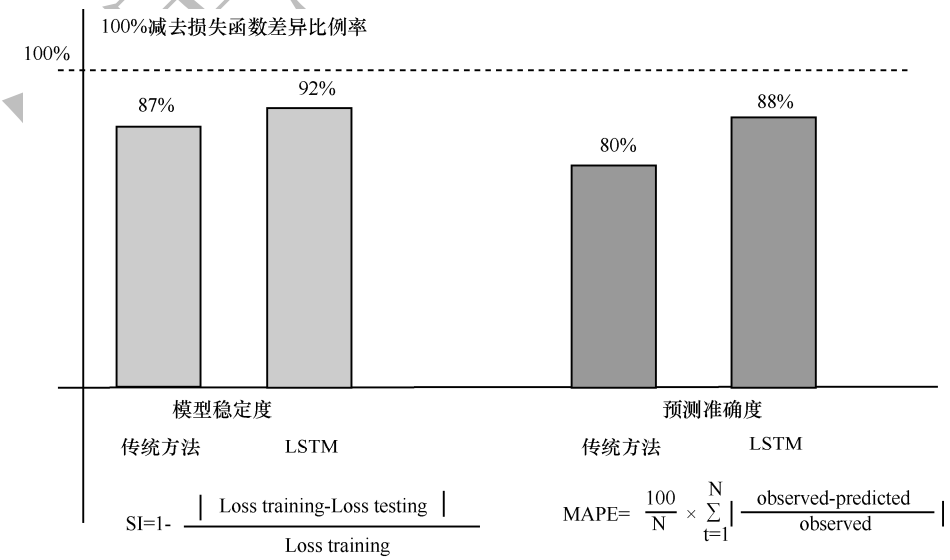


图 12　传统与本方法预测结果对比

及算法参数选择，找到更优算法还有待进一步探究。

- 关联算法，关联分析可以客观识别水库之间的波动关系，这比主观判断也许更好，因为水库之间不仅有上下游关系，而且横向之间关系也错综复杂，但是，这种关联的影响程度到底多大，或者说其支持度、置信度设置多少更加科学，这也需要进一步研究。

参考文献：

[1] 乔欢欢, 沈清, 黄永兴. 我国大力发展水电的必要性研究[J]. 能源环境, 2015(7).

[2] 王庆荣. 上海市水情中长期预测研究[D]. 南京: 河海大学, 004.

[3] 雷杰. 金沙江中游水电站水库中长期预报调度研究[D]. 北京: 华北电力大学, 2011.

[4] 王国锋，陈晓君，黄灵芝. 智能调度系统清洁能源接入及水电预测研究[J]. 华电气制造, 2015(2).

[5] 曾思明，吴杰康，陈永进. 小水电站流域径流量的评估方法[J]. 四川电力技术, 2019(2).

[6] ROGERSS, GIROLAMIM. 机器学习基础教程[M]. 北京: 机械工业出版社, 2014.

[7] 张亮. Python 机器学习基础教程[M]. 北京: 人民邮电出版社, 2018.

[8] 张树京, 齐立心. 时间序列分析简明教程[M]. 北京: 北方交通大学出版社, 2003.

[9] 罗序良. 基于 Holt-Winters 时间序列预测模型的电力大数据应用[J]. 机电信息, 2016(33).

[10] 杨建萍. 基于 ARIMA 模型的用电量时间序列建模和预报[J].工程数学学报, 2008, 25(4).

[11] 王美. 基于 Holt-Winters 指数平滑法的地下水水位预测[J]. 青年时代, 2016.

[12] 沙川. Holt-Winters 时间序列模型参数估计和预测[D]. 南京: 南京大学, 2011.

[13] 庞新生. 缺失数据插补处理方法的比较研究[J]. 统计与决策, 2012 (24).

[14] 崔贯勋, 朱庆生. 一种改进的基于密度的离群数据挖掘算法[J]. 计算机应用, 2007(3).

[15] 赵新想. 基于密度的局部离群点检测算法的研究与改进[D]. 武汉: 华中师范大学, 2014.

[16] 陆丽娜, 陈亚萍, 魏恒义, 等. 挖掘关联规则中 Apriori 算法的研究[J]. 小型微型计算机系统, 2000(9).

[17] 崔贯勋, 李梁, 王柯柯. 关联规则挖掘中 Apriori 算法的研究与改进[J]. 计算机应用, 2010(11).

[18] 唐寅. 长短时记忆神经网络模型改进[J]. 时代金融, 2016(24).

[19] 王书芹,华钢. 基于灰狼优化算法的长短期记忆网络在时间序列预测中的应用[J]. 中国科技论文, 2017(20).

[20] ZHANG YH, QIU CM. A Short-term load forecasting based on LSTM neural network[J]. Electric Power Information and Communication Technology, 2017(9).

人民邮电出版社

基于加权 Apriori 算法的电力光传输网故障诊断

吴宜聪，彭蔚，黄一双，黄舒畅
(中国能源建设集团广西电力设计研究院有限公司，广西 南宁 530000)

摘　要：电力通信网是保障电网安全稳定运行的重要基础设施，目前光传输通信系统在电力通信中占主导地位。光传输网的规模庞大、结构复杂、承载业务多样，因此难免发生众多的故障。本文根据光传输网产生的大量告警信息提出了一种基于加权 Apriori 算法的故障诊断方法，并通过实例仿真例证了该算法在保留出现频次极少但又十分危险的告警项和故障项以及诊断结果可靠性方面的优势。

关键词：电力光传输网；告警分析；Apriori；故障诊断

1　引言

随着电网向着自动化、智能化的方向不断发展，电力通信系统在电网的运行中发挥着愈发重要的作用。其中，光传输网作为电力通信网的核心部分，也成为了近年来国内外研究者探讨的热点。随着应用业务的扩展以及建设规模的扩大，光传输网发生故障的概率大大提升，而传统的故障诊断方法无法在很短的时间内对故障做出准确的判断，因此迫切需要有效的方法能够及时对网络进行故障诊断。光传输网作为一个统一的整体，每项功能的实现都需要整个网络的协调运行，任何一个结构出现了故障，都会导致整个网络相关部分发生一系列异常。因此可通过告警反映网络的异常状况，并对告警记录进行相关性分析以找到故障发生的根源。这就是基于告警分析的故障诊断。

随着近年来各行业对大规模数据的处理以及深度分析的需求，数据挖掘成为了研究者广泛关注的课题。数据挖掘是从大型数据集中挖掘出隐藏在数据中的人们事先不知道但客观存在的知识及规律，并通过挖掘出的规则进行相关决策。目前，数据挖掘已经被广泛应用于故障预警领域。参考文献[1-2]分别应用随机森林算法以及支持向量机不同的故障预测场景进行分析。参考文献[3]结合 MapReduce 技术和关联规则从检修工作分布情况、检修对业务的影响等角度分析通信网的检修方法。

对于海量告警记录的告警相关性分析，也需要使用数据挖掘技术作为实现方案。目前基于数据挖掘的告警相关性分析多采用关联规则的方法。参考文献[4]针对网络故障复杂、告警数据库信息量大的问题，应用基于 Apriori 的增量式算法减少冗余规则，提升告警规则挖掘效率。参考文献[5]通过 FP-growth 算法对业务支撑网的告警相关性进行分析，参考文献[6]针对频繁模式树加权出现的问题提出了 WPFPT-WARM 算法，更有效地进行了通信网告警规则挖掘。

本文采用了一种加权 Apriori 算法进行频繁项集的筛选。通过该算法得到的频繁项集能保留出现频次很少但实际上十分危险的告警项与故障项，使对电力光传输网的故障诊断更加可靠。

2　Apriori 算法

关联规则技术的一个经典算法是 Apriori 算法，该算法包括两大部分：筛选频繁项集和生成关联规则。某一项集 C 支持度大于最小支持度 $S_{\min}$ 时，该项集为频繁项集 L。Apriori 算法筛选频繁项集的原则是：任一频繁项集的非空子集也是频繁项集；任一非频繁项集的超集也是非频繁项集。筛选频繁项集是一个迭代的过程，第 k 次迭代在频繁项集 L_{k-1} 基础上生产候选项集 C_k，在 C_k 中寻找支持度大于 $S_{\min}$ 的项集成为频繁项集 L_k，直到无法产生候选项集为止。Apriori 算法逐级减少搜索范围，提高了频繁项集产生的效率。从最终的频繁项集中选择置信度大于给定最小置信度 $\mathrm{Con}_{\min}$ 的项集，组成有效关联规则集合。

3　基于加权 Apriori 的光传输网故障诊断模型

电力光传输网规模庞大且业务多样，导致产生的

告警类型丰富、数量繁多。通常一个故障的发生伴随着多个相关告警项的出现[7]。通过对海量的历史告警信息进行数据挖掘，获取隐藏在其中的规则并将此作为故障诊断的依据，很大程度上提高故障诊断的效率，减少用于故障检测带来的损失。光传输网的告警项分为网元告警、环境告警和性能告警。其中，网元告警指网络设备通过自检产生的告警，用于判断网元设备工作是否正常；环境告警指机房动力环境设备产生的告警，用于表明放置网络设备的机房环境是否可以继续满足设备正常工作的要求；性能告警是系统或设备指标超过阈值时产生的告警。

3.1 处理流程

基于加权 Apriori 的故障诊断模型如图 1 所示。

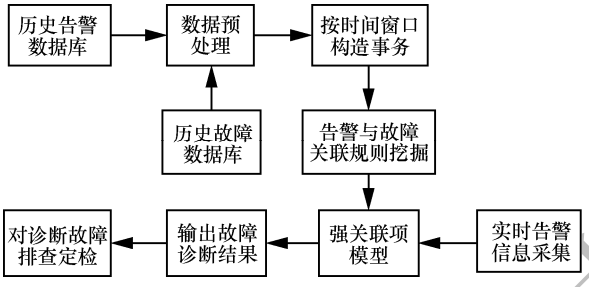


图 1　基于加权 Apriori 的故障诊断模型

3.2 数据预处理

根据历史告警数据库与历史故障数据库，提取其中具体项构造总项目集 I。假设全部告警项的集合为 X，告警项的总数为 m，全部故障项的集合为 Y，故障项的总数为 n，得到总项目集 $I=\{x_1,x_2,\cdots,x_m,y_1,y_2,\cdots,y_n\}$。

应用告警分析方法针对具体项进行预处理，建立总事务集。考虑以下两种类型[8]：

• 告警压缩：按照一定的原则将多个告警项压缩成一个告警事件；

• 告警过滤：过滤掉出现频率不属于规定合法值的告警项。

由于告警记录和故障记录都是时间序列，需要选定一个固定的时间间隔，将记录分成多个固定的时间段，称为时间窗口[9]，每个时间窗口包括多个告警项和故障项，且每个窗口的项经过告警压缩与过滤后仅在该窗口出现一次，这样的一个时间窗口便可看作是一个事务。所有的时间窗口构成总事务集 D。

3.3 权 Apriori 算法

传统 Apriori 算法在实际运用过程中存在着一个明显的问题：在事务总数据集中存在一些出现频次很低而被剪枝过滤的告警项，但事实上这些项往往隐藏着十分重要的信息[10]。因此采用一种改进的加权 Apriori 算法，将支持度乘上一个与概率有关的权值作为重新定义的支持度，进行频繁项集的筛选。权值仅根据 X 集中的项来确定。设 $w(x_i)$为 x_i 项的权值，定义 $w(x_i)=1/p(x_i)$，其中，$p(x_i)$表示 x_i 在事务集中出现的概率，即 $p(x_i)=\text{count}(x_j)/|D|$。对于多个告警项构成的 X 集的子项集 A，其权值 $w(A)$ 定义如式（1）所示，即该项集中所有 X 项权值的均值。

$$w(A)=\frac{1}{|A|}\sum_{x_i\in A}\frac{1}{p(x_i)} \tag{1}$$

具体的算法如下。

（1）扫描总数据集，将所有第一次扫描到的告警项加入 X 集，故障项加入 Y 集，记录每个项出现的事务数，并对所有 X 项根据权值大小进行降序排列得 $X'=(x_1',x_2',\cdots,x_m')$。

（2）将 X 项和 Y 项进行结合得候选 2 项集 C_2，重新扫描总数据集并记录所有候选 2 项集次数 $\text{count}(x_i,y_k)$，计算其支持度 S_2 如式（2）所示，给定最小支持度 $S_{\min}$ 并进行剪枝操作，得到所有频繁 2 项集 L_2：

$$S_2=\frac{\text{count}(x_i,y_k)}{|D|}\cdot w_i \tag{2}$$

（3）根据 L_2 中的 X 项 x_i 选出 X' 中排在 x_i 后面的所有 X 项 x_j，将 x_j 逐一与该频繁 2 项集结合构成候选 3 项集 C_3，重新扫描总数据集，记录所有候选 3 项集的次数 $\text{count}(x_i,x_j,y_k)$，并记录所有涉及到的 2 项 X 集的次数 $\text{count}(x_i,x_j)$，计算候选 3 项集的支持度 S_3 如式（3）所示，进行剪枝操作得到所有频繁 3 项集 L_3；

$$S_3=\frac{\text{count}(x_i,x_j,y_k)}{|D|}\cdot w(x_i,x_j) \tag{3}$$

（4）重复上述操作，直到剪枝后得到的频繁 k 项集 L_k 的个数为 0，得到所有的频繁项集；

（5）给定最小置信度 $\text{Con}_{\min}$，根据式（4）计算所有频繁项集的置信度，将置信度大于 $\text{Con}_{\min}$ 的频繁项集定义为强关联项集，算法结束。

$$\text{Con}=\frac{\text{count}(x_i,x_j,\ldots y_k)}{\text{count}(x_i,x_j,\cdots)} \tag{4}$$

人民邮电出版社

3.4 故障诊断

根据上述算法建立的由告警项与故障项共同构成的强关联项集，即网管系统的光传输网故障诊断模型。采集实时的光传输网告警信息并输入所建模型，系统生成当前光传输网的故障诊断报告，对诊断出的故障进一步排查可完成对光传输网的故障定检。

4 实例仿真与分析

4.1 告警项与故障项的选取

本文结合广西电网光传输网告警记录表中的部分样本进行仿真分析，选取一些告警项与故障项见表 1、表 2，x 项表示告警项，y 项表示故障项。

表 1 部分告警项表

项 ID	中文名称	告警级别
x_1	物理接口连接信号丢失	紧急
x_2	帧失步	次要
x_3	误码率越线	主要
x_4	支路单元告警指示信号	次要
x_5	信号标签失配	紧急
x_6	DCC 连接失败	紧急
x_7	远端缺陷指示	紧急
x_8	红外异常	次要
x_9	信号劣化	次要
x_{10}	发送失效	紧急
x_{11}	主备设备配置不同步	次要
x_{12}	定时输入丢失	紧急

表 2 部分故障项表

项 ID	中文名称
y_1	管理盘通信中断
y_2	设备倒换失败
y_3	网元脱管
y_4	电路通道故障
y_5	备板硬件故障
y_6	单元盘故障

4.2 仿真与结果分析

根据光传输网告警记录，选择包括上述告警项与故障项的时间窗口作为参考事务，构造事务数据集，并用一个只含有 0、1 的矩阵 D 来表示。该矩阵的每一行表示一个事务，每一列表示一个项，每个项对应的列即为它的项代号，元素 0 和 1 分别表示某一项在某时间窗口内未发生与发生。经过对告警记录表的分析，最终建立了一个 1 000×18 的 0-1 矩阵 D 进行仿真分析，并设置最小支持度为 0.4，最小置信度为 0.6。

通过仿真所得的结果为所有强关联项集。经过本文算法筛选，提取出其中具有参考意义的强关联规则见表 3。

表 3 本文算法筛选的关联规则

序号	告警项	故障项	置信度	加权支持度
1	x_1,x_2,x_5,x_7	y_1	0.900	0.625
2	x_4, x_{12}	y_2	0.900	0.642
3	x_1,x_4,x_6	y_3	0.889	0.500
4	x_3,x_9,x_{10}	y_4	0.875	0.875
5	x_8	y_5	0.857	0.857
6	x_6, x_{11}	y_6	0.800	0.516

该表反映了与每个故障项强关联的告警项，并给出了每一个强关联规则的置信度，表示当前网络某种告警状况下各个故障可能发生的概率。例如，某区域光传输网当前时间段发生的告警有物理接口连接信号丢失 x_1、帧失步 x_2、信号标签失配 x_3 与远端缺陷指示告警 x_7、支路单元告警指示信号 x_4、DCC 连接失败 x_4 以及定时输入丢失 x_{12}，那么由关联规则 1、2、3 可以诊断出该区域光传输网发生的故障为管理盘通信中断、设备倒收失败以及网元脱管。

另外，由表 3 可以看出，本文算法各强关联规则的支持度都很大，而传统 Apriori 算法设置最小支持度时如果设置过小则达不到筛选的目的，而设置过大则会过滤掉很多强关联规则。本文根据每个项的出现频次给予每个项一定的权值，出现频次越少的项获得越大的权值，这样就解决了传统算法中支持度的问题，使挖掘得到的强关联项集更加全面可靠。

5 结束语

随着电网向着智能化的方向发展，电力通信网业务也呈现爆炸式的增长，对电力通信网的故障诊断也提出了更高的要求。以电力通信网的核心部分光传输网为例，通过数据挖掘技术中的关联规则算法对告警相关性进行了分析，将告警项与故障项之间的关联作为故障诊断的依据，为快速查找、定位网络故障提供了可行性，具有一定的实际意义。

提出的基于概率加权的 Apriori 算法得到的频繁项集可以保留那些由于出现频次太低而被过滤掉的关

人民邮电出版社

联规则，因此保证了该网络告警故障关联规则的完整性与可靠性。经过仿真验证，该算法可以有效而全面地找出告警与故障之间的关联规则，适用于建立网管系统故障诊断模型。

参考文献：

[1] 吴海洋, 缪巍巍, 陆智敏. 基于随机森林算法的电力骨干通信网故障诊断研究[J]. 信息通信, 2018(12): 218-220.

[2] 刘松国, 韩树新, 李伟忠, 等. 电梯运行状态监测与故障远程报警系统研究[J]. 自动化与仪表, 2011, 26(10): 42-46.

[3] 杨志敏, 吴斌, 舒然. 基于大数据处理技术的电力通信网检修工作分析方法[J]. 电信科学, 2015, 31(11): 172-179.

[4] 李金凤, 王怀彬. 基于关联规则的网络故障告警相关性分析[J]. 计算机工程, 2012, 38(5): 44-46.

[5] 赵学健, 熊肖肖, 张欣慧. 不确定数据频繁项集挖掘算法研究[J]. 计算机技术与发展, 2019(7): 1-6.

[6] 罗明, 孟传伟, 黄海量. 基于加权频繁模式树的通信网络告警规则挖掘方法[J]. 计算机工程, 2016, 42(4): 190-196.

[7] STERRITT R, SHAPCOTT C M, ADAMSON K. High speed network first-stage alarm correlator[EB]. 2000.

[8] 黄灿, 王东, 殷舒怡. 基于气象数据挖掘的输变电设备故障预警[J]. 新型工业化, 2016,6 (5): 33-39.

[9] 李彤岩, 肖海林, 李兴明. 通信网告警加权关联规则挖掘算法的研究[J]. 电子科技大学学报, 2008, 37(6): 807-810.

[10] 高会生, 李英敏. 基于综合相关置信度的告警关联规则挖掘[J]. 电信科学, 2014, 30(10): 110-115.

人民邮电出版社

基于开源平台的 Docker 安全性分析

徐孝晋，伍泽军，邓文杰，陈霄楚
（中国广核电力股份有限公司，广东 深圳 518026）

摘　要：数字化转型时代背景下潜藏无穷的技术发展力。近年来，受到业界追捧的云计算和大数据技术孕育出各种不同类型的容器技术。Docker 开源技术凭借着超轻量级、高效部署以及简便的迁移特点被广泛应用。对 Docker 技术的发展进行了简要介绍，针对 Docker 安全方面展开详细论述，最后阐述结构安全方面的部署指南及预防措施。

关键词：容器技术；Docker；轻量级；安全性

1　引言

容器的应用受安全浪潮影响，同虚拟化技术一样，在安全方面不是一蹴而就的，是一个循环渐进的过程。容器的优点主要得益于资源设计、管理以及利用上的突破。同样有着虚拟化技术的身影，但是它却和传统的虚拟化技术有明显的区别，例如高效部署和低开销。

本文所述的 Docker 类型的容器在应用层实现信息隔离，在资源开销以及使用的便捷性上有优势。但由于 Docker 技术产生比较晚，成熟度欠佳，因此也就带来了诸多安全问题。

2　Docker 内部结构和技术

Docker 从狭义上的定义就是进程，从广义方面的理解是虚拟容器，Docker 是一个应用容器，它的组成部分可以拆解为进程和构建的应用镜像文件，容器与宿主机结构如图 1 所示。

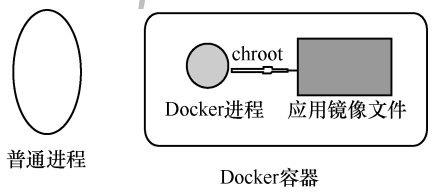


图 1　Docker 容器与宿主机

Docker 与虚拟化不同的理解，在于它通过上层的应用实现软件虚拟，并且构造十分轻盈，初看整体结构犹如虚拟化的虚拟机，Docker 的架构图层如图 2 所示。

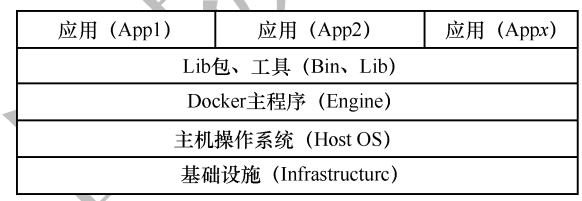


图 2　Docker 架构

Docker 的层级很清晰，与虚拟化平台的虚拟机在同个层级，但是它提供的是单用户资源，有别于虚拟机的多用户混合多租户类型。在实际的应用场景中它所提供的隔离粒度并不丰富。Docker 本身是自由软件，而且处在上层，因此它不与硬件直接打交道。它利用操作系统的资源隔离机制，通过 Docker 引擎调用接口完成资源隔离。它运行的过程只利用一部分基础设施的资源，因此 Docker 在系统中对资源的开销小、启动速度快、部署与迁移十分高效，目前 Docker 原生态只能在 Linux 发行版的平台支撑下应用。

进一步对 Docker 架构进行剖析拆解，从上层调用底层的视角剖析，如图 3 所示。

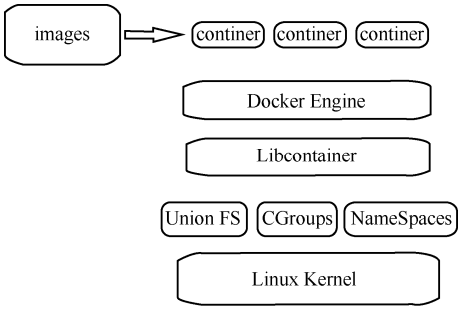


图 3　操作系统层

人民邮电出版社

Docker 容器依托的 Host OS 层：Linux Kernel 有 3 项技术支撑 Docker 容器。NameSpaces 充当隔离的第一级，让容器拥有独立的 Hostname、IP、PID，同时各进程直接相互独立，互不干预；CGroups 是容器对宿主机资源进行核算并对其有一定限制的关键功能；Union FS 是对镜像（容器的 image）的支持，采用 copy-on-write 技术。Libcontainer 则提供相关的库，作为下层的技术封装。

基于开源的容器生态系统尚不支持 Windows，其主要源于 Linux 内核的平台转换。从技术上，Linux 分为内核态和用户态，Docker 容器的设计是为了独立地完成一个应用或一组应用，本着进程的动态和静态不同模式构建而来。因此 Linux 的内核态提供上层的技术封装容易实现，并且基于内核的稳定性是通过开源手段实现独立且能共享的最佳选择方案，并且只要通过自由软件包解决依赖问题可以很容易实现容器的迁移和后期管理及扩展问题。相对于 Windows 的闭源模式，从商业和技术上是受到阻隔的。

3 Docker 安全性弱点综述

本文研究的内容是针对容器的安全性问题，平台构建和部署基本不涉及。对于 Docker，相比重量级虚拟化技术，容器技术实现的是非硬件级虚拟化。但是它的实现和设计原理，是将主机内核进行隔离。相比传统虚拟化技术才具有更高的安全性，主要在于传统的虚拟化技术是围绕虚拟机内核通信处理，阻断主机内核层的通信。而容器技术没有这个限定。由于容器技术的主机内核呈“曝光式”，因此攻击者也就可以直接对内（主机内核）发动恶意攻击，无需绕行。直接参与主机内核处理的过程便是容器安全性的关键问题所在。

既然容器存在这样的风险为什么还要努力探索？对此的理解是：缺陷补偿。可以动员所有的技术力量对抗局部问题，并进行修复。有效数据显示，Docker 容器技术是目前所有容器应用中的桂冠。对于它的深入理解，通过以下内容进行介绍。

3.1 Host OS 弱点

开源系统的内核实现底层硬件的分管和支撑上层接口系统的调用。Docker 容器既然可以和主机内核打交道，内核就可以通过调度管理着所有容器的进程和操作。

如果在内核层出现了弱电，则 Docker 容器所运行的应用程序直接面对攻击的威胁，容器的共享结构体将直接曝光。经探查，对于专业研究容器的团队，他们可以利用特权发起重定向或劫持攻击，包括容器在内的主机平台将受此威胁。

目前，Docker 同样重视安全问题，官方通过加固方案解决内核级漏洞，例如在构建上加固，通过运行 Docker Engine 时执行 App Armor 或 SElinux 设置。若可以接受牺牲业务通信，可将文件系统状态设置为只读，并关闭通信。除此之外通过白名单策略限制软件包的应用也是减小风险的较佳方案。

3.2 拒绝服务攻击

造成拒绝服务的条件是资源合法性开销，并且资源共享，单一任务造成资源无法合理地进行收场，例如将所有的访问权限均消耗在一个计算单元，导致队列其他的任务无法正常运用。把基于容器中的内核共享作为一个大的单元，对于其他的容器目前无法运转，在这种近乎“饿死”其他容器的状态下，判定已满足拒绝服务条件，业务随时可以瘫痪。容器的体系结构是内核资源共享，因此该类风险无法躲避。

有可选方案解决：文件系统隔离、进程隔离、设备隔离、网络隔离和控制资源分配及在网络上通过流量清洗技术（上层协议）解决。图 3 操作系统中的 Cgroups（控制组）是可以解决此类问题的有效办法，它的设计主要是提供一种计算方法来限制每个容器的资源，保证磁盘读写、CPU 运算及存储器的管理，保证资源的合理性开销及针对每个容器的资源约束与标准设置。

3.3 横向提权

横向提权常用来作为扩张性渗透，但是在容器技术中，可以将其理解为横向突破，它可以利用单个容器的攻击获得合法性利用后，将权限传递到其他容器进而转移攻击。

因为容器可以通过调用相应的函数，发动攻击以此绕过 simfs 限制。通过容器获取的权限进行提权或使用超级权限访问主文件系统上的目录树，此类风险的攻击，可以认为横向提权。官方指导建议，通过将 Docker 版本升级 0.12 以上便可修复。

3.4 镜像投毒

镜像投毒是伪造的一种攻击方式，因容器镜像版本过低易受侵害。镜像采用系统验证，该验证通过白名单的方式进行下载确认，更多地依托于校验。一旦攻击者劫持了镜像并进行投毒后伪造签名一起返回请

人民邮电出版社

求端，请求者无法辨别，对签名信任后，引起镜像中毒。该问题容易造成潜在的后果影响，就像是蠕虫，由于它可能会被再次依赖而很快扩散。Docker 的镜像是从 HTTPS 服务器下载，通过守护程序中一系列的管道传递，在内部不受安全管束，因此中间存在被利用的风险。

只要稍加不注意通过社区或非官方渠道获取恶意的镜像升级包，需要小心辨别镜像代码。通过信任的渠道下载，这主要通过人为意识和经验判别。另外还有一种更专业的做法：选择在本地阻止 index.Docker.io，该方法同样可以在 Docker 加载导入 Docker 平台之前鉴别、下载。

3.5 密钥泄露威胁

SQL 注入是 Web 常见的危害比较大的漏洞，可以导致整个数据库被脱库。容器的安全威胁之一在于密钥窃取和数据库密码泄露，这个影响是非常巨大的。当攻击者通过遍历文件目录或通过社工学套取了密钥或数据库的密码情况下，利用撞库、密钥传递技术在系统层面实施密码破解。因为 Docker 是一个可运行多个容器，此类漏洞可以不断扩散，如果攻击者盗走了管理员的账号和密码，则可以尝试做任何事情。

通过设置容器文件系统为只读，可以降低数据改写的风险。密码设置多管制，多因子认证技术可能帮助不了容器本身的密码安全，但是可以将共享机密的方式通过最小化权限细粒度的管理，人为地运行没有特权标志的容器可以减小伤害程度。

3.6 中间人攻击

中间人攻击是一种在正常通信中双方建立的欺骗、嗅探、伪造的第三者，在容器安全威胁中以篡改镜像为目的，在传输的过程中镜像可能遭到篡改。对于此类的攻击采用网络隔离技术是有效预防方法。目前新版本的 Docker 已经提供了校验机制来预防这个问题。通过 TLS（传输层安全协议）加密实现虚拟专用网络（VPN）方案，该方案用途非常的广泛，并且技术在不断演进。在日常中访问一个安全的网站 URL 的开头所使用的 HTTPS 就是嵌入了 TLS 加密技术。

Docker 直接采用了封装 OpenVPN 服务器方案。该方案可以直接操作 OpenVPN 服务器进程与数据管理。

4 安全机制与构建

人造系统没有绝对的安全。因此了解产品、深入理解安全性有助于提高人为设计的安全理念，通过采取预防性安全措施可以减少面对漏洞带来的灾难。本节主要对 Docker 平台构建和部署在安全性方面如何加固进行阐述。

4.1 内核更新

Docker 是直接和内核资源组及系统调用交互，因此内核直接影响了 Docker 的安全。有些软件系统设计不良，常曝光零日漏洞、官方无法及时解决补丁等问题。内核的版本应该是越新越好，这样可以直接解决内核级漏洞问题。至于版本的迭代问题可以交给专业人士。

对于不同的发行版，更新内核与系统的指令各有区别，例如 debain 和 ubuntu 的软件采用 sudo apt update&&apt upgrade，对于 redhat、centos 的软件，则使用 yum install，但是前期做好业务数据的备份，提供国内最好的 YUM 仓库是非常重要的。在有些版本操作系统中，如果通过将内核与 GRSEC 或 PAX 结合使用，可以有效地防范内核损坏错误导致的业务数据丢失问题。

4.2 Cgroups 安全机制

Cgroups 安全机制主要是防止拒绝服务攻击，通过提供一种计算方法对每个容器的资源进行限制。避免单一的容器分配过多导致资源被“合理化”利用而失控。关于操作样式基本参考如下：

CPU 使用率：docker run -it --rm --cpuset=0,1 -c 2 ...

内存使用率：docker run -it --rm -m 128m ...

4.3 访问权限控制

在 Docker 构建过程，小心控制权限的最小化。如前文所综述，设定文件系统只读是一个良策，但是可以通过具体配置、规划进行进一步控制，把它划分以下几个类别。

（1）SELinux/AppArmor

Docker 提供 Linux 内核安全模块，如 App Armor 和 Security-Enhanced Linux（SELinux），通过设置内核模块安全策略进行资源控制。可以设定配置要求，进行访问控制以限制系统资源。一般的 Linux 系统都会自带 SELinux 工具，通过标签来管理内容。在 Docker 系统中，每个进程、文件/目录和系统对象都有一个标签，可以通过编写规则限定进程和对象的访问属性。

而提供的 App Armor 也是一套安全策略控制方案，它是对程序进行控制。可以在 Docker 中新通过添加安全参数实现关键实例的配置。

（2）特权控制

施行--privileged 命令控制。因为增加--privileged

命令可以允许容器访问主机上的所有设备，并且它将为容器提供显式 LSM（即 AppArmor 或 SELinux）配置。拒绝使用带--privileged 的命令可以帮助提供安全性。建议合法用户应该使用-u 选项启动守护程序，它可以减少容器内强制执行的权限。类似 ubuntu 的 sudo 命令设定合法用户权限的使用是在环境变量上设定了访问关卡与记录。例如：

>docker run -u -it /bin/bash

存储使用率：>docker -d --storage-opt dm. basesize= 5G

4.4 Docker 镜像安全

在安全性综述中提到的镜像投毒的安全问题上，其实 Docker 开发人员已经提供了一种在镜像仓库客户端使用证书认证的安全处理机制，可以检测攻击者投毒建立后门的恶意行为，并设定策略进行阻断。其实在 Docker1.3 及以后的版本中已经提供了加密签名支持技术，该技术可以发现镜像是否受到“污染”。这个方案目前相对比较可靠，在一定程度上起到降低可能的安全威胁，所以在构建镜像和引入镜像的过程需要从经过身份验证的下载源下载并支持加密签名。

4.5 安全保密措施

Docker 有个特权获取的方式，通过在 TCP 端口上运行 Dcoker 程序的通信进程，以实现任意人员访问容器内部。当然这些操作可以在构建的时候限制，需要确保已经充分使用了 SSL 加密协议以保证通信过程的保密性。另外可以对 Docker 组的权限管理进行控制，审计组内账户的安全行为，通过在服务器系统上的防火墙设置部分指令集的阻断策略（如区域 IP 地址访问控制、端口号出入站规则等）。一旦允许任何人访问特定的端口以获得对容器的访问和控制，则可以容易取得超级管理员的权限，当获取 root 权限后，相当于从数据库引擎中获取了所有账号信息。因此采取监视组内账户的安全行为审计，可以预防未授权的账号交叉利用，以达到防止数据泄露的目的。

4.6 日志审计

开启系统、应用、安全等日志记录和审计，设定保留的存储大小或周期数，可以提高异常追溯的可靠性。这种作为额外的保护策略，虽然需要有日志存储介质作为开销，但是一旦出现入侵或破坏迹象，可以达到监视的效果。当然需要另外考虑一步，是定期还是实时对日志进行灾备，以防日志记录被清洗。

4.7 服务安全控制

服务本身也是一种程序，通过运行被抽象为进程，服务之间往往不是单独运行的，若由于依赖关系容器运行了诸多的敏感服务。一旦服务被植入后门或种植代理，可长期潜藏利用。例如攻击者一般会在尽可能短的时间内进行进程迁移，对于 Linux 进程的父进程，一旦被植入后门运行，则只有重启服务器由攻击者自愿放弃才能解除威胁或已经完成了长期代理植入提供反弹 shell。前文介绍过的，操作系统的安全是相对存在的，永远没有绝对的安全。可以在应用层进行相对安全的保护，比如在容器内设定白名单，以限制不受信任的用户运行管理员权限；对远程协助类服务在非使用期间关闭。

4.8 Docker 内容信任

从官方文档了解到，Docler1.8.0 版中已经添加了内容信任一项新功能，该功能为容器提供外部的安全保护措施，即对用户在下载 Docker 镜像之前进行合规性检查。

4.9 全面虚拟化升级

虚拟机的应用相对容器虚拟化更加安全，但是资源的开销是相当浪费的。如果采用全面升级虚拟化技术，让资源力量得到充分扩展，可以将风险压得更低。值得庆幸的是，开始 Docker 已经提供了 KVM 虚拟化层的功能，并且技术不断地演进。

5 结束语

人们一直在研究如何最大化地利用资源，因此出现了虚拟化，为了应用的合理化使用又出现了容器技术。如今，对 Docker 带来的安全性问题进行探讨，希望有朝一日安全问题得到彻底解决。但落到实际，围绕 Docker 类型的容器安全问题继续讨论，并努力构建部署方案来解决问题。与此同时，也提供了一些安全部署策略思路。相信随着技术的演进，这些问题终将作为能源企业、互联网发展的推动剂。

参考文献：

[1] 郭甲戌, 胡晓勤. 基于 Docker 的虚拟化技术研究[J]. 网络安全技术与应用, 2017(10): 28-29.

[2] 李娜. Docker 容器技术的发展及应用研究[J]. 数字技术与应用, 2018, 36(11): 95-96.

[3] 鲁涛, 陈杰, 史军. Docker 安全性研究[J]. 计算机技术与发展, 2018, 28(6): 115-120.

人民邮电出版社

基于“零信任”的工业信息安全防护研究

向人鹏
（北京天地和兴科技有限公司，北京 100193）

摘　要：工业信息安全、工业控制系统的网络安全防护，已经成为了当前国内外网络安全研究的热点话题。在当前工业 4.0、智能制造、两化融合等大背景下，物联网、云计算等技术与工业生产深入融合，传统意义上的边界、相对隔离的控制系统已经不复存在，针对国家关键信息基础设施、工业控制系统、智能无线终端等工业生产环境中重要的系统、设备，已经成为了安全研究人员漏洞挖掘、攻防研究新的对象。“零信任”框架的特征，与工业信息安全的防护理念极为相似，重点探讨构建工业控制系统的“零信任”框架以及在其下打造工业控制系统的安全可信区域的可行性。

关键词：工业控制系统；“零信任”；安全

1　引言

我国自 2011 年 9 月工业和信息化部发布《关于加强工业控制系统信息安全管理的通知》（工信部协【2011】451 号）后，就已经进入了工业信息安全行业高速发展的时期。近年来，随着国家对工业信息安全项目的投资、政策支持日趋饱满，各行业协会、产业联盟、安全服务/产品厂商的积极参与，工业信息安全的防护手段已经从单纯的依靠防火墙、网闸进行区域隔离，发展出了以工业防火墙、安全审计为主的被动防御体系，以可信计算、终端加固为主的主动防御体系以及多重防护做支撑的纵深防御体系。

随着 2016 年《工业控制系统信息安全防护指南》（以下简称指南）、2017 年国家《网络安全法》、新的等级保护 2.0（送审意见稿）的颁布，对于工业控制系统的安全防护有了更多指导性的意见，文中旨在依托于国家政策标准文件，结合现行主流的防护手段，讨论在“零信任”框架下建立可信的工业控制系统的可行性。

2　工业控制系统安全防护主流技术体系

2.1　被动防御体系

被动防御体系下的信息安全防护依靠工业防火墙、工业网闸等通过对关键网络节点和数据流量出入口进行访问控制和权限控制，通过策略的部署调整来实现系统的安全防护建设[1]。

常用的防护手段如下。

（1）区域隔离

通过在工业控制网络与外部网络之间建立物理的或逻辑的访问控制手段，实现对工业控制网络的相对隔离。在当前工业互联网、两化融合时代，随着物联网、云计算等技术在工业控制领域的推进，工业控制系统与外部网络在物理上的隔离不复存在，单纯的区域隔离手段已不能满足当前安全需求。物理隔离通常由工业网闸等实现，对传输方向有要求；逻辑隔离一般采用 VLAN 及工业防火墙实现，部署简单，适用性强。

（2）边界防护

一般企业中的工业控制系统内外会根据业务流程、数据流量内容等划分不同的区域，这些由业务内容不同而形成的区域化的网络结构需要在区域边界采取必要的防护手段，进而能够有效地控制各区域边界出入的数据和流量的安全。

边界防护作为被动防御体系的核心，除通过工业防火墙等实现以外，还需要部署能够对常见类型的威胁和攻击以及未知威胁和 APT 攻击行为进行有效监测防护的检测防御设备。

（3）主机防护

工业控制系统内的上位机作为对底层控制设备进行直接控制、监控的设备，是黑客们重点关注也是目前工业控制系统内受到攻击最多的风险点。通过对主机的操作系统、物理环境进行加固，关闭与生产业务无关的端口和服务来实现端口和服务最小化，从而降

人民邮电出版社

低潜在的风险来源。

（4）安全审计

安全审计要求包括对安全事件和数据流量的审计记录，对安全事件的溯源追踪，也包括对工业控制系统内的漏洞进行扫描和修复，特别是在当前世界范围内对工业控制系统漏洞的研究逐渐深入的环境下，对于安全审计的部署尤为重要。

2.2 主动防御体系

主动防御[2]作为与被动防御相对应的概念，通过对控制层、网络层、监控层的主动防护及关键信息的提取，实现在入侵行为对工业控制系统发生影响之前就能够及时精准地进行预警，进而降低、规避、转移工业控制系统所面临的安全风险。目前国内两大构建主动防御体系的思路是可信计算技术和白名单技术。

（1）基于可信计算技术的主动防御

安全可信采用主动免疫的计算架构，以密码为基因实施身份识别、状态度量、保密存储等功能，及时识别“自己”和“非己”成分，在主动免疫可信计算架构下，建立安全计算环境、安全边界、安全通信网络的主动免疫三重防护框架，做到可信、可管、可控，以此构建可信计算环境下的工业控制系统主动防御体系[3-4]。

（2）基于白名单技术的主动防御

工业控制系统环境下的白名单，通常是指文件、工业控制软件程序、进程、服务级的白名单。白名单的配置通常以业务流程为中心，通过对业务软件、应用行为进行监控与防护，实现在控制层、网络层的信任传递。构建以白名单为基础的主动防御体系，能够有效地对应用进行管控，防止业务应用被恶意软件、木马等破坏，实现比主机加固更好的安全效果[5-6]。

2.3 纵深防御体系

纵深防御通常会将工业控制网络内的资产划分为不同的安全域，通过不同功能的安全产品的堆叠部署、协同防御，最终得到立体的、全面的、连续的工业控制安全防御体系[7]。

纵深防御的关键是加强安全域的边界防护，在不同安全级别的域间配置不同的防御措施，首要目的是阻止安全事件的发生，同时应具备危害控制、应急响应措施，以保证在阻断失效时可及时响应，将安全事件的影响降至最低。

3 “零信任”框架下的可信工业控制系统

“零信任”网络模型是约翰·金德维格在 Forrester 时于 2010 年提出的，谷歌也在 2011 年启动了 BeyondCorp 计划，该计划旨在构建基于“零信任”模型的安全架构，该计划的核心理念是最基本的身份安全认证应该基于受控的设备和合法用户，而不是基于网络访问控制，即传统的网络安全手段。

“零信任”作为一个新的安全概念，已经逐渐被安全研究人员、企业 CIO、CISO 所接受，其中心思想是来自于企业网络内部外部的行为、数据流量、移动介质均不应被信任，在验证身份并授权之前任何试图接入企业网络的行为、数据流量、移动介质都是不可信的。简言之，在“零信任”模型下，任何操作行为、用户、数据流量等在公示自己的清白授权之前都应被拒绝在系统或网络之外。

3.1 “零信任”的必要性

国内越来越多的工业企业在国家的号召下已经开始关注工业控制系统的安全，诸如电力、智能制造等行业也都开展了各自的试点示范项目，可是在 ICS SERT 披露的报告中可以发现，虽然国内外工业控制安全领域的先行者们已经部署了一定的工业控制安全防护手段，但是工业控制安全事件发生的频率并没有降低。有趋势研究显示，虽然来自网络的威胁仍是工业控制系统的主要威胁来源，但是来自企业工业控制系统内的风险已经不容忽视。随着黑客们对工业漏洞的研究，越来越多的工业设备及其工业控制软件、工业协议暴露出了其易受攻击的不稳定性。同时，工业生产的特性决定了“人”也是生产流程中的一个重要环节，绝大多数的工业现场，如汽车制造流水线、炼油厂装置现场操作室都需要工程师长时间的驻守，在生产停工检修期间还需要大量第三方运维人员对现场设备、终端进行检维修。这些因素都使得工业控制系统的风险来源变得复杂多样，对于工业控制系统的防护不能够再单纯地依靠传统的防护理念。

工业控制系统计算机的主要威胁来源如图 1 所示，工业控制系统计算机的次要威胁来源如图 2 所示。

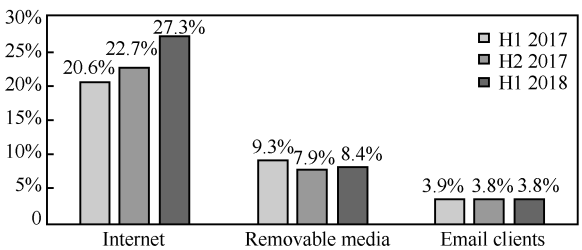


图 1 工业控制系统计算机的主要威胁来源

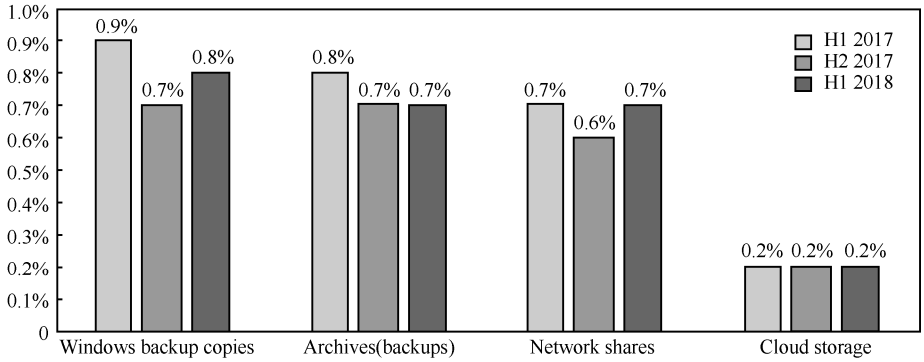


图 2　工业控制系统计算机的次要威胁来源

上文提到了目前 3 种主流的工业控制系统安全防护体系，一般来讲，企业在构建自己的工业控制安全体系时都会定义出清晰的边界，无论使用哪种方法，都会强化自己的网络边界防御能力来构建工业控制系统的城墙。但是随着云计算、移动互联等技术的进入，现场无线热点、智能终端的增多，传统的边界防护在这种复杂多变的新环境下很难发挥作用，层层保护的工业控制系统可能已经暴露在外，安全的边界也会变得不再可信。

当然，黑客攻击和复杂的未知威胁不是驱动“零信任”概念的唯一因素。工业控制系统网络的特性也保证了“零信任”概念在工业环境下的适用性。

工业信息安全的本质是保证生产控制环境的可信，进而才能够保证工业生产的持续性。现代化、自动化的工业生产流程依赖于控制设备，在冗长的工艺流程中，任何一环的变化、中断，都会导致当前生产流程被破坏，严重的会使工厂停产，带来巨额的直接或间接经济损失甚至危害国计民生。这就意味着在工业控制系统内部，企业所面临的安全风险一方面来自于外部的网络攻击、内部的病毒感染传播；另一方面，内部人员的误操作和恶意破坏、数据泄露一直是企业安全的巨大挑战，长期以来都没有好的解决方案。也就是说，工业控制系统相对隔离的内网是可信区域的传统看法会使得企业面临更大的风险。

很多的安全研究者、企业高管们已经认识到了现有的安全手段和措施并不足以应对愈加严峻的安全态势，而“零信任”的出现可以很好地解决当前工业生产所面临的安全问题。因为，在“零信任”框架下，企业不需要担心用户从哪里登录，数据从哪里进入，不用担心攻击者在突破边界后潜藏于网络中进行破坏；在“零信任”的框架下，不以用户、数据的来源或地址为控制准则，其策略是建立在用户、数据、设备的属性、状态、身份的基础上，更注重用户的行为和设备状态的关联分析。

3.2　在“零信任”框架下打造可信工业控制系统

3.2.1　如何实现“零信任”

安全的本质是信任，而信任本身就是危险的漏洞，容易被攻击者利用。“零信任”框架下的安全应是由内而外的安全，而不是由外而内的安全，企业关心的是所要保护的设备、资产。打造“零信任”环境时应遵循的关键原则如下。

（1）任何人、设备、网络都不可信，应监视所有的用户、数据流量、设备，而不仅仅是外部用户、流量；

（2）在被验证可信之前，任何人、设备都不应访问关键资源，网络本身不应确定用户可以访问哪些服务、设备、资源；

（3）授权用户的信任，不应基于用户进行访问的源地址，而应基于用户信息、设备信息及其访问的资源信息；

（4）重点是用户验证、访问权限控制。

3.2.2　用户可信

工业控制系统的特点决定了网络内会有不同权限的工程师频繁接入监控生产状态、调整工艺流程。对于无论是内部还是外部接入的用户，首先要清楚用户的身份，保证用户是其声称的那个身份；其次要保证用户所使用的终端或设备是受信的，或该终端/社保处在安全状态；最后，还应有安全策略指定所保护的资产资源可以被哪些受信用户、终端访问。

“零信任”下的用户可信依赖多因子身份认证、身份与访问管理、加密等安全技术，应坚持最小权限原则，由内而外地进行控制。用户可信应实现的目标是通过安全技术来保证“无法证明可信即无法获得访

人民邮电出版社

问权限”。

以内部接入用户为例，在汽车制造、半导体生产等典型的流水线生产作业的企业中，第三方厂商的运维人员是日常生产流程的重要组成部分。当生产参数、工业流程发生变化时，需要第三方运维人员在生产现场接入工业控制系统或操作现场工业设备、终端。对于这些接入点的不可信用户，首先应限制其接入，对用户身份及其要访问的资源进行多次验证并授予权限，这些用户所使用的终端或设备也应按企业管理流程进行验证、杀毒、授权等操作，若这些用户需要在控制系统内部进行远程运维等操作，仍应该再次进行验证并与外部接入用户一样通过堡垒机等设备进行统一授权管理。

3.2.3 设备可信

工业生产环境中存在着种类丰富的设备终端，包括无线智能仪表、手持终端、移动终端、计算机、HMI、工业控制设备等，所有设备都应是受控设备，所有受控设备都需具备唯一身份标识。在设备全生命周期管理过程中，应全程跟踪设备的状态及信息，这些信息应可以被存储、保护、分析，并且可以在工业控制系统中共享，共享的对象主要是设备可能关联的业务、应用数据库。同时，设备的身份标识在匹配时需被二次验证证书存储的有效性，只有当一个设备被认为具有足够的安全性时，才可以称之为受控设备，只有合法的受控设备才可以在工业控制系统中发生行为。当然，设备的身份信息、证书应定期进行更新。

3.2.4 网络可信

工业控制网络作为企业网络中一个身份特殊的网络通常相对隔离并且会部署在专用网络地址内，工业控制网络仅会通过少数特殊的业务系统与外部网络连接，同时在这个连接过程中往往有严格的访问控制，访问控制往往基于业务需求。在“零信任”框架下，即使再独立、相对隔离的工业控制网络也是不可信的，网络对进入其内的受控用户、设备、数据流量的信任程度取决于这些用户和设备所关联的资源。如访问与数据采集相关的网络内资源，必须是具备对应身份标识的用户及其设备。由于内部与外部网络都被认为是不可信的，所以必须始终通过验证身份来判定会话是否合规，要做到始终验证，就意味着必须记录所有的流量。所以在网络层面需要借助成熟的安全技术来使得基于用户、数据、位置信息的细粒度策略访问控制、流量记录审计分析以及应急措施手段能够具备机器学习能力，最终打造动态访问控制的可信网络。

在石化行业中以炼油厂为例，一个炼油能力一千五百万吨左右的炼油厂通常包含催化、裂化、延迟焦化等十几个装置，每个装置的控制网络在原则上互相独立，但是受制于生产数据采集的需要，很多装置间的控制网络往往会通过数据采集网络连接起来并与外部办公网相联，这些链路往往是工业信息安全中最主要的风险来源。在“零信任”的框架下，即使是装置本身的控制系统网络，对于另一个不同装置的网络来说也是可能会影响到自身生产业务的不可信的网络。所以在炼油厂场景下，工业控制网与办公网之间，不同装置区域的工业控制网之间，都应该通过具备自主学习能力、安全可控的工业防火墙、网闸等隔离设备，结合安全审计、入侵检测等技术手段，并且以严格的管理制度辅助，对网络部署基于用户、数据、位置信息的访问控制策略、流量审计记录及适用于工业控制系统的应急响应措施。

4 结束语

大数据、云计算、物联网、人工智能为代表的新一代信息技术应用推动了工业生产的进步，同时也带来了工业信息安全的研究热潮。安全问题并没有随着技术的进步、时间的更迭变得更少，安全研究应不断学习工业环境下新的业务模式，用发展变化的安全思路去防范新业务形态下的安全威胁。文中结合现有传统防护体系，认为在“零信任”框架下打造可信的工业控制系统是未来值得发展的新思路。

参考文献

[1] 王昱镔, 陈思, 程楠.工业控制系统信息安全防护研究[J]. 信息网络安全, 2016(9): 35-39.

[2] 张大伟, 沈昌祥, 刘吉强, 等.基于主动防御的网络安全基础设施可信技术保障体系[J]. 中国工程科学, 2016(6): 58-61.

[3] 沈昌祥, 张焕国, 王怀民, 等. 可信计算的研究与发展[J]. 中国科学: 信息科学, 2010(2): 139-166.

[4] 邵诚, 钟梁高. 一种基于可信计算的工业控制系统信息安全解决方案[J]. 信息与控制, 2015(5): 628-633.

[5] 章翔凌, 王欢. 基于白名单技术构建主动防御体系[J]. 信息网络安全, 2013(10): 188-190.

[6] 汪锋, 周大水. 白名单主动防御系统的设计与实现[J]. 计算机工程与设计, 2011 (32): 2241-2244.

[7] 李辉.在线安全监测及纵深防御系统对工业控制系统安全防护的意义[J]. 2018(5): 20-21.

人民邮电出版社

基于流程匹配技术的库房管理调度系统

帅率，尹飞，宋煜，陈佐
（江苏方天电力技术有限公司，江苏 南京 211100）

摘　要：研究了一种应用于电力计量生产的库房管理调度系统，解决库房传输线利用率低和系统不够灵活的问题。运用流程匹配，获取任务单和特殊站台，匹配具体作业流程；通过库房调度，进行库房任务分配调度计算和传输线分配调度计算，生成搬运作业；使用半双工设备控制，下达搬运作业，指导搬运任务执行。最后经试验验证，所设计的库房管理调度系统流程匹配准确，调度算法精准，满足用户对库房管理的个性化需求。

关键词：流程匹配技术；任务分配调度计算；传输线分配调度计算；半双工设备控制

1　引言

随着计量中心生产统一调度管理的进行，对自动化库房空间利用率管控水平和生产效率保障提出了极高要求。为将库房纳入统一调度，提高库房的精益化管理水平，研究了一套基于流程匹配技术的库房管理[1-4]调度系统，用来解决复杂通信架构下传输线利用率低和系统不够灵活等问题，提升自动化库房运行效率和稳定性。

2　系统结构与原理

库房管理调度系统包括任务管理、库房调度和设备控制 3 部分。系统整体架构如图 1 所示。

任务管理层接收上层系统下发的出入库任务，将出入库任务进行细化分解，并将细化分解后的任务信息保存到数据库中；库房调度层进行调度策略配置，通过流程调度计算，生成出库搬运作业；设备控制层向库房调度层上报电控信息，接收库房调度层下发的搬运作业，对硬件设备进行管理。

3　系统硬件设计

库房管理调度系统设备层如图 2 所示，包括堆垛机、提升机、穿梭车、射频门、电控设备和输送设备等，主要通过 PLC 控制器、OPC 控制器来实际控制硬件运转，利用 OPC 和 Socket 通信技术将这些设备与生产内网进行关联，接入库房管理调度系统。

4　系统软件设计

库房管理调度软件系统主要实现任务管理、流程匹配、调度计算和设备控制等功能。

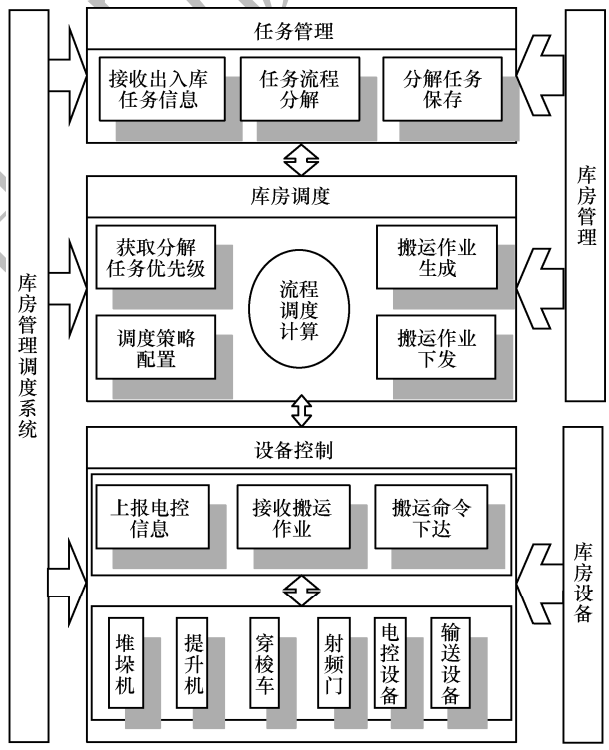


图 1　系统架构

4.1　任务管理

库房管理调度的目的是根据出入库任务指导资产出入库。第一步接收上层系统下发的出入库任务，将资产出入库任务按业务进行具体分类，包括库前区出入库、检定出入库和封印出入库。在接收到上层系统下发的出入库任务后，基于流程分解机制，根据具体业务将接收到出入库任务进一步细化，如将库前区出

入库又细分为整箱到货设备入库、空箱到货入库和设备配送发货出库，将检定出入库细分为检定设备返库、检定设备出库和检定空箱出库，将封印出入库细分为封印设备返库、封印设备出库和封印空箱出库，并将细化后的任务信息保存到数据库中，供库房调度使用。也可以根据具体的生产状况进行出入库任务进一步细分，通过对出入库任务进行分解，为库房调度计算提供科学依据。

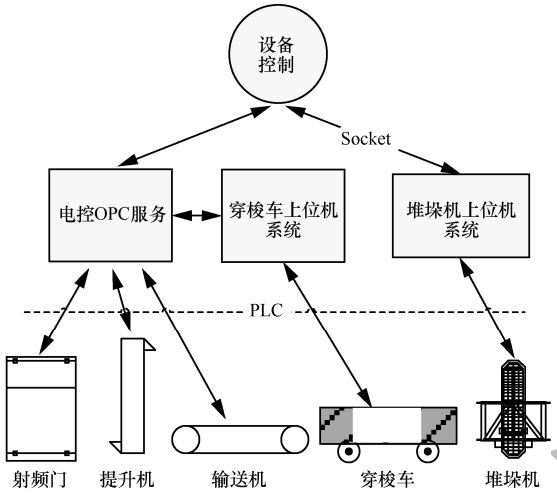


图 2　系统硬件设备

4.2　流程匹配

流程匹配是衔接任务管理和库房调度之间的桥梁，分为任务流程匹配和站台流程匹配。任务匹配流程如图 3 所示，是指根据获取的任务单中出入库类型字段，判断所属的出入库流程，出入库类型是对分解后的任务进行的类型定义，如果属于设备配送发货出库、检定设备出库、检定空箱出库、封印设备出库和封印空箱出库等库房出库业务流程，则需要调用调度算法生成出库搬运作业。

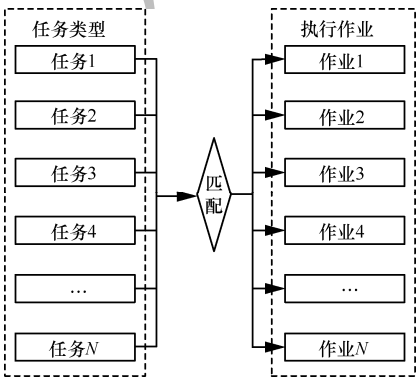


图 3　任务匹配流程

站台匹配流程如图 4 所示，指根据获取的特殊站台，匹配执行作业流程的过程。站台匹配通常用来辅助任务匹配流程，适用于任务匹配后仍然无法找到具体的作业，结合站台匹配进行精确定位。

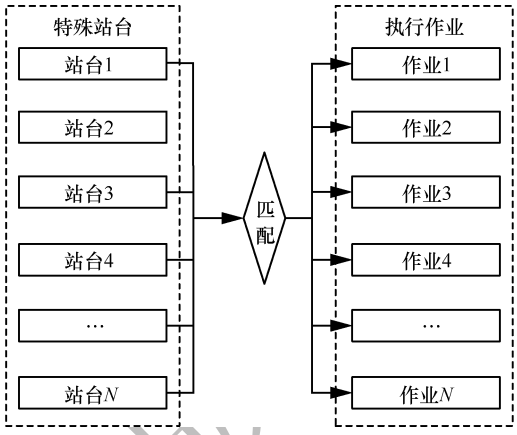


图 4　站台匹配流程

4.3　库房调度

库房管理调度[5]的核心在于流程调度计算，因为库房管理入库是实物驱动的方式，实物在传输线上流动的过程中，到达特殊站台会自动上报电控信息，生成入库申请单，所以入库流程产生的搬运作业，能够保证入库有序进行，不会造成拥堵，无需进行调度。库房管理出库搬运作业需要定时产生，如果不进行调度，将会造成任务执行混乱、库房传输线拥堵或传输线空置，这 3 种情况都会造成生产效率低下，所以针对库房出库业务流程进行调度控制，定时生成出库搬运作业就变得非常必要。

出库搬运作业定时生成规则采用了流程调度计算方法，包括任务分配调度算法和传输线分配调度算法两方面。影响任务分配的因素包括任务优先级和并行出库任务数，针对优先级不同的任务，采用优先级算法如图 5 所示，保证优先级高的先执行生成出库搬运作业。

如果任务优先级相同，采用任务片轮换算法，如图 6 所示，将任务分成作业片段，每个任务轮换执行生成出库搬运作业。

出库搬运作业不是无限制地生成，还需要结合传输线分配调度算法控制搬运作业生成节奏，当传输线正在执行的作业数达到传输线最大容量时，这时库房调度就停止生成搬运作业，只有当正在执行作业数小于传输线最大容量时，才重新生成搬运作业，这样可

人民邮电出版

以保证传输线利用率最大化。

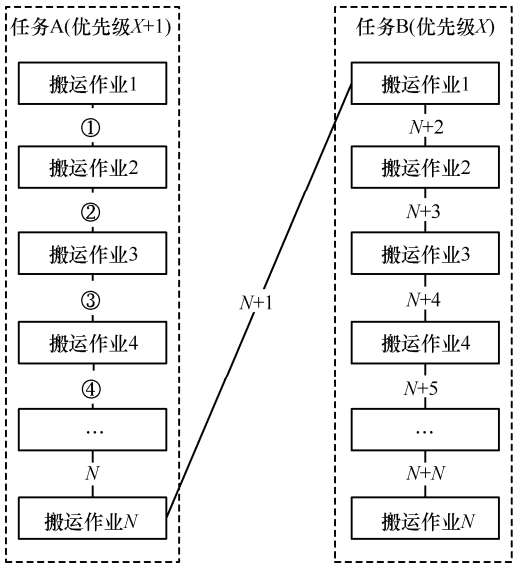


图 5　优先级算法

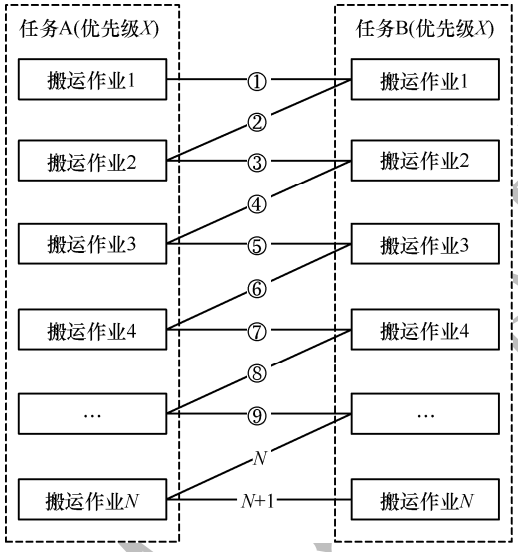


图 6　任务片轮换算法

影响传输线分配的因素包括：传输线流转速度、传输线最大容量、作业系数和执行作业间隔频率。执行作业间隔频率计算方法为：

$$R = \mu \times \frac{1}{V} \tag{1}$$

其中，R 为执行作业间隔频率，μ 为保证传输线利用率最高且正常运行的作业系数，V 为传输线流转速度。作业系数 μ 是固定的，如果提高传输线流转速度，则需要降低执行作业间隔频率 R。例如设备配送发货出库的传输线的作业系数 μ 为 10，传输线流转速度为 1 m/s，则计算出执行作业间隔频率 $R=\mu/V$ =10/1=10 s，将执行作业间隔频率设为 10 s 是最优的调度方案。

在执行搬运作业的过程中，不可避免会有异常出现，造成生产停滞，这时需要暂停生成搬运申请单，假设传输线最大容量为 Q_{max}，当前正在执行作业数 Q_c，差值为 Q_t，即：

$$Q_t=Q_{max}-Q_c \tag{2}$$

其中，Q_t=0 时，说明传输线正在执行作业数 Q_c 已经达到传输线最大容量 Q_{max}，这时库房调度就停止生成搬运申请单，等待一段时间（执行作业间隔频率 R）后，再次进行判断，直到 Q_t>0，正在执行作业数小于传输线最大容量，再重新生成搬运申请单。

4.4　设备控制

计量生产库房硬件设备包括堆垛机、提升机、穿梭车、射频门、电控设备和输送设备。在库房管理调度中，通过设备控制层[6]对硬件设备进行统一控制，库房管理层只需向设备控制层下达搬运作业，不必与硬件设备本身直接交互，简化了库房管理工作，同时保证库房管理系统改造升级的时候，不用再进行硬件调试，节约调试时间，保证了软件系统和硬件设备的独立性。

库房调度层和设备控制层之间的接口采用半双工模式，如图 7 所示。库房管理层接收到设备控制层上报的电控信息后，及时进行回复，然后单独启用新的线程进行流程调度计算，生成搬运作业，最后再次调用接口将生成结果通知设备控制层，设备控制层接收库房管理层下发的搬运作业，及时进行回复，并向各硬件设备下发搬运命令。

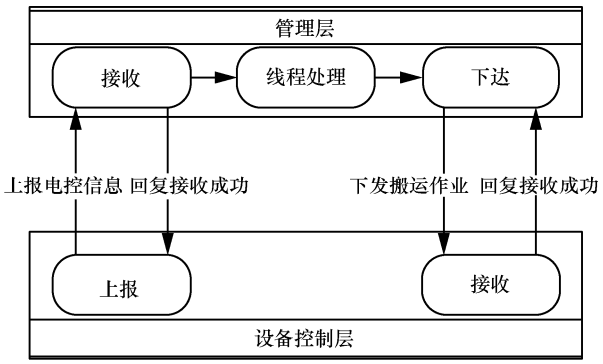


图 7　半双工交互模式

这种半双工模式能够减少设备控制层等待时间，

设备控制层接收到管理层回复接收成功信息后，可以继续走到下一个节点，不必等待管理层处理结果，另外这种接口处理方式还能够减少接口调用出错的几率，快速提高库房的运转效率。

5 系统仿真试验

为了进一步修正库房调度层的调度策略配置参数，保证参数在一个合理区间内，需对系统进行仿真实验分析，仿真实验包括流程匹配、调度计算和作业执行 3 个步骤，如图 8 所示，通过对仿真实验结果进行分析，根据分析结果对调度策略配置参数进行调整。

以库前区设备配送发货出库流程为例，因为执行中的配送出库任务会根据任务优先级进行降序排序，取优先级最高的任务，在仿真实验中，如果想控制设备配送发货两个出库口同时执行同一个比较紧急的出库任务 A，在策略配置中，将 A 任务优先级调至最大，并行出库任务数设置为 1 个，库前区传输线最大容量设置为 10 垛，执行作业的间隔频率 R 设置为 9 s，传输线平均流转速度 V 设置为 0.2 m/s，根据式(1)，可以推算出作业系数 μ 的值为 $R\times V=9\times0.2=1.8$，如果此时分析结果发现传输线利用率还不高，可以将执行作业的间隔频率 R 设置为更小的值，直到库房达到最大吞吐量，此时推算得到的 μ 值即可作为保证库前区出库传输线利用率最高且正常运行的作业系数。

以封印设备出库流程为例，因为封印线现在只支持一个执行中的检定任务，所以同时执行的封印出库任务优先级相同，并行出库任务数设置为 3 个，若存在多条优先级相同的封印出库任务，则执行前 3 条，传输线最大容量设置为 8 垛，执行作业的间隔频率 R 设置为 7 s，传输线平均流转速度 V 设置为 0.2 m/s，根据式(1)，推算出作业系数 μ 的值为 $R\times V=7\times0.2=1.4$，如果此时分析结果发现传输线存在拥堵的情况，可以将执行作业的间隔频率 R 设置为更大的值，直到库房封印出库线路拥堵解除，运行平稳，此时推算得到的 μ 值即可作为保证封印设备出库传输线利用率最高且正常运行的作业系数。

后期系统上线以后可以根据实际生产情况进行策略调整，得出更合理的值。

6 结束语

目前，本成果已在江苏电力计量信息化车间得到成功应用，系统将复杂的软件算法与单纯的硬件任务执行相结合，并对软件系统进行流程分解，做到灵活可配，既能保证系统通用性，又能够满足用户个性化

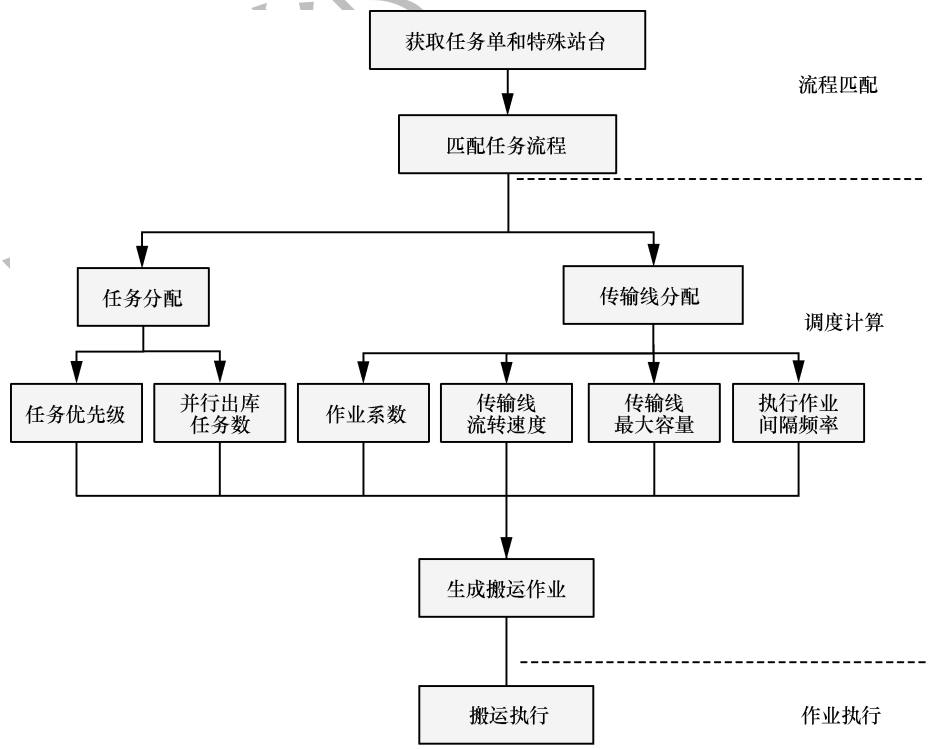


图 8 仿真实验流程

需求，极大提高了传输线的利用率和库房周转率，保证库房的出入库稳定。

系统部分成果已于多个网省计量中心推广使用，在其它工业领域自动化库房管理方面也具有广阔的推广前景。

参考文献：

[1] 陈祉如，王平欣，杨杰，等. 智能电能计量器具库房管理系统的研制[J].制造业自动化, 2016(1): 1-3.

[2] 赵成. 省级计量中心智能化仓储系统的规划设计[J]. 电测与仪表, 2014, 51(12): 17-22.

[3] 王永辉，董增波，张颖琦，等. 电能计量装置智能仓储系统研究及其运维管理[J]. 电测与仪表，2015，52(7): 17-18.

[4] 刘进亮, 赵运涛. 自动化立体仓库在备件存储方面的应用[J]. 一重技术, 2015(6): 21-25.

[5] 孙卫明, 方彦军, 肖勇, 等. 电能计量设备检定中心智能立库调度优化研究[J]. 自动化仪表, 2014(9): 1-4.

[6] 林立霖. 电能计量表自动化仓储设备控制系统的优化设计[D]. 福州：福州大学, 2014.

人民邮电出版社

基于区块链的电力数据共享机制

李旭[1,2]，王合建[1,2]
（1. 国网电子商务有限公司（国网雄安金融科技集团有限公司），北京 100053;
2. 国家电网有限公司电力金融与电子商务实验室，北京 100053）

摘　要：在当今的大数据时代，电力大数据的运用和发展在电力系统中发挥着举足轻重的作用。由于电力大数据涉及用户隐私、商业秘密等，无法向社会开放。基于区块链的几乎不可篡改性、加密传输、全链共识、全流程可溯源的特点，提出了一套安全、隐私、互信的电力数据共享解决方案。详细介绍了电力数据共享机制，通过区块链技术记录数据抽取、建模、共享等全部流程，实现全流程加密传输、原始数据“永不出数据持有方的硬盘”。既满足需求方对数据的使用，同时避免数据持有方数据泄露的风险，从而消除数据持有方信息安全的担忧和顾虑。

关键词：区块链；数据共享；数据安全

1　引言

随着网络和计算机技术的发展，数据与人们的生活结合的越来越密切，可以说人们的一举一动在网络世界中都有据可循。比如人们的出行数据、消费数据，企业的运营数据、经济活动数据，政府的政务数据等都会在网络中归集、固化，共同组成一个数字世界。数据不再是存在硬盘中的一个符号，而是一种重要的资源，看似一堆无用的数据经过大数据挖掘分析后，可以了解一个人的生活习惯、一个企业的运营情况甚至预测一个行业的发展状况。可以说，在当今的大数据时代，数据是堪比石油、黄金的重要资源。

目前，在大数据收集、存储和使用的过程中面临着诸多安全风险，大数据泄露导致的隐私问题为用户带来严重困扰。据相关数据统计，每年发生的数据泄露事故触目惊心，Facebook 公司 8 700 万用户数据泄露事故、华住旗下连锁酒店 2.4 亿入住信息泄露、Under Armour 旗下健身应用 MyFitnessPal 1.5 亿用户数据泄露等，类似的数据安全事件举不胜举。这些信息被用于总统选举、电话诈骗、商业收购等，严重影响了社会秩序和人民财产安全。电力数据涉及众多企业和公民的电力数据，还包含电力行业生产、营销数据。一旦发生数据安全事故，后果将不堪设想。

本文提出的电力数据共享模式，将区块链技术与数据共享相结合，利用区块链技术的几乎不可篡改性、加密传输、全链共识、全流程溯源的特点，为电力数据共享提供了一套安全、隐私、互信的解决方案。共享过程中原始数据“永不出数据所有者的硬盘”，数据所有者根据数据需求方提供的算法，处理原始数据生成数据报告返回需求方，数据共享平台监督共享双方的全部行为，并将共享全步骤写入区块链中，确保数据共享流程的安全可信，为电力数据能够更好地服务社会、服务大众，发挥更大的作用。

2　现有的数据共享体系

在电力行业内，电网公司依托数据中心建设，对电力数据（包括营销数据、综合数据、ERP 数据、生产数据等）进行归集与整理，在内部单位之间实现数据共享，数据流转如图 1 所示。

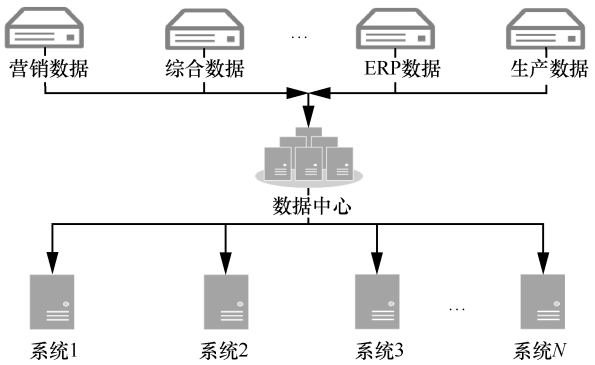


图 1　电网公司数据共享流转

在互联网行业内，数据共享主要是通过数据交易平台进行，数据平台通过网络爬取、合作、购买等方

人民邮电出版社

式获得上游数据，经过数据清洗系统，将原始数据清洗、融合，提升数据的价值，最后通过 API 或者数据分组的形式与数据需求方进行共享或交易，数据流转如图 2 所示。

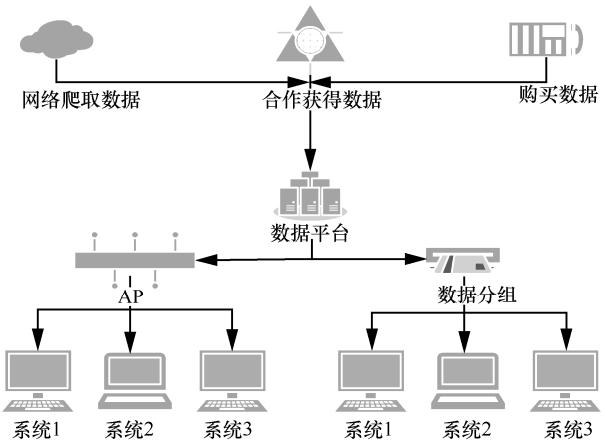


图 2　互联网行业数据共享流转

目前，无论电力行业还是互联网行业的数据共享模式都存在一些问题。电力行业对于信息安全的投入很大，并且数据在行业内部单位之间流通，信息安全和信息泄露事故发生的可能性非常小。但是电力数据共享模式，由于各种客观条件的约束过于保守，没有最大地发挥电力数据的作用。互联网数据共享模式存在的问题很多，在数据来源方面，主要通过网络爬虫爬取数据、通过合作获取数据、通过购买获取数据 3 种方式，上述数据获取方式均存在来源驳杂、数据质量难以保障、数据版权不清晰难以追溯等问题，给数据平台留有很大隐患；在共享模式上，平台获取上游原始数据后经过清洗机制对数据进行清洗增值，然后共享或交易给数据需求方，主要是通过 API 或者数据分组的形式将清洗后的数据进行共享，该方式存在数据泄露、隐私、数据版权、数据无法溯源等问题。虽然目前已有多家机构或企业开展数据共享业务，但由于没有相关标准规范约束，使得数据共享行业存在数据隐私、数据泄露、数据所有权不清等诸多问题。本文将区块链技术与数据共享相结合，能有效地解决这些问题。

3　基于区块链的电力数据共享体系

3.1　区块链技术

区块链并不是一种新技术，而是一种综合技术的简称，最早于 2008 年由化名为“中本聪（Satoshi Nakamoto）”的学者在密码学邮件组发表的奠基性论文《比特币：一种点对点电子现金系统》中提出。从技术角度上说，区块链可以看作一个分布式的公共数据库（或者称为公共账本）。它由多个关键要素组成，其中区块链技术主要包括现代密码学、分布式点对点网络通信技术、去中心化一致性共识算法、激励机制以及可编程脚本代码五大关键要素。

从区块链节点组成上说，区块链可以分为公链、联盟链和私有链。公链对全网公开，任何组织和个人都可以作为节点加入，并且链上数据全网公开，用户无需授权可以任意访问链上数据，真正意义上做到了去中心化；当前公链的典型代表有以太坊、比特币等，但是由于公链的节点众多并且大多使用工作量证明法（PoW），使得区块生成速度很慢，以比特币为例，新的区块生成需要 10 min，完成一次交易需要近一个小时的时间，显然不能满足当今互联网的要求。联盟链与公链不同，由参与联盟的机构共同建设节点组成区块链，区块链的共识规则由联盟成员共同制定，联盟链的数据有限开放，只有得到联盟授权的机构和个人才有权限访问链上数据，联盟链对交易时延和并发量有较高要求，因此节点数量相对较少，一般不会超过一百个，共识算法多采用 PBFT、RAFT 等。私有链不具备可推广性，在此不再进行介绍。

3.2　基于区块链的电力数据共享

基于区块链的电力数据共享机制利用区块链技术的几乎不可篡改、加密传输、全链共识、全流程可溯源的特点，为解决现有数据共享机制的安全隐私、数据版权不清晰、数据泄露等问题，提供了一个更为完善的解决方案。本方案的实现需要搭建区块链系统（电力数据共享链）、数据共享平台，并对现有系统进行一定程度的改造，结合搭建的“一链一平台”使电力数据更安全、便捷的共享给社会，发挥其更大的作用。总体架构如图 3 所示。

与现有的共享机制不同的是，本文提出的电力数据共享机制不是直接共享原始数据或者清洗过的源数据，而是在数据中心搭建一套算法沙盒系统。根据数据需求方提供的算法，使用数据中心的数据进行计算并生成报告返回给需求方，在此过程中沙盒使用过一次后自动销毁，生成的报告需要经过数据中心预设的关键字过滤机制进行过滤，并将共享全过程通过数据共享平台上链存证。具体流程如图 4 所示。

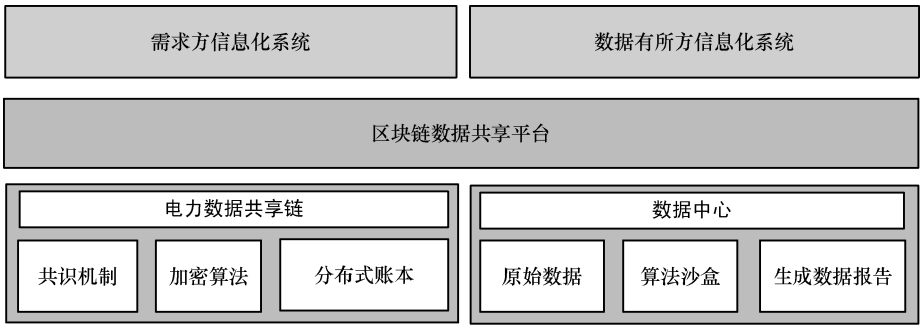


图 3　区块链电力数据共享总体架构

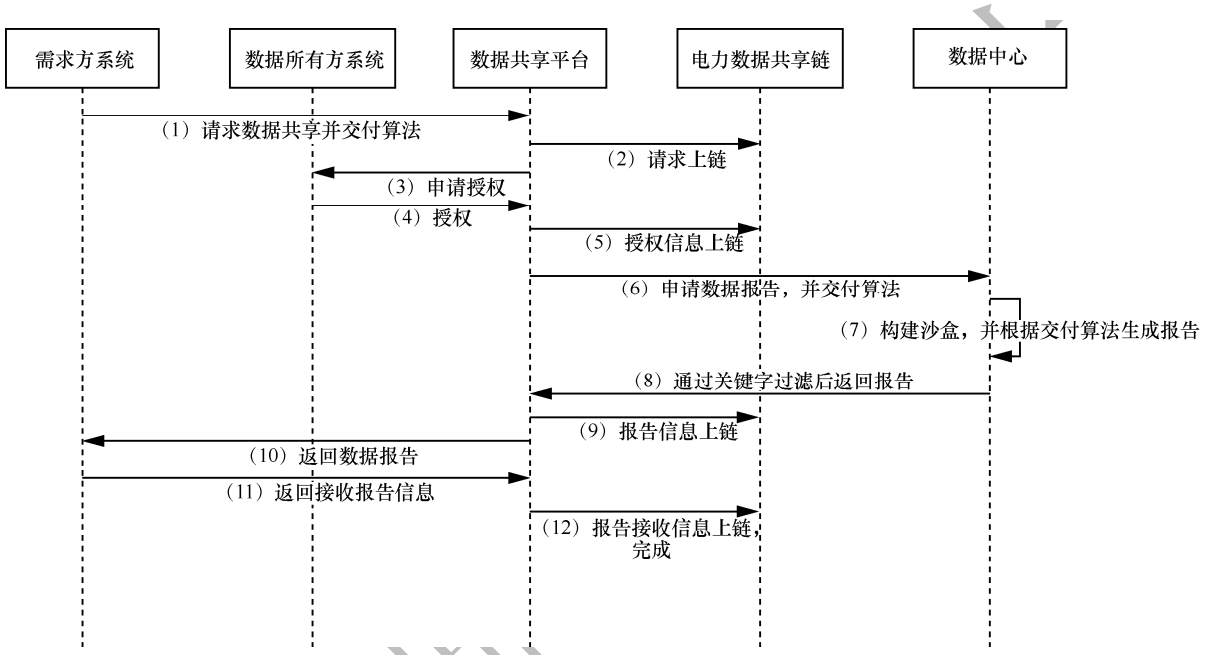


图 4　区块链电力数据共享流程

3.2.1　区块链电力数据共享实现

区块链电力数据共享主要分建链、建平台、现有系统改造 3 步实现。首先需要搭建电力数据共享链，记录关键业务流程信息和报告信息，防止信息被篡改、验证信息完整性、全流程可追溯；其次搭建电力数据共享平台，为电力数据共享提供服务支持；最后对数据中心进行改造，添加算法沙盒系统，保证原始数据的安全。

（1）搭建电力数据共享链

电力数据共享链是提供底层存储及技术支持的系统，采用联盟链的模式搭建区块链，节点分为核心节点及二级节点，核心节点数量不超过 10 个，二级节点数量不做限制，二级节点通过侧链技术与核心节点通信。核心节点由电网、大型数据共享平台及大型数据服务提供者共同组成，相互监督从而达成共识；电力数据共享链包括共识机制、区块链超级账本、电子数据摘签名等。

共识机制采用基于 Kafka 的高速共识算法和拜占庭容错算法算法（PBFT）相结合，基于 Kafka 的高速共识算法对总节点数没有特定要求，能容忍半数以下的节点发生故障，拜占庭容错算法能容忍最多 1/3 的拜占庭错误节点。

分布式超级账本负责可信区块链系统的信息存储，包括收集交易数据、生成数据区块、对本地数据进行合法性校验以及将校验通过的区块加到链上。账本层将上一个区块的签名嵌入下一个区块中组成块链式数据结构，使数据完整性和真实性得到保障，这正是区块链系统防篡改、可追溯特性的来源。典型的区块链系统数据账本设计，采用了一种按时间顺序存储的块链式数据结构。

电子数据摘要是对文件内容数据通过逻辑运算得到不可逆的唯一数据散列值。“电力数据共享链”在

将数据保存到区块链上之前，可以将敏感的数据或文件通过数字摘要的方式，将其数据指纹保存在区块链上。可以把数据通过安全的加密方式，对敏感的隐私数据进行有效的保护。

（2）搭建电力数据共享平台

数据共享平台是业务系统与电力共享链的连接纽带，同时也具备对电力共享链和业务系统接入的管理功能，对业务系统主要是负责审核业务系统的接入资质和权限的管理，对电力共享链主要是负责数据写入和查询的统一管理，对新增节点和跨链接入的审核与管理，还有对电力数据共享链运行情况的监控。

（3）改造现有系统

本文提出的数据共享机制与现有共享机制最大的不同主要有：一是利用区块链技术实现共享流程和共享数据的几乎不可篡改、全流程可溯源，解决现有共享机制数据所有权不清晰的问题；其次是共享数据是基于数据所有方的数据运算出的报告而不是源数据，所以要对数据中心进行部分改造或升级，在其原有的基础上部署一套数据运算沙盒系统，实现使用需求方的算法、所有方的源数据、加工出符合需求方要求的产品（即数据报告）的功能，并且确保运算沙盒计算完成及时销毁，从而保证供需双方的数据安全，防止数据泄露。

4 结束语

由于信息安全问题，现阶段电力数据只实现了内部共享，使得电力数据资源未得到充分利用，为了促进电力行业健康持续地发展，电力数据共享是一个必然的趋势。然而，现有的数据共享应用方式存在很多不足，数据所有权不清晰、隐私数据泄露、共享过程难以追溯等问题严重阻碍了数据共享的健康发展。为解决这些问题本文提出了基于区块链技术的电力数据共享机制，利用区块链技术链上数据几乎不可篡改、隐私、全流程数据可溯源的特点，实现共享数据的确权、隐私保护、共享溯源等；利用本文特有的共享数据报告的形式来保证数据所有方源数据的安全性，防止数据多次共享及数据泄露。基于区块链的电力数据共享机制有利于推动电力数据对外共享，打破行业内信息壁垒、遏制数据信息“孤岛”、促进数据资源利用率，推动电力企业向共享型企业转型，促使电力企业能更好地履行服务社会的责任。

参考文献：

[1] 孙毅, 范灵俊, 洪学海. 区块链技术发展及应用现状与挑战[J]. 中国工程科学, 2018(2): 35-40.

[2] 胡建宏, 胡斌彦. 电子签名技术研究综述[J]. 卫生职业教育, 2007(10).

[3] 宁蕊, 梁国兰, 焦靖, 等. 浅析“区块链”在金融领域的应用[J]. 现代商业, 2018(13).

[4] 唐红玉. 大数据背景下廉洁政治生态建设研究[D]. 长沙: 湖南大学, 2017.

[5] 马立川, 裴庆祺, 冷昊, 等. 大数据安全研究概述[J]. 无线电通信技术, 2015.

[6] 郭凯. 区块链技术下的金融展望[J]. 财讯, 2018(7).

[7] 江晓珍. 区块链技术在金融领域的应用研究[J]. 四川文理学院学报, 2018(4).

[8] 侯衡. 区块链技术在电子政务中的应用优势、制约与发展[J]. 电子政务, 2018.

[9] 孙柏林. 装备制造业发展的新动向:区块链+制造业[J]. 自动化技术与应用, 2018(7).

[10] 侯衡. 区块链技术在电子政务中的应用优势、制约与发展[J]. 电子政务, 2018(6): 31-39.

[11] 陈新林, 王政铭. 一种基于区块链和 NFC 芯片的动态信息防伪技术[J]. 物联网技术, 2018(3): 3.

[12] 中国信息安全. 最高人民法院出台互联网法院审理案件规定[J]. 中国信息安全, 2018(9): 30-33.

[13] 袁勇, 王飞跃. 区块链技术发展现状与展望[J]. 自动化学报, 2016, 42(4): 481-494.

人民邮电出版社

基于区块链和泛在电力物联网的安全体系

王丹，赵训威，王文华
（国网信息通信产业集团信通研究院，北京 102211）

摘　要：区块链是一个去中心化的分布式账本数据库，具有几乎不可篡改、不可伪造的特点。任何授权节点都可以对这个公共数据库内容的合法性进行核查。区块链中的数据，必须由网络中的参与节点，按照严格的规则和共识来进行修改。在研究区块链系统特性的基础上，提出了将区块链与泛在电力物联网安全结合的安全体系架构设计，具有数据安全可靠、防篡改、安全策略规则可重配置的特性，可以极大地提升泛在电力物联网的安全性能。

关键词：区块链；泛在电力物联网安全；链状数据结构；身份密钥；共识机制；分布式存储

1　引言

国家电网提出，建设世界一流能源互联网企业的重要物质基础是要建设运营好“两网”，即“坚强智能电网”和“泛在电力物联网”。坚强智能电网概念，早在 2009 年就被提出，目前以特高压为骨干网架的多级电网协调的坚强智能电网建设，已经比较成熟。相对而言，泛在电力物联网刚刚起步，需要一系列先进信息通信技术的配合，同时结合电力领域实际，有效地应用先进技术来解决实际问题。如果说坚强智能电网解决的是电力流的问题，那么泛在电力物联网解决的侧重点就应是业务流和数据流。

目前国网的物联网应用已具有一定基础，接入智能电表等各类终端 5.4 亿台（套），采集数据日增量超过 60 TB，覆盖全国约 4.71 亿客户的用电信息实现在线采集，车联网接入充电桩超过 28 万个。这为国网的泛在电力物联网建设提供了坚实的基础，同时也带来了新的挑战。泛在电力物联网的网络和智能化特质，决定了新一代的物联网设备有比传统设备更易受到网络攻击的可能，采集数据的篡改、敏感信息的盗取、智能节点被劫持，都可能造成电力网的巨大损失甚至是瘫痪。如何解决这个问题呢？区块链技术也许能提供一种新的思路。区块链本质上是一个去中心化的分布式账本数据库，具有几乎不可篡改、不可伪造的特点。任何授权节点都可以对这个公共数据库内容的合法性进行核查，单一用户是不可以对它进行控制的。在区块链系统中参与者，共同维持数据的更新，只能按照严格的规则和共识来进行修改。

2　区块链技术与电力物联网安全

2008 年，中本聪发布了著名的《比特币，一种点对点的电子现金系统》白皮书，又在 2009 年公开了其早期的实现代码。不同于传统的银行或者第三方电子支付系统，由银行或支付服务商来验证并记录系统中发生的交易，比特币第一次实现了去中心化的电子货币发行和交易，不需要第三方认证机构或账务管理系统对交易进行验证和记录，而是由全部网络成员共同维护并更新一份相同的帐本。这种“公共账本+共识”的模式正是由区块链技术实现的。

虽然比特币白皮书中并没有直接提出“区块链（Blockchain）”这一概念，但其交易数据记录的方案可以认为就是区块链的原型：客户端发起交易，然后向全网广播等待确认，系统中的各个节点（矿机）将若干待确认的交易和上一个块 Hash 值打包放进一个块（Block）中，并审查块内交易的真实性以形成一个备选数据块，随后节点开始不停尝试增加不同随机数，如果备选数据块的 Hash 值小于某一特定值则该数据块可以认为合法，之后系统节点向全网进行广播，网络内其他节点对该区块进行验证，超过一定数量节点公认该区块合法后，此时新的区块数据就会被添加到链上，进而区块中记录的所有交易数据，也被确认合法。如此往复，形成一个历史数据不停堆叠的数据链。

但是，正是由于区块链同比特币、以太坊等数字

人民邮电出版社

token 的发展紧密联系，人们对于区块链的传统看法，往往同交易或者账本联系，但是笔者认为，区块链的本质在于：（1）链状的数据存储结构——数据的防篡改机制；（2）节点的密钥策略——身份认证机制；（3）“非”中心化的认证策略——多节点决策机制；（4）分布式存储机制——“灾备”及对抗机制。这些特性，使得区块链天然对电力物联网的发展有着极大的帮助。

2.1 链状的数据存储结构——数据的防篡改机制

区块链中的链状数据存储结构，代表着每一个新的区块都包含前一个区块的 Hash 信息，形成一个链状的结构，如图 1 所示。随着链状存储结构的不断延长，篡改数据的难度也会越来越大，区块链上任何一点信息的篡改，都要修改整个区块链数据，造假的代价很大。

物联网系统中，每一个节点采集的数据，都可以用这种方式记录下来，链状的数据结构，可以有效地防止恶意篡改数据和伪造数据，为物联网系统打造第一重安全保护。

2.2 节点的密钥策略——身份认证机制

信息安全及密码学技术，是保证整个系统稳定的基石。区块链中大量使用了现代安全和密码学的技术成果，包括 Hash 算法、数字签名证书、同态加密、零知识证明等。区块链节点安全的核心，在于采用一系列加密算法，利用非对称加密机制，通过公私钥的方式，完成数据加密、签名等任务，这使得区块链节点天生具有防劫持、防伪造的特性。只要私钥不丢失，就不存在冒名伪造信息的可能。节点的密钥生成方式如图 2 所示。

安全密钥机制，进一步完善了节点的安全性能，使得电力物联网中各个组成设备，不容易被劫持或攻击，也使得入侵者很难伪装成合法节点，攻入网络内部进行破坏或数据窃取活动。

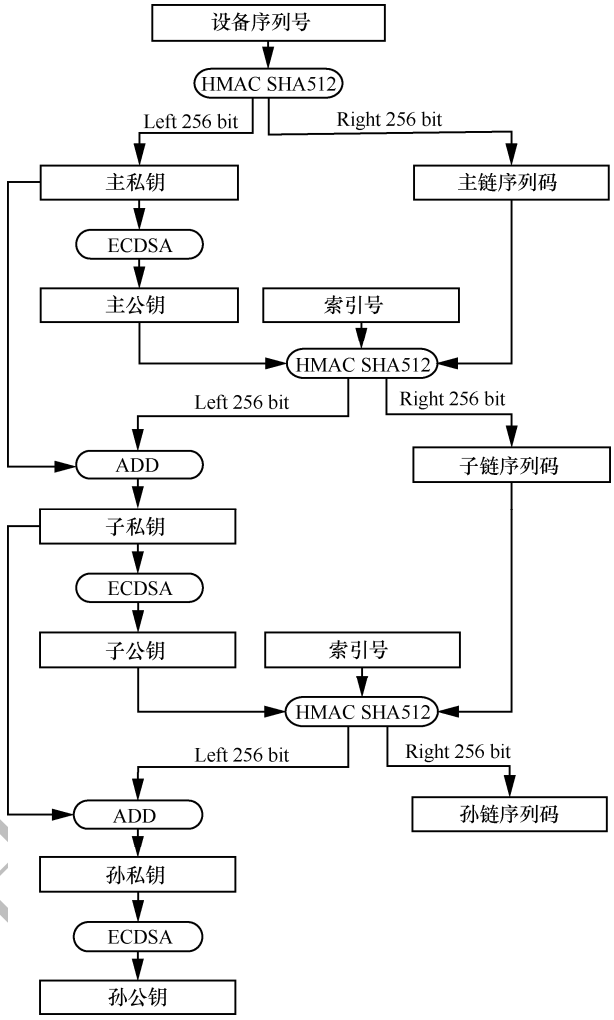


图 2　节点的密钥生成方式

2.3 “非”中心化的认证策略——多节点决策机制

区块链中的事务（传统的或者说狭义的区块链定义称为“交易”（transaction）），事务的生效是需要大多数节点共同投票决定的，所以，除非网络中大多数节点都被攻陷，区块链网络都可以完成正常地数据交换与校验工作。这是由于区块链本质是一个数据可追溯、几乎不可篡改、解决非完全信任环境下多方互

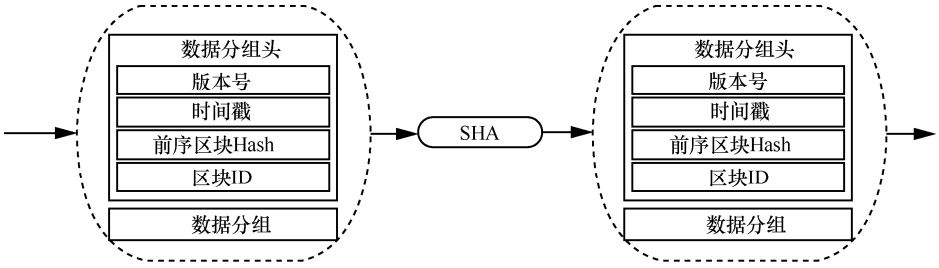


图 1　链状的数据存储结构

信问题的分布式系统，系统中的各个成员通过一定的共识算法（consensus）来解决分布式系统中的一致性问题。

分布式系统的共识达成需要依赖可靠算法，共识算法通常解决的是由哪个节点发起提案以及其他节点如何就此提案达成一致的问题。根据传统分布式系统与区块链间的区别，将共识算法分为可信节点的共识算法和不可信节点的共识算法。

一般对于区块链的描述，喜欢使用“去中心化”这样的说法，但是笔者认为这样的说法是很狭隘的，完全去中心化的网络是有很大弊端的。区块链的结构，只是一定程度地将单一中心的角色分散成多个中心的结构，从而提高网络的健壮性，而不是绝对取消中心。所以，只能称之为“非”中心化，或者“非”单一中心化，而不能称之为“去”中心化。“非”中心化的决策策略如图 3 所示。

目前区块链多以不可信节点的共识算法为基础，根据不同的场景，又可以分为几个类型。以工作量证明（PoW）和权益证明（PoS）等算法为代表的适用于公链的共识算法以及以 PBFT（practical byzantine fault tolerance，实用拜占庭容错算法）等适用于联盟链或私有链的共识算法。

针对物联网场景和电网业务的实际需求，共识算法需要有新的变化。针对非中心化的结构，同时根据电网系统中业务角色和重要性的不同，泛在电力物联网中的各个节点可以划分为两大类：核心节点和普通成员节点。核心节点通过投票完成规则的起草、修改和认定，网络中的所有节点都可以有上传和访问数据的权利，但这个权利是受核心节点控制的，普通成员节点可以访问的数据域由核心节点确定的规则和权限来决定。核心节点并不唯一，全部核心节点组成分布式的系统设计，全体核心节点实现共识的过程可以大致描述如下。

（1）区块链规则的设计和修改。由某个或某些核心节点发起，通过投票的方式确认，当规则通过，则下发所有节点知悉，节点接收到规则更改通知后，更新本地规则。

（2）区块链数据的上传与校验。首先由核心节点选举产生当期 Leader 节点，接着赋予 Leader 完全的权力管理数据记录，由 Leader 节点从客户端接收数据记录请求，完成操作，生成区块，并复制到其他节点，其他节点可以对操作的合法性进行验证。Leader 节点可能失效或与其他节点失去联系，也可能定期重新选举，这时，系统就会重复之前的过程，选出新的 Leader 节点。

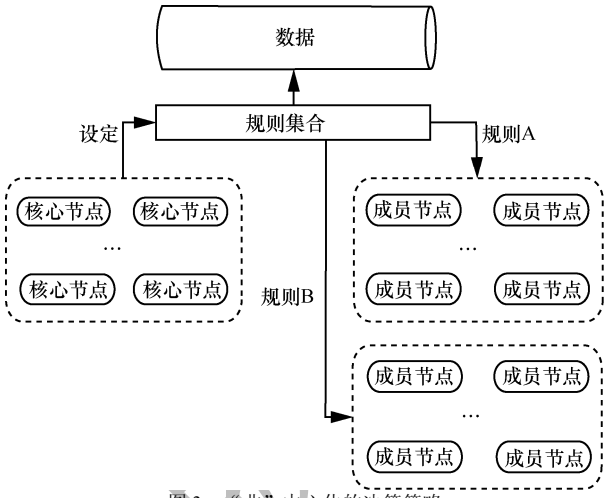


图 3 “非”中心化的决策策略

由于协商机制的存在，泛在电力物联网的共识和安全策略的确定与变更，可以由核心节点随时协商处理，具有可重配置的特性，对于整个网络的安全性，也有极大地提高，当旧的共识与安全策略存在隐患时，随时可以切换到新的策略，甚至定期或不定期地在多个策略中切换，极大地增加了攻击的难度与成本。

2.4 分布式存储机制——“灾备”及对抗机制

区块链中的数据，不是存储在单一节点中，而是可以存储在任何有授权的节点上。这样单一节点的数据损坏或者丢失，都不会造成全部数据的丢失。只要有一个节点保存有完整的区块链数据，其他节点都可以进行数据验证，确认数据真实性，如果数据真实有效，每个节点都可以从这个副本中恢复数据。

另外，由于分布式存储数据中任何一方的节点都各自拥有独立的、完整的一份数据存储，可以通过共识机制达成数据存储的最终一致性。由于各个节点均各自维护了一套完整的数据副本，任意单一节点或少数集群对数据的修改，均无法对全局大多数副本造成影响。所以，无论是服务提供商在无授权情况下的修改，还是来自外部网络的恶意攻击，均需要同时影响分布式存储数据集群中的大部分节点，否则正常节点将很快发现并追溯到系统中的恶意行为并进行纠正，大大提升了业务系统中数据的可信度和安全保障。分布式存储数据如图 4 所示。

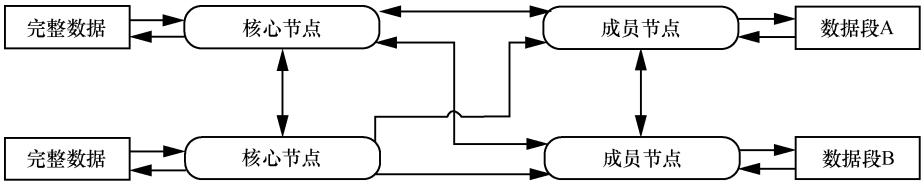


图 4　分布式存储数据

除此之外，传统分布式存储系统还是受某单一中心节点或个别机构控制的数据管理机制，而区块链结构中的分布式账本往往基于一定的共识规则，采用多方决策、共同维护的方式进行数据的存储、复制等操作。随着数据的不断增长，单一中心组织构建数据管理系统会面临越来越大的压力，包括计算、网络、存储等各种庞大资源池效率的问题，还有伴随不断推升的系统规模和复杂度带来的可靠性问题。区块链的分布式数据存储机制可以有效减少系统臃肿的负担，同时有效利用网络中大量零散节点沉淀的资源池，包括计算能力、带宽分配和存储介质等。

3　结束语

总而言之，区块链的特性决定了它在安全领域的巨大潜力。但是，作为计算机网络和分布式系统的一个子方向，现在的不少研究方向，还仅仅集中局限于区块链在金融交易方向中的应用。泛在电力物联网，作为电网系统中不可或缺的信息通道，安全至关重要，如果出现问题，小则部分地区停电，严重的甚至会上升到危机国家经济、安全的地步，所以，如果能合理地将区块链结构与泛在电力物联网结合，可以为泛在电力物联网提供更加稳固的安全基础。电力物联网区块链架构，可以划分为云平台、网络和端侧的可信硬件执行环境 3 个部分。云平台提供业务执行的接口与环境，网络保证区块链结构中的多节点访问的安全性和稳定性，端侧的可信硬件执行环境在系统层或芯片层来保障区块链安全运算实现和性能加速。将三者有机结合、共同作用，可以打造出一个可控、可信、可靠、安全稳定的电力物联网信息安全环境，为电力系统的发展添砖加瓦。

参考文献：

[1] FERNNDEZ-CARAMS T M, FRAGA-LAMAS P. A review on the use of blockchain for the internet of things[J]. IEEE Access 6, 2018: 32979-33001.

[2] NOVO O. Blockchain meets IoT: An architecture for scalable access manage-ment in IoT[J]. IEEE Internet of Things Journal , 2018, 5(2): 1184-1195.

[3] 杨保华, 陈昌. 区块链原理、设计与应用[M]. 北京: 机械工业出版社, 2017.

[4] DEBUS J. Consensus methods in blockchain systems[R]. 2017.

[5] 华为区块链技术开发团队. 区块链技术及应用[M]. 北京: 清华大学出版社, 2019.

人民电出版社

基于区块链技术的电力系统信息交换平台

袁野，李向阳
（北京国网信通埃森哲信息技术有限公司，北京 100032）

摘　要：区块链作为一种分布式计算技术，是继“大云物移智”后又一项具有颠覆性的信息通信技术。区块链技术为电力系统、能源行业乃至国家社会层面带来了重大的变革。区块链技术具有非中心数据共识和数据开放自治功能等特点，并且各个数据单元具有可追根溯源的特性，从而其存储的数据单元具有无法私自篡改的特点，依托于此固有特性，区块链技术可用于多个信息系统之间的数据交换与共享。在电力系统中，常常需要多个信息系统之间互相配合，共同处理信息，这对各个信息系统的处理时间提出了更高的要求。通过在区块链中遍历分布的各个节点完全可信任且无法盗用的信息交换功能，能够实现可靠的日志时间保留。该项目通过在区块链中分发可信和不可破解的信息交换功能，开发了基于区块链技术的电力系统信息交换平台。经过大量测试和数据验证表明，基于区块链技术的电力系统信息交换平台比传统电力系统信息平台交换技术更加符合电力系统之间信息交换安全性的严苛需求，将区块链应用于电力业务平台将有效地提高信息系统的安全性。

关键词：区块链；电力系统；信息交换；不可篡改

1　项目背景

1.1　电力系统对信息交换的需求

近年来，中国电力系统信息化水平一直处于行业领先水平。信息化建设发展速度持续加快。在信息系统的大力支撑下，电力系统业务迅速发展，通过信息交换，实现电力系统的业务流转。电力系统的信息交换也主要分为两种方式：一是特定系统之间的点对点通信，二是基于通信中间件的数据交换。具体内容如下。

（1）特定系统之间的点对点通信

早期，各种信息系统两者之间的信息交换通常基于系统的具体业务需求和业务流程。在信息系统之间建立通信逻辑通道，以特定系统之间的点对点通信的方式实现信息交换。这种信息交换方式将对信息系统的开发改造带来极大的影响，效率低下。

（2）基于通信中间件的数据交换

通信中间件起着通过集中服务为信息系统提供通信接口的功能，所有数据的交换是通过标准接口存储和访问的。该方法大大提高了可靠性，有效增强了开发的便利性。然而，通信中间件具有更高的权限，并且访问的数据量很大，可以获取所有通信数据。所以，如果通信中间件出现故障导致其无法正常使用，那么整个系统将面临单点故障的风险。

在大多数业务场景中，需要多个部门和多个系统相互合作和协作才能完成业务流程。信息交换的可靠性和可信性非常重要。例如，在故障修复方案中，它涉及诸如热线访问、营销系统查询和维护调度工作订单之类的过程。明确响应时间要求是进一步提高服务质量和服务效率的先决条件与基础，在实际场景分析中，一旦响应时间用尽，应该对其超时的因素进行对比分析并且追究责任。一旦每个信息系统擅自修改了本地日志，导致日志中的数据发生变化，将无法为原因分析提供真实准确的数据支撑，分析结果也将失去意义。如何确保日志不被篡改，满足信息流传输的可靠性是任何通信传输技术的基本需求，同时更是电力系统信息交换平台数据交换的重中之重。

1.2　区块链技术的概念和架构

区块链是计算机技术的一种新的应用模式，包括分布式账本技术、分布式数据存储、点对点传输、共识机制和加密算法。区块链的本质是一个分散的 Internet 数据库，它的特点是安全、稳健、智能、分散、开放和透明。

区块链是分布式体系结构。它们是按块结构链接在一起的有序列表，其中每个块存储一组信息。每组信息都组织在一个名为 Merkle Tree 的特殊数据结构

人民邮电出版社

中。其中，叶子节点通过信息的散列值标记，其他节点则通过子节点的散列值标记。在区块的顶部，存储着根节点的散列值和上一个区块的散列地址。由于散列指纹会根据数据的细微变化而发生剧烈变化，且加密散列算法具有不可逆转性，因此，区块链中的数据将难以被恶意攻击，具备极高的安全性。

在区块链网络中，每个参与者在存储整个块链的本地副本之后建立与公钥基础结构的通信机制。只有在所有对等体之间获得有效匹配时，才向网络广播信息。因此，即使攻击者可以伪造单个副本，它也不会影响整个区块链，除非它控制超过 50%的对等节点，基于这种方式，智能网格可以在攻击行为中取得力量，从而提高抵抗恶意攻击行为的能力。

1.3 区块链技术的特性与发展

区块链作为一种分布式计算技术，它最初旨在应用于加密“货币”系统。此外，由于其特性，它还可以用作分布式分类帐服务器来存储各种数据。区块链技术可以让零散在各个遍历节点的数据产生“共识”机制。区块链的安全特性包括以下 3 个方面。

（1）数据共识

在没有中心节点的环境中，可以通过参与节点之间的分布式协议来对数据进行分散。参与节点之间地位一致，从根本上完全避免将数据写入单个节点或用户单独控制系统的情况发生，也避免了数据不同步、前后端数据缺失等情况的发生。

（2）数据防篡改

假设，在信息系统中，诚实节点的比例很大，一旦数据被写入，就不能修改数据，以避免由于兴趣驱动的篡改而对数据进行篡改。

（3）数据防擦除

数据写入区块链之后，所有共识节点将自动保存数据，数据同步更新，所产生数据无法擅自删除，使所有数据都可追溯且不可篡改。

区块链主要包括公共链和联盟链两种应用场景。公共链方面，主要用于完全分散的加密数字货币的发行和流通，它具有良好的可扩展性，但吞吐量低。联盟链方面，主要用于行业用户和信息系统之间通过对未经证实的数据共识机制，以支持用户和节点身份验证和针对所输入信息真伪的验证，并为信息系统实体提供更严格的安全性。

联盟链的实现主要分为以拜占庭协定为基础的协商一致和基于 Sorting-endorsement 协议的共识两种方式，具体内容如下。

（1）以拜占庭协定为基础的协商一致。这种协议来自一般拜占庭问题，此类问题对于安全性的要求非常高，但参与节点的数量有限且性能不能满足需求。

（2）基于 Sorting-endorsement 协议的共识。该协议实现了节点的数据排序和预处理，协商一致节点通过后，通过投票的方式来实现协商一致。这种协议具有更高的可扩展性和更好的性能。

本文设计的电力系统信息交换平台将支持具有高可扩展性和吞吐量的各种信息系统的数据共享和交换。考虑到性能和安全性，本文选择了 Sorting-endorsement 协议的一致性算法，如图 1 所示。

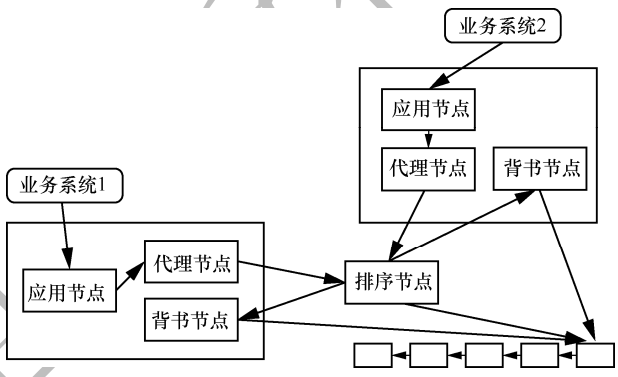


图 1 基于 Sorting-endorsement 的共识协议

2 系统设计

系统采用分层设计的思想，可以实现数据存储层与应用层之间的区块链共识和逻辑隔离。通过易于使用的标准接口在层之间实现数据访问。

2.1 系统整体架构

系统架构主要包括基础层和应用层，并通过多个标准接口连接，如图 2 所示。其中主要功能描述如下。

基础层实现数据共识和存储。排序节点根据固定算法对网络中的事务数据进行排序，并将其打包到原始数据块中，见证节点通过数字签名认可原始数据库。当获得足够数量的批准数据块时，形成共识。基础层还支持数据块和数据库的混合数据存储模式。通过验证区块链中的数据并验证它不会被篡改，实现了更加实时、灵活、高效的数据查询功能，可以在区块链上验证存在质疑的数据。

应用层支持电力系统的各种应用场景以及场景间的数据循环和日志保留。应用层和基础层之间有 3 个标准接口。

（1）RESTFul 接口

该接口实现了信息系统查询和访问功能的标准封装，应用层以封装形式访问底层数据。

（2）智能契约接口

此接口实现RESTFul和区块链系统之间的数据访问转换。

（3）数据库访问接口

该接口可以高效地访问数据。

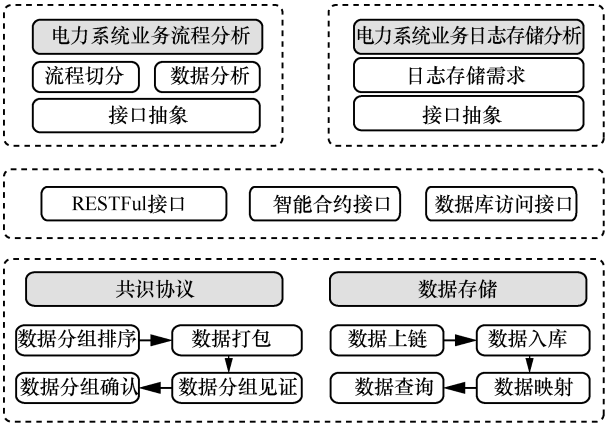


图 2　系统整体架构

2.2　系统流程设计

系统流程设计支持电力系统之间的数据交互，包括数据交换和过程访问，并通过标准接口隔离访问。两个信息系统之间数据流的应用场景如图 3 所示，假设系统 A 向系统 B 发起数据访问请求。系统 A 通过 Web 服务的标准接口向平台提交访问请求，平台转换将请求访问到系统支持的代码中。代码通过共识节点写入区块链以形成确定性数据并将内容写入数据库。系统 B 通过轮询从系统 A 获得访问请求。获取访问结果后，通过 Web Service 界面将其转换为智能合约，并写入区块链和数据库。系统 A 最终获取访问结果，并且中间进程以日志的形式保留在区块链中，从而实现不可更改的日志记录。

3　系统实现与测试

通过封装智能契约并使用 Web 服务实现业务系统的访问接口，建立了电力系统典型业务逻辑的仿真测试环境，采用标准方法封装数据的采集和写入。应用程序系统需要调用标准接口，以 XML 格式将所需数据写入区块链。为保证系统的安全性，系统提供身份注册接口，并通过认证过程进行访问。系统设计的接口见表 1。

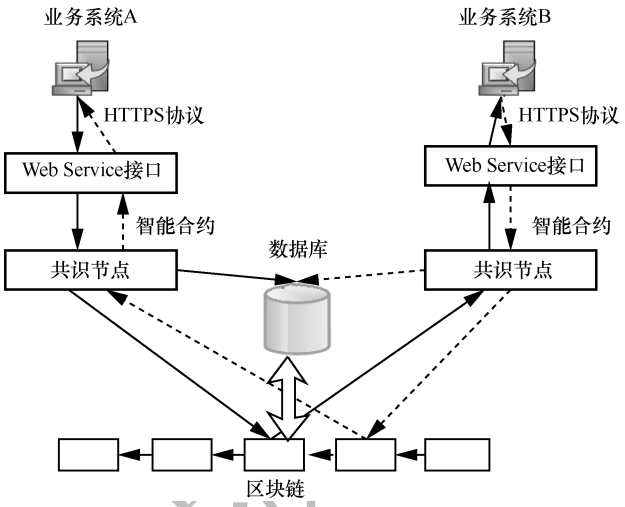


图 3　信息系统间的数据流转

表 1　信息交换接口定义

序号	接口名称	接口用途	方法
1	/users	注册合法用户	Http Post
2	/data	查询数据接口	Http Get
3	/channels/transactions/write	推送数据接口	Http Post
4	/channels/transactions/{txid}	根据 txid 查询信息	Http Get
5	/num	根据业务主键查询交易数据集合	Http Get

4　结束语

本文提出了一种基于区块链技术的电力系统信息交换平台。测试表明，系统可以实现数据交换和信息共享，生成的数据访问可以在区块链中留下不可改变的日志记录，已达到预期目标。

参考文献：

[1]NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[J]. Consulted, 2008.

[2] 中华人民共和国工业和信息化部. 中国区块链技术和应用发展白皮书(2016)[EB]. 2016.

[3] Hyperledger[EB]. 2016.

[4] 蔡亮, 李启雷, 梁秀波. 区块链技术进阶与实战[M]. 北京: 人民邮电出版社, 2018.

[5] MILLER A, XIA Y, CROMAN K. The Honey Badger of BFT Protocols[EB]. 2016.

人民邮电出版

基于区块链与第三方的混合智能合同应用

边新宁，周晶，孙喜民，张宾
（国网电子商务有限公司，北京 100053）

摘　要：讨论了如何将传统的商业合同转化为智能合同。它们的电子信息可用于实时系统地监测和执行合同权利、义务和禁令。解释了新的块链技术是实现智能合约的一个有效的平台，发现了区块链技术的缺点与不足。建议在分散化和透明化必不可少的应用程序中，开发人员可以地将智能合同和区块键技术这两种方法结合成混合解决方案，其中一些操作由部署在块链上的执行者执行，其余由部署在可信第三方上的执行者执行。

关键词：智能合同；区块链；可信第三方

1　引言

在传统业务中，通常在这些情况下使用的机制是由分类账支持的商业合同。合同规定各方应执行哪些行动，而分类账则用来记录已执行行动的历史记录。人们普遍认为，电子商务也需要同等机制。目前正在探讨解决这一问题的一个新的办法是建立在区块链技术基础上的智能合同[1,2]。这类技术的例子有比特币[3]、Etalum 和 Hyperledger。然而，基于区块链的智能合同仅仅处于初始研究阶段，它们的可伸缩性、性能、交易成本和其他问题都困扰着研究人员，这些问题都是由于它们的分散性质而产生的。

本文作出以下分析。

（1）实施智能合约的方法各有不同，从集中到分散不等。

（2）解释了这些方法的优缺点，并认为它们在解决问题方面的适用性取决于应用程序的特殊性、对应用程序所作的假设以及可用的区块链技术提供的便利。有一大类应用程序可以从混合解决方案中受益。

2　应用场景

一个合同制物联网应用的示例如图 1 所示。

正如在参考文献[1]中所解释的那样，现实的传统法律合同是复杂的文件。通常，这些文件包括不一致和含糊不清的文件，这是可以容忍的，因为它们期望

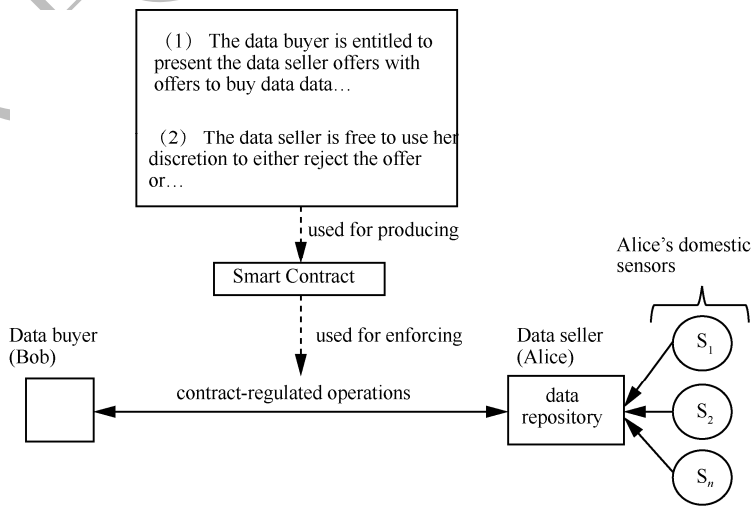


图 1　由智能合约监管的数据交易

在人类判断的帮助下被解释。工作重点是合同的具体条款，这些条款需规定得足够精确，使它们能够适应计算机语言编码。

合同条款包括几项合同操作，如要约购买数据、拒绝要约、接受要约、发出要约接受通知、发送付款等。

3 智能合同背景

智能合同是一种事件、条件、动作有状态的计算机程序，由两方或多方之间执行，双方不愿毫无保障地相互信任。它可以被认为是有限状态机（FSM），它是保持一个状态模型的发展（从启动到完成）的共享活动。

可执行契约的研究可以追溯到 20 世纪 80 年代中期和 90 年代初[5,6]。1997 年，Szabo 使用了智能合同[7]一词，指可转换为计算机代码并执行的合同。然而，智能合同的商业兴趣是在 2008 年才出现的，原因是 Satoshi 的比特币论文[8]的出版激发了密码货币、智能合同和其他分布式应用程序的发展。Satoshi 背离了以往研究中采取的集中化方法，并展示了如何将明智的合同分散。

根据用于监视和执行合同的智能合同的实例（副本）的数量，区分了集中化和分散化（分布式）方法。

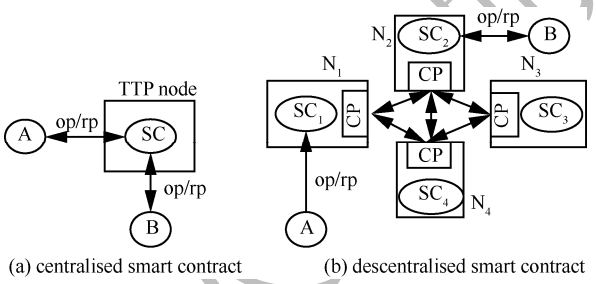


图 2 智能合同的集中化和非集中化实施

智能合同的集中化和非集中化实施如图 2 所示。A 和 B 是业务合作伙伴，例如，A 和 B 的合同部分；SC 是相应的智能合同；op 代表针对 SC 执行的操作，rp 是对应的响应；TTP 节点是受信任的第三方控制的节点；N_1～N_4 是不受信任的节点；CP 代表协商一致的议定书。如图 2（a）所示，契约可以实现为一个集中化的应用程序，它使用在 TTP 节点中运行的智能契约（SC）的单个实例。除了 TTP 引入的缺点（单一故障点、对 TTP 的信任等），相对于分散化的方法，这种方法相对简单。分散化方法依赖于一组不受信任的节点，而不是用于运行智能合同的几个相同实例（如 SC_1～SC_4）的单个 TTP。在这种方法中，A 和 B 可以自由地对任何实例进行操作。分散化方法摆脱 TTP 的代价是，不受信任的节点必须运行协商一致的协议，以验证给定操作是否已正确执行，并保持 SC_1～SC_4 的状态相同。根据所使用的协议，其计算、通信和性能退化成本可能无法承受，或其一致性保证不足[9]，导致使分散化办法不合适。

4 实施方案

下面重点介绍 3 种实施方案的优缺点。

（1）集中化的实现方法

集中实施如图 3 所示。SC 的作用是由纽卡斯尔大学开发的 CCC（合同符合性检查员）执行的。本节使用的 CCC 和 SC 是同义词。CCC 是用 Java 编写的 FSM，它接受以 Drools 语言[4]编写的业务规则编码的合同条款。FSM 的状态因业务伙伴发起的合同操作（op）的执行而改变，例如提供购买数据和发送付款。在 CCC 中运行的 FSM 跟踪 B 和 A 之间执行的业务流程的状态，并在此基础上确定给定的操作是否为合同。

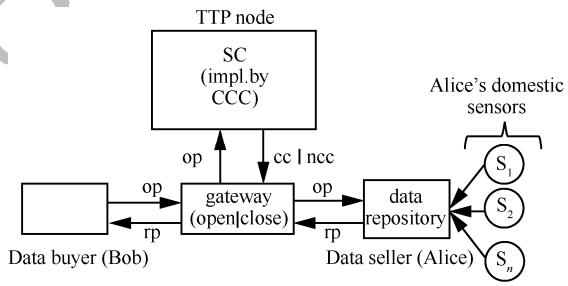


图 3 集中智能合同

符合合同（cc）或不符合合同（ncc）。CCC 用于控制允许访问 Alice 数据的网关。例如，当 Bob 希望访问 Alice 的数据时，他对网关发出相应的操作；网关将操作转发给 CCC；CCC 根据其业务规则对操作进行评估，该业务规则编码合同条款，并分别以 cc 或 ncc 响应打开或关闭网关；网关的打开允许 Bob 的操作到达数据存储库并检索传递给 Bob 的响应（rp）。注意，为了保持图的简单性，图 3 中箭头只显示由 Bob 发起的操作所遵循的方向。

（2）非集中化的实现方法

一个分散的体系结构如图 4 所示。智能契约的 4 个实例 SC_1～SC_4 部署在区块链平台的 4 个节点 N_1～N_4 中（每个节点一个）。由业务伙伴发起的每个操作

都是根据合同执行的；合同确定操作是符合合同的还是不符合合同的，并相应地响应两个业务伙伴。相应地，响应也被发送到网关以打开或关闭它。

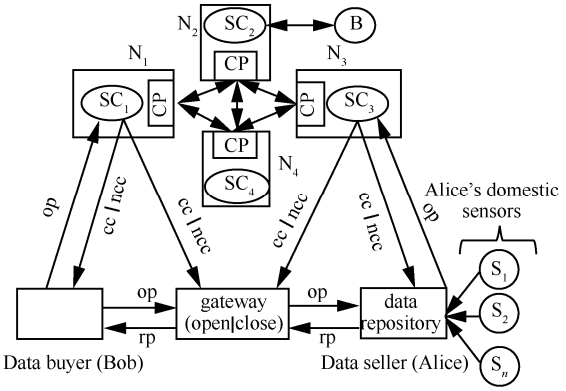


图 4　非集中化智能合同

为了保持图的简单性，图 4 中只显示数据买方、SC_1 和网关之间的通信线路，以及数据卖方、SC_3 和网关之间的通信线路。然而，假设给定的操作可以呈现给智能契约的 4 个实例中的任何一个，并且它们中的任何一个都可以响应业务伙伴和网关。

分散执行的显著特点是复制聪明的契约，因此不依赖于单一的一方。支付这一好处的成本是在实例之间执行协商一致的协议，这会对智能合同的性能产生重大影响，因为它可以分析每秒的操作数（即区块链术语中的事务），以及完成事务的响应时间。

（3）混合实现

图 5 显示了混合实现的结构。它结合了集中化和分散化方法的特点。将合同操作分为两类：需要区块链支持的分散操作（d-op）和可以集中化执行的操作（c-op）。d-op 操作使用去集中化的方法进行编码，并由实例（SC_1～SC_4）执行，而 c-op 类别的操作是使用集中化方法编码并由 CCC 执行。

集中化和去集中化的集成可以通过几种方式操作，包括如下两种。

• 不可消除的基于区块链的日志

可以操作图 5 中基于区块链的部分，作为记录各方认为值得在区块链和 TTP 节点中复制的事件的被动日志。被动的意思是 SC_1～SC_4 不参与执行活动，这完全是 CCC 的责任。当一个或多个缔约方不愿盲目信任 TTP 时，这种安排是有用的，例如因为 TTP 部署在买方的房地内，这是一种目前常见的商业惯例[10]。在这一安排中，d-op 集将包括旨在创建附加记录的操作，而 c-op 将包括所有合同操作。CCC 和 SC_1～SC_4 相互独立运作。

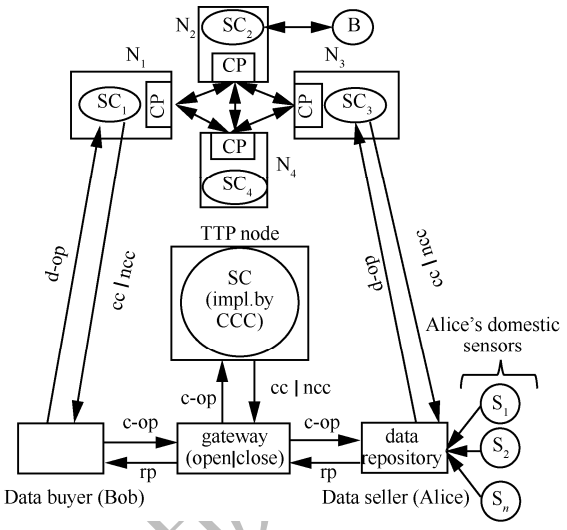


图 5　混合实现

• 基于加密货币的支付渠道

数据买家可以利用公共区块链（如比特币）提供的支付服务，并使用图 5 中顶部的 Satoshis 支付。只有在支付业务明显大于交易费用且不重复的情况下，才建议采用这种方法。在这项安排中，d-op 套装只包括发送付款操作；并且，CCC 只有运行在区块链（SC_1～SC_4）中的智能合同的协助下，才能验证数据买方已履行了支付义务。例如，数据买方应用程序可以通过比特币提交付款，等待交易确认，收集证据并提交给 CCC。

5　结束语

本文的中心目的是论证传统的商业合同可以实现自动化，并且取决于几个因素，集中化方法适合一些应用程序，而另一些则需要去集中化地实现，甚至是混合实现。刚刚开始探索智能合同的混合实现，但在研究比特币、Etalum 和 Hyperledger 提供的 API（JSON-RPC）的基础上，这一想法似乎是可以实现的。此外，它还具有实际意义，因为它将为当前块链平台的可伸缩性问题提供一个务实的答案。

参考文献：

[1] KIERON O. Smart contracts– dumb idea[J]. IEEE Internet Computing, 2017, 21(2): 97-101.

[2] MASSIMO B, LIVIO P. An empirical analysis of smart contracts:platforms, applications, and design patterns[C]// Financial

Cryptography and Data Security, 2017.

[3] ANDREAS A. Mastering Bitcoin[M]. New York: O'Reilly, 2017.

[4] MOLINA J C, SHRIVASTAVA S, STRANO M. A model for checking contractual compliance of business interactions[J]. IEEE Transactions on Service Computing, 2012, 5(2):276-289.

[5] MINSKY N H, LOCKMAN A D. Ensuring integrity by adding obligations to privileges[C]// 8th Int'l Conf. on Software Engineering, 1985: 92-102.

[6] MARSHALL L F. Representing management policy using contract objects[C]//IEEE First Int'l Workshop on Systems Management,1993: 27-30.

[7] SZABO N. Smart contracts: Formalizing and securing relationships on public networks[J]. First Monday, 1997, 2(9)

[8] NAKAMOTO S. Bitcoin: A peer-to-peer electronic cash system[Z]. 2008.

[9] BaiLis P, Ghodsi A. Eventual consistency today: Limitations, extensions, and beyond[J]. ACM Queue, 2013, 11(3).

[10] MOLINA-JIMENEZ C, SHRIVASTAVA S, WHEATER S. An architecture for negotiation and enforcement of resource usage policies[C]//IEEE Int'l Conf. on Service Oriented Computing & Applications (SOCA 2011), 2011.

人民邮电出版社

基于人工智能的输电线路鸟害检测方法

孙建刚，刘月灿，张晓亮，董耀众，贾真，李伟良
（国家电网有限公司信息通信分公司，北京 100761）

摘　要：为了保证电网能够安全稳定运行，输电安全在电力系统中起着中流砥柱的作用。输电线路在运行中会受到多种因素影响，其中鸟害直接导致电路发生闪络、短路、跳闸等现象。目前针对鸟害现象采取的物理防治方法效果不明显，人力物力投入巨大。提出采用人工智能的方法检测鸟类，根据检测结果决定是否启动超声波驱鸟，达到高效、准确、节能的效果。主要利用卷积神经网络算法中 YOLO 模型来实现小目标的检测，网络结构中使用残差模块增强图像特征提取的能力，使用多尺度的方法来保证对于小目标检测的准确性。通过摄像头采集样本图片，搭建网络模型，利用迁移学习的思想进行模型的训练。通过实验结果表明，人工智能的鸟类检测方法能够达到高效、准确的目的。

关键词：人工智能；卷积神经网络；输电线路；鸟害检测

1　引言

随着社会发展，电力需求急剧增长，电网安全稳定地运行是保障社会正常用电需求的前提。国家电网的业务包括：发电、输电、配电、变电、用电，任何一个环节出错都会对国民经济和人民生活带来巨大影响。输电在电力系统中起着中流砥柱的作用，是电网系统必不可少的部分，但是一般输电环节都处在野外环境，导致输电线路在运行中会受到多种因素影响。经调研，威胁输电线路安全运行的 3 个主要的灾害是鸟害、雷击和外力的破坏。鸟害是威胁输电线路安全运行的三大主要危害之一，会造成闪落、短路、跳闸等问题。江苏省鸟类繁多，据统计苏北地区 60%的输电线路故障是由鸟类造成的。可见鸟害的问题产生危害巨大，严重影响电力系统的安全，已经成为电力部门重点关注的问题[1]。

针对鸟害的防治工作，国家电网防治鸟害措施主要有：杆塔上安装防鸟刺、防鸟网、驱动风车，绝缘子上增加伞盖等[2]，这些措施存在鸟类对去鸟装置快速适应、设备安装初期就有防鸟死角、无风天气无法启动等问题。稍微有效的是超声波驱鸟[3]，但也存在声波发射器一直发射，鸟类可快速适应且设备耗能问题。因此提出一种基于人工智能的鸟类检测方法，对摄像头拍摄的图像进行分析来决定是否触发驱鸟器。

1962 年 Hubel 和 Wiesel[4]提出了卷积神经网络（CNN），在一次比赛中，Yann Lecun 首次使用 CNN 进行手写数字识别，并在此问题上保持了主导地位。CNN 算法在目标检测分为两类：一种是基于候选区域的 R-CNN 系列算法，分为两步，首先需要进行区域的提取产生候选区域，然后在候选区域上面进行分类与回归；另一类是 YOLO、SSD 系列的端到端算法，通过神经网络进行特征的提取得到特征图，在网络的最后同时进行预测分类的结果和区域的位置[5]。虽然人工智能在目标检测方面的应用很广泛（如人脸识别、无人驾驶等），但是在输电线路鸟害检测方面没有应用。针对输电线路上鸟类的检测是通过卷积神经网络算法中的 YOLO 模型进行图像检测。

2　概述

图像识别驱鸟装置由图像识别系统和驱鸟器系统两大部分组成，如图 1 所示。图像识别系统包括太阳能供电储电、摄像头、云台、运算处理器板等构成，驱鸟器系统包括太阳能供电储电、驱鸟超声波喇叭、驱鸟激光器组成。基于人工智能的输电线路鸟害的防治方法主要是通过图像识别系统拍摄输电线路的场景产生图像，通过服务器实施目标检测，预测目标矩形框并计数，当达到一定的阈值时，启动驱鸟系统，达到对鸟类进行驱赶的效果。本文主要研究使用卷积神经网络对输电线路上的鸟类进行检测。

人民邮电出版社

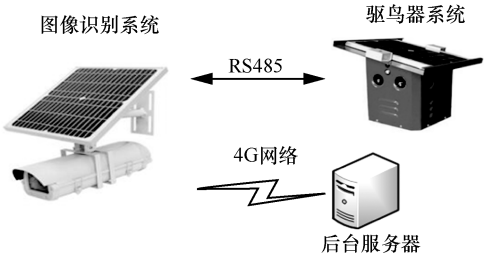


图 1　图像识别驱鸟装置

3　卷积神经网络算法介绍

卷积神经网络是由 3 部分组成，第一部分是输入层，第二部分是隐藏层，由卷积层和池化层的结合构成，第三部分是全连结的多层感知机分类器作为输出层[6]，如图 2 所示。输入层输入一张图像，通过隐藏层的卷积和池化层特征提取器提取图像的特征，输出层会根据提取的特征进行预测，长方体的长度代表概率的大小，可见属于鸟的概率是最大的。

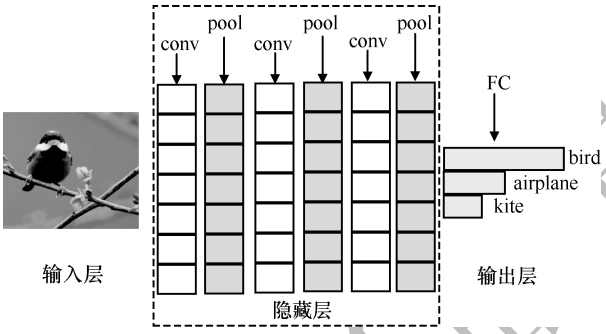


图 2　卷积神经网络组成

卷积层的功能是执行特征提取，卷积运算能够让原信号特征加强，并能够减低噪音[7]。图 3（a）是输入图像，图 3（b）是卷积核（权重），图 3（c）是输出图像。图 3 中每个格子中的数值代表图像的像素值，卷积核对左边图像做卷积操作，步长为 1 分别向横向和纵向移动。图 3（c）阴影部分的数值是通过图 3（a）中左上角浅色阴影的部分和卷积核进行卷积操作得出，具体为 1×1+1×0+1×1+0×1+1×1+1×1+1×0+0×1+0×0+1×1=4。

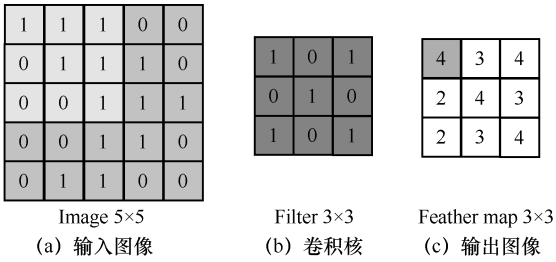


图 3　卷积层原理

池化层是可使特征图压缩以提取主要特征，从而简化神经网络计算的复杂度。池化有最大池化和平均池化两个种类[8]。最大池化是取池化核中最大的像素值输出，YOLO 模型采用最大池化，如图 4 所示。

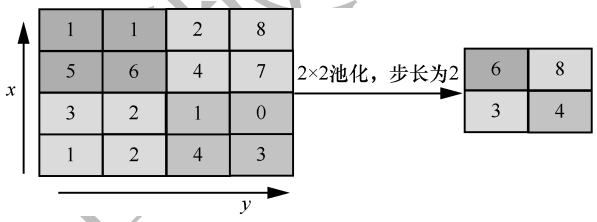


图 4　最大池化层原理

4　卷积神经网络中 YOLO 模型介绍

采用卷积神经网络算法中的 YOLO 模型进行检测，YOLO 模型首先将输入的图片调整为统一大小方便后面输入网络结构进行检测，接着调整好的图片进入卷积神经网络结构进行种类和位置的预测，最后采用非极大抑制的方法，抑制不是极大值的元素，搜索局部的极大值，通过对置信评分采用非极大抑制可以在检测结果所有框住物体的边界框中，去掉不合适的，找到最准确的方框。YOLO 模型的整个检测过程如图 5 所示。

下面详细介绍卷积神经网络算法中 YOLO 模型的原理，网络结构将输入的图片分成 $S\times S$ 的网格，简称栅栏，如图 6 所示。

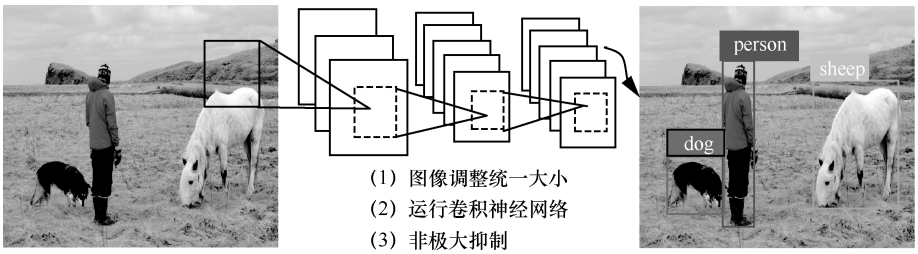


图 5　模型检测过程



图 6　网格划分

每个网格只负责预测物体的中心点落在该网格的目标。图 6 中，小狗的中心点落在一个网格中，则该网格只负责预测这只狗。预测的过程中，每个网格会划分 B 个边界框（bounding box），网络结构会预测边界框的置信度和边界框的大小（X,Y,W,H），分别表示边界框中心点的坐标与其宽高。边界框的置信度等于边界框含目标的可能性即 Pr(object)和边界框准确度 IOU 的乘积，置信度如式（1）：

$$\text{confidence} = \Pr(\text{object}) \times \text{IOU}_{\text{pred}}^{\text{truth}} \tag{1}$$

如何判断边界框含目标的可能性即 Pr(object)，若网格中含有目标中心则 Pr(object)=1，若网格中不含有目标的中心则 Pr(object)=0。IOU 表示预测的边界框与真实物体标注的实际框重合的部分占边界框与真实物体标注的实际框合并起来部分的比值。每个边界框可预测出属于 C 个类别概率值，预测的概率值就是在各个边界框所属类别的条件概率。置信度评分就是所属类别的概率与置信度的乘积，如式（2）：

$$\Pr(\text{class}_i \mid \text{object}) \times \Pr(\text{object}) \times \text{IOU}_{\text{pred}}^{\text{truth}} = \Pr(\text{class}_i) \times \text{IOU}_{\text{pred}}^{\text{truth}} \tag{2}$$

边界框的置信评分代表目标属于边界框中每个类别的概率和边界框匹配目标的准确度。最后通过置信度和非极大值抑制（non-maximum suppression，NMS）算法筛选网络的边界框，找到准确的边界框和所属的种类。

5　基于 YOLO 模型的鸟类检测

用于鸟类目标检测的网络结构的设计主要分成图像的特征提取和目标检测两部分。网络使用的是卷积神经网络，网络中包含卷积层、池化层、激活层、BN 层和全连接层。图像特征提取和目标检测的整体网络结构如图 7 所示。

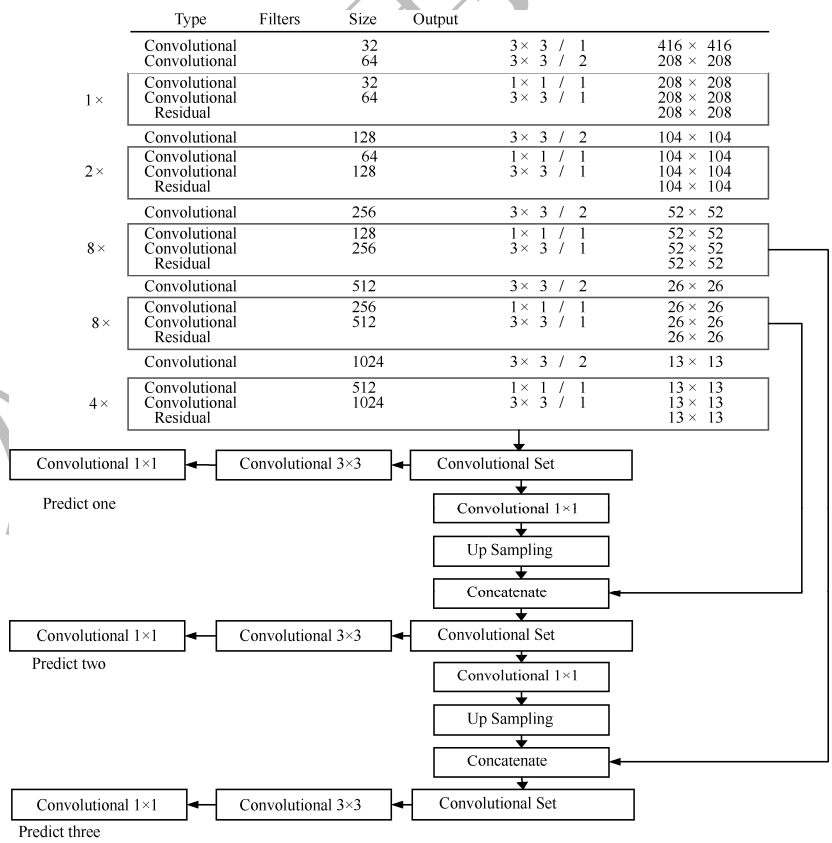


图 7　网格结构整体设计图

采用卷积网络来提取特征，主要用到 53 个卷积层，卷积层主要使用 1×1 卷积来进行卷积核的减少，使通道减少，然后是 3×3 卷积核。增加网络的深度能够提升网络的准确率，也会导致过拟合现象，因此网络中采用残差模块。残差模块可以有效地提取特征，将进入残差盒前的特征和残差盒输出的特征相结合，有效地对特征进行提取，残差模块结构如图 8 所示。

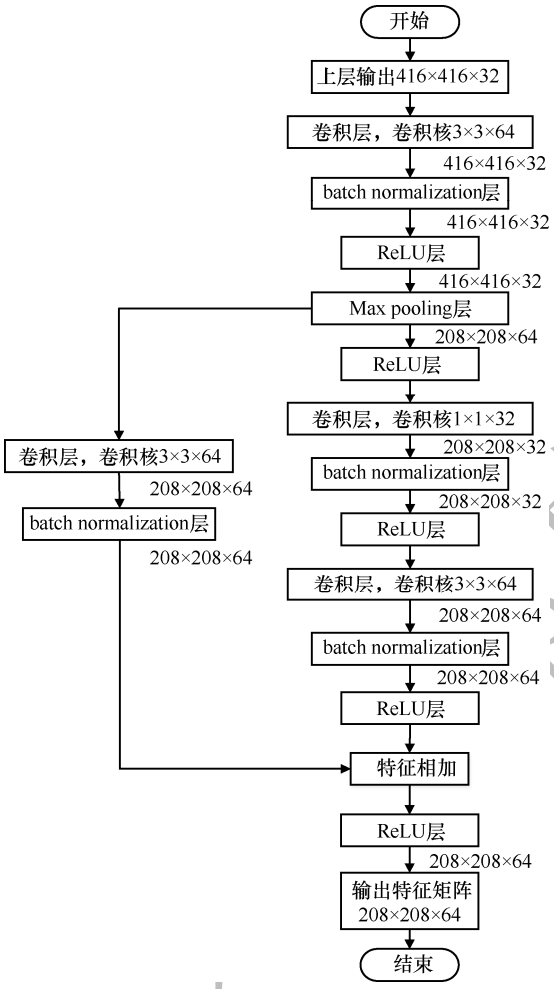


图 8 残差模块内部结构

目标检测的网络结构采用多尺度的预测方式，根据对 YOLO 设计理念的介绍，每个网格只负责预测物体中心点落在该网格的物体。试想对于小目标的物体，每个网格可能有多个物体的中心点，因此 YOLO 不能预测这种情景的物体，而对于输电线路鸟类的检测正好符合小目标检测的这种场景。YOLO 算法经过改进使用多尺度的方式针对小目标进行预测。

多尺度预测就是经过前面特征提取网络结构之后，经过 7 次卷积操作后得到第一个特征图，接着通过卷积操作和上采样并且与神经网络的 61 层提取的特征相结合，再通过 7 次卷积操作后得到第二个特征图，重复的操作可以得到第 3 个特征图。这就形成了 13×13、26×26、52×52 的 7 个特征图，分别进行检测得到物体的位置和种类。特征图大小对应的使用范围见表 1。

表 1 特征图大小对应的使用范围

特征图	13×13	26×26	52×52
适用目标	较大的目标	中等的目标	较小的目标

实验检测结果如图 9 和图 10 所示。



图 9 单只鸟检测

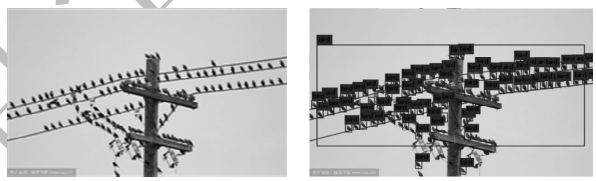


图 10 多只鸟检测

6 结束语

基于人工智能的输电线路鸟害检测方法通过新的角度对鸟害的防治工作采取新的策略。随着深度学习与人工智能的迅速发展，在电力系统中通过引进新的技术来达到电网安全稳定运行的效果。鸟害防治的主要过程是通过图像识别系统采集图像信息，检测系统快速做出响应，决定是否驱动超声波驱鸟器进行驱鸟操作，保证输电的安全。从实验结果来看，针对输电线路上面的小目标，模型能检测出来。但是对于一些不同角度摄像头的拍摄，还存在鸟类无法检测以及与鸟类相似形状如飞机等物体的误检测，因此在之后还需要进一步对数据集进行扩充，对算法进一步优化，以提高检测的精确度。

参考文献:

[1] 唐子峰, 袁翔, 廖志雄, 等. 广东韶关电网鸟害跳闸故障统计分析及防护[J]. 电瓷避雷器, 2018(2): 20-24.

[2] 陈淦. 110kV 输电线路防雷及防鸟害设计[D]. 北京: 华北电力大学, 2016.
[3] 朱子剑. 输电线路的鸟害防护[D]. 长春: 长春工业大学, 2018.
[4] 王祎瑞. 基于深度卷积神经网络的变电站设备识别[D]. 沈阳: 沈阳农业大学, 2018.
[5] 黄莉芝. 基于深度卷积神经网络的目标检测算法研究[D]. 成都: 西南交通大学, 2018.
[6] 杨洁. 基于卷积神经网络的目标检测研究[D]. 衡阳: 南华大学, 2018.
[7] 李涛. 基于卷积神经网络的图像分类模型的研究与应用[D]. 武汉: 湖北工业大学, 2018.
[8] 吴阳阳. 基于卷积神经网络的字符识别算法研究和实现[D]. 广东: 广东工业大学, 2018.
[9] BASAEED E, BHASKAR H, AL-MUALLA M. CNN-based multi-band fused boundary detection for remotely sensed images [C]//6th International Conference on Imaging for Crime Prevention and Detection (ICDP-15), July 15-17, 2015, London, UK. Piscataway: IEEE Press, 2015.
[10] 列剑平, 于江萍, 鄂明菊,等. 高压输电线路防鸟设施应用及效果研究[J]. 东北师大学报(自然科学版), 2013, 45(2):118-121.

人民邮电出版社

基于深度学习的高效实时性 *M*:*N* 模式人脸识别方法

郑开发[1,2]　李宏伟[1,2]

（1. 国网电子商务有限公司（国网雄安金融科技集团有限公司），北京 100053;
2. 国家电网有限公司电力金融与电子商务实验室，北京 100053）

摘　要：文中系统提出一种人脸识别方法及可用系统，首先将视频分为识别帧与普通帧，通过构建跟踪器的方式对人脸进行跟踪识别。其中，跟踪器获取摄像头采集的图像中的识别帧图像；并对识别帧图像进行人脸检测与识别，获取识别帧图像中的人脸位置信息与身份信息。同时，对已识别人脸进行周期性的身份核实，通过引入缓冲机制，过滤掉短时间内的误判。本方法有效避免了已识别人脸与人像数据库的重复比对，进一步提高了计算效率，且有效避免了人脸误判及反复识别问题。这种人脸识别方法非常适合国网电商的应用场景，具有一定的创新性。

关键词：人脸识别；身份信息；跟踪器；国网电商

1　引言

在人工智能的图像、语音、自然语言和知识图谱的几大领域中，图像识别技术占据着极为重要的地位，而随着产业的升级和信息技术的不断发展，AI 领域图像识别技术的应用场景不断扩展，刷脸支付、车牌识别、医疗诊断、人脸识别、指纹识别以及遥感图像识别等都属于图像识别技术的典型应用场景。在电力系统和电商行业中，图像识别技术也有着较为广泛的运用，为了保证人工智能中的图像识别技术能够较好地服务于电力行业，文中提出了基于电力电商场景的一种时效 *M*：*N* 模式的人脸识别方法，正是文中就人工智能中的图像识别技术展开具体研究的目的所在。

为了较好地完成文中就人工智能中的图像识别技术展开的研究，首先需要深入了解图像识别技术。作为人工智能领域的重要组成部分，图像识别的发展先后经历了文字识别、数字图像处理与识别、物体识别三个发展阶段，而在今天的图像识别技术中，其本身所具备的功能早已超过了人类的极限，这也是人工智能的图像识别技术能够在我国多种领域实现较好应用的原因所在[1]。图像识别技术本身的原理并不算太过复杂，信息的处理是这一技术的关键点所在，由于应用计算机实现的图像识别技术本身与人眼识别并不存在本质的差别，这就使得图像识别技术同样需要根据自身对图像的记忆完成具体的识别工作。在人类进行图像识别的过程中，人类的大脑会将图像的特征进行提取，并结合大脑中以往对各类图像的认知判断自身是否对图像存在过印象，这就是人们能够在观看一张图片后快速对其识别的原因所在[2]。结合人类识别图像的原理，在计算机进行的图像识别中，计算机首先就能够完成图像分类并选出重要信息、排除冗余信息，根据这一分类计算机就能够结合自身记忆存储结合相关要求进行图像的识别，这一过程本身与人脑识别图像并不存在本质差别[3]。对于图像识别技术来说，其本身提取出的图像特征直接关系着图像识别能否取得较为满意的结果。值得注意的是，由于计算机归根结底不同于人类的大脑，计算机提取出的图像特征存在不稳定性，这种不稳定性往往会因为计算机提取图像特征的明显与普通影响图像识别的效率与准确性，由此可见图像特征对人工智能中图像识别技术的重要意义[4]。

2 主流技术现状和缺点

随着电子技术的不断发展，人脸识别技术得到了广泛的应用。目前，人脸识别技术主要采用的是人脸识别 *M*：*N* 模式，人脸识别 *M*：*N* 模式是通过计算机对场景内所有人进行面部识别并与人像数据库进行比对的过程，是动态人脸比对，能充分应用于多种场景，例如安防、迎宾、机器人应用等。

基金项目：国家电商公司综合计划项目（5100/20191-72002B）

人民邮电出版社

在实际应用过程中，人脸识别 *M*：*N* 模式还存在一些问题：实时对整个场景内所有人进行面部识别并与人像数据库对比，需要庞大的计算量，对终端设备的性能要求过高；人脸识别 *M*：*N* 模式虽然具有动态比对与非配合性等优点，但由于场景内人数自由变化，人物位置自由变化，人脸角度、方向等随意变化等因素，会造成人脸在场景内的一段时间内出现已识别人脸又被判断为陌生人、同一人脸反复识别等问题。

因此，如何有效快速地进行人脸识别，是一项亟待解决的问题。文中针对上述两种问题，采用隔帧检测的策略减轻计算压力，并引入跟踪器机制实现对场景中人脸的跨帧记忆功能，并通过根据已记忆的人脸进行 1：1 模式人脸识别进行身份校对及跟踪器的位置校对，避免了已识别人脸与人像数据库的重复比对，进一步提高计算效率，最后通过加入识别缓冲机制，有效避免人脸误判及反复识别问题[5]。

3 *M*:*N* 人脸识别方法思路

文中提出一种人脸识别方法思路，当需要对人脸进行识别时，首先构建跟踪器，其中，跟踪器中包括人脸位置信息和对应的身份信息；然后获取摄像头采集的图像中的识别帧图像，对识别帧图像进行人脸检测，获取识别帧图像中的人脸位置信息；将识别帧图像中的人脸位置信息与跟踪器中的人脸位置信息进行比对，判断识别帧图像中的人脸位置是否与预先构建的跟踪器中的人脸位置重叠，若重叠，则判断跟踪器中的人脸位置对应的身份信息是否为已注册人员，若是，则将识别帧图像与跟踪器中的人脸位置对应的图像，采用 1：1 模式进行身份核实，输出识别结果。

3.1 隔帧检测

程序获得摄像头捕捉的图像后，可根据设置的参数跳帧数 *N*，实现每隔 *N* 帧对图像进行一次识别（在文中，跳过的帧被称为普通帧，进行识别操作的帧被称为识别帧）。识别过程如图 1 所示。首先从待识别图像中检测出人脸部分，并获得人脸位置信息，然后对检测出的人脸进行特征提取，得到人脸特征集合，最后依次将每个人脸特征与人脸信息库中的数据进行比对，对比方式为通过计算特征向量之间的欧氏距离来得到人脸相似程度，相似度计算式为：

$$y=\sqrt{(x_1-d_1)^2+(x_2-d_2)^2+\ldots+(x_n-d_n)^2}$$

$(x_1,x_2,x_3,\cdots,x_n)$：待检测人脸特征向量；

$(d_1,d_2,d_3,\cdots,d_n)$：人脸信息库中的一条人脸特征向量；

$y_{\min}$：待检测人脸与人脸信息库比对后的相似度最小值；

当 $y_{\min}$ 小于阈值 k 时判定当前人脸为注册人脸，否则为陌生人。

识别结果将与人脸位置信息一同传入跟踪器，在后续帧进行人脸跟踪。

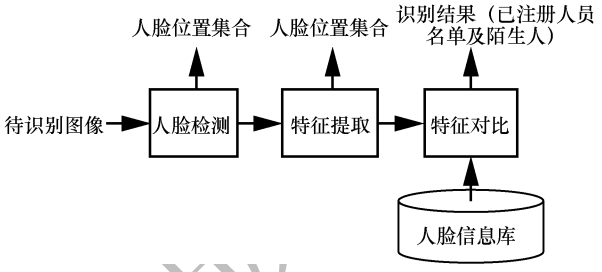


图 1　多目标人脸识别流程

3.2 跟踪器跨帧记忆

本发明引入跟踪器机制实现对已识别人脸的跨帧记忆功能，具体跟踪流程如图 2 所示。

在识别帧，首先将识别结果及对应的位置信息传入跟踪器池，即对所有的人脸及识别结果分别设置跟踪器。

在普通帧，跟踪器正常跟踪人脸图像，在识别帧，跟踪器的位置信息会与当前帧人脸检测出的人脸位置信息进行比对，根据各跟踪器的比对结果，采用以下不同的处理方式。

在人脸检测出的位置集合中，如果存在未和跟踪器重叠的人脸，视为新增人脸，将按照图 1 流程进行人脸识别；

所有跟踪器中，如果不包含当前帧的人脸位置，视为该跟踪器的人脸消失，将销毁该跟踪器。

当跟踪器与当前帧的人脸位置重叠时，视为该跟踪器为之前识别帧的记忆信息，根据跟踪器所携带的身份信息，采用以下不同处理方式。

跟踪器的身份为陌生人时，将按照图 1 流程进行人脸识别；

跟踪器身份为已注册人员时，将按照 1：1 模式进行身份核实，核实以后将对跟踪器进行校准。

3.3 1：1 模式跟踪校正

对于已识别的人脸跟踪器，后续每个识别帧将对其验证及位置校正，流程如图 3 所示。

人民邮电出版

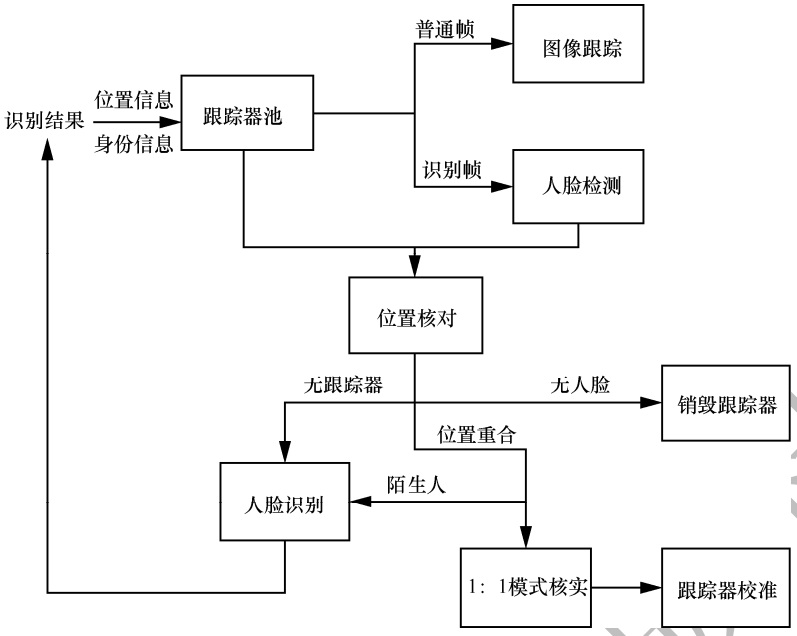


图 2　跟踪器工作流程

首先根据跟踪器携带的身份信息，从人脸信息库中将对应的特征信息查出，然后与当前帧与之重叠的人脸所提取的特征做对比，计算两个特征向量之间的欧式距离 y，当 y 小于阈值 j 时，该跟踪器身份核实成功，然后将该与之重叠的人脸位置信息重新输入该跟踪器，进行位置校正。

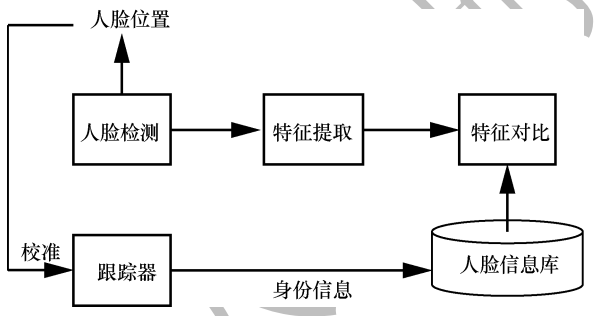


图 3　1：1 模式跟踪校正流程

3.4　容错缓冲

本研究中跟踪器状态除已识别、陌生人外，还加入了缓冲状态来提供识别容错功能，容错缓冲机制如图 4 所示。

在识别帧，人脸识别成功的情况下，跟踪器为已识别状态，即当前人脸识别结果为已注册人脸；在识别失败的情况下，跟踪器为缓冲状态，即暂时保留当前识别状态，不输出识别结果。

在识别成功状态的跟踪器被 1:1 校验成功的情况下，保持成功状态，输出识别结果；在校验失败的情况下，转入缓冲状态，不输出识别结果。

在缓冲状态的跟踪器被识别成功的情况下，转为已识别状态，输出识别结果；在再次识别失败的情况下，跟踪器转为陌生人状态，输出识别结果。

在陌生人状态的跟踪器被识别成功的情况下，转

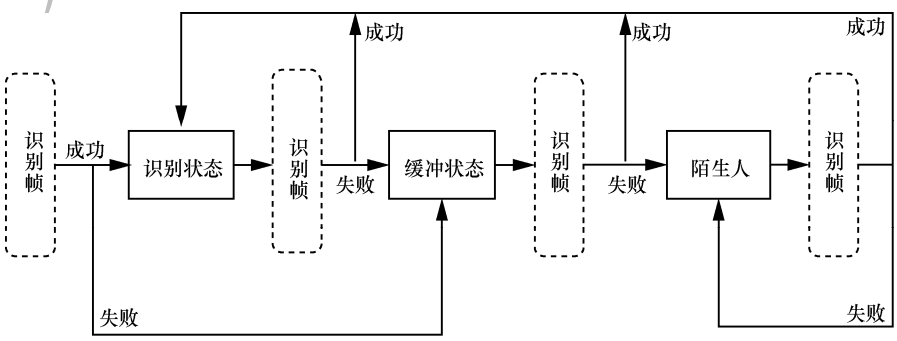
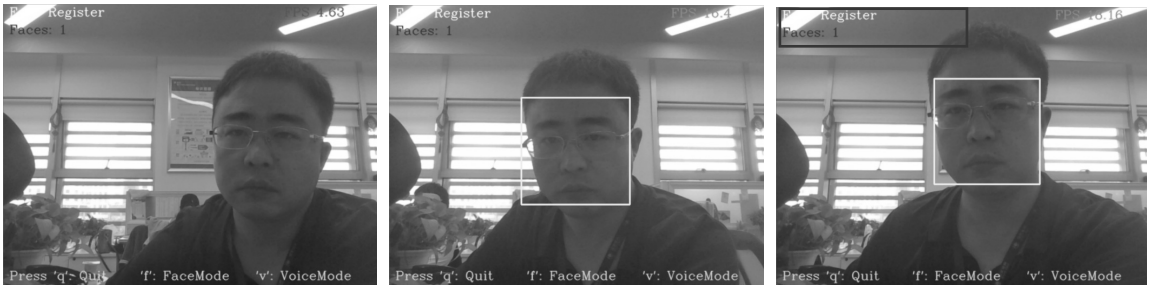


图 4　容错缓冲机制流程



（a）逐帧识别 FPS　　（b）跨帧识别 FPS　　（c）跨帧跟踪识别 FPS

图 5　人脸识别三种实现方式对比

为已识别状态，输出识别结果；再次识别失败的情况下，跟踪器转为陌生人状态，输出识别结果。本步骤可根据设备识别效率适当改变缓冲次数，以保证场景中人脸角度或方向变化导致的容错率。当前缓冲次数为 1。

本文系统提供了一种人脸识别方法，采用隔帧检测的策略减轻了计算压力，并引入跟踪器机制实现了对场景中人脸的跨帧记忆功能，并根据已记忆的人脸进行 1：1 模式人脸识别进行身份校对，避免了已识别人脸与人像数据库的重复比对，进一步提高了计算效率，最后通过加入识别缓冲机制，有效避免了人脸误判及反复识别问题。

4　*M*：*N* 人脸识别方法实例

4.1　识别性能

文中应用 dlib 库中的相关模型对上述方法进行了实现，其中，人脸检测方法使用 get_frontal_face_detector 函数[6]。同时，人脸的特征参数提取算法应用了 dlib_face_recognition_resnet_model_v1.dat 模型[7]。如图 5 所示，本次分别对人脸识别过程采用逐帧识别、跨帧识别、跨帧跟踪识别 3 种方式进行实现，对 3 种实现方式的实现性能做对比分析，其中跨帧数设置为 7 帧。同时，为了体现该方法的实用性以及泛用性，本次实现在 CPU 环境下，型号为移动版 i7 4700MQ 四核八线程处理器[8]。

实验显示，逐帧识别的情况下，图像显示的平均每秒帧数 FPS 为 4.63；跨帧识别的情况下，FPS 数为 16.4；跨帧跟踪识别的情况下，由于跟踪器记忆功能，只对已识别人脸做 1：1 核对，因此进一步提高了效率，FPS 数达到了 18.16，三者对比如图 6 所示。

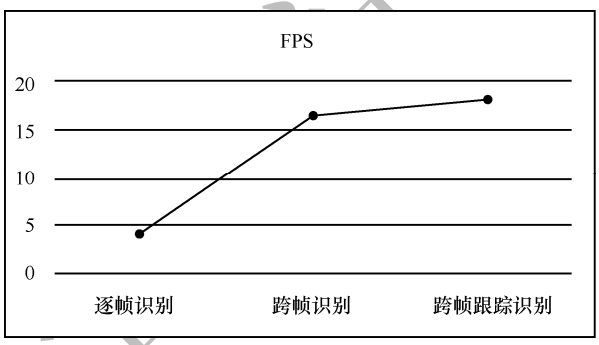


图 6　识别性能对比

4.2　缓冲容错

从上图中可以看出，已识别人脸框显示为白色实线，当已识别人脸因移动角度等问题导致在当前帧不能识别时，人脸框显示为白色虚线，即缓冲状态，如图 7 所示，缓冲状态时间范围内会依然保存之前识别人脸身份信息，若人脸再度被识别则恢复成已识别状态。若缓冲状态结束时依然是未识别状态则判断为陌生人，人脸框转为黑色实线[9]。

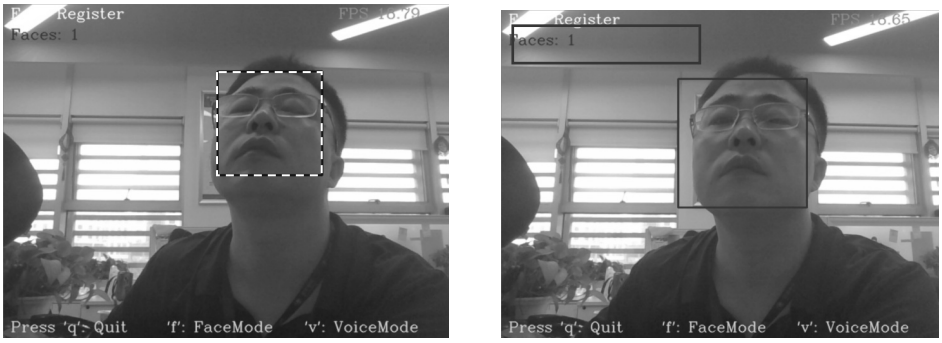
5　结束语

文中主要的创新点及优点如下：

文中采用隔帧检测的方式进行人脸识别，对于未参加检测的帧，采用了轻量级跟踪器进行标记，从而大大减轻了计算压力；

在已识别的帧，文中由于使用了跟踪器，实现了人脸信息的记忆功能，因此对于之前已识别过的人脸，只需要进行 1：1 模式的验证处理，而不需要重新对比人脸信息库中的所有人脸，因此减轻了计算压力；

文中加入识别缓冲机制，对一段时间内处于场景内自由活动的人脸具有识别容错性，有效避免人脸误判及反复识别问题。



（a）缓冲状态　　（b）未识别状态

图 7　缓冲容错示例图

参考文献：

[1] 卜富清. 基于人工神经网络的图像识别和分类[D]. 成都：成都理工大学, 2010.

[2] 刘军. 人脸图像识别关键技术的研究[D].北京：北京邮电大学, 2015.

[3] 孟广仕. 图像识别技术在人工智能中的应用[J]. 信息与电脑, 2018(12): 152-153.

[4] 杨琛.试析人工智能中的图像识别技术[J]. 信息通信, 2017(1): 16-17.

[5] JOHNSON D, MENEZES A, VANSTONE S. The elliptic curve digital signature algorithm (ECDSA)[J]. International Journal of Information Security, 2001, 1(1): 36-63.

[6] 王晓华. 深度学习与计算机视觉实战[M]. 北京：清华大学出版社, 2018.

[7] BERTINO E, SHANG N, WAGSTAFF SS. An efficient time-bound hierarchical key management scheme for secure broadcasting[J]. IEEE Transactions on Dependable and Secure Computing, 2008, 5 (2): 65–70.

[8] MIGUEL C, LISKOV B. Practical byzantine fault tolerance. USENIX Technical Program - OSDI 99.1999.

[9] JOHNSON D, MENEZES A, VANSTONE S. The elliptic curve digital signature algorithm (ECDSA)[J]. International Journal of Information Security, 2001, 1(1): 36-63.

人民邮电出版社

基于数据中台的电力企业统一数据模型优化完善方法

王家凯，冯定东
（国家电网有限公司大数据中心，北京 100031）

摘　要：随着中国大数据技术的不断发展，数据作为一种资源已经成为社会共识。目前，中国电力企业已经在开展统一数据模型的设计和应用，对数据资源进行标准化管理，并取得了较大的成果。随着业务的不断发展和管理的变革，结合数据中台概念，需要不断地对数据模型进行优化完善。结合数据模型管理方面的经验，探索基于数据中台、具有电力企业特色的企业级数据模型优化完善及应用方法，为解决数据共享、实现数据价值再造提供借鉴。

关键词：数据模型；数据中台；大数据；优化完善

1　引言

大数据时代，数据已经成为金融企业的战略资源。从信息化建设的源头发现并定义好数据资产，促进业务围绕数据的高效协同管理和应用，夯实企业数据资产质量，从而为企业带来及时有效的决策指引以及业务创新，发挥出数据资产的真正价值。

信息化建设中各单位依据各自需要所建设的信息系统形成了大量的信息孤岛，制约了数据与信息共享应用的发展。特别是随着编制体制的调整改革，以前归属于同一部门的业务系统现在可能分散在多个不同的部门。随着社会的不断发展，跨部门、跨单位、跨层级的跨域信息共享成为信息化建设新的增长点。传统的通过整合或组织系统内部的接口和数据映射的方式，导致开发接口多且复杂、开发成本高等问题。

2015 年年底，阿里巴巴对外宣布全面启动中台战略，构建数据处理技术时代更具创新性、灵活性的“大中台、小前台”组织机制和业务机制，即作为前台的一线业务会更敏捷、更快速地适应瞬息万变的市场，而中台将集合整个集团的运营数据能力、产品技术能力，对各前台业务形成强力支撑。

本文结合数据模型管理方面的经验，探索建立基于数据中台、具有电力企业特色的企业级数据模型优化完善及应用方法，为解决跨域、跨部门、跨层级的数据共享问题提供借鉴。

2　数据模型优化完善思路

2.1　业务驱动、问题导向

以解决目前电力企业横向业务协同面临的突出问题为切入点，以支撑重点业务以及纵向业务数据贯通为重点，基于数据中台建设开展模型设计工作。

2.2　业务驱动、问题导向

继承现有成熟的企业级端到端业务的流程设计和核心业务应用系统的设计成果，进行全域核心业务数据模型设计，实现成果复用。

2.3　示范应用、迭代完善

统一组织集中开展模型设计，在企业总部和下属单位开展试点示范应用，迭代完善模型设计成果，提升模型可用性。充分考虑可持续性，确保成果根据业务变化的适应性与扩展性，不出现体系性的重大颠覆，且保证现有业务系统持续稳定运行。

2.4　质量优先、实用可控

充分考虑任务的复杂性，模型设计应采用先进的方法论，遵循先进的技术架构，建立阶段性输出成果评审机制，对成果进行严格的质量把控；分期分批对接试点示范单位开展实用性验证与评价工作，确保模型设计成果实用可控。

3　优化完善需求分析

基于电力企业前期数据模型及核心业务系统建设成果，结合目前数据中台的相关技术，根据数据中台

人民邮电出版社

数据库选型，对统一数据的物理模型进行设计，形成适用企业全过程的物理模型，支撑数据中台建设。

3.1 确定数据中台核心业务范围

基于发输变配用等核心业务，参照跨业务、跨层级间的数据共享范围，明确核心业务范围及涉及的核心业务系统，形成《核心业务范围列表及核心业务系统清单》。

3.2 收集核心业务系统数据字典

基于《核心业务系统清单》，开展数据字典的收集梳理工作。由涉及业务系统建设的厂商配合完成从运业务系统中导出数据字典信息，同时完成表、字段、关联关系及涉及的编码表等业务描述信息的补充完善工作，形成《核心业务系统数据字典》。

3.3 识别核心业务数据对象

（1）核心业务数据对象基础版

基于业务系统建设的现有成果，识别出核心业务数据对象及跨域数据对象，结合《核心业务系统数据字典》补充核心业务对象的属性，确定数据表唯一性，统一数据属性的含义、名称及相关编码规则等信息，明确数据来源、所属业务部门以及是否为主数据对象等信息。

（2）差异分析

将初步形成的《核心业务数据对象清单（基础版）》下发至试点下属单位，由试点单位结合本单位实际业务情况与《核心业务数据对象清单（基础版）》进行差异对比分析，并形成《全域核心业务数据对象清单差异清单》。

（3）核心业务数据对象最终版

结合试点单位的《全域核心业务数据对象清单差异清单》，对《核心业务对象清单（基础版）》进一步修订完善，最终形成《核心业务数据对象清单（确认版）》，为概念数据模型的设计完善奠定基础。

4 数据模型完善设计

企业数据模型主要包括概念模型、逻辑模型和物理模型 3 部分内容，其中，数据模型在数据中台中的最终体现形式为物理模型。结合电力企业现状和实际面临的问题，基于《全域核心业务数据对象清单差异清单》，结合 IEC 61970/61968/62325 CIM 标准，优先完成逻辑模型设计工作，在逻辑模型设计成果的基础上，完成概念模型校核，并基于数据中台选型，完成物理模型的设计，最终形成一套完整的企业数据模型设计成果。

4.1 逻辑模型映射关系建立

基于《全域核心业务数据对象清单差异清单》，分别对照国际标准 IEC 61970/61968/62325、SG-ERP 模型，与核心业务数据对象和属性建立映射关系，并将映射结果填写到《全域核心业务数据对象清单差异清单》中。如存在不能映射的数据项，则作为本次逻辑模型扩充完善的需求。

4.2 逻辑模型完善设计

根据业务需求，梳理并分析 IEC 61970/61968/62325 CIM 和 ERP 中的实体、属性、关联关系，如果 IEC 61970/61968/62325 CIM 和 ERP 中有用的实体能够满足实际业务需求，则直接使用此实体及其属性；如果某个实体能够部分满足数据对象的数据需求，根据实际业务情况，则选择此实体，并创建一个新实体，所创建的新实体继承所选择的实体，并根据业务需求在所建新实体中添加属性及关联关系；如果没有完全符合数据对象的数据需求的实体，则创建一个新实体，新创建的实体要继承其他实体或直接继承基实体 Identified Object（有个别实体本身就是基实体），然后根据实际业务在新建实体中添加新属性，最后根据业务需求与其他实体进行关联。

基于各业务领域的设计成果，结合全域核心业务对象清单中的跨专业数据对象进行分析讨论，将数据模型进行规范、统一含义、去重、归并、整合、拆分，形成一套统一的企业级一体化逻辑模型设计成果。

4.3 概念模型校核

按照整合后的逻辑模型设计成果，在概念模型的基础上，结合逻辑模型调整内容，反向对概念模型进行进一步校核，调整概念模型实体及实体间的关系，形成企业数据概念模型。

4.4 物理数据模型设计

物理模型设计阶段，以逻辑模型和概念模型为输入，将实体和属性转换为物理数据模型的数据表和字段，逻辑模型中实体之间的关系转化为表之间的主外键关系。依据源端业务系统典型设计，结合业务应用需求，在满足三范式规范化要求的基础上，根据数据库产品特性，完成物理数据模型设计。完成实体、属性与表、字段的映射关系的梳理。编制形成《全域核心业务物理数据模型说明书》。

人民邮电出版社

5 中台数据表设计

GBase 8a 是一种 MPP 型数据库产品，采用列式存储、列式压缩、智能索引等特有技术对数据进行存储、计算，具体包括复制表、随机分布表、哈希分布表、临时表和 Nocopies 表 5 种实体型表数据。

以 GBase 8a 为例作为数据中台的数据库选型，将初步设计的物理表按照复制表、随机分布表、哈希分布表、临时表和 Nocopies 表 5 种形式进行划分，完成基于 GBase 8a 数据库技术特性的数据表存储优化设计。

5.1 数据表存储优化设计

（1）哈希分布表

将数据表中的某一列指定为哈希列，数据将按照哈希算法的取值存储到不同的节点上。每个节点上只存储一部分数据。这种存储策略，将大表数据进行分拆，实现分布式存储。

（2）随机分布表

随机分布表创建时不需要定义哈希字段，数据随机存放在不同节点，数据存储比较分散。当表数据量较大时，不能确定哈希列字段，在单表多条件随机组合查询场景较多的情况下，可以创建为随机分布表。

（3）复制表

复制表中的数据是在 GBase 8a 集群各数据节点上分别存储相同的、完整的全量数据。使用该实体型表数据时，直接访问各数据节点并读取复制表中的数据，接着进行查询、计算等操作，减少表数据的网络传输频率，提升查询性能。

（4）临时表

临时表中的数据仅存在于当前会话中，会话中断后临时表被释放。

（5）Nocopies 表

Nocopies 表中的数据不产生副本；使用 Nocopies 表既可以提升数据加载、insert 等性能，也可以节省磁盘空间，但存在单点故障风险。

5.2 字段数据类型转换

按照 GBase 8a 数据库特性要求，将数据表字段类型转化为 GBase 8a 支持的数据类型。

5.3 生成建库脚本

基于物理表分类规划结果，填写物理数据模型类型表清单，并从物理数据模型中导出标准 Oracle 建库脚本，基于脚本转换程序，生成 GBase 8a 数据库脚本。

6 结束语

统一数据模型是一种数据管理标准，基于统一的标准进行数据中台的建设，既能保证数据中台的功能、性能等，又能规范数据格式、统一企业全部的数据资源类型。数据作为一种资源，已经成为了社会共识。数据在通过数据模型进行标准化之后，如何发挥更大的作用是亟待解决的问题。标准化的数据，应该根据一定的规则进行分类和编码，方便用户对数据资源的检索和获取，因此，数据模型在设计过程中，要考虑后续的一些数据资源目录方面的内容。

参考文献：

[1] 陆燕. 企业概念数据模型研究与实践[J]. 金融电子化, 2018(6): 68-70.
[2] 高国伟. 阿里巴巴技术中台的“云启示”[J]. 项目管理评论, 2018(3): 26-27.
[3] 车品觉. 建设数据中台, 赋能创新改革[J]. 新经济导刊, 2018(10).
[4] 梁国迪. 基于公共信息模型的电网信息建模研究及应用[D]. 郑州: 华北水利水电大学, 2017.
[5] 朱鹏. 基于 IEC-CIM 标准的电力安全生产管理系统设计与实现[J]. 科技创新与应用, 2019(8): 82-83.
[6] 国家电网有限公司. 全域核心业务数据模型设计方法及规范[Z]. 2018.
[7] 张宿新. 基于 IEC_CIM 的营配调一体化模型互联网应用研究[J]. 微型电脑应用, 2017(4): 65-68.
[8] 刘玉玺, 欧阳红, 李刚, 等. 基于 IEC_CIM 的营配网末端设备公共信息模型设计[J]. 智慧电力, 2019(2): 75-81.
[9] 邹红霞, 王桢, 胡欣杰. 基于标准化建模的跨域信息共享应用研究[J]. 计算机应用与软件, 2019(2): 29-32.

人民邮电出版社

基于物联网标识的物资安全电子追溯

崔九鑫[1,2]，吕梓童[1,2]
(1. 国网电子商务有限公司(国网雄安金融科技集团有限公司)，北京 100053;
2. 国家电网有限公司电力金融与电子商务实验室，北京 100053)

摘　要：能源电力行业是国民经济发展中最重要的基础产业之一，涉及面广、产业链长，与国家安全、社会稳定、人民生活密切相关，也是我国工业互联网建设的重点布局领域之一。同时面向能源电力行业的生产、制造、运行、服务特色，建设电力设备全生命周期管理应用能力、分布式能源数据共享支撑应用能力、用能需求共享服务能力、电力设备重要产品追溯管理应用。打造基于标识技术的用能需求共享服务应用，是适应企业综合能源业务发展需要，符合国家智慧能源政策，满足工业互联网技术要求，迎合用户用能需求的必由之路。通过物联网标识的物资安全电子追溯，既体现企业作为落实物资安全追溯的主体的责任，又能起到对产品的宣传作用，上下游企业亦可通过日常用软件进行追溯信息的查询，方便快捷。该方案可较好地权衡企业、政府、用户之间的权利和利益，是一种复杂度较低、可快速部署的物资安全电子追溯方法。

关键词：物资安全；追溯系统；编码

1　引言

物资安全问题是所有企业共同面对的一大挑战，它不仅直接关系到生产安全，严重影响各行各业的生机，还关系到全球的经济发展、社会的生态建设和可持续发展等诸多方面[1]。2019 年，国家电网有限公司提出了“三型两网、世界一流”战略目标。作为推进“三型两网”建设的重要内容和关键环节，泛在电力物联网的建设正在加快推进。“兵马未动，粮草先行”，物资作为核心资源对企业发展至关重要。现代（智慧）供应链是泛在电力物联网在物资领域的具体实践与应用。

国家电网公司党组向全系统发出了新时代践行“人民电业为人民”的呼吁倡议，着力推进电网高质量发展，大力实施质量强网战略，建设本质安全电网。设备质量是电网安全稳定运行的物质基础，“选好选优”设备是实现质量强网、推动企业高质量发展的关键。全面提升采购设备的质量，既是全面贯彻落实质量强网战略的重要举措，也是电力工作为民出发、为民所想，服务社会、服务民生，落实“人民电业为人民”的具体体现。物资的安全存在于从原材料、生产、供给、配送到最终实施的全生命周期的每个环节中，任何一个环节的问题，都可能导致严重的安全问题，甚至于引发安全事件。因此，让物资的整个生态链活动处于有效的监控之中，将可追溯所有安全键点，实现物资从“材料到产源”全程保质保量的管理可行方案。

我国对“战略物资储备安全”的立法审议，已在各界人大集体讨论进行中。对物资实行追溯制度即是国家法律法规的要求，又是所有生产企业的义务。根据当前的政策，物资追溯体系的建设应以企业为主体进行，亦可由第三方平台为企业提供电子追溯的服务。

2　相关工作

物资储备是一个国家的地区国防建设和国民经济建设的重要组成部分，古今中外无论哪一个国家、哪一个帝王都十分重视国家战略物资的储备工作。按照储备的主体和物资储备的品种可以分为生产者储备、缓冲储备、行业储备、特种储备、民间储备等。

2009 年国家电网为了满足应对重特大自然灾害抢险救援的需要，全面提高公司应急物资供应保障能力，于 8 月 20 日印发《国家电网公司应急物资储备实施方案》。物资按照“统筹管理、科学分布、合理储备、统一调配、实时信息”的原则储备。应急物资储备工

基金项目：国网电商公司综合计划项目（5100/2019-72002B）

人民邮电出版社

作主要根据物资种类、占用资金量、市场供应情况及减少维护等综合因素，视不同情况采取实物储备、协议储备、动态周转相结合的储备方式[2]。所以物资的安全的重要性不言而喻，使用电力物联网标识进行物资安全电子追溯的关键性需求大大加强。

物资安全电子追溯系统是利用电力物联网标识来追溯，关键技术是标识每一件商品、保存每一个关键环节的管理记录，通过自动识别技术将实物流与信息流相结合，追踪和溯源物资从供应链的原材料、生产、销售到消费整个过程中相关信息的体系[3]。物资安全电子溯源系统主要采用物品编码和自动识别等信息技术手段，对供应链上的安全信息进行采集、管理并予以追溯[4]。

物资安全追溯系统的建设早就起步，至今已发展出诸多技术方案。在自动识别技术的载体技术上，目前使用较多的有条形码、矩阵码（二维码）、无线射频识别技术（radio frequency identification devices，RFID）、传感器标识等。在编码技术上，各个产业领域存在多种编码体系的运用，包括 GS1（globe standard 1）[5]、OID（object identifier）[6]、Handle（handle syetem）[7]、第三方平台自编码、企业自编码等。

我国越来越多与生产及相关的企业，都建立了属于本企业的追溯系统，用于支持企业与用户进行相关信息的查询，但实际的应用推广却严重受阻。一方面，企业间、地区间的信息不能互联互通，导致供应链上的信息碎片化，用户能查询到的有用信息甚少，而企业也很难挖掘到有价值或能对企业效益产生影响的信息；另一方面，查询接口不便捷，大多需要专用的扫码软件，这极大地制约了企业追溯系统在用户群体内的推广。

随着移动互联网的发展、扫码软件的普及，用户的查询越来越便捷，这培养了用户扫码操作体验的习惯。大批企业和第三方溯源平台采取了直接在二维码中存入网址的方式，以此来实现对产品信息的展示或对追溯信息的查询。虽实现了便捷的信息查询，但未能实现多环节数据的关联，只有部分对上下游控制能力强的企业能将追溯信息汇聚到自己的平台上进行展示。对于大多数企业来说，扫码还仅限于对产品的展示和介绍，并不能提供追溯服务。

项目参考了泛在电力物联网标识平台的结构，并在此基础上建立了用于物资安全电子追溯的物联网的网络架构，通过建立物资供应链的解析服务、目录服务和信息服务，为物资从生产、采购、运输到使用自行进行溯源数据的采集、存储和分发提供了解决方案。本文针对采用智慧供应链物资自行编码的安全追溯应用场景，提出通过“泛在电力物联网标识管理平台”——物码标识技术方式进行电子追溯的方法。

3 实现方案

方案以电力物资的生产品类、批次及权限的方式来实现物资安全电子追溯服务，下面将分别描述具体实现方法、追溯实现过程、追溯信息的查询过程。最后，针对系统可能存在的信息篡改问题，提出几点建议。

3.1 系统框架

整个追溯系统的工作框架如图 1 所示，由以下 3 个部分组成。

（1）电力生产企业直接使用标识技术对产品进行自行编码。例如 CT.cn/abcde，其中，CT.cn 为企业域名的网址，/abcde 为该企业某一产品的代码；此标识作为该产品的追溯信息服务入口，生产企业可在该标识对应的信息资源上添加厂商必需的安全追溯信息，如生产日期、原材料、有效期等。

（2）由编码部门或第三方已有资质企业建立公共的发码目录服务和标识解析服务。其中，发码目录服务可作为物资一级节点溯源监管平台的功能之一，监控产品从生产、运输到销售整个环节中，所有经历的信息服务的索引；同时在电力智慧供应链系统中接入一个标识解析服务的功能，通过泛在电力物联网标识系统查询对应的信息、服务、资源等功能，并开放给相关企业或用户不同的权限，进行管理和维护。发码目录和标识解析服务可通过国家物联网标识管理公共服务平台进行具有国家公信力的系统搭建。

（3）电力生产经营企业根据生产、检测、运输、销售各自负责的追溯环节与泛在电力物联网标识管理平台系统对接，并分别在各个环节所属的信息服务系统中，记录和存储产品全周期中所经历的每一项事件的详细信息，在标识解析平台查询并输出接口。

3.2 追溯信息采集

追溯系统框架如图 2 所示，其中追溯信息采集过程如下。

（1）电力生产企业按照要求在编码服务器注册其目录服务信息并生成标识。

（2）当在检测、运输、销售等环节产生与该网址

人民邮电出版社

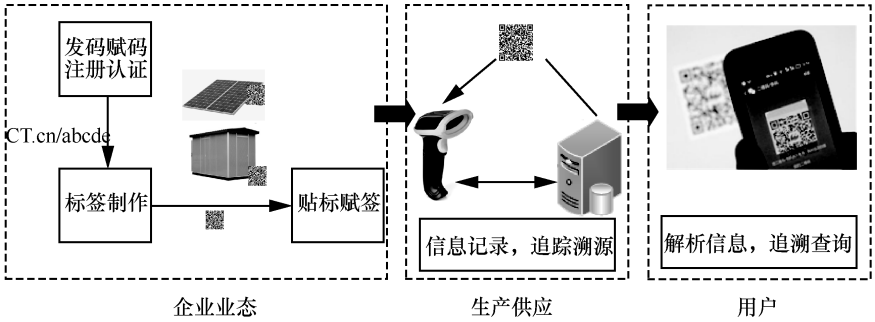


图 1　物资安全电子追溯系统工作框架

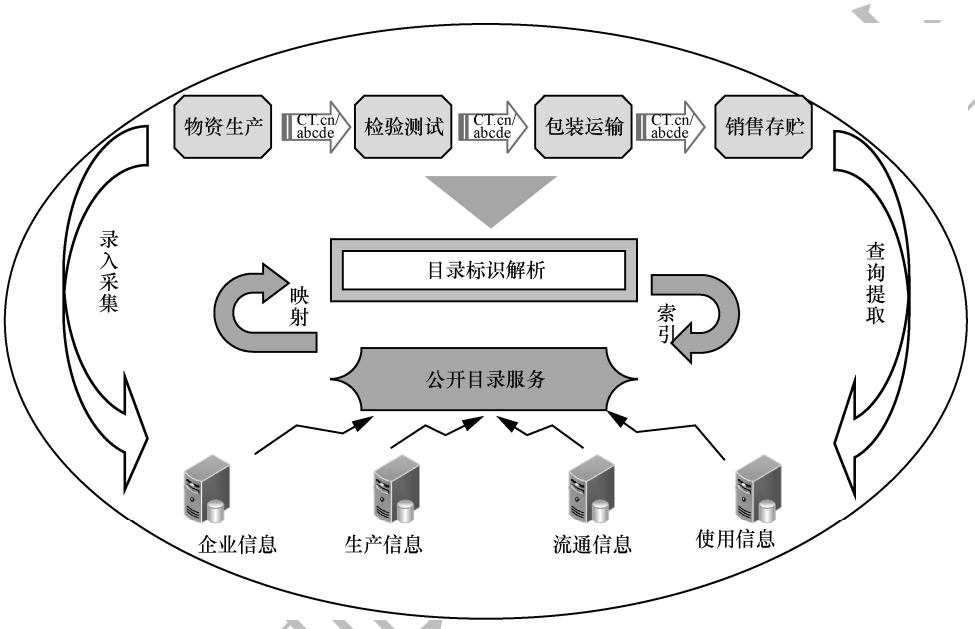


图 2　物资安全电子追溯系统框

有关的事件信息时，通过标识编码服务查找到对应的目录服务器，并注册该标识对应的 CT.cn/abcde 与新信息的映射关系，如 CT.cn/abcde 与 xiaoshoCT.cn/CT_cn_abcde 的对应关系。

3.3　追溯信息查询

物质信息溯源查询流程如图 3 所示，整个追溯标识信息的查询过程如下。

（1）企业及用户使用专用 App 扫描产品二维码，访问生产企业的标识编码服务器。

（2）生产企业服务器查询对应标识编码目录服务器上各个环节事件的详细信息。

（3）生产企业服务器读取出各环节数据库的标识信息数据。

（4）生产企业服务器对各环节数据进行编排，再设计一套用于追溯的自定义元素，使不同环节标识信息可明显区分。

（5）如自定义< tracking information > 元素。

```
< tracking infor-mation>
<info-type type= “shengchan”>
<a href =” ...” >生产</a>
</info-type>
<info-type type= “jiance”>
<a href =” ...” >检测</a>
</info-type>
<info-type type= “yunshu”>
<a href =” ...” >运输</a>
</info-type>
<info-type type= “xiaoshou”>
<a href =” ...” >销售</a>
</info-type>
</ tracking -information>
```

通过引入如上自定义标签即可实现对不同溯源环

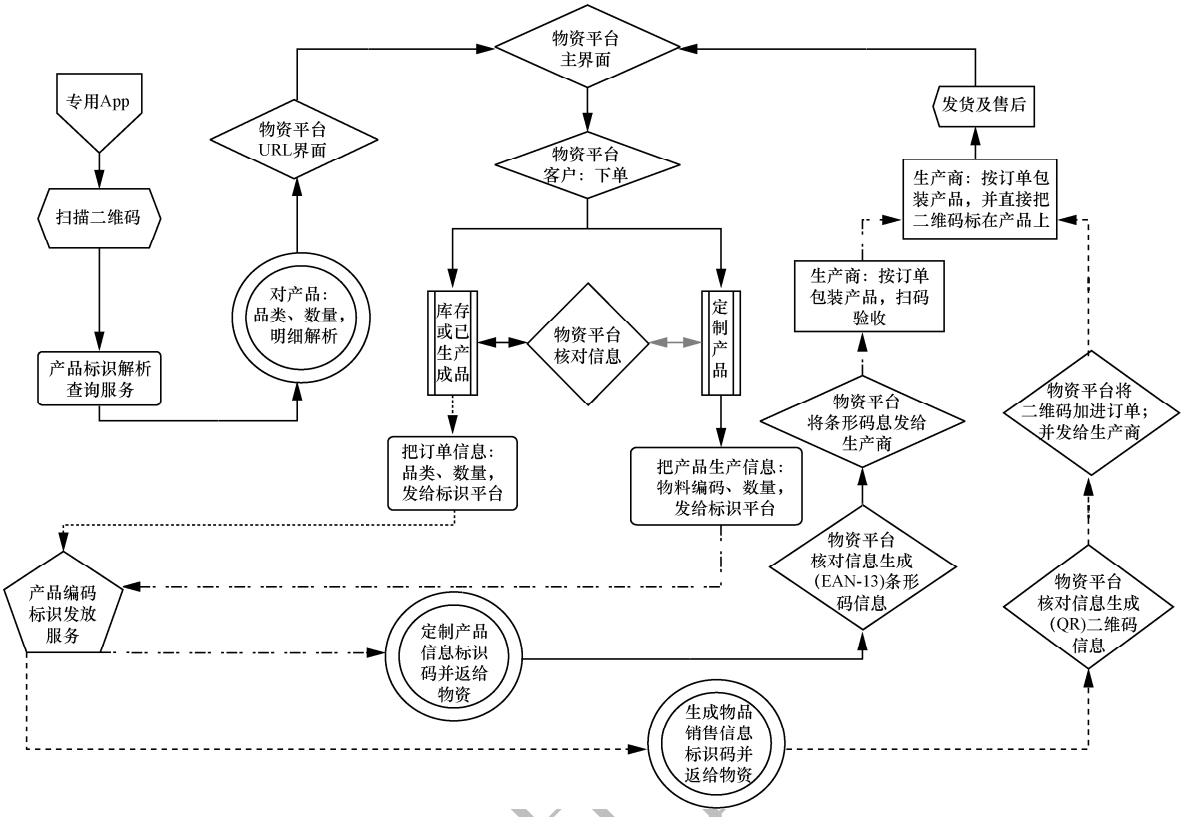


图 3　物资信息溯源查询流程

节（包括生产、检测、运输、销售等）标识信息的区分，语义性非常好。将<tracking -information>元素的样式与脚本，封装在一个 HTML 文件 tracking -information.html 中，即可实现该自定义元素的复用。引入 tracking -information.html 后，就可以使用<tracking -information>。

（6）将完整信息展示到查询客户端。

3.4　防止企业篡改上下游信息

在上述直接采用企业物码标识进行溯源的追溯方式中，生产企业作为溯源信息的最终整合和发布机构，可能存在生产企业对上下游负面信息和问题信息进行篡改后再显示的情况。针对此问题，在系统中增加一种监管和认证机制，以保证上下游信息的真实性、可靠性、唯一性，提高信任度。

追溯信息第三方验证如图 4 所示，由电力相关监管部门或委托第三方企业在本方法的基础上开发物资安全溯源标识信息监管平台，采用与企业服务器相同的方式，从标识信息数据库中直接抽取各环节的溯源信息。另一方面，监管平台从企业服务器中抽取经企业服务器整合的标识信息，并与直接从供应链上的信息服务器中抽取的信息进行比对和认证，以达到及时发现或规避因生产企业对追溯信息进行整合后再发布的方式带来的生产企业对上下游溯源信息进行篡改的目的。

4　验证与评价

物资安全电子追溯要想真正发挥其作用，必须能有效权衡用户、企业和监管部门（第三方权威平台）之间的关系。对用户来说，便捷的查询入口和有效的供应链追溯信息是必需的，其中任何一点的不完善，都会阻碍追溯系统在用户群体中的推广；对企业来说，如何以最低的资金投入，从追溯系统中获取企业的最大化效益是关键，这会直接影响企业在追溯系统建设方面的决策；对监管部门来说，对物资安全达到全面有效的监管，营造一个健康、安全的物资消费环境是主要目标。表 1 通过在上述几点关键问题项目上对比不同方法的性能特点，展示了本文提出的直接使用物联网标识的物资安全电子追溯方法的优势。

在客户端方面，基于条形码和泛在电力物联网标识的溯源系统，根据各自需要开发不同的 App 实现扫码查询功能，而企业自编码的方法支持用户直接通过

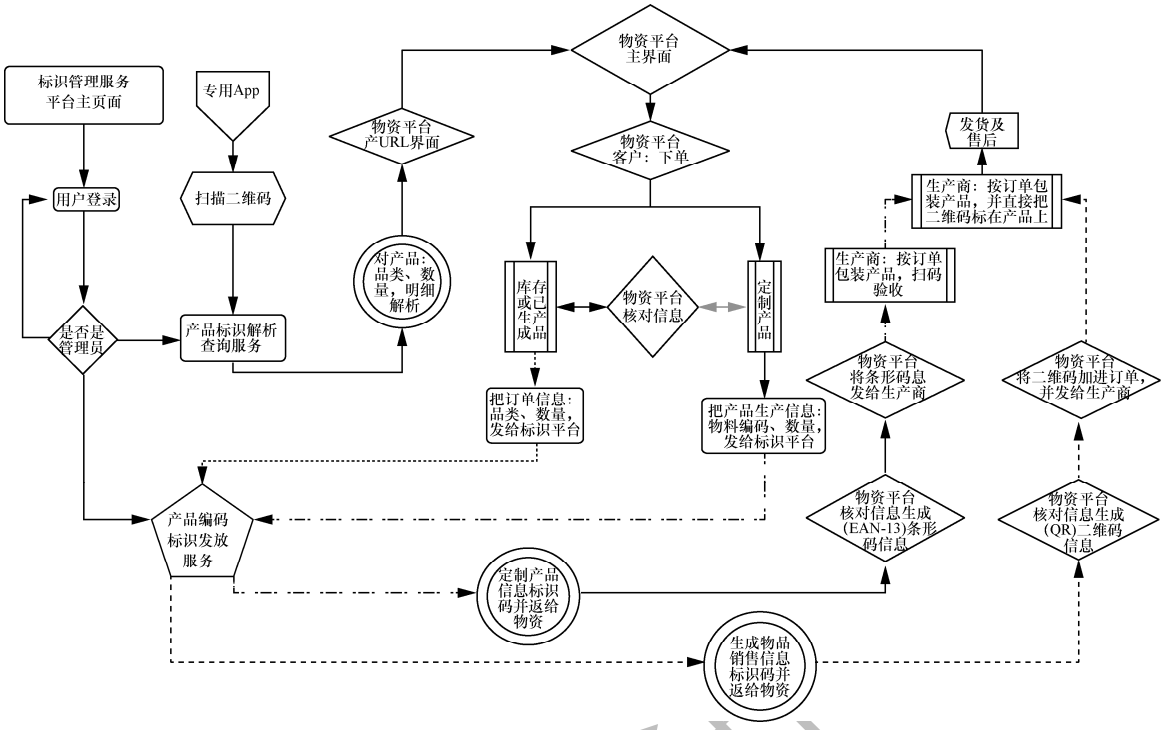


图 4　溯源信息第三方验证流程

表 1　企业自编码与标识编码的对比

分类	项目	基于企业自编码	条形标识码	泛在电力物联网标识
客户端	是否需要专门 App	否	是	是
信息追溯	是否支持商品宣传功能	否	否	是
	是否支持显示完整供应链追溯信息	否	否	是
成本	是否需要支付赋码费用	否	是	是
能力扩展	是否兼容多种编码体系	否	否	是
	是否支持统一定义的功能和统一规范	否	否	是

常用 App 实现查询，如微信、支付宝等；在成本方面，对于采用条形码技术的追溯系统，企业需要向条形码标识平台支付发码费用；在追溯信息方面，基于普通自定义编码的追溯系统，由于编码不统一，无法实现供应链上信息的互联互通，普遍不能提供完整的供应链追溯信息，通常只能显示一些商品的宣传信息，基于泛在电力物联网标识的编码支持显示完整的供应链追溯信息，其中企业基于泛在电力物联网标识平台为查询入口的，还支持商品宣传信息的显示功能。

5　结束语

物资安全电子追溯是实现物资从生产到销售全程质量安全管理的一种可行方案。本文针对现有电力物资智慧供应链追溯系统进行了改进，提出了一种直接使用泛在电力物联网标识服务体系的电子追溯服务的方案，并描述了具体实现方法和信息追溯过程。通过分析可知，该方法能够以较低的复杂度和通用的查询入口搭建物资安全电子追溯系统，对实现以企业为追溯系统建设主体的架构具有重要的参考意义。

参考文献：

[1] 徐立青, 孟菲. 中国食品安全研究报告[M]. 北京: 科学出版社, 2011.
[2] 韦科. 国家电网公司制定《应急物资储备实施方案》[N]. 国家电网报, 2009.
[3] 刘俊华, 窦延平. 自动识别技术在质量追溯中的应用[J]. 计算机仿真, 2005, (2): 225-227.
[4] 赵林度, 钱娟. 溯源与召回[M]. 北京: 科学出版社, 2009.
[5] GS1 系统标准[OL].
[6] ISO/IEC 和 ITU 国际权威机构共同推动的标识体系[OL].
[7] CNRI. Handle system [OL]. [2013-03-20].

人民邮电出

基于物联网标识技术的智慧供应链管理

王焕娟，秦日臻
（国网电子商务有限公司（国网雄安金融科技集团有限公司），北京 100053）

摘　要：阐述了物联网标识技术对智慧供应链管理的支撑作用，梳理供应链管理业务的现状，提出了基于物联网标识技术的智慧供应链管理平台，分析了物联网标识技术对供应链管理的影响。最后总结了物联网标识技术在智慧供应链管理中的意义。

关键词：物联网标识；智慧供应链管理；架构设计

1　引言

全球经济已进入供应链时代，企业与企业之间的竞争开始转变为企业所处的供应链与供应链之间的竞争。供应链是以客户需求为导向，以提高质量和效率为目标，以整合资源为手段，实现产品设计、采购、生产、销售、服务等全过程高效协同的组织形态。随着信息技术的发展，供应链已发展到与互联网、物联网深度融合的智慧供应链新阶段[1]。供应链管理是指从用户的角度，通过供应商、制造商、分销商等企业间的协作整合供应链中的所有活动，使各种业务和信息实现集成和共享，谋求供应链整体最佳化。随着市场竞争的加剧，供应链管理能力已成为行业发展的核心驱动力。

由于供应链管理涉及多方，在供应链管理过程中存在编码异构、信息不透明、协同性差、流程不统一、成本控制难度大等问题。随着供应链管理趋于全球化、敏捷化，这些问题逐渐成为制约企业发展的瓶颈，应利用信息技术提高供应链的智能化水平。

物联网标识技术作为物联网的基础核心技术，适用于在一定范围内唯一识别物联网中的物理和逻辑实体，以便网络或应用基于此技术对目标对象进行相关控制和管理以及相关信息的获取、处理、传送与交换，它是物联网中最重要的基础资源，是物联网世界各对象的“身份证”[2]。物联网标识技术可全面兼容现有二维码、RFID、GS1 等异构编码规则，在不改变已有信息系统的基础上快速、低成本地对接供应链上下游企业的信息系统，有效解决信息孤岛问题，实现供应链企业间的数据互联和协同共享。

2　基于物联网标识技术的智慧供应链管理

2.1　业务现状分析

智慧供应链管理具有上下游产业链企业众多、流程复杂、设备种类多样等特点，在实际实施过程中主要存在以下问题。

（1）各企业信息系统独立

目前设备生产厂商多数未实现智能制造和部署工业互联网平台，造成相关环节（研发设计、物料采购、生产制造、仓储、物流、运维状态）的数据比较分散，存在于多个系统（如 ERP、MES、PLM、SAP 等）内，供应商、制造商、分销商、零售商和客户的信息系统相对独立，信息流、资金流和物流没有实行集约经营管理，致使企业资源无法实现最优化配置。

（2）编码标准不统一

目前企业利用条形码、二维码、RFID 标签、IC 卡、芯片等存储标识编码，但供应链上下游企业产品编码标准不统一，每一种编码标准对应不同的解析机制，各标准间不能互通。在物料、配件、产品等流通过程中，难以实现信息的准确关联和自动获取，导致供应链管理存在信息不透明、协同性差、流程不统一等问题，需对各类编码统一管理，实现机器和物品的唯一性的定位和信息查询，从而实现供应链系统和企业生产系统的精准对接。

（3）供应链不可视

由于上下游企业之间缺乏标准、有效的信息共享机制和实现方式，供应链企业在产品交付率、库存降低比率等方面信息不可视，企业无法对产品的供产销过程实现全面的了解，仅从自身流程和业务等比较单

人民邮电出版社

一的成本因素考虑如何选择供应商和销售商，致使企业无法切合市场需要进行有序生产管理，不能形成良好稳定的合作关系。

（4）信息难追溯

供应链管理信息的可追溯，对于实现供应链管理至关重要。当发现有缺陷产品时，需要追溯查询产品的零件信息、生产信息、安装位置等历史信息，这些信息往往分散于生产厂商、物流服务商和零售商等各个环节，缺乏记录或信息不互通，造成追溯困难。

2.2 物联网标识技术的应用

物联网标识是物联网物理和逻辑实体以及资源和服务的身份标识技术，是物联网世界的“身份证号码”，可有效应用于物联网信息获取、处理、传送与交换。物联网标识技术是开发、部署和运行大规模物联网应用和服务的先决条件。物联网标识管理是对物联网标识进行编码、分发、注册、解析、寻址以及发现等贯穿物联网标识产生和应用全过程的管理[3]。

物联网标识技术可有效解决供应链管理中遇到的问题，通过对产品、服务、物流等信息进行唯一性标识，可在产品编码、管理系统、管理方法等方面提供标准化规范化管理体系，实现上下游企业之间信息的互联互通、动态共享与信息管理，支持分布式数据的互操作性和信任，实现数据的广泛访问，并通过数据的访问权限、用户的权限等实现安全管理。

针对供应链管理存在的问题，基于物联网标识技术构建智慧供应链管理平台，可以低成本、高效率地实现跨主体供应链信息采集与关联，并为不同的用户组（整机制造商、物流商、经销商或客户、维护服务商）提供不同的授权解析机制，提供指定信息实时共享增值服务。供应链各环节的企业将各自系统相关的信息（如零部件产品信息、物流信息、生产信息、销售信息等）分别注册物联网标识编码，在注册时关联上一级信息的标识编码，可将上下游信息均关联在整机产品标识编码中，客户或用户解析一个物联网标识编码即可同时获取曾经关联过的其他标识编码信息，从而做到整机产品信息追溯和全生命周期管理。

3 智慧供应链管理平台架构设计

基于物联网标识技术的智慧供应链管理平台，主要实现供应链全景可视、数据互联、协同共享，满足各企业的采购管理、物流管理、智能仓储管理、产业链协同、产品可追溯等业务需求。

平台从下至上由基础设施层、标识解析层、应用服务层及用户访问层构成，如图 1 所示。

- 基础设施层，该层为平台运行提供底层基础环境、系统级软硬件资源的支撑保障、数据存储和数据分析处理功能。
- 标识解析层，平台以物联网标识技术为基础，完成智慧供应链中对象标识的注册、解析、信

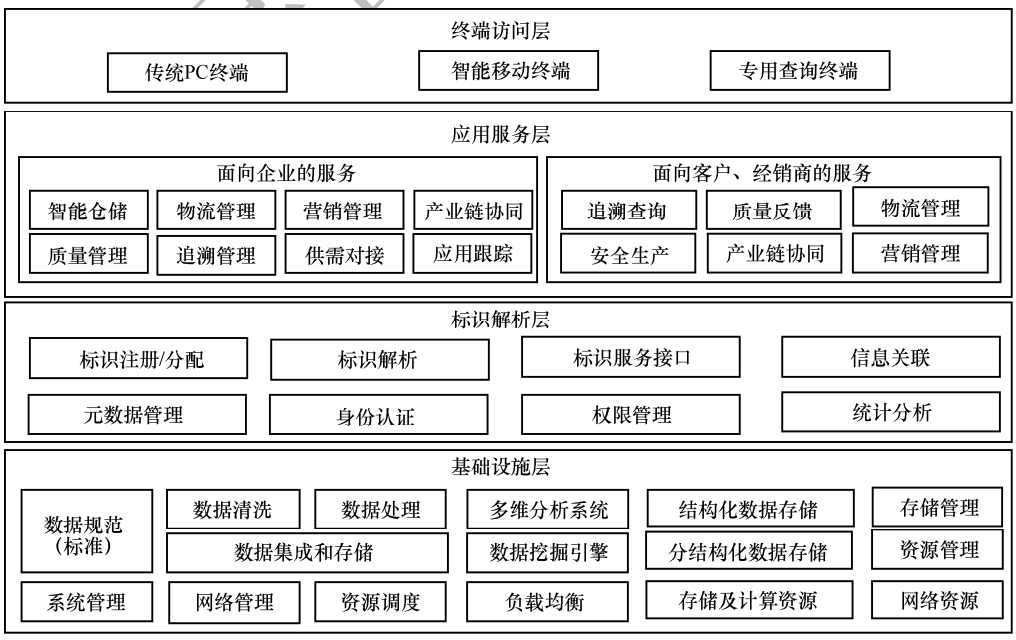


图 1 智慧供应链管理平台架构

息关联、访问权限控制等功能，实现对象的唯一标识注册与解析、不同企业及异构系统间安全可控的信息互联与互操作等。

- 应用服务层，平台面向企业、客户、经销商等不同用户提供覆盖零部件采购、加工制造、产品储存、运输、销售、产品追溯、安全监控等全过程的服务。
- 终端访问层，不同类型的用户可以通过传统 PC 终端、智能移动终端、专用查询终端等多种访问形式获取平台所提供的智慧供应链服务。

通过各企业现有核心基础业务平台与物联网标识技术的深度融合应用，平台实现制造商、供应商、物流商、经销商、客户间的综合信息共享与业务协同，并实现任意有需求双方的直接对话与互动。通过提升管理精细化水平，促进企业提高生产计划准确率，降低各方成本，真正实现零库存管理目标，促进供应链管理可持续健康发展，最终形成企业供应链全价值链生态圈。

4 物联网标识技术对智慧供应链管理的影响

（1）提升供应链可视化水平，重塑企业管理决策新方式

物联网标识的应用，为供应链建设管理过程中实现数据共享、打破信息孤岛、解决“数据烟囱”问题提供了一种新思路，打破了生产企业、供应商、物流公司、采购商等供应链各方之间的信息屏障，实现了供应链各环节跨区域、跨企业内外部信息的及时传输、实时共享和集成应用。供应链各方可以实时监测产品的生产、运输、销售等动态信息数据，提升了供应链可视化水平和透明化管理。通过各方的协作和交互，可及时了解采购方的采购需求及采购计划变动情况，动态预测市场的需求变化，合理配置资源、减少产品库存，提高生产效率、降低企业成本，重塑企业管理决策的新方式。

（2）打造协同生产一体化模式，重构供应链企业合作共赢新态势

传统生产模式下，众多的生产商、供应商、分销商、零售商构成了冗长的、复杂的流通渠道，供应链各方合作效率低下，同质化企业竞争激烈，供应链上下游企业的横向竞争和纵向打压严重破坏了生产和流通的规律及次序。物联网标识的应用、智慧供应链的打造，可以通过信息共享将上下游企业整合为一个紧密的整体，打造协同生产一体化模式，从设计、生产，到运输、销售各环节，加强交流与协作，实时掌握市场动态，合理进行资源配置，整合全链条企业的资源和优势，实现社会资源的最佳配置。促进上下游企业形成良好的合作关系，打造新型全价值链生态圈，使上下游企业共担风险和利益，避免企业间的恶性竞争，使供应链内的企业竞争转变为供应链之间的竞争，转变为科学的管理和组织手段的竞争，降低供应链管理的总成本，提升整个供应链及整个行业的生产水平，形成规模化效应，重构供应链企业之间合作共赢的新型态势。

（3）挖掘商业运营新模式，助推传统产业生产运行生态新发展

针对传统的生产模式，智慧供应链的建设，可以有效地规划和管理产业链上发生的采购供应、生产运营、分销流转和所有物流活动，实现采购、物流、信息流、资金流的全方位融合，既提高了生产效率，又大大降低了企业运营成本。此外，物联网标识作为打通企业信息系统、形成数据流通的技术引擎，是供应链上下游企业接入供应链体系的关键入口。标识管理平台汇聚了各方的核心数据和优势资源，通过云计算、人工智能、大数据等先进技术，可以基于标识流量提供全生命周期管理、产品质量追溯、生产在线监测、产业需求挖掘、产品质量分析等增值服务，打造新的商业运营模式和利润增长点。通过实时同步、分析和展示产品在全链条过程中的生产、运输、销售、售后、质量检测、用户评价等信息，打造产品生命周期透明化管理，可以进一步完善供应链跟踪服务机制，提升供应链的社会公信力，主推传统产业打造生产运行的新生态、新模式，实现更好的经济效益和社会效益。

5 结束语

本文提出的基于物联网标识技术的智慧供应链管理方式及应用形式，打破了企业内部及企业间已存在的业务孤岛、信息孤岛，将上下游企业组成整个产业系统的协同供应链网络，通过集成产业链各方的核心能力和优势资源，获得供应链在管理、技术、资源等各方面的强大竞争优势。借助智能供应链体系打造新型全价值链生态圈，可重塑产业链、供应链、价值链，引领工业企业向服务型制造企业进行转变。同时，物联网标识、人工智能、云计算、

人民邮电出版社

大数据、区块链等新兴技术在智慧供应链中的成功应用，形成了新型生产运行和商业运营模式，培育出集成创新应用新模式，随着物联网标识等技术在供应链管理中的不断深入应用，将进一步地提升供应链管理的数字化、自动化、智慧化水平，带动上下游企业降本、提质、增效、节能，促进传统产业转型升级。

参考文献：

[1] 国务院. 国务院办公厅关于积极推进供应链创新与应用的指导意见: 国办发(2017)84 号[S]. 2017

[2] 田野, 刘佳, 申杰. 物联网标识技术发展与趋势[J]. 物联网学报, 2018, 5(2): 12-21.

[3] 徐勇军, 刘禹, 王峰. 物联网关键技术[M]. 北京: 电子工业出版社, 2012.

人民邮电出版社

基于物联网的智慧小区综合能源管理系统

王卫卫
（北京中电飞华通信股份有限公司，北京 100070）

摘　要：为建立节约型、智能型小区，文中运用物联网技术研究综合能源管理系统，实现对小区家庭用户、充电桩、光伏系统/储能系统、供电系统和照明系统的可视化集中监控；收集小区用户实时用能情况，进行分析统计，分析多场景下的用能需求，通过设备实时控制或者执行预置策略，综合优化调度，指导小区优化用能，并作为中继站向能源综合服务平台进行信息转发。充分运用需求侧主动响应的市场机制，实现小区用户与电网供需友好互动，通过综合能源管理系统，调动小区用户负荷参与互动，从而降低智慧小区综合能耗及减小电网峰谷差。

关键词：智慧型小区；综合能源；物联网；用能需求；需求侧主动响应

1　引言

电力资源[1]是国民经济的基础性资源，它既是促进国民经济发展的生产资料，又是人们生活不可缺少的资源。随着城镇用电规模的扩大和用电结构的改变，用电负荷[2]增长迅速，尤其是夏季空调、热水器的使用，造成小区用电负荷在用电高峰时期快速增长，再加上小区用户用电比较集中，造成小区区域用电负荷的急剧波动，打破负荷平衡的局面，使得小区用户用电供不应求。所以迫切要求调整和优化能源资源配置，推进节能减排，进一步实现电网运行削峰填谷，提高电网设备利用率和电网运行效率，保障电网安全稳定运行，指导小区用户参与综合能源管理以及节能降耗[3]，通过小区用户用电智能化、远程化、可视化、清洁化，大幅度提升小区用户用电行为的感知水平，探索小区用户与电网运行友好互动新模式，最终实现小区用户与电力企业的双赢。

物联网[4]是互联网的延伸和扩展，主要通过射频识别技术、红外感应器以及全球定位系统等，按约定的协议，将无处不在的末端设备和内在的智能传感器、视频监控系统等通过有线或无线设备与互联网连接起来，在内网、外网或者互联网环境下，采用信息安全保障机制，进行信息交换和通信，实现智能化的识别、在线监测、定位跟踪、报警联动、预案处理、远程控制以及对物品高效、节能、安全、环保的管控。物联网主要包含 3 个基本要素：传感器、网络系统以及终端应用系统。

2　物联网在智慧小区中的应用

智慧小区[5]是利用新一代物联网信息通信技术及能源技术来感知、监测、分析、控制、整合小区各个环节的信息化及能源资源，在此基础上实现对各种需求做出智慧的响应，使小区整体的运行具备自我组织、自我运行、自我优化的能力，为小区企业创造智能、绿色、安全、高效、便捷的发展环境。综合能源管理平台融合物联网、云计算、大数据三大技术，实现小区用户的整体互联。平台依托技术领先、功能集成、应用创新的支撑平台，全面集成小区内的家庭用户、充电桩、光伏系统/储能系统、供电系统和照明系统等子系统，形成透彻感知、泛在物联、高度融合、智能联动的智慧有机体，实现“高效率运营、高质量办公、高品质生活”[7]。

基于物联网技术，应用大数据分析技术和模型自适应控制方法，分析市场竞争机制下的用户用电和行为特征、多元用户侧的可调度潜力和可靠性分析方法，并建立用户互动模型，探索激励小区用户参与能源管理的新模式，探索小区用户主动参与需求响应的新机制，实现电力用户能源管理“可视化、数字化、网络化、专业化”，帮助小区用户提高科学用能水平，提供用户能效在线监测节能服务，降低电力用户的综合能耗。

人民邮电出版社

3 综合能源管理系统

基于物联网的智慧小区综合能源管理系统针对小区家庭用户安装入户型互动终端设备或非入户型互动终端设备等，通过 APP 实现小区用户家用电器的智能化控制，为小区用户提供能源管理服务，并与小区能源管理系统相联，实现家庭能耗分析和节能目标。针对空调、电热水器等重要设备安装智能化监测、控制设备，实现家庭智能电器的数据采集、监控和家庭能源管理、分析、优化控制。实现对家用电器的智能化控制以及小区用户的用电量、电器的启停状态及使用时间的监测，实现即时及定时控制。同时，通过小区能源管理系统，实现对小区家庭用户、充电桩、光伏系统/储能系统、供电系统和照明系统的可视化集中监控，掌握小区实时用能情况，进行分析统计，通过设备实时控制或执行预置策略，分析多场景下的用能需求，综合优化调度，指导小区优化用能。综合能源管理系统架构如图 1 所示。

3.1 家庭能源管理系统

家庭能源管理系统根据收集到的需求，进行标准化设计，统一组织软件系统，为家庭用户提供智能化改造建设，建设家庭能源管理系统实现家庭综合能耗远程化、可视化管理，同时通过互动参与电网移峰填谷。为家庭用户建设家庭能源管理系统，安装入户型互动终端设备或非入户型互动终端设备等，通过 APP 方式，为居民用户提供能源管理服务。

针对普通居民小区进行大规模互动型家庭的改造建设。建设面向用户的家庭互动化改造方案，助推智能电网建设，依托物联网技术，综合用电量、用户意愿等因素对用户进行差别化改造建设。入户型建设方案主要针对配合程度比较好的电力用户，通过安装入户型互动终端设备实现；非入户型建设方案针对配合程度一般的电力用户，通过安装非入户型互动终端设备实现。通过互动终端设备提升能源感知深度，为用户提供能源管理服务，降低家庭综合能耗，通过互动参与电网移峰填谷，实现小区用户与电网之间能源和信息的双向交互，同时保障系统的不间断、可靠运行。

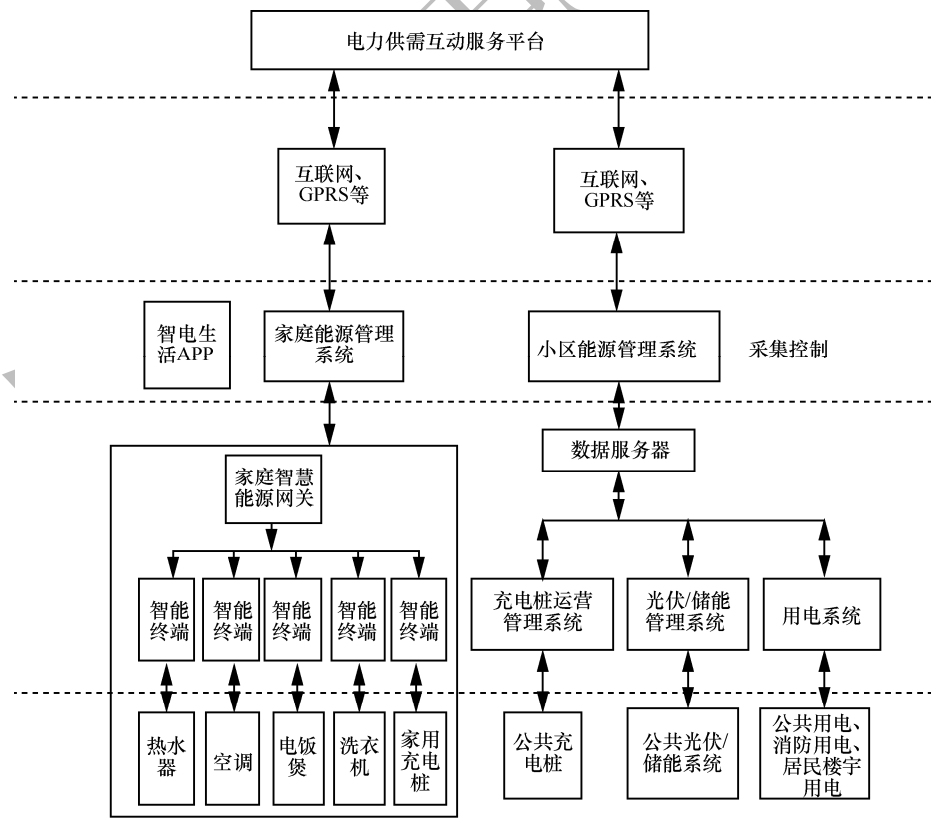


图 1 综合能源管理系统

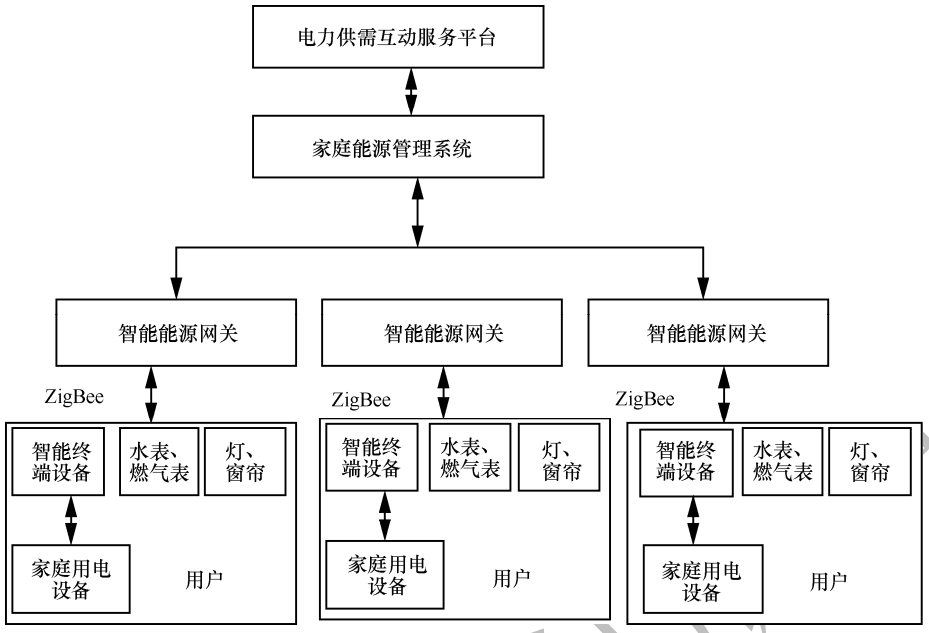


图 2　家庭能源管理系统

家庭能源管理系统如图 2 所示。

3.2　小区能源管理系统

小区能源管理系统如图 3 所示。

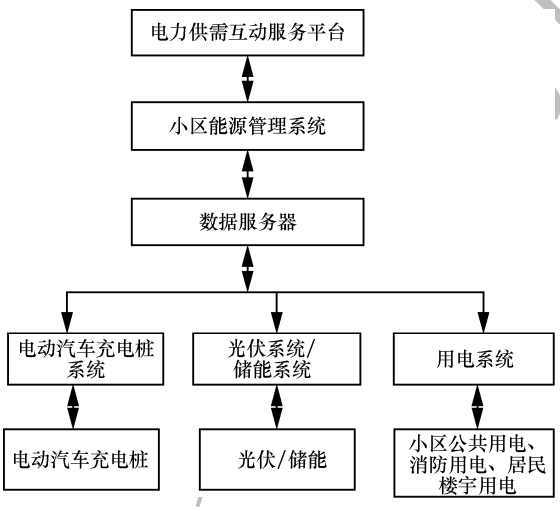


图 3　小区能源管理系统

通过小区能源管理系统实现对小区家庭用户、充电桩、光伏系统/储能系统、供电系统和照明系统的可视化集中监控，掌握小区实时用能情况，进行分析统计，分析多场景下的用能需求，通过设备实时控制或执行预置策略，综合优化调度，指导小区优化用能，降低小区整体能耗，并作为中继站向能源综合服务平台进行信息转发。

构建小区能源管理系统，集成配电系统、充电桩、光伏系统/储能系统、照明系统和家庭能源管理系统等，实现小区内“多类型能源—多元负荷”的互联互动以及小区综合能源的集中监控及小区用户的能源管理，提升终端负荷的灵活可控性，降低小区整体能耗，节约运营成本。小区能源管理系统主要实现如下功能。

（1）小区综合能耗可视化

小区综合能耗可视化集成家庭用能数据、配电自动化系统、电动汽车充电桩系统、分布式光伏系统/储能系统的数据，对小区的综合能耗进行可视化展示。

（2）小区能效优化管理

结合电价、天气、公共分布式光伏系统/储能系统、家庭用户用能的实时/历史数据，对小区整体能效进行诊断，生成以小区综合能耗最低为目标的小区能源管理策略，对小区可调度资源进行直接/柔性控制。

（3）用电信息发布服务

电网运行和检修信息、实时电价、用电政策、用电服务等信息的发布；用户用电量、电费余额或剩余电量以及购电等信息的实时推送。用户可实时查询各种电价信息，包括实时电价、分时电价、阶梯电价。

（4）增值服务功能

根据用户用能信息对用户进行分类，向类似用户发布特定的天气、股票、广告、商品优惠等信息。

3.3 接口技术

（1）与内网业务系统接口

小区能源管理系统通过中间库方式与能源综合服务平台建立数据交互接口，获得所需数据资源。通过在系统间部署内网中间库，将能源综合服务平台中辅助分析决策系统所需信息存储到中间库中，系统通过访问中间库获取数据，并通过防火墙实现安全隔离。

（2）其他数据信息系统接口

与小区能源管理系统外网业务系统（家庭能源管理系统、电动汽充电桩系统、分布式光伏系统/储能系统）的集成，主要通过 Socket 方式建立数据交互接口，获得所需数据资源，Socket 方式建立在 TCP/IP 通信协议之上。通信双方的网络均以 TCP/IP 为基础，双方的通信得以实现，且不受网络类型、传输距离等因素的限制。

3.4 物理部署

物理架构如图 4 所示。

在内网部署能源综合服务平台应用服务器、数据库服务、应用接口服务器。对电力公司用户，通过浏览器完成小区能源管理系统提供的各种业务操作和服务。当需要设备台账数据时，通过应用接口服务器向内网中的能源综合服务平台发送请求，通过应用服务器对该请求返回值进行解析和处理，然后将这些数据返回至小区用户。

在信息外网部署小区能源管理系统应用服务器，家庭总体的用电数据查询，通过应用接口服务器向内网中的用电信息采集系统发送请求，并将查询结果返回给用户来实现。

4 结束语

文中综合利用嵌入式系统集成技术、云计算、移动互联网等新一代信息技术，构建基于物联网的智能小区综合能源管理系统，集成配电系统、充电桩、光伏系统/储能系统、照明系统和家庭能源管理系统等，实现小区综合能源集中监控及居民用户能源管理以及对光伏、分布式储能、电动汽车、柔性负荷的互动协调控制，打造友好互动的崭新模式。通过家庭能源管理系统和小区能源管理系统，实现小区综合能源的节能降耗，同时通过互动参与电网移峰填谷，最终实现降低小区区域峰谷差、提升小区能效水平的目的。文中通过加强电网与用户之间的双向服务渠道，有效降低日益增长的电力负荷，缓解日益突出的电力资源供需矛盾，提高电网设备利用率和电网运行效率，保证电网安全稳定运行。

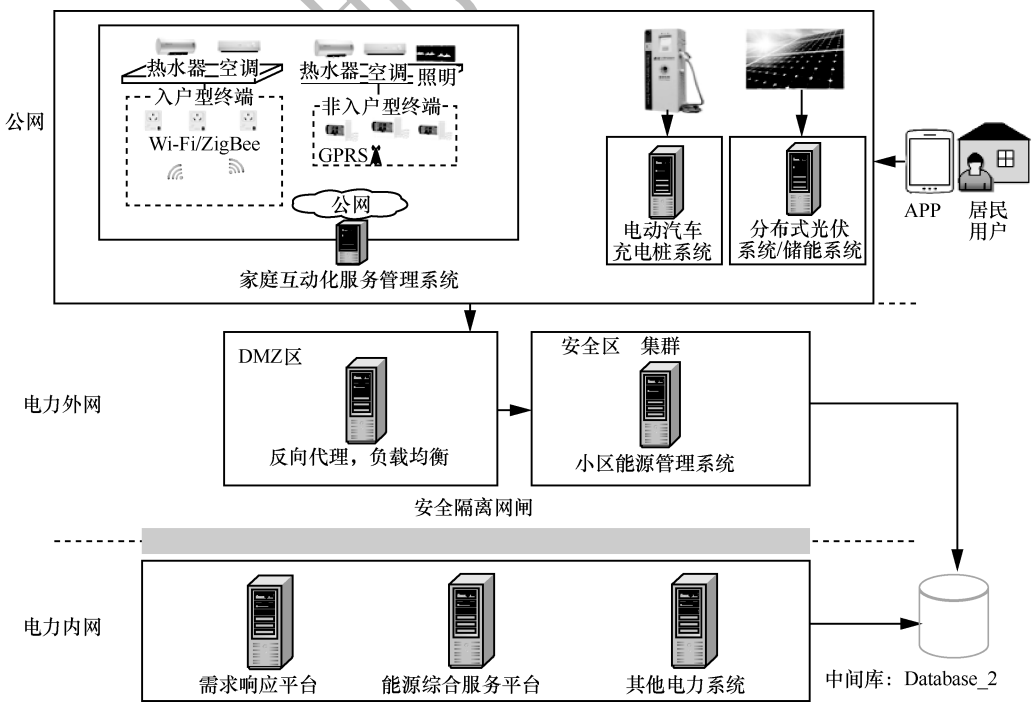


图 4 物理架构

综上所述，基于物联网的智慧小区综合能源管理系统，为小区创造了智能、绿色、安全、高效、便捷的发展环境。建立高效、科学、便利的智慧小区能源管理体系；提供方便、快捷、经济的信息通信服务；打造温馨、舒适、便利、科学和数字化的现代化智慧小区环境系统。物联网的技术特征、性能特点决定了它将在智慧小区、城镇化建设中发挥独特的作用，避免了重复投资，满足了小区用户、企业、商业等多方的需求。

参考文献：

[1] 申斌, 张桂青, 汪明, 等. 基于物联网的智能家居设计与实现[J]. 自动化与仪表, 2013, 28(2): 6-10.

[2] 李稚萱. 云计算在基于 NGB 的智慧家庭业务平台上的应用[J]. 物联网技术, 2012(7): 83-85.

[3] 娄岩. 物联网技术在智能建筑中的应用研究[D]. 成都：电子科技大学, 2014.

[4] 杨宇峰, 朱婧, 曹敬. 智能社区低碳能源管理系统设计[C]//智能电网新技术发展与应用研讨会, 2017.

[5] 夏炳军, 权锐, 蒋秋兵. 智慧小区能源管理系统研究与设计[J]. 电气时代, 2018(3): 101-106.

[6] 张丹, 沙志成, 赵龙. 综合智慧能源管理系统架构分析与研究[J]. 中外能源, 2017(4): 7-12.

[7] 曹敏, 暴海峰, 魏龄, 等. 基于 LiteOS 的家庭智慧能源管理系统设计[J]. 电子技术与软件工程, 2017(19): 175-178.

人民邮电出版社

基于物联网的智能电网信息化建设研究

石孟磊，周军，杨志强
（国网西藏电力有限公司，西藏 拉萨 850000）

摘　要：物联网的发展促使智能电网形成全新的运行模式，加快了信息化建设的步伐。首先对物联网、智能电网之间的关系进行阐述，然后分析实现信息化建设所需要的关键技术。这一前提下，提出几点与信息化建设相关的建议、措施，目的是为相关人员提供参考，充分发挥物联网技术的作用，并推动我国智能电网的发展。

关键词：物联网；智能联网；信息化建设

1　引言

对于智能电网的提出而言，在根本上破除了传统电网的供应模式，使得开放性成为电网显著的优势。但是，为了确保智能电网能够稳定运行，需要实现更加精准的测量、监控。为此，必须以“智能+”为基础，对电网运行的模式进行合理调整，充分发挥更多先进技术的作用。同时，基于物联网开展信息化建设工作，完善智能电网的发展架构，为可持续发展奠定基础。

2　物联网与智能电网的关系分析

物联网、智能电网具有十分紧密的关系。具体而言，要想实现智能电网的建设并构建信息化模式，必须以物联网为基础，以得到先进技术的支持。在智能电网的长期发展中，物联网可以帮助其形成更加完善的电力系统，最大程度上提高信息化技术水平。究其原因，是因为物联网能够实现对信息的高效、可靠传输，并能够实现对信息的感知。在这一前提下，还可以完成对信息的处理。也就是说，在智能电网信息化建设的过程中，如果可以将物联网技术应用在其中，就可以为信息化建设提供先进的技术支持。简言之，物联网与智能电网之间具有十分紧密的关系，物联网可以在发展的过程中为智能电网信息化建设指引方向，同时以更加密切的关系，为智能电网信息化的建设予以不竭的动力[1]。

3　基于物联网的智能电网信息化建设的关键技术

由于物联网技术与智能电网关系紧密，因此在建设信息化的过程中，必须充分发挥物联网技术的作用。在此前提下，可以有效推动我国智能电网的建设高速发展。为了实现智能电网信息化建设的目标，必须以物联网为基础，将诸多先进的技术应用在其中。

3.1　云计算技术

在智能电网长期发展的背景下，电网中所包含的信息呈现海量增长的趋势，如果仅仅依靠传统的运算方式，并不能满足电网系统构建的需求。因此，在信息化建设的过程中，必须运用强大的云计算技术，对数据进行分析、处理。在弥补传统运算方式不足的同时，还能够为工作人员提供诸多便利，并提高数据信息的利用率。

3.2　通信技术

智能电网在信息化建设的过程中，必须不断提高通信方面的能力，以此来实现对物联网技术的充分运用。不仅如此，还能够实现信息化建设的目标，能够提升通信技术水平，提高信息化建设的标准性、简化性。对于先进的通信技术而言，智能电网信息化建设期间所存在的问题，均可以以物联网形式为基础，利用通信技术进行有效处理。在发挥物联网技术优势的同时，推动智能电网的发展。

3.3　虚拟能量存储技术

在智能电网推进信息化建设的过程中，以物联网为基础，可以实现对虚拟能量的存储。这一过程中，同样需要发挥通信技术的作用，同时对分布式响应、能源需求予以合理协调。除此之外，还应该建设可充电、放电的电力设备，从而最大程度上满足双向潮流虚拟存储的需求。

人民邮电出版社

3.4 智能电表

从当前的情况来看，智能电网中所使用的智能电表是一种为用户提供优质服务的硬件设施，更是电网体系实现智能化发展的技术之一。为了能够切实实现信息化建设的目标，电力企业必须对智能电表进行充分利用，从而实现对用户能源使用模式的准确预测与分析。以此为基础，可以对智能电网进行针对性的规划，实现对用户供电量、质量的合理调整。在满足用户实际需求的同时，推动电网发展不断迈上新台阶。

4 基于物联网的智能电网信息化建设的主要措施

4.1 重视信息技术的推广与应用

从当前的情况来看，智能电网属于我国未来电网构建的主要发展方向，可以将其应用在通信信息、调度电、用电、输变配电、发电等环节中。在以上的环节中，智能变电站是其核心部分，直接影响着智能电网发展的质量、水平。对此，电力企业可以运用物联网技术的优势，实现智能电网信息化建设。也就是说，应该重视信息技术的推广，并将其应用在智能变电站的建设与发展中。具体而言，智能变电站可以运用先进的技术、设备，并保证其具备低碳、环保、可靠、集成、先进等特点。基于此，可以为智能电网的信息化建设与发展奠定坚实基础[2]。

在开展信息化建设的过程中，智能变电站可以结合通信平台对网络化的要求，以及信息共享、标准化、信息数字化等方面的具体标准，实现对信息的自动采集、自动控制、自动测量、自动计量、自动保护以及自动监测。通过该方式，最大程度上提高智能电网的功能水平。除此之外，还必须结合信息化建设过程中的需求，支持电网实现智能化发展，同时可以实现自动调控、在线分析、决策、协同互动等高级功能。也就是说，要切实发挥先进技术的作用，并顺应互联网时代的发展趋势，在提高智能电网整体水平的同时，实现信息化建设目标。由此可以发现，电力企业在推进智能电网信息化建设的过程中，必须重视信息技术的推广与应用，以此来充分发挥其价值。

4.2 设置智能电网信息化的计划

在新时代的背景下，我国大力推行“互联网+”模式。正是这一因素，为智能电网的建设与发展指引了正确的方向，有利于其明确信息化建设的标准。基于此，电力企业可以制定智能电网信息化建设计划，确保后续工作可以分阶段分步骤地进行，坚持守正创新，顺应新时期的发展趋势。除此之外，在“互联网+”背景下，“智能+”逐渐进入人们的视野，并应用在电网的建设与发展中。因此，在推进信息化建设的过程中，应该结合“互联网+”“智能+”的理念，实现对物联网技术的合理利用。在细化各项工作、计划指标的同时，将移动互联网等技术切实渗透在智能电网的建设中。

同时，将物联网技术、大数据技术、云计算技术、信息安全技术以及智能电表技术等充分融合。此时智能电网中所产生的海量信息，可以在新技术的前提下，得到更加深入广泛的发掘与利用。另外，可以将数据信息渗透进发电、输电、变电、配电、用电等环节中。也就是说，以信息化技术为基础，可以使各个环节之间的关系更密切，深化智能电网建设的意义。以此为前提，电力企业可以实现输变电智能化，并对源网荷进行协调优化。在实现智能调控、智能配电的基础上，提高企业经营管理的质量与效率，并为电力信息的通信协调奠定坚实基础。因此，在建设信息化的过程中，电力企业必须充分发挥物联网、“互联网+”“智能+”的作用，使其能够为智能电网的发展提供更加优质的服务[3]。

4.3 构建统一的信息化集成平台

在电力企业的长久发展中，为了能够充分发挥物联网的作用，实现智能电网信息化建设的目标，应该结合实际需求，构建统一的信息化集成平台，以此来实现对海量信息的保存、分析与利用。这一过程中，电力企业应该将原有的信息管理平台进行整合，转变以往分别建设业务系统的模式，确保各个业务的数据可以以平滑的方式完成整合、融合。具体而言，企业应该建立符合业务发展的平台系统，为企业自身的高效运行提供信息支持，最大程度上提高信息体系的层次。

在这一过程中，电力企业可以建立不同的信息系统、服务系统、集中式系统以及兼容式系统，然后将其以集成的方式融入到信息平台中。然后，利用通信技术确保不同系统、不同主体之间，可以对电网信息进行交换、识别。该方式可以使得不同部门与系统关系紧密联结的同时，提高数据信息的利用率，确保电力企业内部可以实现协调运行的目的。在集成平台中，还可以对运行数据、计量数据、电网拓扑结构数据、外部应用系统数据以及用户数据进行共享，打破传统信息孤岛的发展模式，从而能够为企业的发展奠定坚

人民邮电出版社

实基础。正是在这一前提下，智能电网可以形成一个完整高效、层次分明的信息化建设机制，促使业务流、信息流、电力流实现协调统一。从而在实现信息化建设目标的同时，满足电力企业内部业务不断变化的发展需求，对于提高智能电网的整体水平具有深远意义。

4.4 建立系统的信息化防御体系

智能电网在构建与发展的过程中，会产生海量的数据信息，这些信息与用户、企业、国家均有直接关系。因此，为了实现信息化建设的目标，并确保电力系统可以稳定运行，企业应该建立信息化防御体系，并将其应用在具体工作中。也就是说，在智能电网建设的过程中，不仅需要重视骨干网架构的安全性，还应该强调冗余能力、抗攻击能力，确保信息化系统可以在不安全的网络环境中稳定运行。

除此之外，以信息化防御体系为基础，还能够实现对各项数据的安全保护，避免发生数据信息泄露等安全性问题，从而构建一个和谐的信息化网络环境。这一过程中，同样需要以物联网技术为基础，明确信息环境对于安全的既定要求，将其作为前提能够为信息化建设物理层、应用层等，提供强有力的防御体系。在应用安全防御体系后，能够确保信息在日益严峻的网络环境中的安全性，防止黑客、恶意软件以及网络病毒的攻击。同时还能结合实际需求，对信息数据进行存储备份，避免信息发生泄露、丢失等问题。

5 结束语

综上所述，物联网技术与智能电网之间存在十分紧密的关系，需要通过恰当的方式应用结合，实现电网信息化建设的目标。这一过程中，不仅要对关键技术予以充分利用，还必须制定系统的策略、计划，为具体的建设工作提供依据与辅助。正因如此，切实实现信息化建设的目标，强化智能电网的功能，对于增强我国电力事业的实力具有重要意义。

参考文献：

[1] 向胜. 智能电网下的电力营销信息化建设分析[J]. 低碳世界, 2019, 9(3): 103-104.

[2] 苏道铜. 基于智能电网的继电保护技术应用探究[J]. 低碳世界, 2017(35): 82-83.

[3] 黄晶. 基于智能电网的国网蒙东电力信息化建设评价研究[D]. 长春: 吉林大学, 2017.

人民邮电出版社

基于物联网与人工智能技术的工程现场安全风险智能预警算法

黄文雯，冯志鹏，韩璐，葛冰玉，安培秀，李丹丹
（国家电网有限公司信息通信分公司，北京 100761）

摘　要：工程施工过程中涉及人员、违章隐患、现场状况等多方面的管控，现有的管理手段主要通过电话、邮件等方式进行信息沟通。对现场人员管理方面，主要依靠人员二维码、考勤卡等进行关键人员到岗到位的管理，难以保障关键人员到岗到位的真实性；对施工现场的违章行为尽管可以通过视频监控来进行监督，但是无法进行自动、及时的发现和报警，仅依靠人工发现现场存在的问题，降低了安全管控的效率。因此可以借助物联网与人工智能视频分析等技术，进行施工过程的人员、安全等方面的管理，创新管理手段，提升管理效率。对施工现场安全风险智能预警算法进行研究，应用到工程现场智能管控系统中，实现工程管理过程中的管理方式信息化、业务过程数字化，提高对工程现场管理的时效性、全面性。

关键词：工程现场安全；智能预警；物联网；人工智能

1　引言

电网配套通信工程施工过程涉及的施工点多且分散、覆盖面大、施工单位多、现场人员多样，参建人员的现场安全施工行为难以掌控，建设管理人力和精力均难以满足现场施工过程管控和安全管控全覆盖要求。针对施工现场管理，目前主要存在以下 3 个问题。

（1）施工现场多且分散，管理层缺乏有效的方法同时对多个施工现场进行直接管控，单靠施工现场人员上报现场信息，难以全面掌握现场的情况，管理层也不能及时发现问题并主动对现场问题进行干预。

（2）施工过程的安全风险问题大多是由于现场责任人员对安全问题落实不到位，且管理层难以对责任人员是否到岗到位进行有效的监督。

（3）众多分散的施工现场和项目部对管理层开展项目管理及协同作业带来很大困难。

为进一步加强通信工程现场管控，实现施工现场安全行为的实时管控，解决现场安全质量管控难度大、进度信息反馈不及时、安全风险问题难以预防控制等问题，对人脸识别技术、入侵检测技术、深度学习等物联网及人工智能技术进行研究，并将其应用到工程现场管控中，建立一套智能化的现场管控系统，实现工程施工现场安全风险智能预警，进一步提升工程现场管控整体技术水平，严格管控现场施工作业的安全、质量、进度，确保工程高质量安全推进。

2　国内外研究水平综述

随着社会的发展，人们对电力的需求量逐年增加，为了保证人们的正常生活与工作，电力工程施工安全管控工作是当前重要工作之一。目前国内外的现场预警手段大都停留在人工阶段，而且普遍存在员工缺乏正确的安全生产意识以及管理不严等现状。在电力施工现场智能管理方面，缺乏有效的智能化手段进行管理，主要还是依靠现场安全员进行人员管控，通过人为判断到场人员以及是否有非法入侵现象、是否佩戴安全帽、现场是否有明火等情况来对现场进行管控。然而在实际工作中，部分地区可能存在管理不严、流于形式的现象，这就造成了电力行业安全施工缺少正确的管理，进而导致工程施工过程中易发生安全事故。

当前国家电网公司在施工现场安全管理智能化提升方面的工作重点是基于人脸识别技术的考勤管理、基于入侵监测算法的人员入侵识别、工作票与操作票识别等技术。以下分别介绍这几类技术的研究现状。

2.1　人脸识别技术

人脸识别是结合人的面部特征数据而完成识别区分的相应识别方式，借助计算机研究人脸图像，从而

人民邮电出版社

获取所需的识别数据，这样就能够实现不同人身份的区分和辨认[1]。这一识别技术关系到图像处理、模式区分和识别等多个领域的学科技术，同时跟人脑的认识能力高度相关[2]。全球范围内人脸识别技术在当下已经发展到较高的水平，早在上世纪 90 年代就已成为科研热点。目前在全球范围内，从事人脸识别技术的机构和企业很多，国外知名的有谷歌、斯坦福大学、卡耐基·梅隆大学等；国内这些年也涌现了很多实力派，如海康威视、科大讯飞、商汤科技、云从科技等。当下海内外在人脸识别方面所运用的技术重点为 3 种：结合几何特征的识别处理；结合代数特征的识别处理；结合连接机制的识别处理[3]。近几年的神经网络方法在人脸识别的研究上取得了显著的成果，尤其是深度学习方法。深度学习的初衷是模拟人脑的认知机理，在某些重要的人脸识别测试集上，深度学习模型已经达到甚至超出了人类的识别水平。

2.2 入侵检测技术

为了确保现场施工安全，国内外多采用安装于防护网上的探测电缆进行检测，同时辅助视频监控系统对现场状况进行确认，当有异物触碰到探测电缆时，启动报警系统。近年来，一些研究机构和电网公司合作开展了试验性的入侵检测研究。朱炜教授提出的输电线路监控系统中运动目标的智能检测与识别系统中，使用基于颜色的特征在前景目标中识别出大型机械，然后定位吊车轮，采用面积、偏心率和紧密度 3 个指标作为分类器特征向量的输入，来检测吊臂而识别危险行为。何冰教授提出的输电线路监控入侵检测系统使用背景减除法进行背景检测，并使用颜色作为大型机械的图像特征，对它进行建模。根据吊臂区域面积、偏心率和紧密度进行吊臂检测，使用 HOUGH 变换计算吊臂伸展角度，根据与输电线路间的距离发出警报[4]。

2.3 烟火检测技术

由于火灾的频发性，尽早预防和避免火灾事故非常重要。现今国内外使用的火灾探测系统一般基于传感器，主要分为静电式、感温式、感光式和复合式。此类触感器一般是对颗粒成分、环境湿度、温度等进行采样，从而展开测试，虽然成本低、见效快，但存在适用空间有限、易受干扰、误报率高、智能度低、不适合在恶劣条件下检测等局限性。近年来，随着视频监视设备的普及和视频图像处理技术的发展，研究者们将目光转向了视频火焰检测。目前主流是基于小波变换的火焰检测算法，借助相应的时域小波理论，创建小波滤波器，对相关的颜色信号完成小波转换，经过对子小波的研究从而能够合理辨别火焰跟具备相似颜色的一般物体运动[5]。这种方法能够及时测定出视频图像内的火焰，同时将火焰跟一般物体进行辨认区别，具备较好的实时性，出现错误的概率较低。

2.4 工作票与操作票识别

为了提高变电站操作的安全性，国家电网公司已经开展了一系列的研究。华伟提出了一种基于光学字符识别技术（optical character recognition，OCR）的防误操作系统，使用 Tesseract 算法对工作间隔和设备标识牌图像中的文字进行识别，与工作票与操作票中的数据进行对比校验，防止误操作。目前，Tesseract 3.0 版本加入了对汉字的识别，并建立了汉字集用于学习训练，在调优识别过程的同时，针对对象的特殊性选择特定的训练集进行识别，进而提高识别的效率和准确性[6]。此外，将深度学习应用于光学字符识别的应用也日益成熟，为工作票和操作票的识别提供了一条新的路径。

3 研究内容

本文基于物联网与人工智能技术，对电网施工现场安全风险智能预警算法进行研究，用于实现对施工现场的智能监控。

3.1 基于深度信念网络的人脸识别算法

当工作人员进入工作区域时，摄像头对人员进行拍照，利用基于深度信念网络（deep belief network, DBN）的学习算法对人物图像进行识别。一个此类信念网络的不同组成模块都含有一定数目的节点（一般达到几百个甚至更多）。在运算的过程中，每层按照输入的信息，结合相应的玻尔兹曼机的学习方法，从而掌握该部分的 RBM 参数，实现初步的训练。当分别完成每组叠加而获得 RBM 后, 继续将初始的训练信息设定成相关的监督数据，按照所需函数，对全部网络实现调整和修正，这一步骤是微调，具体划分成两阶段。

（1）初始化

对相关网络划分为通过相邻两层形成的满足一定受限条件的玻尔兹曼机，分别完成数值的训练，对网络实现初始化设定。

（2）微调

为了让模型具备更为理想的表现性能，在实现一

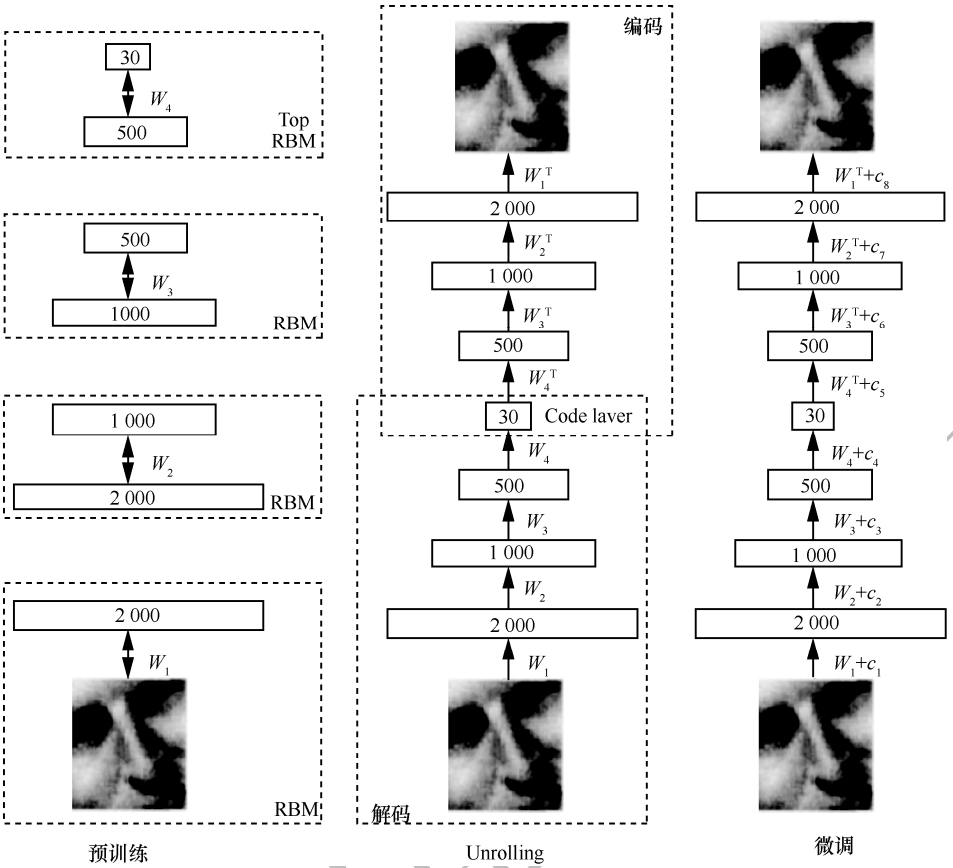


图 1　微调过程示意图[7]

组 RBM 后，逐渐展开，随后结合梯度下降法对 DBNs 完成优化，具体步骤如图 1 所示[7]。

结合贪婪的学习方法不管是初步训练还是微调时期，在时间、空间两个方面的复杂度上均为线性。因此在进行大量数据信息过程中，该方法效果突出。可以将基于深度信念网络的人脸识别算法应用于移动、考勤、异常人员检测。在工程施工现场设置门禁，将人脸识别算法嵌在前端摄像头中，利用摄像头对现场的工作人员进行识别，能够判断现场人员是否属于工作人员，当识别出非工作人员时发出报警。

3.2　运动目标检测和跟踪算法

当施工现场指定区域范围的安全距离内有异物（比如人、动物或小型车辆）入侵时，可以对运动目标进行检测和跟踪。具体的实现方式为先对视频内出现的运动目标做检测，然后跟踪此目标，系统会实时监控指定区域，当其进入高压线的安全距离时，触发报警。如何识别出运动物体进入到安全距离内是本文的研究内容之一。

假如并未出现异常情形，此时前后时间点获取到的视频图像是保持相同的。相应的不同像素点也不会出现变化，二者之间的像素相减等于 0。当出现了异常情形，此时其对应的局部范围将会出现变化，图像中一定范围的像素也会出现改变。这种情况下，前后两幅图像的像素相减不会为 0。结合该原理，对相减形成的变化范围展开检测运算，然后分析判断并及时报警[8]。

3.3　形态颜色特征分析算法

火灾已成为威胁变电站等现场最严重的自然灾害之一。因此，迫切需要对施工现场采取有效的监测，提前发布火灾预警，提高火灾防控能力。一般运用的火焰和烟雾识别是结合图像方面的高亮度范围的面积、边缘等特征而实现的。可利用图像方面烟火范围的变化以及边缘圆形度实现识别任务[9]。对火灾的识别判据主要分为以下两步。

（1）灰度图像分割

首先对图像进行灰度处理，然后对灰度图像采用

阈值分割法进行图像分割，该方法是根据图像中不同物体的灰度值不同而将物体区分开，而分割阈值是通过统计灰度图像直方图，并计算每个灰度级个数，最后应用灰度级个数计算得到阈值，具体如式（1）：

$$T=\frac{1}{2}\left[\frac{\sum_{k=0}^{T_i}h_k\cdot k}{\sum_{k=0}^{T_i}h_k}+\frac{\sum_{k=T_i+1}^{L-1}h_k\cdot k}{\sum_{k=T_i+1}^{T_i}h_k}\right] \quad (1)$$

（2）烟火面积检测算法

对于烟火的面积大小，可运用相关图像序列中相邻两帧进行相减而得到。就干扰物体而言，通常无法同时符合高亮度与面积随时间正比增长两个特征。当图像在分割处理后的差值大于 0 且不超过设定的阈值时，需要对序列展开相应的面积增长性分析，若分析结果为面积不断变大，那么需要结合边缘圆形度来进行区分；当差值超过阈值，则直接使用边缘圆形度来分析，差值的计算如式（2）[10]：

$$K_N(x)=(2\pi)^{-d/2}\exp\left(-\frac{1}{2}\|x\|^2\right) \quad (2)$$

3.4 基于 OCR 的双票检测算法

工作票和操作票制度是保证电力系统正常运行的重要措施，通过机器学习加强工作票和操作票的管理具有重要使用价值。其中主要用到了光学字符识别（optical character recognition，OCR）和 Tesseract 算法。OCR 基于图像识别为前提，经过识别图像方面的数据信息从而实现辨识目标。在图像识别前先对噪声和干扰等因素进行过滤，完成预处理后，若图像信息仍无法识别则进行强化、矫正颜色等处理；其次，分割图像、定位分离要识别的文字，接着提取文字特征展开参数运算与检测，并按照检测结果完成分类；最后根据提取的特征量识别分类，明确文字内容[6]。

本文研究 OCR 技术，特别是针对汉字的 OCR 技术，并根据电网工作票和操作票内容定制识别率高的字库或训练模型。电网工作人员通过客户端上传包含完整工作票和操作票的图片，或通过前端摄像机拍摄工作票和操作票，系统能够识别出工作票和操作票中的文字内容，并加以分析判断，如工作人员是否进入了正确的工作间隔，或者票上时间与当前时间是否相符等。

4 关键技术难点

虽然不少算法在实验室环境中有不错的效果，例如人脸识别算法的识别率可达到 90%以上。但将各种算法运用到整个项目管理过程中，由于现场环境复杂多变，在实际测试中发现，当把各个算法集成在一起检测时，在复杂的背景中识别准确率并不理想。如何将算法集成在一起运用到现场管控，并提高识别准确率是研究的重点与难点。

4.1 算法适应性

在人脸算法的研究中，算法将 3D 模型的先验知识添加到变化多彩的人脸识别分析中，将二维人脸映射到相匹配的三维模型中，相应地运算得到姿态的外观、纹理数据等，最后将信息合成运用到识别上。因为人脸含有表情、姿态、光照等多种因素，因此受到了不同方面的影响，如何排除各种复杂变化的干扰准确地将二维人脸映射到三维先验模型上是研究的一个关键技术和难点。未来人脸识别的主要研究方向将围绕目前面临的一些问题，如人脸面部结构的相似性、人脸的姿态、年龄变化、复杂环境的光照变化、人脸的饰物遮挡等。

4.2 入侵检测物判断

如何判断入侵物体是入侵检测算法的关键。通过设置检验图像状态发生改变的最小阈值和最大阈值，再对改变值与最小阈值和最大阈值进行比较，只有当处于最小阈值和最大阈值之间，才认为是监测场景中发生了某种预定的异常。实际过程中天气、风向、背景，如风吹草动等因素都会对改变值造成影响，如何消除这些因素影响也是研究的一个关键技术和难点。

4.3 工作票与操作票识别

OCR 对于手写汉字的识别率不高，最根本的原因是手写汉字的字形变化太大。不同的人书写的字是千差万别、各不相同的，即使是同一个人所写的同一个字，也因时因地而有变化。因此，手写的操作票和工作票对于机器学习识别来说仍然是一个难点，如何提高识别手写汉字的正确率是研究的关键。

5 结束语

针对电网通信工程施工现场安全管控存在的问题，基于物联网和人工智能技术，对深度信念网络人脸识别算法、运动目标检测跟踪算法、形态颜色特征分析算法、OCR 双票检测等算法进行研究，并将这些算法应用到工程现场安全管控系统，实现施工现场视

人民邮电出版社

频监控、违章行为自动分析、安全隐患管理、作业现场管控等业务功能，辅助开展工程现场高效快捷管理，提升工程全过程管控能力。

参考文献：

[1] 林妙真. 基于深度学习的人脸识别研究[D]. 大连：大连理工大学, 2013.

[2] 琚生根, 周激流, 王朝斌, 等. 基于统计特征融合的人脸识别[J]. 四川：四川大学学报(自然科学版), 2009, 46(3): 618-622.

[3] 卢世军. 生物特征识别技术发展与应用综述[J]. 计算机安全, 2013(1): 63-67.

[4] 朱炜, 何冰, 刘新平, 等. 输电线路监控系统中运动目标的智能检测与识别[J]. 华东电力, 2011(10): 1699-1704.

[5] 吴铮. 基于视频的火焰检测[EB]. 2019.

[6] 华伟, 孙文凯, 单光瑞, 等. 基于 OCR 技术的变电站防误操作系统[J]. 电力信息与通信技术, 2017(4): 74-79.

[7] 林妙真. 基于深度学习的人脸识别研究[D]. 大连：大连理工大学, 2013.

[8] 赵建利, 张晓妍, 赵建坤, 等. 基于图像和应力的输电线路覆冰监测方法研究[J]. 自动化与仪表, 2018, 33(10): 55-59.

[9] 冷春艳. 基于红外图像处理的森林火灾识别关键技术研究[D]. 成都:电子科技大学.2016.

[10] 朱思思, 丁德红, 陈朝迎, 等. 基于图像处理的森林火灾识别方法研究[J]. 红外技术, 2016, 38(5):7.

人民邮电出版社

基于现代（智慧）供应链的重大电网工程智慧供应平台研究

马敏，王平，李梦渔
（国网冀北电力有限公司物资分公司（国网冀北招标有限公司），北京 100075）

摘　要：从现代（智慧）供应链建设出发，应用“大、云、物、移、智”等先进技术，针对重大电网工程建设特点，高效聚合内外部资源和数据信息，打造智慧供应平台。通过构建融合内外部的全量数据资源池、供应链全景可视化监控、全业务多维智慧决策层、精准供应体系四大模块，实现了资源开放共享、供应全息感知、多维智慧决策、物资智慧供应，全面提升物资供应保障和协同运作能力，保障了重大电网工程建设平稳有序。

关键词：现代（智慧）供应链；重大电网工程；智慧供应平台

1　引言

2019 年，国家电网有限公司提出“三型两网、世界一流”战略目标，建设枢纽型、平台型、共享性企业，在坚强智能电网基础上建设泛在电力物联网，共同构成能源流、业务流、数据流“三流合一”的能源互联网。现代（智慧）供应链建设是“两网”融合在物资专业的具体实践，不仅具有泛在电力物联网的基本特性，还具备供应链资源配置的枢纽优势，推动电网高质量发展[1]。

国网冀北电力有限公司承担 2022 年冬奥会、北京副中心建设、70 周年庆典等多项重大电力保障任务，需完成廊坊、唐山、张家口等多地煤改电建设，电网建设任务极为繁重。物资作为企业的核心资源，供应及时性对电网建设影响巨大，客观上要求物资管理更加精益高效。传统的电网工程物资管理中，存在资源统筹不足、供需匹配度低、应急保障时效性不强等痛点，同时受环保限产、原材料价格波动、产能饱和等影响，存在履约任务重、供需矛盾大、管控难度高等困难。面对物资供应管理新形势，冀北公司加快推进现代（智慧）供应链建设，打造具有冀北特色的数字物流体系，开发了重大电网工程智慧供应平台。

2　重大电网工程智慧供应平台介绍

冀北公司应用大数据、云计算、物联网、移动互联、人工智能等先进技术，高效聚合内外部资源和数据信息，打造重大电网工程智慧供应平台，为建设“三型两网”世界一流能源互联网企业提供优质高效服务支撑。因此，开发智慧供应平台是保障电网工程建设和提升物资管理水平必然的选择，对现代（智慧）供应链发展至关重要。

重大电网工程智慧供应平台是电网物资管理核心基础设施，在现代（智慧）供应链建设中发挥着重要作用，其系统架构如图 1 所示。平台通过打造全量数据资源池、供应链全景监控、全业务智慧决策、精准物资供应体系，实现资源开放共享、供应全息感知、物资智慧供应，为电网工程建设提供了智能决策和数据支撑，真正实现物资供应的数字化和信息化管理，为电网建设提供坚强物资支撑。

3　融合内外部的全量数据资源池研究

3.1　基于大数据的物资资源池

通过全业务统一数据中心[2-3]，采集 ERP、ECP、WMS 中物资数据，运用大数据深度挖掘实物库存、协议储备库存、未执行合同等物资资源，集中共享各级数据资源，建设全网和省级物资资源池。充分应用物资资源池，实现各层级各单位库存资源的日常可视化查询、调取和应用。向项目单位开放资源查询功能，实现物资资源开放共享，便于电网工程建设紧急情况下对物资资源的调用。主界面如图 2 所示。

通过物资资源池主界面，展现实体库存、协议储备库存、合同物资等资源，可查询其物料编码、物料描述、库存地点、库存数量及金额等信息，分析各地市物资资源分布趋势，根据不同情况精确获取可用物资资源，如图 3、图 4 所示。

人民邮电出版社

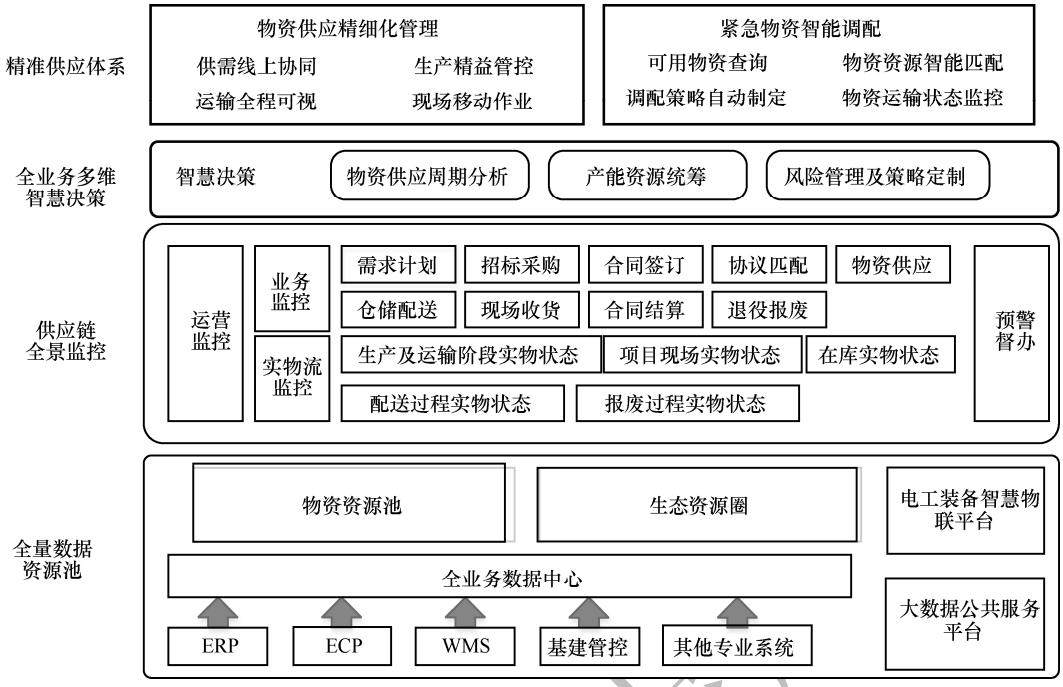


图 1　重大电网工程智慧供应平台系统架构



图 2　物资资源池主界面



图 3　物资资源池查询界面



图 4 物资资源池分析界面

3.2　链接外部的生态资源圈

通过全业务统一数据中心，对接基建管控系统，可实时获取电网工程里程碑计划、需求计划等信息，实现建设专业与物资供应专业的数据共享。对接电工装备智慧物联平台，全面掌握供应商图纸设计、生产备货、供应商寄存、产能运能、物资发货、运输计划、资金付款等信息，实现对物资生产的精准管控。对接大数据公共服务平台，获取全国范围内的供应商征信情况，为提前预警提供数据支撑。

通过与工程基建系统、供应商生产系统以及征信系统的紧密链接，打造枢纽型、共享型的内外部物资生态资源圈，共享工程、应急、征信、物流等信息，实现跨专业智联互通，如图 5 所示。

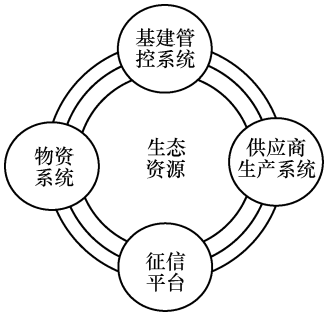


图 5　内外部生态资源圈

4　供应链全景可视化监控的研究

4.1　供应链全业务运营监控

对接全业务统一数据中心，从 ERP 和 ECP 动态获取贯穿物资全寿命周期的各业务流转状态及关键节点信息，涵盖需求计划、招标采购、合同签订、协议匹配、物资供应、仓储配送、现场收货、合同结算、退役报废九大业务环节，通过 47 个监控点跟踪物资供应各业务数据信息，动态预警计划、合同、供应、库存、配送、报废等业务完成状态，为电网工程物资供应决策提供数据化支撑，如图 6 所示。

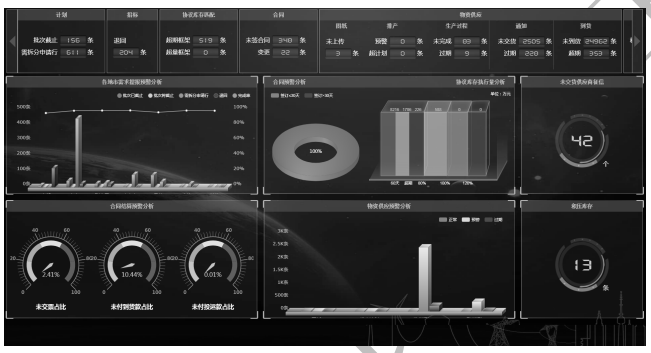


图 6　全业务链运营监控主界面

4.2　基于实物 ID 的实物流跟踪监控

实物 ID，即电网资产统一身份编码，是贯通电网资产各阶段管理中存在的唯一不变的项目编码、WBS 编码、物料编码和资产编码[4]，如图 7 所示。运用实物 ID 编码，可实现实物资产在规划计划、采购建设、运维检修和退役报废全寿命周期[5]内的信息共享与追溯，提升资产精益化管理水平。



图 7　实物 ID 安装实景照片

在重大电网工程物资供应管理中，以资产实物 ID 为纽带，通过关联设备参数、供应商名称、采购订单号等，建立实物 ID 跟踪监控模型，全程记录物资在规划计划、需求提报、合同签订、合同履约、物资发货、物资收货、工程建设、竣工验收、设备运维、退役报废等环节的实物状态信息，在线监控物资所处的位置和状态，实现对资产全寿命周期的有效管控。实物 ID 跟踪监控流程如图 8 所示。

在物资生产运输阶段，通过电工装备智慧物联平台获取供应商生产过程数据，实时掌握物资图纸确认、备料生产、组装试验、物流运输等全过程信息，实现物资生产全过程精细化管理，如图 9 所示。

在物资到货后，通过实物 ID 及相关信息，跟踪项目物资的到货时间、现场交接、物资验收、设备投运状态，自动扫码完成现场移动收发货，实现现场移动作业。

物资入库在库时，通过实物 ID 监控物资入库、在库、出库等数据及信息，通过视频监控良心中心库、

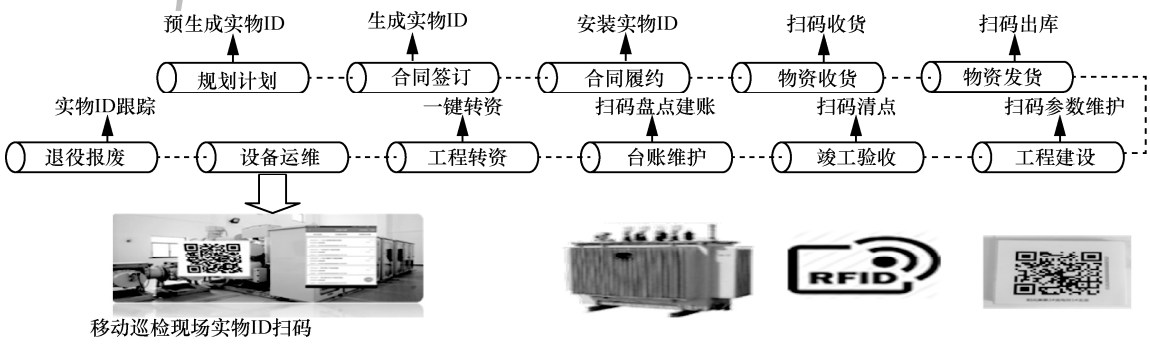


图 8　基于实物 ID 的实物流跟踪监控

唐山应急库、地市周转库、县级仓储点的库存状况，在线指挥出库入库作业，如图 10 所示。

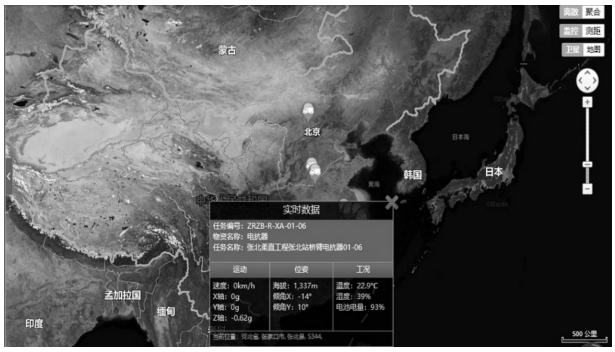


图 9　物资运输阶段跟踪信息



图 10　库存在线监控

配送施工现场途中，对物资运输计划、任务调度、车辆推荐、运输轨迹、货物交接等环节进行定位、跟踪与监控，实现配送全过程管控。

5　全业务多维智慧决策层研究

5.1　基于大数据的物资供应周期模型研究

应用大数据构建物资供应周期数学模型，科学分析需求计划、招标采购、合同签订、物资生产、运输配送等环节的标准用时信息，为各业务环节管理提供支撑，预防由前期、中期、后期各环节用时不合理带来的合同履约和物资质量风险。根据基本原理，建立如下计算模型：

$$T_a = T_p + T_b + T_c + T_m + T_t$$

其中，T_a 为供应周期，即需求计划提报开始至到货完成的理论周期；

T_p 为需求计划提报理论周期，即发布公告日期-计划申报截止日期；

T_b 为招标采购环节理论周期，即中标结果下达日期-发布公告日期；

T_c 为合同签订环节理论周期，即合同生效日期-中标结果下达日期；

T_m 为物资生产环节理论周期，即开始发运日期-合同生效日期，包括图纸确认、备料、生产、出厂试验、包装周期；

T_t 为运输环节理论周期，即到货完成日期-开始发运日期。

根据物资供应周期模型的建立，按照物资维度和供应商维度，分析各环节合理物资供应用时信息，建立供应周期标准，自动监控物资供应实际节点信息，及时发现并预警合同履约风险，为物资的有序供应提供智慧决策。

5.2　供应商产能资源分析

自动获取供应商产能数据信息，根据全网同期中标量分析可用于冀北重点工程的剩余产能信息，建立产能资源模型如下：

$$\begin{cases} Q > C_a - C', \text{红色报警} \\ Q = C_a - C', \text{黄色预警} \\ Q < C_a - C', \text{正常} \end{cases}$$

其中，Q 为某供应商当前在冀北地区的月均供货量；C_a 为某供应商当前月均总产能；C' 为某供应商在其他地区月均已使用产能。

通过冀北地区月均供货量、总产能和已用产能对比分析得知：当供货量大于剩余产能时，标志着已经存在供应风险，应进行红色报警；当供货量等于剩余产能时，标志着可能存在供应风险，应进行黄色报警；当供货量小于剩余产能时，标志着物资供应满足产能要求，为正常情况。通过对产能进行综合分析，掌握物资生产前期信息，为统筹供应商产能提供数据支撑。

5.3　风险分级及策略定制化

基于全业务数据中心和链接外部的生态资源圈，建立内外部一体化风险数据库，对各类风险进行分类分级管理。设置风险权重区间，自动发布六级履约风险预警信息，定制相应的处理策略，实现履约风险提前感知、有效应对。风险分级及策略定制见表 1。

6　精准供应体系的构建与应用

6.1　物资供应全过程精细化管理

通过电子商务平台（ECP）[6]主动获取重点工程物资到货需求计划，线上协同项目单位、供应商按照实际需求确定物资交货期，系统根据各类物资生产工

水电邮电出版社

表 1　供应风险分级及策略定制

风险等级	风险内容	应对策略
1 级	未造成供应滞后	持续关注供应商履约情况
2 级	存在供应滞后轻微风险	采取电话催交、专题约谈等方式处理
3 级	存在供应滞后较严重风险	需及时协调供应商，组织专业人员前往厂商进行生产巡查，及时上报国网物资调配中心协调解决
4 级	影响工程投运	需立即上报国网物资调配中心，组织人员赴现场核实，及时采取产能统筹、跨省调配等措施，防范合同履约风险
5 级	影响电网运行安全	应及时采取跨省调配、解除合同、重新采购等措施，防止风险范围扩大
6 级	严重危害电网正常运行	应立即采取中止合同、重新采购、暂停支付货款等措施，防止公司资金流失及法律诉讼风险

序节点，制定科学合理的供应计划，实现供需精确协同。

通过电工装备智慧物联平台获取供应商原材料备货、生产进度、物流状态等信息，实时掌握物资供货进度，与供应计划自动对比，对于进度滞后的采购订单进行分级预警提示，根据预警等级采取定制化的供应策略，为物资人员提供决策依据。图 11 为物资生产全过程管控界面。

系统自动对接物资运输监控平台，获取供应商运输信息，跟踪物资运输状态、运输车辆和运输人员等内容，并与获取的运输管控平台中相关数据进行自动对比，对异常信息及时预警，实现在途物资有效管控。到货后，使用“e 物资”APP 扫描实物 ID 芯片，实现收发货作业线上移动办理。图 12 为移动作业平台界面。

6.2　紧急状态下的物资智能调配

工程建设中，时常遇到供应商产能不足、征信不良、破产倒闭等紧急情况，导致物资无法正常供应，从而引发履约风险。当达到 3 级风险及以上时，根据定制的供应策略，考虑采取物资调配方式解决掣肘问题。



图 12　“e 物资”移动作业平台界面

系统根据物资调配需求，在物资资源池中进行查询，根据固化匹配规则智能分级匹配可调配物资资源，智能制定物资调配策略，自动下达调配方案。图 13



图 11　物资生产全过程管控界面



图 13　应急物资智能调配界面

为智能调配功能界面。在调配过程中，运用物资配送管理系统，实时监控调拨物资运输状态，确保物资安全、及时运抵需求现场。

比如，在 2022 年冬奥会配套电网工程建设中，系统通过大数据公共服务平台、天眼查、启信宝等外部征信系统，获知某供应商因法律纠纷导致生产异常，已无法正常履行合同。系统启动资源池进行库存查询，发现库存满足应急要求，智能采用协议库存匹配作为调配策略，立刻下达调配方案，24 h 内完成调配工作，保障冬奥工程建设有序推进。

7　结束语

文中主要讨论了基于现代（智慧）供应链的智慧供应平台在重大电网工程建设中发挥的重要作用。首先对开发重大电网工程智慧供应平台的必要性进行阐述，就智慧供应平台整体架构和功能进行介绍；然后对智慧供应平台中全量数据资源池、供应链全景可视化监控、全业务多维智慧决策层和精准供应体系四大模块进行详细说明。全量数据资源池为智慧供应提供数据支撑，供应链全景可视化监控自动感知物资供应状态，多维智慧决策层为供应过程提供策略支持，最后通过精准供应体系实现物资有序供应，为重大电网工程建设提供物资智慧。

参考文献：

[1] 电“联”世界 智“链”未来—国家电网泛在电力物联网之现代（智慧）供应链建设纪略[N]. 国家电网报.

[2] 基于大数据的全业务统一数据中心数据分析域建设研究[J].电力信息与通信技术, 2017, 15(2): 91-96.

[3] 全业务统一数据中心建设助推电力人工智能发展[C]//2018 年中国电机工程学会年会论文集, 2018.

[4] 电网资产统一身份编码信息系统建设及应用[J].电力信息与通信技术, 2018, 16(1): 102-105.

[5] 国家电网公司资产全寿命周期管理规定[M].北京: 中国电力出版社, 2017.

[6] 国家电网公司电子商务平台系统建设研究[J].中国科技成果，2011, 12(17): 44-48.

基于知识图谱的电力通信网智慧大脑技术研究

周晶，孙喜民，张宾
（国网电子商务有限公司，北京 100053）

摘　要：在电力通信网领域，通过知识图谱技术对领域产生的大规模数据进行处理，构建知识图谱，为电力通信网管理、运检、风险监测、业务调度、知识沉淀提供人工智能服务，结合研究成果，可以构建基于知识图谱的电力通信网安全智慧大脑，提高领域内管理者、运营人员、消费者的生产效率。

关键词：人工智能；知识图谱；深度学习；知识大脑

1　引言

“Books are the ladder of human progress”这句名言出自著名文学家高尔基之口，浓缩了人类以知识为传承并不断取得进步的方法论，揭示了知识对于人类进步的重要性。在经典科幻电影《星球大战》中，机器人 C-3PO、R2-D2、R4-P17 等的戏份不可谓不多，特别是 C-3PO，是会多种语言的礼仪机器人，会搞笑、多愁善感。电影同样表达了人类对终极人工智能的憧憬，C-3PO 机器人每一句简单的台词，都需要具备世界认知、情感认知、自我认识等大量的数据以及知识来支撑、辅助机器人处理接收到的各种信息，了解信息包含的意思，形成自主决策，这些认知模块、决策模块，都需要机器人具备学习组织推理的能力。人工智能正在改变人们的日常生活，而知识图谱就是为实现这个目标应运而生的。

近年来，各大科技公司都在推出自己的人工智能系统和产品[1]，发展到今天，深度学习和知识图谱已成为人工智能的两大技术驱动力。相对于深度学习，知识图谱技术具有可广泛应用于不同任务，从海量数据中进行学习和挖掘，可理解、可解释，类似人类的思考方式等特性优势，知识图谱中的知识可沉淀、可重复使用，结合深度学习的计算能力，必将成为未来人工智能发展的趋势。在电力通信网领域，可以通过知识图谱技术对领域中的大规模数据进行处理，构建知识图谱，为电力通信网管理、运检、风险监测、业务调度、知识沉淀提供人工智能服务。

人工智能在人们生活中的应用如图 1 所示。

2　知识与数据结合驱动的后深度学习时代

当前，人工智能的方法已进入下半场，基于知识图谱的电力通信网安全智慧大脑（以下简称“智慧大脑”）是以知识图谱和数据计算来驱动的人工智能应用，都是在具有充分知识或数据、稳定性、完全信息、静态、特定领域与多任务的场景下应用的，通过学习重复出现的片段、具有语义的特征，开展后深度学习时代数据驱动与知识驱动结合应用的研究。

从科学技术研究的角度来说，“智慧大脑”就是做



图 1　人工智能在人们生活中的应用

人民邮电出版社

3 件事：感知、思考决策和动作。第一件事就是感知，让机器具备人脑的理解能力，也就是感性、感知、听觉、视觉等能力，能够对事件、场景进行识别；第二件事就是模拟人脑的思考决策，依托知识对识别的事件数据进行深度学习和计算，并根据计算结果决策；第三件事就是最后的动作，决策系统会发出动作指令，引导实施。

从应用场景的角度来说，电力通信网安全智慧大脑赋能 5 个标准体系，其中对标人工智能感知的监控体系，赋予电力通信网安全业务数据采集能力；对标人工智能辅助决策的驱动体系和计算体系，赋予电力通信网安全业务知识数据构建、业务数据计算的能力；对标人工智能动作的安全预警体系和运检调度体系，赋予电力通信网运检业务风险预警和调度实施的能力。

电力通信网络安全智慧大脑能力如图 2 所示。

3 “智慧大脑”构建

3.1 基于知识图谱的电力通信网安全“智慧大脑”

如图 3 所示，“智慧大脑”的研究和构建主要服务的对象为 3 类用户，一是面向电力通信网业务部门管理侧，提供智能调度、辅助决策等服务能力；二是面向电力通信网业务运营侧，提供风险预测、安全预警、实时监控、知识库构建、物联网通信等服务能力；三是面向电力通信网业务消费者侧，提供人机交互、用户互动等服务能力。

从管理者的视角来看，“智慧大脑”是电力通信网物联网以及人工智能的应用，可以兼容传统的业务管理，还可以充分、广泛和有效地利用历史业务数据、实时业务数据实现业务的智慧管理，实现日常业务管理基本可通过“智慧大脑”调度，突发业务可通过“智慧大脑”提供的辅助决策方案进行管理，释放人工，提升管理的效率和工作的有效性。从业务运营者的视角来看，“智慧大脑”会及时发现可能存在的风险点，对可能存在的风险进行预警，做到提前防范；还可以对电力通信网的设备运行情况进行实时数据采集，可以第一时间发现事件突发点，对故障进行精准定位，根据类似故障的历史解决方案提供故障解除辅助决策方案，大幅提高运检效率和安全防护的可靠性。从消费者角度来看，电力通信网不仅提供了传统的通信网络服务，还提供了机器人客服、人机互动、用户互动等人工智能服务的方式和渠道，用户满意度得到提升，也提升了用户对电力通信网相关产品和服务的认可度。

3.2 “智慧大脑”技术链

人工智能应用产品的宗旨是为人类服务，从各个维度替代人类的一部分劳动或全部劳动，提高生产力。“智慧大脑”也是一样，其目的就是提升电力通信网业务的服务效率，提高领域生产力。针对电力通信网业务分布广、运维成本高、管理难度大的特性，“智慧大脑”在技术层面，结合图像识别[2]、自然语言处理、知识图谱、物联网通信等前沿计算机和物联网技术，从根本上解决和改善业务痛点，用人工智能服务提升

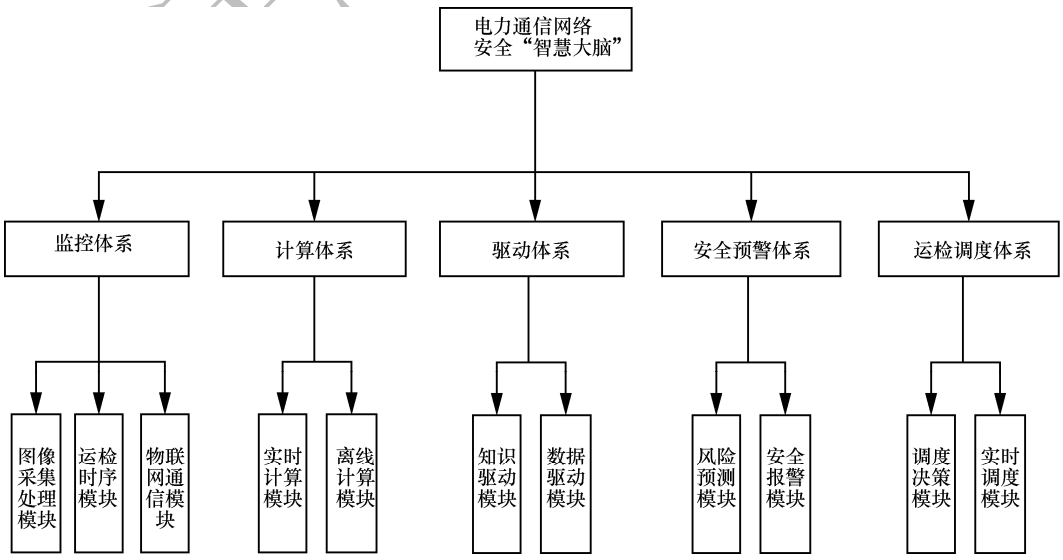


图 2　电力通信网络安全智慧大脑能力

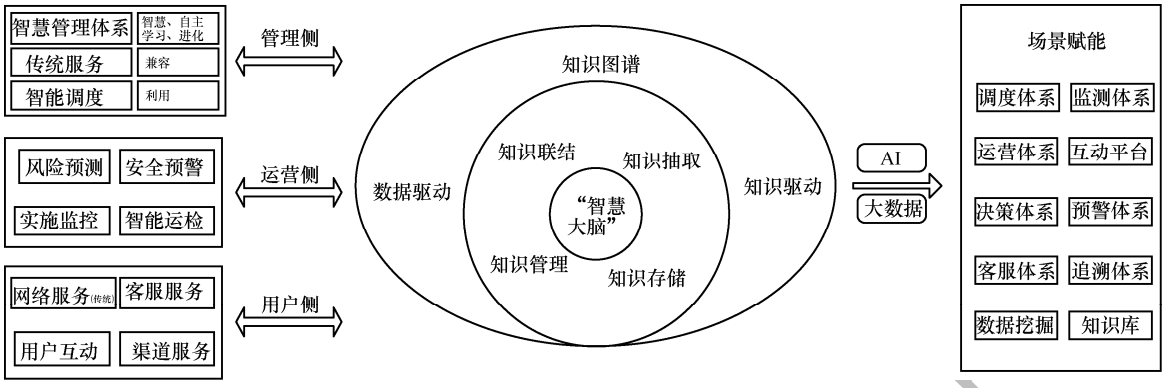


图 3 “智慧大脑”用户赋能

电力通信网体系的生产力。

知识图谱技术是“智慧大脑”的核心技术，通过挖掘电力通信网体系各业务场景数据，用 AI 技术让机器“阅读”设备知识、业务流程、故障处理等数据，理解电力通信网体系的全业务过程，构建基于时间、空间、事件的设备运行维护知识体系，构建知识图谱，形成一个“知识大脑”，从而赋能业务。“智慧大脑”技术链分为数据采集层、知识抽取层、知识融合层、知识存储层、知识应用层 5 个核心层次，以科学的理论支撑进行人工智能服务，如图 4 所示。

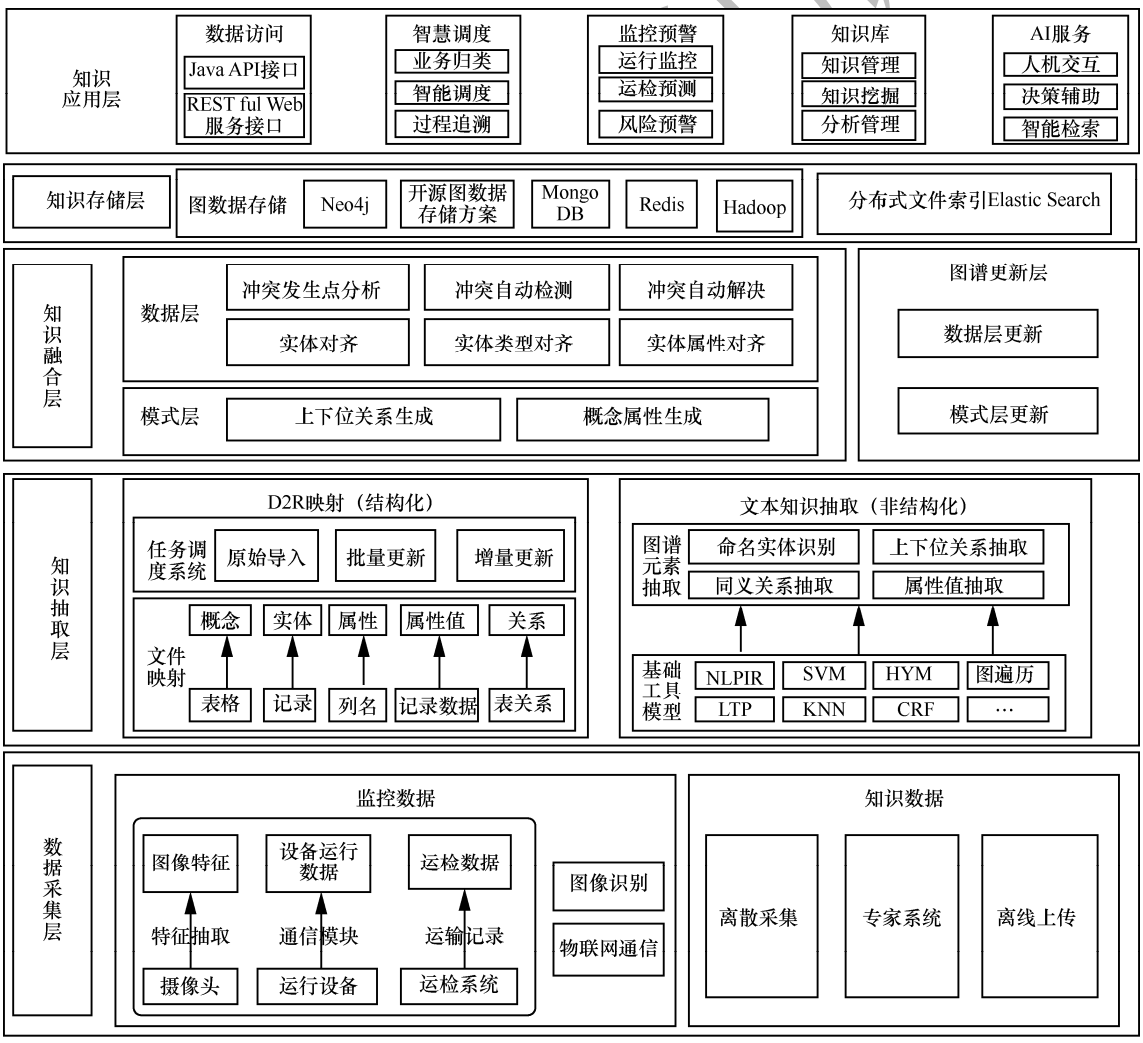


图 4 “智慧大脑”知识图谱技术链

（1）数据采集层

电力通信网的源数据来自多个维度、多类数据，以数据来源渠道来划分，主要分为两个类别，一是来自监控系统的数据，包含从摄像头采集的图像数据、从运行设备采集到的设备运行数据和从运检系统采集到的日常运维数据；二是知识数据，主要来源于网络采集、离线采集、专家系统沉淀的知识采集，知识数据主要包括电力通信网设备知识、运营维护知识、论文、专利等固有知识数据。在数据采集的过程中，需要大量前沿技术支撑，特别是图像特征采集的图像识别技术、设备通信技术和大规模数据存储技术。在上述两类业务层数据之外，还有时间、空间、事件、用户日志等基础数据，这些数据都是“智慧大脑”赋能人工智能服务的支撑数据。

（2）知识抽取层

知识抽取层的目的是对采集到的电力通信网业务数据进行知识抽取，抽取相关实体、属性、关系、事件等知识，构建业务知识图谱。从数据结构划分，采集到的数据分为结构化数据、半结构化数据和非结构化数据，每一类数据的处理方式都不一样。通常来说，结构化数据指关系型数据库表示和存储的二维形式数据，处理简单、准确率高，其自有的数据结构设计对数据模型的构建有一定指导意义，通常使用 D2R 映射技术来进行知识抽取，抽取规则[3]如下。

- dbtype：源数据库的类型，有 MySQL、Oracle、SQLServer 等，类型决定了连接时使用的驱动。
- dburl：数据库连接字符串，指定数据库的地址、端口和使用的数据库等信息。
- dbuser：数据库的用户名。
- dbpwd：数据库的密码。
- table：源数据表。
- concept：导入目标概念。
- name 的 colname 属性：实体名称来源列。
- synonym 的 colname 属性：同义实体来源列。
- parent 的 tablename 属性：父概念的表名。
- attribute 的 colname 指定属性来源列，attrname 则指定属性名。

对于半结构化数据，将使用 Wrapper 技术来结构化相关的金融知识，同时提供周期性的数据更新。对于非结构化数据，即自由文本类数据，将使用自然语言技术和机器学习模型，在文本中进行命名实体识别[4]，并抽取文本中概念或实体的上下位关系、同义关系和属性信息。

Schema 是知识图谱的数据模型，实体是知识图谱 Schema 的核心单位，从文本中抽取实体是知识获取的一个关键技术，对文本中的实体进行识别后，才能抽取实体。传统的实体识别方法以统计模型如 HMM、CRF 等为主导，随着深度识别技术的兴起和发展，Bi-LSTM+CRF[5]模型逐渐被用来识别文本中的实体，该模型避免了传统 CRF 的特征模版构建工作，同时双向 LSTM 能更好地利用前后的语义信息，能够明显提高识别效果。Bi-LSTM+CRF 模型如图 5 所示。

“智慧大脑”的建设过程中，电力通信网设备是图谱中重要的实体之一，监控系统中设备的监控信息、运维人员对设备的运检信息、设备的知识信息、设备通信模块数据都能够很好地反馈设备的运营情况，可以根据设备情况进行风险预警、运检调度等处理，减低风险带来的负面影响。

（3）知识融合层

在知识融合层，也就是知识图谱数据模型 Schema 的构建过程，主要解决电力通信网业务多源异构数据整合问题，即将不同来源、不同结构但表达统一实体或概念的数据融合为一个实体或概念。融入来自多源数据的知识，必然会涉及知识融合工作，实体融合主要涉及 Schema 融合、实体对齐、实体链接等技术。

知识融合主要解决知识抽取获得的结构化数据产生的知识冲突，知识冲突主要包含 Schema 冲突、实体冲突以及属性冲突等问题。知识融合将对从知识抽取获得的结构化数据进行实体与概念的识别、实体合并、实体对齐、上下位关系学习、关联关系学习，把记录型业务数据转化为知识图谱形式的三元组知识；同时提供自动实体的冲突检测，并根据预定的冲突解决策略对融合过程中产生的冲突进行解决。

（4）知识存储层

在“智慧大脑”的知识存储层，旨在为电力通信网全业务提供对以图形数据为主体、多种数据共存的应用的一站式存储、查询、分析[6]和挖掘平台服务。知识存储主要包括三部分：知识存储、采集存储和其他存储。其中，其他存储是用于存储图谱计算过程中的一些中间数据，如标注结果、图挖掘结果等；采集存储主要用来存储采集体系采集到的业务数据；知识存储则是用于存储图数据，基本设计理念如图 6 所示。

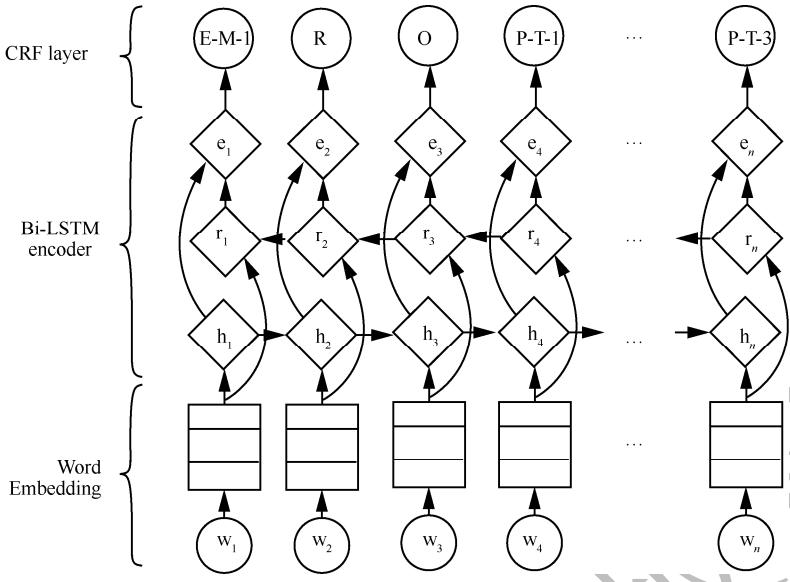


图 5　Bi-LSTM+CRF 模型

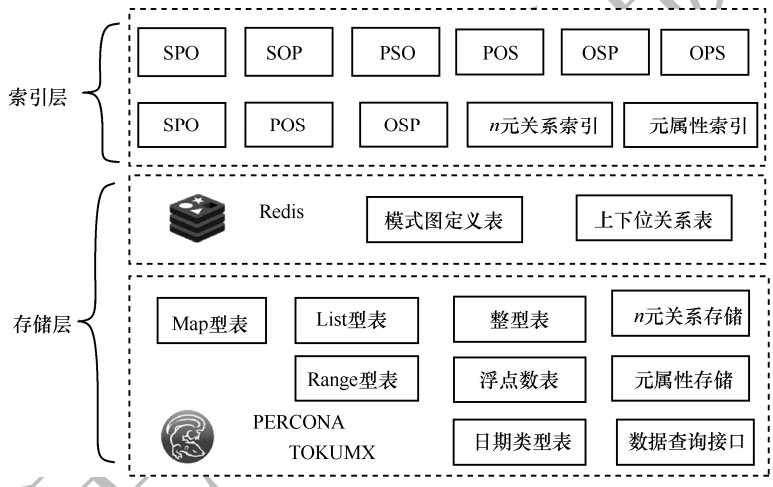


图 6　图存储设计框架

（5）知识应用层

知识应用层就是“智慧大脑”的服务层，以实现业务目标、解决用户问题、提升电力信息网生产[7]为宗旨，为管理者提供智能调度管理、管理辅助决策等服务，为运营人员提供风险预警、智能监测、数据挖掘、智能运检等服务，为消费者提供人机交互、机器人客服、资源共享平台、知识查询、消费决策等服务。

针对电力信息网业务管理者而言，根据历史业务发生的时间、地域、共性等知识数据，结合区域消费者的消费习惯，通过数据计算，精准预测未来一段时间内消费者可能产生业务的地点和业务需求点，通过“智慧大脑”知识图谱共词分析挖掘相关数据，如图 7 所示，通过共词数据可以确定在 2018-2019 年这个时间周期内，光纤接入业务[8]的需求、故障常发生的地点、时间段和关联数据的趋势。

针对设备运营团队而言，通过“智慧大脑”可以快速发现故障地点、故障问题点、故障解决方案、可能关联的故障点。在某台设备产生故障时，“智慧大脑”会在第一时间对采集到的实时故障数据进行分析、比对，结合历史故障点、故障问题，出具辅助决策解决方案，并把解决故障的指令发送到故障点就近空闲的工作人员，对故障进行解决实施。

针对消费者而言，可以在“智慧大脑”消费者侧通过基于知识图谱技术的 FAQ 系统、机器人客服系统、检索系统进行问题的查找和知识的检索，快速找到故障点和故障解决方案。

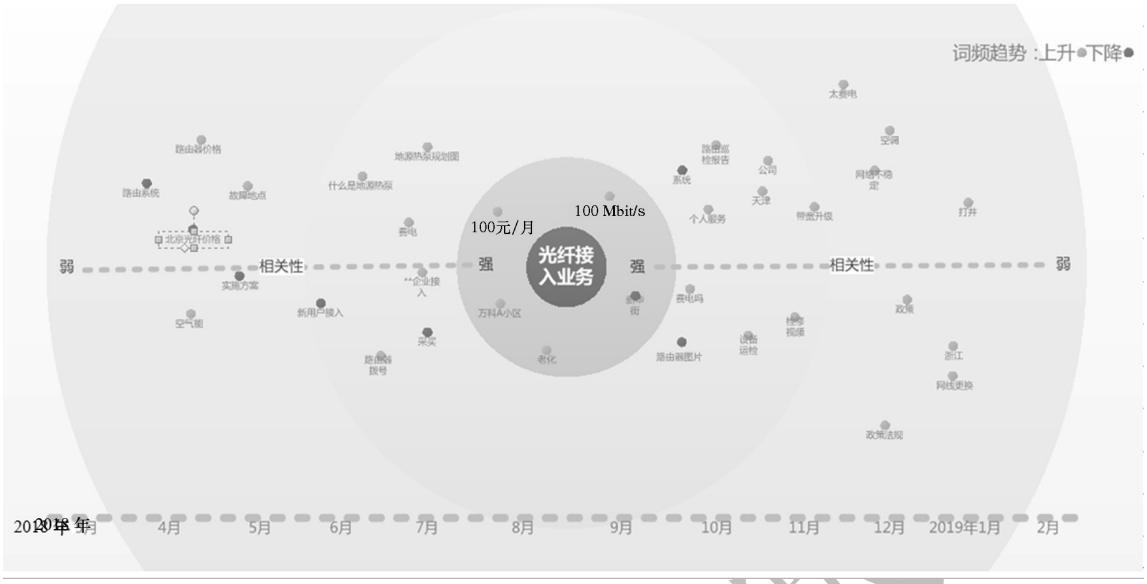


图 7　知识共词系统的数据挖掘决策辅助

3.3　“智慧大脑”赋能应用

“智慧大脑”在研制过程中，对电力通信网络全业务数据进行了采集和针对业务的知识图谱构建，生产出大量宝贵的知识数据，这些数据都是机器可以读懂的“三元组”关系数据，除了当前面向 3 类用户的服务支撑，特别是在智能搜索、智能推荐、机器人知识库构建、电力通信网语料标准化处理方面都能提供高效、安全、稳定的技术和数据服务支撑。

3.4　“智慧大脑”面临的挑战

通过对基于知识图谱技术的电力通信安全智慧大脑的研究和探索，遇到了诸多具有挑战性的难点。

（1）多源数据不一致问题

在知识图谱 Schema 的构建和更新过程中，遇到数据源众多、数据质量差、数据不一致等问题，可以通过针对不同的数据进行特定清洗，元数据约束校验、业务逻辑正确性校验等，设置严格的数据接入和更新规范。

（2）千亿级大规模数据的搜索引擎

“智慧大脑”的广泛应用将可能面临千亿级数据的存储、计算、查询和处理问题，针对此问题，可以对数据进行分层存储、实时增量、离线增量、全量图三层 Merge 查询。

（3）知识图谱应用

在基于知识图谱的“智慧大脑”应用过程中，算法设计、系统实现和实时应用都是难点，在算法问题上，需要有效融合数据驱动和知识引导，才能提升算法效果和提供更好的解释性，这属于研究前沿领域。

4　结束语

基于知识图谱技术的电力通信网安全智慧大脑只是知识图谱技术的应用之一，知识图谱技术是一门强大、适应性强、应用面广的技术和方法论，在各领域都可以借助其进行业务知识图谱的构建，把业务文本的自然语言转化为机器语言，构建可解释的关系型的“三元组”关系数据，以此来服务人工智能，驱动人工智能的发展。

参考文献：

[1] 王志宏, 杨震. 人工智能技术研究及未来智能化信息服务体系的思考[J]. 电信科学, 2017, 33(5): 1-11.

[2] 马思伟, 罗法蕾, 黄铁军. AVS2 视频编码标准技术特色及应用[J]. 电信科学, 2017, 33(8): 3-15.

[3] ZHENG S C, WANG F, BAO HY, etal Joint extraction of entities and relations based on a novel tagging scheme[J]. 2017. arXiv: 1706.05075.

[4] ZHENG S C, HAO Y X, LU D Y, etal Joint entity and relation extraction based on a hybrid neural network[J]. Neurocomputing 2017(257): 59-66.

[5] HUANG Z H, XUW, YUK. Bidirectional LSTM-CRF models for sequence tagging[J]. 2015. arXiv: 1508.01991.

[6] 汪来富, 金华敏, 刘东鑫, 等. 面向网络大数据的安全分析技术应用[J]. 电信科学, 2017, 33(3): 112-118.

[7] 姜红红, 张涛, 赵新建, 等. 基于大数据的电力信息网络流量异常检测机制[J]. 电信科学, 2017, 33(3): 134-141.

[8] 崔秀国, 刘翔, 操时宜, 等. 光纤通信系统技术的发展、挑战与机遇[J]. 电信科学, 2016, 32(5): 34-43.

人民邮电出版

基于智能合约的 IBC 密钥更新方案

甄平[1,2]，史睿[3]，陈绍真[1,2]，杨珂[1,2]
（1. 国网电子商务有限公司（国网雄安金融科技集团有限公司），北京 100053;
2. 国家电网有限公司电力金融与电子商务实验室，北京 100053;
3. 国家电网有限公司信息通信分公司，北京 100761）

摘　要：利用区块链智能合约，解决 IBC（identity-based cryptography，基于身份的密码技术）密钥更新难题，提出一种去中心化的密钥管理及身份认证方案。本方案同时支持受监管模式和非受监管模式，以兼顾监管和隐私要求。在受监管模式下，由监管机构充当 KGC（key generation center）角色，完成用户 IBC 密钥更新过程；在非受监管模式下，用户可以自发完成密钥更新，在此过程中身份标识符作为公钥保持不变。密钥更新过程以交易的形式记录在区块链上，通过区块链数据的不可篡改性保证了密钥管理的真实可靠性和可溯性。提出的方案在泛在电力物联网海量终端设备的安全认证场景中能够发挥重要的应用价值。

关键词：智能合约；IBC 密码；密钥更新；物联网；区块链

1　引言

2019 年，国网公司“两会”做出全面推进“三型两网”建设、加快打造具有全球竞争力的世界一流能源互联网企业的战略部署，加快推进泛在电力物联网建设，充分应用移动互联、人工智能等现代信息技术和先进通信技术，实现电力系统各个环节万物互联、人机交互，打造状态全面感知、信息高效处理、应用便捷灵活的泛在电力物联网。目前国网接入的终端设备超过 5 亿台，其中，有 4.7 亿台电表，各类保护、采集、控制设备几千万台。规划到 2030 年，接入泛在电力物联网系统的设备数量将达到 20 亿台，整个泛在电力物联网将是接入设备最大的物联网生态圈。泛在电力物联网能够为电网安全运行、提高经营绩效、改善服务质量以及培育发展战略性新兴产业，提供强有力的数据资源支撑，但同时也面临着巨大的安全挑战，其中如何实现海量终端设备的身份认证是个难题。

现有的认证方式通常采用公钥基础设施（public key infrastructure，PKI）体系[1]，由认证机构（certificate authority，CA）负责管理 PKI 结构下的所有用户（包括各种物联网设备和应用程序）的证书，把用户的公钥和用户的其他信息捆绑在一起，在网上验证用户的身份，CA 还需要负责用户证书的黑名单登记和黑名单发布。但 PKI 认证机制并不适用于物联网海量终端设备认证问题，否则将导致 CA 证书管理异常复杂，一旦网络收到的终端请求超过了资源处理能力，出现单点故障，会导致整个系统瘫痪，并且 CA 证书存在成本高昂的问题。

基于身份的密码技术(identity-based cryptography，IBC)由 Shamir 首次提出[2]，其中每个实体具有一个有意义的、唯一的标识作为公钥，无需数字证书将身份信息与公钥绑定，能够避免 PKI 中复杂的证书管理难题，很适用于物联网终端设备的认证领域。2001 年，Boneh 和 Franklin[3]利用双线性实现了 IBC 加密算法构造。2013 年国际上发布了关于 IBC 的密码体系标准 IEEE Std1363.3[4]。我国也已启动了基于身份的密码体制的标准化工作，国家密码管理局于 2016 年 3 月正式发布《GM/T 0044-2016 SM9 标识密码算法》，对于完善我国商用密码体系具有重要意义。SM9 算法可以使用用户的手机号码或邮件地址作为标识，简单易用，无需申请数字证书，非常适用于电子邮件、智能终端安全、物联网安全等热门应用。

但是 IBC 认证机制需要可信第三方 KGC（key generation center）为用户分发和管理密钥，其中密钥更新是一个难题，若某个用户私钥泄露，或需要用户更换身份信息，那么身份的自证性会大打折扣，或由 KGC 更换主私钥和主公钥，此时所有用户的私钥都需要更

基金项目：国网雄安金融科技有限公司科技项目（No.5100/2019-72005B）；国家电网公司科学技术项目（No.5700-21972227A-0-0-00）

新，造成非常大的麻烦，并不实用。为解决这些难题，去中心化的认证机制提供了一个良好的选择，具有更快并且更安全的物联网接入，较低的认证代价，另外还能避免认证节点堵塞的瓶颈。区块链技术目前的研究热点，提供了物联网去中心化应用的良好解决方案[5]。区块链是一种去中心化的分布式账本，可以简单理解为分布在全球各个节点的分布式数据库，数据库由区块按时间顺序相连而成，形成一个链条，任何一个区块内数据的改变都会引起后续区块链的变化，这种特性使其具有几乎不可篡改性[6-7]。目前主流的区块链平台包括比特币[8]、以太网（ethernet）[8]和超级账本（hyperledger fabric）[10]等。研究人员相继提出了基于区块链的去中心化数据隐私保护方案[11]、固件升级模型[12]、电子商务交易模型[13]、身份管理模型[14]等。

本发明拟采用基于区块链的智能合约，提出一种去中心化的密钥管理方法，解决 PKI 数字证书管理复杂和 IBE 密钥更新难题，具有非常重要的实用价值。本方案支持 2 种密钥更新模式，可以实现监管要求和隐私保护的平衡。在受监管模式下，由监管机构充当 IBC 密码体制 KGC 的角色，可以获取用户的私钥，实现监管功能，并为用户执行密钥更新过程；在非受监管模式下，由用户自身充当 IBC 中 KGC 角色，密钥更新过程完全由用户操作，保证用户私钥的隐私性。密钥更新过程以交易的形式记录在区块链上，通过区块链数据的几乎不可篡改性保证密钥更新过程的安全可信。通过智能合约，还可以实现密钥的自动化更新过程，大幅降低了密钥的维护成本，在物联网场景中具有重要应用价值。

2 背景知识

2.1 区块链

区块链的结构如图 1 所示，区块中记录着多笔交易，通过 Hash 计算，根据 Merkle 树的形式最终得到 Merkle 根，保存在区块头上。每个区块头都保存着上一个区块的 Hash 值，由此形成一个链式结构。它基于密码学原理而不是基于信用，使得任何达成一致的双方直接支付，不需要第三方中介的参与。

交易通过共识机制写入区块链中，共识机制算法是区块链的核心技术之一，它决定了到底由哪个节点来记账，而记账方式将会影响整个系统的安全性和可靠性。常见的共识机制主要有 PoW[15]、PoS[16]、PBFT[17]等，文中主要研究基于区块链交易模型的密钥更新方案，并不依赖具体的共识机制。

2.2 智能合约

智能合约[8]是一套以数字形式定义的承诺（promises），包括合约参与方可以在上面执行这些承诺的协议，一旦相关事件触发，节点就会执行这个代码，进而更新总账本（ledger），目前以太坊是智能合约最常用的平台。智能合约原理如图 2 所示。

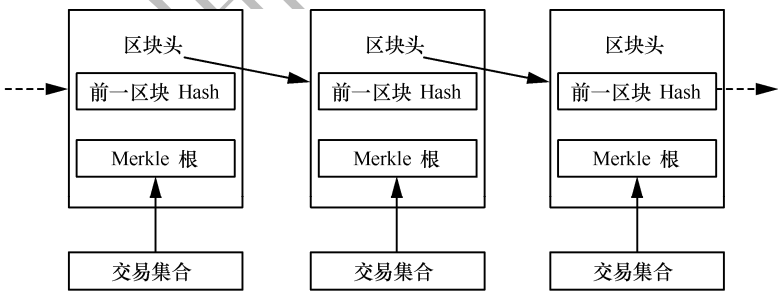


图 1 区块链结构

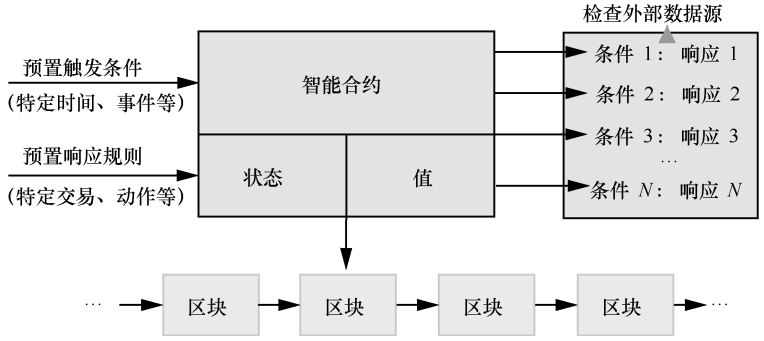


图 2 智能合约原理

2.3 基于身份的密码体制

基于身份的密码技术（IBC）[2]，能够有效地解决PKI数字证书管理的难题。它首先由KGC生成主公钥和主私钥，然后KGC再利用自己的密钥根据用户的身份信息ID（如名称、E-mail、身份证号等）为用户生成私钥，用户的ID即为公钥，无需数字证书绑定。文中主要采用国密SM9标准算法作为IBC密码体制的一个实例。SM9标准分为总则、数字签名算法、密钥交换协议、密钥封装机制以及公钥加密算法和参数定义5部分，详见《GM/T 0044-2016 SM9标识密码算法》。下面主要对SM9数字签名算法进行介绍。

设 P_1 为椭圆曲线加法循环群 G_1 的生成元，P_2 为椭圆曲线加法循环群 G_2 的生成元，$H(\cdot)$ 为Hash函数，$e(\cdot)$ 为双线性对。假设A为签名者，B为验证者，SM9数字签名过程如下。

密钥生成：KGC产生的随机数 $ks \in [1, N-1]$ 作为签名主私钥，计算 $P_{\text{pub-s}} = [ks]P_2$ 为签名主公钥，则加密主密钥对为 $(ks, P_{\text{pub-s}})$。用户A的标识为 ID_{A}，为产生用户A的签名私钥 ds_{A}，KGC在有限域 F_N 上计算 $t_1 = H(ID_{\text{A}}, N) + ks$，$t_2 = ks \cdot t_1^{-1}$，得到 $ds_{\text{A}} = [t_2]P_1$。

签名过程：设待签名的消息为 M，A签名过程如下。

（1）计算 $g = e(P_1, P_{\text{pub-s}})$；

（2）选择随机数 $r \in [1, N-1]$；

（3）计算 $w = g^r$，$h = H(M \| w, N)$，$h = (r - h) \bmod N$；

（4）计算 $S = [l]ds_{\text{A}}$，则 M 的签名为 (h, S)。

验签过程：为了验证消息 M' 的签名 (h', S')，B执行以下过程。

（1）计算 $g = e(P_1, P_{\text{pub-s}})$；

（2）计算 $t = g^{h'}$，$h_1 = H(ID_{\text{A}}, N)$；

（3）计算 $P = [h_1]P_2 + P_{\text{pub-s}}$，$u = e(S', P)$，$w' = u \cdot t$。

（4）计算 $h_2 = H_2(M' \| w', N)$，若 $h_2 = h'$，则签名验证通过，否则失败

3 方案设计

3.1 系统架构

文中提出了基于智能合约的IBC密钥更新方案，整体架构如图3所示，区块链网络可以是公链或联盟链，由多个全节点和监管节点构成，全节点和监管节点都保存着所有链上数据，但监管节点相对于普通全节点有更高的权限，负责用户初始身份信息的注册，并在监管模式下能对用户的密钥进行更新。用户（代指人或各种物联网终端设备）通过全节点连接到区块链网络，实现相互身份认证和网络信息交互。

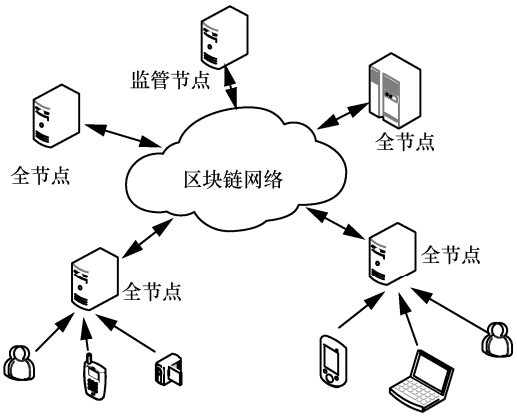


图3 基于区块链的密钥更新系统架构

本方案的密钥更新模式分为2种：监管模式和非监管模式。监管模式是指监管机构可以获取用户的私钥，可以监控用户加密的相关信息，非监管模式则表示监管机构无法获取用户的私钥及相关加密信息等。在监管模式下，由监管机构充当IBC密码机制中KGC的角色，并且作为交易发布者，通过更改用户可变身份标识符部分，为用户更新密钥，此时参数部分保护不变；在非监管模式下，由用户自身充当KGC角色，可以通过更改可变身份标识或改变主私钥等参数方式，完成密钥更新过程。

3.2 方案执行过程

区块链网络需要支持智能合约，通过部署一个密钥管理合约，该合约有一个或多个管理员，管理员为可信认证机构，对用户的身份ID信息进行初始认证。管理员首先利用IBC方案生成主公钥和主私钥，在认证合法用户的ID后，为其生成相应的私钥。本方案执行包括初始注册、密钥更新、密钥修复、用户身份变更和用户密钥注销几个过程，实现对用户IBC密钥全生命周期的管理，下面分别对这几个过程进行介绍。

（1）初始注册

用函数RegisterID (f_ID， v_ID， b_supervised，b_valid) 表示，该函数由合约管理员调用，对用户的ID身份信息进行注册，其中f_ID和v_ID是注册的身

人民邮电出版

份信息，即 ID = (f_ID || v_ID)。 f_ID 为 ID 固定不变的标识部分，如名称等；v_ID 为 ID 的可变部分，可以是日期或其他的随机数，主要用于密钥更新，初次注册时为空值。b_supervised 是一个布尔变量，主要表示该注册的 ID 是否为受监管用户，若为受监管用户，则管理员能够得到用户的私钥，并且后续需由管理员对其密钥进行更新；若为非受监管用户，则管理员在用户注册后无法得到用户的私钥，后续由用户自己对其密钥进行更新；b_valid 表示用户 ID 目前是否有效。

（2）信息查询

用函数 getID(ID)表示，可以被任意用户调用，用于查询某个 ID 的状态信息，例如是否已注册，是否为受监管 ID 以及目前状态是否有效。

（3）监管状态下的密钥更新

用函数 keyUpdataByAdmin(ID)表示，当用户密钥需要更新的时候，若为受监管用户，需要由管理员进行操作。非受监管用户只有在密钥泄露的时候才需要管理员为其更新密钥。此时管理员充当 IBC 中 KGC 的角色，改变其 ID 身份的 v_ID 部分，再利用其主私钥，重新为用户新的 ID 生成对应的私钥，并分发给相应的用户。

（4）非监管状态下的密钥更新

用 keyUpdateByUser(ID，sign)表示，若用户为非受监管用户，用户自身充当 KGC，可以自发地更新自己的私钥，此时用户需要生成自己的主私钥和主公钥，用户无需再更改 ID，直接生成其 ID 所对应的私钥。sign 为用户利用更新密钥前的私钥对更新后的状态进行签名，以保证其有效性。在不改变 ID 的情况下更新用户的密钥，能够极大提升用户身份信息的自证性。

（5）身份无效设置

用 disableID (ID)表示，当用户的私钥泄露时，管理员将用户 ID 的 b_valid 置为无效状态，然后需要调用 keyUpdataByAdmin(ID)函数，为用户更新密钥。

（6）身份撤销

用函数 removeID (ID) 表示，当用户的身份信息超过有效期或因为其他原因导致无法使用时，可由管理员和用户调用该函数，实现 ID 身份信息的注销。

上述函数只是密钥管理合约的基本实现，还可以扩展更多功能，使方案更加完善。例如可以记录用户使用 ID 签名的次数，以便更好地追踪用户的私钥是否已泄露；设置每次密钥更新后的使用有效期等，利用智能合约实现用户密钥的自动更新。

4 安全性能分析

文中方案采用商用密码 SM9 标准算法实现 IBC 身份签名体制，利用区块链智能合约实现去中心化的密钥更新过程。SM9 算法的安全主要依赖于椭圆曲线离散对数难题：对于有限域 F_N 上的椭圆曲线 E 和其上的两点 P 和 Q，计算整数 x，使得 $Q = xP$，其目前仍是公认的 NP 难题。影响 SM9 算法效率的主要是双线性对的计算，可通过不断优化提升其效率。Beuchat 等[18]开发出 BN 曲线上 O-Ate 双线性对的快速运算软件库，在 Intel i7 2.8GHz 的处理器上，一次双线性对计算仅需要 0.832 ms，具有重用的实用价值。区块链的安全性依赖于 Hash 函数，以天河二号的算力估计[19]，产生比特币 SHA256 Hash 算法的一个 Hash 碰撞大约需要 2^{48} 年，充分说明了区块链的安全性。

区块链要求每个节点保存一份数据备份，随着海量用户接入网络，必然导致海量数据的扩张，可通过关键节点保存所有数据备份，其他节点保存需要以数据的方式解决，或在保证安全性的前提下舍弃陈旧的历史数据以减少数据容量。区块链可以实时监控智能合约的状态，并通过核查外部数据源，确认满足特定触发条件后激活并执行合约。通过智能合约，可以实现本方案中密钥的自动更新过程，设定密钥有效期作为触发条件，监管节点和用户节点可以自动选择相应的参数计算密钥，生成交易并写入区块链。通过智能合约，可以实现密钥更新过程的高效自动化运行。

5 结束语

为了解决泛在电力物联网海量终端设定安全认证难题，文中利用区块链智能合约，提出一种去中心化的密钥管理及身份认证方案，实现 IBC 密钥更新过程。本方案支持 2 种密钥更新模式，在受监管模式下，由监管机构充当 IBC 密码体制 KGC 的角色，可以获取用户的私钥，实现监管功能，并为用户执行密钥更新过程；在非受监管模式下，由用户自身充当 IBC 中 KGC 的角色，密钥更新过程完全由用户操作，保证用户私钥的隐私性。IBC 密钥更新过程以交易的形式保存在区块链上，通过共识机制保证了更新过程中数据的真实性和可追溯性。通过智能合约，能够实现对密钥更新过程的自动化管理，保证密钥更新的高效实现。文中提出了方案设

人民邮电出版社

计的基本框架，未来仍需深化研究，实现其在泛在电力物联网应用场景下的实用价值。

参考文献：

[1] 关振胜. 公钥基础设施 PKI 与认证机构 CA[M]. 北京: 电子工业出版社，2002.

[2] SHAMIR A. Identity-based cryptosystems and signature schemes[C]. Proceedings of the Advances in Cryptology Nov 24, Ssnta Barboara, California, VSA. Nev Yark: ACM Press 1948: 47-53.

[3] BONEH D, FRANKLIN M K. Identity-based encryption from the Weil pairing[J]//SIAM Journal on Compating, 2003, 32(3): 586-615.

[4] IEEE Standard for Identity-Based Cryptographic Techniques using Pairings[S]. 2013.

[5] CHRISTIDIS K, DEVETSIOKIOTIS M. Blockchains and smart contracts for the IoT[J]. IEEE Access, 2016(4): 2292-2303.

[6] 张宁, 王毅, 康重庆, 等. 能源互联网中的区块链技术: 研究框架与典型应用初索[J]. 中国电机工程学报, 2016, 36(15): 4011-4022.

[7] 张赵阔, 邢永恒. 区块链技术驱动下的物联网安全研究综述[J]. 信息网络安全, 2017, 17(5): 1-6.

[8] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system [EB].

[9] BUTERIN V. A next-generation smart contract and decentralized application platform[EB].

[10] Hyperledger. Hyperledger architecture working group paper[EB].

[11] GUY Z, OZ N P. Decentralizing privacy: using blockchain to protect personal data[C]//2015 IEEE CS Security and Privacy Workshops, Map 21-22, 2015 Washington, DC, VSA. Piscatcaoy: IEEE Press, 2015.

[12] BOOHYUNG L, JONG H L. Blockchain-based secure firmware update for embedded devices in an Internet of Things environment[J]. J Supercomput. 2016(9).

[13] ZHANG Y, WEN J T. The IoT electric business model: using blockchain technology for the internet of things[J]. Peer-to-Peer Netw. Appl, 2016(4): 1152-1167.

[14] JOSÉ G. FAÍSCA, JOSÉ Q. Rogado decentralized semantic identity[J]. SEMANTiCS 2016, September 12-15, 2016, Leipzig, Germany.

[15] DWORK C, NAOR M. Pricing via processing or combatting Junk Mail [C]// 12th Annual International Cryptology Conference, Aug 16-20, 1992, California, USA. Now York: ACM Press.

[16] LARIMER D. Transactions as proof-of-stake[EB].

[17] CASTRO M, LISKOV B. Practical byzantine fault tolerance and proactive recovery[J]. ACM Trans on Computer Systems, 2002, 20(4): 398-461.

[18] BEUCHAT J L, GONZALEZ D E, MITSUNARI S, et al. High-speed software implementation of the optimal ate pairing over Barreto-Naehrig curves[C]// 4th Zntemational Conference, Dec 13-15, 2010, Yamanaka Hot Spring, Jopan, Berlin: Springer Verleg, 2010.

[19] YUAN Y, WANG F Y. Blockchain: the state of the art and future trends[J]. Acta Automatica Sinica, 2016, 42(4): 481-494.

人民邮电出版社

可穿戴 AR 单兵系统在电力检修工作现场的应用

刘启才，陈兵，吕小锋
（中国广核电力股份有限公司，广东 深圳 518124）

摘　要：智能穿戴设备以“解放双手、高效交互、智能辅助”的理念并融合多媒体技术、计算机技术、通信技术、传感技术、光学虚拟显示等技术，而产生可穿戴增强现实（augmented reality，AR）单兵设备。对可穿戴 AR 单兵系统技术做了简要描述，并对系统在电力检修工作中的应用功能进行了分析总结。将 AR 技术应用到电力检修工作中，可以实现现场检修人员与后台管理人员建立“零距离”交互的智慧型体验。

关键词：AR；可穿戴设备；交互；远程指导；智能

1　引言

近年来，可穿戴设备逐步进入各行各业并得以应用，以 AR（augmented reality，增强现实）单兵智能眼镜为代表的科技产品也逐步在工业维修领域使用。AR 单兵智能眼镜具备可穿戴、便携、可移动的特性，结合其可交互性、智能性，在电力检修工作场景中能得到广泛性的应用，电力检修工作过程对人机交互、数据传输、业务指导、即时通信、辅助决策等提出了更高的应用需求。电力企业建全大数据、云服务及各业务应用服务等，使电力检修人员工作水平逐步向单兵智能性发展，电力企业向智慧型电站/厂迈进。

网络通信技术和计算机芯片技术的高速发展为软件开发应用提供强大的硬件基础，整个社会快速进入了大数据和互联网时代。各个电站/厂互联网建设已经成为智慧电站/厂的标志性里程碑，电力检修工作依托大数据和互联网的各种应用需求越发强烈。为了使移动互联网建设的成果更适应智慧电站/厂的发展需要，研究 AR 新技术来改变传统工作模式，适应智慧型工作方式。将电力检修人员与 AR 技术结合，贯穿电力检修工作全过程，运用后台数据资源，音视频实时交互和便捷性操作，摒弃离线式作业缺点，对电力检修工作过程精细化管理，提高检修效率，节约成本具有非常大的意义。

2　AR 增强现实技术说明

2.1　AR 增强现实技术原理

增强现实技术，是一种将真实世界信息和虚拟世界信息“无缝”集成的新技术，是把原来在现实世界的一定时间、空间范围内很难体验到的实体信息（视觉信息、声音、味道、触觉等）通过电脑等科技技术，模拟仿真后再叠加，将虚拟的信息应用到真实世界，被人类感官所感知，从而达到超越现实的感官体验，真实的环境和虚拟的物体实时地叠加到同一画面或空间同时存在。

2.2　AR 单兵系统组成

一套完成可穿戴 AR 单兵系统基本由可穿戴 AR 设备、无线传输网络及后台管理部分组成，如图 1 所示。

（1）可穿戴 AR 设备

可穿戴 AR 单兵设备基本由计算机视觉（包含计算机算法、计算机硬件、传感器、通信模块等）、显示（光学透视式显示屏）、其他设备（供电部分、电池、机械承载附件等）3 部分组成。

便捷的可穿戴 AR 设备结合其硬件技术与相关的软件技术协同实现，能够将真实与虚拟两者空间信息集成实现完美融合，并在 AR 可穿戴设备虚拟显示屏显示，穿戴者和后台人员之间进行“零距离”交互，实现多媒体、通信、信息反馈、显示与控制等应用的技术融合，使电力检修工作在提高效率的同时更具有智慧。

（2）无线传输网络

可穿戴 AR 设备与后台之间的数据交换、交互控制等业务须由无线网络承载，由于每个电力企业的无线网络环境不同，使用场景也不同，有自建的 Wi-Fi 网、4G 专网和借助运营商的 4G/5G 网络。

（3）后台管理部分

后台管理部分是 AR 单兵设备扩展应用的中枢部

人民邮电出版社

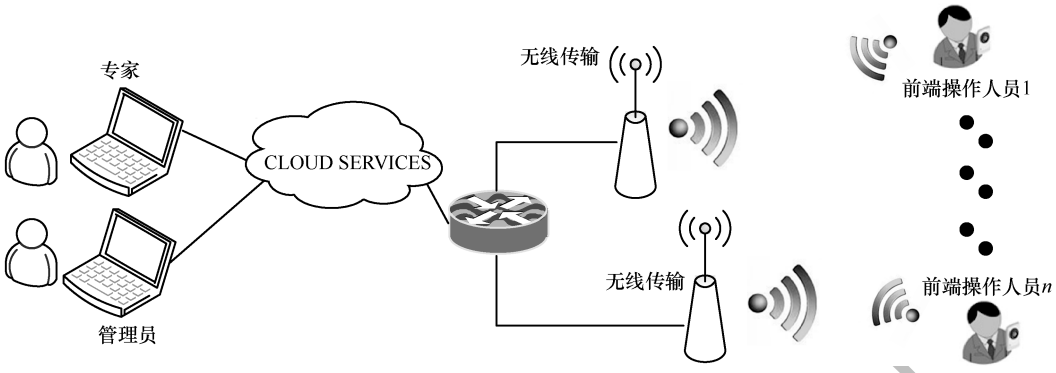


图 1　AR 单兵系统组成

分，后台管理人员对 AR 单兵终端设备、人员、资源管理（维修程序、设备建模、设备图纸、专家库、工作流库以及云端数据等）等进行管理，在电力检修工作时，后台中枢部分与前端 AR 单兵终端之间建立“高效交互”渠道，建全“辅助决策”机制，搭建“数据资源”平台，赋予每个 AR 单兵智能基因。

2.3　AR 单兵设备可穿戴方式

（1）眼镜架适配

眼镜框架适配 AR 智能眼镜，采用单目显示方式，AR 智能眼镜从重量上能做到尽可能轻便，主机部分和电池部分与眼镜分离，采用其他形式的佩戴方式（如卡箍在脖子、固定在腰间或手臂）以更好地进行移动使用。对于佩戴近视眼镜的人群，选配眼镜架适配器，调整焦距。在不接受后台指令等操作时，这种佩戴方式无法从视线范围内移开。

（2）护目镜适配

智能眼镜主机、电池都配装在护目镜镜架上，采用一体化设计增加护目镜整体的重量，护目镜采用鼻托支撑的方式，工作中佩戴时间长久后对鼻子产生压痛感，且作业期间若出汗很容易下滑，影响施工人员作业。护目镜适配的智能眼镜有个优点是根据个人用眼习惯可以左右眼镜互换，也可缓解长时间作业眼镜疲劳。对于戴近视眼镜的人群只能同时佩戴，这对鼻子、耳朵增加受力，相应地增加不少负担来应对护目镜和眼镜的稳定性。

（3）安全帽适配

在电力检修及施工现场施工人员一般都会佩戴安全帽，与安全帽标准适配孔适配后可增加稳定性，将着力点转移到颈部和头部，可根据工作内容调整棱镜显示屏观看或调整到视线外，对于检修人员行走或不使用智能眼镜时的工作减小工业安全的风险。由于眼镜佩戴方式的改变，可适当增加智能眼镜供电容量，增加眼镜续航能力，安全帽适配的佩戴方式在电力检修工作中应能得到广泛应用。

3　电力行业中的应用

3.1　单兵作战应用

在传统的电力设备抢修工作中，只能通过电话方式汇报描述现场情况，后台管理人员无法第一时间了解现场状态，现场人员只能获得单一的电话指导，对于重要的电力检修工作耽误工期，甚至影响检修关键路径实施，耽误正常供电时间。基于 AR 技术的应用在电力行业现场故障抢修、巡视等单兵作业工作领域，借助现场 Wi-Fi、4G/5G 网络实时回传音/视频数据，并与后台管理人员进行数据交互通信。电力检修工作人员佩戴智能可穿戴设备，通过图像识别和增强现实技术，快速正确地指引设备位置，进行后台管理者之间音视频实时通话，并且直观、快速地从云端业务大数据获取到现场设备信息，通过智能可穿戴设备的光学显示器将多种辅助信息叠加在现实世界之上并显示，可实时申请调用检修所需资料，减少检修人员数量，提高检修效率。

3.2　指挥调度

大型电站在运行一个周期后对电力设备进行定期检查及检修，这期间多个佩戴单兵设备的电力检修人员分布在电站各个角落，也有多个现场巡视人员佩戴单兵设备进行设备及现场巡视；在这种情况下需有一个管理平台统一管理现场所有 AR 智能终端，以便合理调配资源，提高检修效率。通过智能终端自带 GPS、Beacon（室内定位导航）模块时刻定位人员信息，指挥平台可实时了解每个智能终端当前的位置，并且每个终端设备在指挥平台注册管理。根据每项工作内容

人民邮电出版社

进行分组管理，指挥平台可实时展示每个智能终端的状态，在线/离线、是否在通话中（音/视频通话或语音通话），电力系统主控中心发现有设备告警、故障等信息时通过智能终端指挥平台调派故障点最近的智能终端进行查障，并把现场图像实时传送到指挥平台与主控中心人员进行第一视角视频确认和沟通。把现场佩戴 AR 终端的人可作为现场移动的摄像头，实时掌控现场设备状态，并能了解设备细节，知晓故障代码等信息。

3.3 远程专家指导

在电力设备检修中遇到棘手的问题时需要设备厂商技术人员或专家远程进行指导时（如图 2 所示），佩戴智能终端检修人员将现场实时图像及语音以第一视角第一现场呈现在技术人员和远程专家面前，摆脱传统的手机、座机、对讲机等通信方式，解放现场检修人员的双手，在通话的同时还可与技术人员或专家实时互动，让远端指导人员有种身临其境的感觉，在指导工作的同时也具备实时监护督导，根据检修问题的难易程度可推送设备相关的资料给前端检修人员棱镜虚拟显示屏显示指导作业，快速解决现场问题，提高效率，节省费用。

设备厂商技术人员或远程专家在做远程指导维修时，与现场佩戴 AR 设备终端工作人员可进行几项功能的互动，AR 虚拟屏可显示以下功能。

- 笔刷功能：对当前视频画面进行画线操作，屏幕可以看到画线标记。
- 箭头说明：对当前视频画面标出箭头供检修人员查看，方便说明。
- 冻屏：冻住当前视频某一帧画面，方便进一步说明。
- 电子白板：局部桌面共享，支持基于图片或直接进行画图供检修人员查看，可写可擦除。
- 短息文本指令：如检修人员处在嘈杂的环境中，后台可发送简短文本短信，显示屏可显示文本信息，接收后台指令。
- 后台拍照：后台专家可对设备实物信息远程控制拍照，拍照后及时上传到后台指定文件夹中保存，供专家集中讨论，做出决策。
- 后台调焦：后台专家想了解设备细节，可从后台通过对前端 AR 眼镜摄像机的变焦调整实现细节实时展现。
- 文件推送：在检修过程中可从后台推送设备连接图、视频、音频、文字等文档，供检修人员参考，指导现场工作。

3.4 远程 QC（质量控制）验证

电站或电厂电力设备检修是为了消除设备缺陷，确保可靠运行，在电力检修过程中，质量体系管理和安全系统管理贯穿整个维修活动，传统的质量和安全管理中需由质检员和安全员赴现场进行验证后，确保达到质量和安全的标准后才放行下一步工序，在工序中设置 H 点（停工待检点）、W 点（见证点）由 QC 人员验证，若多个现场同时施工，势必耽误工期。若采用施工班组佩戴 AR 智能终端，QC 人员远程进行 H 点和 W 点的验证，解决多个施工现场远程 QC 现场验证，减少 QC 人员，提高检修效率。

3.5 多方视频会议

在电站或电厂进行检修活动时需讨论问题或组织召开工前会时，AR 眼镜终端可一对一进行音视频会话，也可创建多人多路视频会议。在通话中，也可以呼叫另一个人或接听另一个人的紧急通话，使自己在

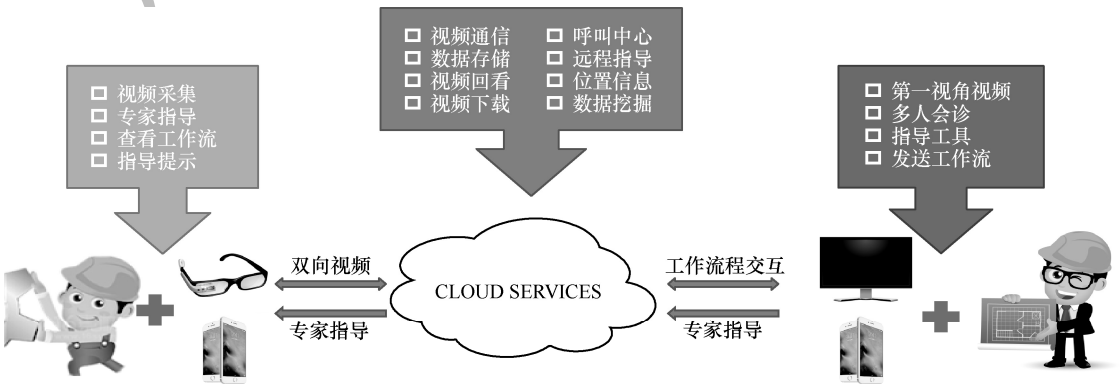


图 2　专家远程指导

当前会话中为暂时离开状态，挂断新通话后，自动返回到之前通话中。通话中的人员可以对第三个人发出邀请通话，对方选择接听可以加入当前会话中。

3.6 工作流可视化

（1）手动工作流

选择文本、图片、音频视频和 3D 模型等素材即可方便快捷地编辑工作流内容。现场操作人员可以直接通过手工操作的方式，从云端数据库查检索故障设备信息、维修方案、操作指导等，并手动按照设定好的步骤指导，完成现场工作。

（2）自动工作流

自动工作流是一套基于 AR 识别的工作流程管理系统。电力企业可以将作业指导书、操作手册等转换为“识别—调用—展示”的 AR 形式，现场人员不仅可以通过 AR 识别调取工作流，每一步操作还需要通过识别确认完成状态，才可以进行下一步，实现过程管理，达到规范作业、培训教学等目的。

3.7 智能识别检测

（1）类别识别

物体分类首先对视频图像进行物体检测，识别出图像上人、设备、车辆、证件、条码等物体对象，在视频流中实时跟踪物体对象的移动轨迹，针对检测到的物体对象调用最合适的识别引擎进行详细识别。

（2）图片识别

用户通过图片识别服务，上传需要识别的图片，图片识别服务自动提取图片的特征值，客户可以自由设定识别后需要展现的内容。

4 AR 技术前景简述

此系统的应用结合工业 4.0 从传统维修到智慧维保的指导思路，并结合电站/厂的实际需求丰富系统应用功能，应用虚拟现实（virtual reality，VR）、混合现实（mix reality，MR）等建立云服务、大数据以及应用业务服务，对施工现场设备信息自动扫描识别、人脸识别、工单创建下发、人员巡检轨迹回查（定位）、走错间隔提醒（语音或虚拟屏提示）、多方远程专家指导、重大设备建模 AR 虚拟操作培训等多种业务应用，为系统电站/厂精细化管理提供科技技术手段。

结合现场安全管控、质量控制、施工进度、降低成本等方面的因素，AR 单兵系统在实际应用中也从安全、质量、进度、成本等为施工现场辅助精细化管理。

- 固定收益：使用 AR 单兵系统后从原有施工工序中可以减少人员投入，减少施工工时。电力检修关键路径使用 AR 单兵系统，从安全、质量、进度等进行精细化管理，一项关键路径节省 10~15 min，将对整个检修工期来说有很高的收益。
- 隐性收益：现场视频留底，提供直观的培训素材；远程专家指导，减少专家去现场次数；出现异常视频回查，减少调查时间；QC 人员远程质量验证；特殊施工现场人员远程监护，减少工业安全的风险。

5 结束语

本文对可穿戴 AR 单兵系统技术做了简要描述，并对系统在电力检修工作中的应用功能进行分析总结。AR 技术借助互联网、物联网的建设成果，在电力检修行业中发挥更大的作用。在 AR 技术应用的同时，结合 VR 技术、MR 技术应用到电力企业管理中代替传统工作模式，在电力检修工作的需求驱动下，让每个单兵检修工作人员更具备智能性，电站/厂向智慧型发展。

参考文献：

[1] 刘建明. 增强现实、虚拟现实和混合现实技术在电力系统的应用研究[J]. 电力信息与通信技术, 2017, 15(4).

[2] 周安, 明德烈. 基于大数据技术的沉浸式虚拟现实可视化展示系统[J]. 电力信息与通信技术, 2016, 14(12): 20-25.

人民邮电出版社

密码技术在能源互联网中的应用及展望

王栋[1,2]，薛真[1,2]，廖会敏[1,2]
（1. 国网电子商务有限公司（国网雄安金融科技集团有限公司），北京 100053;
2. 国家电网有限公司电力金融与电子商务实验室，北京 100053）

摘　要：随着能源互联网战略的持续推进，电力系统“广泛互联、高度智能、开放互动、灵活服务”的全新特征愈发明显，电力业务全面互联网化的发展步伐日益加速，随之而来的是风险暴露面的不断扩大，能源互联网面临着巨大的安全挑战。密码是网络安全的基础设施，利用密码技术能够有效实现身份认证、访问控制、数据加密和信任管理，构建基于密码的安全防护体系是确保能源互联网安全发展的核心任务。提出加快构建以密码为核心的能源互联网综合防护体系，分析了密码技术在坚强智能电网和泛在电力物联网中的创新应用，并对量子密码和区块链等密码新技术的发展前景进行了展望，全面助力能源互联网网络安全主动防御能力建设。

关键词：能源互联网；密码技术；智能电网；泛在电力物联网；区块链

1　引言

能源互联网是以电力系统为核心，以互联网及其他信息技术为基础，构建的包含多种类型能源的互联网络，是互联泛在的坚强智能电网。概括来讲，坚强智能电网和泛在电力物联网构成了能源互联网。电力系统作为能源互联网的核心，是集发电、变电、输电、配电、用电于一体的电能生产与消费系统，自诞生之日起就具有高度自动化的特点。电力系统需在各个环节和不同层次设置相应的信息与控制系统，以便对电能的生产和运输过程进行测量、调节、控制、保护、通信和调度，确保用户获得安全、经济、优质的电能。如果电力系统的信息控制系统出现问题，整个电力系统就会出现严重的问题。随着坚强智能电网和泛在电力物联网的建设，电网信息化、智能化、互联化的程度不断加强，信息控制系统已经成为电力系统发展的重中之重。在信息化不断发展的同时，随之而来的能源互联网安全问题也日益突出：2015 年乌克兰电网遭受攻击，导致 22.5 万民众失去电力供应；2016 年以色列电力系统遭遇大规模攻击，造成相关计算机设备被迫关闭；2019 年委瑞内拉遭受网络攻击导致全国大范围停电。每一次的事故不仅造成重大信息和经济损失，更是造成居民生活的不便，甚至危害人身和社会安全[1]。不法组织和分子通过网络攻击基础设施，已经成为现代战争的一个重要作战手段。因此保障电力系统中信息控制系统的安全性至关重要。密码技术作为提供信息安全的一种重要手段，在电力系统的信息控制系统中发挥着关键作用。

2　密码技术

密码技术是信息安全的基石，能够提供信息的保密性、真实性、完整性以及信息的防抵赖性：信息的保密性主要通过加密密码技术来实现，信息的真实性、防抵赖性主要通过数字签名密码技术实现，信息的完整性主要通过散列技术来实现。

2.1　加密密码技术

保证信息的秘密性，是密码技术最初被应用的重要目的，也是密码技术的重要作用之一。提供保密性的密码技术为加密密码技术，现今被应用的加密密码体制分为两大类：对称加密密码体制和公钥加密密码体制。公钥密码体制的运算复杂度比较高，效率一般低于对称密码体制。因此在处理大量信息的加密时，一般使用对称密码体制，少量信息的加密一般使用公钥加密体制。国际上通用的对称加密算法有 AES 和 DES 等，公钥加密算法包括 RSA、ECC 等。我国商用密码大多采取国密系列密码算法，其中，对称密码算

基金项目：国家电网公司总部科技项目“电力业务动态身份安全认证与风险控制关键技术研究”；国网雄安金融科技集团科技项目“基于国产密码算法的移动应用数据安全和隐私保护关键技术研究与应用”

法包括 SSF33、SM1、SM4、SM7、祖冲之密码等；公钥密码算法包括 SM2 和 SM9。

2.2 数字签名技术

由于对称密钥分发和管理比较复杂，1976 年，Diffie 和 Hellman 提出了公钥密码体制的概念和设计思路[2]，很好地解决了对称密钥分发问题，同时提出了基于公钥密码体制实现数字签名的技术，为密码学在信息安全领域开辟了更加广阔的运用场景。数字签名技术利用私钥的私有性，实现了网络环境中通信双方身份的认证，系统中所有需要对用户身份进行鉴定的操作都可以使用数字签名技术来完成，从而保障了信息来源的真实性，防止参与方的抵赖。国际上通用的数字签名算法有基于 RSA、DSA、EC-DSA 以及 Elgamal 等的签名算法，目前我国国产密码算法（国密）系列中的公钥密码 SM2 和 SM9 都包含数字签名的实现机制和标准。

2.3 散列技术

密码技术中的单向散列函数，也称为 Hash 函数。是对任意长度的输入串变化成固定长的输出串，并且难以由输出串得到输入串。输出串也称为消息摘要值。通常输入串中发生任何改变，Hash 函数运算后的消息摘要值都会发生改变且不可逆运算，从而保证了信息的完整性。散列技术通常结合数字签名技术使用，也被应用于系统中存储用户口令的 Hash 值。国际上通用的散列算法是 MD 和 SHA 系列算法和 HMAC，HMAC 是在原有的 MD 和 SHA 算法的基础上添加了密钥，进行了加密运算。目前我国国密系列算法中 SM3 为散列算法。

密码技术从系统的用户登录入口开始，就能够进行用户口令 Hash 加密传输和存储保护，依靠数字签名技术对用户和设备进行强身份识别，然后根据识别的用户身份进行系统权限管理，从而实现不同用户的访问控制，保障系统的安全运行。加密技术和数字签名技术可以为传输在网络中的重要和机密信息保驾护航，具体可采取的安全通信协议如 HTTPS、SSL/TLS、IPSec 等。系统数据库中的敏感或机密信息可以采取对称加密将数据加密存储。

综上所述，密码技术一方面通过实现身份认证将攻击者阻挡在系统之外；另一方面，即使攻击者能够侵入系统，其权限也是受限的；即使攻击者能够获取系统中的重要数据或者截获网络中传输的机密信息，由于这些都是加密后的数据，攻击者在不知道密钥的情况下也无法获取到信息的明文。

3 常用密码技术体系

密码技术的应用一般基于特定的密码技术体系，目前常用的密码体系包括基于证书的公钥密码体系（public key infrastructure，PKI）和基于标识的密码（identity based cryptography，IBC)公钥体系。

3.1 PKI 公钥密码体系

为方便用户使用公钥密码来保障各种网络应用环境中的信息安全性，由 Internet 工程任务组（internet engineering task force，IETF）的 PKIX 工作组定义了一套国际标准协议—公钥基础设施 PKI。

PKI 体系的主要功能是将用户的公钥和其他标识信息绑定到一起，如用户名、电子邮件地址等，按照国际标准 X.509 格式封装到数字证书中，通过数字证书的管理完成公钥的管理，包括数字证书的生成、发布、注销、更新等，即对用户数字证书的整个生命周期进行管理。

PKI 系统由认证中心（CA）、注册中心（registration authoristy，RA）、密钥管理中心（KMC）、证书发布系统几个组件组成。其中，CA 是 PKI 的核心，负责所有数字证书的签发、更新、注销以及证书注销列表的签发等管理功能。注册中心 RA 负责录入数字证书的申请者的信息录入、审核等工作，密钥管理中心 KMC 为 CA 提供加密密钥的生成及管理服务，证书发布系统负责发布证书和证书撤销列表（certificate revocation list，CRL），以供查询。

PKI 体系可以为网络应用提供数字证书服务，为身份认证、访问控制、机密性、完整性、抗抵赖等安全服务提供全面的支撑，是目前技术最为成熟、性能稳定、适合大规模部署的一种密钥管理体系，但同时也是一种结构和流程比较复杂的管理系统。随着 Internet 的普及和深入，对 PKI 的应用需求不断增强，基于 PKI 的应用随处可见，如 Web 服务器和浏览器之间的通信、安全的电子邮件、电子数据交换、Internet 上的商务交易等；PKI 作为一种可靠的网络安全解决方案，已遍布在政务、金融、医疗卫生、电信、电力、教育、交通等领域的应用系统中。图 1 为 PKI 体系基本原理。

3.2 IBC 公钥密码体系

3.2.1 IBC 简介

由于 PKI 体系管理的复杂性，PKI 在提供了通用性的同时，也限制了公钥密码体制的灵活运用。尤其随着各种智能终端的出现以及移动网络的广泛应用，

人民邮电出版社

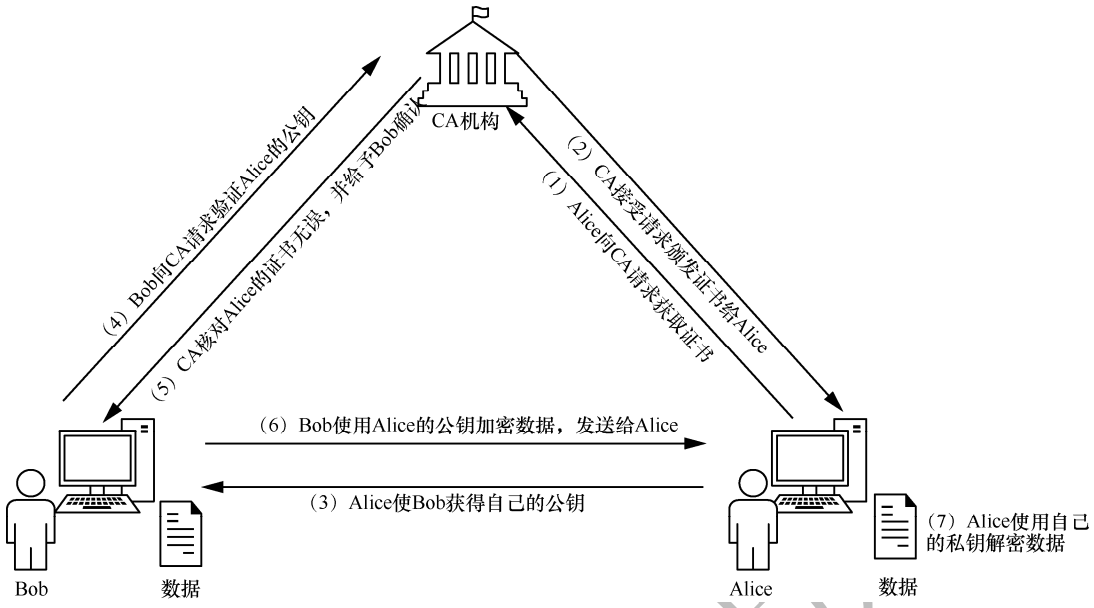


图 1　PKI 体系基本原理

PKI 在管理上的缺陷也逐渐暴露：证书查找、更新、撤销等证书操作占用大量网络资源，同时也给应用系统带来了较大的存储开销和计算量。针对 PKI 体系中存在的缺陷，1984 年，Shamir 开创性地提出了基于标识的密码公钥体制的概念[3]，在 IBC 中使用跟实体相关的公开信息作为实体的公开密钥，比如实体的手机号、邮箱、设备编码等标识码或标识码的组合。这些标识码或者组合能够代表实体的唯一性，以防止实体抵赖。公钥也可以由标识信息在具体的密码方案中计算得出。

在 IBC 体系中，存在一个私钥生成中心（private key center，PKC），负责根据实体标识 ID 生成对应的用户私钥。当一个实体加入一个基于 IBC 体系的系统中时，首先由 PKC 为其生成对应标识的私钥，并以离线或者在安全通道中的方式颁发给用户。IBC 做为公钥密码的一种应用体系，同样能够构建基于标识的公钥密码加密方案和数字签名方案。

IBC 体制解决了公钥与实体标识的绑定问题，不再需要数字证书作为公钥载体，也不需要如 CA 的第三方提供服务，绕开了 PKI 基于证书目录认证体制的束缚，极大简化密钥的管理，去除了繁琐的证书申请和管理过程，认证过程更加简单，对于普通用户来说更加容易操作和理解。IBC 体制使用户标识作为公钥，无需申请和查询数字证书，非常适用于如电子邮件安全、智能终端安全、物联网安全、大数据和云存储安全等应用。

在万物互联的物联网中，各种智能设备纷繁众多，而且数量一直在飞速增加，如果使用 PKI 体系来保障物联网中的信息安全性，生成及管理数字证书的成本以及在后期数字证书应用中的通信和计算成本，将是不可估量的。物联网引入对物理世界的感知和控制，使得人与设备、设备与设备间的通信与协作成为可能，而作为用于识别和区分不同设备和逻辑实体以及信息资源的物联网标识则是实现以上通信与应用的基础和前提。IBC 机制天然地可以把实体的物理标识作为公钥的特点，可以方便地为物联网提供身份认证、网络通信安全、数据机密性等安全防护[4]。图 2 为 IBC 体系基本原理。

3.2.2　IBC 在国内外的应用情况

最初，IBC 概念的构思是为了简化电子邮件系统中证书的管理。目前国外应用 IBC 比较成熟的也是安全电子邮件系统，如美国 Voltage 公司，采用标识密码技术的密钥数量已超过 5 000 万个，而基于标识加密邮件云 2017 年处理超过 30 亿封加密电子邮件，后续逐年处理的安全邮件数量将翻倍。

2007 年，我国基于标识密码技术标准正式通过评审，2008 年国家密码管理局正式颁发商密算法 SM9 算法型号，并于 2016 年 3 月正式对外发布。2017 年 11 月，SM9 标识签名算法成为 ISO/IEC 国际标准，2019 年 4 月，SM9 标识加密算法、密钥协商协议正式在 ISO/IEC 获准标准立项，SM9 将成为中国第一个完整非对称密码算法体系国际标准。

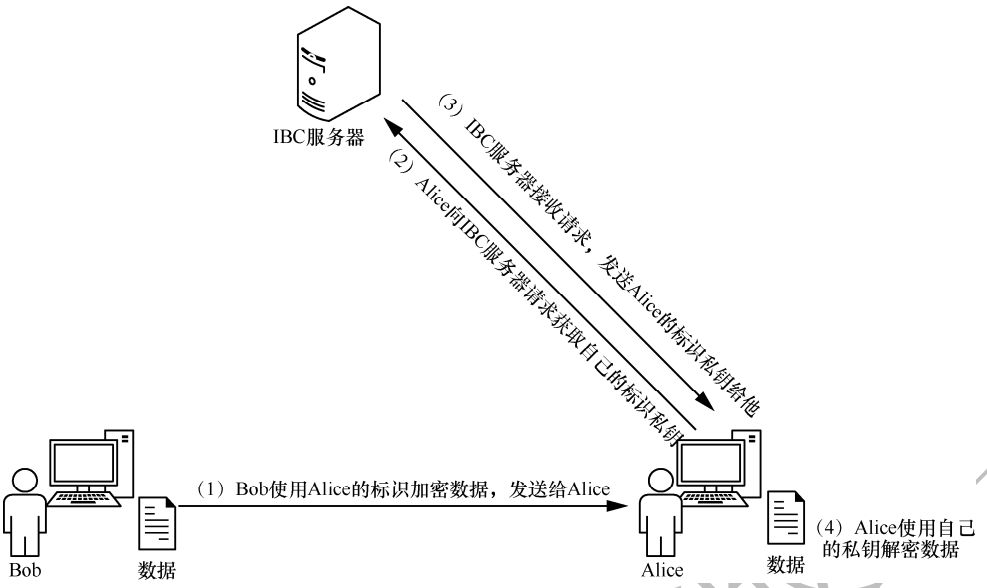


图 2　IBC 体系基本原理

3.2.3　IBC 的密钥托管和撤销问题

由于 IBC 体系中的私钥生成中心 PKC 掌握着生成所有用户私钥的系统主密钥，且生成私钥的算法是公开的，因此用户私钥和系统的安全性完全依赖于 PKC，一旦 PKC 的主密钥泄露，或者 PKC 被非法分子攻击并利用，便可冒充用户进行操作，这就是 IBC 固有的密钥托管问题。自 IBC 出现以来，学者们提出了很多针对密钥托管问题的解决方案，主要包括可追踪的基于身份的公钥密码方案、使用分布式 PKC 的方案、结合（短）证书的解决方案和无证书公钥密码（certificateless public key cryptography，CL-PKC）方案[5-6]。其中无证书的公钥加密概念和方案是由 Riyami 和 Paterson[5]在 2003 年的亚洲密码年会上提出的，在无证书公钥密码体制下进行签名可以达到真正意义上的不可伪造性，同时也克服了 PKI 体系中的证书存在问题，对公钥真实性的认证不再需要证书，大大地减轻了系统的复杂性和系统的开销，从根本上解决了上面两种密码体制存在的密钥托管和证书存在等问题。基于无证书的这些良好的性质，引起了学者们的浓厚兴趣，先后提出了大量的无证书加密方案[6-14]。

另外由于 IBC 体系中，用户的公钥是从用户的标识信息中获得，撤销用户的公钥相当于撤销用户的标识，因此不能简单撤销。设计合理的密钥撤销方案，也是 IBC 体系在应用中需要根据具体应用场景进行特别设计的部分。在当今信息爆炸、万物互联的时代，使用 IBC 体系来保障各种系统的信息安全性是一种必然趋势。趋利避害，如何利用好公钥密码体系 PKI 和 IBC 的各自优势，尽量规避每种体系的缺陷是密码技术应用领域需要多加探索的方向。

4　密码技术在坚强智能电网中的应用

4.1　坚强智能电网简介

随着社会的发展，传统电网面临一系列突出问题：信息获取不及时造成峰值使用时的“电荒”，能源利用效率低、环保性差等方面的问题比较突出。为解决以上问题，国家电网公司提出了“坚强智能电网”概念。智能电网将现代信息系统融入传统能源网络构成新电网系统，从而使电网具有更好的可控性和可观性，增强用电和发电的互动，及时获取电力系统中的数据，提高电力设备和能源的利用率。同时基于能量流的实时调控，便于分布式新能源发电、分布式储能系统的接入和使用。智能电网包括智能发电、智能输电及智能配电三大部分，智能配电网是电力公司与用户交流的边界，因此，智能配电网包含了电力与通信的双重任务，也是电网安全问题的高发地带。

传统电网与智能电网的区别如图 3 所示[15]，从图 3 中可以看出，传统电网中用户和电网之间没有通信，或者只有电网向用户发送信息。传统电力信息网络采用专用通信网络或设备，实现与外部网络的严格物理隔离，安全风险主要来自于内部网络和人员。智能配

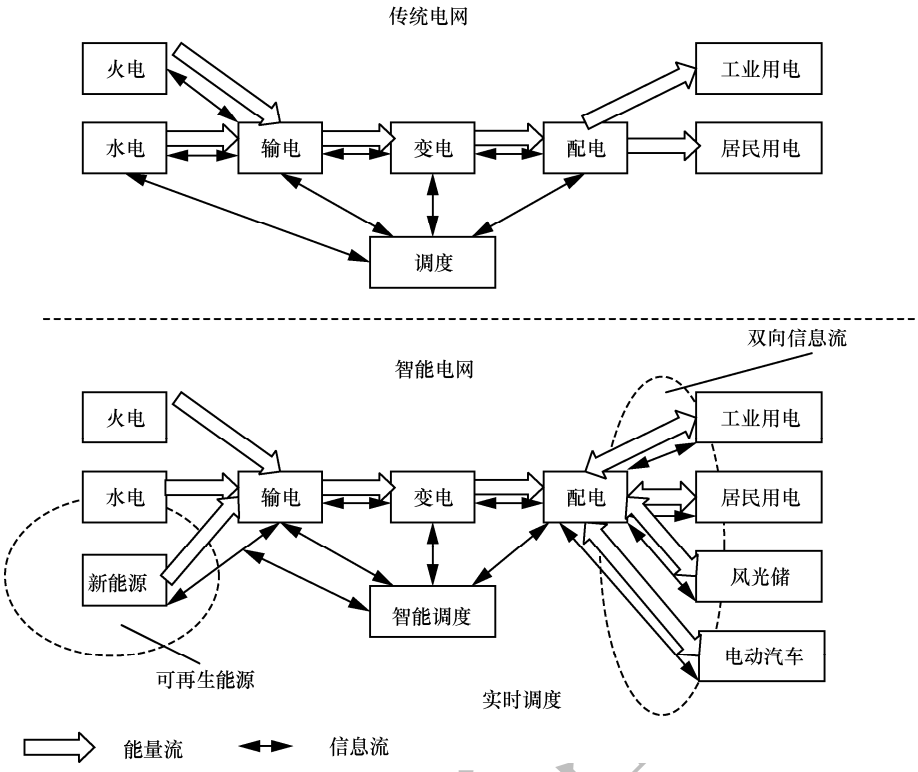


图 3　传统电网与智能电网区别

电网实现了用户和电网的双向通信，实现信息实时交互，暴露在互联网中的用户及用户终端在给电网提供实时信息的同时，也几乎将整个电力系统暴露在了公网之中，成为了攻击电力系统的最薄弱点。智能电表是用户最常用、最容易接触的终端设备，一旦被攻破，就可能对电力网络其他的设备造成威胁。因而，智能电网对网络通信技术、存储技术、信息安全技术提出了更高的要求[16]。因此为保障智能电网的信息安全应实现对每一个加入到电网中的智能电表进行认证，确保设备的合法性和独立安全性，确保用户和电网之间传输数据的完整性和机密性。

4.2　密码技术应用设计

虽然利用基于 PKI 的传统电力系统中的数字证书系统，可以通过为每个智能电表颁发数字证书，来实现对用户智能电表的认证。并且用户和电网双向通信时的数据安全性也可以使用 PKI 技术体系来实现。但由于电网中电表的数量多达数亿，而且数量还会不断增加，因此在电力调度数字证书系统中需要维护大量的数字证书，大大增加了系统的计算和存储要求。因此在保留原有电力调度数字证书系统的基础上，可以采取增加 IBC 公钥密码体系来保障用户和电网互动的安全性，在智能电网安全性建设中逐步设计合理的轻量级密码技术支持方案。方案设计思路如下：

步骤 1　在智能电力系统中设置 IBC 私钥生成中心 PKC，公布中心公开参数；

步骤 2　为每个智能电表安装安全专用芯片，为其分配唯一标识码；

步骤 3　在每个智能电表加入配电系统之前，由 PKC 为其生成对应标识码的私钥，离线加密存储在智能电表的安全芯片中；

步骤 4　在电网和用户进行双向通信时，首先使用 IBC 体系的数字签名算法实现双方的强认证；

步骤 5　双方认证通过后，使用 IBC 体系秘钥协商算法生成会话密钥；

步骤 6　使用会话密钥对双方的通信数据进行加密传输，保障数据传输时的机密性。

在电网和用户进行双向通信时，通信双方能够直接根据彼此身份 ID 和系统公开参数计算出对方的公钥，使用公钥完成对方身份的验证，避免了使用数字证书查询和验证的过程，减少了业务流程，降低了系统计算复杂度。因此，基于标识的密码体制的安全防护方法既能满足变电站通信的认证安全需求，也降低

了证书管理复杂度，适用于智能电网中安全防护[17]。

5 密码技术在泛在电力物联网中的应用

5.1 泛在电力物联网简介

国家电网公司在2019年1号文件中明确指出:“建设世界一流能源互联网企业，重点建设运营好‘坚强智能电网’和‘泛在电力物联网’，推动电网与互联网深度融合”。国家电网公司在《泛在电力物联网建设大纲》中定义：泛在物联是指任何时间、任何地点、任何人、任何物之间的信息连接和交互。泛在电力物联网将电力用户及其设备、电网企业及其设备、发电企业及其设备、供应商及其设备以及人和物连接起来，产生共享数据，为用户、电网、发电、供应商和政府社会服务；以电网为枢纽，发挥平台和共享作用，为全行业和更多市场主体发展创造更大机遇，提供价值服务。泛在电力物联网由感知层、网络层、平台层、应用层 4 层结构构成。图 4 描述了泛在电力物联网的结构。

如果把智能电网看作一个相对封闭的系统，泛在电力物联网则是一个完全开放的智慧服务系统。在这个系统中，通过广泛应用大数据、云计算、物联网、移动互联、人工智能、区块链、边缘计算等信息技术和智能技术，汇集各方面资源，为规划建设、生产运行、经营管理、综合服务、新业务新模式发展、企业生态环境构建等各方面，提供充足有效的信息和数据支撑。泛在物联网的开放性带来信息充分对称的同时，也意味着风险的增加，对此国家电网公司制定了全场景安全防护的原则，实现可信互联，安全互动、智能防御。图 5 描述了泛在电力物联网全场景安全防护体系。

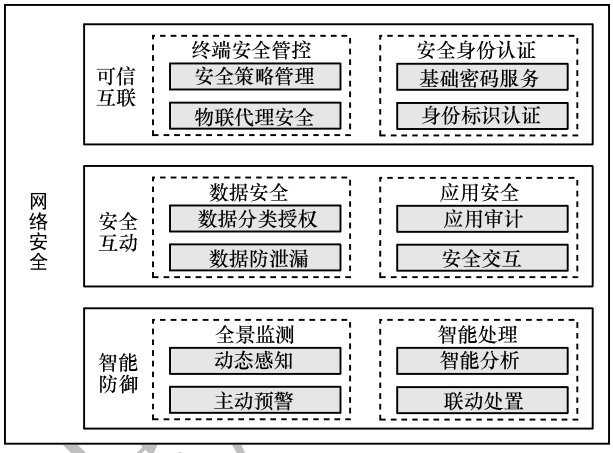


图 5 泛在电力物联网全场景安全防护体系

5.2 密码技术应用设计

对泛在电力互联网中的所有互联互动，包括“物—物”“人—物”“人—人”实现安全管控，即基本做到了整个网络的安全防护。可信互联通过终端安全管控，和安全身份认证来实现联通双方的合法性，安全互动通过数据分类授权，对不同数据进行不同级别的保护，防止数据在互动中的泄露。对泛在电

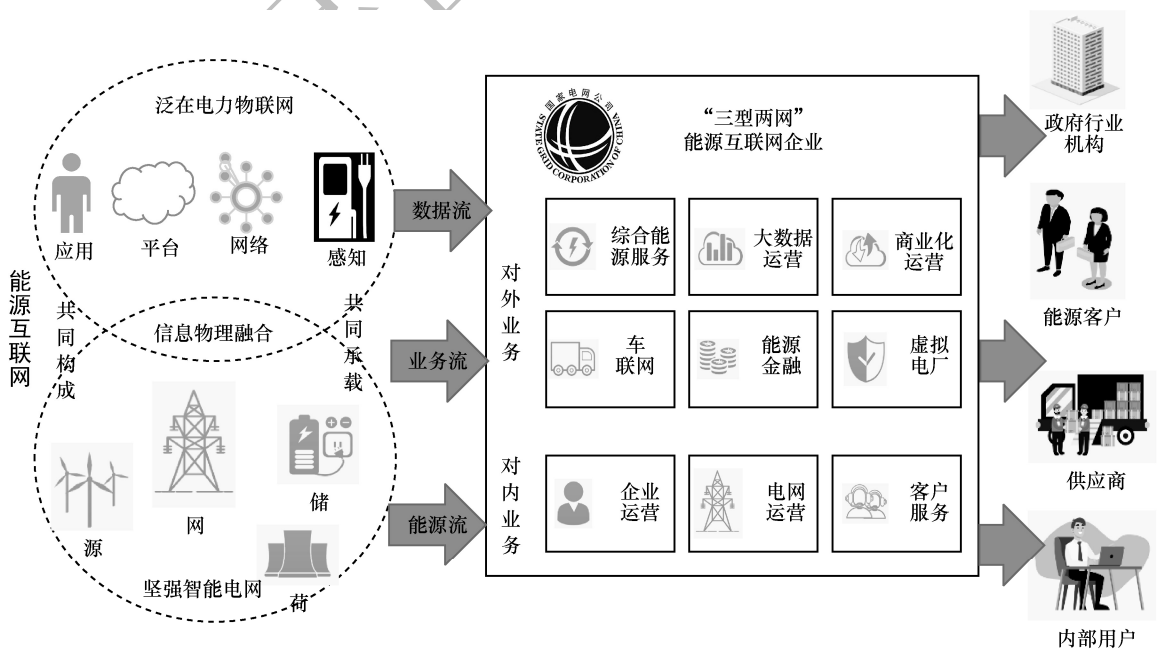


图 4 泛在电力物联网结构

力物联网中的各种应用进行审计、认证、建立安全通道保证能源互联网和应用的安全。密码技术在泛在电力物联网安全防护中起到至关重要的作用。按照泛在电力物联网 4 个层次分析常用密码技术在安全防护中的设计。

（1）感知层安全，泛在电力物联网通过终端感知层收集状态和数据，并传送至网络层，基础密码服务要为各终端提供身份认证的支持，如使用终端标识码、基于 IBC 体系的实现身份标识认证。

（2）网络层安全，可通过使用专用密码认证网关、安全通信协议实现网络中的数据安全。

（3）平台层安全，主要是平台数据的安全，主要是将密码技术运用在云存储和云计算中来保证全业务数据中心数据的安全性。

（4）应用层安全，通过对接入泛在物联网的应用严格审计，对应用使用密码技术进行强身份认证，确保应用安全和互动安全。

6 密码新技术在能源互联网中的展望

由于能源互联网信息和结构的复杂性以及新信息技术的融入，常用的密码技术在满足其安全需求上略显不足，需要研发新的密码技术来适应电力系统的新需求。

（1）建立能源互联网密码保障体系。设计研发专门适合泛在电力物联网的密码算法及应用方案，研发能源互联网中的关键密码设备、设计新的或改进原有的密码应用标准体系。

(2)在云计算和云存储的环境下进行设计和研发。泛在电力物联网中大数据隐私保护技术研发，确保电力系统的生产数据的机密性和电力用户数据的隐私性得以保证。

（3）进行适合泛在电力物联网的轻量级密码应用体系研发。包括轻量级密钥管理系统、轻量级加密认证技术和各种轻量级密码应用服务。

（4）建立泛在电力物联网的统一认证服务。包括泛在电力物联网中所有人、设备、应用的认证，以保证可信互联，安全互动。

6.1 量子密码

量子时代理论上可以实现无条件安全。量子密码是量子时代最为稳妥的密码体制，基于量子力学原理，由量子不可克隆定理、不确定性原理等来保证其安全性。为了满足电力新业务的发展，更好地实现网络安全防护，电力行业在量子保密通信投入了人力财力，进行了初步的研发，开展了示范工程工作，建设完成了电力量子域域网和电力量子广域网。电力系统中的量子密码应用和理论研究方面的部分成果有：参考文献[20]通过分析智能电网信息安全威胁的基础上，展望了量子密码在智能电网中的应用前景；参考文献[21]梳理了电力系统中量子保密通信发展现状，重点解决存在的关键问题，包括结合量子秘钥的电力专用对称加密算法研究、面向国网一体化云平台的量子密钥云服务等；参考文献[22]提出了将量子密钥分配网络与电网 SSL VPN 相融合的方案，利用量子密钥协商技术实现密钥安全分配的问题，使通信双方间能共享无条件安全的密钥。

随着计算机计算能力的不断增强，尤其是量子计算机概念的提出，对于公钥密码 RSA、ECC 等密码体制形成了严重的威胁，这些体制所基于的大整数分解、离散对数等问题的困难性，在量子计算下已不再是一个难题。后量子时代的密码研究成为密码学领域的一个重要方向。其中基于格的密码体制，被认为是目前唯一一种可以抗量子攻击的、基于数学上计算困难问题的密码体制。基于格的密码体制基于格上的困难问题 SVP、CVP 等，被证明是可以抵御量子计算攻击的。1996 年，Ajtai 提出基于格上困难问题的构建密码方案的可能性之后，二十多年来不断有基于格问题构造的方案出现[18]，包括散列函数、公钥加密方案、数字签名方案。基于格的密码还可以构造全同态加密方案[19]，为后量子时代云计算提供同态加密服务奠定基础。目前基于格的密码体制尚处在理论研究阶段，没有达到实际投入使用的要求，所以在电力系统中还未有应用。

6.2 区块链技术

国际可再生能源署（IRENA）发布可再生能源领域的创新报告，介绍了区块链在电力领域的应用。基于区块链的智能合约可以提供推动实现电网的现代化，增加使用可再生能源，特别是难以吸纳的间歇性来源，同时降低成本，加快交易流程。具体而言，区块链在电力行业的主要用途主要包括：点对点交易、电网管理和系统运行、通过混合资产为可再生能源融资、可再生能源证书管理以及电动交通等[23]。区块链技术的去中心化、开放、智能和共享与国家电网公司“三型两网”发展能源互联网的战略高度契合，可以有效地解决泛在电力物联网建设过程中面临的数据融

通、设备安全、个人隐私和多主体协同等问题，在引领和支撑泛在电力物联网建设方面具有不可替代的重要作用。

随着电子商务及电力金融业务规模的不断扩大，产业链上下游的合同签订履行、商品排产销售、金融信贷等业务面临的可信风险越来越大。为了提升电力商务及电力金融业务的安全性，国家电网公司紧密结合泛在电力物联网、电子商务、金融科技等业务发展需求，积极开展电力区块链技术业务场景研究，构建了可信区块链平台，提供司法级可信认证服务。同时，结合电力业务的行业特殊性，国家电网公司持续推进电力区块链技术实用化研究，并获批了工业和信息化部区块链重点实验室电力应用实验基地，形成成果已在供应链金融、企业信用评价、光伏并网签约、电子发票等业务领域实现具体应用，更好地发挥了区块链技术在泛在电力物联网建设中的基础性和引领性作用[24]。

7 结束语

能源互联网信息化程度进展飞快，但是却面临着安全防护与信息化发展不对等的现状，亟需构建安全可靠的防护体系。密码法的颁布实施使得密码技术在保护网络与信息安全中的作用得到进一步加强，构建以密码技术为支撑的安全防护体系将对能源互联网的发展提供强有力的安全保障。在坚强智能电网安全性建设中逐步设计合理的轻量级密码技术支持方案，采取增加 IBC 公钥密码体系来保障用户和电网互动的安全性；在泛在电力物联网安全性建设中，按照泛在电力物联网感知层、平台层、网络层和应用层 4 个层次构建密码防护体系。安全防护体系的建设是能源互联网安全稳定运行的基础，无论是坚强智能电网，还是国家电网公司提出的泛在电力物联网，以密码技术为基础的加密密码、数字签名、散列技术、PKI 体系和 IBC 体系都已经在电力系统的身份认证、数据安全、隐私保护和安全隔离等方面发挥了重大作用。随着泛在电力物联网建设的全面展开，可以预见，常用密码技术和以量子密码、区块链等为代表的密码新技术，将在能源互联网中发挥更大的作用。

参考文献：

[1] 陈梅. 商用密码技术在电力行业中的应用研究[J]. 信息安全与通信保密, 2018(5): 50-56.

[2] DIFFIE W, HELLMAN M. New directions in cryptography[J]. IEEE Transactions on Information Theory, 1976, 22(6): 644-654.

[3] SHAMIR A. Identity-based cryptosystems and signature schemes[J]. Workshop on the Theory and Application of Cryptographic Techniques, 1984(196): 47-53.

[4] 周传玉, 王吉伟, 李明. 物联网中标识密码应用研究[J]. 信息安全研究, 2017, 3(11): 1040-1044.

[5] 尹璐. 基于格的非托管 IBC 理论与技术研究[D]. 长沙: 国防科学技术大学, 2016.

[6] 张志. 基于标识的密码体制研究[D]. 武汉: 华中科技大学, 2009.

[7] A1-RIYAMI S S, PATERSON K. Ct certificateless public key cryptography[C]//Advances in Asiacrypt'03. LNCS2894. Berlin：Springer-Verlag, 2003: 452-473.

[8] A1-RIYAMI S S, PATERSON K. Certificateless public key cryptography[C]//Asiacrypt' 03, LNCS2332. Berlin: Springer-Verlag, 2003: 452-473.

[9] A1-RIYAMI S S, PATERSON K. CBE from CL-PKE: a generic construction and efficient schemes[C]//PKC'05, LNCS3386. Berlin: Springer-Verlag, 2005: 398-415.

[10] CHENG Z H, COMLEY R, VASIU L. Remove key escrow from the identity-based encryption system[J]. IFIP International Federation for Information Processing, 2004, 155: 37-50.

[11] CHENG Z H, COMLEY R. Efficient certificateless public key encryption[R]. Technical Cryptology ePrint Archive, 2005.

[12] 电力二次系统安全防护总体技术介绍[Z]. 2017.

[13] 国家电力监管委员会. 电力二次系统安全防护规定: [2005] 第 5 号令[EB]. 2005.

[14] 王文, 鲁玉华, 陶静娜, 等. 电力调度证书系统的特点及应用[J]. 电网技术, 2007(12): 23-27.

[15] 曹军威, 万宇鑫, 涂国煜, 等. 智能电网信息系统体系结构研究[J]. 计算机学报, 2013, 36(1): 143-167.

[16] 淮晓烨. 基于无证书公钥密码、RBAC 的智能配电网访问控制方案[D]. 成都: 西南交通大学, 2012.

[17] 王萌希, 侯春风, 商利平. IBC 在物联网中的应用研究[J]. 数据通信, 2012(6): 1-4.

[18] AJTAI M. Generating hard instances of lattice problems[C]//The 28th annual ACM symposium on Theory of computing. New York: ACM, 1996: 99- 108.

[19] GENTRY C. A fully homomorphic encryption scheme[D]. Stanford: Stanford University, 2009.

[20] 佟为明, 卢雷, 金显吉. 量子密码在智能电网信息安全中的应用[C]//中国电工技术学会电器智能化系统及应用专业委员会学术年会, 2013.

[21] 陈智雨, 郝悍勇, 王栋, 等. 电力量子保密通信实用化技术研究进展与展望[J]. 电力信息与通信技术, 2018, 16(4): 15-23.

[22] 刘东, 王双, 周静, 等. 量子密钥在电网 SSLVPN 中的应用[J]. 电网技术, 2014, 38(2): 544-548.

[23] 何永远, 庞进. 区块链技术在电力行业的应用展望[J]. 电力信息与通信技术, 2018.

[24] 朱怡. 区块链重点实验室落地国家电网[N]. 中国电力报, 2019-04-01(001).

人民邮电出版社

面向 6G 的高阶 APSK 软解调及简化

张长青
（中国移动通信集团湖南有限公司岳阳分公司，湖南 岳阳 414000）

摘　要： 5G 和 6G 的研究工作者，都支持将卫星通信融入移动通信系统，但融入 6G 的可能性更大。面向 6G 的卫星通信系统将是面向普通公众的普通应用，数据吞吐量将会很大，数据传输品质也会低于传统的专用应用，所以基带调制解调方式必须采用高阶 APSK。通过星座理论较为详细地分析了 PSK 和 APSK 的基础技术，分析了解调技术中的简化问题。通过仿真和格雷码映射，对高阶 APSK 调制解调技术中的简化进行了深入浅出的分析，对工程技术人员了解高阶 APSK 具有一定的帮助。

关键词： 相移键控；幅度相移键控；格雷码；软解调简化

1　引言

3GPP 确定 5G 系统可以融合物联网、车联网、工业互联网和城市市政功能服务网等网络，支持的基带调制解调方式是传统的 π/2-BPSK、QPSK、16QAM、64QAM 和 256QAM 等成熟技术[1]，5G 系统覆盖区域仍然只能是面向人类活动密集的陆地区域，虽然有专家开始探索将卫星通信融入 5G，初步思路已经包括体系架构、空中接口和协议优化等项目[2]，但在 3GPP 的 5G 规划中并没有明确表述。在 6G 移动通信的初步规划的课题中，有学者开始考虑将卫星通信网络直接融入其中，实现陆地与太空通信网络的大融合，使移动通信真正成为陆地和海上无死角的全球通信系统，真正实现移动通信的“全球通”愿景[3]。显然，将卫星通信系统融入到移动蜂窝系统中，正在成为未来移动通信系统的重要研究课题。

卫星通信系统中的太空卫星与地面终端的距离一般在几千到上万 km，大部分是真空太空，距离地面约 50 km 厚的是大气层，大气层以上厚约 1000 km 的是电离层。不仅外太空与电离层、电离层与大气层之间是一层突变介质层。在约 1 000 km 厚的电离层中和约 50 km 厚的大气层中，虽然它们都为同种介质，但介质分布的密度随着高度的不同而不同，介质分布并非线性。另外，电离层和大气层是一种易受到扰动的介质层，加之卫星远在太空，极大地限制了卫星的收发功率。所以，在卫星与地面终端相互通信时，承载信息的传输信道实际上是一种典型的且十分复杂的非线性介质，收发设备功率受到极大限制，因而很少采用只适应陆地表层空域线性传输介质的基带调制方式，大多使用适应非线性信道的相移键控（PSK）方式[4]。

传统的卫星通信系统是一种特殊的专用系统，实际工作中的通信容量和数据吞吐量非常有限，但对通信信息的可靠性要求极高，因此采用调制效率较低、调制性能较高的 PSK 方式，就完全适应系统通信的业务需求（如每个基带调制符号仅包括 2 bit 信息的 QPSK）。若将卫星通信系统与现代蜂窝系统结合，形成泛在的、真正的全球通系统，从传统的特殊应用领域延伸到寻常百姓家的商业应用场景，卫星的通信容量和数据吞吐量将会快速增长，而普通商业信息传输的可靠性要求会降低，传统的基带调制方式 QPSK 失去了应用价值，采用更高阶 PSK 虽然可以提高数据吞吐量，但传输品质较差，同样不能适应面向 6G 进入通用商业领域的卫星通信系统的应用要求，唯有采用调制性能和吞吐量同样较高的幅度相移键控（APSK）方式才能满足要求。

APSK 与 QAM 一样，是一种幅度相位共同调制的二维调制解调技术，但 QAM 的相移调制仅固定在 4 个相角中，本质上调制符号仍然是包络线型恒定、调制功率效率较低的幅度调制信号，QAM 是将两个相互正交的 ASK 相结合的方式[5]。APSK 以相位调制为主、幅度调制为辅，相位和幅度的调制阶数可以同时调整。由 APSK 调制符号组成的星座是分布在以幅度为半径分层的多层圆圈上，调制信号的幅度起伏相对较小，且仍可以获得较高的频谱效率。更重要地，

人民邮电出版社

由于 APSK 的幅度和相位的调制阶数可以同时改变，系统根据实际应用需要，适当调整幅度和相位调制阶数的比例，使其可以获得最佳调制效果，而不是如 QAM 只能选择方形星座的调制阶数才能获得，从而限制了调制阶数的任意选择。在调制阶数的选择方面，APSK 较之 QAM 具有更好的灵活性。

2 MPSK 调制与软解调[6]

2.1 PSK 调制原理

APSK 方式实际上是 PSK 的通用式，PSK 则相当于 APSK 的特殊式。

根据通信理论并参考文献[5]，M 进制相移键控（MPSK）的调制信号，是用 M 个相位不同的载波分别代表 M 个调制符号。载波相位有 M 种取值，即 $\varphi_n(t)=n2\pi/M$，n=1,2,⋯,M，调制阶数为 M、调制效率（每个调制符号包含的二进制比特数）为 $L=\sqrt{M}$ 的 MPSK 调制符号可以表示为：

$$S(t)=R\cos\left[\omega_c t+\phi_n(t)\right]=R\cos\left[\omega_c t+n2\pi/M\right]=I(t)\cos\omega_c t+Q(t)\sin\omega_c t \quad (1)$$

其中，R 是频率为 ω_c 的调制载波的幅值，$\varphi_n\in\{\pi/M, 3\pi/M,5\pi/M,\cdots,(2M-1)\pi/M\}$，同相分量 $I(t)=R\cos\varphi_n=R\cos(n2\pi/M)$，正交分量 $Q(t)=R\sin\varphi_n=R\sin(n2\pi/M)$，$\varphi_n=\mathrm{tg}^{-1}[I(t)/Q(t)]$，n=1,2,⋯,$M$。

若载波频率 ω_c 是基带信号速率的整数倍，则式(1)可以表示为：

$$S(t)=\sum Rg(t-n\mathrm{T}_s)\cos\left[\omega_c t+\phi_n(t)\right]=R\{\cos\omega_c t\sum g(t-n\mathrm{T}_s)\cos[\phi_n(t)]-\sin\omega_c t\sum g(t-n\mathrm{T}_s)\sin[\phi_n(t)]\} \quad (2)$$

其中，$g(t)$是高度为 1、宽度为 T_s 的矩形脉冲，即成型滤波函数，OFDM 采用的就是这种滤波器。

式(2)表明，MPSK 调制符号可以等效为两个正交载波的 MASK 调制符号之和，所以 MPSK 调制符号的带宽和 MASK 相同，说明 MPSK 系统是一种高效率的信息传输方式。但当 M 值较大时，相邻载波间的相位差会随之减小，从而使得调制符号的抗噪性能变差，实际应用中限制了 M 的取值，也限制了 PSK 的调制效率。

当载波频率远大于信号带宽时，传输信道可以等效为一个窄带高斯信道，经过窄带高斯信道传输后的高斯噪声可表示为：

$$n(t)=n_I(t)\cos(\omega_c t)+n_Q(t)\sin(\omega_c t) \quad (3)$$

接收端信号可以表示为：

$$R(t)=S(t)+n(t)=B_I(t)\cos(\omega_c t)+B_Q(t)\sin(\omega_c t) \quad (4)$$

其中，$B_I(t)=n_I(t)+I(t)=n_I(t)+R\cos\varphi_n$ 和 $B_Q(t)=n_Q(t)+Q(t)=n_Q(t)+R\sin\varphi_n$ 与给定的 φ_n 相比，是相互独立的随机变量。高斯噪声对 MPSK 符号的幅度和相位同时产生影响，从而增加了接收信号的误码率。

2.2 PSK 软解调及简化

若仅分析 MPSK 调制星座图，则式（2）可以去掉时间因子，用复数相移表述发送端的调制符号，即：

$$S=R\cdot\exp[\mathrm{j}\cdot(n\cdot2\pi/M+\theta)],\ n=0,1,2,\cdots,M \quad (5)$$

其中，S 是圆周上的星座集，即 MPSK 的所有调制符号；R 是圆周半径；M 是圆周上的星座点数，也就是 MPSK 的调制阶数，或调制符号数；θ 是星座点的初始位置（初相）。

若取 $\theta=\pi/M$，则式(5)可简化为：

$$S=R\cdot\exp[\mathrm{j}\cdot(n\cdot\pi/M)],\ \mathrm{n}=1,3,5,\cdots,2M-1 \quad (6)$$

发送调制符号 S 经过高斯信道传输后，调制符号的幅度和相位同时受到干扰，但因系统只对相位调制，MPSK 接收符号只能随机分布在原始星座坐标的周围，要解调这些接收端的调制符号，传统的软解调方法是用 LLR 算法求出每个接收符号中的每个比特值的对数似然比，判决接收 MPSK 符号属于哪个星点的概率可以表示为：

$$P_i=\frac{1}{\sqrt{2\pi\sigma^2}}\exp\{-|R-S_i|^2/(2\sigma^2)\} \quad (7)$$

其中，i=0,1,⋯,M 为 MPSK 星座中的星点数，σ 为高斯信道标准方差，S_i 为发送端 MPSK 符号在星座图中的标准位置坐标，R 为接收端 MPSK 符号在星座图中的随机位置坐标。基于概率 P 的映射比特 b 对应的对数似然比为：

$$L(b)=\ln\frac{P(b=0|R)}{P(b=1|R)} \quad (8)$$

对于高斯白噪声信道，如果每个码字是等概率发射，将式(7)代入式(8)，并取 $M_i=|R-S_i|$，则有：

$$L(b)=\ln\left\langle\frac{\sum_{S_i\in S_0}\exp\{-|R-S_i|^2/(2\sigma^2)\}}{\sum_{S_i\in S_1}\exp\{-|R-S_i|^2/(2\sigma^2)\}}\right\rangle=\ln\left\langle\frac{\sum_{S_i\in S_0}\exp\{-M_i^2/(2\sigma^2)\}}{\sum_{S_i\in S_1}\exp\{-M_i^2/(2\sigma^2)\}}\right\rangle \quad (9)$$

人民邮电出版社

其中，S_0 表示发送端星座图中在 b 位置所有取值为 0 的点的集合，S_1 表示发送端星座图中在 b 位置所有取值为 1 的点的集合。按照格雷码取值，S 很有规律，非常适合程序处理，所以系统采用 PSK 调制时，一般都会对 PSK 星座采用格雷编码与之对应。基本流程是：先根据调制符号的调制比率，将传输数据的自然二进制比特流按调制比特数转换成格雷码对应的二进制比特流，再用二进制格雷码映射给 PSK 符号，完成 PSK 调制过程。

从式（7）和式（9）中可以看出，每计算一个比特的对数似然比 LLR，都需要进行平方、指数和对数等运算，说明 LLR 算法具有较高的运算复杂度和较大的资源开销。由于采用硬件实现指数、对数算法复杂度极高，所以 LLR 算法一般不适合用可编程门阵列 FPGA 固件实现。最大值取值算法能够有效地避免计算每比特对数似然值中的指数和对数运算，根据式 $\log(M/N)=\log M-\log N$ 和 $\log\sum_i r_i \approx \max(r_i)$，式（9）可以简化为：

$$L(b)=\ln\left\{\sum_{S_i\in S_0}\exp\left[-M_i^2/(2\sigma^2)\right]\right\}-\ln\left\{\sum_{S_i\in S_1}\exp\left[-M_i^2/(2\sigma^2)\right]\right\}\approx \max_{S_i\in S_0}\left[-M_i^2/(2\sigma^2)\right]-\max_{S_i\in S_1}\left[-M_i^2/(2\sigma^2)\right] \quad (10)$$

其中，式（10）将式（9）中原有的对 M 个数据求自然指数、累加、相除以及求自然对数的复杂运算，简化成对 $M/2$ 个数据求最大值，后求减法的简单运算。式（10）不仅降低了算法的难度，还减少了算法类型。采用式（10）求解软解调，理论上比式（9）更快，占用系统的资源也更少。

2.3 16PSK 调制软解调分析

以 16PSK 为例，每组由 4 比特数据组成的格雷码二进制比特流，映射的 16PSK 调制符号在发送端星座图上的位置，可以用表 1 所示的复数表示，即每个 16PSK 调制符号为：

$S_i=R\cdot exp(-j n\pi/16)$，$i$=1,2,3,⋯,16，$n$=1,3,5,⋯,31（12）

根据式(9)、式(10)和表 1 中格雷码对应的二进制位数，接收端符号对应的比特值的对数似然比分别为：

$$L(b_4)=\ln\left[\frac{P_1+P_2+P_3+P_4+P_5+P_6+P_7+P_8}{P_9+P_{10}+P_{11}+P_{12}+P_{13}+P_{14}+P_{15}+P_{16}}\right]=\max[m_1,m_2,m_3,m_4,m_5,m_6,m_7,m_8]-\max[m_9,m_{10},m_{11},m_{12},m_{13},m_{14},m_{15},m_{16}]$$

$$L(b_3)=\ln\left[\frac{P_1+P_2+P_3+P_4+P_{13}+P_{14}+P_{15}+P_{16}}{P_5+P_6+P_7+P_8+P_9+P_{10}+P_{11}+P_{12}}\right]=\max[m_1,m_2,m_3,m_4,m_{13},m_{14},m_{15},m_{16}]-\max[m_5,m_6,m_7,m_8,m_9,m_{10},m_{11},m_{12}]$$

$$L(b_2)=\ln\left[\frac{P_1+P_2+P_7+P_8+P_9+P_{10}+P_{15}+P_{16}}{P_3+P_4+P_5+P_6+P_{11}+P_{12}+P_{13}+P_{14}}\right]=\max[m_1,m_2,m_7,m_8,m_9,m_{10},m_{15},m_{16}]-\max[m_3,m_4,m_5,m_6,m_{11},m_{12},m_{13},m_{14}]$$

$$L(b_1)=\ln\left[\frac{P_1+P_4+P_5+P_8+P_9+P_{12}+P_{13}+P_{16}}{P_2+P_3+P_6+P_7+P_{10}+P_{11}+P_{14}+P_{15}}\right]=$$

表 1　基于格雷码的 16PSK 星座坐标对应值

十进制数	二进制数	格雷码 $B_4b_3b_2b_1$	16PSK 符号	半径	相移角(复数表示)
1	0000	0000	S_0	R	exp(−jπ/16)
2	0001	0001	S_1		exp(−j3π/16)
3	0010	0011	S_2		exp(−j5π/16)
4	0011	0010	S_3		exp(−j7π/16)
5	0100	0110	S_4		exp(−j9π/16)
6	0101	0111	S_5		exp(−j11π/16)
7	0110	0101	S_6		exp(−j13π/16)
8	0111	0100	S_7		exp(−j15π/16)
9	1000	1100	S_8		exp(−j17π/16)
10	1001	1101	S_8		exp(−j19π/16)
11	1010	1111	S_{10}		exp(−j21π/16)
12	1011	1110	S_{11}		exp(−j23π/16)
13	1100	1010	S_{12}		exp(−j25π/16)
14	1101	1011	S_{13}		exp(−j27π/16)
15	1110	1001	S_{14}		exp(−j29π/16)
16	1111	1000	S_{15}		exp(−j31π/16)

人民邮电出版社

$$\max[m_1,m_4,m_5,m_8,m_9,m_{12},m_{13},m_{16}]$$
$$-\max[m_2,m_3,m_6,m_7,m_{10},m_{11},m_{14},m_{15}] \quad (12)$$

根据式（11）和式（12）及表 1 数据仿真得到的 16PSK 发送端、接收端星座图以及简化软解调后的误码率曲线如图 1 所示。可以看出，发射端星座上表示的格雷码、符号码是按照逆时针方向、等相移间隔排列的，显示的信息内容与表 1 所示从上至下排列的内容是一致的。接收端星座表述了接收信号分布在原星座点的周围，说明传输信道的高斯噪声对信号的幅值和相移角都产生了随机干扰。误码率曲线表明 16PSK 简化软解调方式的性能较好，从接收端星座图中的随机星座点分布也可以出看出，16PSK 相邻接收端星点之间的区分边界较为明显。

3 MAPSK 调制与软解调[7-8]

3.1 APSK 调制

APSK 是 PSK 的扩展，不同的是，APSK 在发送端中采用不同的半径 R 对应不同的相移组进行调制，而接收端的解调方式与 PSK 一样，可直接用式(5)拓展 APSK 发送端的映射星座数学表达式。

设星座图由 K 个不同半径的同心圆组成，每个圆圈上分布数量不同的等间隔 PSK 信号点，每个星座点代表 1 个 APSK 调制符号，对应的星座星点复数信号集的表达式为：

$$S_k = R_k \cdot \exp[\mathrm{j}\cdot(n_k \cdot 2\pi / N_k + \theta_k)] \quad k=1,2,\cdots,K$$
$$n_k=0,1,2,\cdots,N_k \quad (13)$$

其中，S_k 是第 k 个圆周上的所有星点，R_k 为第 k 个圆周的半径，N_k 为第 k 个圆周上的星点数，n_k 为第 k 个圆周上的一个星点，θ_k 为第 k 个圆周上星点的相位偏差，可决定第 k 个圆周上第 1 个星点的初始位置，如 θ_k=0 时第 k 圆周上第 1 个星点位于 $2\pi/N_k$ 位置，后面星点位置等角度排列在圆周上。

若取 $\theta=\pi/N_k$，则式（13）可简化为：

$$S_k = R_k \cdot \exp[\mathrm{j}\cdot(n_k \cdot \pi / N_k)] \quad k=1,2,\cdots,K$$
$$n_k=1,3\ 5,\cdots,2N_k\text{-}1 \quad (14)$$

为了充分利用整个星座图上的信号空间，需要合理规划每个圆周上的星点数，基本条件是各圆周上的星点数排列满足条件 $N_k>N_k+1$，即外圆星点数要大于内圆星点数。为了规范 APSK 符号表述方式，定义 APSK 符号可以表示为 $N_1+N_2+\cdots+N_K$-APSK，且 $M=N_1+N_2+\cdots+N_K$，M 是星座图中星点的总数，即调制阶数，如 16APSK=12+4-APSK，32APSK=16+ 12+ 4-APSK。

3.2 APSK 软解调

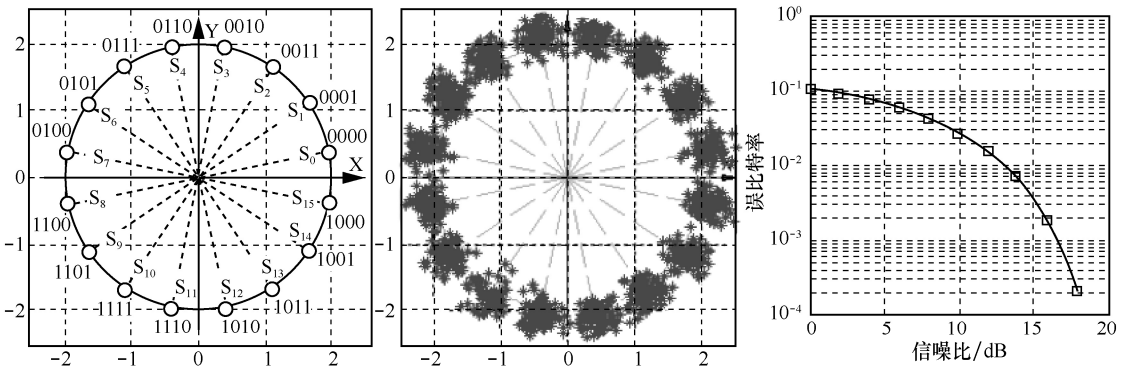
根据式（7），每个接收的 MAPSK 符号属于对应星座的概率，可以表示为：

$$P_i = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\{-|R-S_i|^2/(2\sigma^2)\} \quad i=0,1,\cdots,M \quad (15)$$

其中，R 是接收端的所有 MAPSK 符号中比特值，S 是分布在星座图中各个圆周上的星座坐标对应的格雷编码二进制序列。若取 $M_i=|R-S_i|$，根据式(9)，经过高斯信道传输后，基于概率 P 的映射比特 b 对应的对数似然比为：

$$L(b) = \ln\left\langle \frac{\sum_{S_i\in S_0}\exp\{-M_i^2/(2\sigma^2)\}}{\sum_{S_i\in S_1}\exp\{-M_i^2/(2\sigma^2)\}} \right\rangle \quad (16)$$

根据式（10）、式（16）可简化为：



（a）发送端16PSK星座图　（b）接收端16PSK星座图　（c）简解调16PSK误码率曲线

图 1　基于格雷码的 16PSK 星座与误码率

$$L(b)\approx \max_{S_i\in S_0}\left[-M_i^2/(2\sigma^2)\right]-\max_{S_i\in S_1}\left[-M_i^2/(2\sigma^2)\right] \quad (17)$$

3.3 32APSK 调制软解调分析

以 32APSK 为例，按照 16+12+4-APSK 格式设计 APSK 星座，则由 5 比特数据组成的格雷码二进制序列、映射 32APSK 调制符号在发送端星座图上的位置，可以用表 2 所示的复数表示，即每个 32APSK 调制符号为：

$$S_q=R_k\cdot \exp(-\mathrm{j}\, n_k\pi/16)\ q=1,2,\cdots,32;\ \mathrm{k}=1,2,3;$$
$$N_k=16,12,4;\ n_k=1,3\ 5,\cdots,2N_k-1 \quad (18)$$

根据式（17）和表 2 中格雷码对应的二进制位数，接收端符号对应的比特值的对数似然比分别为：

$$L(b_5)=\max[m_1,m_2,m_3,m_4,m_5,m_6,m_7,m_8,m_9,m_{10},m_{11},m_{12},m_{13},m_{14},m_{15},m_{16}]-\max[m_{17},m_{18},m_{19},m_{20},m_{21},m_{22},m_{23},m_{24},m_{25},m_{26},m_{27},m_{28},m_{29},m_{30},m_{31},m_{32}]$$

$$L(b_4)=\max[m_1,m_2,m_3,m_4,m_5,m_6,m_7,m_8,m_{17},m_{18},m_{19},m_{20},m_{21},m_{22},m_{23},m_{24}]-\max[m_9,m_{10},m_{11},m_{12},m_{13},m_{14},m_{15},m_{16},m_{25},m_{26},m_{27},m_{28},m_{29},m_{30},m_{31},m_{32}]$$

$$L(b_3)=\max[m_1,m_2,m_3,m_4,m_{13},m_{14},m_{15},m_{16},m_{17},m_{18},m_{19},m_{20},m_{29},m_{30},m_{31},m_{32}]-\max[m_5,m_6,m_7,m_8,m_9,m_{10},m_{11},m_{12},m_{21},m_{22},m_{23},m_{24},m_{25},m_{26},m_{27},m_{28}] \quad (19)$$

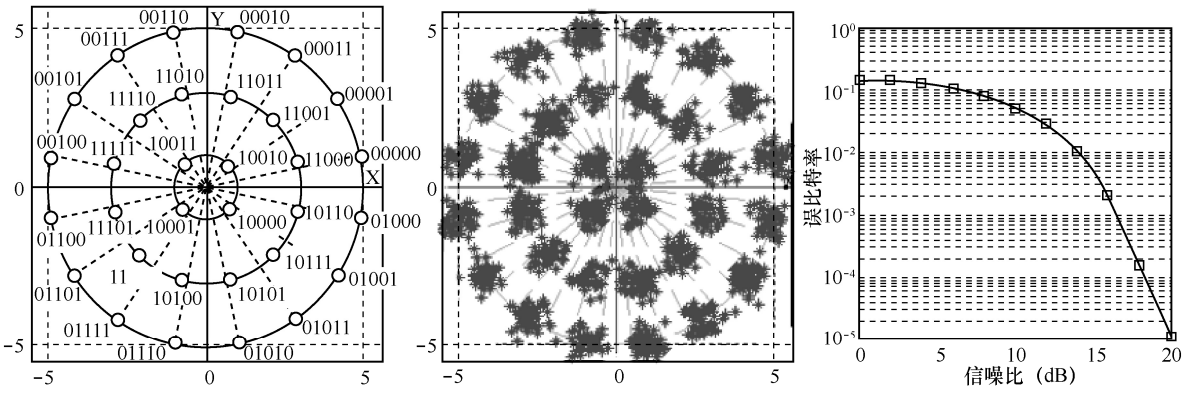
$$L(b_2)=\max[m_1,m_2,m_7,m_8,m_9,m_{10},m_{15},m_{16},m_{17},m_{18},m_{23},m_{24},m_{25},m_{26},m_{31},m_{32}]-\max[m_3,m_4,m_5,m_6,m_{11},m_{12},m_{13},m_{14},m_{19},m_{20},m_{21},m_{22},m_{27},m_{28},m_{29},m_{30}]$$

$$L(b_1)=\max[m_1,m_4,m_5,m_8,m_9,m_{12},m_{13},m_{16},m_{17},m_{20},m_{21},m_{24},m_{25},m_{28},m_{29},m_{32}]-\max[m_2,m_3,m_6,m_7,m_{10},m_{11},m_{14},m_{15},m_{18},m_{19},m_{22},m_{23},m_{26},m_{27},m_{30},m_{31}]$$

根据式(18)和式(19)及表 2 数据仿真得到的 32APSK 发送端、接收端星座图以及简化软解调后的误码率曲线如图 2 所示。可以看出，发射端星座上 3 个圆周表示的格雷码、符号码是按照逆时针方向、等相

表 2 基于格雷码的 32APSK（16+12+4-APSK）星座坐标对应值

十进制数	二进制数	格雷码 $B_5b_4b_3b_2b_1$	半径	相移角 (复数表示)	十进制数	二进制数	格雷码 $B_5b_4b_3b_2b_1$	半径	相移角 (复数表示)
1	00000	00000	R_1	exp(-jπ/16)	17	10000	11000	R_2	exp(−jπ/12)
2	00001	00001		exp(-j3π/16)	18	10001	11001		exp(−j3π/12)
3	00010	00011		exp(-j5π/16)	19	10010	11011		exp(−j5π/12)
4	00011	00010		exp(-j7π/16)	20	10011	11010		exp(−j7π/12)
5	00100	00110		exp(-j9π/16)	21	10100	11110		exp(−j9π/12)
6	00101	00111		exp(-j11π/16)	22	10101	11111		exp(−j11π/12)
7	00110	00101		exp(-j13π/16)	23	10110	11101		exp(−j13π/12)
8	00111	00100		exp(-j15π/16)	24	10111	11100		exp(−j15π/12)
9	01000	01100		exp(-j17π/16)	25	11000	10100		exp(−j17π/12)
10	01001	01101		exp(-j19π/16)	26	11001	10101		exp(−j19π/12)
11	01010	01111		exp(-j21π/16)	27	11010	10111		exp(−j21π/12)
12	01011	01110		exp(-j23π/16)	28	11011	10110		exp(−j23π/12)
13	01100	01010		exp(-j25π/16)	29	11100	10010	R_3	exp(−jπ/4)
14	01101	01011		exp(-j27π/16)	30	11101	10011		exp(−j3π/4)
15	01110	01001		exp(-j29π/16)	31	11110	10001		exp(−j5π/4
16	01111	01000		exp(-j31π/16)	32	11111	10000		exp(−j7π/4



(a) 发送端32APSK星座图　(b) 接收端32APSK星座图　(c) 硬解调32APSK误码率曲线

图 2 基于格雷码的 32APSK 星座与误码率

移间隔排列的，3 个圆周从外向内显示的信息内容与表 2 所示从上至下排列的内容是一致的。接收端星座表述了接收信号分布在原星座点的周围，说明传输信道的高斯噪声对信号的幅值和相移角都产生随机干扰。误码率曲线表明 32APSK 简化软解调方式的性能较好，从接收端星座图中的随机星座点分布可以看出，32APSK 不同圆周间的接收端星点和圆周上相邻接收端星点之间的区分边界非常明显。

将图 2 与图 1 比较，虽然 32APSK 的阶数是 16PSK 的阶数一倍，从误码率曲线来看，32APSK 的误码率曲线与 16PSK 相差不大；从接收端星座图来看，32APSK 接收端星座图中的星点分辨率与 16PSK 几乎没有区别；从发送端星座图来看，32APSK 发送端星座图中的星点分布密度明显高于 16PSK，说明 APSK 中充分利用了半径 R 的空间。

4 高阶 APSK 调制解调仿真

4.1 APSK 仿真建模

为了使仿真能够逼近现实场景，使仿真具有较高的实用参考价值，专门设计了如图 3 所示的包括 MAPSK 调制解调过程的流程建模，其中的信道编译码器采用的是基于 5G 的 LDPC，校验矩阵是 6×9 阶正交稀疏矩阵；多址寻址采用的是面向 5G 的滤波器组 OFDM，滤波器组是多相滤波器，由于 LDPC 编码的校验矩阵 H 与 MAPSK 调制解调器、多址技术 OFDM 的子载波映射和 IFFT 等都是独立的处理系统，矩阵 H 的维度数、基带调制的阶数、傅里叶变换中的采样数等没有交集，互不影响。所以，图 3 所示仿真建模中的调制解调器，可以适应任何阶数的 APSK。

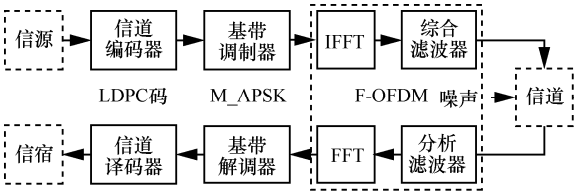
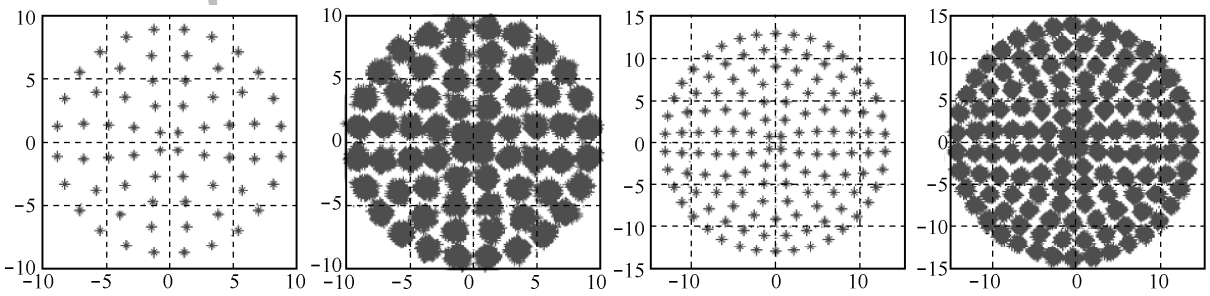


图 3 M-APSK 仿真原理

4.2 高阶 APSK 调制解调仿真

在传统的卫星通信或其他特殊通信系统中，高阶 MAPSK 主要是指 8APSK、16APSK 和 32APSK，应用中以 16APSK 为主。一方面是因为传统的卫星通信和其他特殊通信系统中的业务量，不需要更高阶的 APSK 调制解调，且传输信息的可靠性要求高，另一方面是因为卫星通信信道的复杂性使更高阶 APSK 的调制解调技术成本更高。当未来移动通信系统融合了卫星通信系统后，与传统的卫星通信标准相比较，相关的信息业务量和数据传输可靠性的技术标准都会发生较大的改变，甚至是完全相反的变化，因为运营商对市场利润的追求永远是首要的。可以肯定，在融入 6G 的卫星通信系统中的基带调制解调技术，必定有更高阶的 APSK。下面所有仿真结果中的解调方式，都是采用式(17)中的简化软解调方式实现的。

64APSK 和 128APSK 的发射端与接收端星座图如图 4 所示，其中 64APSK=24+16+12+8+4-APSK，星座是由半径分别为 1、3、5、7、9 共 5 个同心圆组成，从外往内圆周上等格分布的星点数分别为 24、16、12、8、4；128APSK=38+28+22+16+12+8+4-APSK，星座是由半径分别为 1、3、5、7、9、11、13 共 7 个同心圆组成，从外往内圆周上等格分布的星点数分别为 38、28、22、16、12、8、4。显然，64APSK 和 128APSK 的调制过程是以相



(a) 64APSK发送端星座　(b) 64APSK接收端星座/25dB　(c) 128APSK发送端星座　(d) 128APSK接收端星座/30dB

图 4 64APSK 和 128APSK 的发射端与接收端星座

人民邮电出版社

位调制为主，幅度调制为辅。从发送星座中可以看出，星点分布密度较密，且比较均匀，几乎没有空间浪费。从接收星座中可以发现，虽然都是高阶 APSK 调制星座，但经过 25 dB 和 30 dB 的高斯信道后，64APSK 和 128APSK 星座图中所有星点之间的界线还是比较清晰的，可为后期解调技术提供较好的解调条件。

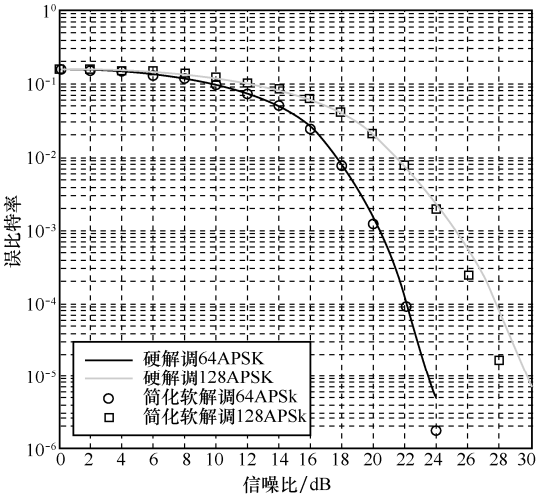
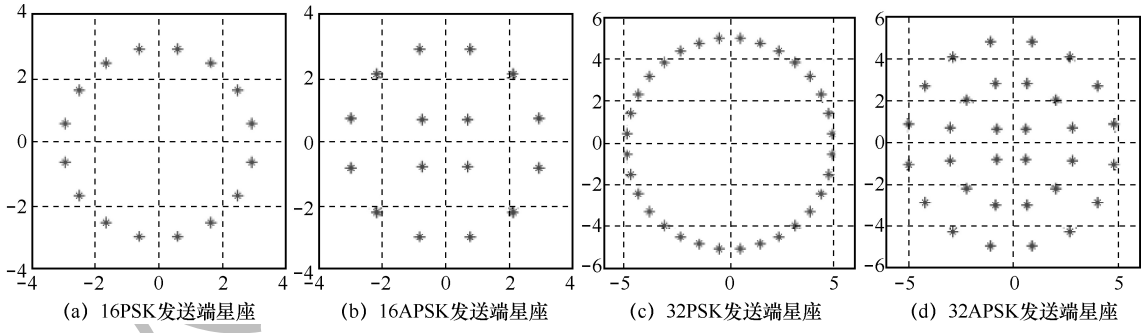


图 5　高阶 APSK 的仿真与理论误码率曲线

根据图 3 所示的建模条件，采用硬解调和简化软解调两种方式，仿真得到的高阶 64APSK 和 128APSK 的仿真误码率曲线如图 5 所示，目的就想以此可以得到较为明显的比较结果。可以看到，采用简化软解调方式的 APSK 的性能优于采用硬解调方式的 APSK。硬解调是指系统直接对符号解调的方法，优点是算法比较简单，缺点是解调性能比较差。软解调是指系统直接对信息比特解调的方法，当调制阶数较高时，由于系统需要对每个符号中的每个比特判决，算法比硬解调复杂很多，但因是对比特解调，所以解调性能也是最好的。简化软解调方式将软解调中的指数、对数和除法等复杂运法简化为普通的求最大值和减法运算，大大降低了软解调的算法难度，能够获得较好的解调性能，是一种优秀的 APSK 解调方法。

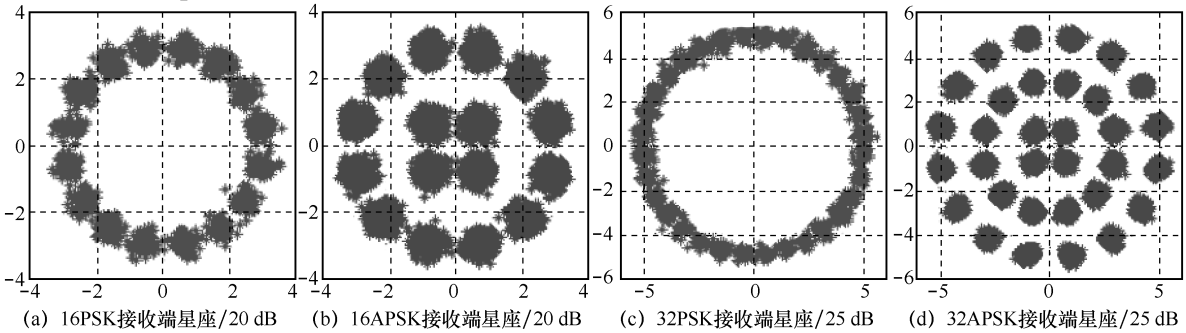
4.3　PSK 与 APSK 比较

PSK 方式将所有星点分布在一个圆周上，APSK 方式将所有星点分布在不同半径的多个同心圆周上，在相同调制阶数时，前者星点间的密度明显大于后者，使两者在接收端的解调分辨判决也完全不同。图 6 所示为发送端 16PSK 和 16APSK、32PSK 和 32APSK 的星座图，可以看出，后者因均匀占用了星座的分布空



(a) 16PSK发送端星座　(b) 16APSK发送端星座　(c) 32PSK发送端星座　(d) 32APSK发送端星座

图 6　相同调制阶数的 PSK 和 APSK 的发送端星座



(a) 16PSK接收端星座/20 dB　(b) 16APSK接收端星座/20 dB　(c) 32PSK接收端星座/25 dB　(d) 32APSK接收端星座/25 dB

图 7　相同调制阶数的 PSK 和 APSK 的接收端星座

间，所有星点间的最小间隔都要大于前者；图 7 所示为经过高斯信道传输后的接收端 16PSK 和 16APSK、32PSK 和 32APSK 的星座图，可以看出，虽然相同阶数的调制符号经过的信噪比一样，前者接收星点间的分辨界限明显模糊于后者，阶数越高，模糊程度越高，从而使得系统后期的解调判决技术难度也将越高。

图 8 所示为 16PSK 和 16APSK、32PSK 和 32APSK 在相同信噪比时的误码率。从图 7 中就可以看出，接收星点间的分辨界限较为清晰；从图 8 中可以看出，经过系统解调判决后的误码率，PSK 明显比 APSK 大，特别是当信噪比为 16 dB 时，32APSK 的性能开始优于 16PSK。另外，16PSK 和 32PSK 的误码率曲线间隔，明显大于 APSK，其间隔差距达两倍。APSK 的误码率曲线走势的陡度也明显高于 PSK，说明随着调制阶数的增加，高阶 APSK 还有较大的技术应用空间可供选择，这也是面向 6G 的卫星通信中有可能采用高阶 APSK 的重要原因。

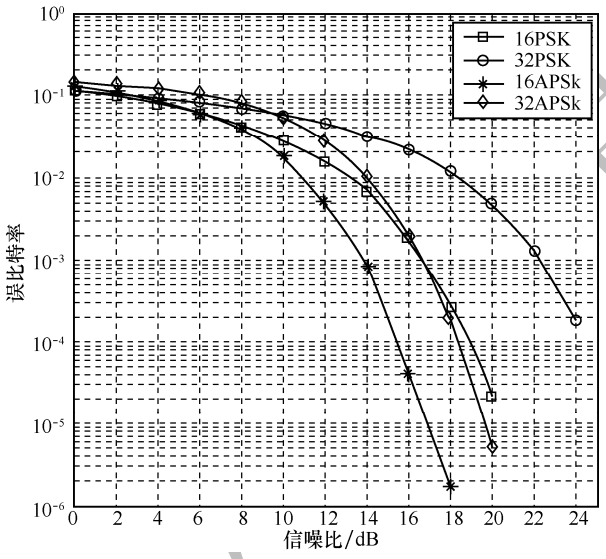


图 8　相同调制阶数的 PSK 和 APSK 的误码率

从星座图示来看，PSK 比 APSK 更难解调；从技术方面来看，PSK 的解调只需判决接收信号的相移，APSK 的解调不仅要判决信号的相移，还要判决信号的幅度，所以 PSK 的判决技术较 APSK 更简单。若设计的通信系统需要高阶调制解调技术支持，使同样高阶的 PSK 达到 APSK 的调制解调效果，PSK 的接收端就必须采用更为先进的技术大幅度提高接收灵敏度，实现中的技术成本会比 APSK 大很多。当调制阶数太高时，就目前的解调技术而言，采用更好、更优的技术，PSK 也无法实现正确解调。所以，对于高阶相移调制解调技术，虽然 APSK 的技术成本可能要高一些，至少是可以实现的。

5　结束语

自从前苏联于 1957 年发射人类第一颗卫星至今，卫星通信已经成功地应用了六十多年，是一项比移动通信应用还早上几十年的成熟通信技术。在人类所应用的卫星通信领域中，都是局限在可靠性要求极高、传输信息量较少，既不需考虑社会效益，也不需考虑成本投入的专用系统。所以，传统卫星通信系统中的基带调制解调技术大多采用调制效率较低，调制性能极高的 QPSK 方式。

卫星通信系统与移动蜂窝系统相结合，这种传统的应用领域格局会被打乱，社会商业利益的动力作用驱使运营商全面提高通信容量和数据吞吐量、降低通信技术成本、方便客户通信，并为客户提供更多的优质服务内容。可以预见，由于追求利益最大化的商业考核指标，将会全面改变现有卫星通信系统中的技术格局，不仅引入移动通信系统最基本的宽带通信技术，还会在基带调制解调技术方面尽量使用高阶 APSK。

APSK 与 PSK 的最大区别是，前者充分利用了星座图中的空间，使高阶 APSK 的星点合理、均匀分布，增加了相邻星点之间的距离，提高了接收端星座的分辨率，降低了接收端符号判决的技术要求，虽然 APSK 需要在发送端同时调制符号的幅度和相移，在接收端同时解调符号的幅度和相移，就目前成熟的通信技术来看，相比高阶 PSK 的相移解调，高阶 APSK 的幅度和相移同时解调技术的难度是完全可以克服的。

参考文献：

[1] RAN1 86 final minutes report[EB]. 2019.
[2] 汪春霆, 李宁, 翟立君, 等. 卫星通信与地面 5G 的融合初探[J]. 卫星与网络, 2018 (9): 14-21.
[3] 关于 6G 的通讯技术和未来展望[EB]. 2014.
[4] 潘亚汉, 朱自强, 张志强. 现代卫星通信调制解调技术的发展[J]. 微波与卫星通信, 1997(4): 11-16.
[5] 张长青. 面向 5G 的高阶基带调制解调器 MQAM 技术[J]. 5G 网络创新研讨会(2018)论文集, 2018: 152-159.
[6] 王磊, 徐大专, 张小飞. 高阶 PSK 调制的比特软信息简化计算方法[J].中国科学: 信息科学, 2012(6): 663-673.
[7] 许光习, 张邦宁, 郭道省. 卫星信道中高阶 APSK 调制的非线性失真补偿算法[J]. 电讯技术, 2010(4): 69-73.
[8] 刘志新, APSK 星座优化设计及其调制解调研究[D]. 长沙：国防科学技术大学, 2007.

面向电网巡检的点云高精度配准算法研究

吴新桥[1]，王昊[2]，杨家慧[2]
（1.南方电网公司生技部，广东 广州 510700;
2.南方电网数字电网研究院有限公司，广东 广州 510700）

摘　要：随着经济建设不断发展，电网建设在国民经济建设中具有越来越重要的地位。点云匹配是三维模型重建的重要环节，倾斜密集点云可以保留丰富的纹理细节信息。为得到高精度电力线路点云数据，基于倾斜密集点云与激光扫描点云进行点云配准，针对传统 ICP 配准方法对点云初始位置要求高的问题设计出一套点云配准的方法。通过粗配准调整两幅点云数据到较好的初始位姿，再通过 ICP 算法迭代最邻近点对，完成倾斜点云与激光扫描点云的精配准。实验证明，本方法可实现两幅电塔点云的配准，且具有良好的配准精度。

关键词：电网巡检；点云配准；ICP；粗配准；精配准

1　引言

随着电网高速发展，规模越来越大，输电线路设备日益庞大，无疑加大了对电网通道巡视、树障分析等工作的难度。如何提早预防、及时发现危害输配电线路的缺陷隐患，成为保障电力供应的一项重要基础工作。目前基于高精度点云的无人机自动驾驶成为电力巡检的新兴手段，如何低成本地获取高精度点云数据是当前研究的重点。应用高精度的线路点云数据，可开展杆塔精细化巡视航线设计，实现杆塔精细化巡视自动驾驶，解决杆塔精细化巡视还需要依靠手工操控的难题，降低人员操作门槛，规范化巡视作业，提高巡视效率、质量与技术水平。另外，针对可见光影像生成的点云导线缺失、树障分析人工工作量大的问题，将倾斜密集点云与导线点云完整的激光数据进行融合匹配，利用激光点云矢量化得到的导线模型与倾斜密集点云中的植被进行树障分析，可满足高频次、低成本的可见光航拍树障隐患分析需求。

本文采用倾斜密集点云与激光扫描点云进行算法的实现。一方面可通过倾斜摄影测量建模技术获取倾斜密集点云；另一方面，激光雷达扫描技术通过发射与接收激光脉冲信号，获取地物的三维点云。其脉冲信号具有良好的穿透性，可穿透一些植被遮挡获取地面地形信息。倾斜影像密集点云具有丰富的纹理信息，但由于其采集手段限制，难免会有遮挡及阴影部分，其点云密度无法保证获取到更多的地物的三维空间信息，而激光雷达扫描可采集到高密度的地物点云，可以弥补这一点劣势。通过对电力塔与电力线的激光点云及倾斜密集点云数据的配准，可以得到高密度包含纹理信息的高精度点云数据，为电力设施三维建模、电网无人机自动化巡视提供了良好的数据来源，进而提升了电力巡线的工作效率。

目前很多学者对点云配准技术进行了研究：

- 参考文献[1]基于点云的集合特征进行点云配准，其通过计算两幅点云数据的曲率信息进行，并通过匹配点云曲率值进而完成点云的配准；
- 参考文献[2]通过结合 Delauney 三角剖分与点特征直方图算子结合计算点云特征进行匹配；
- 参考文献[3]提出了基于遗传算法进行最优空间变换矩阵的计算，将变换矩阵应用于点云配准，通过投影空间点云到二维平面上进行特征匹配进而实现点云配准。

2　研究方法

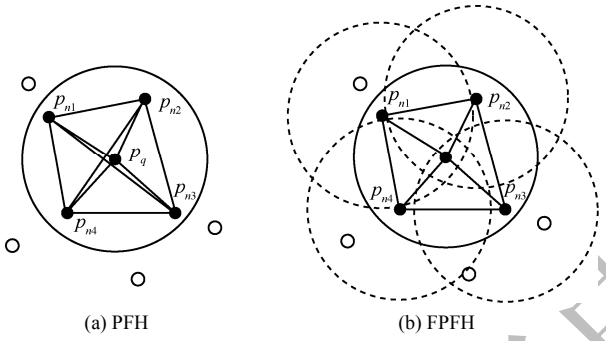
2.1　粗配准

对于倾斜密集点云和激光扫描点云来说，由于其获取手段不同，两种数据在空间尺度上难以避免地会发生偏差，因此需要对两种点云数据进行粗配准，粗配准就是通过寻找两幅点云之间正确的对应关系，以其中一幅点云为基准，另一幅点云计算出到基准点云的刚体变换矩阵，再进行刚体变换配准到基准点云的步骤。与此同时，ICP 算法在进行点云的精配准时，

人民邮电出版社

对点云的初始位置的要求很高，如果初始位置不当很容易出现局部最优或者针对比较对称的地物，很容易出现错误的点对匹配，所以粗配准就解决了点云初始位置的问题。本文粗配准所采用的方法为分别计算两点云的快速点特征直方图算子（fast point feature histograms，FPFH），再通过随机采样一致性算法（random sample consensus，RANSAC）进行点云刚体变换矩阵的迭代，进而获取最优的变换矩阵实现的点云的粗配准。

FPFH 由点特征直方图算子（point feature histograms，PFH）简化而来，FPFH 算法降低了特征计算的复杂度，但是仍保留了点特征直方图算法的大部分识别特性。点特征直方图描述算子如图 1 所示。



(a) PFH　　(b) FPFH

图 1　点特征直方图描述算子

PFH 算子通过参数化查询点 P_q 与邻域点 P_n 之间的空间差异，形成一个简化的点特征直方图算子（simple point feature histograms，SPFH）对查询点 P_q 的 k 邻域几何属性进行描述。SPFH 的算法是首先根据选取点的法向量构建一个固定的局部坐标系，然后通过计算邻域内点的法向量与选取点法向量的偏差 $<\alpha,\varphi,\theta>$ 以及邻域点与选取点的欧氏距离 d 共 4 组值作为该选取点的 SPFH 算子。

FPFH 算子相较于 PFH 算子的简化在于取消计算了邻域点之间的 SPFH 算子的计算，只计算选取点与邻域内点之间的 SPFH 特征，并重新确定每个点的邻域计算出最终的 FPFH 算子，计算式如式(1)所示。

$$F_q = S_q + \frac{1}{n}\sum_{i=1}^{n}\frac{1}{d_n}S_n \tag{1}$$

其中，F_q 为选取点的 FPFH 算子，S_q 为选取点的 SPFH 算子，d_n 为选取点与邻域点之间的距离，S_n 为邻域点重新确定邻域后计算的自身的 SPFH 特征。所以相较于 PFH，FPFH 算法大大降低了特征计算的整体复杂度，进而提升了配准的效率。

倾斜密集点云与激光扫描点云计算全局特征之后，采用随机采样一致性初始配准算法（SAC-IA）通过对两幅点云的 FPFH 特征进行匹配，依据点云数据旋转不变性的数据特点，计算出点云数据的刚体旋转矩阵。SAC-IA 首先利用对代配准点云中的点进行随机采样点，通过设置点与点之间的距离以确保点与点之间的 FPFH 特征具有足够的差异性，其设置的距离要大于计算 SPFH 时的邻域距离。利用贪婪算法与采样一致性算法结合，在目标点云中搜索随机采样点 FPFH 特征相似度高的点并组成点集。通过迭代随机采样点击与相似点集对应点之间的旋转矩阵，找到最优的旋转矩阵并完成粗配准。

2.2　精配准

粗配准后的倾斜密集点云与激光雷达点云已经处于较好的初始位置，为精配准迭代最邻近点算法（iteratire closest point，ICP）提供了良好的前期准备。ICP 算法的步骤如图 2 所示，具体如下。

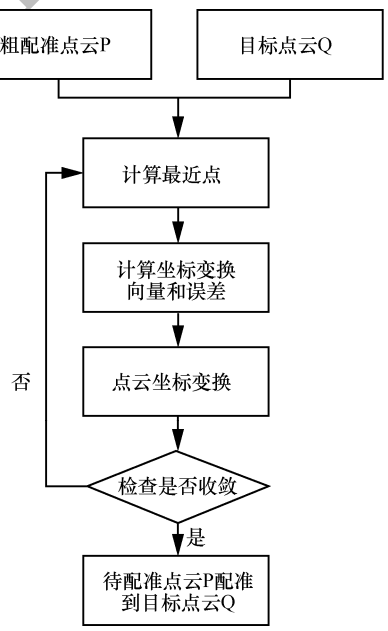


图 2　ICP 运算流程

（1）在待配准点云 P 中取点集 P_n，并依据距离最短原则在目标点云中 Q 中找出对应点集 Q_n。

（2）利用四元素法计算出两点集对应点的旋转矩阵 $\boldsymbol{R}$ 与旋转矩阵 $\boldsymbol{t}$。并对待配准点云进行刚体变换得到对应点集 $P_n^{'}$。

$$P_n^{'} = \{\boldsymbol{R}p_i + t, \boldsymbol{p}_i \in P_n^{'}\} \tag{2}$$

人民邮电出版社

（3）计算点集的平均距离 S，根据新点集 $P_n^{'}$ 与目标点云点集 Q_n 所有对应点距离平方和除以数据点总数 n，作为迭代收敛判断依据。

$$S=\frac{1}{n}\sum_{i=1}^{n}\left|p_i-q_i\right|^2,(p_i\in P_n^{'},q_i\in Q_n) \qquad (3)$$

（4）通过设置 S 的阈值，如果迭代后 S 的值小于阈值时则停止迭代；或设置最大的迭代次数，当到达最大迭代次数时迭代停止。不满足上述两种情况则返回第（1）步直到满足其中一条收敛条件。

3 实验分析

本实验基于 Visual Studio 2013 编译器，使用 C++ 语言借助 Point Cloud Library(PCL)点云开发库辅助开发实现电塔倾斜密集点云以及激光扫描点云的“粗配准+精配准”流程。

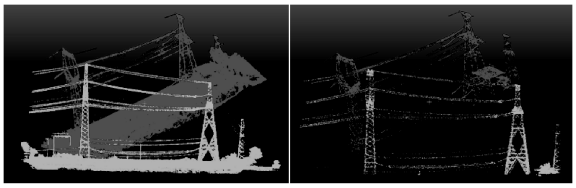
实验平台配置为：DELL OptiPlex 主机，CPU 为 Intel Core i7-7700，GPU 为 Nvidia GTX1050Ti，操作系统为 Windows 10。

3.1 实验流程

本实验所采用的原始数据为某电塔的倾斜摄影密集点云及激光扫描点云，两种点云初始位置存在较差异，利用本文介绍方法首先对两点云数据进行粗配准操作，并记录粗配准的旋转矩阵 R 及平移矩阵 t。在点云粗配准前，需对两点云数据进行去噪、降采样等操作。在电网通道中，利用电塔的位置不变性，只需配准电塔得到刚体变换参数即可实现整体点云的配准，同时树木等地物很容易受到自然环境变化（如风吹等）产生位置变化，会影响到配准的精度与整体配准速度，所以在进行数据预处理是将其剔除。原始点云数据与预处理后实验数据如图 3 所示。

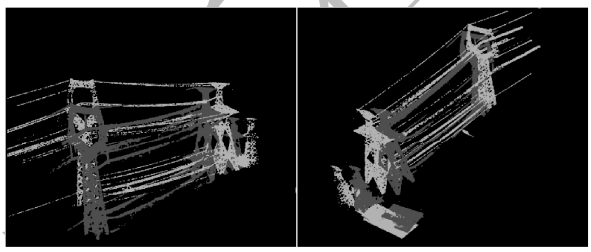
通过计算两幅点云的法向量之后进而计算 FPFH 特征，最后 SAC-IA 算法根据 FPFH 来迭代计算粗配准的旋转矩阵和平移矩阵，粗配准结果如图 4 所示

粗配准后的倾斜密集点云经刚性变换后与激光扫描点云已经处于良好的初始位置。导入程序中做 ICP 迭代，在经过 55 次迭代之后，两幅点云的平均距离 S 趋于稳定。精配准结果如图 5 所示。



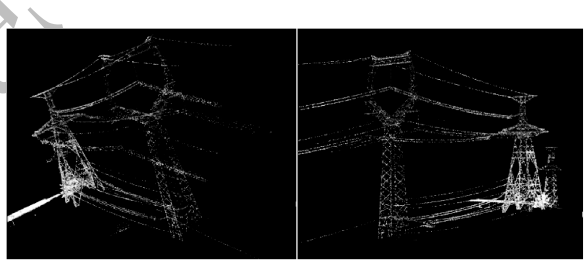
（a）原始点云数据　　（b）预处理后两点云

图 3　实验数据



（a）粗配准结果视角1　　（b）粗配准结果视角2

图 4　粗配准结果



（a）精配准结果视角1　　（b）精配准结果视角2

图 5　精配准结果

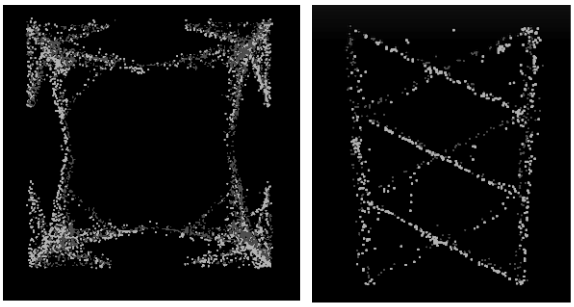
3.2 实验结果

配准结果见表 1。

两点云数据经点云数据预处理后点云数量分别为：113 767、111 753，通过本文算法进行程序的编写，经实际验证可以做到将倾斜密集点云与激光扫描点云进行自动配准。精配准后电塔横截面如图 6 所示。

表 1　配准结果

点云类型	点数/个	原始点云/m		粗配准点云/m		精配准点云/m	
倾斜密集点云	113 767	平均距离	标准差	平均距离	标准差	平均距离	标准差
激光扫描点云	111 753	25.92	15.7	2.65	1.73	0.16	0.12



(a) 横截面图1　　(b) 横截面图2

图 6　精配准后电塔横截面

4　结束语

本文介绍了一种面向电网巡检的倾斜密集点云与激光扫描点云数据的配准方法，针对 ICP 配准方法对点云初始位置要求过高的缺点，提出了一种利用点云全局特征进行粗配准，计算出两点云的刚体变换参数后，再进行精配准的方法。经实验验证此方法可实现点云自动配准，并具有良好的配准精度。此方法为倾斜密集点云与激光点云融合的树障分析提供了数据基础，同时为精细化电力线巡视的无人机自动航线规划提供了高精度的数据支持，可减轻人工工作量提升电力设备监控检修的工作效率。另外，经过此方法配准的点云数据可进一步进行数据融合，为生成精细化的线路通道三维模型奠定基础。

参考文献：

[1] 王蕊, 李俊山, 刘玲霞, 等. 基于几何特征的点云配准算法[J]. 华东理工大学学报(自然科学版), 2009, 35(5): 768-773.

[2] 刘剑, 白迪. 基于特征匹配的三维点云配准算法[J]. 光学学报, 2018, 38(12): 240-247.

[3] 江盟, 蔡勇, 张建生. 基于投影的点云配准算法[J]. 自动化仪表, 2019, 40(4): 14-18, 23.

[4] 杨现辉, 王惠南. ICP 算法在 3D 点云配准中的应用研究[J]. 计算机仿真, 2010, 27(8): 235-238.

[5] 宋林霞. 三维点云配准方法的研究[D]. 济南: 济南大学, 2013.

[6] 夏坤,孙水发. 点云配准中的初始配准研究[J]. 信息通信, 2019(2): 12-14.

人民邮电出版社

某企业园区网改造工程规划设计与实施

谢金友，王燕杰

（北京中电飞华通信股份有限公司，北京 100085）

摘　要：根据员工需求，近几年来某企业园区计算机网络基础平台及其网络信息平台应用进行了不断的改进，但是，随着网络和信息技术的不断高速发展，用户的应用需求趋向于高带宽和不受时空限制，小范围局部的改动已经不能满足企业发展。该企业以建设统一管理的、资源共享的数字化园区网为目标，基于对现行运行计算机网络和未来应用需求的深入分析，对园区网升级建设规划设计和改造工程实施进行了阐述。

关键词：网络升级改造；网络结构；无线网建设

1　园区网升级改造的需求分析

原有计算机网络采用单核心星型拓扑结构树状分层的整体架构，通过路由器接入互联网，出口是中国联合网络通信有限公司（以下简称中国联通），带宽为100Mbit/s，可以满足全体员工利用互联网资源的基本需求，升级前网络拓扑结构如图 1 所示。

该网络已经连续运行 10 多年，设备稳定性与可靠性目前已不能满足企业发展和公司员工日常工作、学习、生活的需要，主要存在以下几个主要问题。

（1）网络出口带宽需要扩容、冗余性差

现有 100 Mbit/s 的出口带宽已不能满足需求，且目前只接入一条线路。如果出现线路中断，直接影响互联网业务需求。

（2）网络存在单点故障问题

主机房出口路由器、防火墙、核心交换机的单核心结构设计，使得每个设备都成为外接出口的关键环节，哪一个出现故障都会影响与外网的正常通信，核心设备工作负荷过重，且型号陈旧，使用中硬件发生故障时很难再次购买到相关设备配件以保证故障及时的处理，从而延长了故障恢复周期，给日常维护带来了极大困难，

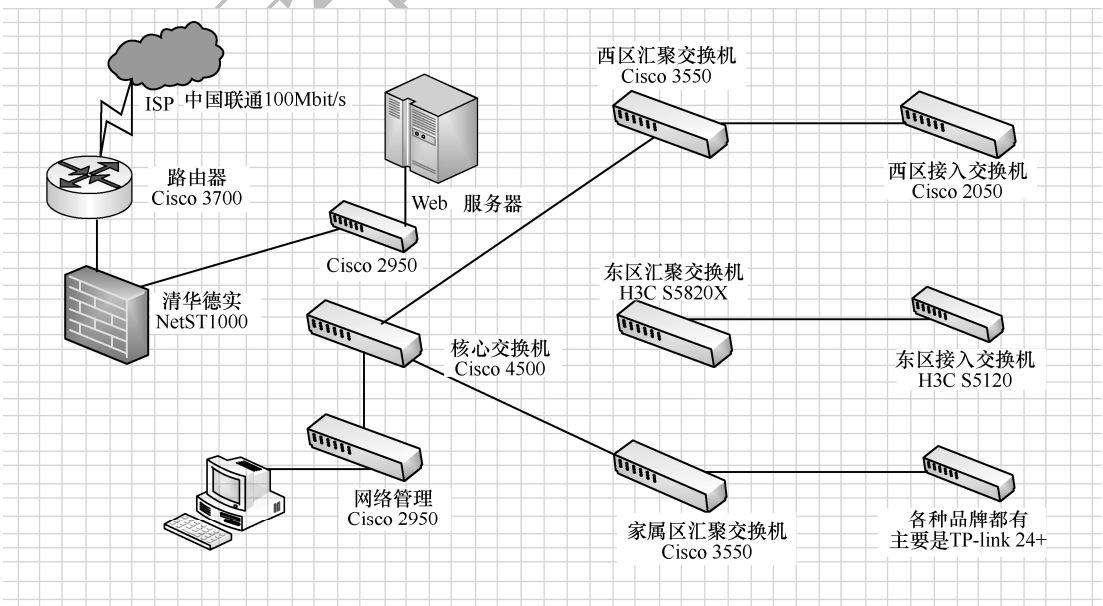


图 1　升级前园区网络拓扑

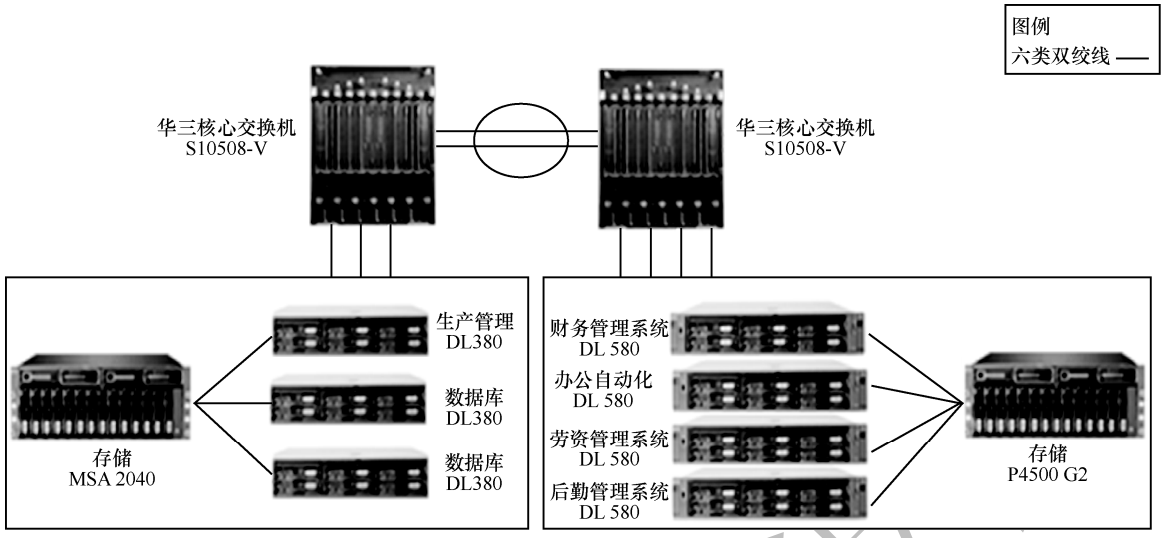


图 2　原有服务应用系统连接

且受设备自身结构影响，不支持万兆功能，已不能满足提升网络带宽的需求。

（3）缺乏统一的网络资源管理平台

园区网自初建至今 20 多年，还没有一个统一的网络信息管理软件平台，使得公司网络资源使用不方便、应用效果不明显。

（4）内部应用系统分散管理

由于历史原因，缺乏统一的规划，各部门的业务系统随着信息化进程逐年增加，应用服务器分散在各个部门自行管理，各部门在购买软、硬件资源时仅考虑本部门的需求，致使大量重复数据、垃圾数据客观上存在，没有统一的业务流程。因部门间所用数据格式的不同，导致不能协同工作，基础数据资源不能得到统一利用，没有充分发挥信息化的优势，极大地影响了公司的数据共享和信息化水平的提高。现有的 7 个管理信息应用系统采用不同公司的业务系统分别部署在 3 台 HP DL380 服务器、4 台 HP DL580 G7 服务器、1 台惠普 MSA2040 存储与 1 台惠普 HP P4500 G2 存储中。其中 3 台 HP DL380 服务器和 1 台 MSA2040 存储于 2006 采购安装，在近两年使用中经常出现硬件故障，导致应用无法正常访问。网络升级前应用系统部署连接如图 2 所示。

（5）园区布线杂乱、陈旧

园区经过多次部门布局调整后，建筑施工多次导致光纤和配线子系统中断，只能采用临时线路，使得线路杂乱；且骨干 1 000 Mbit/s，桌面 100 Mbit/s 布线系统已经不能满足开展远程监控和协同工作的需求。

（6）园区缺少无线网线覆盖

虽已实现全部楼宇使用有线接入网络，但随着通信技术全面迈进移动通信网络和移动终端 App 业务应用软件在公司运营中的普及率不断增加，对于方便、快捷、免费的无线接入需求越来越高，作为有线网络的有效补充，无线网络建设势在必行。

2　园区网升级建设方案设计

在明确网络改造需求目标和工作内容后，公司在遵循提出的总体设计理念和原则的基础上，最终确定了网络基础环境建设升级方案。

2.1　网络结构设计

园区网络主体结构仍采用当今局域网络工程中使用最广泛的树形拓扑结构，为了解决单点故障问题，根据万兆骨干、千兆到桌面的需求，采用了双核心层次局域网结构，如图 3 所示。

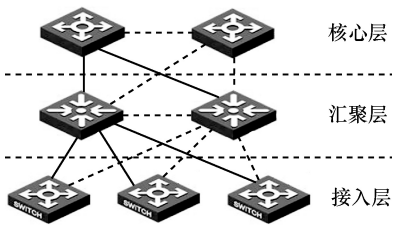


图 3　双核心层次局域网结构

通常网络层次化结构设计，能够使网络结构更加清晰、方便维护和无需改动原网络就可以容易地进行工作站扩展。按照网络规划的大小，将网络分为接入

人民邮电出版

层、汇聚层和核心层。

（1）接入层设计

接入层是网络的边缘，技术也相对成熟，各厂家产品的技术指标相差无几，一般都属于可堆叠/可扩充式固定端口交换机，能够提供各种类型大量接入端口，实现接入的安全、速率控制等，选择时要考虑稳定性、经济性和可管理性等因素。本次园区网接入层采用华为 H3C S5120-28P-SI，通过 1 000Base-X SFP 千兆以太网端口上行与汇聚交换机 H3C S5820X-28S 进行连接，通过 1 000Base-T 以太网端口 6 类双绞线下行与工作区信息点连接，实现千兆到桌面的目标。

（2）汇聚层设计

汇聚层是核心层和接入层的分界点，为了提高网络的安全性、稳定性，保证数据传输、交换的效率，在每一个区域的大型接入点都需要配置汇聚层设备，考虑到安全因素对资源访问的控制、考虑到性能的因素对通过核心层流量的控制等功能通常都在该层实现，要想层次化的特性得以实现，汇聚层应该向核心层、接入层屏蔽网络其他部分的信息，如果运行不同协议，各种协议的转换也应在汇聚层完成，在设备选型时为了发挥厂家核心技术带来的好处，汇聚层交换机、核心层交换机最好选用同类品牌。本次园区网接入层采用与核心交换机同品牌的 H3C S5820X-28 汇聚交换机，此交换机全面支持 IRF2（intelligent resilient framework，智能弹性架构），可满足用户网络的高度弹性智能扩展。利用 IRF 技术，用户可以通过堆叠接口连接多个设备，形成一个联合设备（Fabric），并将这些设备视为单一设备进行管理和使用，从而扩展设备端口数量和交换容量，还可以通过多个设备之间的备份来提升设备的可靠性、降低管理成本，同时实现按需购买、平滑扩展，在网络升级中最大限度地保护现有投资。通过 1 000 Mbit/s 电接口上联核心交换机，实现骨干网带宽提升到万兆的需求目标，通过 10G SFP 端口下联接入交换机、配置两台汇聚交换机通过 1 000 Mbit/s 电接口连接服务器集群，同时满足了园区网高带宽接入的需求，也节省了设备资金。

（3）核心层设计

核心层主要连接建筑群和服务器群，应能容纳来自汇聚层设备上的绝大部分数据流量，是网络的骨干，连接一般采用光纤作为传输介质，典型的核心层网络技术目前应用最广泛的是以太网，核心层设计时通常都要考虑设备和线路的冗余，核心层的关键设备是核心交换机。本次园区网升级的目标之一是建成万兆级骨干交换网络，考虑到未来 5 年内局域网的发展，核心层新添加两台了 H3C S10508 作为核心交换机，配置二块主控单板 LSU1SUPA0 业务处理引擎。

配置一块 LSU1TGS16SF0（16 端口万兆 SFP、光纤接口以太网业务板）通过 1 000 Mbit/s 电接口链路与汇聚层 H3C S5820X-28S 连接，配置一块 LSU1GT48SE0（48 端口 10/100/1000Base-T 千兆以太网业务板）通过千兆链路连接服务器集群汇聚交换机，能够实现骨干网需求，两台核心设备分别负责东、西区来自汇聚层数据快速的交换，配置虚拟路由冗余协议 VRRPv3，解决了局域网中配置静态网关出现单点失效问题，选用此以太网交换机虽然初期投资压力大，但双核心的设计即保证了带宽的扩容，又为网络将来升级做好准备，同时实现了实时的热备份，保证了局域网内部数据的不中断，从长期投资回报率看实际上为单位节省了资金的投入。

2.2 局域网技术选型设计

以太网技术以其结构灵活、技术成熟和易于管理等特点成为大多数单位局域网组建首选技术，特别是网络升级过程中可以花费很少的投资就可以实现，随着万兆以太网技术的成熟，进一步推广到广域网应用中。因此，本次园区的网络基础环境升级建设中骨干交换设备间采用万兆位以太网技术设计方案，采用高性能稳定的 10 Gbit/s 交换机作为网络的核心，利用虚拟局域网（VLAN）技术采用基于端口的划分方法隔离开局域网数据，不改动原有依据网络 VLAN 在交换机上的划分方案基础上，增加 WLAN，采用以太网供电技术（power over ethernet，POE）通过以太网线路为无线接入点设备直接提供电源，可以避免大量的独立铺设电力线，简化了系统布线，降低了网络基础设施的建设成本。

2.3 网络出口线路设计

本次园区网在保留原中国联通 100 Mbit/s 出口的基础上，增加一条 200 Mbit/s 电信通出口，不同 ISP 出口即满足了增加出口带宽的目标，同时满足了出口线路冗余，提高了可靠性。公司现申请 8 个 C 类公网 IP 地址，通过在防火墙配置网络地址转换，实现全园区使用 C 类私有地址访问互联网的需求。

2.4 无线网络搭建设计

根据园区网的总体需求，此次无线网络的建设

主要是东、西两个区域在有线网络基础上实现无线网络扩充，包含各个楼宇内部及其附近广场区域，使员工与临时用户可以在各楼宇内区域和经常出入的活动空间都能任意地访问网络，无线网络设备实现统一管理，布线与有线网络物理线路分开，采用独立线路确保网络的安全性，同时要考虑用户使用无线网络的方便性，达到提供高效、稳定的网络服务的目标。作为有线网络的一个有益的补充，本方案采用 802.11g 无线局域网技术，为了增强无线网络安全性，要实现不同等级用户只能访问相应网络应用资源的权限控制，通过花费较少的资金成本搭建一个可以管理、安全性高、易于使用、方便扩展的移动办公环境。

各个楼宇无线 AP 接入无线接入交换机，通过无线 AC 分别接入东、西区的核心交换机，设置认证系统并结合智能无线控制平台进行工作，无线网络的搭建对现在有线网络结构不会进行任何改动。

原有网络地址规划采用 C 类私有 IP 地址通过 VLAN 划分为逻辑网络，此次无线网络搭建仍然沿用以前 IP 地址规划方案，增加相应的逻辑 VLAN，公司移动终端用户从无线接入点自动获取 IP 地址，DHCP 服务器由无线设备承担，无线接入设备的管理地址同样统一分配。

无线网络和有线网络进行统一认证，要求 AP 支持标准的 IEEE802.1X 用户接入认证和 Web Portal 认证方式。

无线漫游机制采用用户始终根据最短路径优先原则选择上联的有线点，保证用户业务的连续性。

无线交换机通过 6 类线连接的无线接入点进行供电，这样在综合布线时就无需进行本地供电设计，节省资金的同时降低了施工难度，但无线接入点的选型均要求支持 POE 供电功能，设备成本会略有增加。

2.5 升级后的网络拓扑结构

园区整体网络架构采用传统基于树型的双星型三层构架设计，数据链路进行了冗余设计，整体网络规划设计的重点内容是主机房网络结构的调整、服务器集群建设和网络信息管理系统，升级后的拓扑结构如图 4 所示。

3 园区网升级工程实施

网络系统集成是指根据应用的需要，将硬件设备、网络系统软件、网络基础服务、应用软件等组织成一体，使之成为具有良好性价比的计算机系统的过程。其中硬件部分包括通信子网硬件系统和资源子网硬件系统，涉及的设备很多，如果要选择适合自身需要的设备，就要对各种设备的性能指标深入地了解。

园区此次工程实施按照统一规划、分步实施的原则分阶段进行，每个阶段安排一组业务相关的子系统集中实施，实施阶段的规划综合考虑实际业务需要、人员培训情况进行安排。

3.1 园区网线路改造

东区综合布线设计已经考虑到未来五年的发展，采用万兆级单模光纤级联，本次通过东、西区电缆沟敷设一条单模光纤连接信息中心主机房新增核心交换机即可。西区根据网络建设总目标万兆骨干的需求，所有楼宇间连接室外光纤全部需要升级，本次采用敷设万兆级单模光纤从各楼宇直接连接到信息中心，配线子系统施工恰逢分厂楼宇重新布局，进行统一的内装修，所以先进行 3 个楼宇的施工，根据实际需要，在不改变原超 5 类的原则下园区网正常运行，进行全新的 6 类双绞线敷设，通过楼道吊顶和桥架方式进行。

本次施工另一项不同之处是全部采用双线路冗余敷设，虽然费用有些提升，但是能够提高系统的可靠性，方便用户的扩充，投入产出性价比在未来几年的维护工作中就会体现出效果。

通过全新线路改造解决了基础线路杂乱的问题，为实现全园区万兆骨干、千兆到桌面的目标提供了线路保障，同时也满足了未来 5 年发展的需要。

3.2 服务器虚拟化建设实现

为提高园区网络应用系统服务效率，采用目前较为成熟的服务器虚拟化技术，将运行在原有服务器上现有业务应用迁移到虚拟化平台。本次服务器虚拟化建设平台采用了深信服科技公司的 aSV 服务器虚拟化平台，该平台是介于硬件和操作系统之间，它采用裸金属架构的 x86 虚拟化技术，能够实现对物理资源的抽象，服务器将内存 I/O、处理器等物理资源分组，统一进行调度、管理和分配逻辑资源，基于这些逻辑资源，相互隔离、多个并发操作的虚拟机执行环境在单个物理服务器中得以构建，使得资源利用率更高，更加灵活的资源分配需求同时得到满足，如 HA、提供热迁移等高可用性，实现更低的运营成本、更高的灵活性和更快速的业务响应速度。

虚拟化软件是 VMware vSphere 5.0，此软件能够

人民邮电出版社

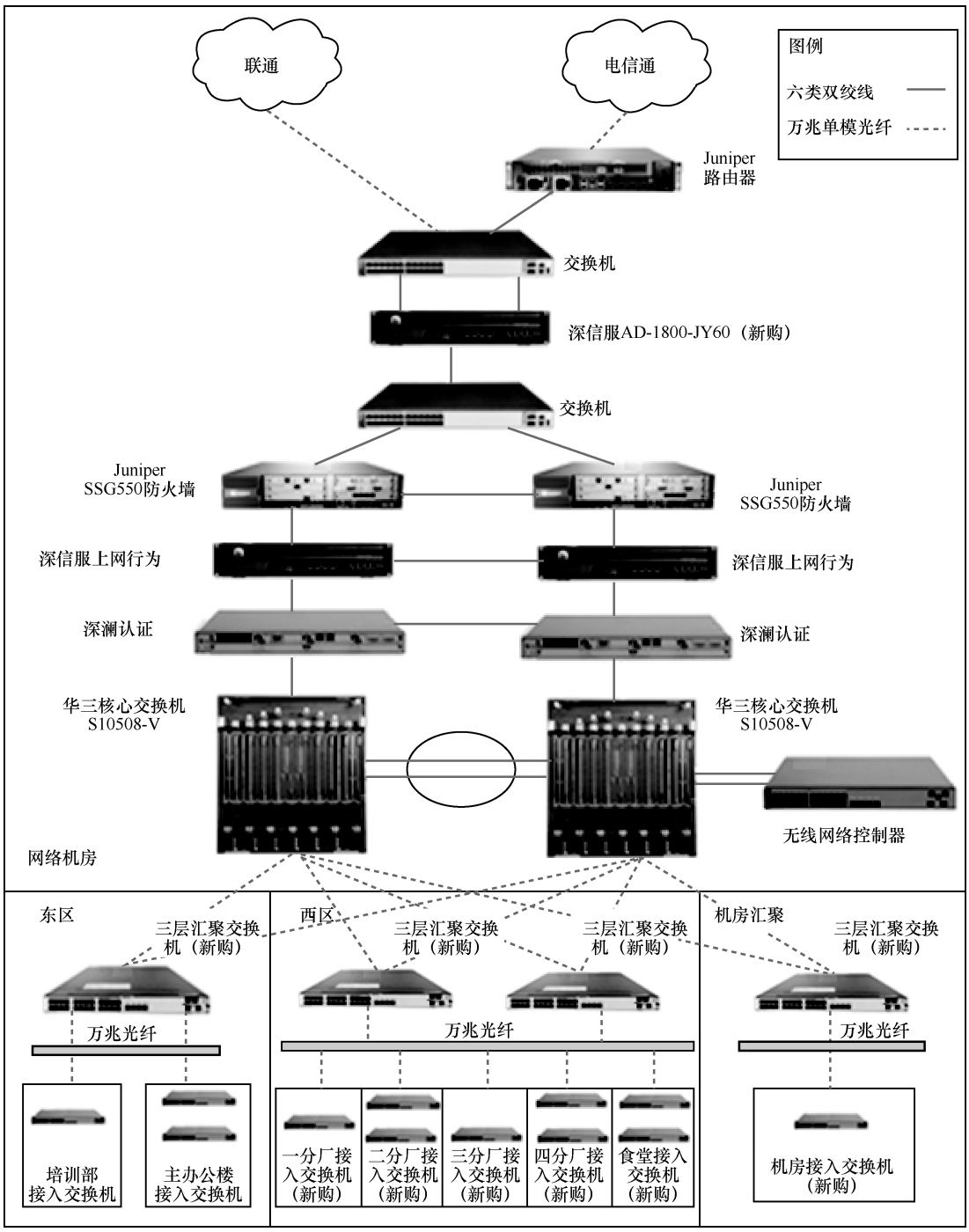


图 4　升级后园区网络拓扑

独立安装于裸机上，实现服务器的全面整合，提高资源利用率。本次采用全设备模拟，一些真实设备可以通过该方式进行模拟，在软件中复制一个设备的全部总线结构或所有功能。该软件作为一个虚拟设备放置在 VMM 中，用户操作系统的 I/O 访问请求同样会嵌入到 VMM 中，与 I/O 设备交互。

服务器虚拟化过程中，搭建了虚拟化服务器集群，并统一进行管理。不影响原有服务器设备的正常运行，同时原服务器与虚拟化服务器有机地融合在一起。通过服务器的虚拟化转移，虚拟化集群的规模继续动态增加，构建的 IT 体系架构更加健康，客户端访问模式不做任何更改，虚拟服务器进行数据交互操作时，相

当于原有的传统物理服务器访问模式，对业务系统不会造成任何不利影响。

通过本次虚拟化系统的建设，对信息化资源进行了有效的整合，提升了信息化管理水平，提高了资源利用率和系统可靠性，对公共服务用户及办公系统提供及时、高效的技术支持服务，原有业务应用系统通过虚拟化技术的部署，让业务系统能承载更多的数据应用，实现了各部门的业务系统应用服务器的集中管理，解决了信息孤岛的存在，同时还避免出现资源闲置浪费情况，满足了未来五年内信息化建设的需要。

同时新增一台康孚（CommVault）存储，作为虚拟服务器备份，确保数据保护的高性能，使网络存储更加便捷。设备存储直接上联光纤交换机，采用 8 GB 双光纤链路，保证存储与光纤交换机链路连接具有足够的冗余能力，使数据的存储不再通过服务器，减轻了服务访问压力。服务器通过采用 8 GB HBA 卡上联双万兆光纤模块连接至核心交换机，保证了数据交换速率。

3.3 用户认证管理机制

园区网络用户管理采用基于 B/S 架构开发的网络信息管理系统，实现了用户认证与应用系统使用的统一，有线与无线用户通过认证系统统一认证，通过认证软件（深澜 Srun3000）和 H3C IMC 的网管平台，该平台能够实现多个终端使用一个账号、登录时间控制等功能，从而建立了功能完备的、统一的网络用户管理系统。用户认证管理得到了进一步加强，实现了一次认证即可以访问公司不同应用系统的需求，改变了原有各部门应用系统使用不同的用户名和密码的现象，认证过程如图 5 所示。

（1）无论有线用户还是移动终端用户通过浏览器访问园区内外资源地址，数据传送到认证网关；

（2）认证网关将请求传送到门户认证平台服务器；

（3）门户认证平台服务器向用户推送认证界面；

（4）用户输入用户名和密码，回送到认证服务器；

（5）认证服务器通过访问数据存储核对用户身份，通过后通知认证网关；

（6）认证网关放行，用户即可以使用互联网、公司应用系统资源。

3.4 无线网络工程实施

无线网络布线与设备安装：按照无线 AP 布置方案，遵循综合布线技术工程技术标准，完成了园区无线网络布线工作，本次无线网络建设使用两台无线汇聚交换设备，东区 1 台安放行政楼主会议室（310），西区 1 台安放信息中心（201），分别通过单模光纤连接东、西区核心交换机，无线接入交换机同样通过单模光纤连接到两台无线汇聚交换机，为实现有线设备与无线设备品牌统一，选用杭州华三通信技术有限公司自主研发的运营级多业务 AC（access controller，无线控制器)。无线接入点设备选用 H3C WA2620i-AGN，采用瘦 AP（Fit AP）方式，通过有线无线一体化交换机，接入 H3C 无线控制器，三者有机的配合组成公司网络。

4 网区网改造后测试与运行情况

整个项目改造过程是循序渐进的，采用一边运行

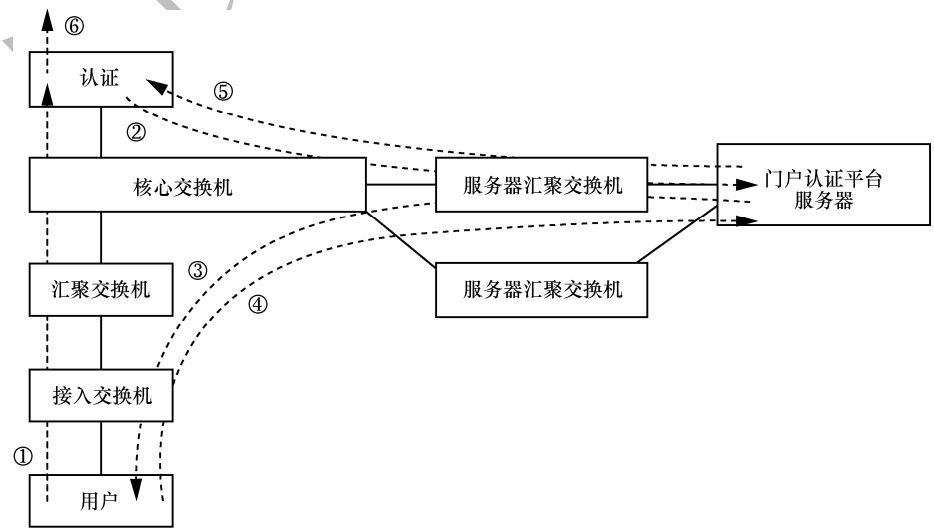


图 5 网络用户认证过程

一边改造的方法，没有影响到园区网正常工作情况下，目前计算机网络部分基本完成并投入使用，通过这次升级改造，信息基础设施平台服务质量得到较大的提高。

改变后的双核心、双链路的三层交换网络，实现了通信子网设备型号的统一，方便了设备的管理工作，通过万兆光纤链路互联建成了万兆位交换以太网络，核心层与汇聚层之间交换设备相互作为备份，骨干网的高可用性和高可靠性得到了保障，通过西区楼宇到信息中心万兆光纤，部分楼宇配线子系统双线路冗余 6 类线敷设，既满足了千兆到桌面的方案需求，又为以后几年带宽的扩展提供了可能，设备安装、调试和布线工作完成后，对所有联网的信息点进行了线路系统连通性测试，方法为每次间隔 1s 的 10 次 Ping 测试，目前为止网络运行平稳。

无线局域网技术已经历了 20 多年的发展，逐步摆脱了网络速度慢、价格高等问题，本次园区无线局域网建成后，满足了用户在园区内楼宇室内外的无线覆盖，解决了有线网络无法克服的困难，是原有园区有线网的有效补充。无线网络基础工程建成后，马上投入了试运行，解决了员工移动终端设备方便、快捷、免费的无线接入需求，接入稳定，接入网速相当于 20～50 Mbit/s 宽带。

参考文献：

[1] 雷震甲. 网络工程师教程[M]. 北京: 清华大学出版社, 2004.
[2] 黄传河. 网络规划设计师教程 [M]. 北京: 清华大学出版社, 2009.

人民邮电出版社

企业“中台”战略研究——以国家电网公司为例

杜栋[1]，杨莉媛[2]，谢炯[1]
（1. 内蒙古电力集团蒙电信息通信产业有限责任公司，内蒙古 呼和浩特 010000;
2. 内蒙古医科大学卫生管理学院，内蒙古 呼和浩特 010110）

摘　要：在梳理研究中台概念、分类以及实施条件的基础上，以国家电网公司为例，分析了实施中台战略的必要性和目前的建设情况，论述了中台在企业数字化进程中占据的重要战略位置，为进一步深化研究企业中台提供了参考和借鉴。

关键词：中台战略；数字化；电力物联网

1　引言

从 2018 年年底到 2019 年年初，国内各大互联网公司（如阿里巴巴、腾讯、京东、百度、美团等）都启动了近几年最大规模的组织调整计划，几乎都聚焦到了构建企业“中台”，“中台战略”成了关注热点。2019 年 3 月，国家电网公司正式发布《泛在电力物联网建设大纲》。建设的基础是“应用云大物移智链等现代信息技术，以及先进的通信技术”，其中云计算和大数据的应用主要就是在平台层推动建设大中台[2]。云计算为大中台提供计算基础能力，大数据通过对业务赋能从而构成大中台的实体。最终为国网“三型两网”中平台型、枢纽型和共享型的建设提供助力。从国内互联网巨头，到“世界五百强”中排第二的央企，不约而同地认可了“大中台、小前台”的模式。本文在梳理中台概念、分类以及实施条件的基础上，重点分析了国网公司中台战略实施进展情况。

2　概念的产生

中台概念产生之前，对于信息系统，主要分为前台和后台两个维度。其中，前台是通过各种前台系统构成的前端平台。前台系统即企业与最终用户的触点，企业的最终用户通过前台系统进行交互。如直接使用的门户、微信公众号、手机 App 等。后台是通过后台系统构成的后端平台。后台系统通常用于企业核心资源（计算+数据）的管理，如 HR 系统、客户管理系统、进销存系统等。前台和后台可以比作两个不同转速的齿轮。因为前台要对前端客户的需求做到快速响应，所以需要具备快速迭代创新的能力，并且转速越快越好；而后台需要相对稳定的后端资源，过往的系统常常是陈旧复杂的，又要满足法律法规审计等相关要求，所以稳定是最主要的，转速往往也是越慢越好。因此，随着企业不断发展壮大、业务要求越来越高，这种前后台模式的“齿轮”速率匹配不平衡的问题就逐步凸显出来。

对于这样的问题，Gatner 在 2012 年的一份报告中，提出一种解决思路[1]：以 pace-layered（步速）的划分维度来看，企业的应用系统可以分为 3 个层次：SOR（systems of record）、SOD（systems of differentiation）和 SOI（systems of innovation），分别对应前中后台。处于不同层次的系统因为需求不同，目标不同，对“速率”的要求也不同，需要匹配不同的管理流程、技术架构、治理架构以及投资策略等。参考文献[1]为“中台”产生提供了理论上的支撑。

国内最早提出“中台”概念的是阿里巴巴。在 2015 年，阿里巴巴集团对外发布中台战略。目标是要适应“互联网+大数据”的时代要求，构建创新、灵活的“小前台、大中台”系统架构[3]，如图 1 所示。即前台业务以更快速、更敏捷的响应去应对瞬息万变的客户市场；中台将整合集团的数据治理能力、产品服务技术能力，对前台一线业务构成有力支撑。“中台”伴随着微服务、云计算、容器化、Devops 等概念和工具的兴起，概念也在不断延伸，分类也越来越明晰。

人民邮电出版社

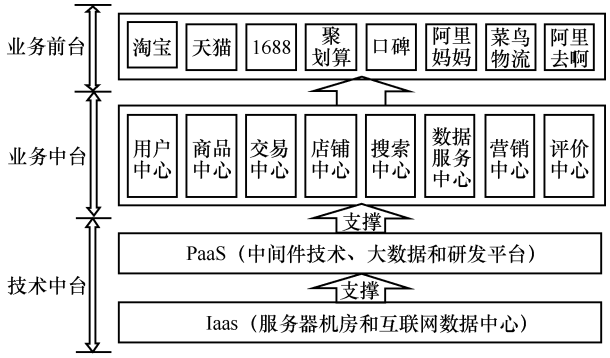


图 1　阿里巴巴集团中台架构

3　分类和实施条件

3.1　中台分类

现在大中台的架构不再局限于互联网行业，随着发展和延伸，大型企业也在探索和实施。通过中台战略为整个企业提供数据治理能力、支撑服务能力、产品技术能力等。对于大中台的分类也不只是技术中台，还包括数据中台、基础中台、业务中台等。

（1）基础中台

大中台架构的底层基础支撑是基础中台，也就是 PaaS 容器层。就中台模式来说，需要灵活高效的平台，所以选择容器云平台和容器集群管理的技术路线变得很关键，Docker、K8S、CI/CD、DevOPS 等工具、理念以及方法作为基础中台重要构成部分支撑中台模式。

（2）技术中台

技术中台架构如图 2 所示。技术中台最下面一层为应用提供层，主要包括通用应用、生态应用、伙伴应用等；上面一层为集成 PaaS 层，将消息总线、数据总线、服务总线、身份认证、Portlet 容器等中间件或者相关产品技术融入，提供技术支撑；DaaS 数据层主要是数据中台，通过大数据相关技术，实现数据计算分析、数据运营管理等能力；服务中台层与共享服务层协同支撑应用层和连接层的相应业务，满足客户的需求，提供对应的服务。

（3）数据中台

在数字经济的浪潮中，“云大物移智（云计算、大数据、物联网、移动互联网、智慧城市）”等新技术推动着传统行业数字化转型。数字化将对企业活动、流程、业务模式以及员工能力等各领域重新定义。在数据中台层面，主要是通过对企业数据治理，实现数字化运营。数据中台除了治理业务数据，还囊括数据治理的上下游过程，包括对数据的采集、计算、存储、配置、展现等。

（4）业务中台

业务中台立足于公司整体，从全局战略、业务支持、客户服务、产品创新等维度统筹规划，由基础中台、技术中台、数据中台等联合支持构建业务中台。

3.2　中台战略实施前提

随着“小前台，大中台”架构的发展，众多公司



图 2　技术中台架构

逐步探索大中台这种业务模式。然而，并非每个公司都具备成功实施中台战略的条件。大中台模式的构建需要满足特定的前置条件，主要包括行业属性、企业体量、技术实力几个方面。

（1）行业属性

大中台战略最初在互联网企业兴起，针对的群体主要是 ToB 的用户，有利于构建产业生态，使企业上下游相关业务有效衔接，帮助企业前台更好的贴合用户，提供更有针对性、更具人性化的服务，改善用户感受，加速业务交互频率。中台和后台为前台提供管控辅助和技术支持。目前来看，“小前台、大中台”模式已经在政府、能源、金融等行业领域探索建设了。

（2）企业体量

通常来说，大中台体系建设在体量较大的企业更容易开展。体量庞大的企业大多是业界标杆或行业楚翘。公司结构层级较多，存在较多有实力的分公司、子公司或其他直属单位。集团整体业务多元化，业务线复杂，多板块、多业态并存。企业内部资金充足、技术团队完善、具备良好的信息化建设基础，有强大的能力去调整上下游业务和信息化系统架构。

（3）技术实力

良好的技术实力对于打造大中台业务架构的企业来说，是不可或缺的。对企业自身业务架构和流程具备较深的认识是实施中台战略的基础，同时，要对中台架构需要的技术或者产品有清晰的了解，便于后期对中台体系的维护、升级。如果企业暂不具备独立建设或维护中台的技术能力，可以与技术实力过硬的厂商合作开展，在构建过程中能够快速地学习对方的能力。

4 国网公司的中台战略

4.1 国网实施中台战略的必要性

从“十一五”开始，国网电网公司围绕着企业管理、电网运营、营销服务等业务领域，开发了各层级的应用。经过 SG186 和 SG-ERP 等系统性工程后，国网公司信息化水平快速提升，仅省公司层面现有统推系统和自建系统就超过 100 个。这些系统的 IT 架构主要为“烟囱式”。这种情况不止在国网，我国大部分企业过去的 IT 系统架构都是以这样的方式。首先业务部门或单位提出业务需求，主管科技信息的相关部门进行立项。其中，对于自身有开发能力的企业，可以自行组织开发实施；不具备条件的，选择外部 IT 公司开发集成。然后经过需求调研、分析设计、开发、实施、测试、试运行的项目周期。可以说，每个新系统的上线都意味着一座“新烟囱”的矗立，这样的信息化架构体系和建设方式导致了很多企业内部系统烟囱林立，形成了资源“孤岛”和信息“孤岛”，带来了很多弊端。

另一方面，国家电网公司的对外业务，包括放开的售电侧、综合能源服务、金融产业板块等，都需要面对市场的洗礼，适应激烈的竞争格局。这种状况与 IT 行业不确定的市场环境非常类似，原有的烟囱式架构体系是无法应对的，所以实施中台化战略是国网为实现改革发展必要举措。

4.2 国网的数据中台

中台战略是一项包含企业组织架构、业务架构和技术架构的整体性战略。国家电网公司作为“世界五百强”中排名第二的超大型央企，管理资产超过万亿，员工数超过百万。在“三集五大”之后，人财物高度集约化，规划、建设、运行、检修、营销等业务也都垂直一体化管理，无法像互联网企业直接调整组织架构、迭代式地实施中台战略。因此，先从体量相对较轻、技术基础较好、文化氛围与 IT 企业相近的信息化部门和单位先进行探索尝试，优先建设数据中台，是最稳妥的落地路径。所以国网公司以信息化部门和单位为班底，以数据中台为转型抓手，助力泛在电力物联网建设。

数据中台具体的架构如图 3 所示。

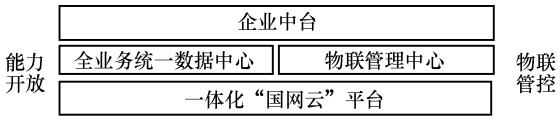


图 3　国网公司数据中台架构

其中，国网云平台作为整个数据中台架构的平台基础，在 PaaS 层提供服务。“国网云”主要包括企业管理云、公共服务云和生产控制云 3 部分[4]。因为国网的业务复杂，对系统并发、精度和时延等各项指标有较高要求，内外部业务系统计算的需求都非常大。不管通过配置多高的单台计算机或服务器，都无法满足不断增长的需求。只有依靠云计算通过服务器集群来对各项需求进行并行的处理，进而实现资源调配更弹性灵活，数据利用更集中智能，服务集成更统一高效，应用开发更快速便捷。

全业务统一数据中心涵盖两方面内容，一方面是数据中心建设需要基础设施资源池（IaaS，基础设施即服务），通过采用云计算、虚拟化等技术手段，将传

人民邮电出版社

统的软硬件架构转变为可资源共享、统一管理、按需分配、动态调度的统一软硬件资源环境。因此需要在不同的地域规划建设数据中心，为上层业务提供物理基础。另一方面指的是全业务统一的数据库，主要包括全域核心业务数据模型设计、数据整合实施、综合应用示范和数据资源管理等内容。这部分在整个数据中台建设中难度最高、工作量最大。需要改变以前烟囱式系统的数据库架构，牵涉的数据需要重新进行定义，海量的数据需要针对数据格式、数据库分库分表、清洗方式等进行重新确定和调整。

物联管理中心初期的建设要求是满足感知层的传感器的接入，包括设备的接入方式统一、传输协议统一、设备全生命周期管理等。2019 年“国网两会”上提出打造“三型两网”的新时代战略目标，物联管理中心的内涵进一步延伸，成为了泛在电力物联网的重要组成部分。物联管理中心的数据来源主要包括两部分：感知层设备的直接接入和网关数据的接入。物联管理中心利用物联网的感知技术、智能装备对物理世界进行感知识别，对识别的信息进行计算、处理和知识挖掘，实现人与物、物与物信息交互和无缝链接，达到精准管理、实时控制、科学决策的目的。

5 展望

战略是为实现企业愿景、对企业未来发展方向作出的长期性和总体性规划。战略的制定要顺势而为，甚至预见趋势。2012 年开始，移动互联网开启了个人用户数字化转型的序幕，互联网企业进入了爆发式增长的“上半场”，如火如荼。2018 年，随着 C 端用户流量战场趋于饱和，人口红利越来越少，用户增长越来越低，互联网企业角逐的战场从需求侧向供给侧战略转移，供给侧企业数字化转型兴起，互联网企业正式进入“下半场”。为顺应趋势变化、获得竞争优势，几乎所有互联网巨头从 C 端转向 B 端，从模式创新转向了技术服务创新，聚焦到建设中台上。国网公司也在同一时间做出了组织架构调整，重新“排兵布阵”迎接新的挑战。各大巨头对于中台战略的重视高度一致。中台建设的过程就是企业发掘、沉淀、打磨、输出自身核心能力的过程，对内共享，对外开放，统一指挥，协同作战。最终作为能力的载体与化身，中台必将在企业数字化进程中占据重要的战略位置。

参考文献：

[1] MESAGLIO M, HOTLE M. Pace-layered application strategy and IT organizational design[R] . Gartner Research Note, 2012

[2] 傅质馨, 李潇逸, 袁越. 泛在电力物联网关键技术探讨[J]. 电力建设, 2019, 40(5): 1-12.

[3] 何菲. 中台战略能否重构阿里[J]. IT 经理世界, 2016(6): 21-23.

[4] 江秀臣, 刘亚东, 傅晓飞, 等. 输配电设备泛在电力物联网建设思路与发展趋势[J]. 高电压技术, 2019, 45(5): 1345-1351.

人民邮电出版社

企业混合云环境数据级容灾的研究与应用

邵腾刚，卓弋凌，李丙超
（中国广核电力股份有限公司信息技术中心，广东 深圳 518124）

摘　要：随着企业信息化的不断发展，企业业务对信息系统的依赖性越来越高。搭建信息系统容灾机制保障信息系统的高可用性和数据安全性成为信息化建设的重要课题。介绍了灾备级别分类和主要技术，提出了混合云数据级灾备建设方案，针对利用公有云搭建云灾备和为公有云搭建灾备机制，提供了不同层面的可行方案，并对公有云搭建灾备两地三中心搭配模式进行了对比。

关键词：数据级容灾；混合云；公有云

1　引言

信息系统对企业业务开展的支撑作用越来越显著，数据的安全、可用以及业务连续性保障要求随之不断被提到，已经上升到法律层面的高度，网络安全法[1]要求：对重要系统和数据库进行容灾备份。在传统的信息化架构中，针对企业自建数据中心已经形成了成熟的灾备方案，如同城灾备、异地灾备、两地三中心模式等。云计算的发展，特别是公有云的广泛使用，形成了企业混合云的新型的信息系统运行环境，给灾备方案带来了新机遇和新挑战：如何使用公有云搭建灾备环境以及如何为公有云搭建灾备环境。

2　灾备级别分类和主要技术

信息系统灾难恢复规范[2]根据灾备机制所能达到的 RPO 和 RTO 指标，分为 1~6 级[2]，数据级容灾一般做到第三级，应用级容灾达到第五级和第六级。

从地域建设模式划分，灾备划分为同城灾备、异地灾备、两地三中心灾备 3 种模式[3-4]。

从灾备效果划分，灾备分为数据级容灾备份、应用级容灾备份、业务级容灾备份 3 个等级，其中前两个级别属于 IT 系统层面的容灾[5]。

其中，应用级容灾主要由备用环境设备、数据复制机制、灾备切换机制等部分组成，其核心是数据复制机制，分为数据库层面复制、操作系统层面复制、存储层面复制等层次，根据数据的同步效果分为实时同步、准实时同步、异步等级别。数据级容灾，和应用级容灾相比，不需要配置系统运行的备用环境，只需要将数据复制到灾备中心保存。根据复制的数据实时性差异，分为备份数据复制和实时数据复制两种。

3　混合云数据级灾备建设方案

3.1　使用公有云搭建灾备环境

灾备建设，传统的方式采用建设专门的灾备中心，配置灾备环境的机房、网络、服务器等资源，建设成本和运维成本很高。而且随着需要纳入灾备的业务增加，如灾备中心资源满负荷、扩容难度大，需要新建更大规模的灾备中心。

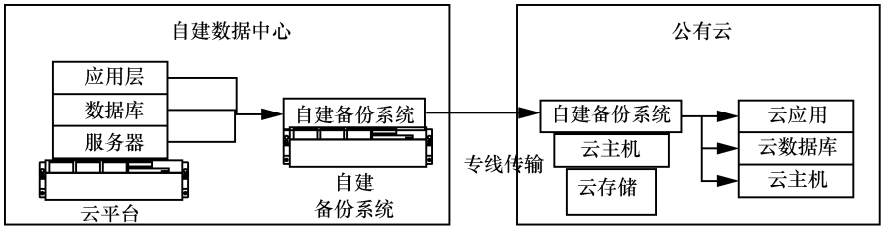
公有云提供了灾备建设的新思路，公有云可以按需申请资源，随着业务增长弹性扩容等优势，降低了灾备建设的门槛。同时，在灾备资源配置上，日常可以采用较低的资源配置，在需要启用灾备环境时，快速弹性扩容，进一步降低灾备运维的成本。

本文重点介绍如何利用公有云搭建数据级容灾环境，应用级容灾和业务级容灾暂不展开介绍。

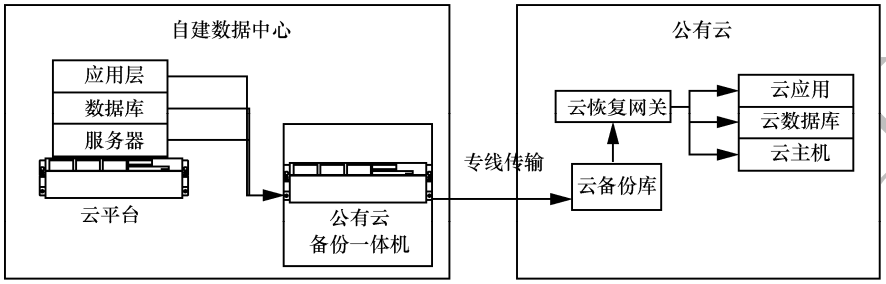
利用公有云实现备份数据复制层次的数据级容灾，主要有以下两种方式。

- 仅使用公有云的服务器和存储资源，采用自建的数据备份系统，在公有云搭建一套数据备份系统站点，同步备份数据。自建备份系统方案如图 1（a）所示。
- 使用公有云提供的备份数据级容灾方案，在私有云数据中心部署容灾一体机，直接对生产环境数据进行备份，并将备份数据同步到公有云环境。公有云整体备份数据级容灾方案如图 1（b）所示。

人民邮电出版社



(a) 自建备份系统方案



(b) 公有云整体备份数据级容灾方案

图 1　公有云备份数据级容灾两种方式

自建备份系统方案采用自身熟悉的备份系统实现，和自建灾备中心建设数据容灾方案一致，但需要自建的备份系统支持公有云部署；而公有云整体备份数据级容灾方案，全面使用公有云的完整方案，建设门槛低，但需要熟悉公有云数据容灾系统的使用。

数据级灾备除了备份数据复制层次之外，还有实时数据复制层次的灾备方式[6-7]。在传统的自建数据中心容灾方案中，可以通过应用系统层次、数据库层次、文件系统层次、操作系统层次、虚拟化平台层次、存储层次实现实时数据的容灾复制[8]。但在公有云环境中，部分层次的数据复制受限制，甚至不可用，对此 6 个层次的灾备复制技术对比和公有云灾备适用性分析，见表 1。

采用公有云搭建实时数据级的容灾，可以采用应用、数据库、文件系统和操作系统层次的数据灾备技术，而基于服务器虚拟化层次的复制技术受限制，仅限于私有云和公有云采用同等的虚拟化 Hypervisor。而公有云底层存储硬件并不直接提供管理，存储系统

表 1　6 个层次的灾备复制技术对比和公有云适用性分析

复制技术	适用范围	数据一致性	带宽	公有云适用性
基于应用的复制技术	全面保护：包括数据库、中间件、前端应用的数据	高：完全确保系统的数据一致性	低	适用
基于数据库的复制技术	仅针对数据库数据	中：确保数据库数据的一致性	较低	适用
基于文件系统的复制技术	适用于 DFS 等分布式文件系统	中等：确保底层存储数据的一致性	中等	适用
基于操作系统的复制技术	全面保护：包括数据库、中间件、前端应用的数据	中等：确保底层存储数据的一致性	中等	适用
基于服务器虚拟化平台的复制技术	全面保护：包括整个云主机	中等：确保底层存储数据的一致性	中等	受限制，仅限私有云和公有云采用相同 Hypervisor 的情况
基于存储系统的复制技术	全面保护：包括数据库、中间件、前端应用的数据	中等：确保底层存储数据的一致性	中等	不适用

层面的复制技术不适用。总体实时数据层次公有云容灾方案如图 2 所示。

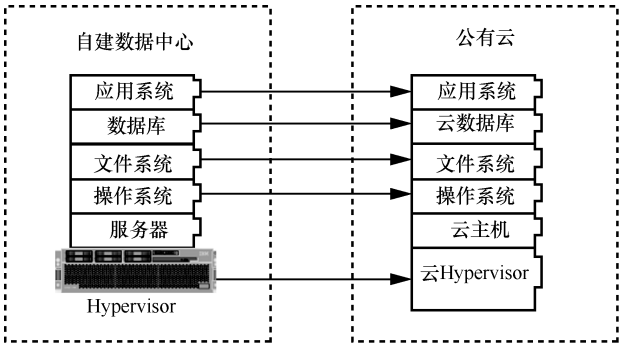


图 2　实时数据公有云灾备方案

实时数据公有云灾备方案，是一种数据级灾备，同时也是应用级灾备的实现前提，在此基础上补充灾备服务器环境资源、灾备环境应急切换方案等，就能实现应用级灾备。

前文介绍的利用公有云搭建灾备环境的方式，是灾备的基本形态，根据公有云和自建数据中心的距离设定要求，可以选择公有云的可用区域位置，满足同城灾备、异地灾备的要求，再进一步设定 2 个公有云区域实现灾备的两地三中心形态。

3.2　为公有云搭建灾备环境

在企业混合云架构中，公有云上也部署了应用系统的生产环境，这部分应用系统也存在建设灾备的需求。

为公有云上部署的系统搭建灾备[9-10]，根据灾备环境的建设位置划分，有 3 种方式，如图 3 所示。

第一种方案，采用同一公有云服务商的不同可用区域搭建，此方式最为简单，只需要采用云服务商的灾备服务，将数据灾备复制到另一个可用区域。此方案优势在于生产环境和灾备环境云平台一致，建设门槛低，同时由于两端都是公有云，其资源配置可弹性扩展，前期只需要配置必需的资源，建设和运维成本低。

第二种方案，采用不同公有云服务商的公有云搭建。和第一种方案相比，也具备生产环境和灾备环境均可弹性扩容的优势，建设和运维成本较低。其难点在于采用的灾备系统需要同时兼容两个服务商的公有云部署和灾备复制。其优势在于灾备机制的可靠性更高，避免了同一公有云服务商服务异常，导致灾备失效，生产环境和灾备环境同时不可用。

第三种方案，采用在私有云中建设公有云系统的灾备。此方式将灾备环境部署在私有云，从企业角度来说，数据存放一份在自建数据中心，可以防止公有云服务商异常导致数据丢失的情况。但其对自建数据中心和私有云的资源预留和可扩展性有较高要求。

结合 3 种方案进行搭配，可以采用多种方式搭建

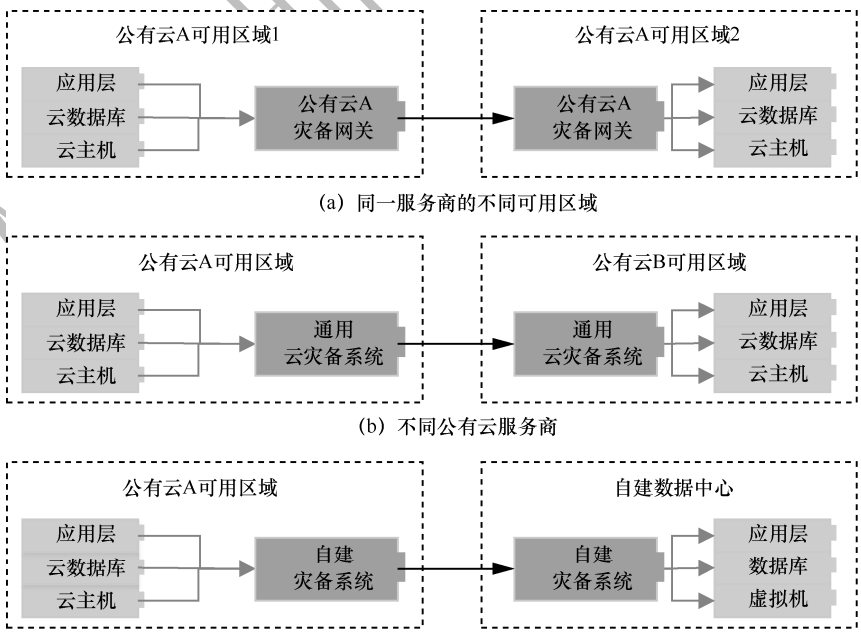


图 3　为公有云搭建灾备环境的 3 种方式

两地三中心模式，可选择的模式见表 2。

表 2　公有云搭建灾备两地三中心搭配模式

序号	同城灾备	异地灾备
1	同一服务商不同可用区域	同一服务商不同可用区域
2	同一服务商不同可用区域	不同服务商的公有云
3	同一服务商不同可用区域	自建数据中心私有云
4	不同服务商的公有云	不同服务商的公有云
5	不同服务商的公有云	自建数据中心私有云
6	自建数据中心私有云	自建数据中心私有云

前文介绍公有云部署的系统搭建灾备的多种实现方式，需要企业根据数据安全性要求、成本和云服务商的服务性能等具体情况，选择合适企业自身条件的灾备方式。

4　结束语

在企业混合云环境中，公有云的引入为私有云容灾如何进行灾备提供了新的可选方案，同时也带来了公有云上的系统如何容灾的问题。针对利用公有云搭建云灾备和为公有云搭建灾备机制，本文提供了不同层面的可行方案。本文提供的灾备方案仅是数据级灾备方案，下一步需要继续研究，在混合云环境中建设应用级和业务级的灾备方案。

参考文献：

[1] 全国人民代表大会. 中华人民共和国网络安全法[S]. 2016.

[2] 全国信息安全标准化技术委员会. 信息安全技术——信息系统灾难恢复规范[M]. 北京: 中国标准出版社, 2007.

[3] 金安,一种同城双活容灾系统设计与实现[J]. 软件导刊, 2018, 17(8): 149-152.

[4] RU W, FAN C J, XIE Q, et al. Research on evaluating information system disaster recovery planning based on the hall three-dimensional structure[C]//2018 4th International Conference on Mechatronic Systems and Materials Application(ICMSMA 2018), 2018.

[5] 吴灿星. 数据容灾备份系统建设分析[J]. 数字通信世界, 2018(8): 145-146.

[6] SINGHA R. A multi-site disaster recovery solution based on IP storage networking[C]//2012 International Conference on Information and Computer Networks (ICICN 2012), 2012.

[7] ZHONG H H, WANG Z X. The method of multi-point data backup in disaster recovery systems[C]//2012 International Conference on Image,Vision and Computing(ICIVC 2012), 2012.

[8] CHEN X, ZHANG L J, CHEN J Y. The design and implementation of disaster recovery in dual-active cloud center[C]//International Conference on Information Sciences, Machinery, Materials and Energy（ICISMME 2015）, 2016.

[9] HONG Y G. Research on data recovery technology in disaster tolerance and recovery system[C]//2016 3rd International Conference on Management Innovation and Business Innovation(ICMIBI 2016), 2016.

[10] WEI C. Disaster recovery of online system based on cloud computing[C]//International Conference on Material Engineering & Application(ICMEA2016), 2016.

人民邮电出版社

企业能力开放平台的研究与应用

马兴，闪烁
(中国广核电力股份有限公司，广东 深圳 518031)

摘　要：经过多年“烟囱式”系统建设，重复功能建设和维护带来重复投资，企业在打通“烟囱式”系统的集成和协作成本高昂，系统建设不利于业务的沉淀和发展。企业能力开放平台成为企业转型的最佳选择，平台的落地有助于形成可持续运营的核心能力，支撑了企业的互联网变革和数字化转型。

关键字：能力开放平台；AEP；运维

1　引言

在传统的系统建设模式下，功能复用没有从全局的角度考虑，每个新系统的上线都预示着一座新的“烟囱”系统被建设起来。完全基于业务需求建设系统的方式已经成为过去企业集团建设信息化项目的标准流程，这导致早期进行 IT 系统建设的企业内部“烟囱林立”。发展到今天，企业受制于巨大的改造成本很难实现互联网转型。企业服务总线（enterprise service bus，ESB）可以很好地解决系统集成问题，但同时 ESB 也面临系统打通的成本高昂，以及大量的协同和开发成本问题。此外，从发展的角度考虑，ESB 不利于业务的沉淀和持续发展。

企业能力开放平台（ability enablement platform for enterprise，AEP）的理念本质上是服务共享。通过服务共享，减少重复建设带来的成本浪费的同时，弥补 ESB 服务灵活性不足的问题，构建共享服务体系，培育业务创新的平台。

2　企业能力开放的源起和构建思路

“能力开放”是赋能和数字产品资产化的过程。“企业能力开放”是指企业在整合和利用现有企业核心能力资源的基础上，采用统一的多层级的开放接口来开发企业核心能力，聚集企业内外有潜力和创造力的开发者，使得开发者能利用这些能力不断地创造出更好的应用和服务，以创新应用和服务促进企业发展和转型的过程。伴随着信息化建设的持续深入，越来越多的企业意识到能力开放不仅仅是技术层面上的变革，更多的是企业信息化建设的重大观念变革。以某企业集团为例，了解企业能力开放的概念后，迅速发现企业信息化建设方向上存在的问题，意识到信息化建设不单是根据业务需要开发系统，更重要的是通过核心能力的沉淀，更快、更好地支撑和引领业务的变革。

企业能力开放的本质是企业能力汇聚、开放和运营的过程，遵循这一思路，构建企业能力开放平台首先需要汇聚现有的能力。能力汇聚可以将信息化建设积累的公共软件资产作为能力汇聚的起点。以某集团为例，能力开放平台是由集成了常见业务场景和流程功能的开发平台（developing platform，DP）和聚合了常用公共组件和服务的应用软件中心（application software center，ASC）发展演变而来。能力的开放和运营是企业能力开放平台的生命线，其中开放可以体现能力的价值，开放能力需要一系列的底层技术变革作为支撑；而运营使能力保持持久的体现价值，需要业务运营团队根据业务需求不断创新，直至引领业务需求。

3　企业能力开放平台的设计与实现

某企业集团的业务架构如图 1 所示，可以看出该企业的信息化程度较高，规划也基本完善。但同时也能反映一些问题：整体的计算资源的利用率比较低；“烟囱式”的建设比较普遍，大多系统包括共用的功能都是单体部署等。该企业的 SOA 实施属于典型的“自上而下”的建设模式，各个需要提供服务封装和改造的系统处在各自的运维期，运维人员缺乏积极性，当新的业务系统期望原有服务得到改造时，运维团队在传统的运维求稳的理念下，大多会放弃对新业务的支持。这种情况下，一方面需求方不得不重新实现该功

人民邮电出版社

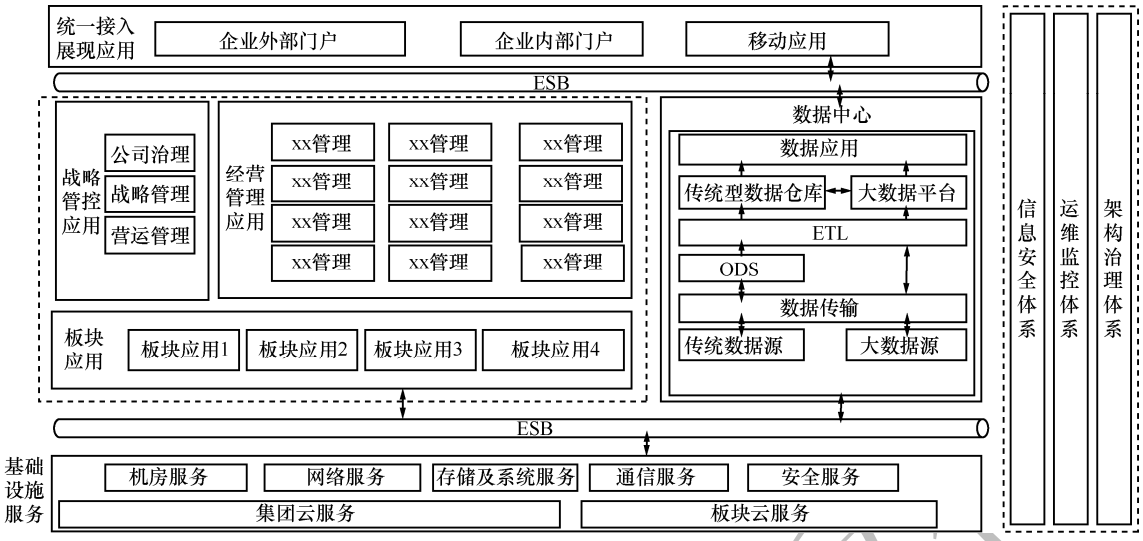


图 1　某企业集团业务架构

能，产生新的烟囱；另一方面受限于服务设计通用性和前瞻性不足，对现有服务做了大规模的改造，耗费较大工作量。这也导致 IT 系统建设中实现的业务得不到沉淀和持续发展。

综上，企业能力开放平台的架构应该摆脱“烟囱式”建设模式的限制，回归 SOA 的本质，通过共享服务的模式来规划企业能力开放平台。

3.1　企业能力开放平台的分层结构

从能力汇聚的角度出发，企业能力开放平台从顶层设计层面对 IT 架构进行调整。能力开放平台涉及多种技术和功能层次，为从根本上解决传统单点部署造成的性能孤岛、数据孤岛和资源利用率低等问题，IT 架构引入分布式的架构和相关技术，其中：在传统基础设施的基础上进行容器化；存储层做了高可用的数据库方案，支持读写分离；中间件层提供支撑高并发、高可靠的集群部署能力；应用层面采用微服务架构，支持水平伸缩；接入层做了统一的转发和缓存，响应更加快捷。除此之外，在容器云和应用之间，引入容器云管理、微服务治理和 DevOps 治理体系，形成了相对完整的分布式 IT 架构方案，可有效支撑能力开放平台的落地建设。企业能力开放平台的分层结构如图 2 所示。

3.2　企业能力开放平台的功能架构

参考企业能力开放平台的分层结构，某集团的能力开放平台的功能架构包括基础的 IaaS 层、容器云平台、DevOps 平台、服务治理平台和共享服务中心，具体如图 3 所示。

IaaS 层：企业内部的私有云已全部进行了虚拟化，与公有云通过专线进行连接，基础设施资源通过容器云平台实现了资源池化的管理，汇聚了基础设施的能力。

容器云平台：提供基于容器的运行引擎，以及基于 Mesos、Kubernetes 的容器调度方案，解决开发、测试、运行环境统一、服务快速部署，运行期服务管理、调度的问题。提供物理机、虚拟机、私有云、公有云统一接入的能力，屏蔽基础设施层的复杂性。

DevOps 平台：提供开发运维一体化平台，解决业务敏捷响应、产品快速发布的问题，支撑微服务架构下的应用监控，自动化运维管理。

服务治理平台：提供微服务架构编程模型和最佳实践，基于服务日志的全链路监控、统计和分析的能力。

共享服务中心：该企业的共享服务中心包括多个服务中心，如人资中心、流程中心、授权中心等，随着业务的发展，越来越多的能力汇聚到共享服务中心。

3.3 企业能力开放平台的运营方案

在完成平台搭建和微服务的部署后，接下来重要的一步就是平台的运营，某集团的能力开放平台运营方案包含能力开放和持续运营这两个范畴：在能力开放方面，平台提供了开发者门户来集中展示能力，如在线的文档、在线申请微服务等功能；在持续运营层面有两个重要内容，一是平台提供了加强版的 DevOps 管理平台（整合了微服务治理平台和容器云平台功能）来支撑应用从开发到部署再到运维的流水线作业，大

人民邮电出版社

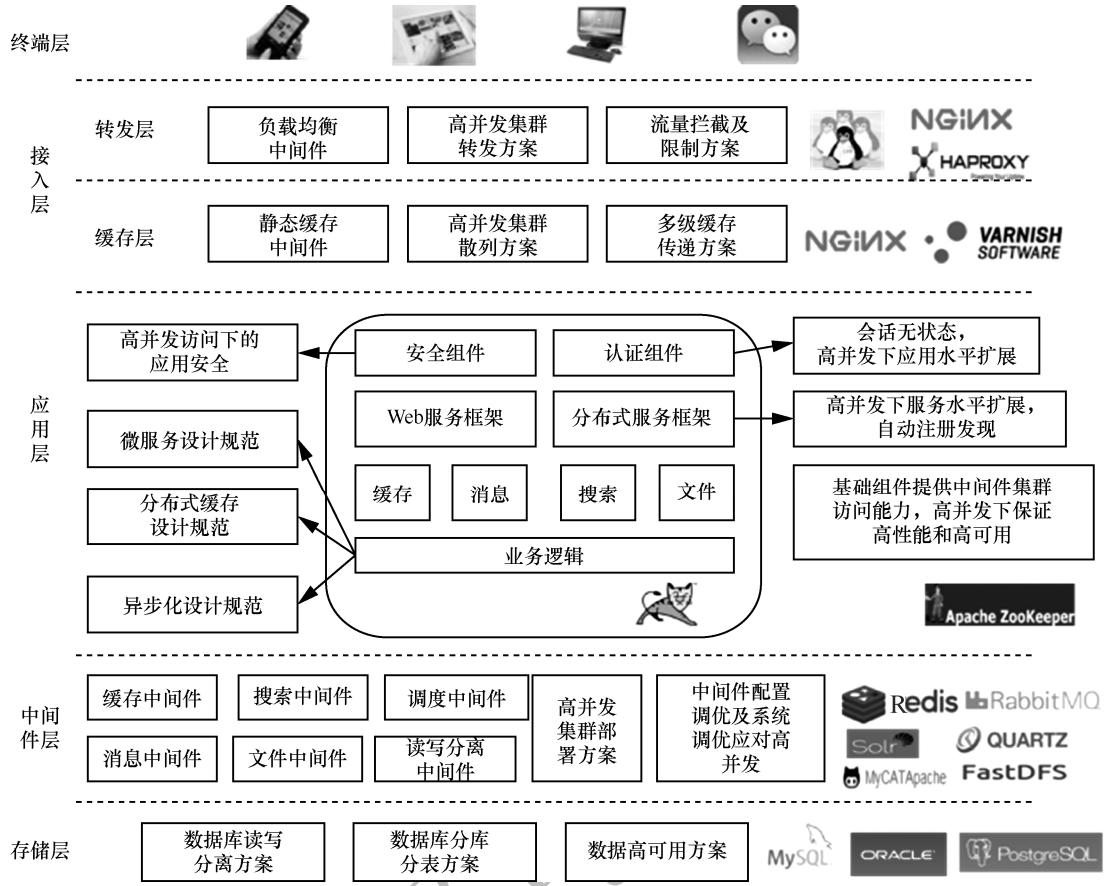


图 2　企业能力开放平台的分层结构

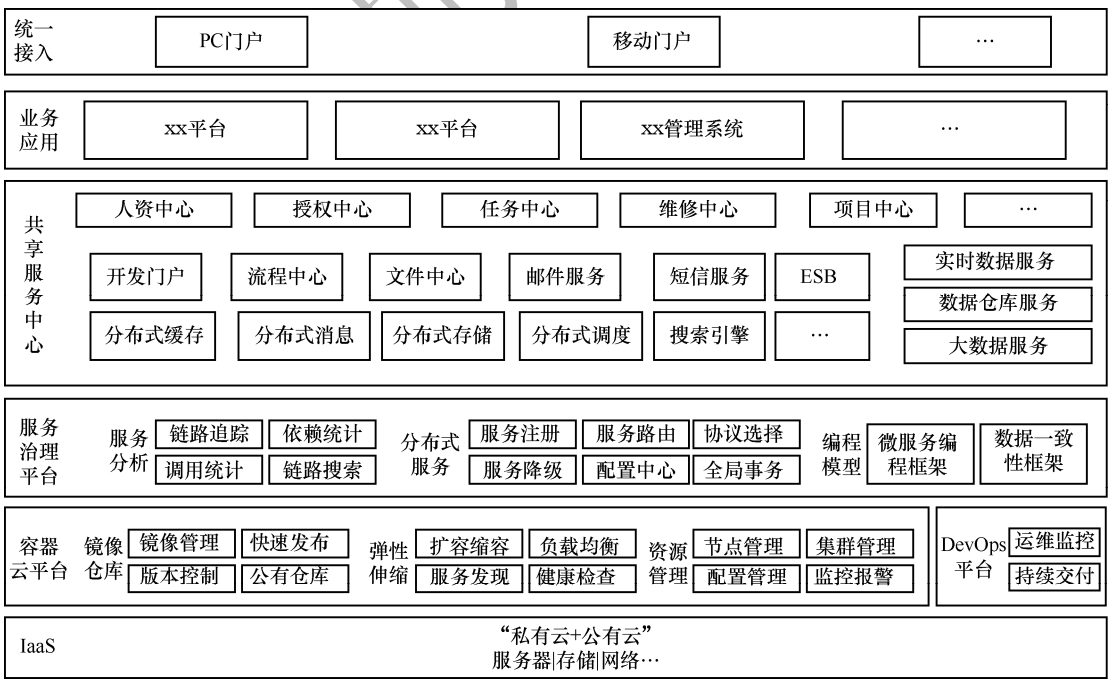
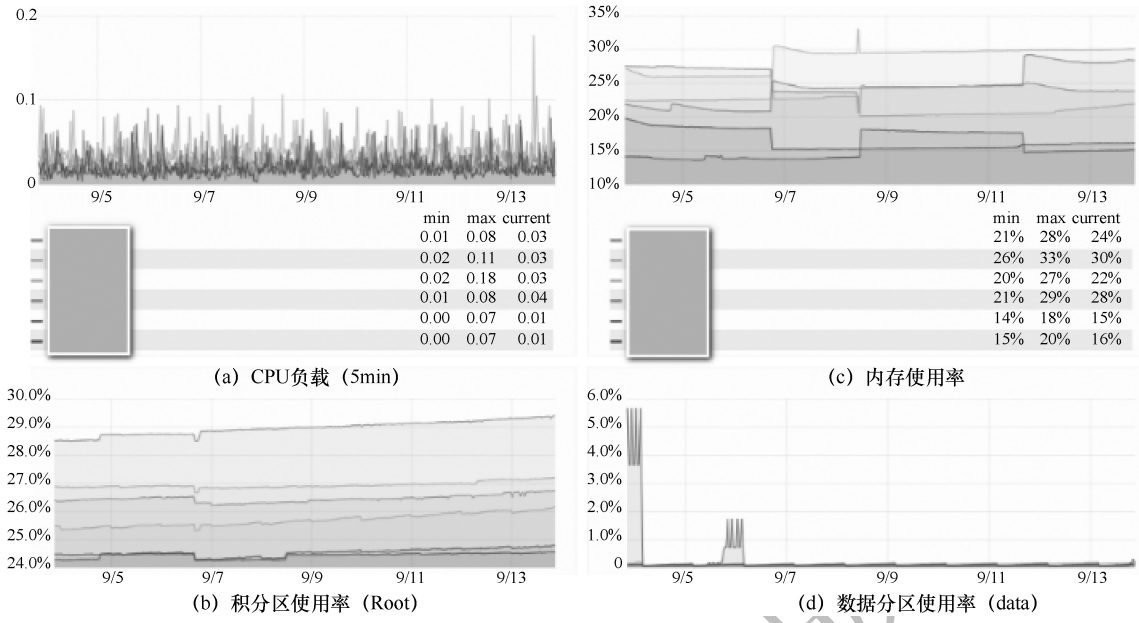


图 3　企业能力开放平台功能架构



(a) CPU负载（5min）　(c) 内存使用率

(b) 积分区使用率（Root）　(d) 数据分区使用率（data）

图 4　资源池监控截图示意（CPU 等的使用情况）

大简化了投产流程，提高了投产的效率和安全性，二是平台提供了能力开放平台运营中心，支撑共享服务中心管理和持续运营。

3.4　企业能力开放平台的初步应用情况

基于以上的平台架构，某企业集团信息部门搭建了基于共享服务模式的能力开放平台，开展了能力开放平台的试点工作，实现了共享服务从开发、部署到运维的流水线作业，同时满足了共享服务的发布和持续运营的需求。图 4 和图 5 反映的是能力开放平台的部分信息。试点阶段，企业能力开放平台实现了服务的全链路监控，可以根据条件查询每一笔交易的详细信息，验证了架构的有效性。



图 5　流水线截图示意（服务部署执行的流水线）

4　结束语

目前已经累计投产 28 类应用，实现了服务的全链路监控，最大限度地保障了服务的高可用性能，满足了企业核心能力开放和运营的基本需求。通过能力开放平台的落地，企业一方面彻底改变了以往“烟囱式”建设一条腿走路的模式，新的项目都基于共享服务模式来建设，项目的建设周期和资源投入效率都有明显的提升；另一方面企业的信息中心可以将组织阵型调整转换成为更高效的共享业务中心，从之前在企业中“业务支持”的职能，转变为基于企业核心业务和数据进行运营的团队，更专注于业务的创新和服务的滋养，从而逐渐掌握企业最核心的业务和数据，为企业培养“业务+技术”的复合型人才。

参考文献：

[1] 陈德华, 潘乔, 王梅, 等. 数据自治开放应用平台设计与实践[J]. 大数据, 2018, (2): 63-71.

[2] 辛笛. 电信企业 IT 能力开放平台解决方案[J]. 通讯世界, 2016 (4): 30-31.

[3] 赵习亮. 能力开放平台方案探讨[J]. 电信技术, 2017(5): 74-80.

[4] 钟致民, 梁峥. 如何打造能力开放平台[J]. 通信企业管理, 2017 (1): 38-42.

[5] 李文明, 崔俊交, 贾宏举. 业务支撑能力开放平台的设计与实现[J]. 电信工程技术与标准化, 2017, 30(7): 31-36.

[6] LUO J, VAN D V A H, JING R, et al. Transitioning from a hierarchical product organization to an open platform organization: a Chinese case study[J]. Journal of Organization Design, 2018, 7(1).

已录电出版

前景理论下分布式发电市场化交易卖方市场行为的预测

那峙雄[1]，王晓岚[2]， 马大燕[1]，沈文涛[1]，孟凡腾[1]
（1. 国网电子商务有限公司，北京 100053；2. 国电科技环保集团股份有限公司，北京 100022）

摘　要：任何市场要素的变化，均会直接反映到市场价格上来，过高或者过低的市场价格都会使得市场难以为继。基于行为经济学中前景理论，提出了不同价格锚点条件下，同一地区存量和新增的发电企业参与分布式发电市场化交易时的卖方市场行为预测；得出在假定电力需求具有价格弹性时，充分利用各个时段的可消纳容量可实现分布式光伏电站总收益最大化，“自发自用、余量上网”消纳方式更具备经济性的特点下，电力市场现货模式可促进卖方参与。该研究能够为我国电力交易监管机构制定与完善分布式发电市场化项目交易规则提供重要参考。

关键词：分布式发电；电力市场；前景理论；行为预测；现货市场

1　引言

2019年5月中华人民共和国国家发展和改革委员会、国家能源局联合发布了《关于公布2019年第一批风电、光伏发电平价上网项目的通知》（发改办能源〔2019〕594号），并公布了2019年分布式发电市场化交易试点名单。这标志着从2013年就已经提出的以“隔墙售电”为主要交易模式的分布式发电交易，正式进入试点落地阶段。另一方面我国电力市场化改革仍处于起步阶段，电力市场的交易规则、监管制度、市场机制等问题有待进一步研究和完善。保障分布式电力市场可持续健康发展的的交易规则，必然符合并体现经济学的两个核心概念，一是经济主体会追求最优化；二是市场会达到均衡[1]。这个市场也必然是电力（电量）这种商品进行交易并且确定显性价格的一种正式渠道[2]。

本次试点名单中能源供给类型为可再生能源中的风电和光伏，这与我国已经开展的电力交易、电源物理特性而言：具有能量密度低、单机容量小和出力特性上的间歇性、波动性。其中分布式光伏电站作为目前分布式发电市场化交易中最常见、分布最广泛、发展最迅速的类型，以其作为代表对象展开研究分析。从电力市场的消费者而言，以更加低廉的价格获得可靠的电力服务是其核心需求所在，而作为卖方参与积极程度与满足这种需求其可接受的电价直接相关，故有效预测分析在电价变化下卖家市场行为模式是形成市场均衡显性价格体系的重点所在。依托笛卡尔建构主义思想，应用行为经济学中前景理论进行预测给出分布式电力市场供给侧中的卖方为追求最优化而形成价格均衡的市场行为，同时也为分布式发电市场化交易规则制定完善提供参考。本文因篇幅所限没有展开讨论市场力的问题。

目前在可再生能源的电力市场监管规则与经济学应用在电力市场领域进行的研究主要有。

参考文献[3]引入了行为经济学的研究方法，通过心理学测试结果以及实际报价数据之间的比较观察，发现决策人风险度偏好曲线和决策人报价调整量之间有着相同的变化规律，这一发现为研究决策人风险偏好问题开辟了新的思路；

参考文献[4]重点关注电力市场监管对发电技术的影响，包括立陶宛和波兰的可再生能源。 旨在确定监管和非监管因素如何影响投资者的选择。分析的主要结论包括：改革理由背后的主要推动力； 电力改革特点；电力市场改革对电价和电力市场改革的影响以及影响投资者对特定发电技术或技术组合的选择的非改革相关因素。

参考文献[5]提出购电用户间进行合同电量交易来完善辅助交易市场及发展电力期货市场两个方面来

基金项目：国家重点研发计划资助项目（No.2018YFB1500805）

完善电力市场体系以对电力市场价格波动进行管理研究。

参考文献[6]提出在竞争性电力市场环境下，采用特殊的价格政策和机制，可以起到鼓励可再生能源发电市场发展和带动技术进步、产业升级的效果。

参考文献[7]以我国电力价格规制为研究对象，运用规制经济学中的激励性规制理论、一般的经济分析方法和博弈论的有关分析方法，对我国的电力价格规制的演进、现状和存在的问题原因进行分析，针对问题改革现有电力价格定价的不足之处，提出实施竞争机制、全面落实竞价上网、改善价格结构、引入激励性竞争机制、完善法律法规建设和监管机构的监管职能。

参考文献[8]在参考借鉴国际成熟电力市场经验和对国内部分地区电力市场实践进行调研的基础上,对后续改革应继续加强顶层设计,完善电力市场体系、丰富交易品种,建立科学高效的交易规则和价格机制,加强与市场化改革相适应的政府价格管理等方面进行思考并提出相关建议。

参考文献[9]介绍了北欧电力交易所 Nord Pool 推出的远期位置价差产品差价合约（CfD）的定价分析。分析得出远期合约的定价理论通过大多数厌恶风险的消费者的存在来解释这一点，这些消费者愿意为接收未来的价格差异支付风险溢价。

参考文献[10]分析得出与供应商的瞬时边际成本相等的时变价格可能无法实现社会最优，而且消费者需求波动应该适当定价。并提出了一种动态定价机制，明确鼓励消费者调整消费，以抵消传统单位需求的变化。通过动态博弈论公式，证明了（在适当的凸性假设下）所提出的定价机制渐近地实现了社会最优性，随着消费者数量增加到无穷大。

2 研究分析

2.1 加州能源危机的二则启示

在 2000—2001 年发生在美国加利福尼亚电力危机，最终导致该州能源成本提高到历史水平的 10 倍，州内电力紧缺和轮番停电，该州最大的电力公司、电力交易所和许多小型发电商破产，该危机使得当时在美国正在进行的电力改革停顿下来[11]。

加州能源危机虽然过去近 20 年了，但它对我国正在开展的电力市场改革依然具有非常大的启示意义。

（1）交易规则所体现的监管思路需要体现市场价格与卖方因满足市场需要而支付的单位成本并不存在相关性。按照费农·L·史密斯的分析结论，导致加州能源危机的根本原因在于贯穿于此过程中错误的监管思路：价格的功能是用来提供收益，收益的功能是用来补偿成本--因此估算费用和收益并据此定价。实际上一个天然的市场原则在于：市场价格以及由需求决定的任何卖方相应提供的产品数量，决定了卖方能负担得起不至于赔钱的单位成本。如果市场价格是卖方已经能够得到的最好价格了，但仍可能低于其支付的单位成本，结果只能生意失败[12]。

（2）交易规则所体现的规则公正是结果公正的起点，如同乔治·斯蒂格勒提出的一个更深入的问题：各种监管法规的真正目的是什么？他的结论是：大多数的监管机构反倒会被受管辖的企业给“俘获”，而这些机构往往会在牺牲公众利益的情况下让这些企业得到帮助[2]。

一个可持续健康的分布式电力市场，电力交易监管机构制定的交易规则必须公平、公正综合考虑对于不同市场参与者的诉求，并进行有效把握。交易规则作为一种交易机制的制度安排，如何使该制度实现“激励相容”，即电力市场中各参与个体与电力市场化改革整体价值目标统一是关键点所在。进一步讲如何平衡需求侧与供给侧各自价格预期上的矛盾，尤其是分析并预测卖方在此矛盾下的行为模式及由此产生的参与程度，是交易规则助推其市场行为的合理化和实现市场均衡的重要问题。

2.2 价格锚点影响下的卖方市场行为预测

价格锚点是在 1992 年由托奥斯基提出的，该理论最初是分析消费者在对产品价格并不确定的时候，会采取两种非常重要的原则：避免极端和寻求对比，来判断这个产品的价格是否合适。价格锚点就是产品价格的对比标杆。价格锚点的逻辑，就是让消费者有一个可对比的价格感知。这种价格感知按照丹尼尔·卡内曼研究成果[13]表明同样适用于生产者对于自身商品的定价上，由此推论分布式发电厂商因所处地域、建设年代不同，会以不同的电价标准等作为参与电力市场交易的价格对比标杆。这种价格描点将直接导致分布式发电厂商是否作为参与电力交易过程的卖方和参与时的定价决策行为。

假定加州能源危机得出市场电价与成本无关性原则已被预期参与分布式发电市场化交易的卖方所熟知和认可，那么结合上文中的价格锚点其市场行为将会

有何种特征？

前景理论的大量个体决策研究表明的那样，参照个体的初始状态，人类被试对同量的损失和收益表现出非对称的反应模式（损失厌恶）[14]。该理论发现人们在面对得失时的风险偏好行为不一致，在面对“失”时变得风险追求，而面对“得”时却表现得风险规避；参照点的设立和变化影响人们的得失感受，并进而影响人们的决策[15]。基于该理论，假定分布式发电市场化的某个卖方在参与交易前的初始售电收益为 X_0，那么就可以假设效用函数 $u(\cdot)$，对于因参与交易而导致收益偏离 X_0 的情况 dX，都有式（1）成立：

$$u(X_0 - \mathrm{d}X) > \mathrm{u}(X_0 + \mathrm{d}X) \quad (1)$$

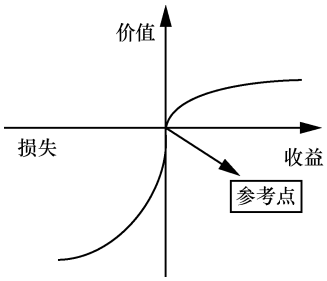


图 1　价值函数[16]

式（1）由图 1 来表示可以看出，决策者对于收益和损失的主观感知是不对等的：相同程度的收益和损失，其对应的价值上升量小于下降量，损失的影响要大于收益的影响。收益的价值函数为凹函数，决策者表现为风险厌恶，相反，损失的价值函数为凸函数，决策者表现为风险偏好[17]，即从效用角度来衡量，付现成本会远重于机会成本，或者说错失收益比同量的实际损失引发的效用变化要小一些。国家发展和改革委员会能源〔2019〕594 号中所规定的“新建项目优先纳入交易，在条件成熟后，存量项目可自愿参与交易（同时放弃国家补贴）”，基于上述理论可预测得出在试点名单对应地区已享受国家补贴的存量分布式发电项目在更加重视付现成本下，放弃国家补贴将面对可能出现收益下降的“失”而导致参与积极性不高，甚至不参与；或其即便参与时其报价水平将至少要保证与目前所“得”售电收益保持一致或有增长。对于新建项目的卖方而言，其选择对标的价格锚点将成为定价行为的决定性因素。

根据相关文献研究指出分布式交易的主要特点之一，即“隔墙”交易，DG 尽可能与电网接入点同一供电电压等级范围内的消费者进行电力交易，实现就近消纳[18]。本文认为正是这个交易特点将导致卖方价格锚点的对标价格极可能为销售电价，即目前现行的居民电价、大工业电价、工商业电价；而对于大多数的消费者而言，价格锚点对标价格将极有可能理解为以“脱硫煤标杆电价”并网且有合理利润为标准。由此买卖双方心理产生完全不同的得失风险偏好行为，交易试点初期交易过程中最终成交电价变化值 dX 将极有可能导致买卖双方巨大的心理落差，这对逐步形成稳定的显性均衡价格为代表的电力市场将直接产生消极影响，也对我国正在大力推动风电、光伏实现以“脱硫煤标杆电价”为特征的平价上网目标实现带来不利影响。

2.3　不同市场化电力电量平衡模式下的卖家市场行为预测

对于分布式发电卖方的准入，市场监督者以实现减少弃风弃光率的目标，根据系统静态条件下的最低可消纳容量来确定电力电量平衡。该容量确定方法基于电力这种特殊商品具有瞬时平衡的物理特点，且电力负荷本身具有很强的随机性与不可预测性的特点，认为电能是一种需求刚性商品，因而价格信号对于电力需求几乎没有影响[19]。但上述论断的逻辑错误在于：在电力分配技术是无弹性的，对价格不敏感，并且发电量不可以自由准入的前提下，是不能得出需求缺乏弹性的结论。本文认为在“隔墙”交易时不考虑线路约束和电力需求响应支持下，电价波动驱使电能需求弹性明显增大。

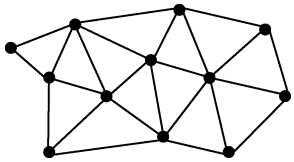


图 2　P2P 交易模型结构[20]

分布式交易中的“隔墙”交易均可被认为是如图 2 所示的 P2P 交易，结合 P2P 交易下卖买双方的日供用电特征，充分利用各个时段的可消纳容量可实现分布式光伏电站总收益最大化[21]。另一方面卖方所在地区实行峰谷电价（或电力现货交易已正式执行时），并且用户用电目录电价与燃煤发电标杆上网电价差值较大，分布式光伏发电自发自用比例将产生显著的影响[22]，在该消纳方式的卖方所占自身发电量的比例越大，光伏发电项目的经济效益越高[23]。

“中发〔2015〕9 号文”配套文件明确定义了中国电力市场建设目标是“现货交易发现价格，中长期交

易规避风险”的现货和中长期交易相结合的市场化电力电量平衡模式[24]。现货市场与中长期市场的协调运行主要体现在时序衔接和交易衔接两个方面。中长期交易的组织一般在现货交易开市前进行，覆盖数年前至月前、周前、数日前等不同时间段[25]。电力市场中的中长期电价就具体一个时间段而言，对买卖双方是唯一并确定的，若卖方收益偏离 X_0 的情况为“失”，那么其将明显表现出厌恶损失，参与度不高，甚至不参与。而现货交易发现价格的特性和上述研究成果，卖方在面对参与中长期交易“失”时，极有可能更愿意在现货交易中表现出风险追求[26]。由此现货电力电量平衡模式更有助于促进卖方的参与活跃度，同时对于吸引已享受国家补贴自发自用存量项目放弃补贴增大参与意愿也将起到积极作用。

3 结束语

如何使分布式发电企业生产的电力（电量）商品的使用标准和信号标准[27]，依托市场化的方式形成符合该商品物理质量特性和经济学价值规律的实现市场均衡的显性价格体系，这是分布式电力市场得以永续健康发展的最为重要的前提。结合论文前述分析，为了减少卖方风险厌恶，有效推动电力市场的交易规则、监管制度、市场机制的进一步完善，建议应考虑以下几方面。

（1）在充分尊重分布式发电卖方企业自身参与意愿的基础上，做好本地区分布式发电市场化交易开展前的价格锚点的认知引导与梳理，并在集中竞价时考虑第二价格密封拍卖法的应用；

（2）在分布式市场化交易 P2P 场景下应加快推进建设现货市场，从国外分布式交易现状来看，随着电力交易逐渐从中长期向短时交易推进和系统中间歇性 DER 比例的提高，对满足供需实时平衡的要求会愈加紧迫。针对分布式可再生能源电站的出力物理特征和商品价格发现需要，可积极考虑建立以区块链技术为支撑的现货电力电量平衡市场模式；

（3）积极引导自发自用分布式光伏电站作为主要卖方，为提高分布式可再生能源电站的发电质量和数量，应考虑推动其应用提升设备可用率、降低非计划停机时间为目标的智慧运维技术，并作为参与市场竞价附加条件；

（4）实现快速需求响应是电网维持稳定和可靠的关键，结合目前国家电网正在开展的泛在电力物联网项目，对于卖方准入条件标准时可考虑对已安装可降低分布式电力现货交易时电力调度复杂性，提升需求响应及时性的边缘计算装置的电站优先。

参考文献：

[1] 理查德 •泰勒. “错误”的行为[M]. 王晋,译.北京:中信出版社, 2016: 52.

[2] 加里 • 贝克尔, 吉蒂 • 贝克尔. 生活中的经济学[M]. 章爱民, 徐佩文, 译. 北京: 机械工业出版社, 2013.

[3] 孙志明. 基于实验经济学的电力市场竞价模式及报价策略研究[D]. 浙江: 浙江大学, 2004.

[4] STREIMIKIENE D, SIKSNELYTE I.Electricity market opening impact on investments in electricity sector[J].Renewable and Sustainable Energy Reviews, 2014, 29: 891-904.

[5] 伏开宝. 电力体制改革中市场价格波动管理研究[D]. 上海: 上海社会科学院, 2018.

[6] 时璟丽. 关于在电力市场环境下建立和促进可再生能源发电价格体系的研究[J]. 中国能源, 2008, 30(1): 23-26.

[7] 严泽民. 中国电力价格规制改革研究[D]. 辽宁: 辽宁大学, 2011.

[8] 王左权, 曹学泸. 完善电力市场交易价格机制及其监管的思考[J]. 价格理论与实践, 2018, 4: 26-29.

[9] KRISTIANSEN T. Pricing of contracts for difference in the nordic market[J] . Energy Policy. 2003 (9): 1075-1085 .

[10] JOHN N T,YUN J X. Pricing of fluctuations in electricity markets[J] . European Journal of Operational Research . 2015 (1) .

[11] 萨利 • 亨特. 电力竞争[M]. 《电力竞争》编译组, 译. 北京: 中国经济出版社, 2004: 407-424.

[12] 费农 •L • 史密斯. 经济学中的理性[M]. 李克强, 译. 北京: 中国人民大学出版社, 2013(2): 35-37.

[13] 丹尼尔 • 卡尼曼. 思考，快与慢[M]. 胡晓姣, 李爱民, 何梦莹,译. 北京: 中信出版社, 2012:166.

[14] 费农 • L • 史密斯. 议价与市场行为:实验经济学论文集[M]. 阮傲, 赵俊, 董志强, 译. 上海: 上海人民出版社, 2017(5): 23-25.

[15] 陆雄文主编. 管理学大辞典[M]. 上海: 上海辞书出版社, 2013:389.

[16] 谭阳红, 张婧, 李肖. 基于复杂网络理论的电网节点重要度评估[J]. 计算机工程, doi: 10.196781j.issn.1000-3428.00530.

[17] 潘俊涛, 彭建春, 孙芊, 等. 基于前景理论的发电商电量分配策略[J]. 电网技术, 2011, 35(4): 170-175.

[18] 林俐, 许冰倩, 王皓怀. 典型分布式发电市场化交易机制分析与建议[J]. 电力系统自动化, 2019,43(04):1-8.

[19] 曾伟民. 在电力市场中引入电力需求弹性的研究[J]. 电网技术, 2008, 43(4): 84-89.

[20] 林俐, 许冰倩, 王皓怀. 典型分布式发电市场化交易机制分析与建议[J]. 电力系统自动化, 2019,43(4): 1-8.

[21] 程临燕, 冯艳虹, 徐林汪, 等. 寿命周期内光伏电站收益最大化建设规模研究[J]. 电力勘测设计, 2018, (S2): 256-260.

人民邮电出版社

[22] 马溪原, 郭晓斌, 周长城, 等. 电网公司投资分布式光伏发电系统的典型运营模式分析[J]. 南方电网技术, 2018, 12(3): 52-59.

[23] 陈梓毅, 曹烨, 邱国玉. 城市分布式光伏发电的经济和环境效益实证分析[J]. 生态经济, 2018, 34(6): 100-105.

[24] 国家发展改革委. 电力中长期交易基本规则[R]. 2016.

[25] 史连军, 邵平, 张显, 等. 新一代电力市场交易平台架构探讨[J]. 电力系统自动化, 2017, 41(24): 67-76.

[26] 刘达，牛东晓，李媛媛，等. 基于周期波动及其影响分析的电力市场中长期电价预测[J]. 中国电机工程学报，2009,29(13): 80-85.

[27] 迈克尔·波特曼. 竞争优势[M]. 陈小悦译. 北京: 华夏出版社, 2007: 140-142.

人民邮电出版社

轻量级自动化巡检系统开发和实践

曹小明
（南方电网数字电网研究院有限公司，广东 广州 510000）

摘　要：随着南方电网信息化建设进程的不断加快，信息系统部署逐步由两级转变为集中或一级部署，南方电网数字电网科研院有限公司运维服务团队承接的信息系统越来越多，对运维工作的精益化水平提出了更高的挑战。Hubble 智汇运维系统是数研院公司运维服务团队自主研发的轻量级自动化巡检系统，是运维“脚本化”走向“Web化”的标志产品。它是一套基于 Bootstrap+Django+Python 的技术解决方案，提供了完善的前后台开发框架、调度引擎、公共组件等模块，也是 Devops 运维敏捷开发的试金石，还能落地运维管理数据和提高管理水平，承担着几十套重要系统线上运营的使命。

关键词：轻量级；自动化巡检；Bootstrap+Django+Python；Devops 敏捷开发

1　引言

随着南方电网公司业务的高速增长和信息化建设进程的不断加快，信息系统部署的模式逐步由两级部署转变为集中部署或一级部署，进而配套的运维模式也逐渐向一级运维模式转变。随着南方电网数字电网科研院有限公司（下文简称数研院公司）运维服务团队承接的信息系统也逐步增多，对信息系统运维工作的精益化水平提出了更高的要求和挑战。

当前采用人工巡检的方式对信息系统进行每日多次巡检，巡检范围包括网络安全设备、服务器存储、备份系统、操作系统、数据库、中间件以及业务系统 URL 等，占用大量的人力资源和时间资源。每次巡检都是较大规模的机械重复性劳动，人工巡检会因注意力下降等非技术因素发生误操作，造成巡检结果的偏差。

自动化的巡检方式通过采用系统自动巡检，提高了巡检效率，节省了人力成本，并且通过预先设计的脚本，提高了巡检的准确率。结合自动化运维发展趋势，通过自动化巡检的操作展示可视化，提高了系统的扩充性和稳定性，方便了巡检人员第一时间了解系统应用的运行状况。

2　现状分析

2.1　日常痛点

（1）日常运维巡检人工占比大，任务重复机械性强，巡检效率低。

（2）巡检非智力化因素导致结果偏差比重大。

（3）现有运维工具系统专业性强，门槛较高不易上手，持续迭代能力弱。

（4）工具系统独立分散部署，业务纵向性关联弱，壁垒高。

（5）缺少统一工作平台界面，沟通成本大，且运营数据质量较差。

（6）工具系统支撑率较低，部分领域覆盖不全。

2.2　面临挑战

（1）业务系统数量快速激增，功能和系统间耦合度日趋错综复杂。

（2）故障时无法快速定位，陷于填坑救火中无法自拔。

（3）新技术更新迭代快，开源文化氛围百花齐放，学习能力和成本要求高。

（4）传统开发模式无法快速响应业务高频率迭代的需求。

（5）持续交付能力受组织架构和流程制度较重的阻滞，需要敏捷和精益化瘦身。

（6）工具系统和人员提高用户满意度的同时，兼顾运营数据质量。

3　系统设计

目前市场和社区存在不少开源的自动化运维系统和项目，好处是可以直接下载安装部署使用、不需要

人民邮电出版社

二次开发；缺点是代码不可控、功能臃肿、用户体验不友好等。加上根据南方电网公司信息化安全要求以及实际生产环境考虑，无法直接使用开源的自动化运维系统。与此同时，数研院公司运维服务团队承接建设的 IT 一体化运维系统距离落地投入使用仍有一段时间，运维服务团队成员需要提前做好技术储备和尝试采用 Devops 敏捷运维思想进行轻量级系统开发。

3.1 需求分析

针对运维工作中的日常痛点和面临挑战及系统定位，确认用户大致需求如下。

（1）应用、数据库、中间服务器和存储等相关邻域日常巡检定时脚本化采集指标数据，并自动按照相关时间粒度形成总览报告。

（2）总览报告可钻取看到具体系统或服务应用实例的巡检详情。

（3）支持历史数据巡检报表查询和导出。

（4）支持保供电时期的特殊运行方式巡检。

（5）支持安全加固基线检查和一键加固。

（6）从用户角度的用户仿真功能巡检。

3.2 系统设计

在 Hubble 智汇运维系统（下文简称 Hubble）的功能开发中，考虑到整个项目开发仅有 2 人，甚至 1 人还要把 40%的时间给到其他运维工作支配的情况，因地制宜借鉴和取舍了敏捷开发方法论 Scrum 和 XP。

- 采用 XP 极限编程方法，在顶层设计和底层架构中集中进行公共模块代码编码和互相测试，同时兼顾负责各自顶功能模块开发。
- 参考 Scrum，每个大功能模块一般都计划 2~3 周的时间算法，并通过小版本快速迭代，提高交付能力，尽可能缩短产品开发周期，让用户尽早参与测试和使用反馈。
- 避免重复造轮子，通过搭建和二次集成开发一系列的 Devops 相关工具链（Gitlab、Jenkins、docker、Bugzila 等），进行快速构建、快速部署和持续集成交付。
- 通过看板，把用户需求和开发进度很好地结合起来，清晰直观地看出每个需求的进展和工作量，方便 Scrum Master 及时调整。

3.2.1 系统架构

Hubble 系统的整体架构采用目前市场上主流、成熟、安全和易扩展的框架：Nginx+uWSGI（Django）+Python。其架构如下图 1 所示。

Hubble 系统后端采集层使用 Python+Paramiko+Shell 框架，通过轻量级 Schedule 调度框架和分布式 Celery 调度引擎按需根据接入对象执行对应的定时任务。兼容大部分的专业巡检数据采集调度，例如 URL、数据库、备份、操作系统。其架构如图 2 所示。

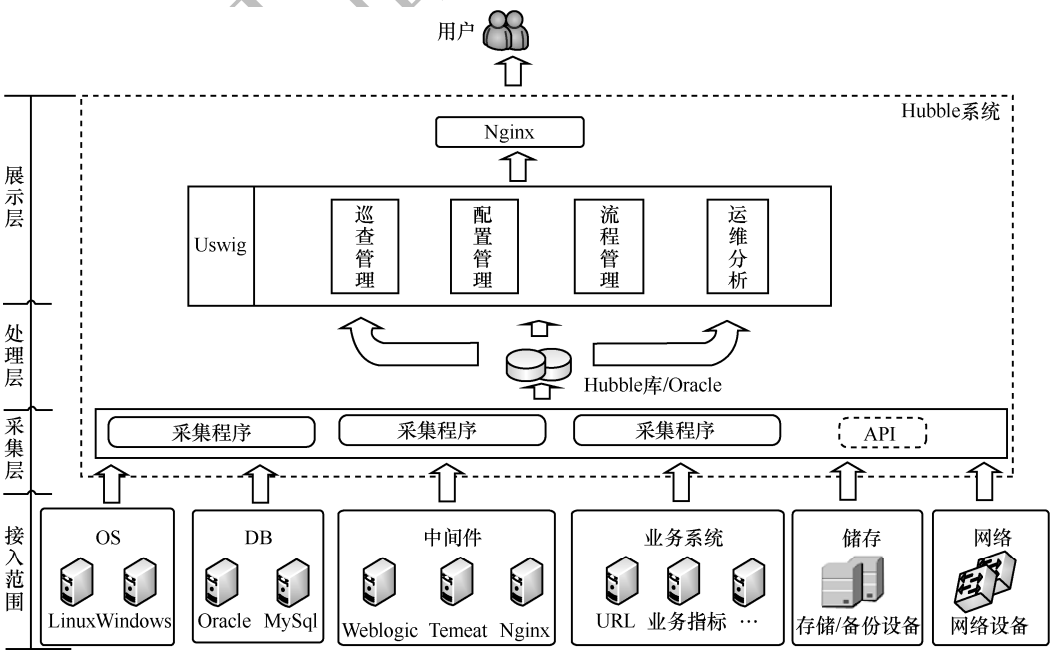


图 1 系统整体架构

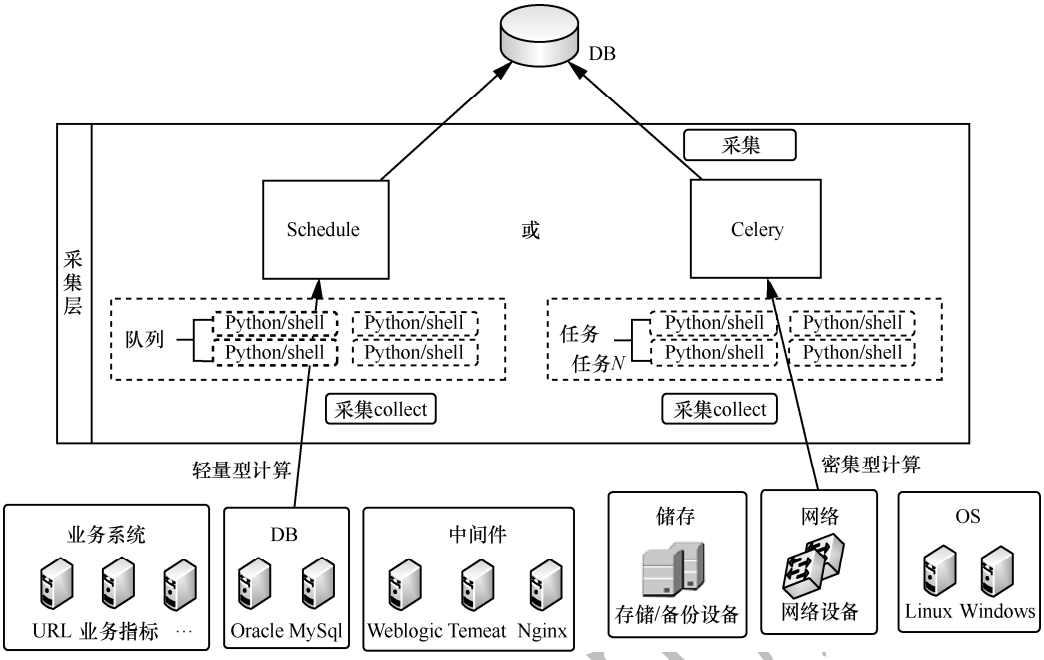


图 2　后端调度架构

针对实际业务生产环境下的用户仿真巡检的后端采集层使用框架：Robotframwork+Selenium2+WebdriverAPI。通过相关框架，业务数据流为：

（1）后端采集层执行定时巡检任务脚本，对用户仿真巡检数据进行调度采集（支持原生的 Selenium2 测试框架 testunit 的 python 用例脚本，也支持基于 Robotframwork-RIDE 开源框架的测试用例文本）,生成 xml 格式的巡检结果原始结果文件；

（2）通过文件同步脚本经过内外网交换平台汇聚原始巡检结果文件；

（3）经过采集解析程序分析入库；

（4）在 Web UI 上进行统一展现。

业务数据流如图 3 所示。

3.2.2　功能设计

通过对需求进行分析和评审后，确认系统重要功能模块如下。

（1）应用系统巡检

此功能模块实现对应用系统的访问地址 URL 进行健康性检测，通过对访问地址的 HTTP 返回码进行判断访问地址是否正常，并且打印详细的建立连接、请求时间等，可用于后续的前端页面优化提供参考数据。并且提供当前数据和历史数据下载功能。点击当前响应时间和返回码，还可以钻取看到其 2 周的趋势图。

（2）数据库巡检

通过采集 Oracle、MySQL 和 SQLServer 等数据库的实例名状态、归档（binlog）日志使用量、表空间大小、用户过期数、主备延时（MySQL）、性能指标等重要指标进行数据库的健康性检查。

（3）中间件巡检

通过采集 Weblogic、Tomcat 和 Nginx 等中间件的服务状态、线程数、线程健康状态、队列等待数等重要指标进行中间件的健康性检查。

（4）备份系统巡检

通过 NBU 和 Networky 提供的原生命令行和 API 进行集成，采集各接入备份系统的业务系统的备份作业状态、策略、可用和已用空间容量等指标。

（5）操作系统巡检

通过 Python 和 Shell 脚本进行平台类性能指标采集（例如 CPU、内存、磁盘、文件系统、网卡的均值和峰值），为系统调优和资源扩缩提供数据支撑。

（6）特殊运行方式巡检

在重大节假日和特殊保供电时期对各业务系统进行囊括上述各项的综合性全面检查和机房动环等硬件巡检。

（7）安全基线巡检

按照南方电网公司信息化安全的相关要求，对应用系统所用到的相关中间件、数据库和操作系统进行

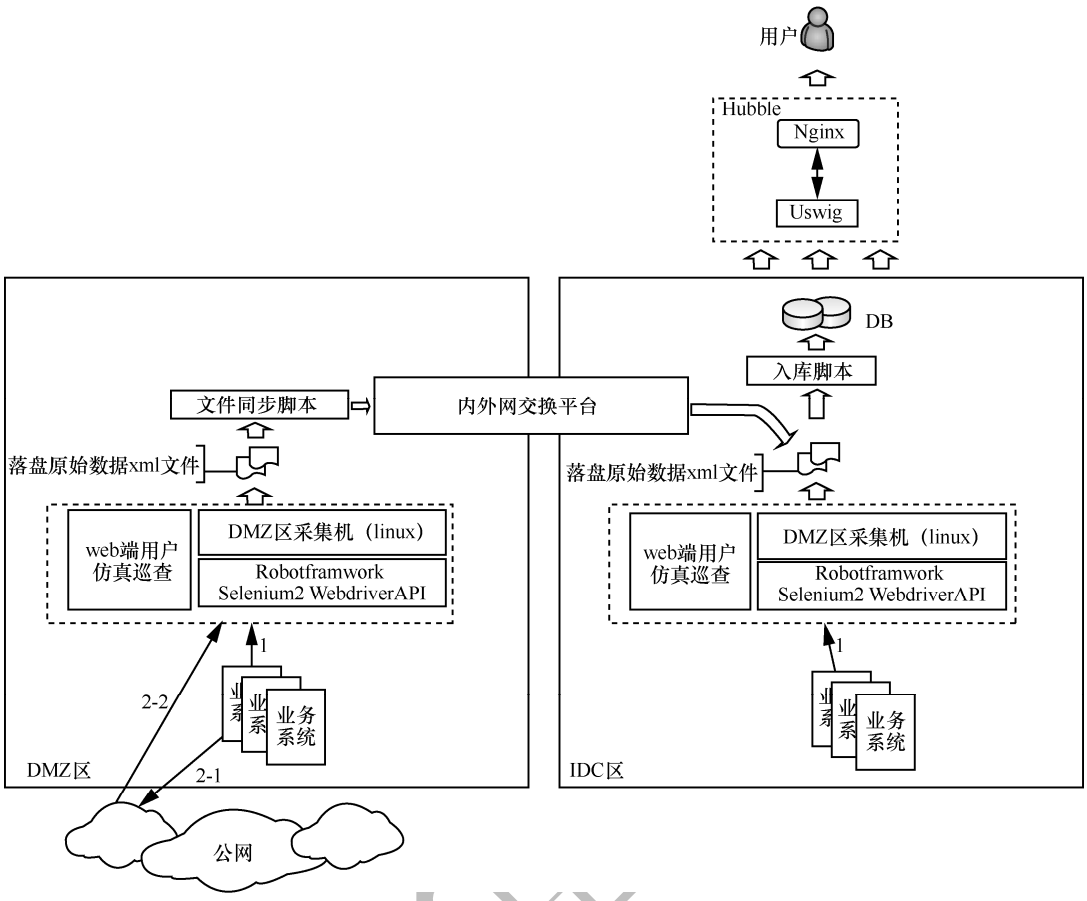


图 3　用户仿真技术框架业务流程图

基线配置检查，为国测、等保/等级评测、渗透测试等日常安全加固工作提供数据支撑和验证。

（8）用户仿真功能 Web 巡检

此功能模块通过封装 Robotframework+Selenium2 框架，集成调用浏览器原生驱动接口来实现各接入应用系统的 Web 功能模块用户仿生操作的巡检。通过模拟真实用户操作使用常用的核心模块，从用户角度主动发现问题，并保留问题重现的截图和详细的功能模块日志报告，全程无人工干预。

3.2.3　界面设计

为了提高可视化效果和用户体验，Hubble 系统基于主流的 Bootstrap（Html+CSS+JavaScript）前端框架，使得界面设计更加快捷、简洁和灵活。对于不涉及敏感信息的巡检报告，用户只需使用浏览器直接访问 Hubble 系统，即可查看各专题的巡检报告。

系统首页采用“三段式”设计风格，界面如图 4 所示。

巡检管理模块的巡检报告采用 dataTables 和 JQuery 框架，分“总览”和“详细”两块，界面如图 5 所示。

后台管理参考 adminLTE（一套开源集成 Bootstrap 的框架）的左右布局风格，界面如图 6 所示。



图 4　系统首页

4　结束语

Hubble 系统旨在提高运维人员的工作效率，解决日常运维工作中的痛点，目前经过多次版本更新迭代，



图 5　巡检报告



图 6　后台管理

系统已经能够快速、直观地实现自动化巡检功能。在解放人力的同时，系统也对其他日常运维管理和决策数据起到了落地和支撑作用。

4.1 效益性分析

（1）时效性分析

其中巡检时间效率提升显著，见表 1。

表 1 业巡检效率提升对比

序号	巡检类型	原时间（s/套）	现时间（s/套）	效率提升
1	应用 URL	15	3	↑80%
2	Oracle	600	3	↑99.5%
3	MySQl	300	14	↑95.4%
4	Weblogic	600	5	↑99.3%
5	Tomcat	60	4	↑93%
6	Nginx	50	3	↑94%
7	备份	120	3	↑97.5%
8	用户仿真	240	30	↑87.5%
9	SQlServer	300	14	↑95.4%

（2）数据准确性分析

此次成果用户仿真巡检及其他功能模块的巡检，其相关统计口径、原始数据、展示数据都经过脚本调度和前端可视化报表框架固化，所以准确率基本能够达到 100%。

（3）可用性分析

系统从 nginx+uWSGI 应用多实例、数据库主备、相关采集程序监听和消费结果缓存、应用和数据周期定时备份等方面，在架构上全面考虑，提高了系统可靠性和可用性。从投运使用以来，月度系统可用性都能达到 99.95%及以上。

4.2 新点

（1）兼容性强，既支持原生的 Selenium2 测试框架脚本，也支持 Robotframework-RIDE 的衍生测试用例脚本、对接入系统做了公共模块代码抽取、为每套业务系统做了核心功能个性化测试用例订制。

（2）解决了现场内外网端物理隔离导致的数据汇聚问题和测试用例场景多路径覆盖，真实模拟了用户分别从公网、DMZ 区、内网访问业务的场景。

（3）备份巡检通过 NBU 和 Networky 原厂提供的原生命令行和 API 进行集成，属于业内首创。

（4）各专业领域的巡检进行归并汇总，为运维监控立体化的综合数据分析提供可能。

（5）开发过程中活用敏捷方法论和 ITIL 方法论，根据实际情况把人/组织、工具系统、流程制度三者紧密结合，调整和解决实际问题，提高用户满意度。

4.3 展望

Hubble 系统，是南方电网运维人员自主研发的自动化巡检系统，是其从“脚本化”走向“Web 化”的标志产品。它是一套基于主流的 Bootstrap+Python+Django 的技术解决方案，提供了完善的前后台开发框架、调度引擎、公共组件等模块，可以降低运维门槛、提升运维效率、落地管理数据，是沉淀多年的技术运维体系的结晶。

Hubble 系统界面风格清晰、简洁易上手，符合南方电网运维人员的实际使用习惯。各模块代码可移植，还支持热拔插式部署，可以在其他分/子公司单位推广使用。

在项目开发过程中，因地制宜活用相关敏捷、ITIL 相关方法论，也为分子单位和其他政企事业单位在新世纪新环境新趋势下，传统国企信息化系统运维人员 Devops 和敏捷开发转型道路上如何把组织/人、工具系统、流程制度紧密结合和落地提供了宝贵经验。

参考文献:

[1] 范文星. 基于 Django 的网络运维管理系统的设计与实现[J]. 计算机科学. 2015(S2): 175-177.

[2] 王洁. ITIL 在电力信息系统中的运用[J]. 科学技术创新. 2017(22): 130-131.

[3] 谭晓英. 配网调控一体化运维体系的建设[J]. 中国新技术新产品. 2018(6): 33-34.

[4] 王东红, 魏广朝, 主编. 信息系统运维基础[M]. 北京理工大学出版社, 2012.

[5] 毛承国, 张卫华, 张进铎, 等. 大规模集群运维自动化的探索与实践[J]. 信息安全与技术. 2014(2): 60-62.

[6] 刘天斯. Python 自动化运维[M]. 机械工业出版社, 2016

[7] 高昂. Django 及国内 Python 社区进展[J]. 程序员. 2009(9): 23.

[8] 王冉阳. 基于 Django 和 Python 的 Web 开发[J]. 电脑编程技巧与维护. 2009(2): 56-58.

[9] 王兆媛. 基于 Django 框架的图书管理系统的设计与实现[D]. 吉林：吉林大学, 2016.

[10] 陈员义, 李艺志. 基于 Bootstrap 响应式 Web 前端研究[J]. 福建电脑. 2015(12): 72-73.

[11] 张辰. B/S 模式下的数据可视化技术研究及其应用[D]. 北京：北京邮电大学, 2014.

[12] 韩晓明. 基于符号有向图和支持向量机的故障诊断方法的研究[D]. 山西: 太原理工大学, 2011.

[13] 李鹏. 精准运维承载 IT 运维之梦[J]. 网络安全和信息化. 2016(8): 17-19.

[14] 韩啸虎. 管理信息系统集中运维平台 IT 解决方案研究[J]. 中国管理信息化. 2014(3): 23-25.

[15] 薛耀伟. 基于 Django 框架管理界面自动生成模块的设计与实现[D]. 哈尔滨: 哈尔滨工业大学, 2014.

[16] 梁德恒. 试论配网运维中配网自动化技术的应用[J]. 科技创新与应用, 2017(11): 156-157.

人民邮电出版社

区块链技术在电子数据存证取证中的应用

朱兴雄 [1,2]

（1. 国网电子商务有限公司，北京 100053;
2. 国家电网电力金融与电子商务实验室，北京 100053）

摘　要：在电子商务、金融服务中存在大量重要数据需要存证取证，以提升数据安全。提出基于区块链技术的电子数据存证取证原理，详细阐述区块链存证取证的技术方案、系统架构。讨论了区块链存证取证流程、方法，并构建 API 以支撑应用。基于区块链技术、身份标识密码技术和电子签名技术，实现电子合同签署和重要文件存证取证。各参与主体和机构把电子商务、金融服务、司法服务和身份认证等过程中的电子证据存储到区块链分布式账本中，并提供取证服务，实现了安全的电子数据存证取证。

关键词：区块链；存证；取证；身份标识密码技术

1　引言

北京互联网法院、杭州互联网法院、广州市互联网法院的设立，引起了社会的广泛关注。2018 年 9 月 3 日最高人民法院审判委员会通过《关于互联网法院审理案件若干问题的规定》，规定当事人提交的电子证据，通过电子签名、可信时间戳、散列值校验、区块链等证据收集、固定和防篡改的技术手段或通过电子取证存证平台认证，互联网法院应当确认[1]。

区块链系统提供值得信赖的记录保存能力[2]，区块链取证实现可追踪的数据分析[3]。区块链改变了传统信任机制，金融监管、法律规范、商业模式等将变革[4]。

在传统的 CA（certificate authority）认证领域，不同 CA 中心证书的互通性受到信任体系和服务协议的制约。区块链分布式记账模式的建立[5]，有助于解决 CA 体系的中心化系统风险问题，同时降低了 CA 体系带来的高额成本。

2　区块链存证取证概述

对电子商务、金融服务中的重要交易数据、合同文件、银票商票、资产证明等数据文件存证，将数据文件进行 Hash 运算后产生的散列值存入区块链。证据取证时，查看区块中存放的内容及生成时间，追溯证据的原始真实性。

研究基于区块链技术的数据存证取证和技术解决方案，在电子商务、金融服务、新能源等领域构建领先的区块链存证取证应用，提升效率，保障安全。

3　区块链存证取证原理

3.1　背景描述

区块链技术与密码算法是信息通信领域的重要发展方向，探索其在电子商务、金融服务、电子存证中的应用具有重要意义[6-8]。

在电子商务、金融服务的合同签署与文件存证中，传统的方式采用数据库存储电子商务、金融服务的交易数据、合同数据，数据容易被篡改，用基于传统 PKI/CA 的电子签名，证书管理烦琐，建设运行维护管理成本高。

3.2　存证取证原理

融合应用基于身份标识的密码系统、身份认证链与可靠电子签名机制和多因子用户私钥模型等技术，实现基于区块链的存证取证。

（1）基于身份标识的密码系统

基于身份标识的密码系统和签名方案，其公钥采用用户身份标识[9]。国密算法 SM9 使用用户的身份标识来生成公、私密钥对，用户的身份证号、手机号、邮箱或其组合都可以当作用户的身份标识[10]。

基金项目：国家电网有限公司电商科技项目（No.5100/2019-72005B）

人民邮电出版社

（2）身份认证链与可靠电子签名融合机制

基于身份标识密码算法的电子签名方法，融合应用区块链技术，跟踪密钥请求、签名申请、签名实施和解密验签全过程，建立签名人、事件、签名时间、签名地点、签名行为和身份认证的全过程溯源。签名行为全链公开，可监督、可追溯，通过区块链技术的防篡改和防抵赖[11]，实现数据可靠存证。

（3）多因子用户私钥模型

针对签名密钥唯一性和抗抵赖性需求，引入时间戳概念，在用户私钥生成模型中加入请求时间，构建用户属性信息、设备物理信息和时间戳的三元素用户私钥模型。

4 技术方案

传统合同文件的存证，往往通过公证机构出具公证书来证明原始合同的真实性。区块链技术通过对原始合同文件的 Hash 值在节点间的分布式记账，结合密码技术，来实现对原始合同的存证，采用分布式账本和密码技术，降低了建立多方信任的成本。区块链技术、身份标识密码技术和电子签名技术，三大技术融合应用，实现重要文件的存证取证。

在电子商务及金融服务中，将重要数据和文件的 Hash 特征值分布式存储于区块链中。取证时，将待验证文件的 Hash 值与存储在区块链中的 Hash 值进行比较，由其 Hash 值是否一致，确定其文件是否一致，确定文件是否未被篡改。

通过区块链防篡改的分布式账本特性，结合电子签名技术，解决多方主体间的信任机制问题，提升系统安全。采用密码学算法组合，在价值传递中不依赖中心化机构，降低价值传递过程中建立信任的成本，实现网络分布式记账。

5 系统架构

可信区块链联盟提供区块链分布式账本服务，身份标识密码系统提供密码技术服务，系统架构如图 1 所示。

整个系统的技术架构设计采用分层设计思想，从基础环境到应用服务将平台总体框架划分为如下 5 个层次。

（1）云平台基础设施

承载云端电子签名系统的云计算物理环境，包括各类主机服务器、存储设备、路由设备、交换设备、安全设备和配套的系统软件等。

（2）基础设施层

区块链基础平台实现共识机制、加密算法、分布式账本等功能。密码技术平台，包括密码机、密钥管理、移动电子签名平台。密码机提供密钥生成和密码运算支撑，密钥管理系统提供密钥全生命周期管理，移动电子签名系统提供移动终端密码算法应用支撑。

（3）运算层

区块链平台为应用提供智能合约服务。密码平台为身份认证、密钥申请、电子合同签署等应用提供密码运算支撑。

（4）应用接口层

接口层提供多种形态的应用接口，如 Hash 运算、随机数生成、区块链存证取证等。

（5）展示层

面向用户提供服务的最终形态及交互展示。重要交易、合同、协议数据均经过加密、签名等过程，并将相应的关键操作上链。区块链浏览器，可详细展示区块中的交易详情，包括存证记录。

区块链与身份标识密码技术系统包括如下模块：区块链平台，提供区块链分布式账本、智能合约等相

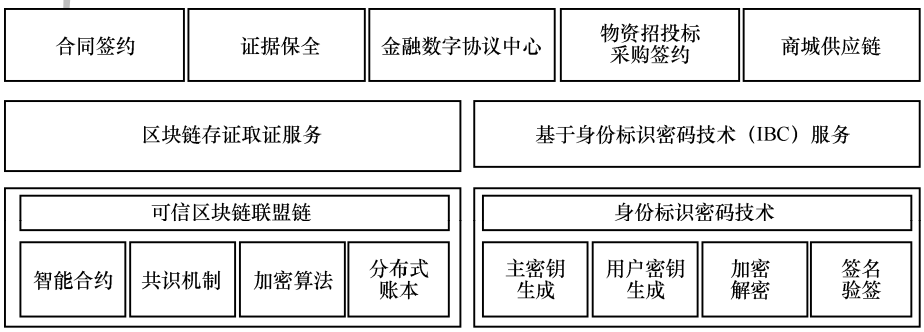


图 1　区块链与身份标识密码技术融合应用系统架构

关服务；云密码服务平台，基于云平台架构提供密码服务；API 及 SDK，提供认证、签名、加密等接口；应用系统，通过调用接口服务实现数据签名、验签、上链等功能。

6 区块链存证取证应用

6.1 流程

基于区块链技术、身份标识密码算法和电子签名技术来实现电子合同的签署、重要文件的存证取证，其中关键流程描述如下。

- 身份认证：用户登录时，使用身份认证校验机制，确认用户主体身份。
- 密钥申请：通过身份鉴别后，向密码平台申请密钥。
- 内容加密与签名：对内容进行加密、签名和封装。
- 存证：关键流程及数据上链，如密钥申请、加密、签名等过程及重要文件的 Hash 值上链保存。
- 解密与验签。
- 取证：出具过程记录；比对文件 Hash 值，确定文件真伪。

通过以上流程，系统实现重要数据文件的存证与取证。

6.2 存证取证应用

（1）存证

利用区块链的技术特点，在电子商务、金融服务、知识产权等领域，应用区块链存证，提升证据确认可信性。

（2）取证

区块链取证，查找、追溯、比对重要文件的原始记录，提供证据。区块链存证取证平台，提升证据取证环节的可信性。

（3）高可信应用

能源电商平台、金融机构、司法机构和电子认证机构等共建区块链联盟链。各机构把电子商务、金融服务和司法服务过程中的电子证据存储到区块链分布式账本中，建立高可信联盟应用。

（4）区块链与电子签名技术融合应用

用户身份信息存证到区块链上，利用区块链上多个机构共同背书用户身份，构建可靠电子签名技术体系，提升安全性。

7 区块链存证取证 API

API 接口提供对应用的支撑，包括区块链服务接口、存证取证接口、签名服务接口、密钥管理接口和密码运算接口等。实现区块链服务、密钥管理、电子签名、数据加密和数据解密等。

7.1 appKey 与 appSecret

appKey 和 appSecret 是平台分配给应用系统的密钥，应用系统调用区块链平台时，传入 appKey、appSecret 参数，获得区块链平台的调用权限。

7.2 存证接口

应用请求存证 URL（IP 地址、端口、路径 /evidence/create），通过 HTTP POST 方法，向区块链平台传入存证数据，存证输入参数见表 1。

表 1 存证输入参数

输入参数	数据类型	参数描述
appKey	字符串	应用 Key，用于区分调用者
evidenceData	字符串	证据 JSON
sign	字符串	sha256Hex (appKey+evidenceData+appSecret)

输入存证证据为 JSON 数据格式，其中 fileHash 是存证文件的 Hash 值，fileName 是文件名称，fileSize 是文件大小，应用系统可自定义更多的证据信息。

存证输出 bcHash，为该证据在区块链上的地址。

7.3 取证接口

应用请求取证 URL（IP 地址、端口、路径 /evidence/query），向区块链平台传入取证请求，取证输入参数见表 2。

表 2 取证输入参数

输入参数	数据类型	参数描述
appKey	字符串	应用 Key，用于区分调用者
bcHash	字符串	区块链地址
sign	字符串	sha256Hex (appKey+bcHash+appSecret)

取证输出，返回证据相关的参数 evidenceData 以及存证的时间 time。

8 区块链存证取证实现

区块链存证取证系统由区块链联盟链、存证取证服务等构成。系统为合同签约、供应链金融、数字协

人民邮电出版社

议中心、商品溯源和征信等应用提供存证取证服务。

应用区块链节点与司法机构节点、司法鉴定中心节点、CA 机构区块链节点等构成区块链联盟，提供区块链联盟链服务。存证取证服务为重要数据文件提供证据存储、查询服务。应用系统通过调用区块链存证服务，区块链平台将需要存证的内容，如文件 Hash 值、文件名、大小等作为存证记录，存储于区块链分布式账本中。存证后，区块链平台返回存证编号（区块链地址）给应用系统。区块链取证，查询存证编号（区块链地址）是否在平台中存在，若查询成功，则返回具体的存证内容，并返回存证时间。

9 结束语

电子商务、金融服务中存在海量数据需要存证，以提升数据安全。文中提出了基于区块链技术的电子数据存证取证原理，详细阐述了区块链存证取证的技术方案、系统架构。讨论了区块链存证取证的应用流程、方法，并构建了区块链存证取证 API，实现了区块链存证取证应用。基于区块链技术、身份标识密码技术和电子签名技术，实现电子合同的签署和重要文件的存证取证。

参考文献：

[1] 最高人民法院关于互联网法院审理案件若干问题的规定[N]. 人民法院报, 2018.

[2] LEMIEUX V L. Blockchain and distributed ledgers as trusted recordkeeping systems[C]//Future Technologies Conference (FTC), 2017.

[3] CEBE M, ERDIN E, AKKAYA K, et al. Block4forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles[J]. IEEE Communications Magazine, 2018, 56(10): 50-57.

[4] 杨东, 潘曌东. 区块链带来金融与法律优化[J]. 中国金融, 2016(8): 25-26.

[5] 朱兴雄, 何清素, 郭善琪. 区块链技术在供应链金融中的应用[J]. 中国流通经济, 2018, 32(3): 111-119.

[6] TWESIGE R L. A simple explanation of Bitcoin and Blockchain technology[J]. 2015, 1.

[7] FREY R, WÖRNER D, ILIC A. Collaborative filtering on the blockchain: A secure recommender system for E-commerce[J]. 2016.

[8] SUBRAMANIAN H. DECENTRALIZED blockchain-based electronic marketplaces[J]. Commun. ACM, 2018, 61(1): 78-84.

[9] SHAMIR A. Identity-based cryptosystems and signature schemes[C]// Workshop on the theory and application of cryptographic techniques. Springer, Berlin, Heidelberg, 1984: 47-53.

[10] 袁峰, 程朝辉. SM9 标识密码算法综述[J]. 信息安全研究, 2016, 2(11): 1008-1027.

[11] CROSBY M, PATTANAYAK P, VERMA S, et al. Blockchain technology: Beyond bitcoin[J]. Applied Innovation, 2016, 2(10): 71.

人民邮电出版社

区块链加密算法研究

朱兴雄

（1. 国网电子商务有限公司，北京 100053;
2. 国家电网电力金融与电子商务实验室， 北京 100053）

摘　要：密码技术是加密货币、分布式账本等区块链应用的核心，保障其数据安全、交易安全，是数字货币价值传递、交易的关键。加密算法在确认交易主体身份、交易数据消息摘要和信息安全编码解码中实现了其独特作用。深入分析了 SHA-256 安全散列算法，包括 SHA-256 逻辑运算、预处理、初始化和散列计算过程。详细阐述了椭圆曲线加密算法，包括椭圆曲线方程、secp256k1 和密钥对。解构了 SHA-256 和 secp256k1 算法源码实现。探讨了密码学技术现状、挑战及其发展趋势。

关键词：区块链；加密算法；散列算法；SHA-256；椭圆曲线加密算法；secp256k1

1　引言

密码技术是加密货币、分布式账本等区块链应用的核心组件，保障其数据安全、交易安全，是数字货币价值传递、交易的关键。确认交易主体身份、交易数据消息摘要、信息安全地编码解码等过程，密码技术都在其中实现其独特作用。

区块链应用中，各参与方无需传统的人际信任和传统的中心化中介，密码技术提供的密码学算法级安全是实现交易和货币流通的基础。

2　区块链加密算法

比特币和以太坊使用椭圆曲线数字签名算法（elliptic curve digital signature algorithm，ECDSA），该算法包括 2 个部分，椭圆曲线和加密散列函数，具体是椭圆曲线 secp256k1 和散列函数 SHA-256[1]。

比特币是数字签名链，每个所有者通过对先前交易和下一个所有者公钥的散列进行数字签名，且把签名加到末尾，将其转给下一个所有者。打包新区块时，使用工作量证明（proof-of-work，PoW）共识算法，搜寻一个值，其满足当使用如 SHA-256 的散列算法散列时，其区块散列值以数个 0 bit 开始。即通过递增区块中的随机数，搜寻求解一个数，使得该区块的散列值满足所要求的数个 0 bit 开始。其平均工作量与所需 0 bit 个数呈指数式增长，且可以通过执行单个散列运算来验证。虽然比特币的所有交易都是公开的，但其公钥的匿名性未公开当事人的真实姓名身份，得以保护隐私[2-3]。

比特币挖矿，需要为散列函数 SHA-256 找到部分预映像。一个区块，区块由交易列表、前一个块的散列值、时间戳、版本号、随机数组成，其 SHA-256 散列值小于目标值，即寻找以数个连续零比特开始的散列，标准策略是尝试随机数，直到找到解决方案[4]。

3　SHA-256 安全散列算法

SHA-256 是迭代的单向散列函数，可以处理消息以产生称为“消息摘要”的精简表示。该算法能确定消息的完整性，消息的任何更改，都会以非常高的概率导致产生不同的消息摘要，此属性在生成和验证数字签名、消息验证码、生成随机数时非常有用[5]。FIPS 安全散列标准定义了 SHA-1、SHA-224、SHA-256、SHA-384、SHA-512、SHA-512/224、SHA-512/256 等安全散列算法。各散列算法使用的块大小和数据字不同，输出的消息摘要大小也不同。比特币、以太坊等加密货币[6]中，使用 SHA-256 散列函数，SHA-256 的最终结果是 256 bit 的消息摘要。

3.1　SHA-256 逻辑运算

SHA-256 算法，将要处理的消息划分为小的消息

基金项目：国网电子商务有限公司（国网雄安金融科技集团有限公司）科技项目（No.5100/2019-72005B）

块，每个消息块有 512 bit，表示为 16 个 32 bit 的字的序列。SHA-256 算法使用 6 个逻辑运算[5]，如式（1）～（6）所示，操作运行在 32 bit 的字上，其中 $\mathrm{ROTR}^n(x)$为向右旋转（环形右移）操作，$\mathrm{SHR}^n(x)$为右移位操作。

$$\mathrm{Ch}(x, y, z) = (x \wedge y) \oplus (\neg x \wedge z) \quad (1)$$

$$\mathrm{Maj}(x, y, z) = (x \wedge y) \oplus (x \wedge z) \oplus (y \wedge z) \quad (2)$$

$$\sum\nolimits_0(x) = \mathrm{ROTR}^2(x) \oplus \mathrm{ROTR}^{13}(x) \oplus \mathrm{ROTR}^{22}(x) \quad (3)$$

$$\sum\nolimits_1(x) = \mathrm{ROTR}^6(x) \oplus \mathrm{ROTR}^{11}(x) \oplus \mathrm{ROTR}^{25}(x) \quad (4)$$

$$\sigma_0(x) = \mathrm{ROTR}^7(x) \oplus \mathrm{ROTR}^{18}(x) \oplus \mathrm{SHR}^3(x) \quad (5)$$

$$\sigma_1(x) = \mathrm{ROTR}^{17}(x) \oplus \mathrm{ROTR}^{19}(x) \oplus \mathrm{SHR}^{10}(x) \quad (6)$$

SHA-256 常量，使用 64 个 32 bit 的字 K_0，K_1，...，K_{63}，分别通过取自然数中前 64 个素数的立方根的小数部分的前 32 bit 得到的。

3.2 预处理与初始化

预处理包括 3 个步骤：填充消息 M，将消息解析为块，赋初始散列值 $H^{(0)}$。填充后，消息总长度是 512 bit 的倍数，消息及其填充，被解析为 N 个 512 bit 块，即 $M^{(1)}, M^{(2)}, \ldots, M^{(N)}$，每个块长为 512 bit。

设置初始散列值 $H^{(0)}$，其由 8 个 32 bit 的字组成，$H_0^{(0)}, H_1^{(0)}, H_2^{(0)}, \ldots, H_7^{(0)}$，分别是通过取自然数中前 8 个素数的平方根的小数部分的前 32 bit 得到的。

3.3 SHA-256 散列计算

使用以上定义的逻辑运算和常量，分步骤运行，顺序处理每个消息块 $M^{(1)}, M^{(2)}, \ldots, M^{(N)}$，在重复循环 N 次后，即在处理 $M^{(N)}$之后，得到消息 M 的 256 bit 的消息摘要，如式（7）[5]。

$$\mathrm{SHA256}(M) = H_0^{(N)} \| H_1^{(N)} \| H_2^{(N)} \| H_3^{(N)} | \\ | H_4^{(N)} \| H_5^{(N)} \| H_6^{(N)} \| H_7^{(N)} \quad (7)$$

4 椭圆曲线加密算法

式（8）是椭圆曲线 $E(\mathbb{F}_p)$的方程表示，$\mathbb{F}_p$ 为素数有限域，p 为奇素数，且 a、b、$\mathbb{F}_p$ 满足式（9）、式（11）的要求，$E(\mathbb{F}_p)$由解集或点集 P 组成，点集 P 由式（10）表示，对于给定点 $P_i = (x_i, y_i)$，x_i 是 P_i 的 x 坐标，y_i 是 P_i 的 y 坐标[7]。

$$y^2 \equiv x^3 + ax + b \pmod p \quad (8)$$

$$4a^3 + 27b^2 \not\equiv 0 \pmod p \quad (9)$$

$$P = (x, y) \quad (10)$$

$$a, b, x, y \in \mathbb{F}_p \quad (11)$$

4.1 椭圆曲线 secp256k1

椭圆曲线 secp256k1，其参数由六元组 T 指定，如式（12）所示，p 是奇素数，G 是曲线上的基点，n 是 G 点的阶，h 是辅因子，p, a, b, G, n, h 参数值可参考文献[8]。

$$T = (p, a, b, G, n, h) \quad (12)$$

secp256k1 的 p、a、b 值如式（13）～（15）[8]所示，256 bit、16 进制表示。由于常数 a 为 0，曲线方程中的 ax 项始终为零，因此椭圆曲线 secp256k1 计算式为式（16）。

$$P = \mathit{FFFFFFFF\ FFFFFFFF\ FFFFFFFF\ FFFFFFFF\ FFFFFFFF\ FFFFFFFF\ FFFFFFFE\ FFFFFC2F} \quad (13)$$

$$a = 00000000\ 00000000\ 00000000\ 00000000\ 00000000\ 00000000\ 00000000\ 00000000 \quad (14)$$

$$b = 00000000\ 00000000\ 00000000\ 00000000\ 00000000\ 00000000\ 00000000\ 00000007 \quad (15)$$

$$y^2 \equiv x^3 + 7 \pmod p \quad (16)$$

4.2 椭圆曲线密钥对

给定曲线域参数 T，与 T 相关联的密钥对(d, Q)，由密钥 d、公钥 Q 组成，密钥 d 是区间[1, n-1]中的 1 个整数，公钥 $Q = (x_Q, y_Q)$，即点 Q，$Q = \mathrm{d}G$[7]，如式（17）～（19）。

$$\mathrm{Key}_{\mathrm{pair}} = (d, Q) \quad (17)$$

$$d \in [1, n\text{-}1] \quad (18)$$

$$Q = \mathrm{d}G \quad (19)$$

5 SHA-256 算法实现

比特币 SHA-256 算法源码[9]如图 1 所示，由 C++ 编码实现。使用内联函数实现 6 个逻辑运算函数，Ch(*x, y, z*)、Maj(*x, y, z*)、Sigma0(*x*)、Sigma1(*x*)、sigma0(*x*)、sigma1(*x*)，其参数类型是无符号整型 uint32_*t*，32 bit。初始化散列值 $H^{(0)}$，一维数组，包含 8 个类型为 uint32_*t* 的元素，并对 8 个元素分别赋初值。

SHA-256 散列计算过程[5]如下：

步骤 1 准备消息清单明细 W_t；

步骤 2 初始化 8 个工作变量，*a*、*b*、*c*、*d*、*e*、*f*、*g* 和 *h*；

步骤 3 执行多次转换，处理 512 bit 的块，即 16 个 32 bit 的字，执行 64 次 Round(uint32_*t a*, uint32_*t b*, uint32_*t c*, uint32_*t d*, uint32_*t e*, uint32_*t f*, uint32_*t g*, uint32_*t h*, uint32_*t k*)；

步骤 4 计算第 i 个散列值 $H^{(i)}$。

重复步骤 1～步骤 4，重复 N 次，得到最终的 256 bit 消息摘要 $H^{(N)}$。

人民邮电出版社

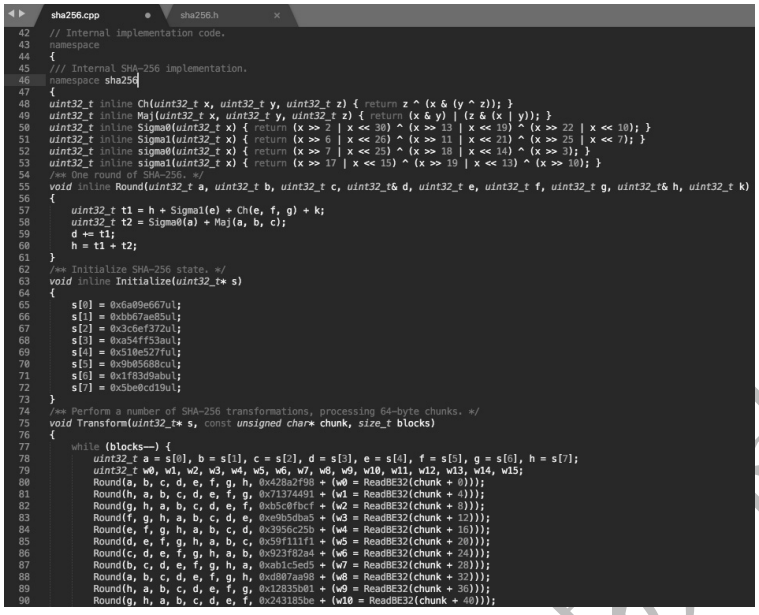


图 1　SHA-256 算法源码

6　Secp256k1 算法实现

椭圆曲线 secp256k1 方程的源码[9]如图 2 所示，实现椭圆方程 $y^2 = x^3 + 7$。

secp256k1 椭圆曲线数字签名算法，实现并支撑签名、验证和密钥生成，实现私钥、公钥、签名的序列化和解析，源码[9]如图 3 所示。

7　密码学技术讨论

数字货币、分布式账本等区块链应用，用到了 SHA-256、secp256k1、RIPEMD-160[10]、base-58 等密码技术和算法。随着在交易中引入加密解密、散列算法、私钥公钥、签名验证、编码解码等环节，在提升安全性的同时，针对如何兼顾效率的提升、如何支撑

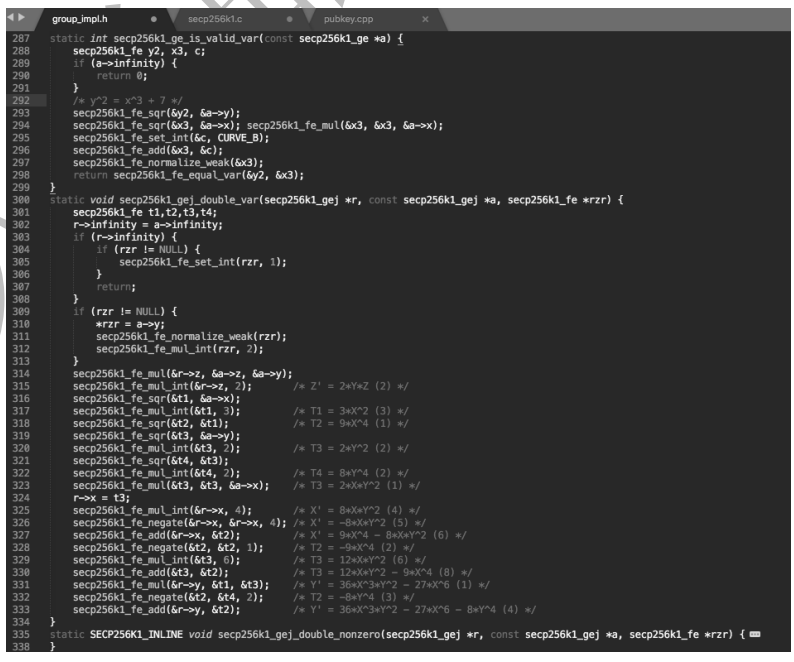


图 2　椭圆曲线 secp256k1 方程源码

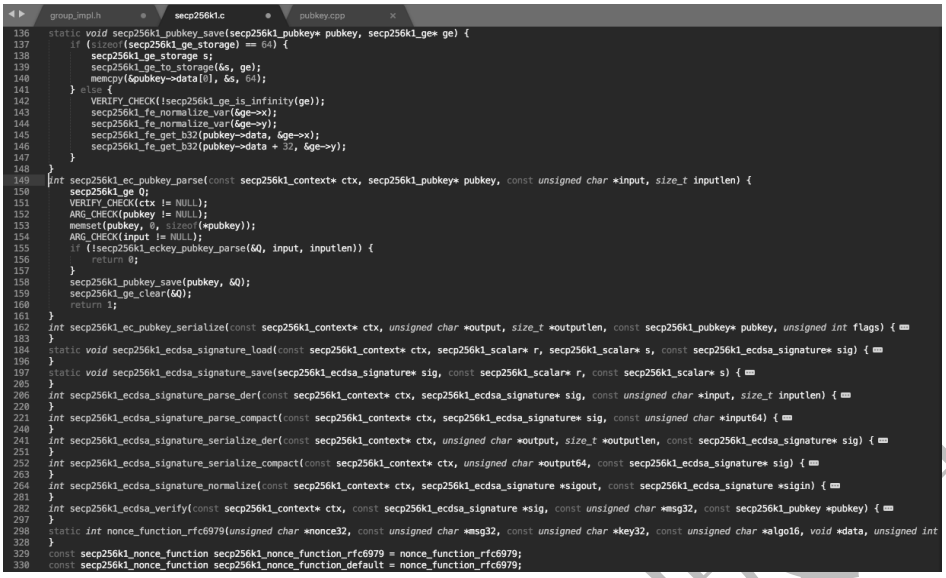


图 3　secp256k1 算法源码

大规模高频交易，提出了新的挑战。

随着量子密码术的兴起，利用光子的偏振特性、光子相位和量子属性进行编码。密码技术基于光子特性、量子密钥、量子理论，而不仅是椭圆曲线、散列算法、逻辑运算等数学理论，为密码技术的全新发展带来了新的契机。

8　结束语

本文深入分析了 SHA-256 安全散列算法，包括 SHA-256 逻辑运算、预处理、初始化和散列计算过程。详细阐述了椭圆曲线加密算法，包括椭圆曲线方程、secp256k1 和密钥对。解构了 SHA-256 和 secp256k1 算法源码实现。探讨了密码学技术现状、挑战及其发展趋势。

参考文献：

[1] MAYER H. ECDSA security in bitcoin and ethereum: a research survey[J]. CoinFaabrik, 2016(6), 28: 126.

[2] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[EB]. 2008.

[3] EYAL I, SIRER E G. Majority is not enough: bitcoin mining is vulnerable[J]. Communications of the ACM, 2018, 61(7): 95-102.

[4] BONNEAU J, MILLER A, CLARK J, et al. Sok: Research perspectives and challenges for bitcoin and cryptocurrencies[C]//2015 IEEE Symposium on Security and Privacy. Piscataway: IEEE, 2015: 104-121.

[5] National Institute of Standards and Technology. FIPS 180-4: Secure Hash Standards[S]. 2015.

[6] VUJIČIĆ D, JAGODIĆ D, RANĐIĆ S. Blockchain technology, bitcoin, and Ethereum: a brief overview[C]//2018 17th International Symposium INFOTEH-JAHORINA (INFOTEH). Piscataway: IEEE, 2018: 1-6.

[7] Certicom Research. SEC 1: elliptic curve cryptography, version 2.0[R]. 2009.

[8] Certicom Research. SEC 2: recommended elliptic curve domain parameters, version 2.0[R]. 2010.

[9] Bitcoin[EB]. 2019.

[10] MEIKLEJOHN S. Top ten obstacles along distributed ledgers path to adoption[J]. IEEE Security & Privacy, 2018, 16(4): 13-19.

全业务数据中心运维探讨

崔乃栋，潘磊，冯志鹏
（国家电网有限公司信息通信分公司，北京 100761）

摘　要：数据是信息化的核心，要实现用数据管理企业、用信息驱动业务，需要全业务数据中心支撑。通过开展全业务数据中心运维工作，确保数据中心的数据得到正常、及时的处理，满足用户对数据中心的访问需求，保证全业务数据中心的正常稳定运行，以实现统一为公司各类应用建设提供海量数据采集处理、存储处理、计算处理、分析挖掘等基础性支撑功能的目标，实现数据资源统一存储、数据统一对外服务。

关键词：数据中心；数据分析；数据处理；运维管理

1　引言

随着各业务信息系统建设和应用的不断深入，逐渐暴露出跨专业业务协同与信息共享不足，数据多头输入，数据准确性、实时性不强，数据反复抽取，冗余存储，质量不高等问题。深入挖掘数据价值、用数据管理企业、用信息驱动业务的需求更为迫切。通过构建全业务结构化数据的企业数据仓库，解决全业务数据的接入与汇聚问题；构建统一存储服务，实现采集监测数据、非结构化数据、外部数据的统一存储和管理，同时满足业务处理应用与分析类应用的使用需求，解决数据多份复制、冗余存储问题；全业务数据中心是前端全业务融合、后端大数据分析的必然选择，对企业信息化具有重要意义。同时，大数据、云计算等技术日趋成熟，为全业务数据中心的建设运维提供了技术保障。

2　总体架构

全业务数据中心是现有数据中心的进一步发展和完善，主要包括数据处理域、数据分析域和数据管理域 3 部分，其总体架构如图 1 所示。

数据处理域是生产经营管理过程中各类业务数据

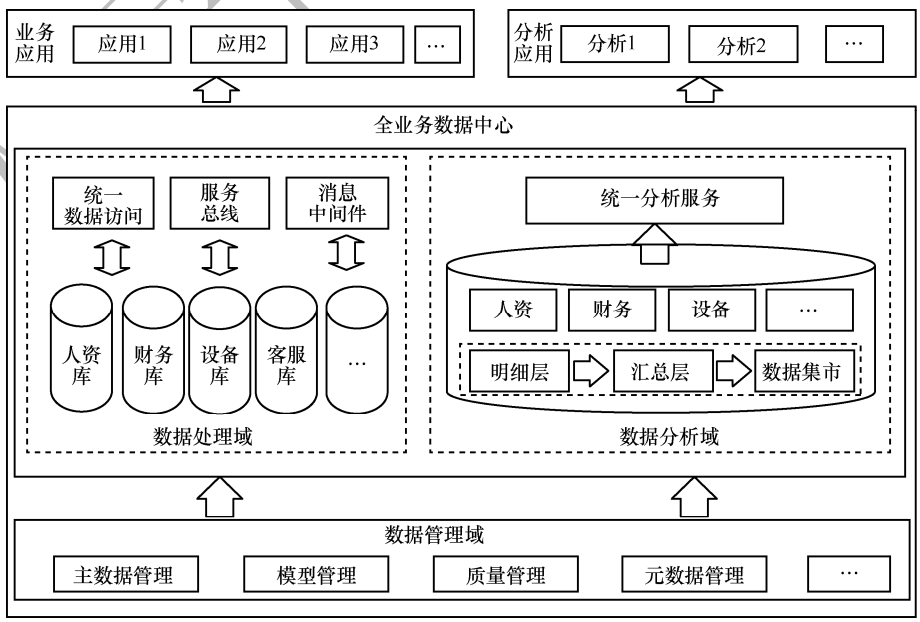


图 1　总体架构

存储、处理、融合的中心，主要支撑业务处理类应用，是推进业务流程贯通、数据共享，保障数据质量的关键，提升数据应用水平的基础；数据分析域是公司各类数据清洗转换、汇聚整合的中心，主要支撑采集监测类和分析决策类应用，是挖掘数据资源价值、提升数据应用水平的核心；数据管理域是公司数据模型管控、主数据应用的中心，是实现数据规范、安全、正确的关键和保障。以上 3 个部分紧密结合，互相促进，是一个有机的整体。

3 运维目标

明确全业务数据中心运维任务，通过开展全业务数据中心运维工作，保证全业务数据中心的正常稳定运行，以实现统一为公司各类应用建设提供海量数据采集处理、存储处理、计算处理、分析挖掘等基础性支撑功能的目标，实现数据资源统一存储、数据统一对外服务。

（1）业务可靠性

全业务数据中心建成后，会将更多的公司应用和服务迁移其中，保证全业务数据中心 7×24 h 可靠运行，才能满足用户服务需求。如果出现模块失效、节点宕机的情况，全业务数据中心依然能够正常提供服务。所以运维人员要能够自动或手动对报错节点提供快速切换、重启或者迁移服务，消除告警。

（2）设备冗余性

全业务数据中心基础设施应保证完全冗余，任意一台设备或路径出现问题进行维护时，都有备用链路或设备保障系统的健壮可用。

（3）数据安全性

对于存储在全业务数据中心的应用和数据，全业务数据中心需要保证安全性，包括完整性、不可篡改、访问控制等。当出现安全问题时，运维人员能够从用户管理、日志分析、网络管理、设备管理等各方面快速发现、隔离和消除安全问题。

（4）服务松耦合

各个功能和服务之间保持松耦合性。当对全业务数据中心的某个功能或组件进行维护时，需保证全业务数据中心仍然能提供服务。

（5）系统可监控

为确保平台正常运转，必须对全业务数据中心进行多方位监控。通过 I6000 系统可以查看全业务数据中心的各个域的监控信息，及时了解核心组件运行情况，当资源使用情况超过既定阈值时及时通知运维人员，根据监控信息对相应的基础环境和应用系统状态进行调度指挥，让公司 IT 整体环境变得更加稳定，为业务提供持续的优质服务

4 运维方案

4.1 运维组织架构

运维组织机构主要包括总部及分部信息化管理部门、运维单位及研发单位。

总部信息化管理部门：负责公司全业务数据中心全生命周期的整体规划，负责确定全业务数据中心的技术路线、架构、演进步骤；负责运维工作总体管理，负责建立运维管理制度、技术标准和规范、架构管控；负责运维工作的监督、检查、评价和考核工作。

各分部信息化管理部门：负责功能需求的调研，对功能需求及功能变更进行统一分析、评估和设计审定；负责全业务数据中心的上下线审核；负责指导本单位开展全业务数据中心运维工作；负责协调组织本单位其他业务相关部门，配合开展全业务数据中心系统运维相关工作。

运维单位：负责按总部要求开展全业务数据中心系统运维工作；负责调度监视、检修、资源管理、客服等日常运维工作；负责监控运维需求收集调研；负责业务需求调研工作；开展自动化运维能力建设。

研发单位：负责全业务数据中心各个模块设计研发实施工作；负责开展运维监控、分析、自动化操作工具设计研发；负责各相关业务系统改造；负责全业务数据中心技术支撑工作，负责全业务数据中心运维培训工作。

4.2 运维保障体系

信息系统运行维护工作按照调度、运行、检修进行专业化细分，实现信息系统运行维护工作的组织形式由专业分工向业务分工的转变。一线承担信息运行的职能，二线及三线承担信息检修的职能，建立以业务分工为划分原则的工作组织模式，形成既协同配合，又互相制约的工作关系。

信息调度是指通过调度指令，对信息系统检修计划、紧急抢修、缺陷管理、两票管理、上下线管理等工作内容进行调控，实现信息资源的高效利用。

信息运行是指通过统一客服事件受理、业务系统及平台巡检、监控、告警管理等工作，实现对信息系统及运行环境的管控。

人民邮电出版社

信息系统检修是指通过检查、维护、风险消缺、隐患排查、变更、调试、优化、升级等工作，确保信息系统正常运行，提升信息系统的运行质量。

5 运维内容

5.1 调度部门

主要负责全业务数据中心的日常监控调度、策略调度、方式资源运维工作。

（1）监控调度

负责全业务数据中心的运行状态监控与预警、应急处置、检修审批；负责组织开展全业务数据中心的日常保障工作。

（2）策略调度

负责组织开展全业务数据中心的应急演练工作；负责编制全业务数据中心的运行方式和应急预案。

（3）方式资源

负责全业务数据中心资源的规划分析、统一调配与管理；负责全业务数据中心运行情况的统计分析工作。

5.2 运检部门

（1）基础设施运维

主要分为机房、网络、主机与存储等硬件设备运维，负责机房的动环运维，包括电源、空调、消防、安防等基础设施的运维、巡视及安全保障工作，配合开展基础设施的隐患排查治理、计划检修、技改大修相关工作；负责网络、安全设备、主机、存储等基础硬件设备的运行维护、故障处理和安全保障工作；负责硬件设备应急预案，定期开展应急演练，开展应急处置。

（2）平台运维

负责全业务数据中心的网络、存储、中间件、数据库以及集成组件等的运维工作。负责组织生产准备工作，组织开展本地全业务数据中心的上线测试；负责账号权限维护、资源配额管理、配置变更等工作；负责全业务数据中心的运维及管理工作，包括主机的增删改查、启动和停止；负责操作系统、数据、集成等平台的运维工作；负责应急预案，定期开展应急演练，开展应急处置等工作。

（3）业务运维

负责业务应用系统的巡视、检修等日常系统运维工作；负责操作系统漏洞整改、安全加固等运维工作；负责研究业务应用系统的特点，分析应用性能，提出优化建议；负责业务应用的数据运维工作；负责业务应用系统应急预案，定期开展应急演练，开展应急处置；负责业务系统一/二线客服工作，包括受理用户需求、投诉、意见、建议等，并进行登记；及时跟踪平台系统问题故障处理情况，负责问题故障的反馈；负责服务类问题故障的确认和处理。

（4）安全运维

负责安全的设计、部署、参数配置、故障排查、性能优化等工作；负责全业务数据中心安全访问控制策略、日志审计、安全加固、安全基线的制定；负责主机防火墙的源地址、目标地址、端口规则的制定；负责业务应用安全检查。

6 结束语

文中对全业务数据中心运维体系做了广泛地探讨，在总体架构基础上，从运维目标、运维方案、运维组织及保障体系方面进行了研究，结合公司信息化应用，对公司全业务数据中心运维管理有非常实际的参考意义。

参考文献：

[1] 中国通信企业协会. 数据中心基础设施维护规程[M]. 北京: 电子工业出版社, 2016.

[2] 钟景华. 中国数据中心运维管理指针[M]. 北京: 机械工业出版社, 2017.

[3] 林予松, 李润知. 数据中心设计与管理[M]. 北京: 清华大学出版社, 2017.

[4] 李嗣喜. 浅谈数据中心的人工智能管理与运维[J]. 计算机产品与流通, 2019(1): 123.

[5] 顾蛟鹏. 数据中心运维管理措施的研究[J]. 计算机产品与流通, 2018(7): 118.

[6] 陈栋. 探索面向服务的数据中心运维新模式[J]. 中国信息化, 2018(7): 54-56.

[7] 钱一飞, 扈永正, 焦斌. 数据中心运维管理之我见[J]. 中国新通信, 2018, 20(12): 36.

人民邮电出版社

适用于输变电工程造价管理的智能化应用平台

叶宝玉[1]，王雁宇[2]，师潇然[2]，梁雯艳[2]，衣丰超[3]
（1. 内蒙古电力（集团）有限责任公司，内蒙古 呼和浩特 010020;
2. 内蒙古电力经济技术研究院，内蒙古 呼和浩特 010090;
3. 内蒙古科电数据服务有限公司，内蒙古 呼和浩特 010010）

摘　要：输变电工程造价管理是工程项目管理的重要内容之一，由于工程造价管理方式较为粗放，造价数据分析较为滞后，不能及时有效地解决工程造价管理相关问题。分析了当前造价管理方式存在的主要问题，结合新形势下输变电工程造价管理需要，建议将大数据、人工智能、移动应用等先进信息化技术应用到工程造价管理业务中，构建输变电工程造价管理智能化应用平台。从平台架构搭建、技术路线选择、应用架构设计、数据集成设计等方面介绍了如何搭建专业化的造价管理智能化应用平台，期望为输变电工程造价管理提供更加系统、专业的解决方案。

关键词：输变电工程；造价管理；大数据分析；人工智能；移动应用；智能化

1　引言

随着国内外电网市场竞争环境愈加激烈，电网企业为了探索新的发展机遇必须不断地全力提升企业核心竞争力。各业务领域在紧跟企业整体发展方向的同时，还需要不断地寻求新的业务管理突破口和效益增长点。输变电工程建设作为电网企业快速发展的基础，每年建设工程数量多，工程建设任务重。以内蒙古电力为例，当前内蒙古电力输变电工程电压等级包含500 kV、220 kV、110 kV 和 35 kV，2018 年上半年，主网工程开复工 130 项，投产 19 项。截至 2018 年 1 月，内蒙古电力公司电网统调装机 6 606.53×10^4 kW，500 kV 变电站 26 座，220 kV 变电站 147 座，110 kV 及以下变电站 938 座。

为了保障电网建设稳步快速推进，同时实现投资效益最大化，需要不断地加强输变电工程造价管理力度。借助先进的信息化技术手段实现造价管理精益化、标准统一化、管控集中化、决策智能化是项目管理部门和造价管理部门的主要任务。

为适应公司发展和电网建设新形势，构建一体化电力经济技术研究体系，规范电网建设甲方职责委托业务，加强电网规划建设评审、技经评价、结算审查、审计审价、运营监控等技术支撑性业务，内蒙古电力公司于 2015 年成立内蒙古电力经济技术研究院，部门包括评价审价中心、运营监控中心、规划评审中心、技术咨询中心、建设项目管理中心等。评价审价中心主要负责电网项目技经评审和输变电工程结算审查，承担公司投资新建、扩建输变电工程及投资在 500 万元以上的其他基本建设项目的结算审计审价工作，负责开展项目后评价、工程技术经济评价与研究等工作。作为蒙西电网输变电工程项目造价管理部门，评价审价中心对工程项目造价管理有着更加深刻的理解和认识，切实以造价管理实际需求为出发点，考虑借助信息化技术搭建输变电工程造价管理智能化应用平台，以实现工程造价智能化管理。

2　输变电工程造价管理现状

国内电网企业经过多年信息化建设，在输变电工程项目管理方面已有一定的信息化基础，覆盖业务包括电网规划管理、项目需求计划及招投标管理、项目合同管理、项目物资出入库管理、项目验收与投运管理、项目结算管理等，但部分地区在工程造价管理方面还缺乏智能化管控平台作为有力支撑，存在的问题主要包括：

（1）造价数据分散存储在各类业务系统中，为全数据造价分析带来一定困难，造价分析精确度和适用性难以得到保障；

（2）造价管理基本停留在对已完工程造价数据的

人民邮电出版社

分析，未覆盖造价管理全部业务内容；

（3）造价分析工作较为复杂，传统的造价分析方式主要依赖人工，效率低下且主观因素对造价分析结果的影响较大。

3 智能化管理应用平台

在信息技术快速发展的今天，信息化技术与传统行业的深入融合已经成为优化业务流程、提升管理能力的最佳途径，造价管理业务同样可以借助大数据分析技术、人工智能技术、移动应用技术等先进信息化技术手段构建输变电工程造价管理智能化应用平台，提升对造价业务的监督、指导、管控水平，实现工程项目造价管理智能化。

3.1 平台技术架构

平台技术架构包括接入展示层、应用层、平台层、基础设施层以及服务安全架构，并使用服务质量规范标准确保平台提供的专业应用功能质量标准统一，技术架构如图 1 所示。

基础设施层：平台基础设施设计充分考虑了系统运行速度以及增量工程造价数据存储需要，采购部分服务器搭建高性能技术环境、大容量存储环境，满足平台注册用户众多、用户并发量大、集中处理数据量大、性能要求高的特点。

数据层：负责数据的统一组织和管理，采用大数据技术抽取各业务系统相关数据，在数据中心构建输变电工程造价管理智能化应用平台数据仓库，对应用层的造价专业管控功能提供数据支撑。

应用层：面向上级管理单位及部门、地市公司、设计单位、施工单位、监理单位、审价单位等各类用户，采用 PC 桌面终端、大屏终端、移动终端等多种手段，通过网络提供输变电工程造价业务管理所涵盖的造价主数据管理、造价数据上报及审批、造价分析管理、造价报告管理、造价控制线管理、造价预测管理、可研初设辅助评审管理、变更签证辅助审批管理、综合管理等应用，通过统一应用门户向用户呈现，以满足各类用户不同应用场景。

展现层：实现客户通过 PC 桌面终端、大屏终端、移动终端等方式访问平台应用功能。

安全架构：包括物理安全、系统安全、数据安全、应用安全、网络安全、运维安全等内容，保障数据存储、传输、访问、共享的安全。

质量规范：标准和规范体系包括认证规范、业务

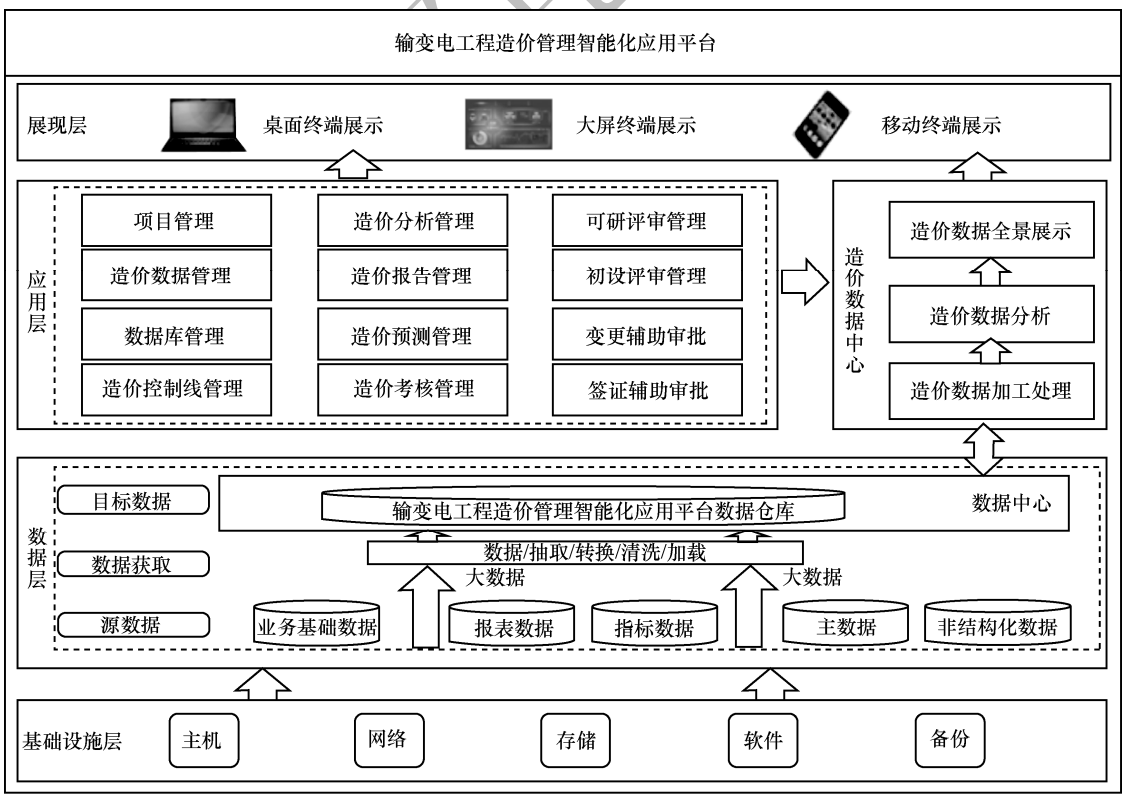


图 1　输变电工程造价管理应用平台技术架构

流程规范、接口规范、数据规范、开发规范和部署规范等方面确保平台各应用组成部分之间以及平台与外部系统交互能够有效衔接和规范运转。

应用平台优先使用基于 J2EE 架构进行开发，同时要求系统也使用相同 SDK 版本的 Java 技术进行开发，保证应用程序的一致性和更好的兼容性。同时架设高性能 Web 站点，提高研发效率、保证软件质量，并引入 WebLogic 服务器进行部署，Java EE 平台和 WebLogic 服务器可以轻松切换到 Linux、Unix 系统下运行，也很适合 SOA（service oriented architecture，面向服务架构）的实现以及各种 SOA 基础服务的架设。

架构设计方面，采用面向服务架构的软件设计理念，以业务驱动服务，以服务驱动技术，使各项功能更好地服务于业务。建设基于标准的统一平台，在标准层面上实现跨平台整合，并提供对其他已有系统的集成机制。

本平台客户端采用 Web 方式，通过浏览器来访问系统功能，客户端零安装、易于使用、界面美观、便于系统升级维护，并且确保平台和协议的一致性，采用 B/S 架构，更能方便实现系统的组件化设计。

3.2 平台集成架构

输变电造价管理包含对工程全生命周期中的所有造价数据的管理，从工程项目造价形成过程和特点来看，需考虑与相关业务系统集成，如工程造价软件、ERP 系统、审计系统等，通过接口实现估算数据、概算数据、结算数据、决算数据等造价数据的实时共享，按照预定规则进行自动抽取和清洗，同时必须保证清洗后数据准确无误，清洗完成的造价数据方可用于造价分析业务。此外，为了方便用户登录系统，考虑与门户系统集成，实现统一入口单点登录系统，系统集成架构如图 2 所示。

3.3 平台应用架构

平台功能包括造价主数据管理、造价分析管理、全过程造价监控管理、造价考核管理等，其中造价信息实时共享、造价分析实施查询、流程审批管理、通知公告管理通过移动应用实现，平台应用架构如图 3 所示。

（1）造价主数据管理

主要实现造价主数据的统一管理，在造价主数据管理中增加资源库，包括定额库、清单库、主要设备材料清单库，造价主数据管理包括造价数据维护管理、造价数据提报与审批。

大数据技术作为先进的数据处理工具可以为造价数据处理工作提供更优解决方案，采用大数据技术按照提取规则自动通过接口提取各业务管理系统中相应的造价数据。由于工程造价计算过程较为复杂，在借助造价软件计算工程造价时仍然会出现部分错误，因此在提取到造价数据后，基于造价软件、定额库、清

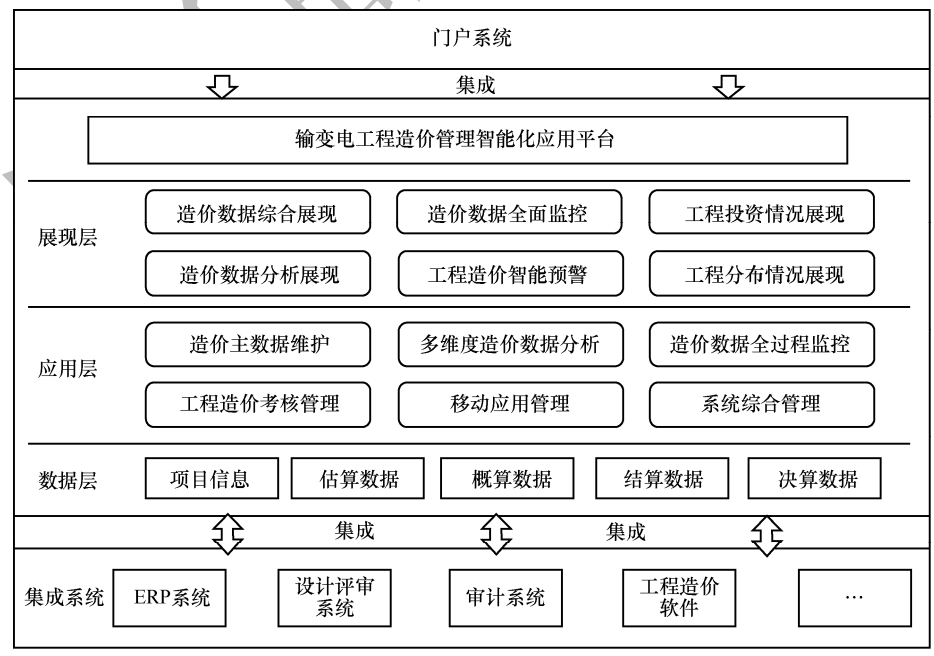


图 2　输变电工程造价管理应用平台集成架构

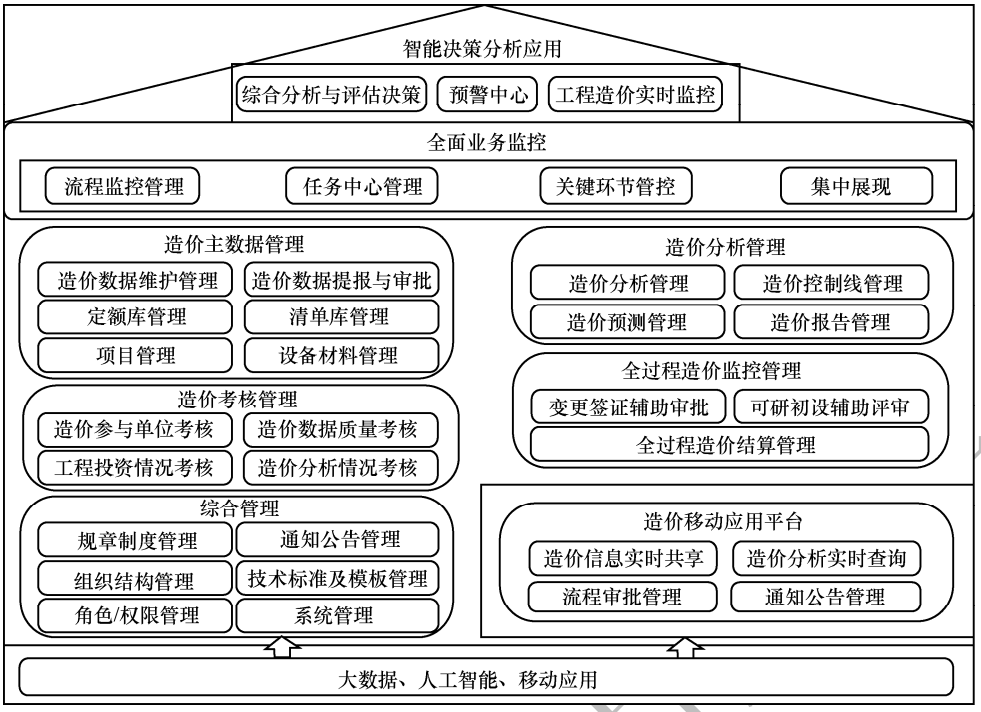


图 3　输变电工程造价管理应用平台应用架构

单库、主要设备材料清单库进行一定的造价数据校验，校验无误的造价数据才可按照既定规则进行清洗，因每个工程项目造价均具有其自身特殊性，造价数据具有多样性和复杂性的特点，为保障清洗完成的数据可以满足不同维度、不同颗粒度的统计分析需要，需确定明确的校验规则、清洗规则和数据存储规则，使清洗后的造价数据能够达到统一性、通用性和正确性的要求。前台展示清洗结果并保存到数据库中，清洗后的造价数据在经领导审批后即可作为造价分析的基础数据。

（2）造价分析管理

造价分析管理主要包括多维度造价分析、造价分析报告管理、造价控制线管理和造价预测管理 4 部分，4 部分内容相辅相成共同构成了输变电工程造价分析管理的主要内容。

梳理输变电工程造价分析内容，将各类造价分析图表样式固化到平台中，电缆工程各部分费用投资占比分析如图 4 所示。

以清洗完成的数据为基础自动计算输出分析结果，项目管理部门需要按照造价分析内容及要求编制造价分析报告，通过平台固化造价分析报告模板，一键式生成造价分析报告，辅助造价分析人员完成造价分析报告编制工作。

为了便于工程投资估算、初涉概算评审，多数企业根据本地区特征制订了适用于本地区的造价控制线，正在将造价控制线用于投资估算和初设概算的评审工作。造价控制线已成为造价管理的主要依据，由于“三通一标”设计仅考虑专业可行性，未考虑外界条件影响，为保障造价控制线可被广泛应用，采用人工智能技术分析影响工程造价的主要因素，并分析影响程度。分析足够数量的工程造价样本数据得出适用于不同地区的造价控制线，造价控制线在实际使用过程中随着时间的推移必须根据实际情况进行不断的调整，使造价控制线不断接近工程实际造价，充分发挥造价控制线在造价管理中的指导作用。

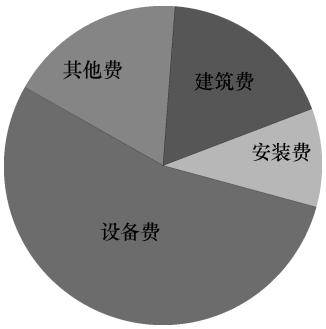


图 4　电缆工程各部分费用投资占比分析

造价预测管理主要指根据影响造价关键因素预测

目标工程的造价，平台使用人工智能技术搭建智能分析模型，分析得出的关键因素和影响程度分析为造价预测提供了重要依据，计算速度快的同时准确性较高。

（3）全过程造价监控管理

全过程造价监控管理主要将造价控制线应用到工程可研评审、初设评审工作中，并将历史工程数据分析结果作为实时监控工程建设过程中可能发生的变更和签证的依据，辅助项目人员判断变更和签证涉及的造价变更是否必要、是否合理，实现工程造价动态监控和预警。此外，将项目施工、监理、设计等合同进度款结算纳入平台管理，完成进度款的提报、审批及查询。

（4）造价考核管理

输变电工程造价相关单位包括设计单位、施工单位、监理单位、审计单位等，各单位分别负责工程不同阶段的造价工作，在相似技术条件和建设条件下各单位计算的工程造价结果有一定的差距。对方案设计深度和现场勘查情况未达到要求而导致投资估算和初设概算与工程实际造价相差较大的情况，应加强造价管理相关单位的考核，建立科学的评价机制，辅以适当的激励机制，可以提高工程造价管理效率。

此外，还应加强工程投资完成情况考核，严格把控投资结余率，提高投资效益，监控结余率较高的相关单位及部门。确保上报的工程造价数据是否准确无误，高质量的工程造价数据是有效造价分析的基础，对造价数据质量不高的单位及部门进行严格监督和考核。全方位的造价数据分析是一项耗时费力的工作，涉及项目管理部门、项目参与单位等，为了保障造价数据分析工作能够顺利进行，通常需要协调相关部门配合完成，也可以借鉴考核的手段督促造价分析部门及时安排造价分析工作。

（5）全面业务监控及智能决策分析

全面业务监控主要包括流程监控管理、任务中心管理、关键环节管控、集中展现，通过智能化应用平台对造价管理全业务进行全面监控，深入造价管理业务的每一个环节。搭建造价管理驾驶舱，采用大屏展示技术综合展现工程造价统计分析及造价管理工作推进情况，相关部门及领导可以全面地了解输变电工程造价情况。

智能决策分析主要包括综合分析与评估决策、预警中心、工程造价实时监控，在基础模块数据分析的基础上对输变电整体造价工作总结宝贵经验，指导造价管理工作，尤其需要加强项目建设过程中的造价监控，将对造价结果数据的传统分析逐渐转向对造价形成过程的监控，不断提高造价工作的指导能力和管理水平。

（6）造价移动应用平台

移动应用平台具有灵活便利的特点，可以应用到工程造价管理中，通过平台发布造价专业数据信息，便于造价人员实时共享造价信息，促进造价管理标准化。通过移动应用平台，造价管理部门领导可以随时掌握造价分析工作进度计划和安排，实时查看造价数据分析结论、掌握输变电工程造价整体情况，相关领导可以在平台上完成相关单据审批等。

4 结束语

近年来，学者专家们对输变电工程造价管理提出了很多建设性的建议，目前正在不断被尝试用于实践，且已初见成效。为了寻找更加专业的解决方案，必须不断深入思考输变电工程造价管理新需求，不断研究管理新模式，才能进一步提高输变电工程造价管理水平。随着与信息化技术融合程度不断提高，输变电工程造价管理工作必将取得长足发展。

参考文献：

[1] 侯方洁, 刘克, 李红. 基于输变电工程结算大数据的造价管理评价[J]. 中国电力企业管理, 2016(12): 48-49.

[2] 胡晋岚，高晓彬. 输变电工程造价影响因素识别及数据建模分析[J]. 华北电力大学学报(社会科学版), 2016, 26(5): 55-59.

[3] 李丽芝. 工程造价人工智能时代的期待与展望[J]. 建材与装饰, 2018, 545(36): 140-141.

[4] 石宝锋. 浅谈智能化信息处理的建筑工程造价短期预测[J]. 黑龙江科技信息, 2013(25): 227-227.

[5] 王玲. 基于网络的电力工程造价智能化管理系统探讨[J]. 价值工程, 2014(19): 192-193.

[6] 黄晓光. 地方性电网输变电工程全过程造价管理的应用研究[D]. 广州: 广东工业大学, 2018.

[7] 商桑, 温卫宁, 任妍, 等. 输变电工程造价控制指标深化研究[J]. 中国电力企业管理, 2018, 528(15): 70-71.

[8] 国际电力网. 2018 年电网工程建设完成投资 5372 亿元 同比增长 0.6%[Z]. 2018.

[9] 蒙电青春公众号. 集团公司 2018 年年中工作会议精神解读[Z]. 2018.

[10] 内蒙古电力集团有限责任公司. 2017 年信息公开年报[Z]. 2017.

人民邮电出版社

输变电工程造价分析与成果应用

叶宝玉[1]，王雁宇[2]，师潇然[2]，梁雯艳[2]，衣丰超[3]
（1. 内蒙古电力（集团）有限责任公司，内蒙古 呼和浩特 010020;
2. 内蒙古电力经济技术研究院，内蒙古 呼和浩特 010090;
3. 内蒙古科电数据服务有限公司，内蒙古 呼和浩特 010010）

摘　要：随着新形势下电网行业的发展快速，作为电网行业发展的重要基石，电网基础建设一直以来都是电网企业重点监管的内容之一。投资巨大的工程建设需要科学合理地分析工程造价，以推进输变电工程造价管理业务标准化、规范化、制度化、科学化、系统化、高效化。详细描述了输变电工程造价分析思路，以内蒙古电力 170 个输变电工程为样本造价数据分析为基础，结合国内同行业造价管理现状，提出了几点关于提高造价管理水平的建议。

关键词：输变电工程；造价分析；成果应用

1　引言

随着电力体制改革不断深入，为电网企业带来压力的同时也带来了新的机遇和挑战。电网企业基础工程建设需与企业发展方向保持一致，在压力与机遇中探索新的发展契机。2018 年，全国电网工程建设完成投资 5 373 亿元，同比增长 0.6%，增速较上年提高 2.3 个百分点。据统计数据显示，2018 年上半年，内蒙古电力主网工程开复工 130 项，投产 19 项，截至 2018 年 1 月，内蒙古电力公司电网统调装机 6 606 53×10^7kW，500 kV 变电站 26 座，220 kV 变电站 147 座，110 kV 及以下变电站 938 座。

输变电工程建设主要包括工程建设管理和工程造价管理等内容，工程建设和工程造价相辅相成、相互制约。在技术条件、建设条件一定的情况下工程造价是否合理、工程造价费用比例是否最优、工程投资效益是否达到预期目标、工程项目整体投资结构与公司发展规划是否匹配等不仅是项目管理部门和计划发展部门业务管控重点内容，更是电网公司领导层主要关注内容之一。为了客观且精确的反应输变电工程造价情况，需要建立更加完善的输变电工程造价分析体系，并根据造价管控需要不断调整和完善。此外，为不断提高造价管控能力，需要不断地将造价分析结论应用到工程造价管理中，根据实际管理需要不断优化。

内蒙古电力经济技术研究院正式成立于 2015 年，主要负责蒙西电网规划和工程咨询的技术归口管理，承担蒙西电网发展总体规划和专项规划的研究与编制，承担蒙西电网主网、配网和信息、通信网规划的研究与编制，负责 220 kV 及以下电网的规划和评审，指导盟市供电单位编制地区电网规划并纳入蒙西电网发展规划和专项规划，加强电网规划建设评审、技术经济评价、结算审查、审计审价、运营监控等技术支撑性业务。

为了更好地落实输变电工程造价管理工作，满足工程造价管理需要，提高工程造价管理效率，对内蒙古电力输变电工程实际数据进行了系统的分析，选取了内蒙古电力公司 170 个输变电工程样本，分别按照电压等级和工程类型对 110 kV 及以上变电工程、110 kV 及以上架空线路工程、110 kV 及以上电缆线路工程、35 kV 变电工程、35 kV 架空线路工程、35 kV 电缆线路工程进行详细分析。

2　输变电工程造价分析过程

本文以 110～500 kV 变电工程、110～500 kV 线路工程为例介绍输变电工程造价分析主要过程，具体如下。

2.1　110～500 kV 变电工程造价分析

（1）变电工程总体情况分析

内蒙古电力变电工程主要分为新建和扩建，分别包括 110 kV、220 kV、500 kV，通过主变容量统计得

人民邮电出版社

出工程数量，从工程类别维度计算工程新建、扩建比例，从电压等级维度分析工程数量占比情况。

在分析变电工程总体造价水平后，分别对新建变电工程和扩建变电工程的造价水平进行详细分析，其中包括对造价样本数据的离散性分析，分析导致离散程度较大的主要原因，见表 1。

（2）变电工程投资结余分析

按照电压等级和变电容量划分，分别对新建变电工程和扩建变电工程的投资结余情况及结余率离散性进行详细分析，见表 2。

分析结余率较高的工程的主要结余费用，并分析造成结余的主要原因。相对标准方差偏移表示从概算到结算阶段工程投资样本数据群离散程度的变化，客观上反应某一类型工程中不同项目结余率的离散性，即各项目之间投资结余率差异较大。

（3）变电工程主要设备材料价格水平分析

在变电工程中，变压器、断路器、电力电缆等构成了变电工程的主要设备，是影响变电工程设备材料购置投资的重要因素，分析主要设备材料投资占比和不同年份设备材料价格，并分析影响主要设备材料价格的主要因素。

2.2 110～500 kV 线路工程造价分析

（1）线路工程总体情况分析

线路工程包含架空线路工程和电缆线路工程，分别按照线路种类、电压等级和导线截面统计线路工程数量及线路长度。在此数据基础上对架空线路工程、电缆线路工程样本数据进行离散性分析，分析导致部分工程离散程度较大的原因，如图 1 所示。

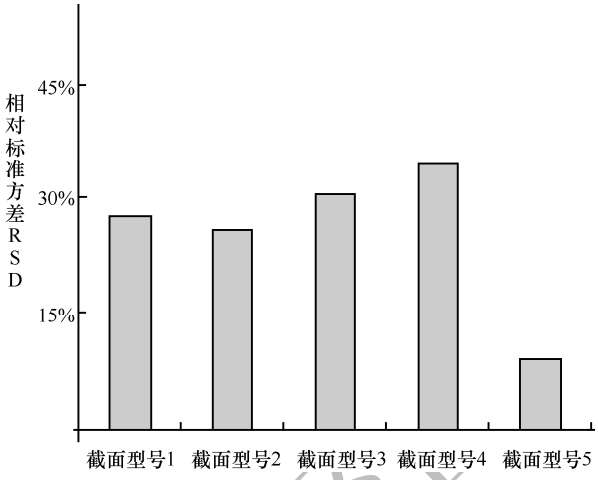


图 1 结算投资样本精密度

（2）线路工程投资结余分析

线路工程结余率可按照电压等级、导线截面等维度详细分析总体结余情况、结余率以及线路工程费用构成各部分结余情况和结余率，分析导致结余的主要原因。

（3）线路工程主要设备材料价格水平分析

主要设备材料价格的分析按照电压等级分别进行分析，除此之外，纵向对比不同年份主要设备材料价格，分析价格变动幅度较大的影响因素，分析线路工程总投资对主要设备材料的敏感性。

2.3 建设场地征用及清理费分析

对变电工程和线路工程分别进行分析，分析各地区影响建厂费用结算指标的影响因素，分析建场费结余及趋势分析，对各盟市建场费结算指标进行对比分析，如图 2 所示。

表 1 新建变电工程概算总投资样本精密度统计

电压等级	主变容量	项目数量	概算		样本均值	样本精密度	
			最大值	最小值		标准方差	相对标准方差
500 kV							
220 kV							
110 kV							

表 2 新建变电工程分类结余情况表

电压等级	主变容量	项目数量	概算总投资	结算总投资	分类平均结余率	相对标准方差偏移
500 kV						
220 kV						
110 kV						

人民邮电出版社

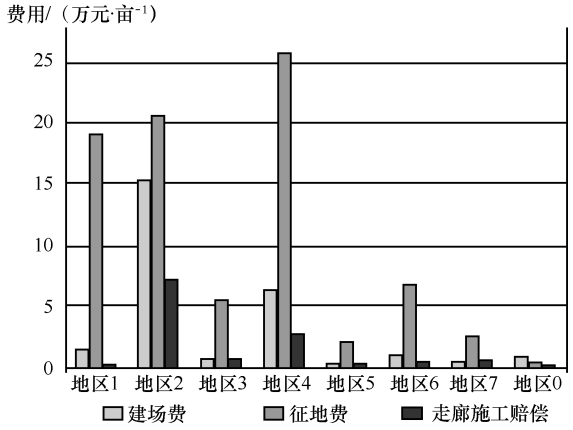


图 2　建场费各费用指标对比

3　完善输变电工程造价管理的建议

3.1　加强设计阶段关键环节管控

根据国内外工程造价资料分析，在项目生命周期中，设计阶段（尤其是可行性研究阶段）对工程项目造价的影响程度最大，因此需要进一步提高电网规划能力，超前谋划工程建设工作（如选线、征地工作等），提前考虑对工程建设有重大影响的因素，尽可能做到早谋划早协商早解决，消除由于不确定因素导致工程造价有较大变化的情况。另外，需要加强可行性研究阶段、初步设计阶段对实地情况的勘察，尽可能全面地掌握外部环境的实际情况，避免由于现场勘察不到位导致工程出现大量变更的情况。此外，还需完善技术方案的比选和造价的评价机制。

3.2　形成各地区造价控制标准

在工程项目造价管理中通常通过评审手段完成对工程造价的控制，若在评审时有据可依，将会大大地提高评审效率。根据电压等级和技术条件等前提，首先形成总体造价管控标准，在总体造价管控标准范围内，各地区根据本地区特点，形成本地区造价管控标准。每年输变电工程项目众多，以本地区造价管理标准为依据，工程项目管理部门造价人员也可以借助此标准提高对工程项目造价的监督效率。

3.3　扩大主要设备材料框架招标效益

从造价分析结论可知，当某种设备材料的采购量达到一定数量时体现出设备材料大批量框架招标带来的规模经济效益，结合地区工程特点可以考虑扩大框架招标范围，可以节约设备材料成本。

3.4　注重造价分析成果的有效运用

造价分析的最终目标是为输变电工程造价管理工作提供真实的数据支撑，但目前造价分析依然主要停留在造价分析本身，缺乏对造价分析的结论开展广泛应用（如缺乏对设计评审工作的应用、缺乏对招投标评审的应用、缺乏对工程建设中造价管理的监督指导等），工程造价的宝贵经验未能被有效用于指导造价管理工作。

以造价分析优化设计标准，电网工程通用设计、通用设备、通用造价、标准工艺是电网输变电工程设计和施工的通用标准。由于技术不断更新和市场供需的动态变化，通用标准也需要不断变化，以满足输变电工程建设管理需要，以造价分析优化设计标准。将通用标准应用到实际工程中施工方案和真实造价数据进行分析，通过对多个样本数据分析总结通用标准优化经验，提高通用标准普遍适用性，从而达到有效控制造价的目的。

3.5　加强施工现场的管理

（1）提高技术经济人员施工现场参与度

设计阶段需要进行设计方案比选和造价评审，造价管理部门尤其重视批复概算对整个工程造价的指导作用。造价主要形成阶段就是工程建设期，因此需要着重提高对工程建设期造价的管理能力。项目负责部门造价管理人员要参与到工程现场相关造价管理业务中，提高在施工过程中的参与度，弥补业主项目部管理人员“重”施工现场进度质量、安全管理，“轻”工程造价管理的不足。

此外还需重视项目管理部门技术经济人员造价管控能力的培养，通过对历史工程结算数据分析和项目施工方案的研究，可以总结并推广造价管控经验，供技术经济人员学习借鉴，快速提高工程现场造价管理的管理水平。

（2）提高工程变更签证管控力度

在工程造价管理中常常无法及时关注施工现场实际情况（如施工是否按照施工图纸要求施工、施工过程是否符合标准化工艺要求等）。在业主项目部和监理单位无法全天候监督工程施工情况时，建议可以借助施工现场监控设备对施工现场进行远程监控，加强施工现场管理，尤其对隐蔽工程及工程变更的管理。

此外，对于线路工程可以借助地理信息系统进行线路走向监控，在设计阶段将设计图纸中线路杆塔坐标固化在地理信息系统上，在施工阶段及时上报工程进度及线路走向。通过移动监控设备核对施工现场情况，可以及时判断工程变更带来的造价增加是否合理，从而及时

人民邮电出版社

了解施工现场情况，实现对工程造价的有效管控。

（3）建立施工阶段性造价快速分析机制

造价分析主要指针对结算完成的工程进行造价分析，由于输变电工程建设周期长，一个工程项目短则一两年，长则三四年，加之工程完工后的结算、审计工作也耗用较长时间，在项目审计后再进行造价数据分析导致分析工作相对滞后，无法及时反映工程造价的真实情况。

为加强造价数据分析的时效性，实现对在建工程造价的实时管控，需要建立施工阶段性造价的快速分析机制。不同于工程结算后造价分析，建设过程中的阶段性分析强调时效性，如在工程建设中，与工程造价最相关的就是工程合同进度款，工程合同进度款一般是施工单位按照合同条款在规定的工程量完成的情况下即可申请进度款支付，为保障阶段性造价分析准确性，需严格管理工程合同进度款，分析结果应用于未完工程的合同监控。

4 结束语

输变电工程项目造价管理是一项复杂的工作，为了达到真正控制项目成本的目的，需要从工程项目的每一个阶段入手，拓宽管理范围，深入分析问题，积极寻找应对方法，并把工程造价分析作为一项常态化的工作开展，不断调整工作思路，造价管理工作一定会迈上一个新的台阶。

参考文献：

[1] 蒙电青春公众号. 集团公司 2018 年年中工作会议精神解读[Z]. 2018.

[2] 内蒙古电力集团有限责任公司. 2017 年信息公开年报[EB]. 2017.

[3] 吴位友, 张圣轩. 全寿命周期工程造价信息数据共享研究[J]. 工程建设与设计, 2019.

[4] 商桑, 温卫宁, 任妍, 等. 输变电工程造价控制指标深化研究[J]. 中国电力企业管理, 2018, 528(15): 70-71.

[5] 徐丹, 温卫宁, 卢艳超, 等. 基于BP神经网络的输变电工程造价偏差动态预警[J]. 中国电力企业管理, 2018, 525(12): 77-78.

[6] 国方媛. 工程造价管理动态评价方法探究[J]. 中国电力企业管理, 2016(6).

[7] 韩放. 500 kV 输变电工程项目后评价实证研究[D]. 北京: 华北电力大学, 2017.

[8] 亓鹏. 基于全寿命周期的输变电工程项目管理分析[D]. 北京: 华北电力大学, 2017.

[9] 卢艳超. 国内外输变电工程造价管理模式对比研究[J]. 工程经济, 2017(4).

人民邮电出版社

数字化审计体系在电力行业的实践

赵恩来，陈曦，崔颢
（北京国网信通埃森哲信息技术有限公司，北京 100032）

摘　要：随着我国持续推进信息化建设，信息技术在企业中的使用范围日益广泛，深刻影响着审计环境、审计模式等，电力行业审计发展的关键在于信息化，信息化的关键在于数字化，审计的数字化转型成为必然。数字化审计的核心是采集、转换、整理和分析数据，其模式包括审计管理、审计实施、质量控制、数据共享等全方位的数字化。通过对数字化审计在电力行业的实践开展研究，阐述数字化审计的主要特点以及党和国家对数字化审计提出的新要求，详述数字化审计平台的构建及功能、预期成效及未来发展趋势，从而促进当前数字化审计的优化和提升。

关键词：数字化审计；电力行业；实践

1　引言

随着我国电力行业信息化水平的逐年提高，信息技术在电力行业日常经营中的使用范围日益广泛，其审计模式也由传统审计方法，逐步向数字化审计模式转型，以适应当前电力行业业务模式在高度信息化环境下对审计方式的新挑战。

数字化审计以计算机信息系统和底层数据为基础，应用计算机和信息化手段方法，对电子数据进行采集、转换、分析等处理，把握审计重点，精确延伸，搜集审计证据，实现审计目标。可以说，数字化审计是审计工作的未来发展方向，推进数字化审计，坚持走科技强审之路，是电力行业实现全面审计、高效审计、优质审计的必由之路。目前，我国电力行业已经开展数字化审计探索，积极创新数字化审计管理模式，并取得了较好的效果。

2　数字化审计的主要特点

数字化审计是传统审计模式在信息化时代发展的必然结果，尽管其与传统审计模式一脉相承，但无论从新时代战略背景与审计要求，还是高新技术与审计方法等方面，数字化审计相较传统审计均存在鲜明的特点。

（1）结合新时代战略，实现高质量发展

实现电力行业高质量发展，一直是党和国家坚持不懈追求的目标。审计人员围绕电力企业提升审计质效、推进审计范围全覆盖，通过数字化的手段，切实解决审计工作中的实际问题。基于国家监督的新要求、公司发展的新需求以及信息技术的快速发展，通过数字化审计体系的构建，数字化审计最终将赋能电力行业的高质量发展。

（2）利用大数据技术，助力风险点控制

利用先进的大数据技术，可以有效分析各个审计风险点，使风险管控融入审计业务，实现审计的全覆盖。此外，通过运用大数据技术构建审计模型并采用多维手段开展审计工作，可以进行全量、跨系统的数据分析及比对核查，精确定位问题风险点，从而实现以抽查为主的传统审计模式向以实时的持续性审计监督为主的新型审计模式的转变。同时，借助大数据技术为数字化审计赋能，通过增强提升的大数据存储、处理、挖掘能力以及非结构化数据的分析能力，可以促进建模灵活性与易用性的提升，以便更为有效地揭示企业管理中存在的风险点与薄弱点，更好地进行风险管控。

（3）区别传统式审计，现代审计新方式

随着我国市场经济的不断发展，党和国家对审计工作提出新要求，被审计数据量日益增大、数据结构日益复杂，传统的审计工作方式已不足以应对企业复杂多变的内外部环境，传统审计的人海战术也已经无法满足审计工作量成倍增长的需求。借助数字化审计，

人民邮电出版社

利用大数据分析技术，改变传统抽样审计、现场审计、事后审计的审计方式，跨越式扩大审计范围，加强审计力度，深层次变革审计理念、深化审计监督事项，强化治理作用，提升监督质效。

3 “三型两网”战略对数字化审计提出的新要求

2019 年国家电网有限公司“两会”做出全面推进“三型两网”建设，加快打造具有全球竞争力的世界一流能源互联网企业的战略部署，为电力行业企业的发展提供了方向。承载电力流的坚强智能电网与承载数据流的泛在电力物联网，相辅相成、融合发展，形成强大的价值创造平台，共同构成能源流、业务流、数据流“三流合一”的能源互联网。泛在电力物联网，实现人、机、物实时在线、广泛互联，与坚强智能电网相互渗透和深度融合，贯通能源汇聚、传输、转换、利用全链条。坚持智能电网与泛在电力物联网的互联互通、融合发展，是国家电网有限公司应对内外部环境及形势，从电力企业向能源互联网企业转型的重要且必要举措。

在对内业务方面，传统审计电网业务领域（如财务、营销、工程、人力资源等）、业务流程及业务实现模式等将随着泛在电力物联网的建设推进发生改变，审计工作需要随审计对象的业务规则的变化而快速响应，迅速变化。对内业务需实现数据一次采集或录入、共享共用，实现全电网拓扑实时准确，端到端业务流程在线闭环；全业务统一入口、线上办理，全过程线上即时反映。

在对外业务方面，非传统领域的全新审计对象（互联网金融、大数据运营、大数据征信、线上供应链金融、虚拟电厂、网上国网等线上率较高的新型业务），需要强有力的数字化手段予以支撑发现新风险、新问题，促进公司治理，向能源互联网企业转型。对外业务建成“一站式服务”的智慧能源综合服务平台，各类新兴业务协同发展，形成“一体化联动”的能源互联网生态圈；在综合能源服务等领域处于引领位置，新兴业务成为公司主要利润增长点。

在业务层面（对内业务、对外业务）带来的变革对于审计是新的挑战，在数据共享、基础支撑层面的变革对于审计工作的开展则是更为有利的支撑。根据当前泛在电力物联网建设方案的《企业中台建设》专项方案规划，数据中台将完善提升全业务统一数据中心相关组件能力，实现人员、组织、客户、供应商等企业级主数据共建共享，构建数据服务能力，促进数据横向跨专业共享、纵向跨层级按需获取；有效支撑营配贯通、泛在电力物联网营销服务、多维精益管理、数字化审计、智慧供应链、网上电网、基建全过程综合数字化管理、供电服务指挥等重点建设任务；推动电力系统各环节终端随需接入，实现电网和客户状态“实时感知”；推动公司全业务数据统一管理，实现内外部数据“即时获取”；推动共性业务和开发能力服务化，实现业务需求“敏捷响应、随需迭代”。

4 数字化审计平台的构建及功能

构建数字化审计平台是电力行业推进数字化审计的重要实践。近年来国家电网有限公司以信息化管理建设应用成果为基础，积极探索数字化审计工作模式，组建数字化审计工作室，开展数字化审计平台建设项目，支撑审计模式向远程持续审计监督和集中非现场数据分析等多项路径转变。

国家电网有限公司以全业务统一数据中心为基础，集成现有审计信息系统，基于公司信息化总体要求，按照“典型设计两级部署统一展示”模式，多方面多层次满足审计管理和审计作业需求，建设“开放、融合、动态、智能”的数字化审计平台。数字化审计平台构建分为 4 个部分：审计门户、审计管理域、审计作业域、审计基础数据域。其中，审计门户是数字化审计平台的统一入口和成果展示平台，采用一级部署、两级应用方式，总部可以通过级联方式穿透查看各单位门户内容；审计管理域是在原综合管理系统基础上，对系统功能进行扩展、优化、深化，并入原审计门户中审计项目统计分析的功能；审计作业域整合 ERP 审计系统、管控业务审计系统、智能持续审计系统，将分散的、重复的、单纯查询式的功能点进行合并优化，并按照业务逻辑流程，参照审计署金审工程功能点分类体系和公司审计业务实际，形成具有查询穿透力强、多维综合分析、智能疑点筛查功能的模型体系，并且增加了模型试验和自主分析等高级应用功能；审计基础数据域从多渠道获取审计数据，以全业务统一数据中心数据为最主要数据来源，期望能够突破多年数据获取不畅、数据质量不高的瓶颈。

5 数字化审计平台的预期的成效

通过对数字化审计的不断探索，国家电网有限公

司明确了数字化审计的基本思路，形成了具有电力行业特色的数字化审计作业模式，通过信息技术的创新应用，突破了现有审计存在的“瓶颈”，推动了审计监督逐步走向预测式审计新格局，为促进公司治理体系和治理能力现代化积累了经验。

（1）多措并举，推动实现新发展

通过信息技术与审计工作的深度融合，国家电网有限公司深层次变革审计理念及创新组织方式，推动审计工作技术水平和人员能力跨越式发展。

1）国家电网有限公司搭建了“1+*N*”工作模式，构建远程非现场数据分析与现场重点核实一体化的项目组织方式。按照“总部适时抽查，区域审计中心重点关注，省公司自主开展”的工作思路，构建多层次远程在线持续监督体系，有效推动审计资源整合，推进向以持续监督为主的现代审计转变。

2)国家电网有限公司主动对接全业务统一数据中心建设进度，运用大数据挖掘工具和分析方法，将成熟的审计思路转化为数字化审计模型，公司系统各单位构建各类审计模型，实现从跨单位、跨专业、跨年度的海量业务数据中快速精准锁定问题疑点信息；强化审计对先进技术方法的创新应用，开展地理信息系统、模糊检索、机器人等审计工具的研发，推动审计技术现代化。

3)国家电网有限公司审计部积极培养审计人员大数据思维，积极部署应用各类数据分析工具和智能审计模型，提升数据处理、分析、挖掘能力，拓宽了系统性审计思路，提高了审计人员从宏观层面分析以及从体制、制度和机制层面解决问题的能力。

（2）技术引领，促进实现新效能

以提升审计监督质量和拓展审计监督广度、深度为着力点，强化信息化技术手段在审计业务各环节的应用，向信息化要资源，向大数据要效率，推动审计效能有效提升。国家电网有限公司依托大数据分析工具和智能审计模型，精准定位审计重点，科学制定审计计划，合理配置审计资源，现场审计工作做到“有的放矢”，现场审计人员减少、时间压缩，审计成本明显降低；发挥大数据全量数据优势，审计监督逐步由抽样向全量审计转变，实现审计监督“由点及面”，全面推进审计“全覆盖”；深挖数字化技术优势，横向拓展业务审计监督领域，纵向对审计发现问题一查到底，跨域梳理风险事项内在关联逻辑，深度挖掘问题产生的根源，深入比对、核查、分析两系统账务、报表等数据，发现一体化存在业务融合不足、系统对接不畅等问题。

（3）持续监督，助力实现新价值

国家电网有限公司利用数字化审计工作室开展持续审计监督工作，发挥数字化作业优势，实现由单一部门存在的问题转变为对普遍性、倾向性问题的集中揭示，审计的整体性和影响力进一步扩大，审计建议更具有针对性、全面性，有效促进公司改革推进和治理提升。

首先，公司适应“上审下”体制变革，发挥审计资源向上集约优势，开展对重点项目、重大决策、重大资金、重大风险的远程在线审计，实现审计工作关口前移，提升审计工作的穿透力和时效性，有效促进了发现问题的立行立改。其次，公司依托数字化审计数据量全、核查速度快、业务覆盖面广的优势，全面扫描被审计单位数据资源，发现问题快速拓展核查范围、不留死角。最后，公司充分利用发现问题成果，剖析问题产生根源，提高审计监督站位，实现审计成果的深度利用，促进审计监督由防御为主向积极控制转变。在抽查工作中发现各被审计单位工作存在落实不到位、流程不畅通等问题，据此建议制定优化业务融合和流程贯通的工作实施细则或指导性意见，指导各单位做好数据差异比对分析及数据治理工作。

6 结束语

国家电网有限公司在构建数字化审计平台，推挤数字化审计工作模式创新方面的实践，对我国电力行业开展数字化审计模式改革创新有着重要的借鉴意义。通过前文对国家电网有限公司数字化审计工作的总结分析，若要大力推进我国电力行业数字化审计工作，需要在继承当前审计工作优点的基础上，积极开展高质量的改革及创新工作，以使电力行业审计模式不断向数字化及信息化迈进。

（1）编制完善的数字化审计规章制度

规章制度是保证企业开展工作规范性及实效性的保障，数字化审计工作也不例外。电力行业应通过实施有效创新的方式，编制完善的数字化审计规章制度，创设出符合自身行业化特色的数字化审计工作体系。

（2）建设高效的数字化审计平台

1）加速数据治理工作，提升电力行业企业数据质量，利用人工智能等技术加速半结构化数据及非结构化数据向结构化数据转变。高质量的数据是开展数字

人民邮电出版社

化审计的基础及保证，只有不断提升电力行业数据质量，才能满足审计工作模式不断变革的要求，促进数字化审计模式创新；2）搭建数字化审计平台，聘请外部承建单位，协同企业内部审计专家设计开发开放、融合、动态、智能的数字化审计平台，支撑数字化审计工作模式的转变；3）对数字化审计平台及数据源开展日常维护，保证数字化审计平台提取数据的安全性和有效性，加强数据的访问权限控制，记录授权使用用户的操作日志，配备技术人员进行数字化审计平台的日常维护和修整，保证平台运行的稳定性。

（3）提升审计从业人员数字化水平

审计专家是电力行业数字化审计工作的实践者，数字化审计模式的转变需要审计从业人员素质及能力的配套升级。数字化审计模式下，不但要求审计人员掌握更多的宏观经济知识，更要求审计人员掌握信息化环境下审计技术、方法和手段，以适应数字化审计模式下对审计人员的更高要求。数字化审计模式下，审计从业人员需要在以下几方面进行能力提升：1）认真学习国家出台的最新审计法规及准则，保持对国家层面审计指导精神的敏锐度；2）提升跨业务、跨领域相关知识储备，充分利用数字化审计平台可以提取全域数据的特点，有效开展数据发掘及分析工作，突破传统审计的局限性；3）成立数字化审计专家小组，重点培养数字化审计专业人才，并以专家培训基层审计人员的模式整体提升电力行业审计从业人员数字化审计工作水平。

参考文献：

[1] 谢志华, 倪志伟, 罗少东. 国家电网公司数字化审计的具体实现路径[J]. 财务与会计, 2018(1): 75-76.

[2] 刘向林. 推动电力行业数字化审计模式发展[J]. 大众用电, 2018, 32(12): 37-38.

[3] 唐玲. 电网企业数字化审计管理模式创新实践[J]. 会计师, 2008, 306(3): 53-54.

[4] 孙静, 邵天龙, 王小静. 企业数字化审计模式的创新与实践[J]. 中国商论, 2018(26): 122-123.

[5] 佚名. 构建数字化持续审计工作体系促进审计监督全覆盖[J]. 科技与创新, 2019, 123(3): 98-99.

[6] 刘晨, 石灿, 王东莲. “多系统”模式下电网企业数字化审计初探[J].中国内部审计, 2019(07): 35-37.

[7] 秦文云, 邓洪跌, 范蓓, 等. 电力企业内部经济责任数字化审计的探索与实践[J]. 中国内部审计, 2019(07): 64-66.

[8] 陈静. 电网公司数字化审计的实现路径[J]. 中外企业家, 2019(14): 19.

[9] 聂炜, 刘向林. 电网企业数字化审计模型的构建[J]. 大众用电, 2019, 34(3): 44-45.

[10] 贾柚. 人工智能对审计行业的影响研究[J]. 中国商论, 2019(11): 172-173.

[11] 金兴华, 谢丹丹. 电网企业物资专业管理数字化审计探讨[J]. 大众用电, 2019, 34(5): 41-42.

[12] 党福香. 数字化审计模式在送达审计中的探索[J]. 中国市场,2019(6): 192-194.

[13] 王向阳, 魏丽雅, 郑勇, 等. 数字化共享审计模式在电网企业防范风险中的应用[J]. 中国内部审计, 2018(12): 12-18.

[14] 傅夏懿. 数字化审计平台的构建与应用[D]. 南京:南京邮电大学, 2018.

[15] 韩锟, 李有华, 张俊民. 国家电网公司内部审计工作的创新与实践[J]. 财务与会计, 2018(19): 80-81.

人民邮电出版社

通信机楼动力母线供电方案

邵正忠
（中国电信股份有限公司南京分公司，江苏 南京 210008）

摘　要：介绍了通信机楼动力母线的 3 种方式：变压器 2*N* 模式配电系统动力母线方案、变压器 *N*+1 模式配电系统动力母线方案、变压器 *N* 模式配电系统动力母线方案。对 3 种方案进行了比较，给出了一般性建议。其中，对第 3 种方案进行了详细列举分析。

关键词：交流供电；动力；母线；路由；切换

1　引言

通信机楼一般设一个集中的配电房，为了将电源输送到各楼层，常采用动力母线供电方案。动力母线上接的负载较多，一旦出故障，影响范围较大。为了防止动力母线故障引起的负载失电，针对不同的供电模式，要制定不同的动力母线备份方案。

2　动力母线备份方案

动力母线备份方案分为：自动切换装置（ATS）如图 1 所示；手动切换装置（MTS）如图 2 所示。

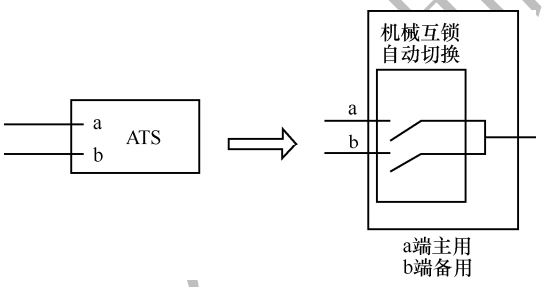


图 1　自动切换装置

2.1　变压器 2*N* 模式配电系统动力母线方案

对于变压器 2*N* 模式配电的系统，变压器之间成对备份。如变压器 T_1 与变压器 T_2 成对备份，则变压器 T_1、T_2 的动力母线成对配置，变压器 T_1 的输出母线 Bus_1 与变压器 T_2 的输出母线 Bus_2 互为备份。为节省投资，一台变压器可以只设一套母线系统。拓扑图如图 3 所示。

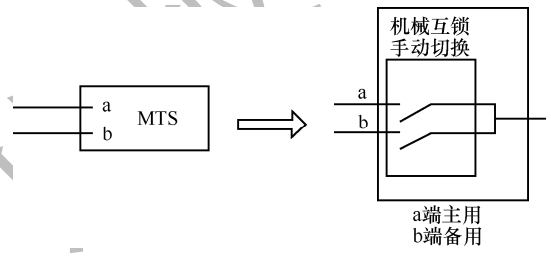


图 2　手动切换装置

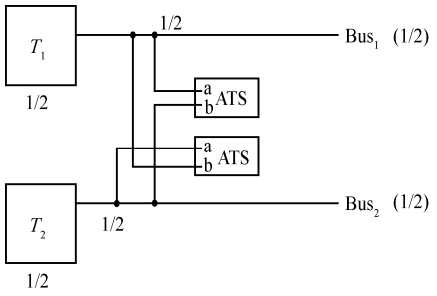


图 3　变压器 2N 模式配电系统动力母线

若单台变压器的容量为 *S*，采用均分负载设计时，则每台变压器的允许常态带载率 η=1/2，单母线的负载常态值为 *S*/2，两台变压器的最大带载能力为 *S*。*n*（*n* 为偶数）台变压器的最大带载能力为 *nS*/2。

2.2　变压器 *N*+1 模式配电系统动力母线方案

对于变压器 *N*+1 模式配电的系统，变压器 T_1–T_n 与 T_{n+1} 进行备份，即 T_{n+1} 为其他所有变压器的备份变压器。所有变压器采用单母线设计时，母线 Bus_{n+1} 为其余母线的备份母线。负载切换装置不宜采用自动切换方式，应采用手动切换方式。拓扑图见图 4。

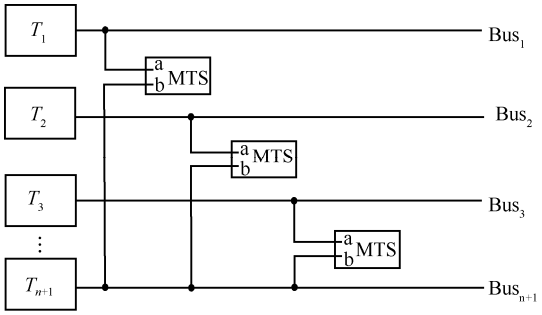


图 4　变压器 N+1 模式配电系统动力母线

若单台变压器的容量为 S，变压器 T_1–T_n 的常态带载能力为 S，最大带载率 η=1。单母线 Bus_1–Bus_n，每条母线的负载带载能力为 S。变压器 T_{n+1} 的带载能力为 S，常态带载为 0，在某一台变压器或母线故障，负载全部切换到变压器 T_{n+1} 时，变压器 T_{n+1} 能够承担切换负载。n+1 台变压器的最大带载能力为 nS。系统最大带载率 $\eta=(n-1)/n$

2.3　变压器 N 模式配电系统动力母线方案

对于变压器 N 模式配电的系统，变压器 T_1–T_n 内部进行容量备份，输出母线 Bus_1–Bus_n 之间采用容量备份，即当一条母线故障时，通过合理设计，可以将全部负载切换到其他无故障母线上。为了便于理解，分别列出两台变压器单母线方案等 9 种情形，进而得出多台变压器多母线方案。

（1）两台变压器单母线方案

两台变压器之间进行容量备份。此种方式，即为变压器 2N 模式配电系统，母线之间可以互为备份，切换装置可以采用自动方式，也可采用手动方式。采用手动切换时，拓扑图如图 5 所示。

若单台变压器的容量 S，采用均分负载设计时，则每台变压器的允许常态带载率 η=1/2，单母线的负载常态值为 S/2，两台变压器的最大带载能力为 S。n 台变压器的最大带载能力为 nS/2，系统最大带载率 η=1/2。

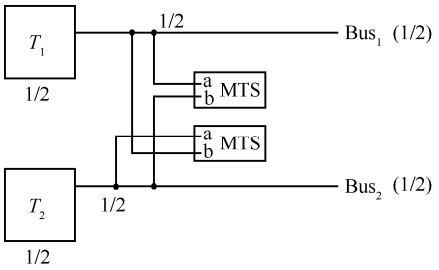


图 5　两台变压器单母线方案

（2）两台变压器双母线方案

两台变压器之间进行容量备份。每台变压器设计两条输出母线，不同变压器的母线之间容量备份，拓扑图如图 6 所示。容量备份方式举例如下：若母线 Bus_1 故障，其一半负载切换到 Bus_3 上，另一半负载切换到 Bus_4 上。

若单台变压器的容量 S，采用均分负载设计时，则每台变压器的允许常态带载率 η=4/5，单母线的负载常态值为 2S/5，两台变压器的最大带载能力为 8S/5。n 台变压器的最大带载能力为 4nS/5，系统最大带载率 η=4/5。

（3）两台变压器三母线方案

两台变压器之间进行容量备份。每台变压器设计 3 条输出母线，不同变压器的母线之间容量备份，拓扑图如图 7 所示。容量备份方式举例如下：若母线 Bus_1 故障，其负载分成 3 份，分别切换到 Bus_4、Bus_5、Bus_6 上。

若单台变压器的容量 S，采用均分负载设计时，则每台变压器的允许常态带载率 η=9/10，单母线的负载常态值为 3S/10，两台变压器的最大带载能力为

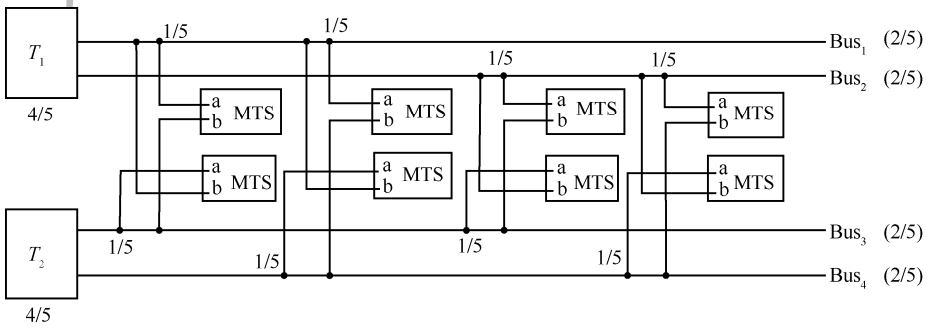


图 6　两台变压器双母线方案

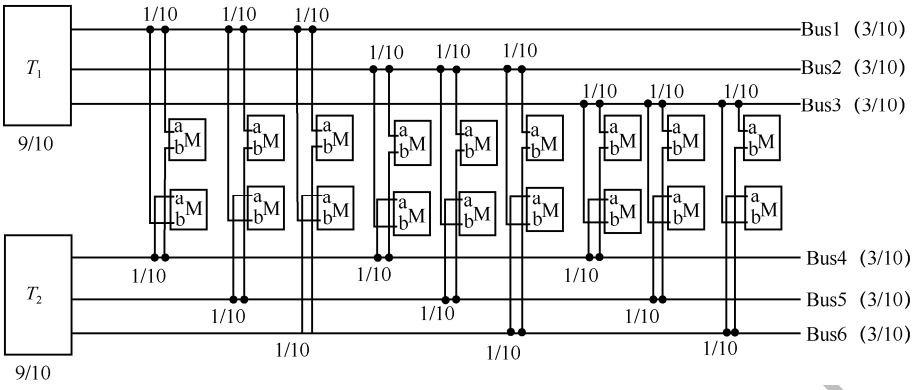


图 7　两台变压器三母线方案

9*S*/5。*n* 台变压器的最大带载能力为 9*nS*/10，系统最大带载率 η=9/10。

（4）两台变压器四母线方案

两台变压器之间进行容量备份。每台变压器设计 4 条输出母线，不同变压器的母线之间容量备份，拓扑图见图 8。容量备份方式举例如下：若母线 Bus_1 故障，其负载分成 4 份，分别切换到 Bus_5、Bus_6、Bus_7、Bus_8 上。

若单台变压器的容量为 *S*，采用均分负载设计时，则每台变压器的允许常态带载率 η=16/17，单母线的负载常态值为 4*S*/17，两台变压器的最大带载能力为 32*S*/17。*n* 台变压器的最大带载能力为 16*nS*/17，系统最大带载率 η=16/17。

（5）3 台变压器单母线方案

3 台变压器之间进行容量备份。每台变压器设计一条输出母线，不同变压器的母线之间容量备份，拓扑图如图 9 所示。容量备份方式举例如下：若母线 Bus_1 故障，其负载分成 2 份，分别切换到 Bus_2、Bus_3 上，。

若单台变压器的容量为 *S*，采用均分负载设计时，则每台变压器的允许常态带载率 η=2/3，单母线的负载常态值为 2*S*/3，3 台变压器的最大带载能力为 2*S*。*n* 台变压器（*n* 为 3 的倍数）的最大带载能力为 2*nS*/3，系统最大带载率 η=2/3。

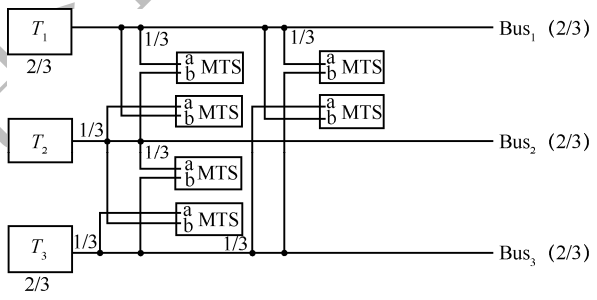


图 9　3 台变压器单母线方案

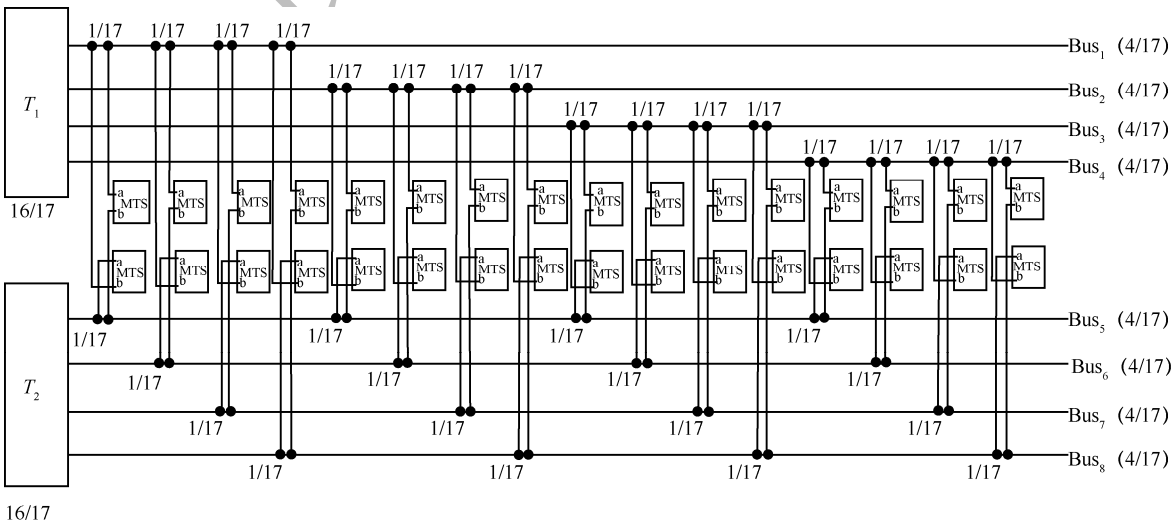


图 8　两台变压器四母线方案

（6）3 台变压器双母线方案

3 台变压器之间进行容量备份。每台变压器设计两条输出母线，不同变压器的母线之间容量备份，拓扑图如图 10 所示。容量备份方式举例如下：若母线 Bus_1 故障，其负载分成 4 份，分别切换到 Bus_3、Bus_4、Bus_5、Bus_6 上。

若单台变压器的容量为 S，采用均分负载设计时，则每台变压器的允许常态带载率 η=8/9，单母线的负载常态值为 4S/9，3 台变压器的最大带载能力为 8S/3。n 台变压器（n 为 3 的倍数）的最大带载能力为 8nS/9，系统最大带载率 η=8/9。

（7）4 台变压器单母线方案

4 台变压器之间进行容量备份。每台变压器设计一条输出母线，不同变压器的母线之间容量备份。拓扑图如图 11 所示。容量备份方式举例如下：若母线 Bus_1 故障，其负载分成 3 份，分别切换到 Bus_2、Bus_3、Bus_4 上。

若单台变压器的容量为 S，采用均分负载设计时，则每台变压器的允许常态带载率 η=3/4，单母线的负载常态值为 3S/4，四台变压器的最大带载能力为 3S。n 台变压器（n 为 4 的倍数）的最大带载能力为 3nS/4，系统最大带载率 η=3/4。

（8）4 台变压器双母线方案

4 台变压器之间进行容量备份。每台变压器设计二条输出母线，不同变压器的母线之间容量备份，拓扑图如图 12 所示。容量备份方式举例如下：若母线 Bus_1 故障，其负载分成 6 份，分别切换到 Bus_3、Bus_4、Bus_5、Bus_6、Bus_7、Bus_8 上。

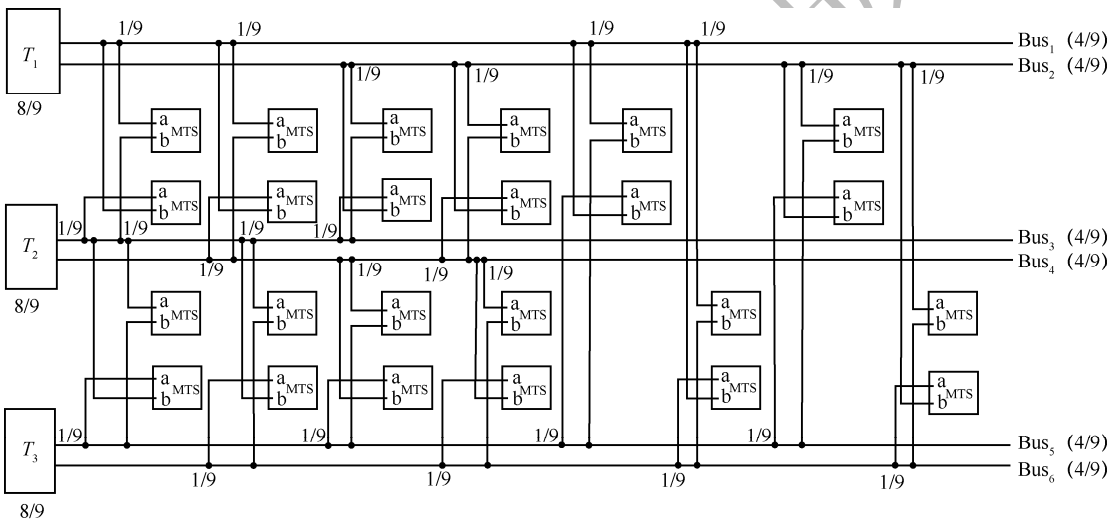


图 10　3 台变压器双母线方案

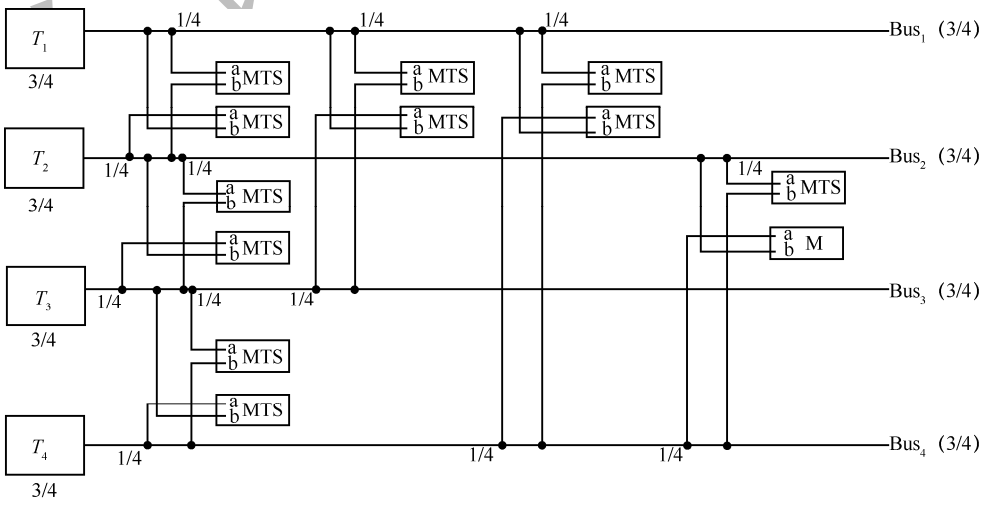


图 11　4 台变压器单母线方案

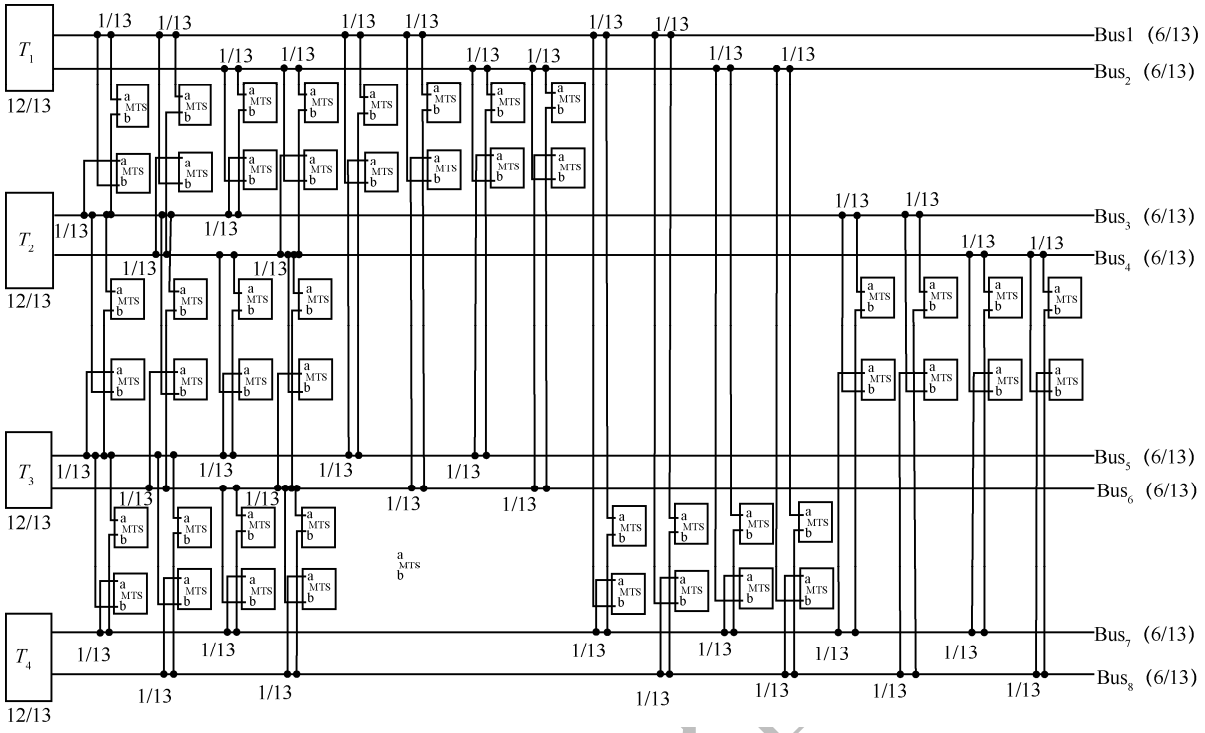


图 12　4 台变压器双母线方案

若单台变压器的容量为 S，采用均分负载设计时，则每台变压器的允许常态带载率 η=12/13，单母线的负载常态值为 6S/13，4 台变压器的最大带载能力为 48S/13。n 台变压器（n 为 4 的倍数）的最大带载能力为 48nS/13，系统最大带载率 η=12/13。

（9）多台变压器多母线方案

n 台变压器之间进行容量备份。每台变压器设计 m 条输出母线，不同变压器的母线之间容量备份，拓扑图如图 13 所示。容量备份方式举例如下：若母线 Bus1 故障，其负载分成（n−1）m 份，分别切换到 Bus $_{m+1}$…Bus$_{nm}$ 上。

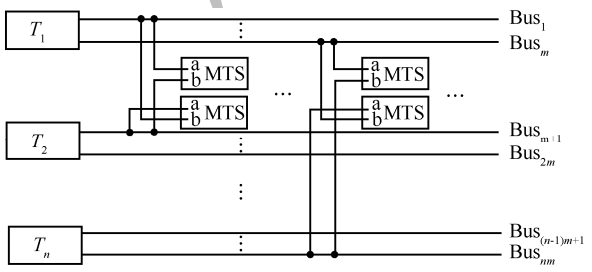


图 13　多台变压器多母线方案

若单台变压器的容量为 S，采用均分负载设计时，则每台变压器的允许常态带载率 $\eta=\dfrac{(n-1)mm}{(n-1)mm+1}$，单母线的负载常态值为 $\dfrac{(n-1)m}{(n-1)mm+1}S$，$n$ 台变压器的最大带载能力为 $\dfrac{(n-1)m}{(n-1)mm+1}nS$，系统最大带载率 $\eta=\dfrac{(n-1)mm}{(n-1)mm+1}$。

根据 n、m 的取值不同，系统最大带载率不同，列表见表 1。

从表 1 中可以看出以下几点。

- 每台变压器输出母线越多，均分负载下，每台变压器允许的常态带载率越大。
- 每台变压器输出母线 3 条及以上时，均分负载下，变压器允许常态带载率≥90%。
- 变压器数量载多，均分负载下，每台变压器允许的常态带载率越大。
- 变压器数量为 5 及以上时，均分负载下，即使每台变压器采用单母线，变压器允许常态带载率≥80%。

人民邮电出版社

表 1　每台变压器允许常态带载率 η 与变压器数量 n 及单变压器母线数量 m 的关系

η		m					
		1	2	3	4	5	6
	2	50%	80%	90%	94%	96%	97%
	3	67%	89%	95%	97%	98%	99%
	4	75%	92%	96%	98%	99%	99%
	5	80%	94%	97%	98%	99%	99%
n	6	83%	95%	98%	99%	99%	99%
	7	86%	96%	98%	99%	99%	100%
	8	88%	97%	98%	99%	99%	100%
	9	89%	97%	99%	99%	100%	100%
	10	90%	97%	99%	99%	100%	100%

3　方案比较

（1）变压器 2*N* 模式配电系统动力母线方案

优点：成对设置，负载端可以配置自动切换装置或手动切换装置。一台变压器的动力母线故障时，负载可以立即切换到对应变压器的对应母线上。当市电电源来自于两条不同的电力线路时，极易做到市电级备份、变压器级备份、母线级备份，系统冗余度较大。

缺点是：系统总的带载率≤1/2。变压器常态运行时，带载率较低，功耗大。系统投资大。

（2）变压器 *N*+1 模式配电系统动力母线方案

优点：专设备份用变压器、备份用输出母线。一旦变压器故障或母线故障时，可以手动方式切换到备份路由。如备份间设置优先级，也可自动切换到备份路由。当变压器数量较多时，系统带载率较高。相对于 2*N* 模式，投资有所减少。

缺点：专设的备份变压器、备份母线在常态下空载，不能发挥应有的带载能力。当变压器数量≤4 时，系统带载率 η≤75%。在 3 个以上的变压器系统中，即使在变压器负载较低的情况，当有 2 个以上的变压器或其母线障碍时，难以全部切换到备份路由。当市电电源来自于两条不同的电力线路时，难以全部做到市电级备份。

（3）变压器 *N* 模式配电系统动力母线方案

优点：变压器、母线间进行容量备份。对于 *n* 台变压器，当 *n* 为偶数时，在系统带载率≤1/2，且均分负载下，变压器及母线可以做到 2*N* 备份；当市电电源来自于两条不同的电力线路时，可以做到市电级备份。当 *n* 为奇数时，在系统带载率≤1/2，且均分负载下，变压器及母线可以做到 *N*+1 备份，部分变压器或母线可以做到市电级备份。对于 *n* 台变压器，当 1/2< 系统带载率 η≤（n-1）/*n* 时，均分负载下，可以做到变压器级备份、母线级备份，部分变压器或母线可以做到市电级备份。当系统带载率 η>（*n*-1）/*n* 时，可以做到母线级备份，不能做到变压器级备份，部分变压器或母线可以做到市电级备份。投资相对较少，系统灵活性较大。

缺点：系统复杂，维护人员熟悉起来较困难。

4　结束语

经过分析，可以给出以下一般性建议。

（1）投资充裕时，可以采用变压器 2*N* 模式配电系统动力母线方案。投资紧张时，可以采用变压器 *N* 模式配电系统动力母线方案。

（2）采用变压器 *N* 模式配电系统动力母线方案时，每台变压器输出母线越多，均分负载下，每台变压器允许的常态带载率越大。每台变压器输出母线 3 条及以上时，均分负载下，变压器允许常态带载率≥90%。

（3）采用变压器 *N* 模式配电系统动力母线方案时，变压器数量越多，均分负载下，每台变压器允许的常态带载率越大。变压器数量为 5 及以上时，均分负载下，即使每台变压器采用单母线，变压器允许常态带载率≥80%。

（4）采用变压器 *N* 模式配电系统动力母线方案时，对于 *n* 台变压器，当 *n* 为偶数时，在系统带载率≤1/2，且均分负载下，变压器及母线可以做到 2*N* 备份；当市电电源来自于两条不同的电力线路时，可以做到市

人民邮电出版社

电级备份。当 *n* 为奇数时，在系统带载率≤1/2，且均分负载下，变压器及母线可以做到 *N*+1 备份，部分变压器或母线可以做到市电级备份。对于 n 台变压器，当 1/2<系统带载率 η≤（*n*-1）/*n* 时，均分负载下，可以做到变压器级备份、母线级备份，部分变压器或母线可以做到市电级备份。当系统带载率 η>（n-1）/*n* 时，可以做到母线级备份，不能做到变压器级备份，部分变压器或母线可以做到市电级备份。

（5）在两台变压器下，通常情况下，变压器运行在 80%时效率最高，考虑到负载分配不会绝对平均，每台变压器的输出母线宜在 3 条以上。

（6）在 4 台变压器下，通常情况下，变压器运行在 80%时效率最高，考虑到负载分配不会绝对平均，每台变压器的输出母线宜在 2 条以上。

（7）在偶数台变压器下，为了减少系统的复杂性，可以两台变压器组成一对，变压器运行在 80%时效率最高，考虑到负载分配不会绝对平均，每台变压器的输出母线宜在 3 条以上。设计的输出母线越多，成对变压器带载率越大。当每对变压器带载率≤1/2 时，可以做到市电级备份、变压器级备份、母线级备份。当每对变压器带载率>1/2 时，只能做到母线级备份。

人民邮电出版社

通信系统集中监控平台建设方案

叶敏倩，詹望
（中国广核电力股份有限公司信息技术中心，广东 深圳 518124）

摘　要：为了确保通信系统安全运行，当通信机房设备出现告警时，运维人员可以第一时间响应，建设一个标准、开放、扩展性良好的机房监控系统很有必要。通过运用计算机网络技术对机房设备及动力环境运行状态的监测，使通信管理部门能够对系统运行参数、变化趋势及故障信息及时掌握并进行分析，采取防范措施并及时处理，确保通信系统安全运行。

关键词：机房监控系统；计算机技术；网络技术

1　引言

随着计算机网络技术的发展，对通信系统维运管理水平提出了较高的要求，实现对通信系统设备、电源、机房环境自动化监控是必然的趋势。电网通信系统承载着保护、自动化、调度电话及数据等网络业务，是电厂调度自动化、网络运营市场化和管理现代化的基础，是电厂安全、稳定、经济运行的重要保障。通信机房作为保障通信网络稳定运行的重要部分，对其进行科学管理是必要之举。通信系统的分布范围较广，设备告警发生时运维人员未能第一时间得知，导致故障处理的时间滞后。为改善这一现状，决定建设一套通信系统集中监控系统，实现对所有的通信系统设备进行实时监控，同时具备手机短信提醒功能，方便运维人员第一时间了解设备的运行状态，缩短故障处理响应时间。通信系统集中监控平台的应用，便于对所有系统设备告警的集中监控，方便运维管理，大大加快了响应的速度，缩短故障处理响应时间。

2　通信系统集中监控平台简介

集中监控平台在设计时参照了 TMN 信息体系结构、功能规范、管理服务模式、接口标准等，特别强调了监控管理系统的综合性、可靠性及适应能力。系统设计以面向对象的思想为主导，在通信设备（电源）、蓄电池、机房环境的管理方面采用了对象化的数据定义方法，在系统的图形界面的设计上也采用了对象化的图形方式。设计思想为系统的可持续发展、数据图形的一致性及接口的开放性打下了基础。

系统使用大型标准商用数据库，只要用来存储监控管理信息数据、网络资源数据、历史记录数据、统计报表数据等，不仅提高了数据的可靠性和共享性，而且降低了数据管理的成本。参照 OSI 的 CMIS 管理信息模型，设计了开放式服务核心 OMIS，提供统一的开放性信息服务接口 OMIP，支持客户、服务方式的数据交互模式；系统还提供一套 API 规范，保证了用户应用功能接口的开放性和接纳第三方应用程序的能力；提供强大的综合接入功能，可接入各种各样的智能设备，如电源系统、机房环境系统、安全保卫系统、火警消防系统等。

3　系统结构

通信系统集中监控平台组网实施方案如下。

（1）在通信机房配置一台数据服务器和一台前置服务器，安装实时数据库、管理信息库、商用数据库以及系统应用软件，构成系统中心服务器，主要负责系统的数据库、数据接口、消息传递、告警处理等的服务器，是集中监控管理系统的核心部分。

（2）在通信机房分别部署一台分站采集单元，实现以太网与串口的转换。配合各种变送器、设备干接点及协议转换，实现数据的接入。

（3）在办公室配置一台工作站。系统工作站用于监控系统本身的维护管理人员使用的应用工作站，配置全套的网管应用界面，同时重点配置了数据库管理界面和图形系统维护界面。通信管理工作站用于监控系统实现监控系统的矢量图形界面、网络管理界面以及各种数据查询、修改界面。采用大屏幕图形应用工

人民邮电出版社

作站、高速的图形功能，提供优越的图形、数据调用功能。

（4）在办公室配置短信发送模块，实现告警等信息的短信发送。

具体拓扑如图 1 所示。

硬件部分包括：网控中心硬件部分，如各种工作站、前置机、协议处理网关等；数据传送网络，如网络交换机、终端服务器、数据传输转发设备等；远方站数据采集系统，如数据传输转发设备。

软件部分包括：系统软件，如操作系统、基本数据库系统等；信息服务及实时数据处理，如管理信息服务、实时数据处理、协议转换、联网数据管理等；数据库，如数据库管理、数据库维护、应用数据；应用程序软件，如各种图形应用平台、各种数据查询站、各种管理工具及报表等工具软件。

每个实际系统的硬、软件各部分的配置，根据实际情况可以有所不同。ECM-INMS 变电站自动化机房监控系统的软件包括系统软件基础平台、应用功能平台、信息服务系统、数据库管理系统及协议处理软件五大部分。

4 配置的原则

（1）开放性与标准化原则

开放性与标准化原则是一个系统赖以生存发展的基础，只有开放的系统才能充分发挥计算机系统的能力，才能体现良好的可扩展性和互操作能力，保护用户投资及系统的长远发展。

（2）可扩展性原则

软件采用分布式设计、模块化构建，可灵活地配置到网络的不同物理地点和硬件设备上。

（3）先进性原则

先进性是一个系统赖以生存和发展的条件。方案推荐的服务器为新的具有服务分层结构的开放性产品，网络设备均支持当前的先进技术，保证用户的投资效益。在设计中，依据先进性与成熟性并重的原则考虑。

（4）可管理性和可维护原则

本系统所选产品具有良好的可管理性和可维护性。在选用硬件设备及系统软件时充分考虑到生产厂商的一致性和兼容性。

（5）可靠性和安全性原则

本系统所采用的主要产品采用可靠性设计，力求系统安全、可靠、稳定地运行。在硬件设备选型中，对硬件设备的关键部件进行严格的高可靠性的评估。

（6）最佳的性能价格比原则

网络、主机设备配置均遵循最佳的性能价格比原则，本配置方案充分考虑到目前被管理的网络情况，并预留足够的容量以支持较长时间内的网络发展状况。

体系结构设计需遵循以下原则。

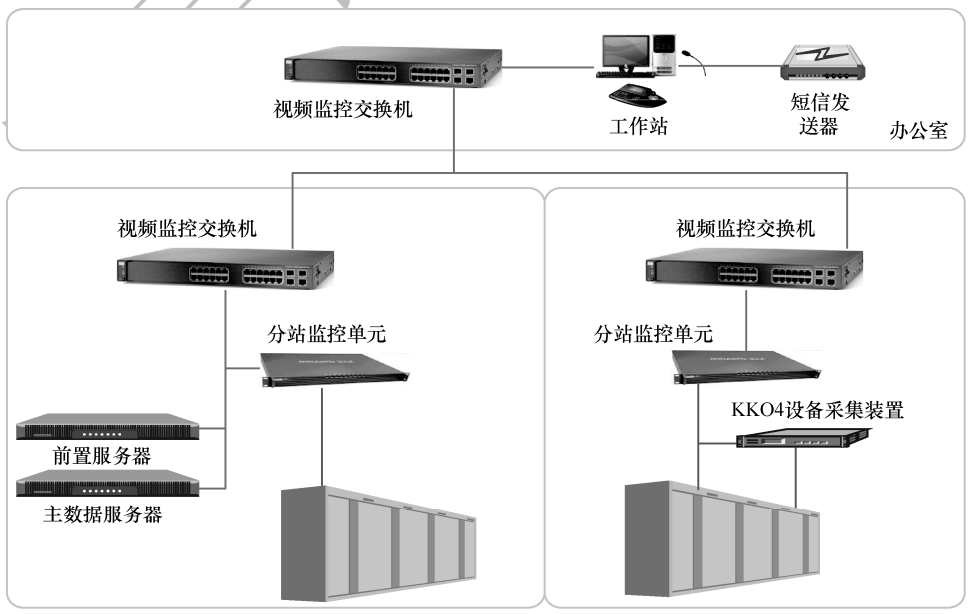


图 1　总体系统结构

- 采集系统完全脱离 PC 平台，采用嵌入式系统实现；具备采集、汇接、转发单台 all-in-one 解决方案，并保证硬件平台的可靠性和数据处理能力。
- 采集系统装置是模块化、分布式结构，便于维护扩容。
- 具备远程维护功能。可在局主站对其进行软件升级，配置参数修改。
- 具备与局主站自动恢复通信功能。
- 支持多种数据采集方式：直接采集、通过协议转换采集。
- 具有接收、处理、执行遥控命令功能。
- 具有优先发送故障告警，越限告警及状态变化信息，如通道受阻，可作缓存处理。
- 各种宽带、窄带、模拟、数据通道的适应能力。数据采集、通信复接、多方向转发、适应宽窄带混合通道网络，宽窄带通道主备自动切换。
- 提供本地功能及本地 LCD 人机交互数据查询界面，支持当地操作。
- 具有系统的自管理、监测功能和故障自诊断能力。

5 设备接入

5.1 通信设备接入

通过现有厂商通信设备网管的接入，资源管理系统实现从厂商传输设备配置的网管采集告警状态信息、配置及性能信息，实现系统功能中提出的拓扑管理、故障管理、配置信息管理、性能信息管理，实现对通信资源配置信息的动态管理，包括网络拓扑动态采集、网元交叉动态采集、电路路由动态采集。对于大量的网元交叉信息、网元端口信息、电路路由信息，可以自动采集存储在资源数据库中，极大地减轻了数据录入的负担。

接口使用条件：

- 厂商网管接口正常开放（包括权限、接口服务）；
- 接口开发系列文档（接口使用手册、接口说明手册）、IDL 文件；
- 北向接口服务器地址、接入用户名/密码。

接口安全配置：

- 厂商网管接口权限设置为只读；
- 通过监控系统为不同用户设置相应的用户权限；
- 增加防火墙限制端口和防病毒。

告警信息采集流程如图 4 所示。

5.2 协议转换接入

交换机设备配置有维护板卡，支持 4~8 个维护口。设备通常具有维护口、计费接口、远程 Modem 口等。综合网管系统将利用采集服务器与设备空闲维护口连接，实现数据的交互和采集。

- 利用现有维护口：将交换机单独的一个维护口接到采集服务器的串口上，协议程序在达到协议转换功能的同时，也可以对交换机进行维护操作，起到维护终端的作用。另外还能作为终端服务器的功能，在多台计算机上，利用标准的超级终端功能，通过本协议程序来维护交换机。
- 开通空闲维护口：通过开通交换机的一个数字电路口，再接一个 DCA，然后接到采集服务器的串口上，完成数据的采集。

接口安全配置如下：

- 分站单元的 RS232 串口具有隔离作用，保护

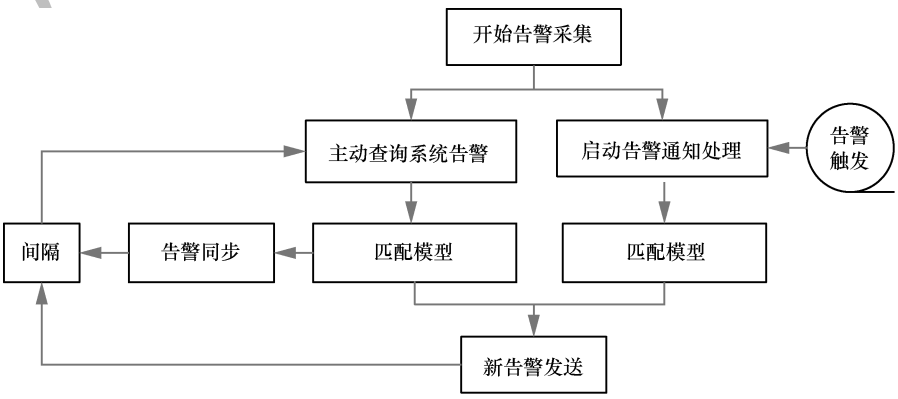


图 4　告警采集信息流程

DCA 设备串口的安全稳定；

- 采用 CDT 规约程序在采集的过程中只接收数据，不主动发送数据，不会对被测设备造成影响；
- 通过监控系统为不同用户设置相应的用户权限。

5.3 通信电源设备接入

接口方式：通过电源设备数据串口连接到前置采集服务器的串口上完成数据的采集。串口协议程序模仿管理程序，按原电源协议顺序地发出取信息命令，从电源设备模块中读出所有的信息，达到监控的目的。

接口安全配置：分站单元的 RS232 串口具有隔离作用，保护电源模块串口的安全稳定；通过监控系统为不同用户设置相应的用户权限。

6 监控管理网络特点

监控管理网络的特点具体如下。

- 设备接入点可以与管理域分离，实现不受地域、行政级别限制的自动化机房监控系统管理域；组成既能分层、分地域管理，又能相互交叉管理的管理网络。
- 系统可以收集各种被管通信设备（电源）的运行状态数据，包括状态量、模拟量及运行参数等，并可以进行显示、分析、统计。
- 系统可以收集通信设备（电源）的性能信息，并通过性能信息来评估通信设备（电源）的运行状态等。
- 系统具有良好的可扩展性，系统的规模及所监控设备的数量都可方便地扩充，系统的网络结构便于系统的硬件平台、软件平台分步骤、分阶段升级。
- 系统能够在统一的应用程序框架内完成所有的功能。对其他应用程序的调用由系统自动执行，并完成相关数据交换。
- 监控管理系统本身具有良好的可管理能力和有效的自诊断功能，它能够监视、查询、诊断各级主机、网络设备、采集设备及数据通道的工作状态，并可对设备参数进行远程设置。
- 监控管理系统支持 Web 浏览器作为系统客户。
- 应用程序具有统一的应用界面框架，框架中可以兼容多种应用程序，并可集成其他通用的应用程序。这些应用程序由系统自动调用执行，并自动完成相关的数据交换。
- 每个应用程序平台作为独立的进程，可独立运行在不同的工作站或主机上，其性能取决于其运行的工作站平台。
- 监控管理系统提供的性能参数分析工具应用软件能够对记录的历史参数进行分析，并能以曲线等方式显示出分析的结果。分析功能包括最大值、最小值、平均值、越限情况等。
- 监控管理系统在其矢量图形系统中提供对网络性能参数的各种显示方式，如曲线、棒图、饼图、仪表等，并可采用对象图形及参数同窗显示的方式。

7 结束语

随着电厂业务的发展，通信机房的数量的增多且分布范围不集中，集中监控平台项目的应用，大大提高了运维人员的工作效率，减轻了人力成本的输出，利用监控系统对机房的动力环境进行实施监控，故障出现即可快速得到响应。对于通信系统的稳定运行具有重要的意义，集中监控平台设计理念与电站安全管理体制保持一致，在投运后给运维人员带来极大的便利。

参考文献：

[1] 杨磊. 网络视频监控技术[M]. 北京: 中国传媒大学出版社, 2017.
[2] 本社. 发电厂电力网络计算机监控系统设计技术规程[M]. 北京:中国计划出版社, 2014.
[3] PROAKISJG. 现代通信系统[M]. 北京: 电子工业出版社, 2017.
[4] 陈显治. 现代通信技术[M]. 北京: 电子工业出版社, 2000.
[5] 陈鹏. 发电厂信息通信机房安防监控系统的实现[J]. 宁夏电力, 2013(2).

人民邮电出版社

新能源城配物流充电站运营服务平台建设与服务

李迪，高立忠，刘冲，马娜
（北京国电通网络技术有限公司，北京 100070）

摘　要：新能源物流车与新能源充电站所承载城市配送的业务具有广阔的市场前景。针对这一市场前景研究分析充电站运营现状，提出了基于泛在物联网的新能源城配物流充电站建设理念，设计了新能源城配物流充电站运营服务平台功能，提出了面向用户的服务方式，形成城市绿色运力网络，打造智能城配生态圈。

关键词：新能源；物流；新能源充电站；储能系统

1　引言

电子商务快速发展，物流配送行业具有广阔市场前景。城市配送作为物流链条中最后的配送环节，担任非常重要的作用。由于燃油车排放的尾气给城市带来了环境污染，造成大部分城市对货车运营时间和运营区域有严格限制。纯电动物流车已经成为城市配送业务升级转型的迫切需求。与传统汽车物流业务相比，电动物流车每百千米成本约 48 元，同类型的燃油车每百千米油耗约 73.2 元，假如一台车每天跑 200 km，每天油电差价约50.4元，一台车一个月至少节约1512元，每年可节省约 1.8 万元。成本的优势导致新能源城配物流业务快速发展，“新能源物流车+新能源充电站”所承载城市配送的业务具有广阔的市场前景。稳定的物流订单使新能源充电站内的充电桩长时间保持的工作状态，可以不断收取车辆的充电服务费，保证充电站运营收益。

2　充电站运营现状

电动汽车的大规模部署将给电网带来压力。充电站大量建设充电桩会对电网的用电负荷造成影响，对现有配电网供给能力提出挑战，部分地区面临扩网配容的问题。大规模电动汽车同时充电也会对电能质量造成影响，对电网造成冲击，考验电网运行可靠性。充电站不能只依靠公共电网，一定要具备储能功能，储存低谷电在储能系统中，在用电高峰期间可以给大量电动车充电，这样才不会对公共用电造成影响。储能系统的建设能够降低充电站一定运营成本。储能系统所创造的价值是由当地的电费构成、充电设备利用率和客户对价格的敏感度决定的。

当前储能充电站建设和运营还处于起步阶段，储能充电站多用于商业园、工业园、商用住宅等。已建设完成的充电设施利用率低、价格机制不健全导致运营商盈利困难。服务费、电力差价和增值服务是盈利的主要来源，商业模式有待创新。

3　新能源城配物流充电站

新能源城配物流充电站选址主要在集散地、主要干线、支线等符合建设要求的场地。搭载了新能源城配物流充电站运营服务平台的充电站能够柔性消纳新能源，具备稳定配电网的特性。新能源城配物流充电站能够离网运行、灵活调度电能、无谐波污染、低碳环保。并且新能源城配物流充电站能够参与优化电力调度或需求侧管理，解决电网峰谷运行矛盾，提升电网消纳新能源的能力，使所在区域公共电网运行稳定，提高能源利用效率。新能源城配物流充电站运营信息流与能源流如图 1 所示。

3.1　电动物流车作为移动式储能单元

电动物流车配有动力电池系统，可以作为分布式储能单元参与系统调节控制，是常规分布式储能的有利补充，降低了电动物流车储能系统建设投资成本。

3.2　退役车载动力电池作为构建储能设施

退役电池容量因为衰减，无法满足电动物流车的运力需求。但可以利用退役车载动力电池作为充电站储能系统的补充，提升电池的利用效率，节省项目投资。

人民邮电出版社

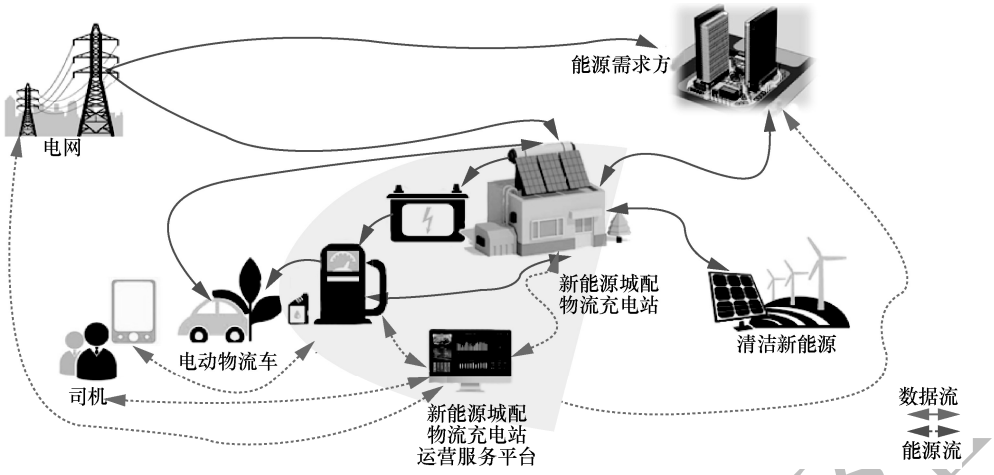


图 1　新能源城配物流充电站运营信息流与能源流

4　新能源城配物流充电站运营服务平台定位及特点

4.1　平台定位

通过建设新能源城配物流充电站运营服务平台，构建城市绿色运力网络，打造智能城配生态圈，建设“车、桩、网、运”生态系统，创新新能源物流运营模式，承载新能源汽车充电服务模式，实现绿色物流充电网络生态系统，提高充电效率，推动新能源物流产业发展。

4.2　平台特点

（1）新能源城配物流充电站运营服务平台的应用能够提高充电站的经济性、柔性消纳新能源，实现新能源综合利用和需求响应。提升配网的稳定性，减少客户变压器压力。实现差别化的优惠费率。

（2）对于电网来说，新能源城配物流充电站运营服务系统能够改善电网运行效率，减小配网过载，提高供电可靠性，避免用能高峰期。促进需求响应、智能电网建设相协调，实现有序供电、谐波治理。

（3）对于充电站运营商来说，新能源城配物流充电站运营服务系统能够实现物流车辆及基础设施管理，利用分时电价赚取收益，实现能源梯次利用，能够为电网提供需求响应、用能数据等辅助服务，增加运营收益。

（4）对于物流运营商来说，新能源城配物流充电站运营服务平台能够合理的安排物流车辆去就近有空位的充电站进行充电。通过物流充电服务生态系统，将司机的价值、物流车的运力发挥到最大值，通过释放油电差价，降低了城配物流运营成本，解决了充电困难的问题，也疏解了城市交通压力。

5　新能源城配物流充电站运营服务平台主要功能

充分利用物联网和云计算技术，实现新能源城配物流充电站运营服务平台的智能化、数字化和便捷化。以能耗管理平台、充电设备和储能系统、物流运营管理、可视化监控系统为核心体系，提供新能源物流电动汽车充电及管理服务，实现储充的联合应用。

5.1　多维物联

基于泛在电力物联网实现新能源物流车运营的智能化运营管理。通过 RFID、传感器、智能识别等技术，采用多种通信的方式，将电动物流车、动力电池、充电设施、充电场所、电网等主体以多重维度进行连接。

5.2　能耗管理

为充电站储能、充电服务提供支撑，保证智能充电桩和电动物流车的能耗管控及调度，实现充电站用电信息统计、监测、分析、电能调配及危险报警。完成电网谷时充电、电网峰时放电，实现需求侧供给，从而达到“削峰填谷”的目的，实现基于能源管控系统的充电、储能服务。

5.3　运力调度

针对新能源车辆运行线路、运行时间、配载量等动态信息，智能安排最佳调度方案。可支撑多种物流业务配送场景，如多地点提货送货、循环配送等。降低了调度工作量，节约时间成本。

5.4　可视监控

基于多维物联采集各系统关键指标和信息。便捷、

高效地实现整个运营管理系统全景监控和可视化管理，具有警报、调度等业务能力，实时监控充电桩运行状态、参数指标、优化调度等相关业务信息。

5.5 数据基础服务

以新能源城配物流充电站运营服务平台为支撑，在充电桩监管、储能用能管理和运营业务开展的基础上，将基础信息、能耗数据、运营等数据整合成应用服务，通过数据服务的方式为电力公司、政府、运营管理、司机提供基础及信息资源综合服务。

5.6 安防报警

确保充电站用电的安全性。充电站需装视频监控、火灾探测器等安防设备。一旦发生异常，监控与报警系统实时联动，视频监控可以根据事故发生位置进行判断，开启监控及录像，平台立即将异常通知相关人员或进行报警处理。

5.7 车辆检测

可实时检测车辆故障，快速获取电动汽车故障解决方案，发布至司机用户。通过建立车辆诊断数据库实现车辆历史故障数据的存储和维护，并保存对应故障诊断推理的中间过程和结果。

5.8 节能驾驶服务

节能驾驶服务可从驾驶员驾驶方式、路况等多角度对行车用电量进行综合分析，根据车辆当前行驶速度、加速度、道路等级、坡度、交通状态等实时数据给出降低行车用电量最佳行驶方案，并通过多种方式发布。节能驾驶子系统定期在线检测电池、电机运行状态、胎压等车辆状态，形成动态保养提示。

5.9 软件及微服务

通过软件及微服务实现物流单查询、工作量查询，可以实时查看物流车运行状态、线路拥堵情况，合理规划充电路径，解决电池续航问题。

6 结束语

提出的新能源城配物流充电站运营服务以电动物流车为主要载体，以新能源为能量媒介，以互联网为基础，联合销售代理商、快递公司、物流公司等合作运营商，通过终端设备或微应用，实现平台业务监控管理。通过整合各参与方资源，实现优势互补，打造利益共享商业模式。整个新能源城配物流充电站运营服务平台，不是单独由一个模块运作而成的业务，是结合多类业务模块、跨行业发挥联动效应协调运作的，提供综合的能源运营及交易服务。

参考文献：

[1] 黄海宾.电动汽车充电设施与电池储能电站结合的应用模式[J].节能与环保, 2017 (12):70-73.

[2] 舒晗, 何永秀. 纯电动汽车替代方案及经济性分析[J]. 电力科学与工程, 2017, 33(4): 26-31.

[3] 陈昆灿, 刘峻, 江熠. 储能电站商业模式初步研究[J]. 能源与环境, 2017 (5) : 34-36.

[4] 北极星储能网. 光储充一体化充电站的未来发展与实际案例[EB]. 2018.

[5] 孙佳伟, 孙晓琼, 刘彤. 电动汽车发展对电网企业的综合影响研究[J]. 管理学家, 2013 (9): 84-84.

[6] 裴标. 分布式电动汽车充电站及其管理系统[D]. 北京:北京交通大学, 2013.

人民邮电出版社

新一代国家级电力交易平台微服务架构设计

詹卫许[1]，张志翔[2]，杜龙[2]，胡学强[1]
（1 南方电网数字电网研究院有限公司，广东 广州 510623；2 广州电力交易中心，广东 广州 510623）

摘　要：随着我国电力体制改革加速推进，电力交易市场蓬勃发展，市场主体、交易品种等市场要素体量增长迅速，交易频率日趋实时化，交易清算与结算复杂度增加，现有系统对业务的支撑越来越困难。提出了构造新一代国家级、基于微服务架构的电力交易平台整体设计思路，有效地提升了用户需求响应速度、解决了系统的大并发访问和海量数据计算问题，并进一步提升了系统的可靠性。

关键词：云计算；微服务；整体设计；基础服务；电力交易

1　引言

自从《中共中央国务院关于进一步深化电力体制改革的若干意见》（中发〔2015〕9 号）及有关电力改革配套文件发布以来,南方电网进一步加快推进电力市场化改革，成立了国家级广州电力交易中心和广东等 5 个省级交易中心。初步统计，2018 年，南方区域经营性行业总数 519 万户，已参与市场用户约 3 万户。2018 年，南方区域经营性行业总电量 6 014 亿 kW·h，市场化电量 3 377 亿 kW·h，占总用电量 56 %。

2015 年起，南方区域各级交易中心相继建成了网省两级电力交易技术支持系统，支撑了双边协商、集中竞价、合同电量转让等 20 多个交易品种的开展。但随着市场发展，系统在用户数据申报、交易品种扩展、清算与结算功能的灵活配置、及时计算等方面的矛盾日渐突出，难以满足新形势下的要求。2017 年 10 月，南方电网发布了《南方区域电力现货市场建设工作方案》，要求以广东为起步，在 2020 年后具备开展南方区域统一集中式电力现货市场交易条件。

综上所述，国家级电力市场迫切需要有新的国家区域统一平台来进行支撑，需要站在新的改革发展的高度上，统筹规划，确保系统的灵活性、扩展性、高性能和稳定性。

目前在电力交易系统建设架构方面的研究主要有以下几个方面。

参考文献[1-6]提出了通过云计算架构和微服务进行系统构建的通用原理、架构设计和相应的案例说明。

参考文献[7]提出了南方区域电力现货市场建设模式、思路及实现路径。

参考文献[8]提出了利用微服务架构来进行省级交易系统改造的架构和技术方案。

2　传统单体架构系统的瓶颈分析

老一代企业级系统主要采用基于 J2EE、.NET 等的单体多层架构，其设计核心是业务客户端只负责输入输出的 UI 界面,中间应用层负责业务逻辑运算，后端数据层主要负责数据点存储和管理。对一些大型的交易型系统，应用层衍生出多采用分布式服务技术，例如 EJB、COM 和 CORBA，其中以 EJB 最为成功，如图 1 所示。

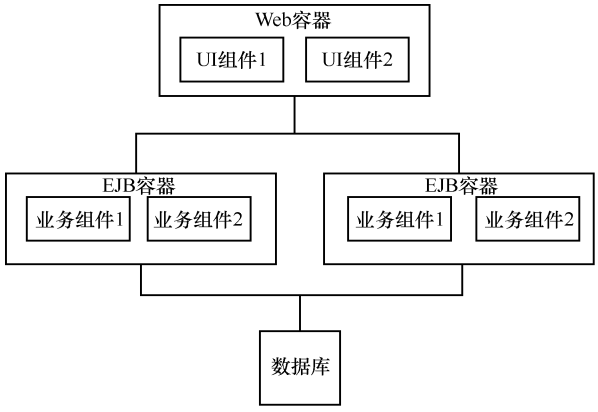


图 1　基于 EJB 的 J2EE 架构

但上述的传统单体建构比较适合于中小级管理信息系统的建设，南方电网老的电力交易系统也均采用此架构，目前存在如下问题。

（1）业务迭代速度慢，由于系统架构对业务没有进行充分解耦，对单一功能模块的修改均会影响整个

人民邮电出版社

系统的功能应用，导致一次局部升级将影响整个系统的被动升级，这将严重影响到电力交易市场快速多变的业务特性。

（2）高并发用户的访问和交易数据的申报响应速度慢，主要是由于大部分系统没有采用基于微应用架构的互联网访问架构，计算能力均严重依赖数据库的运算能力，导致数据访问和写入的瓶颈。

（3）市场交易、交易结算计算性能低下，不能满足日清月结的业务需要，主要是由于架构方面没有引入云计算容器技术（Doker 容器）的弹性扩展计算能力，在业务没有解耦的情况下不能提供精准性的资源调配。

3 新一代国家级电力交易平台技术架构设计

传统的单体架构已经不能很好地支撑新一代国家级电力交易平台的技术要求，经过反复论证、测试，采用微服务架构能够很好地解决目前遇到的技术性问题，是国内电力行业首个整体采用微服务设计的大型国家级电力交易平台。

3.1 基于微服务的架构设计

提出的整体技术架构核心是云计算、微服务架构，将平台构建于南方电网企业管理云平台和大数据平台之上，分为 IaaS 基础设施层、PaaS 技术组件层、PaaS 业务组件层、SaaS 应用层和渠道层共 5 层，包括云计算、微服务的开发、运维支撑（DevOps）和基于等保三级安全保护体系，具体架构如图 2 所示。

（1）基础设施（IaaS 层）

由云平台提供存储、网络等虚拟化环境支撑，实现资源的弹性收缩，满足系统对计算能力的硬件要求。

（2）平台（PaaS 基础组件层）

在基础设施上，通过平台服务，统一维护、统一管理，简化业务系统的基础运维服务，提升系统运维效率、质量，这些服务包括数据库软件、分布式缓存、多租户环境、微服务网关等以及相关人工智能组件服务，如机器学习、人脸识别等公共服务。为了保障平台业务系统的通用服务能力，云平台通过部署公共业务服务组件或服务，便于统一能力组件和通用服务。

（3）服务（PaaS 业务组件层）

统一平台功能主要分为业务应用服务和数据应用服务。业务应用服务采用多中心建设模式，通过 10 个微服务中心部署相关应用微服务；数据应用服务则是对业务应用服务生产的业务数据，进行多维度分析，构建多主题的多维度数据在此基础上开发数据应用功能，如用户属性服务、客户画像等分析型应用服务，统一为应用层提供功能服务。

（4）应用（SaaS 应用层）

部分平台的功能通过部署在 PaaS 环境上，应用层

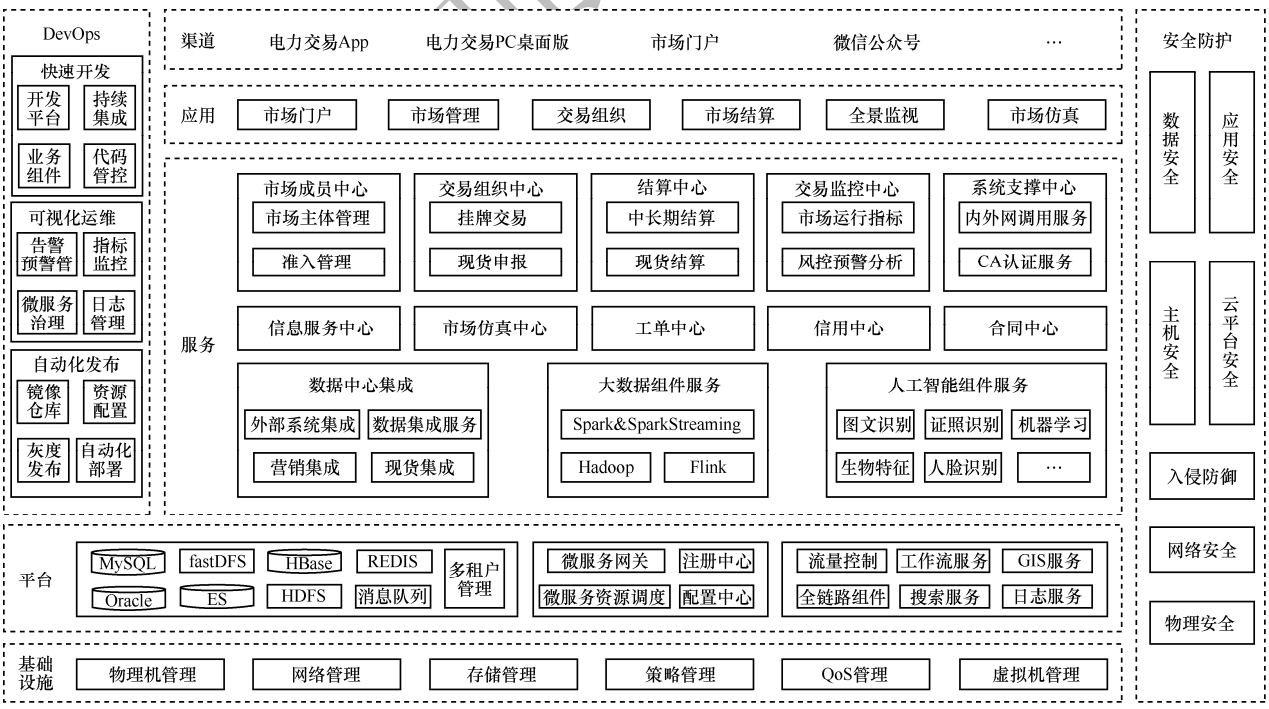


图 2 基于微服务的新一代国家级电力交易平台架构

组合相关服务，实现复杂的业务功能。基于服务的功能组装在该层完成，该层主要负责组装用户界面和交互操作，业务操作通过服务实现。

（5）渠道层

针对不同的渠道，通过组合各种服务，可快速、高效组合多渠道用户界面，通过服务访问，构建统一操作功能，一致化全网用户服务体验。

3.2 新一代微服务架构能力分析

微服务作为一种新兴的架构模式，通过按照业务领域设计方法（DDD 领域驱动）有效对业务系统进行解耦[9]，划分出服务边界和粒度，形成相对独立的松耦合、高内聚的微服务业务中心，能够全面提升软件管控水平和开发效率，本文提供的按照微服务的架构设计的电力交易平台，将很好地克服目前和将来一段时间中出现的问题。

（1）加快业务迭代速度，提升用户体验，通过对业务进行解耦，提炼出市场成员中心、交易组织中心、结算中心、工单中心等十大独立的中心，并进行开发和部署，对需求的升级迭代将更加精准，相互的影响较小，提升开发和部署的效率。

（2）系统的性能将大幅提升，十大中心将按照业务和计算特点，采用不同的技术进行构造，互不影响，将每个中心按照微服务的技术组织方式，根据用户的特征进行有针对性的优化和重构。

（3）系统稳定性将通过云平台保障，微服务中心通过 Docker 容器技术进行封装镜像，再通过云平台对 Doker 容器进行资源的弹性分配，实现对业务性能的快速、自动响应，提升系统的性能和稳定性。

（4）系统的稳定性将大幅提升，前端采用“互联网+”的技术访问架构，针对性地采用动静态分离、前后端分离的 VUE 技术，按照微应用的方式进行构造，能有效解决互联网应用的峰值访问问题，高效地应对多用户高并发的场景[7]，提升系统的稳定性。

4 关键技术场景设计

4.1 应用层（SaaS 层）高并发用户访问设计

为应对外网区用户高并发访问，本文提出采用两种方式的高并发负载均衡技术实现，如图 3 所示。一种是面向静态资源集群的反向代理水平扩展机制，另一种是面向微应用/微服务的网关集群水平扩展机制。

（1）静态资源集群

采用 NGINX 高可用双活模式应对用户高并发访问，静态资源通过站点服务路径直接实现负载均衡，当遇到高并发需求时，可通过水平扩展静态资源节点数量线性扩展。

（2）微服务大并发负载均衡

一方面通过部署微服务网关集群，在负载均衡（硬件）上获取横向网关高并发访问能力，另一方面通过配置微服务 K8S 资源调度策略，当某微服务出现资源紧张时，动态生成新的 Docker 实例扩展微服务的并发访问能力。

4.2 组件服务层（PaaS 层）实时连续撮合竞价设计

连续竞价在业务过程上表现出实时性的特点，即无论卖方或买方进行交易申报后需要及时对不同方向的买方队列或卖方队列按照价格优先进行撮合计算，具备成交条件的达成交易，未成交的加入对应队列。在连续竞价交易开市后，无论卖方或买方申报交易，都将按照时间优先的原则进行及时的撮合计算，参与市场交易的成员越多，对于系统形成的压力越大，需要应用新的内存技术进行新的架构设计，连续撮合竞价架构如图 4 所示。

以上解决方案中的关键技术点如下。

（1）定序处理

定序服务的主要作用是在用户请求到达系统服务器后，第一时间进行定序，以确保用户请求的先后顺序，在连续竞价业务场景下，时间是规则中考虑的重

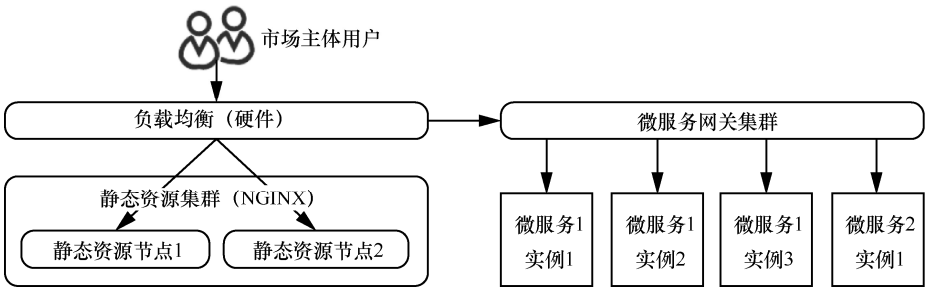


图 3 大并发负载均衡架构

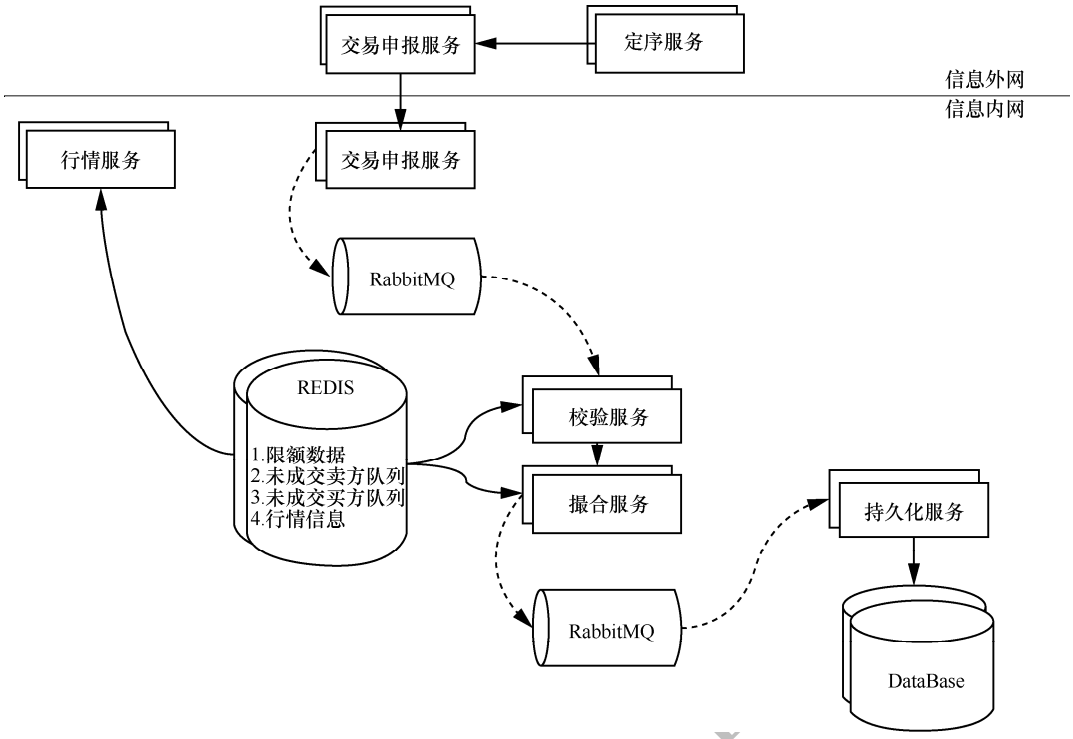


图 4　连续撮合竞价架构

要因素之一，在实现上要求时钟服务器确保时间处理的一致性。

（2）消息服务

连续竞价业务是以时间紧密相关的交易方式，强调的是在价格优先的前提下，先到先得。针对高并发的情况，采用消息队列进行申报响应，以确保响应效率。同时，也要求对用户请求必须顺序处理，且不能丢失。

内网“交易申报服务”在接收到用户请求后，首先进行顺序号校验，发现非顺序后需要向外网“交易申报服务”请求获取对应顺序的请求。“交易申报服务”作为消息服务的生产者，“校验服务”作为消息服务的消费者。为确保消息的可靠生产和消费，使用 RabbitMQ 提供的生产者消息确认机制和消费者消息确认机制。

5　结束语

首先介绍了南方区域统一电力市场交易平台建设背景，分析了目前系统存在的问题和挑战，挖掘出系统架构中存在的问题，从而提出了按照微服务架构来进行国家级的南方区域统一电力交易平台建设的架构，并对架构的能力进行了分析，最后对架构下的几个核心技术要点进行了方案设计，确保能够解决近期发展中遇到的快速迭代、高并发访问、大数据内存计算等问题。

参考文献：

[1] CHRIS R.微服务架构设计模式[M]. 北京: 机械工业出版, 2019.
[2] 郑天民.微服务设计原理与架构[M]. 北京: 人民邮电出版社, 2018.
[3] 李林锋. 分布式服务框架原理与实践[M]. 北京: 电子工业出版社, 2016.
[4] SAM N.微服务设计[M]. 北京: 人民邮电出版社, 2016.
[5] 肖仲垚. 微服务通信框架的设计与实现[D].北京: 北京交通大学, 2017.
[6] 韩佼男. 浅析微服务架构在企业信息系统构建中的应用价值[J]. 中国管理信息化, 2018. 21(2): 53-56；
[7] 梁志飞, 陈玮, 张志翔, 等. 南方区域电力现货市场建设模式及路径探讨[J]. 电力系统自动化, 2017, 41(24): 16-21.
[8] 承林, 王海宁, 高春成. 微服务在电力交易系统中的应用研究.电网技术, 2018, 42(2): 440-446.
[9] ERIC E.领域驱动设计：软件核心复杂性应对之道[M]. 北京: 人民邮电出版社, 2018.

信息化技术在绿色供应商评价管理中的应用

潘晓婷[1,2]，王俊生[1,2]
（1. 国网电子商务有限公司（国网雄安金融科技集团有限公司），北京 100053;
2. 国家电网有限公司电力金融与电子商务实验室，北京 100053）

摘　要：研究了在当前物联网、区块链、大数据等新兴技术高速发展的背景中，如何将新技术融入传统绿色供应商评价管理方法。通过分析现有关于供应商评价的参考文献，建立了适合电力企业的绿色供应商评价指标体系，并在指标体系中加入信息化因素。然后采用“定性+定量”的研究方法，构建了绿色供应商评价模型。通过评价模型，实现企业对绿色供应商的精细化管理要求，促进供应商的精准选择和持续迭代。

关键词：信息化技术；绿色供应商评价；层次分析法；主成分分析法；模糊评价法

1　引言

近年来，随着生态环境问题日益严峻，党中央、国务院高度重视绿色发展问题。2018 年 4 月，生态环境部联合商务部等 7 部门共同印发《关于开展供应链创新与应用试点的通知》，特别强调要发展全过程全环节的绿色供应链体系，将绿色供应链纳入供给侧改革等重要战略部署中。国家电网公司积极响应政府号召，在物资领域的多个阶段应用绿色发展理念，同时把信息化建设作为绿色发展的重要抓手，从 2010 年开始，逐步建成了电子商务平台（e-business platform, EBP）和企业资源管理（enterprise resource planning, ERP）系统。未来，国家电网公司电子商务平台将围绕“互联、物联、智能”的供应链发展趋势展开建设。

2019 年国家电网公司提出“三型两网”战略，大力建设泛在电力物联网成为未来几年发展的重要事项。本文选择绿色供应链发展过程中的关键环节——绿色供应商选择问题（又被称为“绿色供应商评价问题”）为研究对象，在当今物联网、区块链、大数据等新兴技术快速发展的背景下，研究如何将新技术应用于研究绿色供应商评价管理。本文通过分析现有关于供应商评价的文献，建立适合电力企业的绿色供应商评价指标体系，并在指标体系中加入信息化因素，以实现对绿色供应商更加科学合理的评价。

2　国内外研究现状

1994 年，学者 Webb 首次提出绿色采购概念；1996 年，美国密歇根州立大学制造研究协会最早提出了绿色供应链的概念。随后，国内外越来越多的学者开始对绿色供应链、绿色供应链管理、绿色采购等议题展开研究。绿色供应商评价作为绿色供应链的重要一环，受到部分学者的关注。

1997 年，Noci 从企业的环境发展战略入手，认为该战略会直接影响供应商评价标准。Noci 将企业环境战略分为积极和消极两类，并提出基于积极环境发展战略的 4 个一级指标和 12 个二级指标，对供应商进行评价。1998 年，Walton 选择了美国 5 家家具制造企业，确定了 10 个供应商评价标准，通过实证分析，研究了基于绿色供应链管理需求的供应商评价标准及影响因素等问题。2002 年，Handfield 运用德尔菲法分别提炼出了绿色采购中 10 个最重要、最易识别的供应商评价因素。

2001 年，王能民等人基于绿色制造与传统制造的差异，提出绿色制造模式下的供应商选择标准，建立了评价模型。2004 年，朱庆华等人通过比较法研究了中美两国对于绿色供应商选择标准的差异。2005 年，张平等人综合考虑了经济、环境等因素，构建了绿色供应链合作伙伴评价指标体系。2007 年，刘志峰等人运用模糊评价法和层次分析法，构建绿色供应商评价指标体系。2010 年，史东成等人运用交叉评价模型和 BP 神经网络，建立了供应商选择模型。2015 年，邹欣等人在传统供应商评价体系基础上，将环境管理体系等多项环境指标纳入评价范围，完善了绿色供应商评价指标体系。2018 年，李海波等人运用层次分析法，

人民邮电出版社

对供应商进行排序，根据排序结果进行选择。

通过上述参考文献的分析，笔者发现，绿色供应链兴起较晚，国内外各界学者对绿色供应商评价体系尚不完善；在现有评价体系中，评价指标的设置大都基于传统因素，现代信息化、技术化因素考虑很少。因此本文将信息化技术特点与绿色供应商评价需求相结合，探索信息化技术背景下绿色供应商评价管理体系，以促进国网公司的绿色供应链业务更好更快地推进。

3 绿色供应商评价方法选取

供应商评价方法众多，主要分为定性分析法、定量分析法、定性定量相结合分析法等。但是单独定性分析法主观因素影响较大，单独定量分析评价又会使许多无法量化的因素无法衡量，因此一般多采用“定性+定量”相结合的方法进行分析。常见的分析方法有类似数据包络法、主成分分析法、层次分析法、模糊评价法等，下面将对各分析方法进行比较，发现不同方法的优劣势，最终选择适合于本文的分析方法组合，尽量做到评价科学合理。

3.1 类似数据包络分析（DEA）

数据包络分析（data envelopment analysis，DEA）方法由美国著名运筹学家 Charnes A 和 Cooper W W 在 1978 年提出，是以相对效率为基础的一种效率评价方法。具体而言，DEA 是一个非参数估计的线性规划模型，表示为产出/投入的比率。在研究多输入、多输出生产函数时，由于不需要估计参数，因此可以避免主观因素干扰，简化算法流程，减少误差。

3.2 主成分分析（PCA）

主成分分析（principal component analysis，PCA）通过不断降维，将多个变量逐渐转化为几个综合变量（即主成分），这些综合变量之间互不相关，且都是原始变量的线性组合。采用这种方法可以克服单一指标不能真实反应实际情况的缺点，引进多方面的指标，但又将复杂因素归结为几个主成分，使复杂问题得以简化，同时得到更为科学、准确的信息。

3.3 层次分析法（AHP）

层次分析法（analytic hierarchy process，AHP），是指将多目标问题看作一个系统，然后将目标分解为准则层、方案层等若干个层次，通过“定性+定量”的方法，计算出层次单排序和总排序，然后根据排序，在多种方案中选择最优方案。该方法结合了定性与定量分析两种思想，但所需定量数据少，更加简洁实用，将研究对象作为一个系统，可以清晰明确的表示各因素对结果的影响。

3.4 模糊评价法

模糊评价法建立在模糊数学的相关理论基础之上，该方法可以将模糊评价对象定量化，评价结果是一个矢量，包含丰富的信息，可以更加准确地评价被评价对象。以这个算法为基础，根据对供应商的了解和客观因素，按照模糊关系矩阵理论对供应商给出相应分数。

综上分析，本文采用“定性+定量”分析方法，综合利用 AHP、PCA、模糊评价 3 种方法，对绿色供应商进行评价。

4 绿色供应商评价体系及模型构建

4.1 指标体系

本文在对国内外现有绿色供应商评价指标体系进行归纳总结的基础上，遵循全面性、科学性、系统性、层次性、定量与定性相结合、可行性等原则，确定绿色供应商评价的一级、二级、三级指标，然后对三级指标识别能力强弱进行判断筛选，并对筛选后的三级指标进行量化，最后构建出绿色供应商评估指标体系，具体见表 1。

4.2 绿色供应商评价模型

综合利用 AHP、PCA、模糊评价 3 种方法，对绿色供应商进行评价。首先，利用 AHP 获得评价准则和决策者对准则的偏好；其次，利用 PCA 方法分别对评价样本的投入准则得分和产出准则得分进行正交投影，从而获得相互独立评价主成分得分，对准则的主观权值进行投影，获得关于主成分的偏好约束；最后采用模糊评价法，通过模糊变换原理和最大隶属度原理，对评价系统内的相关因素进行综合评价。综合评价步骤如下。

步骤 1 根据 AHP 法画出层次图，确定评估准则；构造判断矩阵，并对其进行一致性检验，得出各因素的偏好权重；根据最底层准则对供应商进行评价，取得供应商的评价样本。

（1）画出 3 个层次结构——目标层、准则层、方案层。

（2）从第二层开始，构建成对对比矩阵。

（3）计算单排序权向量，并进行一致性检验。

一致性指标可表示为：

人民邮电出版社

表 1　绿色供应商评价指标

一级指标	二级指标	三级指标
环境效益指标	绿色生产	绿色研发费
		原材料清洁度
		生产过程中能耗率
		污染预防、治理费
	绿色包装	包装材料环保度
		包装材料回收利用率
	绿色仓储	仓库利用率
		货物流通率
		货物损坏率
	绿色回收	材料循环利用率
		设备循环利用率
	绿色文化	绿色文化普及度
		绿色法规遵从度
企业信息化指标	信息化支撑系统	信息系统建设年投资额
		数据库建设规模
		信息安全技术建设水平
		物联网建设水平
	信息化应用	办公自动化水平
		核心业务流程信息化水平
		电子商务应用水平
		财务管理信息化水平
	信息化人才	信息化人才比率
		信息化人才培训频率
		管理层信息化素质
		信息化人才流动率

$$\mathrm{CI}=\frac{\lambda-n}{n-1} \tag{1}$$

其中，λ 为判断矩阵特征根，n 为 n 阶一致阵的唯一非零特征根。

当 $\mathrm{CI}=0$ 时，有完全一致性；CI 接近于 0，有满意的一致性；CI 越大，不一致越严重。

为衡量 CI 的大小，引入随机一致性指标 RI，通过随机构建 500 个成对比较矩阵 $A_1,A_2,\cdots,A_{500}$，得到 500 个一致性指标 $\mathrm{CI}_1,\mathrm{CI}_2,\cdots,\mathrm{CI}_{500}$，计算可得：

$$\mathrm{RI}=\frac{\mathrm{CI}_1+\mathrm{CI}_2+\cdots+\mathrm{CI}_{500}}{500} \tag{2}$$

因此，定义一致性比率为 $\mathrm{CR}=\frac{\mathrm{CI}}{\mathrm{RI}}$，当 $\mathrm{CR}<0.1$ 时，通过一致性检验。

（4）计算总排序权向量，并进行一致性检验。

总排序一致性检验可用一致性比率表示为：

$$\mathrm{CR}=\frac{a_1\mathrm{CI}_1+a_2\mathrm{CI}_2+\cdots+a_m\mathrm{CI}_m}{a_1\mathrm{RI}_1+a_2\mathrm{RI}_2+\cdots+a_m\mathrm{RI}_m} \tag{3}$$

当 $\mathrm{CR}<0.1$ 时，则通过检验。

步骤 2　进行主成分分析，将样本数据标准化；根据样本数据分别计算每个样本投入准则和产出准则矩阵的样本协方差的无偏估计，并分别求出各自的特征值，分别对投入矩阵和产出矩阵的协方差的特征值进行排序，计算累计贡献率；分别对投入准则的权重和产出准则的权重进行投影，分析结果。

假设：研究对象可以用 p 个变量进行描述，可以表示为 $X_1,X_2,\cdots,X_p$，这 p 个变量可以构成 p 维随机向量 X：

$$X=(X_1,X_2,\cdots,X_p) \tag{4}$$

设 X 的均值为 μ，协方差矩阵为 Σ。假设 X 是以 n 个标量随机组成的列向量，并且 μ_k 是其第 k 个元素的期望值，即 $\mu_k=E(x_k)$，协方差矩阵被定义为：

$$\Sigma=E\{(X-E[X])(X-E[X])\}=$$
$$\begin{bmatrix} E[(X_1-\mu_1)(X_1-\mu_1)],E[(X_1-\mu_1)(X_2-\mu_2)],\cdots, \\ E[(X_1-\mu_1)(X_n-\mu_n)] \\ E[(X_2-\mu_2)(X_1-\mu_1)],E[(X_2-\mu_2)(X_2-\mu_2)],\cdots, \\ E[(X_2-\mu_2)(X_n-\mu_n)] \\ \cdots \\ E[(X_n-\mu_n)(X_1-\mu_1)],E[(X_n-\mu_n)(X_2-\mu_2)],\cdots, \\ E[(X_n-\mu_n)(X_n-\mu_n)] \end{bmatrix} \tag{5}$$

对 X 进行线性变化，考虑原始变量的线性组合为 Z_p：

$$Z_p=\mu_{p1}X_1+\mu_{p2}X_2+\mu_{pp}X_p \tag{6}$$

其中，$Z_1,Z_2,\cdots,Z_p$ 互不相关，且为原始变量的主成分；Z_1 是 $X_1,X_2,\cdots,X_p$ 的线性组合中方差最大者，Z_2 是与 Z_1 不相关的线性组合中方差最大者，…，Z_p 是与 $Z_1,Z_2,\cdots,Z_{p-1}$ 都不相关的线性组合中方差最大者。

人民邮电出版社

步骤 3 进行模糊评价，根据主成分分析结果，确定指标集 U 和评价集 V，计算各个隶属的权重和隶属度向量，得到模糊评判矩阵，然后根据模糊评判矩阵和各因素的权向量，进行模糊计算，然后做归一化处理，得到模糊综合评价结果。具体步骤如下所示。

（1）确定评价因素，将被评价对象的 m 种因素（即评价指标）表示为 $U=\{u_1,u_2,\cdots,u_m\}$，其中，m 是评价因素的个数，由具体指标体系来决定。

（2）确定评价等级，被评价对象的评价等级有 n 种，表示为 $V=\{v_1,v_2,\cdots,v_n\}$，其中，n 为评级个数，每个评级对应一个模型子集。n 取值一般为（3,7）中的整数，其中 n 取奇数的情况较多，这样可以有一个中间等级，容易判断被评事物的等级归属。

具体等级可以根据评价内容描述，本文将供应商绿色化程度分为 5 种，表示为：V ＝｛强，较强，一般，较弱，弱｝。

（3）构造评价矩阵，首先对单因素 u_i（i=1,2,⋯,m）作单因素评判，从因素 u_i 入手，判定该事物对抉择等级 v_j（j=1,2,⋯,n）的隶属度为 r_{ij}，这样就得出了第 i 个因素 u_i 的单因素评价集：$r_i=(r_{i1},r_{i2},\cdots,r_{im})$。

这样 m 个因素的评价集就组成了一个总的评价矩阵 R，如下：

$$R=(r_{ij})_{m\times n}=\begin{matrix} r_{11} & r_{12} & \cdots & r_{1n} \\ r_{21} & r_{22} & \cdots & r_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ r_{m1} & r_{m2} & \cdots & r_{mn} \end{matrix} \quad (7)$$

（4）确定评价因素的模糊权重 A：获得模糊关系矩阵后，由于各评价因素在综合评价中占有不同的比重，因此还不能对事物做出评价。我们假设引入 U 上的一个模糊子集 A 作权重分配集，表示为：

$$A=(a_1,a_2,\cdots,a_m),\ \text{其中}a_i>0,\ \text{且}\sum a_i=1 \quad (8)$$

其中，a_i 为各因素的权重。

（5）利用合适的合成算子将 A 在各被评事物的 R 合成得到各被评事物的模糊综合评价结果向量 B。

（6）对模糊综合评价成果向量 B 进行归一化后，得到不同供应商的绿色化指标值，根据数据大小，判定不同供应商的绿色化程度。

4.3 绿色供应商管理机制

根据对供应商的评价结果，将评价得分分为 A、B、C、D 4 个等级，A、B、C 级为合格，其中 A 级代表最优，D 级代表不合格。将供应商根据是否绿色分为 4 类，分别为各级供应商颁发绿色等级认证，实行差异化分级管理。同时为了激励供应商不断向绿色转型，提高绿色发展水平，在管理中设计激励机制和退出机制，每期评价后，对当期评价成绩优秀的供应商采取奖励等激励措施，对评价不合格的则进行淘汰，不断更新供应商库，加快绿色供应商库的建设完善。

5 结束语

本文选取了 AHP、PCA、模糊评价 3 种方法，并在供应商绿色评价指标中加入了信息化技术因素，构建信息化背景下绿色供应商评价体系，并通过 3 种方法结合，从“定性+定量”方面综合提出了绿色供应商评价模型，有效实现了对绿色供应商的科学、客观评价，有利于企业准确选择绿色供应商，并对供应商进行管理，实现优胜劣汰。

参考文献：

[1] WEBB L. Green purchasing: forging a new link in the supply chain[J]. Engineering and Technology for Sustainable World, 1994, 1(6): 14-18.

[2] NOCI G. Designing ‘green’ vendor rating systems for the assessment of a supplier’s environmental performance[J]. European Journal of Purchasing & Supply Management,1997, 3(2): 103- 114.

[3] WALTON V S. The green supply chain: integrating suppliers into environmental management process[J]. International Journal of Purchasing and Material Management, 1998, 34(1): 2-10.

[4] HANDFIELD R, WALTON S, SEEGERS L, et al. Applying environmental criteria to supplier assessment: a study in the application of the analytical hierarchy process[J]. European Journal of Operational Research, 2002, 141: 70- 87.

[5] 王能民, 孙林岩, 汪应洛. 绿色制造模式下的供应商选择[J]. 系统工程, 2001, 19(2): 37- 41.

[6] ZHU Q H, SARKIS J. Relationships between operational practices and performance among early adopters of green supply chain management practices in Chinese manufacturing enterprises[J]. Journal of Operations Management, 2004, 22: 265- 289.

[7] 张平, 吴春旭. 绿色供应链管理中合作伙伴的评价与选择[J]. 价值工程, 2005(2): 44-46.

[8] 刘志峰. 基于模糊 AHP 方法的供应商绿色评价研究[J]. 机械科学与技术, 2007, 26(10): 1249-1252.

[9] 史成东, 陈菊红, 张雅琪. 基于 BP 神经网络和 DEA 的物流供应商选择[J]. 工业工程, 2010, 13(4): 112.

[10] 邹欣, 丁丹, 张梦岑. 基于 AHP-PCE 法的绿色供应商选择决策研究[J]. 物流科技, 2015(1): 125-129.

[11] 李海波, 张晨曦, 赵丽, 等. 基于 AHP 的绿色供应商选择的评价研究[J]. 河北建筑工程学院学报, 2018, 36(3): 68-74.

[12] 徐光华, 赵雯蔚, 黄亚楠. 基于 DEA 的企业减排投入与产出绩效评价研究[J]. 审计与经济研究, 2014,(1): 103-110.

[13] 李佳桐, 刘媛华. 基于主成分和灰色层次关联的供应链金融信用风险研究 [J]. 物流科技, 2014(11): 16-21.

[14] 袁泉, 姚金江. 浅议绿色物流评价指标体系的构建[J]. 物流科技, 2014(1): 41-44.

人民邮电出版社

一种基于遗传算法的数据脱敏方法

李澜，杨华，马维青
（国网阳泉供电公司，山西 阳泉 045000）

摘　要：数据工程在当今的预测与分析领域中起着至关重要的作用，随着数据搜集的速度不断提高，数据量也逐渐增大。各个组织和机构都希望从大数据中挖掘具有业务价值的多种信息。介绍了一种基于遗传算法的数据脱敏方法，对敏感数据进行信息内容的变换，在保留原有语义和数据源特征的同时，完成数据的脱敏处理。通过设置可调整的遗传终止条件，令脱敏效率可以基于应用场景自由调整。

关键词：大数据安全；数据脱敏；信息安全

1　引言

随着信息技术的发展，信息社会的数据迅猛增长的同时，人们获取和利用信息的手段也逐渐丰富。数字信息在社会活动的各个领域中扮演着愈加重要的角色，网上购物、电子支付、远程多媒体应用等新兴应用和服务极大地改变了人们的生活方式。社会的各个方面与大数据技术的结合愈加紧密，隐私信息以各种形式被记录和存储，隐私保护已经成为一个巨大的挑战。

2　相关研究

隐私保护涉及密码学、通信、信息论等领域。为解决隐私保护和数据脱敏等问题，诸多学者进行了大量的研究，并提出了很多有效的解决方法，主要包括基于匿名的隐私保护技术、基于加密的隐私保护技术、基于噪声的隐私保护技术和差分隐私保护技术。

匿名隐私保护技术在发展初期最具有代表性的是 *k*-匿名方法[1]，这是数据聚类隐私保护技术中的第一种方法，通过将待脱敏数据中的标识符泛化并进行等价类划分，来保证脱敏处理的有效性。其安全性与等价类中元素的个数 *k* 呈负相关，但由于不能保证等价类内元素的多样性，脱敏后数据仍有较大概率被攻击成功。为了解决 *k*-匿名方法等价类内元素单一的问题，进一步提出了 *L* 多样性模型[2]，有效克服了 *k*-匿名方法的缺陷。同时后来提出了 *t*-closeness 方法[3]进一步解决 *L* 多样性模型易受倾斜攻击的问题。因此，可以发现基于匿名的隐私保护技术往往在脱敏效果方面不尽如人意，这是由于匿名本身无法掩盖敏感数据的其他维度特征，使攻击者可以轻易地通过其他信息破译脱敏数据。

基于加密的隐私保护技术以密码学为理论基础，安全性取决于破译密码学算法的难易程度，在多方安全计算、同态加密、区块链技术中得到了广泛的应用，但其依然存在诸多局限性。虽然攻击者无法直接通过破译密码算法完成攻击，但是通过中间人攻击、差异攻击等方式，依然可以有效地截获或推断解密后的隐私数据。同时，密码算法的性能严重影响了数据脱敏效率，为终端带来了巨大的性能开销。

Dwork 等人为解决差分攻击问题，进一步提出了差分隐私保护框架[4-5]，这是一种严格的隐私保护模型，并在 2010 年提出了差分隐私保护的统计解释[6]。同时根据隐私保护的研究路线，提出了差分隐私保护框架的差异可识别性[7]和成员隐私[8]的概念。但是大量的隐私框架，都假设所有用户共享相同的隐私标准，并忽略个人隐私的差异，于是又产生了个性化的隐私保护方法[9-10]。

综上所述，目前的多种隐私保护技术存在着不能兼顾安全性和脱敏性的问题，设计一种有效的数据脱敏方法，在保证安全性的同时能够有效地提高数据脱敏效率，具有重要的应用价值和研究意义。

3　基于遗传算法的数据脱敏方法

本节主要介绍一种基于遗传算法的数据脱敏方法，在定位敏感数据后进行脱敏处理，在保证脱敏后

人民邮电出版社

数据安全性的同时，能够通过阈值动态调整算法效率。

遗传算法以一种群体中的所有个体为对象，并利用随机化技术指导对一个被编码的参数空间进行高效搜索。其中，选择、交叉和变异构成了遗传算法的遗传操作；参数编码、初始群体的设定、适应度函数的设计、遗传操作设计、控制参数设定 5 个要素组成了遗传算法的核心内容。表 1 对比了自然界的遗传规律、遗传算法及本文中所提出的数据脱敏遗传算法。

表 1　遗传算法对比

自然界	遗传算法	数据脱敏遗传算法
染色体	特征串	敏感数据
基因	特征	敏感数据编码
等位基因	同位置特征	同位置编码
基因位置	特征位置	编码位置
基因型	结构	结构
表型	参数集、译码结构	参数集、译码结构

3.1　数据脱敏遗传算法流程

本文中提出的数据脱敏遗传算法可表示为 $\mathrm{GA}=(C,E,P,M,\Phi,\Gamma,\Psi,T)$。算法主要包含 8 个元素，分别为敏感数据编码方法 C、脱敏效果评价函数 E、待脱敏数据 P、待脱敏数据种群大小 M、选择算子 Φ、交叉算子 Γ、变异算子 Ψ、遗传运算终止条件 T。

算法主要流程如图 1 所示。步骤为：（1）首先根据选择算子 Φ、交叉算子 Γ、变异算子 Ψ，模拟基因遗传的自然选择和遗传过程中发生的繁殖、交叉和基因突变现象；（2）在每次迭代中都保留一组候选解，并按选择算子 Φ 从解群中选取较优的个体；（3）利用选择算子 Φ、交叉算子 Γ、变异算子 Ψ 再对这些个体进行组合，产生新一代的候选解群；（4）重复此过程，直到满足遗传运算终止条件 T 为止。

3.2 敏感数据编码方法及脱敏终止策略

首先制定敏感数据编码方法 C。由于在大数据中数据来源种类繁多，但在底层均以二进制形式进行存储，因此在基于遗传算法的数据脱敏方法中，敏感数据编码方法遵循各数据源的底层二进制形式编码字符，实现对数据源的通用型，形成二进制形式的待脱敏数据 P_0。如敏感字符串 P 为 1234，编码后为 0001001000110100，记作 P_0。

进一步设置待脱敏数据种群大小 M，将待脱敏数据 P_0 从右至左平均分为 M 份，每份二进制位数为 $\lfloor P_0/M \rfloor$，位数不足 $\lfloor P_0/M \rfloor$ 用 0 补齐。最终得到初始种群 $S1=\{s_1,s_2,\cdots,s_m\}$。例如，编码后敏感字符 P_0 为 0001 0010 0011 0100，设置种群大小 M=4，则初始种群为 $S1=\{s_1=0001,s_2=0010,s_3=0011,s_4=0100\}$。

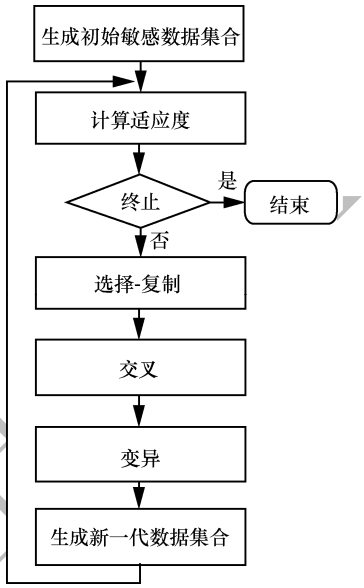


图 1　数据脱敏遗传算法流程图

同时遵循数据脱敏的基本原则，最大程度使脱敏处理后的数据与原数据间关联性最低。因此由脱敏效果评价函数 E 决定经过遗传算法脱敏后数据的适应度，其计算方法为将初始种群 $S1$ 和遗传算法衍生的种群 Sn 均表示为向量形式，记做 $(s_{11},s_{12},\cdots,s_{1m})$ 和 $(s_{n1},s_{n2},\cdots,s_{nm})$。然后通过计算 $S1$ 和 Sn 两个向量间的相似度，判断数据脱敏的效果。适应度计算式如下：

$$f(S1,Sn)=1-\frac{S1\cdot Sn}{|S1|^2+|Sn|^2-|S1|\cdot|Sn|} \tag{1}$$

此时适应度的值域为[0,1]，适应度越趋近 1 时，$S1$ 和 Sn 两个向量相似度越低，脱敏前后数据的关联性越低。当满足遗传运算终止条件 $T:f(S1,Sn)>x$ 时，遗传算法停止，其中 x 为适应度阈值，通过 x 可对数据脱敏程度及数据脱敏算法效率进行调节。

3.3　种群个体遗传策略

种群个体遗传策略包括选择算子 Φ、交叉算子 Γ、变异算子 Ψ 的设置。

设置选择算子 Φ。对初始种群 $S1$ 中的每一个体元素 S_i 计算其选择概率 $P(s_i)=\frac{s_i}{\sum_{i=1}^{m}s_i}$。并应用轮盘赌机制，作为个体选择算法，在[0,1]区间产生 1 个分布均匀的随机数 q。若 $q<q(s_1)$，则种群中第 1 个个体 $S1$ 被选中；若 $q(s_{i-1})<q<q(s_i)$，则种群中第 i 个个体 s_i 被选中。其中，$q(s_i)$ 为个体累积概率，$q(S_i)=\sum_{j=1}^{i}p(S_j)$。例如，在区间[0,1]产生 4 个随机数为 q_1=0.4，q_2=0.1，q_3=0.5，q_4=0.9，则经选择算子生成选中结果见表 2。生成下一代种群 $S2=\{s_1=0001,s_2=0011,s_3=0011,s_4=0100\}$。

表 2　选择算子种群生成表

染色体	适应度	选择概率	累积概率	选中次数
$S1$=0001	1	0.1	0.1	1
$S2$=0010	1	0.2	0.3	0
$S3$=0011	1	0.3	0.6	2
$S4$=0100	1	0.4	1.0	1

设置交叉算子 Γ。设交叉率为 p_Γ%，即为种群 Sn 中 p_Γ%的染色体参与交叉，交叉方式为染色体两两间交换集合 c 中的每一位二进制字符。若 p_Γ=100，c\{0,1\}，则种群 $S2$ 中 s_1 与 s_2 交换第 0 位和第 1 位的字符，s_3 和交换第 0 位和第 1 位的字符，得到种群 $S3=\{s_1=0011,s_2=0001,s_3=0000,s_4=0111\}$。

设置变异算子 Ψ。设变异率为 p_Ψ，则种群中的所有个体每一位上的二进制字符以概率 p_Ψ 进行变异（取反）得到种群 $S4$。若 $S1=\{s_1=0001,s_2=0010,s_3=0011,s_4=0100\}$，$S4=\{s_1=0011,s_2=0001,s_3=0000,s_4=0111\}$，根据种群适应度计算式，得到群 $S4$ 的适应度 $f(S1,S4)$=0.629。经过以上步骤对每一个二进制形式的敏感数据进行脱敏处理。若种群 Sn 适应度大于预先设置的阈值 x，则算法迭代结束；若种群 Sn 适应度小于阈值 x，则重复以上算法过程直到满足算法终止条件 $T:f(S1,Sn)>x$。

4　实验与评估

本节将对文中提出的数据脱敏方法设计实验进行验证，以评估该方案的性能优劣。实验过程中硬件环境为 CPU 为 Intel i7 3.4 GHz，内存 8 GB，软件环境为 Red Hat Enterprise Linux 7，采用 UCI machinelearningrepository 数据集进行试验测试。

由于算法对隐私数据脱敏处理后的安全性由遗传算法终止条件 T 所保证，所以其脱敏处理后的数据一定是安全的。同时将数据集划分为不同数据量大小，测试算法的运行时间。同时设置不同的遗传算法终止条件 T，验证 T 与算法性能间的依赖关系。

当终止条件 T 的阈值 x 设置为 0.5 时，在不同的数据量下，算法的运行时间整体与数据量呈线性增长，由于待脱敏的数据量越大，处理时间也会相对延长。同时对于相同数据集，参与对比试验的基于数据聚类技术的 t-closeness[3]方法、面向数据挖掘的差分隐私保护算法 SmartTrunc[11]的 CPU 执行时间（s）都在逐步增加。本文方法与 SmartTrunc 性能基本接近，并优于 t- closeness 方法的性能。不同数据量对 CPU 执行时间的影响如图 2 所示。

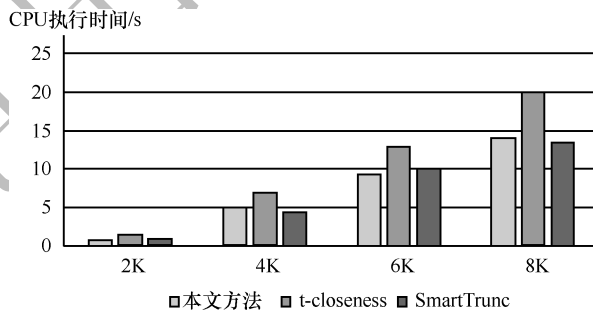


图 2　不同数据量对 CPU 执行时间的影响

同时，通过设置不同的终止条件 T 的阈值 x，进行了性能的测试。测试结果表明终止条件 T 的阈值 x 越大，算法的 CPU 执行时间越长，因此设置合理的终止条件 T 不仅能够有效保证脱敏后数据的安全性，同时能够有效提高算法脱敏的效率。不同终止阈值对 CPU 执行时间的影响如图 3 所示。

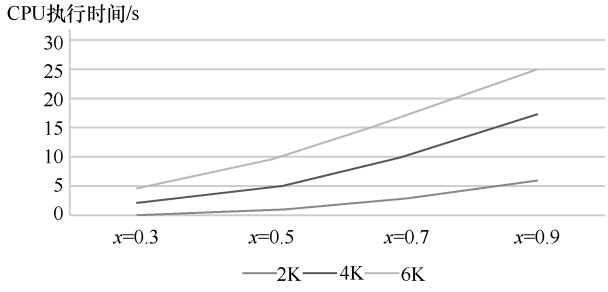


图 3　不同终止阈值对 CPU 执行时间的影响

人民邮电出版社

5 结束语

本文提出了一种基于遗传算法的数据脱敏方法，对敏感数据进行信息内容的变换，在保留原有语义和数据源特征的同时，完成敏感数据的脱敏处理。通过设置可调整的遗传终止条件，令脱敏时间可以基于应用场景自由调整。实验证明该方法能够有效地对不同数据源的敏感数据进行处理，同时有着较高的脱敏效率。

参考文献：

[1] SAMARATI P, SWEENEY L. Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression[C]//1998 IEEE Symposium on Research in Security and Privacy, May 3-6, 1998, Oakland, CA, USA. Piscataway: IEEE Press, 1998: 1-19.

[2] MACHANAVAJJHALA A, KIFER D, GEHRKE J, et al. L-diversity: privacy beyond *k*-anonymity[C]//22nd International Conference on Data Engineering (ICDE'06), April 3-7, 2006, Atlanta, GA, USA. Piscataway: IEEE Press, 2006.

[3] LI N, LI T, VENKATASUBRAMANIAN S. Closeness: a new privacy measure for data publishing[J]. IEEE Transactions on Knowledge and Data Engineering, 2010, 22(7): 943-956.

[4] DWORK C. Differential privacy[C]//33rd International Colloquium on Automata, Languages and Programming (ICALP 2006), July 10-14, 2006, Venice, Italy. New York: ACM Press, 2006: 1-12.

[5] DWORK C, MCSHERRY F, NISSIM K, et al. Calibrating noise to sensitivity in private data analysis[C]//3rd Theory of Cryptography, Lecture Notes in Comput. Berlin: Springer, 2006: 265-284.

[6] WASSERMAN L, ZHOU S. A statistical framework for differential privacy[J]. Journal of the American Statistical Association, 2010, 105(489): 375-389.

[7] LEE J, CLIFTON C. Differential identifiability[C]//ACM Sigkdd International Conference on Knowledge Discovery & Data Mining, August 8-12, 2012, Beijing, China. New York: ACM Press, 2012: 1041–1049.

[8] LI N, QARDAJI W H, SU D, et al. Membership privacy: a unifying framework for privacy definitions[C]//2013 ACM SIGSAC Conference on Computer & Communications Security. New York: ACM Press, 2013: 889-900.

[9] JORGENSEN Z, YU T. Conservative or liberal? Personalized differential privacy[C]//IEEE 31st International Conference on Data Engineering (ICDE 2015), April 13-17, 2015, Seoul, South Korea. Piscataway: IEEE Press, 2015: 1023–1034.

[10] PAI M M, ROTH A. Privacy and mechanism design[J]. ACM SIGecom Exchanges, 2013, 12(1): 8–29.

[11] ZENG C, NAUGHTON J F, CAI J. On diferentialy private frequent itemset mining[C]//39th Conference of Very Large Databases (VLDB 2013), August 26-31, 2013, Trento, Italy. [S.l.: s.n.], 2013: 1087-1098.

人民邮电出版社

应用软件自动化变更的方法与实践

卓林贵，李胜德，朱晓玲
(中国广核电力股份有限公司信息技术中心，广东 深圳 518000)

摘　要：信息系统自动化是企业信息化发展的趋势，统一的平台、先进的工具是信息系统运维自动化的基础。通过对应用软件部署方法、过程的分析研究，将原本重复低效的方式整合成统一的平台，实现集约化管控、自动化运行，提升自动化运维的程度，解决了企业应用部署成本高、用户需求响应不及时的问题。

关键词：应用部署；自动化部署；IT 系统自动化运维

1　引言

企业的信息化建设中，应用的部署架构依赖于 IT 基础架构的规划和建设，不同的 IT 基础架构，能够形成多样的应用部署方式。随着互联网技术的发展，企业数据库、服务器的存储经历从一体机到 PC 机再到虚拟机（容器化）的演变，部署模式也经历了从单机到双机再到分布式的多元化。在互联网企业中，基于云平台、中台等技术，已经发展出多套全新的技术研发、运维体系，颠覆了原有的开发框架、运维框架甚至是企业组织架构和项目管理方式。在这样的架构体系中，服务器存储资源集群化、共享化，通过平台管理工具能便捷地管理服务器资源和应用程序，就像它们都运行在同一台服务器上一样，集开发、编译、部署、配置于一体，使得应用的部署、代码的发布变得快速、持续、可靠和规模化高效的部署方式，满足了用户不断提高的对业务快速响应的需求。

但是，更多的传统企业，因行业安生性、合规性等因素的制约，无法快速地完成信息化转型，并且现在已有很多“烟囱式”的独立业务系统，像烟囱一样高高耸立，系统间的交互错综复杂，如果转型，将面临着技术重构和业务重构等多重问题。而这些系统大多采用原始的单机部署方式，因此应用系统的发布就存在手动执行、可靠性低等问题。新实施的项目越来越复杂，体系结构各自不同，一次批量上线发布，涉及多个应用系统，涵盖不同的数据库、中间件、操作系统、外部接口等，这种情况导致更新发布工作非常繁琐，容易出错，并且效率低下。

对于采用“局域网+自建服务器“的大中型传统企业，类似的部署方式如果普遍存在，那企业在应用部署成本和资源优化方面就面临很大压力，故在现有技术中，如何快速精确地进行应用程序的发布是一个亟待解决的问题。这时，自动化的变更工具就显得尤为重要，通过自动化的工具替代手动的步骤和脚本，可重复、可视化、可追溯地变更过程，不仅能提高发布效率、降低成本，同时能实现用户需求的快速响应和交付，最终保障应用系统的稳定运行。

2　背景和目的

某企业目前大部分的应用部署于“内部局域网+自建的服务器”之上，基础设施运维与开发使用部门权责分离，这种方式方便管理，稳定性、安全性相对较高，缺点是需要搭建专属的机房环境，需要专业的维护、安保人员保障服务器环境的正常运行，使得对投产资源、成本要求较高。同时，需要各部门紧密的工作协同，以保障设备、应用的频繁变更，跨部门的沟通、跨专业的协作，也增加了沟通成本。

为保障投产过程规范、系统成功投产，在流程上形成了标准的作业卡及程序规范，组织上成立了投产协调组，对投产的内容进行严格的测试扫描和多层级审查，对投产过程进行监控记录等。但是一系列的保障措施，又会带来更多其他方面的问题，跨部门、多专业协作，审核流程复杂，加上多途径沟通、环境差异等情况，导致投产准备工作多、时间紧，最终导致代码质量不高、验证异常等问题；投产相关的辅助工具缺失、技术方法落后，纯手工作业，出现人为干预、

水电部电力出版社

人为失误因素的概率增大，导致过程成本增加、效率低下。

基于以上情况，统一的管理平台、高效的投产工具就显得非常重要，自动化变更平台通过角色授权，能将多部门工作整合到一个平台中，能将投产准备、检查、审核、分发、执行、验证等多环节工作融合到一套流程体系中，既优化了管控、审核流程，同时减少了多途径沟通问题。对于投产过程出现的问题能及时捕获、实时提醒，提升问题处理速度，投产步骤能后台定义、自由组合，满足了不同类型系统的投产需求，具体操作在平台中逐步自动执行，不再需要执行人员频繁登录服务器设备手动操作，从根本上规避了手动操作、人为干预的问题，减少人为失误的同时，还很大程度上提升了执行效率。投产过程数据集中，便于统计查询，为信息展示、管理改进提供了基础。

2016 年，在集中投产业务范围逐渐扩大、投产系统逐步增多的背景下，开始进行自动化变更平台的设计和研发工作，并于 2018 年投入使用。

3 方案选型

比尔盖茨曾说过，“任何技术在一个业务中使用的第一条规则就是，将自动化应用到一个高效的操作上将会放大高效；第二条就是将自动化应用到一个低效操作上，则放大了低效”。为了实现高效的投产，平台在前期方案选型方面，结合了业界的方法和企业环境背景，对多种部署方式、技术和工具进行了分析比较，具体分为以下几类。

3.1 传统纯手工部署

单机集中式部署方式，在中小型企业、工作室使用，适用于单站点应用、部门和个人网站，系统规模小，用户量少，运维人员有限，成本投入有限，但是版本更新快，具体的部署操作由开发人员执行，服务器数量少，没有专业的服务器设备管理部门。具体的操作步骤主要靠人工手动执行，包含代码文件打包，准备脚本、登录产品应用服务器，文件、数据库备份，上传至服务器共享文件夹，代码复制、粘贴，解压，登录产品数据库客户端，SQL 脚本编译、执行等。

这种方式的优势是简单、方便，在不影响使用的情况下可实时发布，实时回滚。但这种手动部署方式既慢又容易出错，需要大量的人力投入来保障实施，并且应用系统结构越来越复杂，开发语言的多元化，对部署环境、存储终端的多样性要求也越来越多，这样对投产人员的技能水平、工作效率的要求也就越高，目前基础设施的人员投入矛盾逐步显现，增加更多的人员也不能解决这方面的问题，甚至可能会适得其反。所以手动部署方式带来的高额成本和低效的工作方式，已经无法满足企业中心日益增长的业务需求。

3.2 自动化变更平台部署

随着云计算、物联网和社交网络等信息技术的发展，企业信息化也将进入一个全新的阶段，应用系统投产管理也经历了从无组织无计划小范围作业的阶段向集中管控、集中投产的模式转换，系统的部署方式也经历了从单机运行到双机负载再到多层分布式的变化，到目前为止已经形成了一套完整的投产管理流程，流程中的各种角色、职责也很明确，但是还缺乏投产相关的工具应用，技术上较为落后。企业存量的老旧系统较多，大部分是单机部署，互联网企业流行的部署方式和工具并不适用，需要将现有的流程、组织架构、人员和技术结合企业现有的实际情况，采用“传统方式+自动化执行工具”的方式，开发一套属于自己的自动化部署平台，以补充在技术、工具方面的短板。

4 自动化变更方案

自动化变更平台使用开发工具 Visual Studio 2012 进行开发，基于.Net Mvc 框架，采用跨平台通信接口，执行服务器命令，实现跨平台、跨操作系统的程序交互。具体方案设计从以下 3 方面考虑。

4.1 人员/组织架构

企业集中投产涉及到的角色包括投产协调组、应用开发人员、基础执行人员和系统用户。投产协调组负责投产活动的统筹管理，投产方案步骤、文档、配置的审核、投产作业过程的管控以及汇总统计等工作，组成人员包含公司分管领导以及应用软件和基础设施的相关同事；应用开发人员指具体的软件开发人员，负责完成代码的实施、测试及投产准备工作；基础执行人员指投产步骤执行人员，拥有应用服务器、数据库权限；系统用户指需求提出人员，配合完成投产后的系统验证；平台将所涉及的人员/组织，根据角色分别对应到具体的功能模块、流程中，配合人员管理、授权体系进行权限控制，以满足投产活动的人员保障。

4.2 流程

平台中有两种类型的流程，一类是投产过程业务流程，另一类是投产执行流程。投产过程业务流程是

人民邮电出版社

投产活动的管理流程，也是业务数据的流转流程；投产执行流程是投产步骤的执行流程，通过编排自由排序、组合投产步骤，平台会根据编排好的投产步骤，按顺序自动执行。

（1）投产过程流程（业务流程）

投产的需求来源于应用系统的变更需求，用户先提交需求申请，接着由开发人员实施、测试，最后再发起投产申请。用户需求通过 IT 服务与信息管理平台简称 IT100，IT100 作为自动化变更平台的上游系统，将获取的用户需求申请流程 BG 单信息作为输入项，最后开始自动化变更投产流程。投产流程在平台中经过审核、分发，再由执行人员一键执行，平台调用投产执行流程，后台自动执行，完成投产作业。投产协调组通过平台对投产过程进行实时监控，完成投产的审核及权限回收工作。

（2）投产执行流程（技术流程）

投产的操作步骤由平台维护人员提前定义，方法独立封装，使用人员根据系统投产的需要编排操作步骤逻辑，并根据提示输入步骤的参数即可，不需要任何编程就能快速定义部署逻辑，实现快速、便捷地完成投产执行流程的准备工作。

同一套系统的投产执行流程可以重复使用，可以配置多台目标服务器，将程序代码、SQL 脚本部署到多个环境中，实现分布式部署。同时，可以提前编排回滚步骤，根据流程执行情况，选择执行，实现投产失败后快速回滚。

投产执行流程为使用者提供了每个流程步骤信息的可见性，可动态显示执行进度，及时获取执行结果。平台预定义了各种类型的异常提示，能帮助使用者在出现执行异常时快速定位异常类型，及时调整执行步骤。

投产操作步骤可通过服务器代理和跨平台通信协议，直接对服务器进行相关操作，操作步骤必须是可靠、安全的。平台对可执行的操作步骤，建立了命令黑名单，自动过滤非法操作命令，规避执行的操作命令对服务器的危害。同时，通过权限对待执行的流程进行控制，投产协调组可以冻结、解锁流程，实现对执行过程的管制。

平台架构及跨平台传输如图 1 所示。

4.3 技术/工具

本平台采用“BS 架构+服务端代理”模式，通过 Socket、SshNet 技术实现与 Windows 和 Linux 服务器、数据库服务器跨平台异步通信，远程执行 C#、Shell 动态指令，完成服务器端的站点部署及文件发布等一系列操作，满足应用系统发布的需求。

（1）平台支持的类型

平台支持 Windows 2003、Windows 2008、Windows 2012、Windows 2016 和 Linux 操作系统，Oracle、SQL Server 数据库，.Net 框架，Java 框架系统。

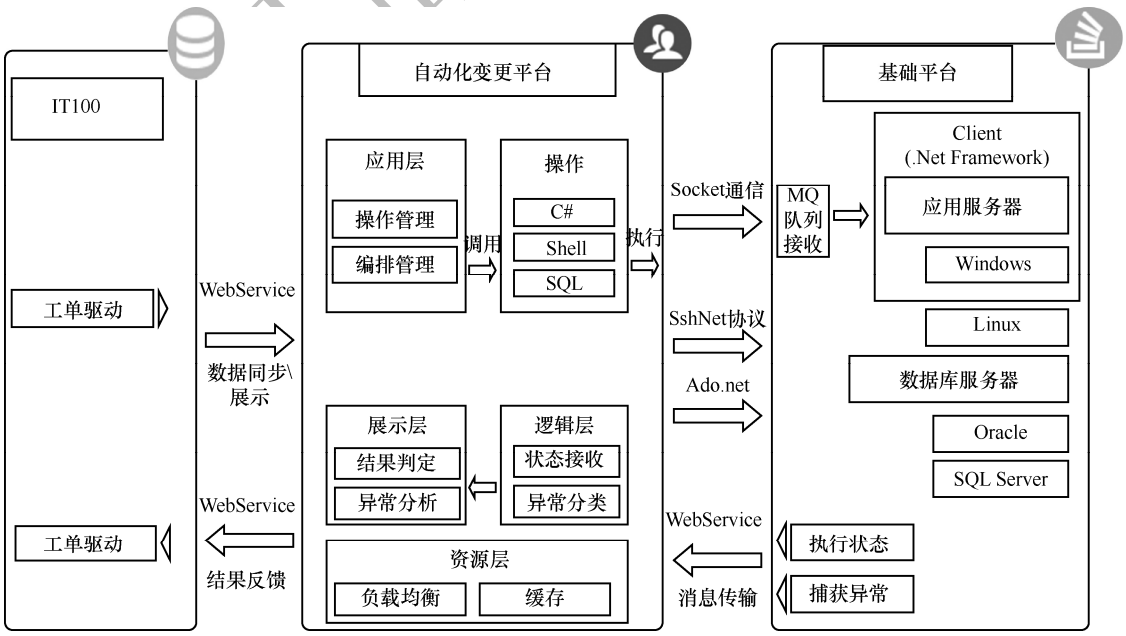


图 1　平台架构及跨平台传输

（2）平台支持的操作步骤

平台中已定义操作步骤 35 项，包括新项目部署、在运系统变更和系统回退等，同时，可根据实际需要，逐步完善和添加更多类型的操作步骤，以满足各种投产场景需求。

（3）平台使用技术

如图 2 所示，平台采用 Socket 方法，通过操作步骤配置的服务器 IP 地址和预设端口，向目标 Windows 服务器发送通信请求，服务器端通过提前安装的服务程序响应请求，实现跨服务器的通信技术。

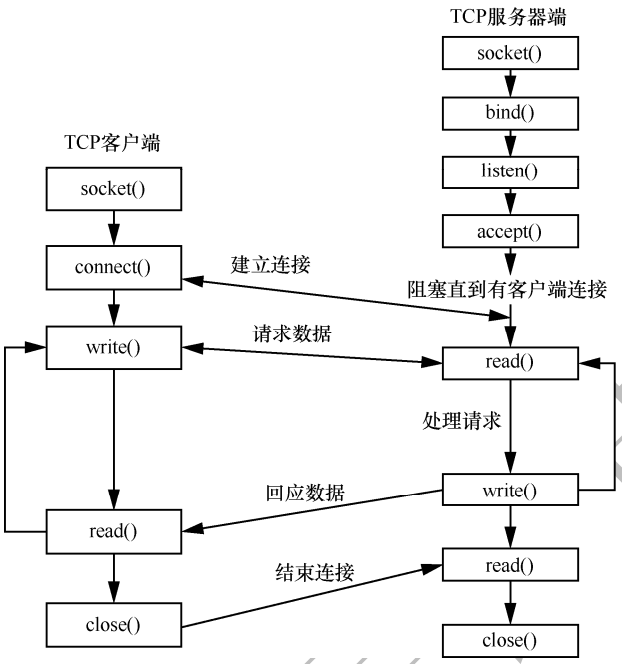


图 2　Socket 通信技术

SSH 安全协议是一种网络协议，专为远程登录会话和其他网络服务提供安全性。平台通过 SSH 协议，实现与 Linux 服务器的加密登录，并配合 Shell 命令脚本，执行投产操作，完成投产步骤的自动化执行。

5　自动化变更平台推广与应用

自动化变更平台支持的投产方式，可以是周期性的集中投产，也可以是每天的实时投产，带来了投产模式的变革。平台上线后在各专业处得到了大力推广，业务范围覆盖了大亚湾、阳江、台山、宁德、防城港、红沿河等多个核电基地的应用系统，目前通过平台投产的系统总数实现占比集中投产的 60%，达到了平台推广的预期。

总结了平台推广应用的情况，从以下几个方面初步实现了平台建设致力于降低成本、提升质量的两个目标。

（1）实施过程管控

实现了投产从线下、低效的管理方式到流程电子化的转变，规范了投产相关的程序标准，集多角色、多活动节点功能于一个平台，改善了投产活动的管控和治理工作。

（2）缩短执行时间

平台简洁的审批流程、便捷的操作编排，减少了投产准备环节的投放。投产步骤的自动化执行，避免了执行人员频繁登录服务器，降低了人为失误的概率，投产过程异常快速定位，节约了问题分析处理的时间，让整个投产执行的时间缩短了近 50%。

（3）降低沟通成本

平台将投产涉及的开发部门、基础设施部门等各专业处集中到统一的平台上协同办公，及时联动，减少了大量的邮件、电话沟通工作。同时，投产执行过程规范、有序，不需要进行监控作业，降低了无效、低效沟通带来的成本。

6　结束语

某企业基础设施从初期的单个基地的物理机房发展到目前多基地的虚拟化集群，单靠人工已经无法满足在技术、业务、管理等方面的要求，因此标准化、自动化、架构优化、过程优化等降低运维服务成本的因素越来越被重视。应用系统运维也需要面对越来越复杂的业务和越来越多样化的用户需求，不断扩展的应用需要越来越合理的模式来保障运维服务能灵活便捷、安全稳定地持续运行。

自动化变更工具作为重要措施之一已经不仅是代替人工操作，更重要的是深层探知和全局分析，关注的是在当前条件下如何实现性能与服务最优化，同时保障投产成本的最小化。自动化运维体系也成为企业在逐步实施的目标，自动化变更平台正是自动化运维体系中的一个具体实现，但是除此之外，还需配合事件自动化监控、异常自动化诊断、故障自动化修复等辅助工具形成联动，才能通过自动化运维方式，提高运维工作的效率，提高运维服务的质量。

参考文献：

[1]　IT 运维自动化正在成为趋势[Z].

[2] 陈思.基于多平台的自动化部署方案的研究与实现[J]. 电子测试, 2011(5): 89-93.
[3] 微服务部署：蓝绿部署、滚动部署、灰度发布、金丝雀发布[EB]. 2017.
[4] 李艳霞, 袁芳, 刘乃嘉, 等. 应用自动化部署平台的研究与实现[J]. 实验技术与管理, 2016, 33(8): 126-128.
[5] 闫龙川, 刘军. 企业信息系统自动化运维工具研究与应用[J]. 供用电, 2015(8): 78-81.
[6] 王树杰. 虚拟化环境下的应用部署系统的设计和实现[D]. 广州: 华南理工大学, 2014.

人民邮电出版社

园区级泛在电力物联网——局域能源互联网研究及应用

寇建涛[1]，贾少堃[2]，白洁[2]，魏建丰[2]
（1.国家电网有限公司客户服务中心，天津 750021;
2.北京中电飞华通信股份有限公司天津分公司，天津 300040）

摘　要：建设泛在电力物联网是实现能源转型目标的必要手段。叙述了园区级泛在电力物联网—局域能源互联网的研究及其定义，分析了局域能源互联网的建设，提出了能源综合管控方式和策略。希望达到有效解决能源问题、促进能源模式的创新发展、推进能源行业转型升级的目的。

关键词：泛在电力物联网；局域能源互联网；运行调控平台；协调优化；经济运行

1　引言

近年来，化石能源的广泛应用虽然给发展中国家带来了经济急速增长，也导致了气候变化、环境恶化等危机。随着可再生能源与信息技术的快速发展，以建立更高效、安全以及可持续的能源利用模式为目标的能源变革已经拉开帷幕。以“互联网+”为手段，以智能化为基础，围绕构建绿色低碳、安全高效的现代能源体系，促进能源和信息深度融合，推动能源互联网新技术、新模式和新业态发展，推动能源领域供给侧结构性改革，支撑和推进能源革命，是社会发展的必然选择。

2011 年，美国学者杰里米里夫金在著作《第三次工业革命》中率先提出了能源互联网的概念，并给出了能源互联网的特征：以可再生能源+互联网为技术核心，实现电网中可再生清洁能源的广泛接入，实现能源的公平交易和高效综合利用。这种借助互联网信息技术改善能源行业的想法一经提出，就受到了国内外学术界和产业界的广泛关注，成为了继智能电网后又一前沿发展方向和重要课题[1]。

2019 年，国家电网有限公司提出了泛在电力物联网的概念。泛在电力物联网是以电力系统为核心，结合智能终端传感器、通信网、人工智能、云平台技术，构成的复杂多能流系统。泛在电力物联网通过电力系统设备信息交互、人物信息交互，实现能源生产与消耗的实时平衡，保障电网的经济安全运行；具有全息感知、泛在连接、开放共享、融合创新的特征[2]。泛在电力物联网不仅是技术创新，更是管理创新，建设泛在电力物联网是社会和科技发展的必然。

本文以国网客服中心园区级泛在电力物联网——局域能源互联网项目为例，介绍局域能源互联网的研究及其定义，分析局域能源互联网的建设及能源综合管控方式和策略。

2　局域能源互联网概况

2.1　定义

笔者研究的局域能源互联网是以电能为中心，灵活接纳多种可再生能源，广泛集成能量流和信息流，实现能源生产和能源消费的协调控制、优化运行，具有分布接入、泛在物联、需求感知、网络共享特征的局域能源互联网，如图 1 所示。

以南北园区局域能源互联网为例，由能源网运行调控平台+能源子系统组成。南北园区局域能源互联网以电能为唯一外部能源，规模化高效应用区域太阳能、风能、地热能、空气热能 4 类可再生能源，建成光伏发电、风力发电、地源热泵、冰蓄冷、蓄热式电锅炉等 9 种能源转换装置，并以电炊具替代传统灶具，按照“经济性、安全性、示范性”为原则建设局域能源互联网，按照“调得起、控得住、调得准”为原则部署能源网运行调控平台，通过调峰调蓄、优化调度、协调控制等策略，验证以电能为中心的区域多种能源联合优化运行及柔性负荷响应潜力，实现区域“源-网-荷-储”优化配置及利用，提高园区能源综合利用效率，实现对园区“冷、热、电、热水”的统一调度、综合分析和优化运行[3]。局域能源互联网呈现多点接入、协调控制、需求感知、高效节能的特点，为园区

人民邮电出版社

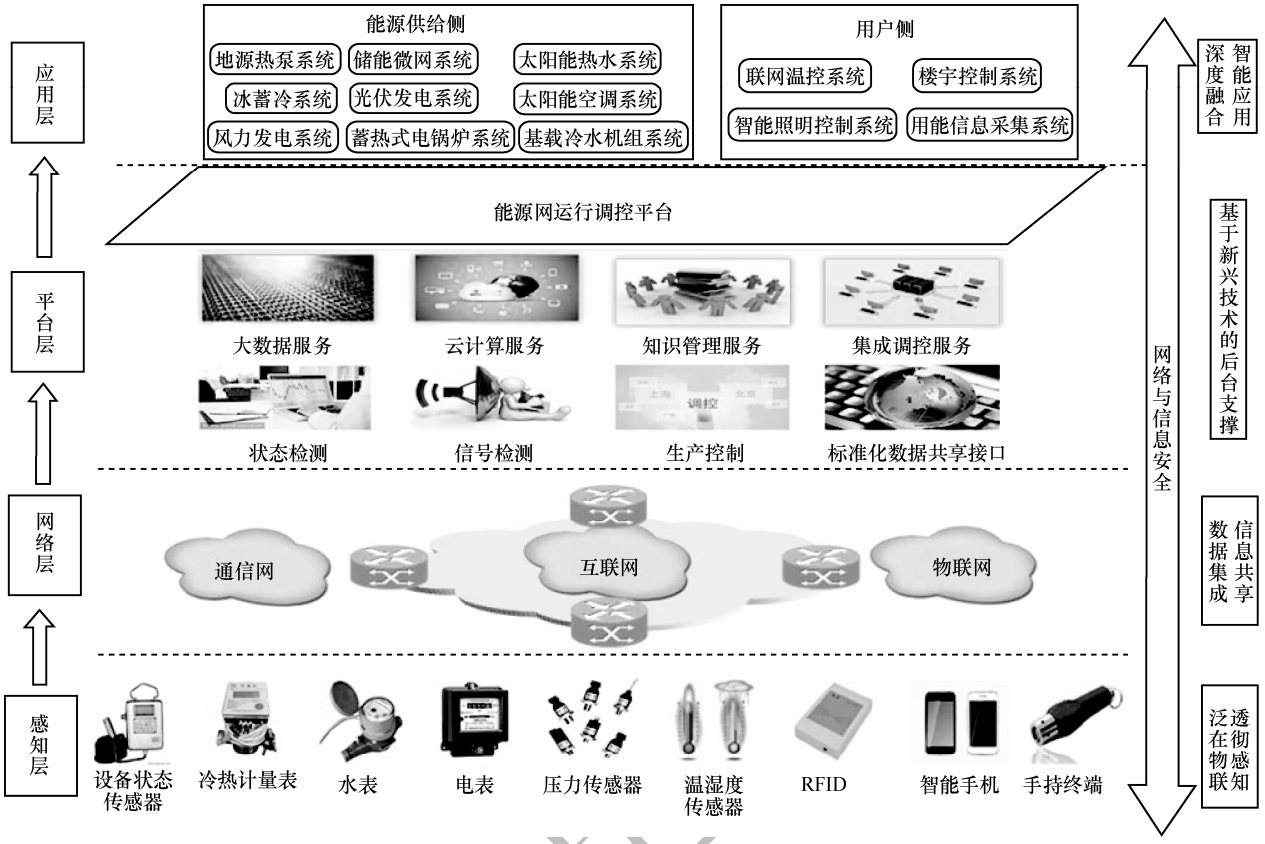


图 1　局域能源互联架构

提供安全可靠、绿色环保和经济节能的能源供应。

2.2　架构模型

国网客服中心南北园区构建了以电能为核心的局域能源互联网架构模型，实现了“源-网-荷-储”优化配置及利用，提升了区域能源综合利用效率，实现了对“冷、热、电、热水”的统一调度、综合分析和优化运行。在架构设计中，以电能为核心构建能源综合供给模型，因地制宜引入各种可再生能源，向用户提供灵活的电、冷、热等多种能源供应形式[4]。研发了能源母线结构建模方法，为局域能源互联网的规划设计和运行优化奠定了基础，通过对不同能源类型定义能源总线，实现了同类能源在同类母线下的汇集；通过不同类型能源转换系统模型的构建，实现了不同能源母线的互联。这一模型可清晰描述系统各组成设备之间的能量传递关系，同时保留了各组成部分的独立性和灵活性，有效协调了设备独立性和系统复杂性之间的矛盾，在系统描述和设备模型建模之间搭建了桥梁，为系统规划设计和调度优化提供了通用建模方法。同时，这种通用模块化的建模方法，也可以结合不同地域、不同项目特点，在架构模型基础上灵活增减、组合或扩展提升，易于项目推广延伸。

3　能源综合管控方式和策略

3.1　精细化分层协调控制

局域能源互联网项目应用物联网先进技术，系统分为调控主系统层、协调控制层、能源系统就地控制层，并精细化到主机设备层。

调控主系统层：根据负荷预测、生产预测、能源系统状态等因素，采用经济效益最优、绿色节能最优、综合最优的目标策略，调控平台自动生成日前调度计划并下发协调控制层。

协调控制层：将顶层运行调控平台的控制调度命令下发到就地控制系统内，并将子系统的运行情况上传到运行调控平台。

就地控制层：按照各自的工艺流程和就地策略控制系统内主机设备运行。

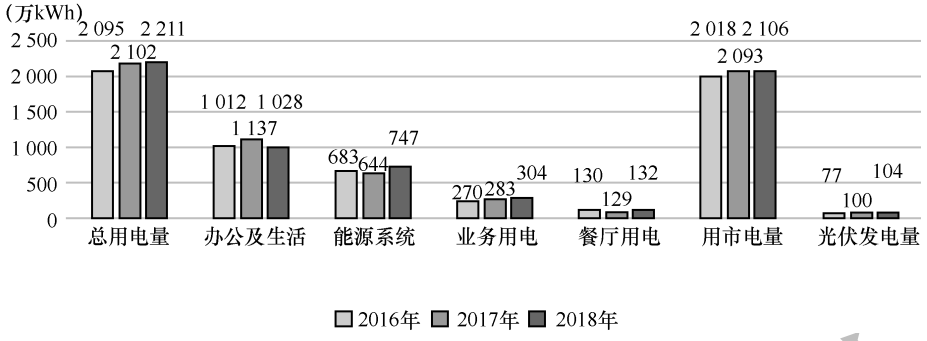


图 2　园区用电量统计

主机设备层：根据协调控制层指令，控制主机启停。

按照目标策略，生成日前调度计划，通过运行调控平台远程控制各子系统出水温度和工况，同时平台实时监测各系统设备运行情况，根据各子系统中主机的额定出力功率，将出力功率换算成主机启动台数，并根据故障状况和运行时长选择相应的主机进行开启，使调度计划深入各能源子系统的主机层面，细化平台调度计划作用的颗粒度，运用精细化分层协调控制技术，实现多能源综合协调优化控制。

3.2　多目标优化、多能源协调、准实时调控

局域能源互联网运用“日前计划与小时级自适应调整相结合”的多能源协调控制方法，开发能源互联网运行调控平台，实现综合能源系统的智能协同优化调控。一是项目根据冷、热、电负荷预测及风电、光伏等生产预测结果，结合能源系统运行状态与运行环境等具体情况，制定经济效益最优、绿色节能最优、综合效益最优 3 种能源协调优化目标及配比策略；二是多能源协调控制，面向电、冷、热、热水等多种用能需求，因地制宜、统筹规划、互补利用传统能源和新能源，充分发挥各能源生产系统的互联耦合作用，通过多能源互补集成，实现区域内多种能源优势互补、互联互享、协调供给及综合梯级利用；三是运用“日前调度与小时级自适应调整”的有机结合，解决动态响应时间尺度大情况下的多种能源优化调度问题，应用能源互联网运行调控平台，自动在每天 23：00 时计算、生成第二天 24 个时间点的各种能源生产调度计划，下发给各能源生产系统执行；还可以根据园区负荷状况和天气状况，或者突发事件的需要，对正在执行的生产配比计划进行及时调整，次日根据冷热、热水、电配比计划及负荷需求按需生产，同时系统能够进行生产微调，根据实际情况及负荷反馈情况，自适应调整，实现多能源系统、多时间尺度的智能协同生产及优化调控。

4　局域能源互联网运行分析

4.1　园区总用电量统计与分析

园区用电量统计如图 2 所示，单位建筑面积电能耗如图 3 所示。

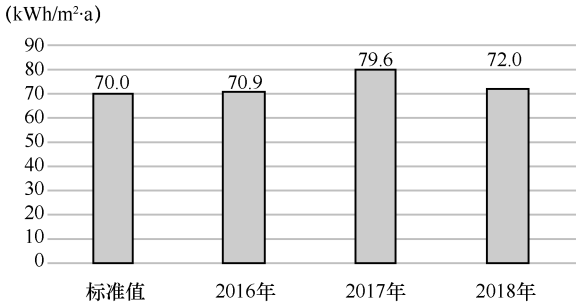
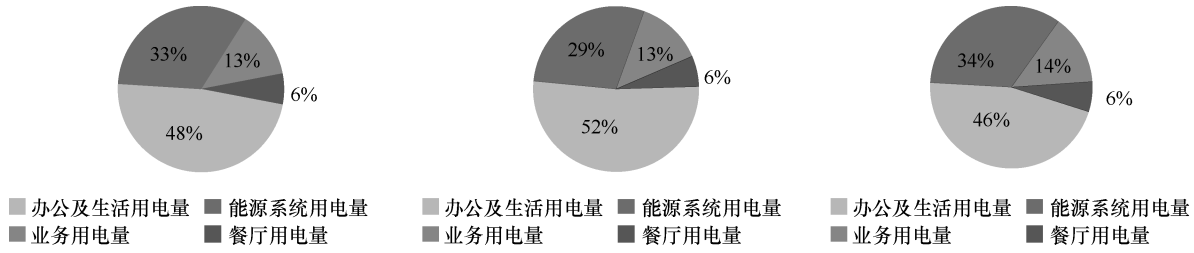


图 3　单位建筑面积电能耗

办公建筑单位建筑面积电能耗主要是办公及生活用电，能耗标准是 70 kWh/㎡·a，园区每年总的单位建筑面积电能耗均超过标准值，其中，2017 年电能耗最高为 79.6 kWh/㎡·a，超过标准值 13.7%。分析主要是因为园区属于 24 h 办公，所以园区单位建筑面积电能耗超过标准值属正常现象。

园区用电量构成如图 4 所示，能源系统用电量占 30%左右，业务用电量占 13%左右，餐厅用电量只占 6%左右，办公及生活用电量是园区的主要用电量，占总用电量的 50%左右，从节能角度考虑，只要办公生活用电量降低 10%，园区总用电量就能降低 5%，加强办公及生活用电量的节能措施，就能有效地降低园区总用电量。

水电部电力出版社



(a) 2016年园区用电量构成　(b) 2017年园区用电量构成　(c) 2018年园区用电量构成

图 4　2016-2018 年园区用电量构成

4.2　园区供冷量、供冷用电量、与供冷用电费用统计与分析

供冷用电成本如图 5 所示。从供冷用电成本分析，冰蓄冷系统供冷用电成本最低，基载机组用电成本最高。主要是因为冰蓄冷采用夜间低谷电蓄冰，高峰电价时融冰供冷，因此冰蓄冷经济效益最高，用电成本最低为 0.36 元/RTh。

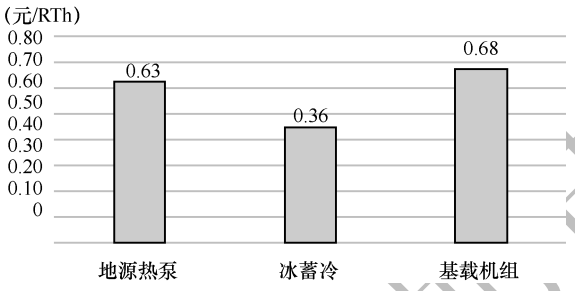


图 5　供冷用电成本

2017 年供冷量 180.9 万 RTh 高于 2016 年 5.67%，2017 年供冷用电费用与 2016 年持平，如图 6 所示。

由于 2017 年冰蓄冷产冷占比较 2016 年提高 11 个百分点，2017 年基载机组产冷量较 2016 年下降 6 个百分点。虽然 2017 年供冷量和用电量都较 2016 年有所提高，但 2017 年冰蓄冷供冷量提高，因冰蓄冷采用低谷电价蓄冰，所以 2017 年供冷用电费用降低，与 2016 年供冷用电费用持平。

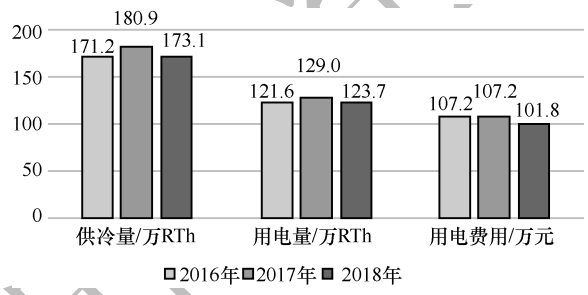


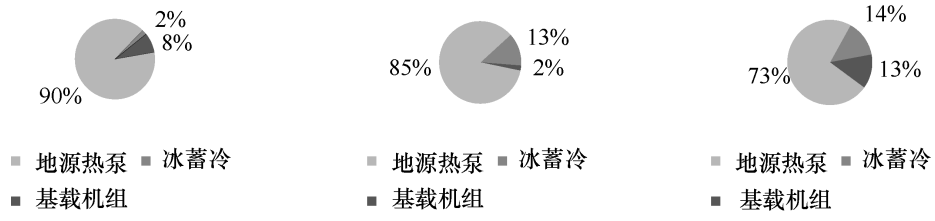
图 6　供冷量、用电量与用电费用

2016-2018 年供冷如图 7 所示。2018 年基载机组供冷量占总供冷量 13%，高于 2017 年 11 个百分点，在满足基载机组运行要求的情况下降低基载机组的供冷量，基载机组供冷量占总供冷量的 2%就可满足基载机组最低运行时长。

2018 年冰蓄冷供冷量占总供冷量的 14%，冰蓄冷系统的综合利用效率仅为 16.4%，在考虑经济运行的情况下，可提高冰蓄冷供冷量，冰蓄冷供冷量占比每提高 10%，就可降低 4%的供冷用电费用。

2018 年地源热泵系统供冷量占总供冷量的 73%，较 2017 年下降 12 个百分点，2018 年供冷季可再生能源占比较 2017 年下降 8 个百分点。

从绿色与经济运行考虑，在地源热泵系统供冷



(a) 2016年供冷　(b) 2017年供冷　(c) 2018年供冷

图 7　2016-2018 年供冷

量充足的情况下要优先使用地源热泵系统进行供冷，其次运行冰蓄冷系统，基载机组只能作为备用。

综合三年来园区供冷运行数据，园区三年平均单位供冷量用电费用比常规中央空调与商用分体空调的成本都要低，经济效益良好，如图 8、图 9 所示。主要是因为园区采用综合能源系统进行供冷，综合三年平均单位供冷量用电费用仅为 0.6 元/RTh。

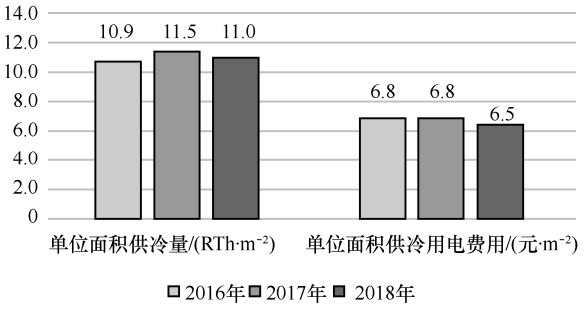


图 8　单位面积供冷量和用电费用

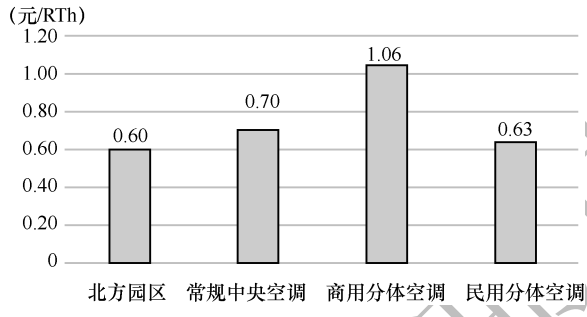


图 9　单位供冷量用电费用

4.3　园区供热量、供热用电量、与供热用电费用统计与分析

园区蓄热电锅炉的供热用电成本要远高于地源热泵供热用电成本，如图 10 所示。因为园区地源热泵供热用电成本为 61.9 元/GJ，虽然蓄热电锅炉供热是使用低谷电价（园区低谷电价 0.451 6 元/kWh），但是蓄热电锅炉的能效仅为 0.95 左右，所以即使蓄热电锅炉使用的是低谷电价，但蓄热电锅炉的供热用电成本还是高于地源热泵。

供热量、用电量与用电费用如图 11 所示，由图可知，2017 年供热量最低，2016 年供热量最高。2018 年供热量较 2017 年上升 13.28%，2018 年供热用电费用较 2017 年上升 21.48%，供热用电费用的增加与供热量不成正比，供热用电费用上升明显。

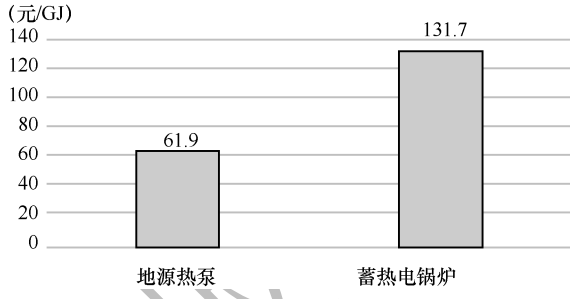


图 10　供热用电成本

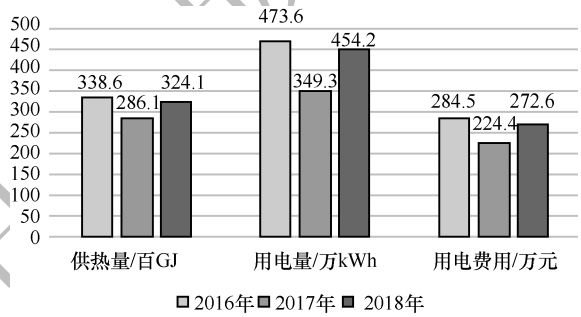
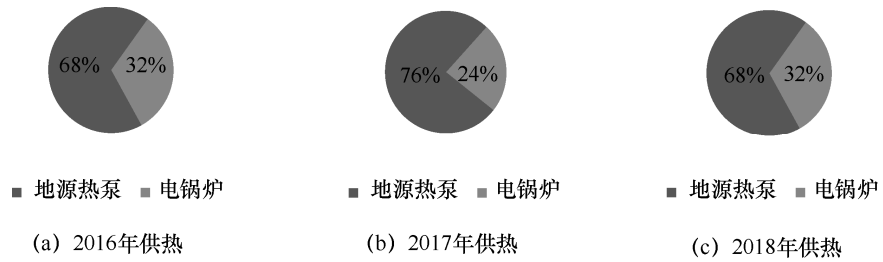


图 11　供热量、用电量与用电费用

因为 2016 年 1 月份−8℃以下天气有 6 天，其中连续 3 天−12℃以下，有 2 天为−14℃，2016 年 1 月份温度最低；2017 年 1 月份有 1 天是−8℃，其余都在−8℃以上，2017 年 1 月份温度最高；2018 年 1 月份−8℃以下天气有 8 天，其中连续 4 天−10℃以下，最低温度−12℃，2018 年 1 月份天气略高于 2016 年，远低于 2017 年 1 月份天气。

2016—2018 年供热情况如图 12 所示，供热由图 12 可知，2017 年地源热泵产热量占比最高为 76%，电



(a) 2016年供热　(b) 2017年供热　(c) 2018年供热

图 12　2016-2018 年供热

锅炉产热量占比最低为 24%，2018 年电锅炉产热量占比较 2017 年增加 8 个百分点，电锅炉产热占比明显增加，因为蓄热电锅炉的供热用电成本高于地源热泵，所以供热用电费用上升明显。

2016 年和 2018 年蓄热电锅炉供热量占比超过 30%，供热用电费用偏高，在考虑绿色、经济运行的情况下，降低蓄热电锅炉的供热量，蓄热电锅炉的供热量占比每降低 10%，园区供热用电费用就会下降 2.5%，经济效益显著。

单位建筑面积供热量如图 13 所示，由图可知，虽然园区的供热时间要比其他地方多，但园区每年单位建筑面积供热量都要低于标准值，说明园区供热节能效益好。单位面积供热用电费用如图 14 所示。

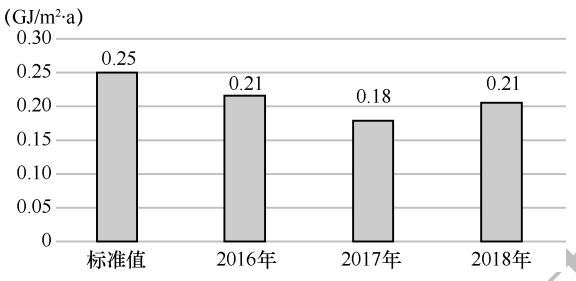


图 13　单位建筑面积供热量

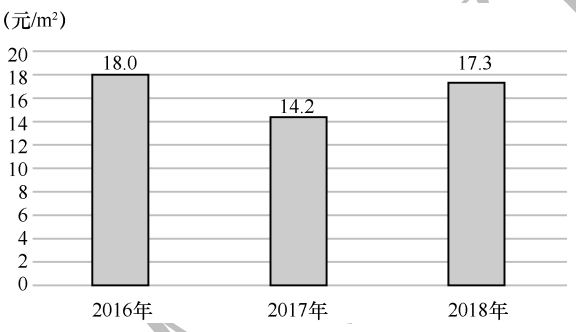


图 14　单位面积供热用电费用

园区采用地源热泵和蓄热电锅炉联合供热，根据 3 年运行数据，其平均单位供热量成本为 82.2 元/GJ，低于燃气供热模式。单位供热量成本如图 15 所示。

4.4　园区供热水量统计与分析

园区供热水量呈逐年上升趋势，2018 年供热水量最高，较 2017 年上升 20.73%，如图 16 所示。分析园区供热水量上升主要是因为生活区住宿人员不断增加，用热水量不断增加。生活区供热水量占总供热水量 60%以上，如图 17 所示，生活区是用热水主要区域，从节能方面考虑，生活区有很大的节能空间。

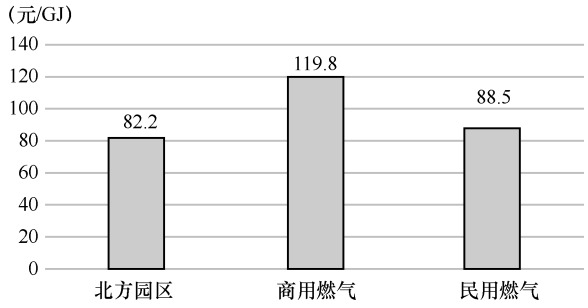


图 15　单位供热量成本

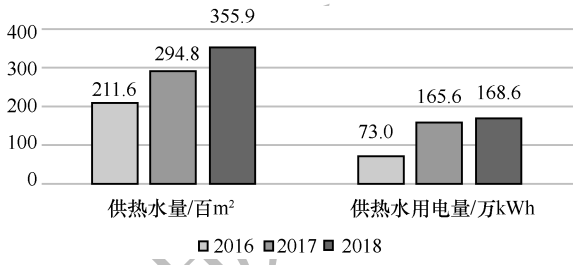
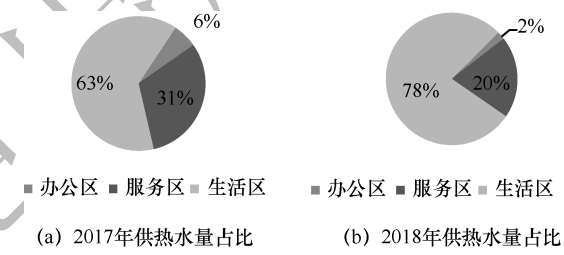


图 16　供热水量和供热水用电量



(a) 2017年供热水量占比　　(b) 2018年供热水量占比

图 17　2017-2018 年供热水量占比

5　局域能源互联网实践结果

国网客服中心南北园区局域能源互联网项目通过“全电、绿色”的节能设计，建成了以电能为中心的“源－网－荷－储”互动型区域能源互联网络，实现了多种能源协调控制和综合能效管理，社会效益显著。该项目年节约标煤 8 248 t，减排二氧化碳 20 558 t、碳粉尘 5 609 t、二氧化硫 619 t、氮氧化物 309 t。同时，根据运行数据，项目实现了 100%电能替代，可再生能源占比年平均值大于 36%，运行最高值 64.17%；能源自给率最高达 56.38%，峰谷电比值维持在 0.75～1.01，削峰填谷效果良好。

项目建设和运行的成功经验，为后续在新城镇、新产业园区等新增用能区域开展局域能源互联网一体化集成供能系统的规划与建设提供了宝贵的实践依据。项目的相关成果已经在天津京津中关村科技城、天津北辰国家产城融合示范区、陕西富平高新技术产

业开发区和河北雄安新市民中心的综合能源规划中进行了推广应用。

6 结束语

建设泛在电力物联网是实现能源转型目标的必要手段，国网客服中心园区级泛在电力物联网——局域能源互联网项目的建设适应能源发展新趋势，注重能源与社会、经济和环境的协调发展，统筹资源的开发、配置与利用，保障能源安全、清洁、高效、可持续供应，实现区域能源供应的复合化、集约化和绿色化。

参考文献：

[1] 别朝红, 王旭, 胡源. 能源互联网规划研究综述及展望[J]. 中国电机工程报, 2017, 37(22): 6445-6446.

[2] 杨东升, 王道浩, 周博文, 等. 泛在电力物联网的关键技术与应用前景[J]. 发电技术, 2019, 40(2): 107-112.

[3] 曾鸣, 杨雍琦, 刘敦楠, 等. 能源互联网“源-网-荷-储”协调优化运营模式及关键技术[J]. 电网技术, 2016(1): 114-124.

[4] 李思维, 李树泉. 一种以电能为中心的绿色复合型能源网设计[J] 中国电力, 2015, 48(11): 117.

人民邮电出版社

园区级供电服务中心用能策略

魏鑫，刘冲，黄嘉浩，张治刚
（国网信息通信产业集团北京国电通网络技术有限公司，北京 100070）

摘　要：基于北京地区气候、地理条件，针对北京地区的园区级供电服务中心的用能策略开展研究。综合运用屋顶光伏发电、市电、电储能和相变蓄冷等设施，结合北京市峰谷电价时段和非居民销售电价表，分析园区级供电服务中心在不同时期的用能策略，为促进园区清洁能源消纳、重要设备安全稳定运行、助力电网“削峰填谷”提供新思路。

关键词：园区级供电；用能策略；削峰填谷

1　引言

园区供电服务中心主要负责工业园区配售电市场开拓、客户用电咨询、有序用电、优质服务[1]，客户工程跟踪服务、协调做好过程管控和服务、配合开展电网前期规划、电力设施建设等工作，全力保障园区入驻企业用电需求，积极促进园区经济有序健康发展。园区供电服务中心的设立，有助于搭建政府、供电企业、入园企业“三方”互通的桥梁，为园区入驻企业提供优质、高效、全方位服务[2]。

北京地区大部分园区不适合风力发电[3]，但比较适合光伏发电[4]。这些园区通常情况下有开阔、平整的屋顶，厂房间距大，不存在遮挡，分布式光伏发电正好迎合了园区需求。对于园区，安装光伏发电可以把闲置的资源再度利用，优化资源配置[5]；可以降低园区碳排放，缓解园区用电负荷；可以经济创收。企业通过光伏发电获得国家给予的补贴[6]，同时还可以节省电费。大容量储能技术的应用打破了电力供需实时平衡的限制，电储能设备的应用可有效降低昼夜峰谷差、提升电网稳定性和电能质量水平[7]，促进新能源并网。

基于北京地区的客观情况（冷暖供应时间、峰谷电价时段、非居民销售电价表），在园区级供电服务中心综合运用屋顶光伏发电、市电、电储能和相变蓄冷等设施，为园区级供电服务中心提供更加绿色、稳定、经济的运行，制定一年内不同时期的更为高效的用能策略。

2　北京市客观情况

2.1　北京市供冷、供暖时间

北京市供冷季：5 月 15 日到 9 月 15 日，8:00-18:00。

北京市供暖季：11 月 15 日至次年 3 月 15 日。

2.2　北京市峰谷电价时段划分

高峰时段 10:00−15:00；18:00−21:00，平段 7:00−10:00；15:00−18:00；21:00−23:00，低谷时段 23:00−7：00；夏季尖峰时段 7−8 月 11:00−13:00 和 16:00−17:00。

2.3　北京市城区非居民销售电价表

2019 年 3 月 29 日，北京市发展和改革委员会根据国家发展改革委《关于电网企业增值税税率调整相应降低一般工商业电价的通知》（发改价格〔2019〕559 号）要求，经北京市政府同意，颁布了北京市非居民销售电价见表 1。

3　园区供电服务中心负荷分析

一般情况园区供电服务中心用电主要包括：中央空调（空气源热泵、相变蓄冷、配套循环泵）用电、充电桩用电、办公用电、机房用电、照明用电等。为方便后续分析，这里假设园区供电服务中心所用空气源热泵用电负荷约 50 kW，相变蓄冷及配套循环泵用电负荷约 10 kW，2 台充电桩用电负荷约 15 kW，办公、机房和照明的用电负荷约 30 kW，经测算，园区供电服务中心最大负荷约 105 kW。

水利水电出版社

表 1　北京市城六区非居民销售电价

用电分类	电压等级	电度电价/（元 • kWh^{-1}）				最大需量/	变压器容量/
		尖峰	高峰	平段	低谷	（元 •（kW • 月）$^{-1}$）	（元 •（kV • 月）$^{-1}$）
一般工商业	不满 1 kV	1.466 0	1.336 7	0.811 0	0.311 3		
	1～10 kV	1.443 0	1.314 7	0.796 0	0.302 3		
	20 kV	1.436 0	1.307 7	0.789 0	0.295 3		
	35 kV	1.428 0	1.299 7	0.781 0	0.287 3		
	110 kV	1.413 0	1.284 7	0.766 0	0.272 3		
	220 kV 及以上	1.398 0	1.269 7	0.751 0	0.257 3		
大工业用电	1～10 kV	1.076 1	0.986 4	0.677 0	0.376 6	48	32
	20 kV	1.061 1	0.972 4	0.667 0	0.370 6	48	32
	35 kV	1.045 1	0.958 4	0.657 0	0.364 6	48	32
	110 kV	1.018 1	0.933 4	0.637 0	0.349 6	48	32
	220 kV 及以上	0.995 1	0.910 4	0.617 0	0.331 6	48	32
农业生产用电	不满 1 kV		0.929 2	0.625 5	0.337 8		
	1～10 kV		0.914 2	0.610 5	0.321 8		
	20 kV		0.906 2	0.603 5	0.315 8		
	35 kV		0.898 2	0.595 5	0.308 8		

（1）在不考虑光伏、储能且不使用中央空调的情况下，园区供电服务中心用电日负荷曲线如图 1 所示。

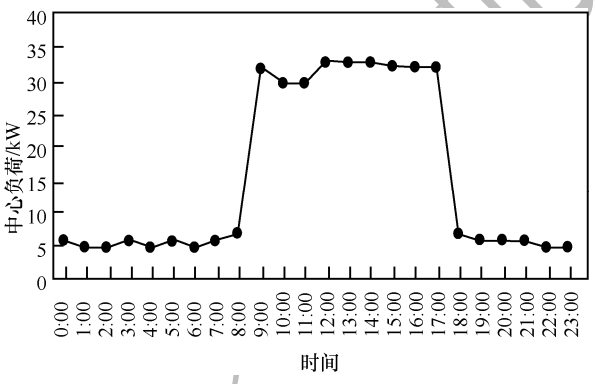


图 1　不使用中央空调的情况下用户负荷曲线

从图 1 可看出，园区供电服务中心用电负荷从早 08:00 开始上升，09:00 负荷上升到 32 kW 左右，从早 09:00-17:00 维持在 30~35 kW 之间，17:00 用电负荷迅速下降，从 18:00 以后用电负荷处于较低水平。

（2）在不考虑光伏、储能，但正常使用中央空调的情况下，首钢冬奥供电服务中心日负荷曲线如图 2 所示。

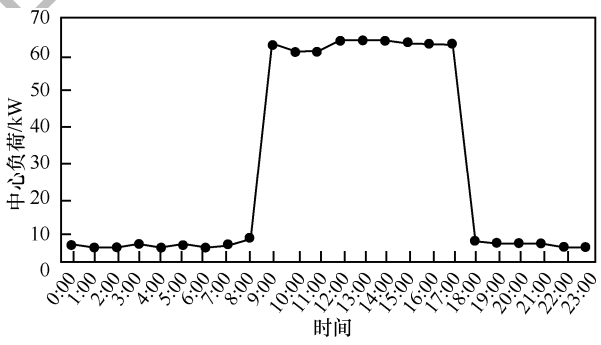


图 2　正常使用中央空调的情况下用户负荷曲线

对比图 2 和图 1，可以看出园区供电服务中心在正常使用中央空调时的用电负荷曲线与不使用中央空调时用电负荷曲线的趋势大体相当，区别在于高峰负荷维持在 60~65 kW，比不使用空调时负荷高出约一倍。

4　用能策略

园区供电服务中心用能策略主要从供冷季工作日、供暖季工作日和其他时期 3 个大的时间段展开论述，其中供冷季是从当年 5 月 15 日到当年 9 月 15 日，

供暖季是从当年 11 月 15 日至次年 3 月 15 日，其他时期是全年除了供冷季工作日和供暖季工作日以外的时期，主要包括其他时期工作日和其他时期节假日。其中，其他时期节假日包括：A 类其他时期节假日（周六、周日）、B 类其他时期节假日（法定小长假：元旦、清明节、劳动节、端午节、中秋节）；C 类其他时期节假日（较长法定假期：春节、国庆节）。

4.1 供冷季工作日用能策略

在供冷季（5 月 15 日到 9 月 15 日），充分利用电网夜晚低谷电为电储能设备和相变蓄冷设备储存电量和冷量，同时根据白天电网负荷曲线，在电网尖峰时段，参与需求侧响应，自发自用，减少电网出力，从而为电网“削峰填谷”。园区供电服务中心供电优先利用屋顶光伏发电系统所发电能，在不能满足中心用电的情况下其余电能由储能设备和市电供给，优先使用电储能设备中的电能，在电储能设备中存储电能不能满足中心负荷的情况下才利用市电供给；在屋顶光伏发电系统满足中心用电还有富余情况下富余电能全部储存到电储能设备中。

（1）优先使用光伏所发电能，促进清洁能源消纳

从图 2 可以看出园区供电服务中心在正常使用中央空调的情况下用电高峰负荷约为 60~65 kW。建议安装屋顶光伏发电系统装机容量 60 kW，供冷季光伏发电效果较好，屋顶光伏发电系统实际日发电曲线如图 3 所示。屋顶光伏发电从早 6 点开始上升至 11 点达到最大 60 kW，之后逐渐下降，至 19 点输出功率下降为 0。通过观察和对比图 2、图 3，可以发现：园区供电服务中心负荷主要集中在每天的 8:00−18：00，而屋顶光伏发电也主要集中在 6:00−19：00，光伏发电与用户负荷具有很强的互补性。

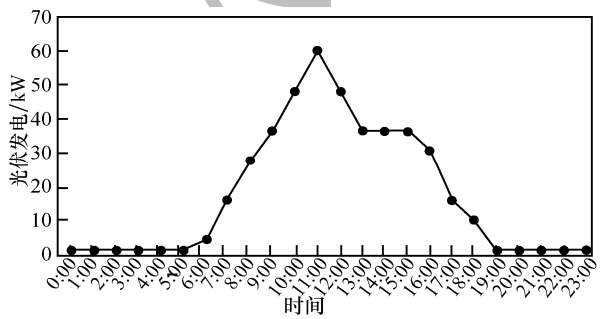


图 3　供冷季屋顶光伏发电日曲线

（2）参与需求响应，促进电网“削峰填谷”

利用园区供电服务中心的屋顶光伏、电储能、相变蓄冷等设备，在夜晚电网低谷电时供电储能设备和相变蓄冷设备储存电量和冷量，同时根据白天电网负荷曲线，在电网尖峰时段，参与需求响应，自发自用，减少电网出力，从而促进电网“削峰填谷”。

在充分考虑电网负荷承载力和夏季尖峰电价情况下，具体实施策略如下。

• 中央空调

23:00−7：00 ，在电网负荷低谷期，空气源热泵进行制冷并存储到相变蓄冷设备中，相变蓄冷设备需要约 6 h，蓄满冷量，蓄满后空气源热泵停机；7:00−10:00，未处于用电负荷高峰期，空调系统由空气源热泵释放冷量；10:00−13：00，属于电网负荷高峰期，中央空调由相变蓄冷设备释放 3 个小时冷量；13:00−16:00，利用空气源热泵制冷；16：00−17：00 由相变蓄冷释放冷量，17：00 时相变蓄冷设备已释放完毕所存冷量；17:00−23:00，工作人员已经下班，关闭中央空调。

• 电储能设备

部署一台 40 kW/80 kWh 电储能设备，储能设备可以有效缓解白天园区供电服务中心对市电供应的依赖。23:00−7:00，在电网负荷低谷期，由市电向储能设备充电，其余时段市电不向储能设备供电；7:00−10:00 储能设备停止工作；10:00−17:00 储能设备与屋顶光伏发电系统协调互补配合，根据用电侧负荷情况调整输出功率，为中心供电；17:00−23:00，储能系统停止工作。

4.2 供暖季工作日用能策略

在供暖季（11 月 15 日至次年 3 月 15 日），充分利用电网夜晚低谷电为电储能设备储存电量，同时根据白天电网负荷曲线，在电网高峰时段参与需求侧响应、自发自用、减少电网出力，促进电网“削峰填谷”。园区供电服务中心供电优先利用屋顶光伏发电系统所发电能，在不能满足中心用电的情况下其余电能由电储能设备和市电供给，优先使用电储能设备中存储的电能，在电储能设备中所存储电能不能满足中心负荷的情况下才利用市电供给；在屋顶光伏发电系统满足中心用电还有富余情况下富余电能全部储存到电储能设备中。

（1）优先使用光伏所发电能，促进清洁能源消纳

屋顶光伏发电系统装机容量 60 kW，供暖季光伏发电效率约为供冷季的 80%，屋顶光伏发电系统实际日发电曲线如图 3 所示。屋顶光伏发电从 6:00 开始上升至 11:00 达到最大约 50 kW，之后逐渐下降，至 19:00

输出功率下降为 0。通过观察和对比图 2、图 4，可以发现：园区供电服务中心负荷主要集中在每天的 8:00−18:00，而屋顶光伏发电也主要集中在 6:00−19:00，光伏发电与用户负荷具有很强的互补性。

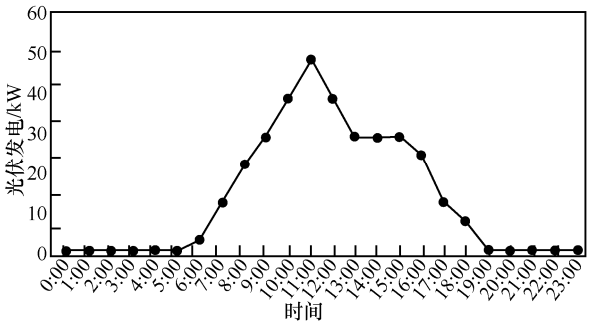


图 4　供暖季屋顶光伏发电日曲线

（2）参与需求响应，促进电网“削峰填谷”

利用园区供电服务中心的屋顶光伏和电储能设备，在夜晚电网低谷电时供电储能设备储存电量，同时根据白天电网负荷曲线，在电网尖峰时段，参与需求响应，自发自用，减少电网出力，从而促进电网“削峰填谷”。

在充分考虑电网负荷承载力和峰谷电价情况下，具体实施策略如下。

- 电储能设备

部署一台 40 kW/80 kWh 电储能设备，储能设备可以有效缓解白天园区供电服务中心对市电供应的依赖。

- 策略

23:00−7：00，在电网负荷低谷期，由市电向储能设备充电，其余时段市电不向储能设备供电；7：00−10：00 储能设备停止工作；10：00−17：00 储能设备与屋顶光伏发电系统协调互补配合，根据用电侧负荷情况调整输出功率，为中心供电；17：00−23：00，储能系统停止工作。

4.3　其他时期用能策略

（1）其他时期工作日用能策略

在其他时期工作日，充分利用电网夜晚低谷电为电储能设备储存电量，同时根据白天电网负荷曲线，在电网高峰时段，参与需求侧响应，自发自用，减少电网出力，从而为电网“削峰填谷”。园区供电服务中心供电优先利用屋顶光伏发电系统所发电能，在不能满足中心用电的情况下其余电能由电储能设备和市电供给，优先使用电储能设备中的电能，在电储能设备中存储电能不能满足中心负荷的情况下才利用市电供给；在屋顶光伏发电系统满足中心用电还有富余情况下富余电能全部储存到电储能设备中。

（2）其他时期节假日用能策略

在其他时期节假日，考虑到首钢冬奥供电服务中心负荷较小可忽略不计，屋顶光伏发电系统所发电能，先存储到电储能设备中，如果电储能设备储满，则多发电能逆变并网。同时根据白天电网负荷曲线，在工作日电网高峰时段，释放电储能设备存储的电能，参与需求侧响应，减少电网出力，从而为电网“削峰填谷”。

5　结束语

针对北京地区的园区级供电服务中心，以时间为维度，按照供冷季工作日、供暖季工作日、其他时期（其他时期工作日、其他时期节假日），合理利用屋顶光伏发电、市电、电储能和相变蓄冷等多种设备，制定了不同时期的用能策略。

在采用上述用能策略后，白天电网负荷高峰时期园区供电服务中心能基本达到自给自足，不为电网增加负荷；夜晚电网负荷低谷时期，园区供电服务中心负荷达到峰值，有效提高了电网电能利用率，助力电网“削峰填谷”，促进了电网经济运行。同时，屋顶光伏和电储能设备的应用，提高了中心用电的应急能力，可保障关键设备稳定运行。

参考文献：

[1] 王远. 浅谈提供优质高效服务的工业园区供电管理——以上饶供电业务探索为例[J]. 低碳世界, 2017(34): 169-170.

[2] 郭小红. 强化管理促发展优质服务创效益——记朔州市区供电支公司客户服务中心[J]. 政府法制, 2009(14): 54-54.

[3] 姚鑫. 中国风力发电装机增长的地区性差异及其原因研究[D]. 北京: 华北电力大学, 2014.

[4] 李轩, 张家安, 吴林林, 等. 可再生能源汇集地区风电与光伏发电的综合容量可信度评估[J]. 太阳能学报, 2017(3):8.

[5] 罗凤章, 米肇丰, 王成山, 等. 并网光伏发电工程的低碳综合效益分析模型[J]. 电力系统自动化, 2014(17).

[6] 李昌. 分布式光伏发电的前景及面临的问题浅析[J]. 太阳能学报, 2014(12): 163-169.

[7] 董旭柱, 郭小龙, 陆志刚. 储能在配电网中应用的实践与思考[J]. 中国电力企业管理, 2015(3): 29-31.

人民邮电出版社

针对终端通信接入网及管理系统的集成优化建设

李文清[1,2]，赵甦[2]，张立[2]，陈鹤[2]，肖云杰[2]
（1. 国网上海电力公司电力科学研究院，上海 200437;
2. 国网上海电力公司信息通信公司，上海 200040）

摘　要：介绍并分析 3 种典型接入网形式以及各自的优缺点，提出终端通信接入网各种典型业务的应用需求。通过实地调研上海地区终端通信接入网发展现状，结合现有信息通信技术，探索出典型建设模式以及针对接入网管理系统的集成优化建设方案，具有推广价值。

关键字：泛在电力物联网；光纤到户；无线专网；无线公网

1　引言

作为推进“三型两网、世界一流”战略目标的重要内容和关键环节的泛在电力物联网建设，将促使相关发、输、变、配电行业及其设备连接起来，充分利用全联接平台系统的协同作用，将产生的信息数据进行互通共享，为电力行业乃至社会各方面提供服务。

终端通信接入网覆盖 10 kV 和 0.4 kV 电网相关站点，包括配电网自动化及需求侧管理、用电信息采集与电能质量监测、精准负荷控制、变压器实时监测、分布式能源控制与管理、汽车充电桩管理以及其他新兴业务等，终端通信接入网整体架构如图 1 所示。

在泛在电力物联网建设大背景下，太阳能、风能等的新能源、电动汽车充电桩、智能家庭、智能路灯等新业务将会不断接入，传统电网控制区域将从输电、变电向配电网、分布式电源和用户侧拓展，控制点数量将呈百万级增长，信息采集点和信息采集量将大幅提升。结合上海地区城市化建设水平高、电力通信网电压等级跨度大、接入网密集程度高的特点，终端通信接入网会发挥越来越重要的作用，因此需要尽快根据不同场景和业务需求来制定优化终端通信接入网建设及管理方案。

2　终端通信接入网典型技术研究

终端通信接入网建设目前处在起步阶段，相应的网络规划、设计、建设、运行、维护等各环节均有待提高。目前适用于终端通信接入网的通信技术主要有光纤通信、无线公网、无线专网、电力线载

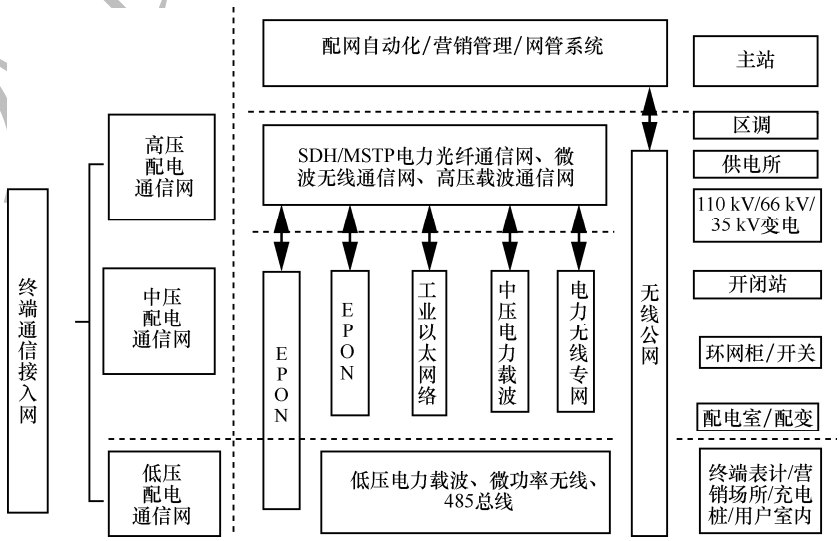


图 1　终端通信接入网整体架构

波通信 4 种，每种通信技术均有其独特的技术性能优势及适用场景。

2.1 无线公网技术

国网公司使用的无线公共网络主要由中国移动、中国电信和中国联通 3 家公司提供运营服务，主要采用 2G 技术 GPRS/CDMA、3G 技术 WCDMA/CDMA2000MHz/TD-SCDMA 和 4G 技术 TD/FDD-LTE 的网络制式。运营商目前主要推广的是 4G 网络，2G 和 3G 网络已经停止扩容。随着三大运营商 5G 网络的大力建设，基于 5G 的无线网络技术在国网公司大力建设泛在电力物联网的大背景下也将逐步进入电力行业应用领域。

无线通信以其建设周期短、投资金额低等特点，使得通信网络在设计、施工、运行和维护方面的工作量得以简化，大大缩短了无线网络建成时间，相比其他通信网络可以快速投入使用。基于无线公网在传输时承载不同类型的业务，为确保通信网络设备的安全可靠，运营商及其他通信单位制定了一系列规范标准，但这些标准的制定基于 APN+VPN 的技术手段实现逻辑隔离，在传输层面无法满足物理上的完全隔离，因此使用无线公网承载相关业务时，需要充分考虑无线通信时的传输问题。

2.2 无线专网技术

在建设泛在电力物联网的大背景下，各类基于智能电网用电侧的，包括电动汽车充换电业务、用电信息采集以及智能用电服务等新型业务将会广泛建设，为满足不同设备灵活接入、即插即用的需要，需要搭建多业务集成使用的灵活终端通信服务平台。

基于 230 MHz 频段的 LTE 无线专网具有全带宽、低时延、抗干扰、覆盖强、低功耗、多样性、全融合的特点，将运维作业实现远程化控制，使其更加适合构建电力综合业务接入网，如图 2 所示。由于无线信号本身的传输特点，恶劣天气和电磁环境的变化会干扰无线电波信号的传输，影响传输信号的性能，用电信息的采集和控制将会受到影响。

通过自主建设无线专网来承载的各类业务，虽然在传输层面与运营商的无线公网实现了物理隔离，但是国网公司仍然应该充分制定面向无线网络的安全管理技术标准，且不宜低于运营商及其他通信单位已制定的规范标准。

2.3 电力光纤到户

光纤到户系统的基本组成包括：光线路终端（OLT）、光网络单元（ONU）和光分布网络（ODN）3 部分，其简化系统模型如图 3 所示。

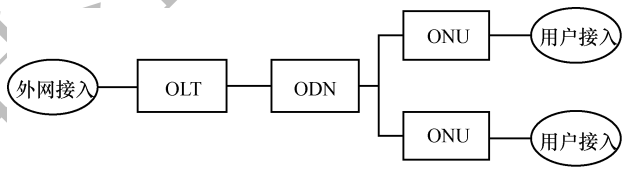


图 3　电力光纤到户 FTTH 系统模型

基于 PON 技术的光纤接入，具有传输容量大、损耗低、抗干扰能力强的优势，在用户相对密集的小

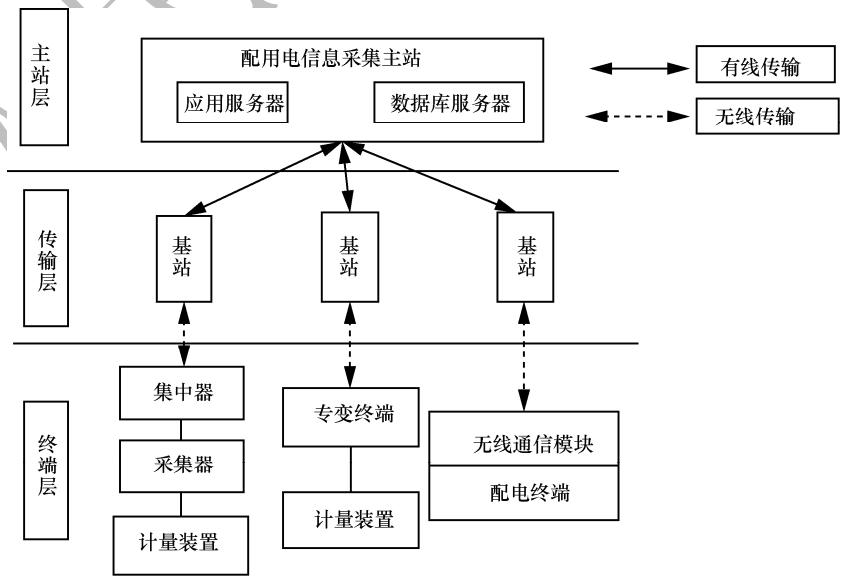


图 2　LTE230 电力无线专网架构

区接入，可以实现接入网的光纤到户。而在用户相对分散的区域使用光纤通信，则会造成高昂的智能电网通信网络建设成本。

3 终端通信接入网业务需求分析

随着全联接智能电网逐渐成为发展趋势，并成为能源互联网的基础，终端通信接入网承载的全覆盖终端通信以及各类海量的用电信息必然会在能源互联网建设中发挥越来越重要的作用。

3.1 信息共享需求

（1）纵向互联信息互通

终端通信接入网综合网管通过纵向加密装置接口与主网系统互联，实现对基础信息与端到端全路由信息的共享，并向省级主网管理信息系统提供业务信息、设备台账等各类信息，实现各级各类信息资源的共享功能，为国网公司大规模建设泛在电力物联网提供信道支撑。

（2）横向集成专业协同

终端通信接入网与配电自动化、分布式能源、营销系统、运营商系统等其他专业管理系统进行横向集成，达到数据资源互联互通，台账信息集成传输，实现全方位互动化专业协同，为建设泛在电力物联网打下坚实基础。

3.2 服务智慧城市管理需求

终端通信接入网对外可作为电力信息的提供者，将电力系统共享型信息数据接入城市管理公共服务平台，通过与市民和政府的三方互动，科学配置城市资源，实现创新低碳的产业经济、绿色友好的城市环境、高效科学的政府治理，最终实现高品质的市民城市生活。在城市建设中，结合城市管理 GPRS 系统，通过电动汽车充电桩信息共享，解决市民寻找停车位问题。在运维管理方面，将市民热线平台与终端通信平台相融合，结合城市管理 GPRS 管理系统，鼓励市民自发拍照上传已损毁电力设备，解决通信电力井盖破损及电力基础设施损坏等问题，产生一种全民监督巡视、远程专家诊断、现场运维抢修的新型电力通信运维方式。

3.3 新兴技术管理集成需求

在大力建设泛在电力物联网的浪潮下，各种新兴技术层出不穷，将这些新兴技术大力推广并应用，最终接入终端通信接入网，与现有系统信息集成会产生协同效应。例如将二维码识别台账资料、动环监控系统、光缆在线测高系统等新技术融合进基于 GIS 的地理信息系统，产生协同作用，达到降低运维压力、提升运行和管理质量的目的。

4 终端通信接入网典型建设模式

在泛在电力物联网的支撑体系建设中，将会有数以亿计的传感器，对各类设备的物理量、电气量、状态量及相应的环境量等进行信息采集；各种“新能源、新业务”大规模的信息通信需求接入，信息采集将呈爆发式增长。这些随业务系统分别建设的，针对终端通信接入网在技术体制、数据模型、接口协议上没有统一的标准，海量通信节点 IP 地址受到限制以及在数据采集频次上趋于双向准实时性的特点，亟需建设互联互通、全方位覆盖的终端通信接入网。

上海地区建设终端通信接入网，落实国网建设“三型两网”的战略目标，在网络架构上宜采用终端直采直控，通信与业务终端融合，统一接口协议和数据模型，终端和平台层能力开放、数据共享的建设方案。利用特大城市电网通信站和通信光缆密度大的优势，上海地区适合大力建设以光通信覆盖、无线公网为主，在特定区域建设电力无线专网的终端通信接入网的建设模式。

（1）光纤覆盖模式

上海中心城区光缆敷设率高，网架结构相对固定，光功率预算充分，为建设 EPON 提供重要的便利条件，此外由于 EPON 结构较为清晰，通信终端成本较低，适合大规模推广，如图 4 所示。

（2）无线专网应用模式

近些年电力无线专网技术得以迅速发展，并且在一些城市逐渐开展试点工作。上海郊区地势平坦，节点分散，在具备条件的地区也可以使用无线专网作为电力通信网络。在 35 kV 变电站内装设无线基站如图 5 所示，通过电力主干光纤资源构建无线专网示意。

无线终端覆盖柱上开关、柱上变、配电室、环网柜、开闭所、故障指示灯等位置。无线专网广泛应用于用电信息采集业务的远程通道，配电网自动化遥测、遥信节点，电动汽车充电桩管理，精准负荷控制以及分布式能源接入，可以实现一网多用。

（3）运营商无线公网的物联网应用模式

电力公司有多类业务正在使用三大运营商提供的无线公网通信服务，包括配电自动化、用电系统信息采集、电动汽车充换电、输变电线路的状态监测、分

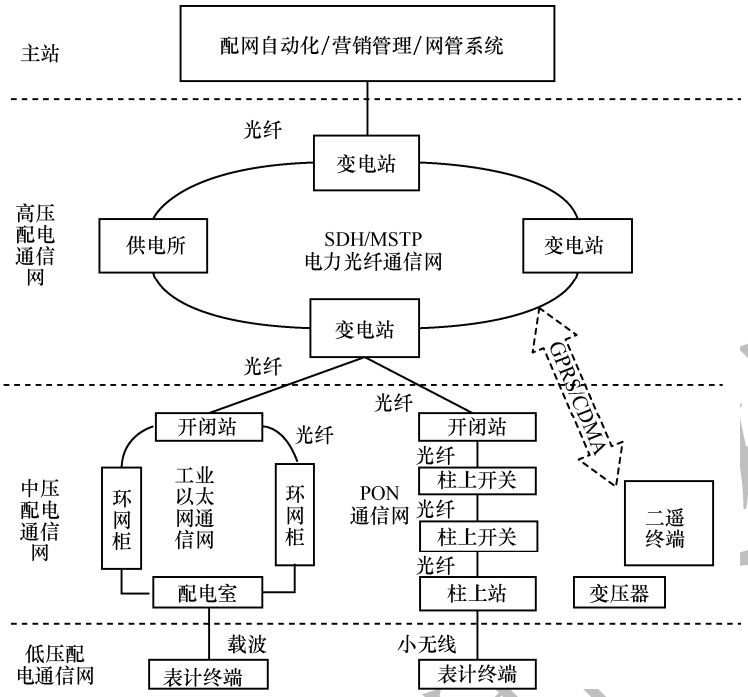


图 4　光纤覆盖模式

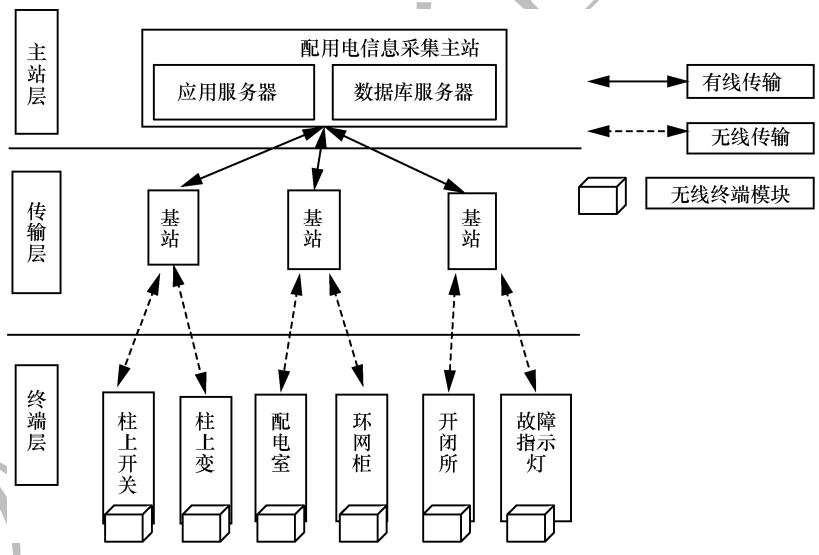


图 5　无线专网应用模式

布式能源等。在整个终端通信接入网的终端规模中，仅以终端的通信方式而论，租用无线公网的方式占比在 90%以上。

运营商网络按 APN、VPN 划分的方式以无线虚拟专网形式接入电网的数据中心，实现企业网与互联网的隔离。除了传统应用领域，无线公网以其全覆盖的优势将会在包括无线监控、无线应急指挥、储能装置、智慧井盖、智能路灯、智能充电站、智能家居等领域服务电网，如图 6 所示。

5　终端通信接入网管理系统的优化建设

终端通信接入网是面向配电、用电数据采集、电力营销、用电互动等环节所建立的通信接入网络，由于各环节设备具有技术体制纷繁不同、设备类型多种多样、业务需求不尽相同且运行环境相对恶劣的特点，从根本上，加大了终端通信接入网的运维和管理难度，

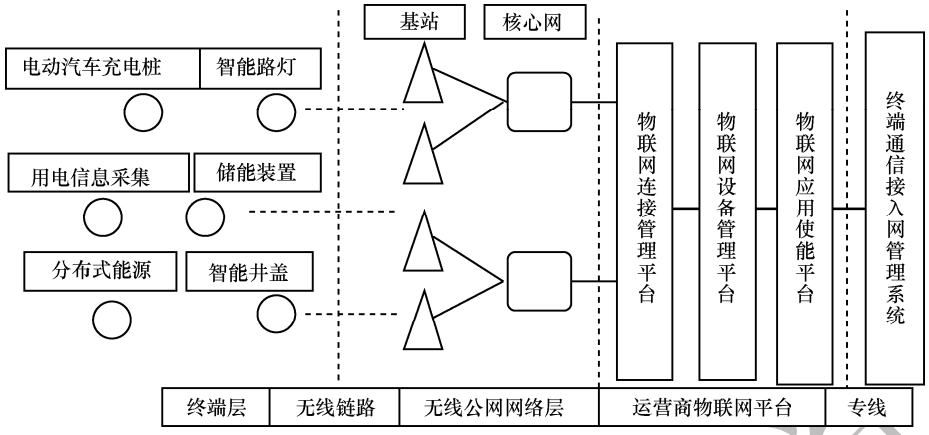


图 6　无线公网平台构架

而目前终端通信接入网的管理手段还主要依靠厂商设备网管，尚未形成统一规范、功能完整的终端通信接入网综合管理系统。

按照国网公司建设泛在电力物联网的目标，要求对内实现“数据一个源、电网一张图、业务一条线”“一网通办、全程透明”，对外广泛连接内外部、上下游资源和需求，终端通信接入网将迎来快速建设和发展的阶段，其管理系统的接入覆盖范围快速扩大、数据处理和存储能力亟需提升、应用功能亟需拓展。

上海地区具有特大城市通信站点和通信光缆密度大、通信网架结构集约化程度高、骨干网和接入网地理区位图重叠面积多的优势，因此将骨干通信网与终端通信接入网管理系统进行纵向互通，通过数据共享、资源共用的方式达到集约建设、共建共享、经济实用的建设目的。无线公网、电力无线专网、EPON、工业以太网等网络横向集成接入具有统一应用接口、统一门户入口的系统，使得配电自动化、分布式能源、营销系统、运营商系统等业务集成接入统一的管理系统，确保了应用的横向互联，达到数据资源互联互通，台账信息集成传输，实现互动化全方位专业协同。

6　结束语

文中通过阐述终端通信接入网 3 种典型技术应用以及各自的组网结构，分析出不同技术各自的优缺点。在国网公司建设泛在电力物联网新型战略目标下，提出终端通信接入网将面临的不同业务需求，并针对不同业务需求展开研究，提出共享终端和平台层能力开放、数据共享的建设方案。最后结合上海地区的区位优势和电网建设现状探索出终端通信接入网典型建设方案以及管理系统的优化建设，为泛在电力物联网的通信网架建设做好专业支撑。

参考文献：

[1] 卢兵, 刘军雨, 于卓智. LTE230 系统在配用电信息采集系统中的应用[J]. 农村电气化, 2019, (3): 9-12.

[2] 廖勤武. 终端通信接入网公共接入平台研究[J]. 电力信息与通信技术, 2016, 14(11): 89-92.

[3] 陈永红, 李建岐, 白杰, 等. 终端通信接入网建设和运行模式探讨[J]. 供用电, 2018, 03: 32-36.

[4] 樊会丛, 赵建华, 邵华, 等. 无线公网 2G/3G 技术在智能电网中的应用[J]. 光通信研究, 2016(4): 75-77.

[5] 李叶, 张琳, 杨凯, 等. 电力无线通信专网的研究与应用[J]. 通讯世界, 2019(2): 128-129.

人民邮电出版社

智慧安防监控系统与综合管理平台在抽水蓄能电站的设计与实现

郑凤柱，马明明，刘宗，王艳如
（北京国电通网络技术有限公司，安徽 北京 100070）

摘　要：国家电网公司提出全面推进“三型两网”建设，加快实现具备全球竞争力世界一流能源互联网企业的战略部署，是国家电网公司在网络强国战略的具体实践，是构建泛在电力物联网实现“三型两网、世界一流”战略目标的核心任务。智慧安监作为泛在电力物联网的典型集成系统，是建设“三型两网”不可缺少的组成部分。因此在抽水蓄能电站工程项目开始前，主要对智慧安监系统进行详细设计，建立抽水蓄能电站基建期作业现场的监控和防范体系，有效弥补传统方法和技术在监管中的缺陷，变传统“监督”为智慧“监控”，同时，安全生产监督管理也将引入新的理念，真正体现安全第一、预防为主、综合管理。

关键词：智慧安防；智能分析；抽水蓄能；人脸识别；联动报警；移动检测

1　引言

随着我国经济、社会的快速发展，电力负荷迅速增长，峰谷缺口不断增大，用户对供电安全质量的期望也越来越高。抽水蓄能电站是电网系统的稳定器，其运行状况直接影响电网的安全稳定运行，对峰谷调节、储能、发电等起着重要作用。“十三五”期间，新开工抽水蓄能电站 6 000 万 kW 左右，2020 年抽水蓄能装机容量 4 000 万 kW，加大了抽水蓄能电站的建设力度，为国家能源革命和电力转型做好准备。因此，抽水蓄能电站的基建安全、生产安全和统一管理显得尤为重要。

建设抽水蓄能电站工程是改造自然、开发利用水资源的重大举措，能为社会带来巨大的经济效益和社会效益。作为国民经济的基础产业之一，水利水电工程异常直接影响自身的经济效益，一旦工程出现问题，将会给社会带来巨大的生命财产损失和人为灾害，严重时甚至会形成社会问题和环境问题。因此，应从社会、环境、经济等全局利益出发，高度重视抽水蓄能工程建设的安全问题。

2　智慧安监系统设计与简介

智慧安监系统主要负责对抽水蓄能电站重要施工区域进行全天候的视频监控，同时能与其他子系统进行联动报警，便于及时掌握各施工区域的施工形象和工程进度，满足对安全管理的要求。除了常规视频监控外，还探讨了智能分析技术，对于重要部位可设置物体移动检测、自动报警、人脸识别、身份验证等。

智慧安监系统由前端采集设备、传输网络和中心控制设备组成，其中，中心控制设备包括存储、中心管理控制和大屏显示 3 部分。本系统网络传输部分统一使用“五系统一中心”设备专网，各类摄像机通过超五类网线统一连接到就近的网络设备箱。为保障抽水蓄能电站视频安保监控图像的稳定性，根据“五系统一中心”建设导则要求，本系统全部使用有线网络传输方案。

在智慧安监系统设计中，最重要的部分是数据存储，它为后期调用视频数据提供保障，也为抽水蓄能电站视频监控的高可靠、高性能、高可扩展性、易管理等多方面需求而量身设计，以确保设计的可行性、可操作性、可维护性以及未来的扩展需求。

3　智慧安监系统功能与实现

智慧安监系统包括视频监控、人脸采集、设备巡检三大部分，可实现远程监控、人脸检测、数据分析、数据管理、联动控制等功能。

3.1　视频监控

视频监控系统通过管理中心的图像显示系统进行

人民邮电出版社

切换、选择，显示在大屏幕上。实现以下功能。

（1）视频图像播放

能播放现有的视频数据压缩格式，能在管理中心的大屏幕和 PC 终端上显示，为抽水蓄能电站的基建期的实时掌控提供准确无误的保障。

（2）视频源选择

可在系统的电子地图上选择需要调用查看的视频源，方便地查看相应的视频信息。可通过配置的距阵键盘对图像进行实时自由的选择。

（3）监控探头调整控制

能实现对监控探头的调整控制。可以通过调整监控探头，实现视频图像的放大、缩小，还可以实现监控探头的方向调整。

3.2 图像传输

图像传输可通过以太网接口实现远程视频传输，采用超五类网线、光纤等作为传输介质。系统采用标准的 TCP/IP 协议，支持跨网段、有路由器的远程视频监控环境。电站内部局域网中的授权用户可通过系统软件远程调用视频监控系统的监控图像，不同的监控用户可根据自己的监控需求灵活切换到任意一个监控点位。

网络用户通过编解码器、数字矩阵、电子地图可以实时远程监控任意摄像机，并可以控制任意摄像机光圈、焦点的旋转。

系统具有视频动态检测功能，可对每一个摄像机实现动态图像检测。每路视频动态检测可划分为多个区域，可以自行设置检测区域，区域的灵敏度可自定义。

3.3 人脸检测

系统具有视频动态检测功能，支持在重要场所选择智能分析摄像机实现图像智能检测。智能检测模式包括围界跨越防范、快速人脸识别通过、物体移走、物品丢弃、人员计数等。

（1）人脸捕捉与跟踪

人脸捕捉是指在图像或视频流的帧中检测人像并将人像从背景分离，自动将其保存。

采集模块使用摄像机抓取监控视频，根据人脸检测算法和人脸质量评估算法对抓取的视频进行人脸检测，获取人脸图像，提取人脸图像的特征，并与数据库中的人脸数据比较面部特征，以获得类似值，将值与预设阈值进行比较，以确定面部是否在数据库中。

数据管理模块接收到人脸比较信息，并将这些信息存储在日志中。将预警信息用二级算法提取图像特征，并利用前端系统返回的 ID 从数据库中找出其人脸特征，得到了一组相似的值，并与预先设定的阈值进行了比较，以决定它是否通过。如果是本单位施工人员，则将对比结果（包括人脸图像、相似值超过阈值的所有身份证照、身份信息、相似值）发送到安全管理平台上，并储存对比日志进行考勤。

人像跟踪是指使用人像捕捉技术，当指定的人像在摄像机范围内移动时，自动跟踪它。

在进场交通洞等人员集中区域布设人脸识别摄像机，支持双向监控，提前将施工人员人脸信息录入库中，通过管理手段要求施工人员列队，脱帽进入隧洞，利用人脸识别摄像机对进场施工人员进行分析比对，使施工人员快速通过，并上报考勤人数，形成日志。

（2）人脸识别计算

人脸识别分为核实式和搜索式 2 种对比计算模式。核实式是对指将捕获得到的人像或是指定的人像与数据库中已登记的某一对像作对比核实确定其是否为同一人。搜索式的对比是指从数据库中已登记的所有人像中搜索查找是否有指定的人像存在。

（3）人脸的建模与检索

对已注册入库的图像数据进行建模，提取人脸特征，并将人脸模板保存到数据库中。在进行人脸搜索时，会对指定的人脸进行建模，并与数据库中的所有模板进行比较，最终根据相似值列出最相似的人物列表。

因此，数据已成为提高人脸识别算法性能的关键因素。在低误判条件下，许多应用越来越重视识别性能。例如，人脸支付需要控制 0.000 01 内的错误接受率，因此未来的算法改进也将集中于提高低误判下的识别率。对于安全监控，可能需要将其控制在 0.000 000 01 以内（几十万人注册库）。人脸识别技术在安全领域更具挑战性。

随着深度学习的演进，基于深度学习的人脸识别将取得突破性的进展。它需要越来越多的数据和样本，重复训练的次数越多，就越容易捕捉到准确的结果并给出准确的答案。因此，当一套人脸识别系统全面引入深度学习算法后，它几乎完美地解决了以往长期变化中的各种问题。

3.4 联动控制

通过系统后台实现与各区域门禁及人员定位系统

人民邮电出版社

的联动功能，在有人员出入刷卡，或接收到门禁及人员定位管理系统的报警信号时，能自动将画面切换至人员活动区域或报警区域。

能通过系统后台实现与应急广播和通信系统的联动功能，在有人员应急呼叫或报警时，能自动将画面切换至人员活动区域或报警区域。

3.5 报警功能

当出现设备故障时，系统立即发出报警信息。当检测到电站内重要区域有人员活动或其他危险时，系统立即将该监控区域的监控画面切换至视频监控终端显示器上，并发出预警信号，待值班人员确定后方可解除。

报警显示信息可在当前画面上显示报警语句（包括报警发生的时间、对象名称、性质等），显示颜色可随报警信息类别而改变。若当前画面具有该报警对象，则该对象标志（或参数）可闪光和改变颜色。闪光信号可在值班人员确定后方可解除。

对于任何确认的误报警，值班人员可以在权限许可范围内，请求退出该报警点。根据对报警事件的应急反应程度，提供多层次的报警，如紧急：需要立即处理的极为紧急的错误；警戒：需要立即纠正的警报；关键错误：需要尽快处理；报警错误：不是关键警报；警告：系统操作中有某种错误。

4 智慧安监系统的特点

4.1 统一的数据中心

智慧安监系统构建统一的数据中心。通过统一的数据管理，可以建立统一的数据标准，方便数据的存储、共享、交换和挖掘。

4.2 统一的支撑平台

统一的支撑平台采用先进的大数据技术进行构建和设计。与传统的分散项目建设模式不同，统一支撑平台实现了集约化建设模式，避免了各个部门或企业的个别建设和应用系统的开发和部署，可以在同一支撑平台上构建自己的业务系统，既不相互干扰，又可以共享和交换数据。可以支持多种访问和使用方式。

4.3 统一的电子地图

整个系统采用统一的电子地图作为各种可视化业务数据的展示和分析手段，所有的业务数据都与电子地图无缝连接。通过电子地图，可以直接查询相关的业务数据详细信息、危险信息等。

4.4 统一的应用系统

在统一支撑平台的基础上，实现各类企业业务系统结构和运行的统一，实现系统互联互通和数据共享，并避免信息孤岛和重复投资。

5 在抽水蓄能电站中的应用

抽水蓄能电站建设存在施工区域分布广、安全监控全覆盖难、施工周期长等工程建设特点，使得安全风险监控难以全面覆盖，特别是重要施工区域现场质量、安全、进度管理受到各种复杂条件限制，目前仍采用传统管理方式，缺乏智能化管控手段，使得电站内部分现场施工很难实现精细化管控，一旦出现事故，不能提供数据调查。

5.1 移动跟踪

针对抽水蓄能电站存在的众多安全隐患，做了深入的分析和考察，为了有效地维护抽水蓄能电站现场秩序和安全，保障基建期工作顺利进行以及为工作人员营造安全的环境，特别地在抽水蓄能电站的主要地点进行移动目标跟踪部控，以实现对施工现场重点区域和场所进行高安全级别的监控和管控。

智能移动跟踪监控主要对抽水蓄能电站的重点部位和重点区域进行主动化，智能化的实时监控，在施工现场，人员众多，各种动作的安全隐患大，容易发生意外事件。可以部署智能跟踪摄像机，监控施工现场的全景和人员运动的细节，可以实时掌控施工现场的安全，对异常事件做到第一时间发现、有效应对和避免安全事件的发生。在抽水蓄能电站门口，出入的人员汽车众多，场面混乱，不法人员借早晚出入高峰乘虚而入的情况从事犯罪活动的事件常有发生，部署智能跟踪摄像机对校工程现场有效监控，能看清场景及细节，出现异常情况实时作出应对，可预防安全治安事件发生。

5.2 人脸识别

随着视频监控发展，生物识别技术也得到了大力推广。计算机人脸识别是生物特征识别中的一个重要技术，是机器视觉和模式识别领域的重中之重，同时它在抽水蓄能电站中具有较为广泛的应用意义。

利用安装在抽水蓄能电站各个关键区域的摄像机获取工作人员的脸部图像。智慧安监系统对获取到的图像进行必要的预处理，将获取的人脸图像存入人脸库并与已存入的数据进行对比，对结果为此人脸图像进行数据计算，超过合理值则系统锁定此人，系统发出警报，需通过人工复合后才能解除禁止，从而有效

人民邮电出版社

防止重点区域内安全问题的发生。

5.3 智能安全帽

智能安全帽包括监督工人的作业行为，提升人员和工程的安全性；扫描各种角度、距离，并智能的提示，提高工作的效率；更由于设备的集成，降低了设备的成本。

智能安全帽是基建期安全设备的组成部分，将基建期智能安监系统中的内容充分利用，发挥工程建设管理最大化效果，实现智能安全帽与基建智能安监系统两者间的无缝对接，还要具备向全国推广的能力，实现抽水蓄能电站施工安全的全面监控，进一步提高工程项目现代化管理能力。

6 结束语

对于电网系统，抽水蓄能电站的安全运行是最重要的。如何掌握抽水蓄能电站的实际安全运行状态，在安全事故发生前处理，并在事故发生时进行必要的救援措施，对抽水蓄能电站的安全监测和建设起到了重要的作用，本文从多方面解释了其重要意义。在此基础上，给出了抽水蓄能电站的安全监测系统，最终为抽水蓄能电站的安全购置了一份可靠的保险。

参考文献：

[1] 唐湘茜. 全球抽水蓄能电站发展前景[J]. 水利水电快报, 2014, (3): 13.

[2] 阎正平. 智慧大庆建设目标与路径探析[J]. 大庆社会科学, 2012, (2): 64-65.

[3] 李建东. OA 系统可靠性设计[J]. 计算机安全, 2013(4): 79-82.

[4] 许家尧，孙苑. 开放场景人脸识别系统及其应用[J]. 指挥信息系统与技术, 2014(4): 39-42, 47.

[5] 安然，王辉麟. 人脸识别系统在铁路车站安检区域应用的研究[J]. 铁路计算机应用, 2012(9): 21-24, 29.

[6] 刘鹃. 水文档案信息化建设的一些思考[J]. 黑龙江交通科技, 2013(2): 189-190.

[7] 王忠勇, 赵毅栋, 李雅琼. 车载嵌入式视频监控定位系统[J]. 单片机与嵌入式系统应用, 2013(12): 41-44.

[8] 杨玉敏. 浅谈电网经济运行的节电技术[J]. 科技与企业, 2013(24): 189-190.

[9] 杨玉敏. 浅谈电网经济运行的节电技术[J]. 科技与企业, 2013(24): 189-190.

[10] 邱银国, 张振国, 王小兵. 井巷三维人员定位系统关键技术[J]. 金属矿山, 2014(7): 130-134.

[11] 邱银国, 张振国, 王小兵. 井巷三维人员定位系统关键技术[J]. 金属矿山, 2014(7): 130-134.

[12] 张并锐, 张蔚. 浅议江苏建设工程智慧安监的研究与应用[J]. 中国建设信息化, 2019(2): 75-77.

[13] 曹旭, 阎峻, 温佩佩, 等. 抽水蓄能电站网络建设方案研究[J]. 电气时代, 2018(10): 91-92.

[14] 应丽骏. 抽水蓄能电站安防系统设计探讨[J]. 水利技术监督, 2018(3): 229-232.

[15] 张忠策. 基于本质安全理论的抽水蓄能电站工程建设安全管理体系的应用研究[D]. 广州: 华南理工大学, 2018.

[16] 单鹏珠, 徐洁, 喻洋洋, 等. 西龙池抽水蓄能电站上位机系统国产化改造技术研究[J]. 水电与抽水蓄能, 2017, 3(2): 59-63, 80.

[17] 唐典典. 抽水蓄能电站资产全寿命周期管理评价研究[D]. 北京: 华北电力大学, 2016.

[18] 涂强. 清远抽水蓄能电站安防视频系统特点[J]. 广东水利水电, 2015(7): 64-67.

[19] 李泓泽. 电力系统多元主体间外部性影响机理及补偿机制研[D]. 北京: 华北电力大学, 2013.

[20] 高建伟，何晓亮，马依文. 抽水蓄能电站工控系统安全防护探讨[J]. 水电站机电技术, 2017(9): 63-66.

人民邮电出版社

智慧变电站设备状态识别技术

程华福[1]，闫蓓蕾[1]，马洪波[1]，刘奔[2]，王鹏[1]
（1. 国网信息通信产业集团有限公司北京分公司，北京 100032;
2. 深圳市铁越电气有限公司，广东 深圳 518116）

摘　要：智慧变电站建设立足于服务基层一线班组及各级运维管理人员，按照“突出设备、强化基层、精益管理”的原则，以现代化信息技术为支撑，以保障电网设备安全运行、提高运检效率为目标，实现无人变电站的信息化、自动化、智能化及可视化建设。通过在变电站内部署图像视频监测系统，可实时监测指示灯、开关等设备状态，使运维检修流程更便捷、更安全；从网络结构优化和模型压缩两方面优化 YOLOV3 算法，提高了目标识别的精准度及运算速度，提升了运维检修的可靠性与时效性。

关键词：智慧变电站；视频监测；设备状态；目标识别

1　引言

随着智慧变电站建设的逐步发展，变电站内的智能化水平显著提升，通过图像视频监测技术可自主检测变电设备的运行状态，实现变电站的信息化、自动化、智能化及可视化建设，使运维检修流程更高效、更便捷、更安全[1]。目标检测技术，作为计算机视觉四大任务（分类、定位、检测和分割）之一，主要是寻找图片中感兴趣的目标或区域[2]，并给出每个目标的坐标信息及所属类别。近年来，目标检测算法如雨后春笋般涌现，在算法性能、精度、速度等方面都有所提升，但是由于真实场景中所需检测的目标存在着不同形态及姿态的变化，以及受到光照和遮挡等因素的干扰，目标检测算法需要针对不同场景进行定制化研发。文中介绍一种改进的 YOLOV3 算法，用于对变电站内的仪表类型、开关状态、指示灯状态和压板状态等的识别。

2　YOLOV3 算法

目标检测算法主要分为两大类，精度型算法和速度型算法。其中，精度型算法的特点是识别精度高，但是其运行速度较慢，代表性算法是 Faster RCNN 系列算法；速度型算法的优势是速度快、实时性高，代表性算法有 SSD 和 YOLO 系列算法。YOLO 算法可以在保证一定精度的条件下，使运算速度更快，该算法在工业界使用较为普遍，号称工业界的标杆算法。YOLO 算法经过不断衍生，目前使用较广泛的是 YOLOV1、YOLOV2 和 YOLOV33 个版本，其在运算精度和速度上逐步提升。本文将重点介绍 YOLOV3 算法。

2.1　YOLOV3 算法原理介绍

YOLOV3 算法[3,4]与 Faster RCNN 系列算法及 YOLOV1、YOLOV2 算法相比，其运行效果最好，能够保证在获得较高识别精度的前提下，大幅提高模型推断速度。YOLOV3 算法的网络结构如图 1 所示。

图 1 中 Convolutional Set 主要用于进一步提取 YOLOV3 网络中的有效信息[5]，获取语义信息，从而将提取结果分发给预测分支（3×3 卷积和 1×1 卷积）进行预测，同时将结果进行上采用操作，与其他特征进行融合，实现多尺度检测。

2.2　YOLOV3 算法特点分析

YOLOV3 算法在保持速度优势的前提下，提升了预测精度，尤其在对小物体的识别能力上效果显著。其主要特点分析如下。

（1）分层特征提取

采用 Darknet-53 网络作为特征提取网络，并以 1×1 和 3×3 的卷积核加上残差模块作为一个基本单元，其结构如图 2 所示。

Darknet-53 特征提取网络由若干个 Conv 1×1+Conv 3×3+Res 组成的卷积模块构成，其中，将 8 个上述卷积模块串联起来可用于小目标和中目标的特征提取；将 4 个上述卷积模块串联起来可用于大目标的特征提取，形成‘8’‘8’‘4’。

人民邮电出版社

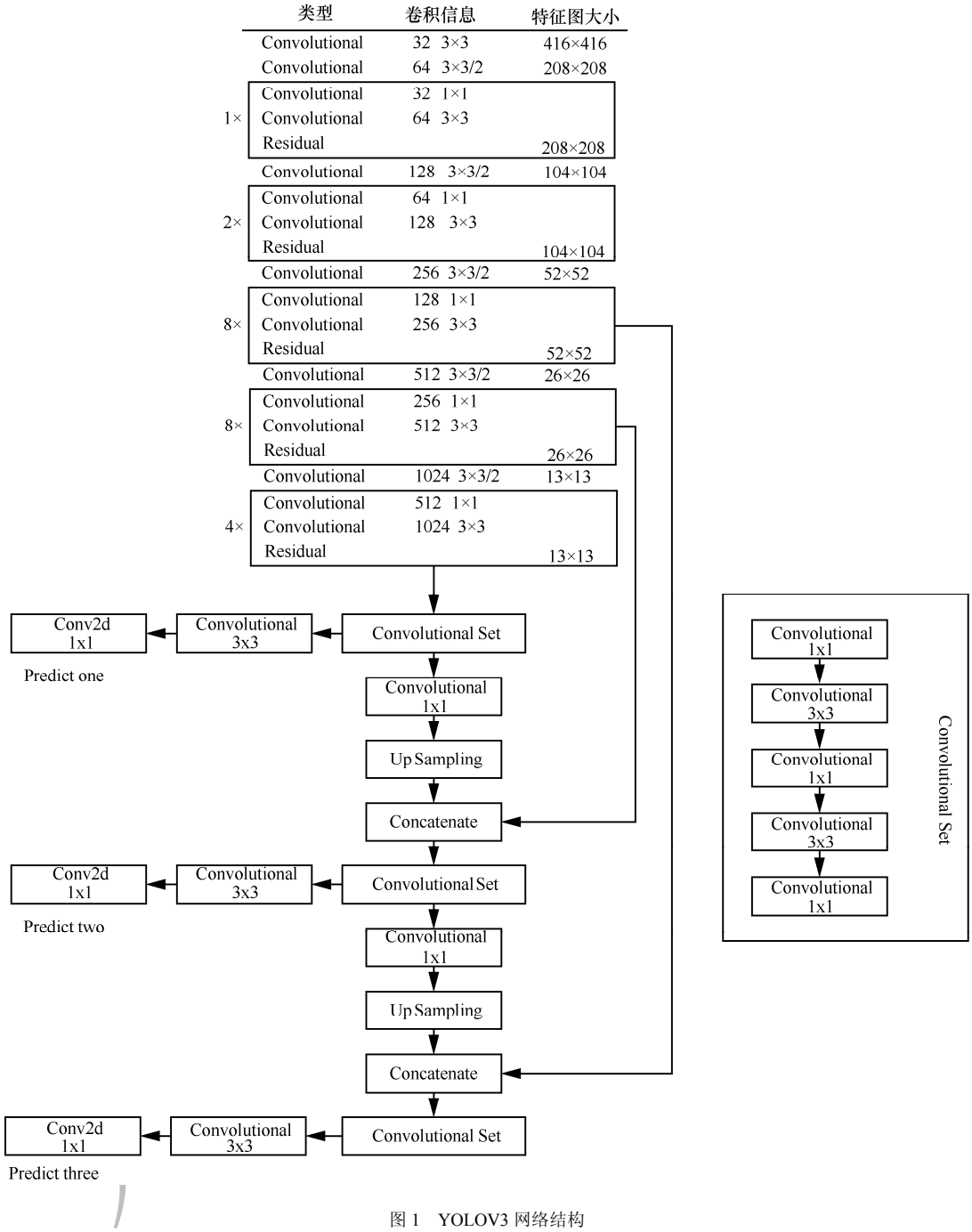


图 1　YOLOV3 网络结构

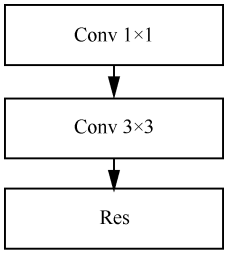


图 2　Darknet-53 网络结构

（2）多尺度检测

YOLOV3 算法通过分层操作及不同层特征融合来实现多尺度检测[6]，基础网络可引出 3 个特征图：13×13×1024 、 26×26×512 、 52×52×256 。 其 中 ，13×13×1024 用于预测比较大的目标；13×13×1024 上采样与 26×26×512 进行特征融合，用于预测中等大小的目标；26×26×512 上采样与 52×52×256 进行特征融合，用于预测比较小的目标。

（3）卷积代替赤化

YOLOV3 算法中利用卷积代替赤化操作，在一定程度上可以减少因赤化操作所造成的信息损失，从而提高精度。

（4）无全连接层

YOLOV3 算法的输出部分使用卷积来代替传统卷积网络中所涉及的全连接，可使网络参数大幅减少，从而提高模型推断速度。

3 算法改进

YOLOV3 算法标准模型是一个通用模型，只能适应于特定场景，并不能适配所有应用场景，所以需要针对不同的应用场景及应用指标对标准的 YOLOV3 算法进行优化，分为纵向优化和横向优化。现选取变电站仪表、开关、指示灯、压板等设备来阐述对 YOLOV3 算法的优化改进方法。

3.1 网络结构优化

网络结构优化属于纵向优化，与网络深度有关。对于复杂场景，需要比较深的网络结构，反之则需要比较浅的网络结构，否则可能会导致过拟合问题，因此要根据识别场景内的环境、光照及识别对象的多样性等复杂因素，对网络进行增删卷积模块。

在智能变电站内，对仪表类型、指示灯状态、开关状态和压板状态等进行识别，根据监测摄像机与被识别设备之间的相对距离，以及设备自身大小等信息可知，被识别目标属于中等目标或大目标，所以需要降低网络中负责大目标特征提取的网络，即减少其卷积模块个数。将标准 YOLOV3 网络进行裁剪，降低其深度，在增强模型泛化能力的同时，减小模型大小，提高模型的推断速度。

3.2 模型压缩

模型压缩属于横向优化，即减小网络模型的宽度。模型压缩主要基于两点：一是网络的计算量主要集中在卷积操作中；二是卷积层中不同卷积对最终识别结果的贡献大小不同。卷积运算会消耗大量计算资源和时间，而适当减少卷积核个数，将间接减少不同层之间卷积核的连接数量。

不同层之间的卷积核是通过权重连接的，每个权重都有一定数值，假设权重值在 0 附近，那么乘积所得的值就会很小，对识别结果造成的影响也会很小。通过卷积核权重的绝对值之和 $\sum|F_{i,j}|$，即 L_1 范数来衡量该卷积核的作用，得到对应每一层卷积中所有卷积核的权重和。删除卷积核的方法有两种：一是将权重和由大到小进行排序，保留前 m 个卷积核；二是随机删除固定个数的卷积核。本文则采用第一种方法，通过删除一些对结果贡献不大的冗余卷积核来防止过拟合影响，同时降低计算量，提高运算速度。

3.3 技术创新点

本文在网络结构优化和模型压缩两方面对算法进行多次试验优化，得到较为完善的网络结构，相对于标准 YOLOV3 网络结构，做出以下调整。

（1）改变特征提取网络结构，将‘1’‘2’‘8’‘8’‘4’变更为‘1’‘2’‘6’‘4’‘4’降低了针对小目标和中目标的特征提取能力以及模型复杂程度，提高了在特定场景下模型的泛化能力，加速了模型处理速度。

（2）只保留 Convolutional Set 模块的 1×1 和 3×3 两类卷积模块，能够降低其复杂程度，对于单一性场景，可在保证精度的前提下降低冗余，减小计算量。

（3）模型压缩优化通过将权重和由大到小排序，保留前 m 个卷积核，删除冗余卷积核，来防止过拟合因素，提高运算速度。

4 试验结果与分析

以变电站设备仪表类型、开关状态、指示灯状态、压板状态和柜头文字识别为例，采用网络结构优化、模型压缩两种方法对 YOLOV3 算法进行优化，得到不同的结果数据。具体见表 1。

选取变电站压板和进线柜两种设备，对其上的压板状态、仪表示数和柜头文字进行识别处理，得到的结果分别如图 3、图 4 所示。其中图 3 可以精准显示压板闭合、断开状态，并自动核算各状态压板的个数；图 4 可以准确识别柜体文字及仪表示数，识别精度高达 90%。

5 结束语

本文在网络结构优化、模型压缩方面对 YOLOV3 算法不断改进，优化了特征提取网络结构，降低其计算量和复杂程度，提高了模型处理及运算速度。选取变电站内压板、仪表等设备状态进行识别处理，识别精度可高达 90%。此图像识别技术为智慧变电站的建设提供了可靠的技术支撑，减少运维人员工作量，保障站内作业安全、可靠开展。

人民邮电出版社

表 1　网络结构优化结果对比

改进说明	改进版本	Precision	Recall	mAP	Speed	Size
原始网络	原版本	0.946	0.993	0.989	17 ms	492.6 MB
	压缩比例 0.2	0.953	0.995	0.990	17 ms	253.3 MB
将‘8’改为‘6’	改进版本一	0.950	0.992	0.980	16 ms	466.3 MB
	压缩比例 0.2	0.948	0.990	0.976	15.7 ms	203.8 MB
修改 ConvoSet	改进版本二	0.936	0.977	0.973	15 ms	382.3 MB
	压缩比例 0.2	0.920	0.970	0.964	15 ms	189.3 MB
降低 predict one 分支分量	改进版本三	0.926	0.972	0.966	13 ms	252.7 MB
	压缩比例 0.2	0.915	0.950	0.940	12 ms	174.8 MB
将‘8’改为‘4’	改进版本四	0.942	0.987	0.984	11.5 ms	197.6 MB
	压缩比例 0.2	0.910	0.940	0.934	11.5 ms	169.3 MB

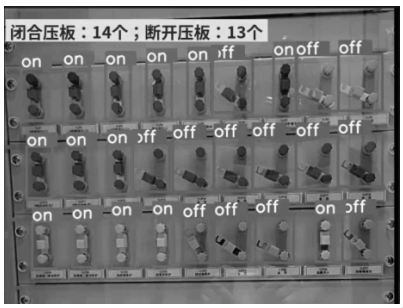


图 3 压板状态识别结果



图 4　进线柜状态识别结果

参考文献：

[1] 国家电网公司. Q/GDW 83—2009 智能变电站技术导则[S]. 2009.

[2] MANOLAKIS D AND SBAW G. Detection algorithm for hyperspectral imaging applications. IEEE Signal Processing Magazine[J], 2002, 19(1): 29-43.

[3] REDMON J, FARHADI A. YOLOv3: An Incremental Improvement [Z]. Computer Vision and Pattern Recognition. 2018.

[4] REDMON J, FARHADI A. YOLO9000: better, faster, stronger [C]//2017 IEEE Conferenceon Computer Vision and Pattern Recognition, Honolulu: IEEE, 2017: 6517-6525[2018-04-01].

[5] 蒋树强, 闵巍庆, 王树徽. 面向智能交互的图像识别技术综述与展望[J]. 计算机研究与发展, 2016, 53(1): 113-122.

[6] SOILLE P. 形态学图像分析原理与应用[M]. 北京：清华大学出版社, 2008.

人民邮电出版社

智慧物联电动自行车充电系统

孙胜宇，蒋月，李琳，庄斌
（北京国电通网络技术有限有公司，北京 100070）

摘　要: 智慧物联电动自行车充电系统打破现有充电方式，为用户提供更加安全、智慧的充电解决方案。系统利用物联网、移动互联网等新一代信息技术，实现对用电设备的智能控制。通过平台数据分析，并与移动客户端或微信小程序对接，实时向用户反馈充电情况，将软件移动支付、信息查看融为一体，为居民提供更优质的用能服务。车棚可选择安装光伏，通过光电互补实现绿色充电和降低用电负荷。通过对电动自行车停放充电车棚的集中控制，实现故障及时发现与定位，保障车棚安全运营。智慧物联电动自行车充电系统的普及，完善居民侧泛在物联网建设，实现居民电动自行车、电网的友好交互，实现电力系统各环节万物互联、人机交互，拓展“智能+”，构建精准用户画像，实现个性化服务，提高电网资产运营效率，保证电动自行车在能源生产消费上的清洁高效。

关键词: 物联网；数据分析；充电系统

1　引言

目前我国电动自行车的使用正处于喷薄发展的阶段。电动自行车不仅为居民生活带来便利，也让居民享受到“高性价比”的生活。电动自行车作为出行的代步工具，与居民的生活紧密相连。同时，电动自行车在社区/停车棚停放、充电的过程中，失火情况屡次发生，造成的人员伤亡和财务损失逐渐增加，引起了社会各界及相关媒体的高度关注，电动自行车的火灾防范预警等相关工作已经成为当前急需解决的问题。2017 年 12 月 29 日，公安部发布的《关于规范电动车停放充电加强火灾防范的通告》提出，有条件的住宅小区、楼院，应当结合实际设置电动自行车集中停放及充电场所。

目前全国范围内其他类型的电动自行车据统计有近 3 亿辆，数量也极为庞大，充电需求日益增加。通过电动自行车充电系统，合理调节电动自行车充电，避免能源浪费，降低电网负荷，通过接入新能源，提高清洁能源消纳。

文中针对智慧物联电动自行车充电系统开展了以下研究。

- 解决小区电动自行车用户私下拉线充电问题；
- 电流过载保护系数增加，大大降低充电事故发生概率；
- 用电采集、充电预约、充电查询、移动支付；
- 故障实时定位，事故自动报警；
- 光伏供能，降低电网负荷；
- 降低事故发生概率，保障居民安全、舒适、智慧社区生活。

2　系统架构

2.1　系统概述

基于智能配电柜的电动自行车充电系统集合新一代物联网技术，构建电动自行车智能充电系统。系统整体由智能墙插、智能配电柜以及运营管控平台构成，提供智能化、数字化电动自行车智能充电服务，通过智能插座用电采集和其他参数采集，运用无线通信技术与智能配电柜信息交互，智能配电柜将信息发送给运营管控平台，平台对数据进行实时处理分析，居民通过手机客户端实时查看电动自行车充电信息、用电信息，也可查看和预约车棚充电位。运营管控平台采集多个小区电动自行车充电信息，实现用电可视化，并可精准定位故障位置，向物业中心实时反馈维修信息。智能配电对故障实时预警和报警，时刻保障居民生命财产的安全。用户通过手机客户端进行消费结算，符合社会移动支付潮流，方便用户使用。

基于智能配电柜的电动自行车充电系统可选择采用光伏结合市电供能，通过使用清洁能源，使用户享受低碳生活。光电互补，不止降低了电网负荷，更降低了充电系统能源消耗，从而降低成本、降低用户充

人民邮电出版社

电费用。

2.2 系统整体框架

基于智能配电柜的电动自行车充电系统，整体由设备层、传输层、平台层构成。设备层智能配电柜采集智能插座和光伏信息，通过传输层中 4G、光纤等技术与运营管理平台进行数据交互，智能插座采集电动自行车充电信息，通过 Wi-Fi 传输给智能配电柜。整个系统运用物联网架构，实现系统分布采集、集中管控的效果。

智慧物联电动自行车充电系统架构如图 1 所示。

3 智能终端

3.1 智能配电柜

电动自行车充电智能配电柜是配电箱和电动自行车充电柜相结合的产品，包括带漏电保护的总空气开关、电源模块、电压电流互感器、综合故障及用电监控模块、开关控制模块、总控模块。综合故障及用电监控模块是包括电量检测、漏电检测、过载检测、过流检测、过热检测、短路故障及电弧故障等快速检测于一体的模块。智能配电柜实现电动自行车充电用电量总路计量、分路计量、远程总路调控、远程分路调控等功能，并将计量数据和监测信息近乎实时上传到充电运营控制平台，第一时间通知用户，传统配电箱与充电柜有机结合，实现电动自行车智能充电管理。

3.2 智能插座

智能插座集信息技术、控制技术和网络技术为一体，实现电源的电压、电流、频率及工作环境温度的监测和显示；实现智能工作状态与普通工作状态的功能切换；智能实现数字功率的分配与负载准入；智能实现过流、过压报警保护；智能实现电动自行车充电信息的采集及监控；具备网络功能。智能插座由电源系统、监测系统、控制系统、通信系统和显示系统组成，通过与智能配电柜无线信号传输，实时上传数据，与智能配电柜用电互动，实现对电动自行车充电信息的采集与控制。

智能插座默认采取 Wi-Fi 与智能配电柜进行数据交互，在不影响数据传输准确性的情况下最大可扩展 32 路。还提供电力线传输智能插座定制款，此款在布线、扩展性、数据安全等方面更加优越。

智能插座带有唯一的二维码，通过手机客户端扫码，进入充电页面，在此页面进行充电开启、充电查询和支付等操作。智能插座具有防伪功能，用户在扫二维码支付之前，提供明确信号，防止假冒收钱码造成用户支付损失。每个智能插座，能够单独设定计价规则，能适应各种用电场景进行计费用电服务。

智能插座采用标准 86 盒外观设计，方便车棚的安装使用，充电运营控制平台远程控制插座的开闭状态，查看设备当前工作状态，并可设定其定时工作时间。

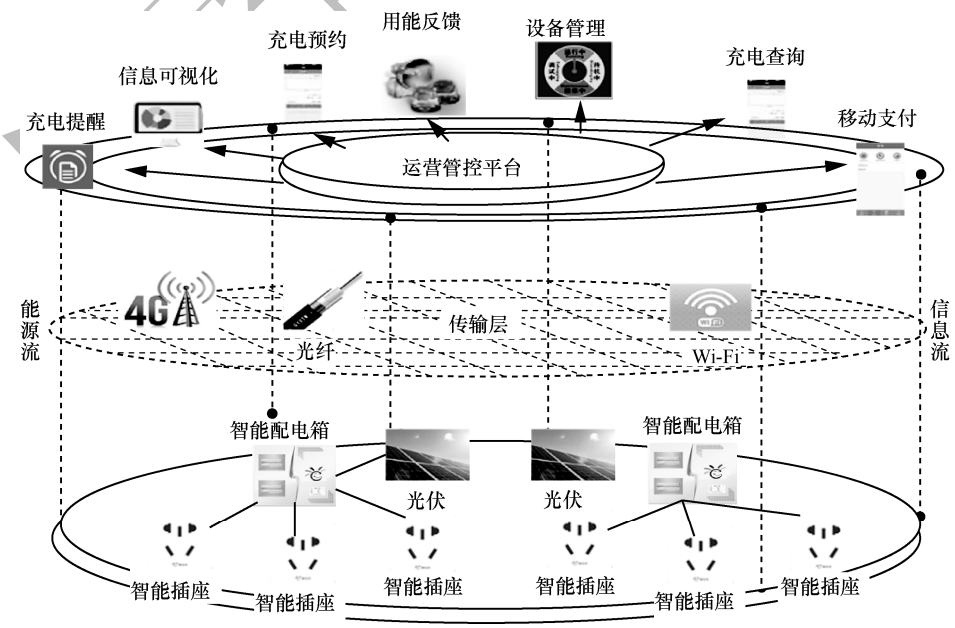


图 1 智慧物联电动自行车充电系统架构

3.3 光伏储能充电停车棚

光伏储能充电停车棚是将光伏发电、储能和车棚相结合的系统。既能为车辆遮风挡雨，又能利用太阳能创造出清洁光伏能源供电动自行车充电、灯光照明。“光伏车棚+智能配电柜”一体化光伏储能充电车棚能够通过光伏发电后储存电能，光伏、储能和充电设施形成了一个微网，根据需求与公共电网智能互动。光伏储能充电停车棚的大范围普及不仅可以实现清洁能源供电，还能缓解大量电动自行车充电时对区域电网的冲击。

光伏储能充电停车棚采用市电、光伏和储能混合供电。白天有光照时，由光伏系统供给充电柜，多余电量存储于储能设备，电池充满后，再供给棚内用电负载使用。夜间车棚优先使用储能供电，市电作为补充能源。

4 电动自行车充电运营管控平台

4.1 系统概述

电动自行车充电运营管控平台主要功能是实现对各个车棚的统一管理，对区域充电信息统一采集、统一管辖，降低人力成本，实现用电智能调配、信息融合和高效利用，实现设备故障运维统一调度，保证各个充电停车车棚安全稳定运行。

电动自行车充电运营管控平台基于物联网、云计算、通信、自动化、新能源等技术，实现信息共享互通，为打造安全高效、智能互动、绿色健康、实时便捷的智慧社区增光添彩。

4.2 功能设计

电动自行车充电运营管控平台对电动自行车充电过程中运行状态进行远程控制，采集智能配电柜数据，实时掌握充电过程状态，通过提前分析、预警等技术，融合现代物联网、大数据分析、自动化控制、故障感知与识别、无线通信等技术手段，实现对用电信息的采集分析、对用电状态的监测以及故障报警、设备增减管理、充电预约、充电提醒、充电查询、移动支付、用能反馈等功能。

应用架构如图 2 所示。

5 应用前景

目前全国电动自行车的数量以每年 30%的速度增长，电动自行车充电市场巨大。基于智能配电柜的电动自行车运用新一代物联网技术，提供更优质的用户体验，更安全的运行保障。该方案的使用，将大幅度提升用户生活水平，保障居民充电安全；光电互补，消费价格更具优势。该方案将会在市面快速普及，不仅获得收益，更降低电网负荷。

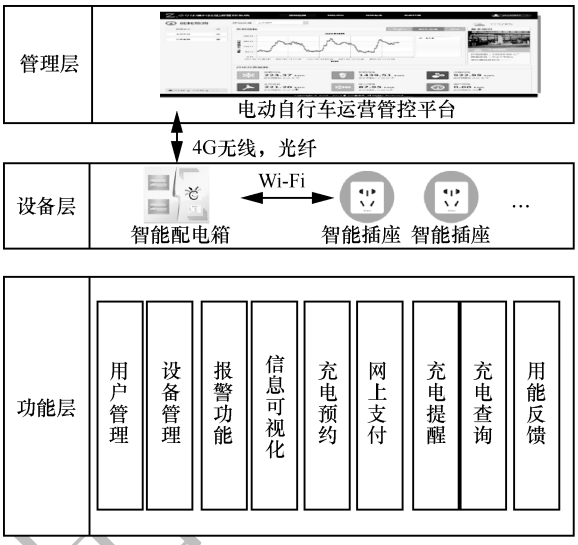


图 2 应用架构

6 结束语

电动自行车在居民生活中的大范围使用，使充电安全、电网负荷日益严峻，通过智慧物联电动自行车充电系统的推广，开展电动自行车充电系统和终端销售实施服务，提升居民用电安全；开展以综合能源服务为核心的智慧能源小区建设和运营，不断提升节能公司的盈利能力；开展电动自行车充电平台推广应用，完善平台的业务功能，提升平台的集成服务和用户支撑能力。智慧物联电动自行车充电系统是物联网在智慧社区中的新应用，是车联网的新覆盖，是能源调配的新方向，是智慧城市的新触角。

参考文献:

[1] 赵树宗, 滕开良, 缪春琼. 以 DSP 为基础的电动自行车智能充电系统[J]. 科学技术创新, 2019(4): 162-163.

[2] 徐松, 蒋伟. 电动自行车无线充电系统设计[J]. 电力电子技术, 2015, 49(10): 89-91.

[3] 杨钰婷. 电动自行车规制问题研究[J]. 电动自行车, 2018(11): 40-44.

[4] 李智超, 刘建伟. 住宅小区电动自行车消防安全的探讨[J]. 消防界(电子版), 2018(24): 33-34.

[5] 王伟. 电动自行车停车库(棚)设置现状及安全对策[J]. 消防科学与

人民邮电出

技术, 2017(8): 1163-1165.

[6] 戴震, 左爱兵, 麻宇蓉. 团体标准助力电动自行车产业提质增效的研究[J]. 标准科学, 2018(6): 117-120.

[7] 叶德辉, 刘佳欢, 杨孝君. 公共电动自行车充电站服务设计研究[J]. 设计, 2018(14): 120-122.

[8] ADITYA S, VENUGOPAL P, PAVOL B, et al. Economic viability study of an on-road wireless charging system with a generic driving range estimation method[J]. Energies, 2016, 9(2).

[9] LAURIE D. Making fast-charging electric vehicles a possibility[J]. Materials Today, 2018, 21(2).

[10] NAZARLOOA, FEYZI M R, SABAHIM, et al. Improving Voltage Profile and Optimal Scheduling of Vehicle to Grid Energy based on a New Method[J]. Advances in Electrical and Computer Engineering, 2018, 18(1).

人民邮电出版社

智慧园区综合能源智能调控算法实现与综合能源用能策略管理

赵鲲鹏[1]，保拉[2]，胡剑[3]
（1. 国家电网有限公司客户服务中心，天津 750021;
2.北京智芯微电子科技有限公司，北京 102299;
3.北京中电飞华通信股份有限公司天津分公司，天津 300040）

摘　要：随着智能互联网的兴起和绿色节约型社会的建设发展，单一式能源的粗放式供给模式已无法适应现代园区企业的用能发展需求，现代园区企业用能需求将向多能供给、多能融合、多能智能调配、用能绿色与经济最优模式发展和演进，新兴能源供需模式将依靠大数据和物联网及人工智能算法，智能化的对园区综合能源供应需求进行多能融合调控，形成不同能源供应流的交叉有序智能供应调配，发掘能源数据的导向价值，为园区智能能源供需调控提供支撑。

关键词：综合能源；智能调控；用能策略

1　园区综合能源供给现状与用能需求分析

1.1　园区综合能源供给侧现状

电能目前是园区现有能源供给中唯一的来自于外部的能源，园区自建能源供给系统还包括太阳能空调系统、光伏发电系统、地源热泵系统、太阳能热水系统、冰蓄冷系统、储能系统、蓄热式电锅炉系统、常规制冷机组系统等 8 大能源供给系统，全方面集成园区风能、光能、微网储能等 9 种分布式能源转换装置。而其中，可以再生的能源利用包括太阳能空调系统、太阳能热水系统、分布式光伏发电系统、空气源热泵、地源热泵系统；蓄能式调节利用包含冰蓄冷系统、储能微网系统、蓄热式电锅炉系统；常规节能利用都包含了基载式冷水机组，通过多种能源供给系统的建设来满足园区对冷、热、电、热水等能源的供应需求，如图 1 所示。

1.2　园区综合能源用能侧的需求现状分析

国家电网客服中心园区能源供应主要旨在服务于

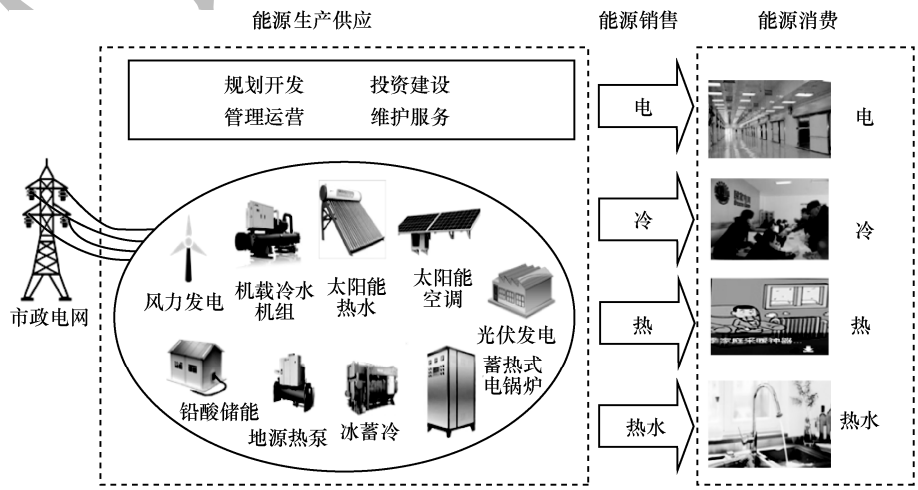


图 1　能源生产供应与能源消费

95598 呼叫中心、电力智能化互动服务及电子商务网站、节能电动汽车展示体验基地及其他的配套办公与维护部门，园区划分为生产办公区域与员工生活区域，共计 10 栋楼宇。园区生产生活用能模式具有显著的周期波动特点，生产区能源消耗波动较为平稳，生活区能源消耗具有明显的潮汐波动变化。结合上述特征，利用信息通信与人工智能、大数据等技术生成能源调控算法模型，对能源预期需求、能源系统出力变化、多能源协同供能优化进行智能化调控管理，能源智能化调控管理如图 2 所示。

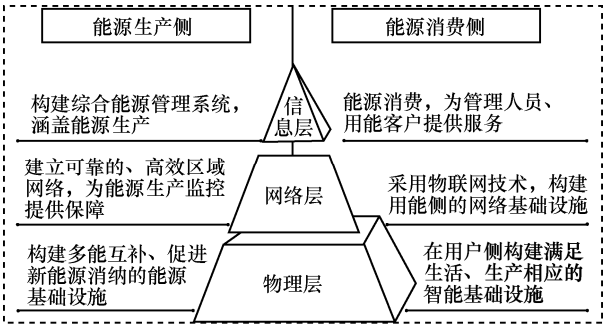


图 2　能源智能化调控管理

2　园区综合能源智能调控技术的策略设计

2.1　基于绿色能源的多能供应智能调控策略设计概要

运用物联网、大数据等技术，促进能源流与信息流深度融合，搭建综合能源服务信息化管理平台，该平台为客户提供用能分析、在线监测、能效诊断、运行维护等关键服务。综合能源服务智能调控策略已成为时下能源物联网智能供给调控热点，在绿色用能要求、时间差异化电价、可再生能源快速发展等背景下，多能的综合互补在中心园区的综合能源智能化调控建设中应用比较广泛，充分利用太阳能技术、地源冷热源技术、蓄冷/蓄热缓控技术与储能等可再生绿色经济能源，结合本地差异化电能来实现多种能源的综合优化调控，用于满足能源供需的双向平衡。

在考虑园区中各楼宇实际功能与环境分布的前提下，运行策略模型会对这 10 栋楼的负荷指标进行初步预测，得出一个总量数，同时结合生产办公与生活作息时间和园区的常住人数，得出一个最初的预测图。在初步预测图的基础上结合不同季节的天气数据，通过数据分析可以得出园区的负荷情况，其中包括每天不同时点的负荷运行要求，依据这个作为能源供给调配的基础，通过能源感知物联网将各能源设备的状态采集，结合开关控制量度控制，可以实现对园区不同能源系统的出力算法设计。能源感知网如图 3 所示。

2.2　基于绿色能源的多能源供应调控策略目标分析

调度计划：按照以小时为单位，制定运行计划，其中包括各种能源设备的启停、工况、功率等。

负荷预测算：用电、用冷、用热负荷可采用现场用能载荷计算并结合同历史与同类型及同规模的行业用电大数据为趋势分析来源，依据 ANN 中 BP 神经网络算法来推算出未来周期的用电模型；光伏出力控制则主要采用历史天气大数据趋势分析法和 BP 多层神经网络算法进行未来一段时间出力策略模型。不同预测对象可用算法见表 1。

表 1　预测对象及对应算法

预测对象	算法
光伏出力	辐照度预测（相似日→GA-BP 神经网络）→光伏模型
电负荷	相似日→GA-BP 神经网络
冷负荷	回归分析法、相似日法
热负荷	回归分析法、相似日法

将光伏出力模型参数、用电、用冷、用热、用水模型和其他能源使用模型，结合园区行业运转特点进行算法公式与天气辅助参数共同定期产生智能调控策略。能

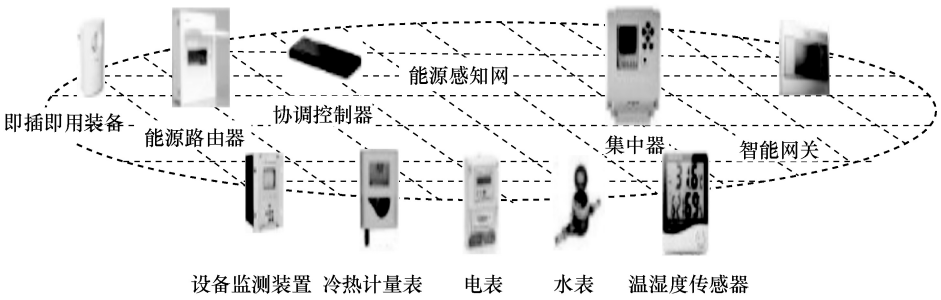


图 3　能源感知网

源智能调控策略包括绿色最优策略、经济最优策略。

2.3 基于绿色能源的多能源供应智能调控策略流程

（1)在未启动其他能源系统进行冷热能源供给时，启动地源热泵系统投入能源供给。

（2）在地源热泵系统投运后，仍无法达到目标设定的能源供给时，将启动冰蓄冷融冰供能。

（3）在冰蓄冷系统仍无法达到供能需求时，则启动双工况主机与常规冷水主机。

（4）当冰蓄冷介入供能后，按照算法需求比对地源热泵机组进行逐对停机。

（5）如果出现在地源热泵、冰蓄冷系统仍不满足供需要求情况下，开启常规冷水主机，仍不满足则启动负荷预警。

智能调控策略如图 4 所示。

3 园区综合能源智能调控策略的实现与管理

（1）多种能源综合智能调控算法与调度策略逻辑实现

园区各综合能源子系统的出力功率是各能源子系统的主机出力功率最高时进行均摊算法的值，得出各能源系统主机的实时投运台数，保障在不满足 1 台设备投运情况下按照最小台数进行投运。

（2）多能源综合智能调控算法与调度策略的判断实现

能源智能调控设备队列的数量逻辑判断可以使能源设备投运数量在保障绿色优先基础下经济最优性，为了防止出现能源主机设备出现短期内大频率的启动与停机现象，能源平台需按照能源智能调控算法对系统当前工作状态与下一个周期将要下发的工作指令进行校对和判断。

- 当运行设备状态相同时，需保障下发调控设备数量与当前运行设备数量保持一致。
- 若判断运行功况与调控出现不致时，可检测不一致来源，判断是出自手动模式实时控制还是自动调控模式，如果是第二种情况出现，需对不一致现象以调控计划为依据进行修订更正，使其保持趋势的一致性。在下一个调控周期依据运行工况进行判断决定是否执行计划任务。

（3）多能源综合智能调控算法与调度策略的控制管理

实时温度调控：当消耗侧的冷热需求量较大时，需增加主机设备的开启台数，用于增大能量的供给，保障需求；当消耗侧的冷热需求量较小时，需关停部分主机设备以减少能量的供给，避免能源的浪费。

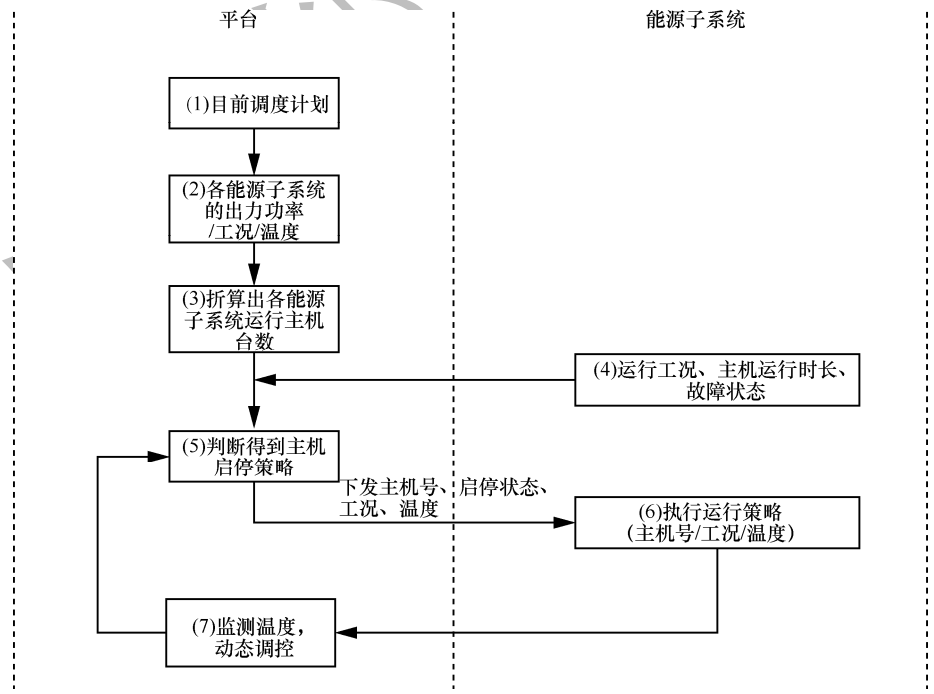


图 4 智能调控策略

管理机制参与智能能源调控:调控算法模型融入绿色节能能源使用管理理念，将客服园区运营工作与电力行业 24 节气生产与服务特点相结合，作为能耗变量辅助调节参数，增强智能调控耗能曲线的平滑度与耗能弹性使用需求。

综上所述，通过生成基于绿色与经济 2 种调控控制方式。

基于绿色能源调控的运营最优。各能源子系统优先级为：地源热泵直供>冰蓄冷融冰>冰蓄冷直供>双工况主机> 常规冷水主机。供冷的协调控制流程如图 5 所示。

4 园区综合能源智能调控技术的展望与挑战

能源智能调控是以能源智能互联网络为载体基础，能源互联网是能源基础设施和信息技术深度融合、开放对等的信息能源一体化平台及泛在、融合、智能

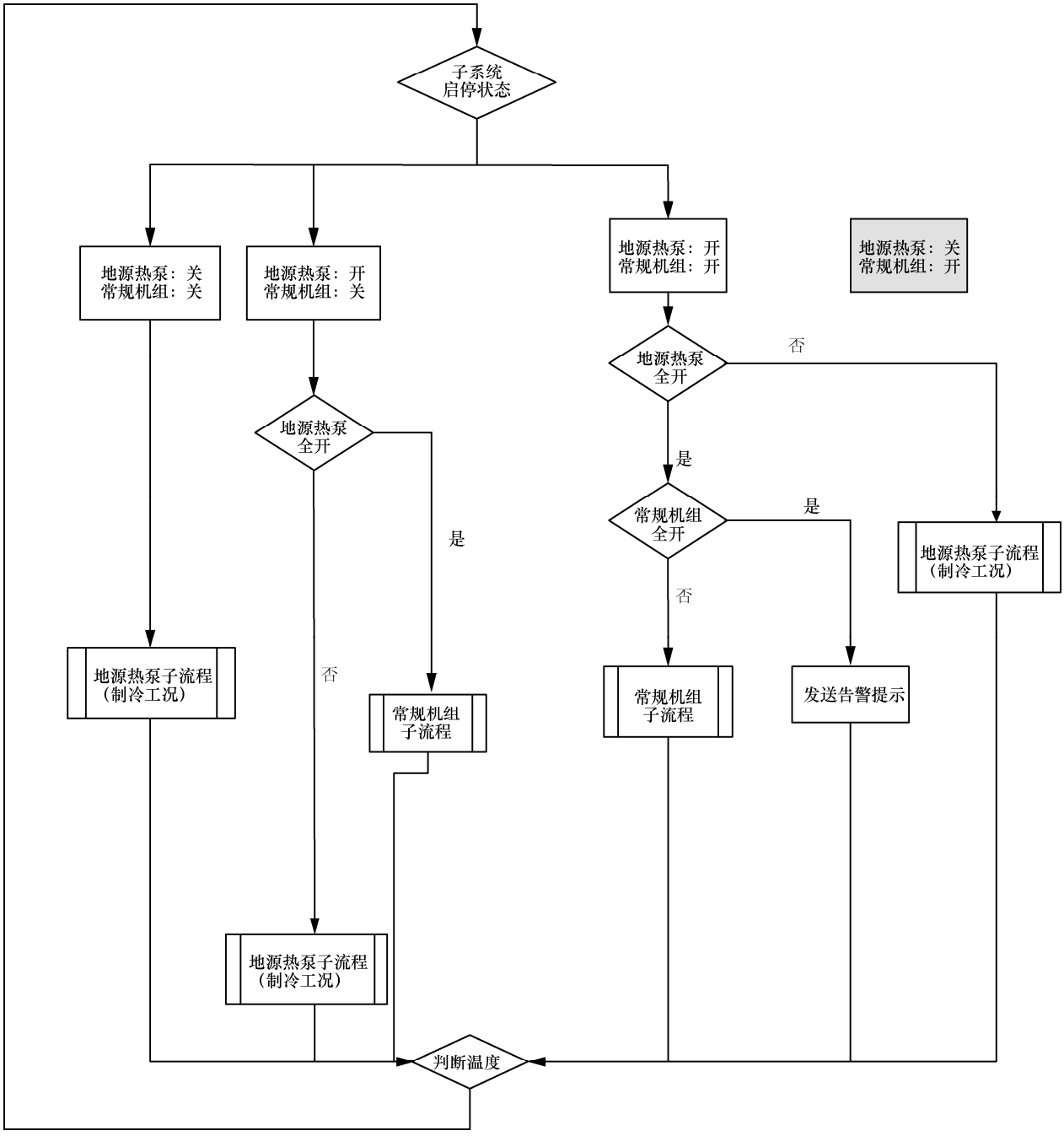


图 5 协调控制流程

低碳的能源互联网络，并形成与之相适应的可再生能源为重点的分布式能源供应与消费系统。

随着综合能源供给智能调控技术的发展，未来综合能源智能调控技术将以物联网和智能互联网为调控载体，结合大数据的数据趋势预测技术，从能源供需侧感知能力细粒度和多系统数据融合交叉运算的深度两个维度提升多能源融合调控精准度与智能化程度。

（1）基于万物泛在物联网的能耗设备用能感知特征与用户用能行为的聚类感知，为综合能源系统中单位、用户的用能行为生成能耗特征曲线，提高能源调控的变化预知能力。

（2）基于多系统大数据智能萃取技术与能源用能调控相结合进行智能综合能源调控的命中精度。

多系统数据交叉算法分析技术，利用智能监测设备和安防、智能楼宇、生活监测数据沉淀进行规模庞大的用能数据建模设计，以机器学习算法和大数据运算平台快速分析并生成未来能耗调控决策，实现多源异构的策略算法，满足用能侧的最优用能调控策略。

5 结束语

基于绿色的综合能源供需智能化调控技术的最终目的是推动能源清洁生产和能源节能高效利用，结合个体生产环境和自然环境对能源因地制宜就近生产与节能利用，充分利用物联网络技术、智能 AI 技术、大数据清洗萃取技术将能源需求方的需求感知融入能源智能调控技术，重构能源供需双方的能源供需安全与绿色节能发展模式。

参考文献：

[1] 冯庆东. 能源互联网与智慧能源[M]. 北京:机械工业出版社, 2018.

[2] 周西梅, 许晓林, 孟慧霞, 等. 电网企业开展综合能源服务的思考[J]. 基层建设, 2018(34).

人民邮电出版社

智能电网与泛在电力物联网的边界互联信息安全防护

曹洋，范义
（中国电建集团江西省电力设计院有限公司，江西 南昌 330096）

摘　要：坚强智能电网和泛在电力物联网融合构成能源互联网，面向综合能源服务的能源互联网具有平台型、枢纽型、共享型的特点，其中,共享特性加强了电网的综合能源服务属性，却给网络的稳定运行带来更多的信息安全风险。在智能电网现有信息安全架构和防护体系的基础上，分析了泛在电力物联网的建设对电网安全带来的潜在影响，针对智能电网与泛在电力物联网的边界安全互联方式进行深入了研究，给出了两网融合深度的建议，从可靠性和开放性两方面综合考虑，提出了两网融合后能源互联网的信息安全总体防护设计。

关键词：能源互联网；智能电网；泛在电力物联网；信息安全防护

1　引言

能源互联网是坚强智能电网与泛在电力物联网深度融合而成能源流、数据流、业务流的三流合一面向综合能源服务的工业互联网。其中，智能电网具有高可靠性、稳定性、枢纽性、封闭性的特性，协同发电、输电、变电、配电、用电、调度环节的高效安全稳定，并已经覆盖信息安全防护体系；泛在电力物联网的建设刚起步，具有高交互性、泛在性、分布性、开放性的特性，实现电力系统的万物互联互通，通过海量大数据的采集、分析、挖掘和应用，让电网运行得更高效、更经济、更合理，同时，物联网得开放特性带来更多的信息安全风险和薄弱环节。智能电网和泛在电力物联网融合方式、深度以及安全防护体系的研究至关重要，是确保能源互联网实现既能泛在互联又能安全可靠稳定运行的关键。

2　信息安全现状

2.1　智能电网

电力系统经历了近十余年快速发展，已建成由发电、输电、变电、配电、用电和调度环节组成，信息通信平台支撑的坚强智能电网。智能电网按照安全分区、网络专用、横向隔离、纵向认证、综合防护的二次系统信息安全防护原则，将基于计算机及网络技术的业务系统划分为生产控制大区和管理信息大区，按业务特点将生产控制大区划分为控制区（安全区Ⅰ）和非控制区（安全区Ⅱ）。安全防护分区见图 1 所示。

生产控制大区的控制区和非控制区业务分别部署纵向认证加密装置，确保业务接入的安全性。生产控制与管理信息两个大区之间部署经检测认证的单向安全隔离装置，根据大区之间业务信息流向，设置正向或反向安全隔离装置，隔离强度接近或达到物理隔离。

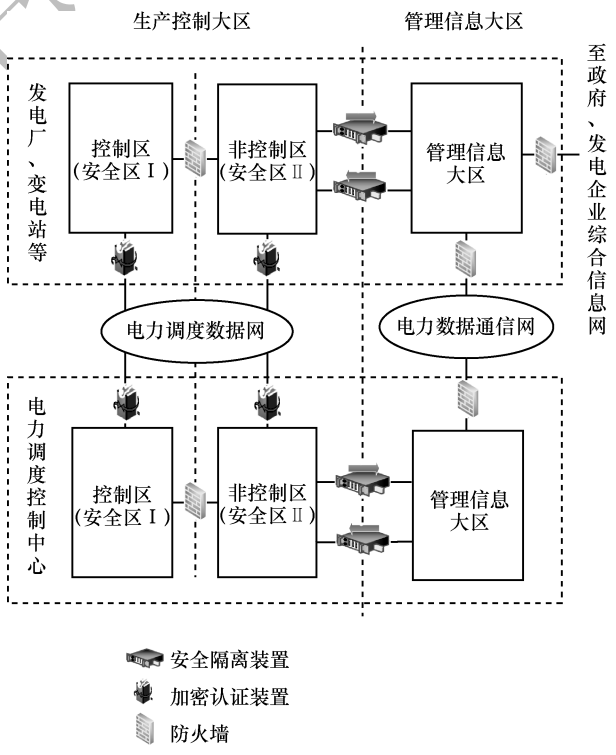


图 1　智能电网安全防护分区

2.2　泛在电力物联网

与智能电网相比，泛在电力物联网具有网元数量

人民邮电出版社

巨大、互联要素多，网络结构复杂，接入方式多样等泛在感知特点。按照经济合理的原则，泛在电力物联网的安全防护体系原则上可参照管理信息大区的安全架构和原则，考虑其对现有智能电网的信息安全影响，划分一个独立的泛在物联安全大区，泛在电力物联相关业务的信息接入至电力大数据中心，业务以营销、配电、分布式能源、微网、综合能源等为主，为确保泛在接入端到端的唯一性和可追溯性，在泛在物联终端接入点，应部署纵向认证装置，确保接入终端身份的唯一性、数据的安全性和信息的可追溯性，物联网终端具备经认证的唯一入网 ID。

2.3 两网边界

智能电网和泛在电力物联网的融合势在必行，但其融合的前提则是在不牺牲智能电网现有安全可靠性的前提下，最大限度的实现两网的深度融合。两网的边界应明确界定各个层级的横向互联原则、形式和方式。

3 安全防护方案

3.1 融合深度

两网融合深度根据技术发展和网络的运行状态适时地选择，在泛在电力物理网建设初期，仍以维持浅融合或局部融合的方式，确保智能电网的较高可靠性，减少开放性带来的信息安全风险。通过业务侧、网络侧、数据侧的逐步融合，最终实现全面融合。

3.2 融合方式

建议采用“横向交互、顶层融合”方式实现智能电网和泛在电力物联网的融合，横向交互的方式可以简化，避免纵向交错接入带来的网络入侵风险，在省级及以上电网中心进行数据交互、网络互联，上层融合集中对两网信息交互数据进行监控、审计、隔离、分析、处理，有效避免底层融合带来的对现有智能电网的安全稳定运行风险。

3.3 边界安全防护方案

能源互联网信息安全防护的重点，就是研究智能电网和泛在电力物联网的互联边界安全防护策略，现有智能电网保持既有的安全防护体系，而泛在电力物联网则建立一套相对开放的安全防护体系，而两网之间的信息交互安全，显得至关重要，尤其具有海量接入的泛在电力物联网侧发起的网络入侵风险，会给电网的安全稳定运行埋下隐患，甚至有可能给社会经济造成重大损失。

智能电网和泛在电力物联网融合下的能源互联网，应不改变目前智能电网的安全体系架构和策略，独立划分一个泛在物联信息大区，考虑泛在物联自身的安全体系，重点研究泛在物联信息大区与智能电网管理信息大区信息交互的方式和边界安全防护的方案。为避免边界过长，在省级及以上的电网中心进行两网互联。根据互联深度和强度的差别，可采取如下两种安全方式，如图 2、图 3 所示。

方式一如图 2 所示，在两网之间通过正反向隔离装置实现互联，同时在智能电网和泛在电力物联网设置信息导入、导出安全池，负责信息数据的安全审核、

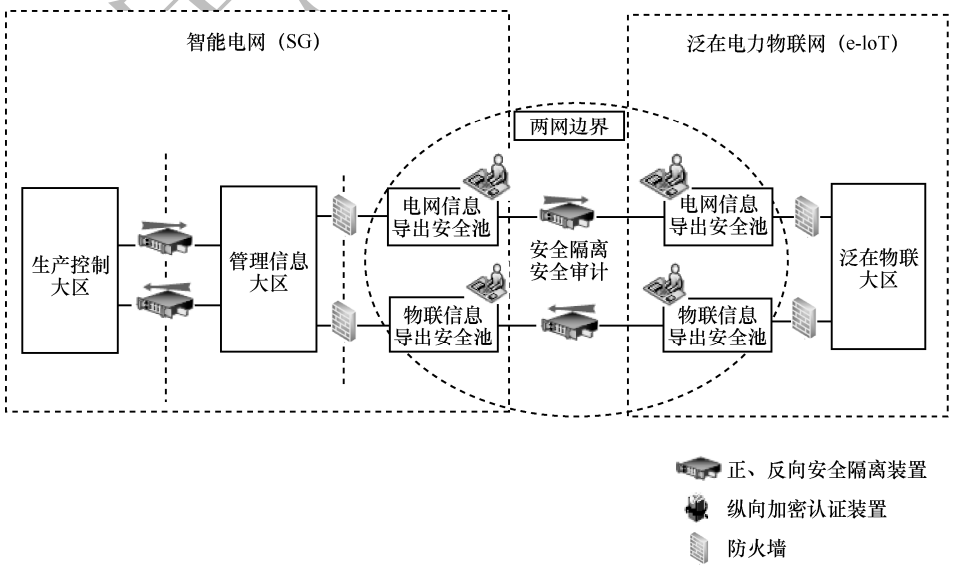


图 2　网络边界安全防护方式一

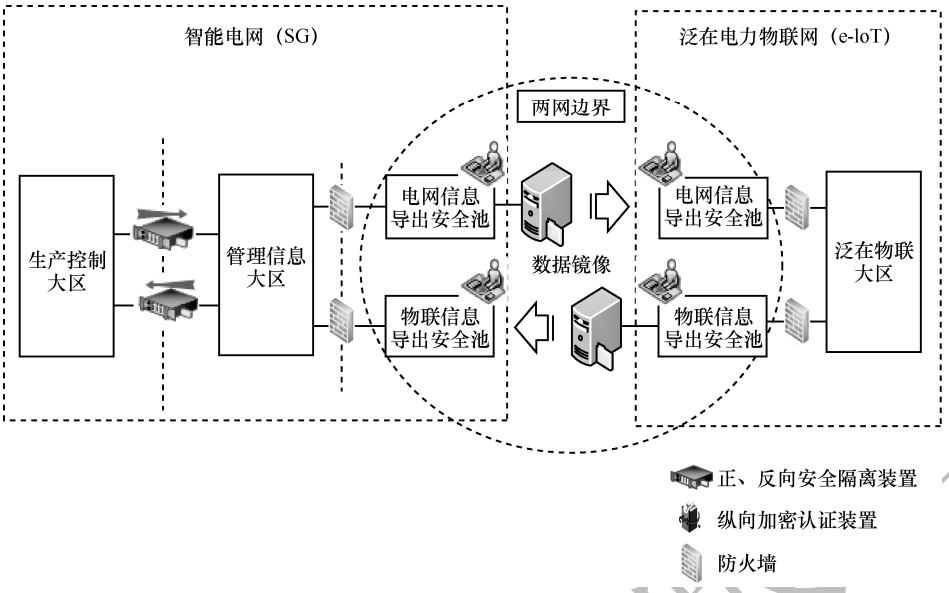


图 3　网络边界安全防护方式二

缓冲备份、数据审计等任务，确保两网信息数据交互的合法性、安全性，一旦出现严重信息安全事故，立即切断两网的互联，迅速及时转变成两张网各自独立运行，以便分区排查和隔离信息安全事故，减小影响范围，确保主网的安全运行。为确保网络可靠安全，两网边界互联的单向安全隔离装置、生产控制区和管理信息区边界互联的单向安全隔离装置选用不同原理、不同厂家的设备，两网边界的安全隔离装置的信息吞吐量和防护策略都应进行充分的论证。

方式二如图 3 所示，两网之间没有物理互联，仅通过数据同步镜像或代理服务等方式进行信息交互，在智能电网和泛在电力物联网设置信息导入、导出安全池，负责信息数据的安全审核、缓冲备份、数据审计等任务，确保两网信息数据交互的合法性、安全性、可追溯性。

3.4　方式比较及推荐

方式一中两网单向隔离互联，能较好的保证信息交互的实时性，但由于两网并非真正物理上的隔离，存在物联网侧的海量接入点入侵智能电网的风险；方式二中两网物理隔离，避免来自物联网对智能电网的实时攻击和入侵，但两网信息数据交互的实时性会较差。

综合考虑能源互联网对智能电网与泛在电力物联网的深度融合需求，推荐泛在电力物联网基本建成后，采用方式一安全部署方案实现两网边界互联，并做好安全风险评估、安全策略研究、建立有效安全机制、开发更高效更安全的隔离装置等方面的应对，最大限度地减小泛在物联海量终端的接入对电网安全稳定运行的风险。必要时可采用分区域切块方式，对安全风险进行快速定位和隔离，减小影响范围。

但是，在泛在电力物联网的建设初期，建议采用方式二实现与智能电网的信息安全防护，待相关技术、机制和管理成熟后，泛在电力物联网基本建成时，再逐步过渡到方式一，实现两网的深度融合。

3.5　能源互联网下的信息安全防护

能源互联网下的智能电网和泛在电力物联网的安全防护重点要考虑横向互联信息安全，智能电网总体上延续既有的安全体系架构，泛在电力物联网根据其海量接入、泛在感知特性，重点研究物联网的海量终端认证和可追溯等信息安全因素。

能源互联网下的智能电网信息安全防护延续已有安全体系，仅与泛在电力物联网交互处部署安全缓冲区，进行数据缓冲、安全隔离和安全审计，主要目标是抵御来自泛在电力物联网的攻击或入侵。智能电网信息安全防护体系如图 4 所示。

泛在电力物联网需考虑接入海量终端设备，因此纵向采用简易加密认证装置或内置加密芯片等方式接入泛在终端，确保接入设备的身份认证、数据加密、访问控制。与智能电网的横向防护，采用设置信息导入、导出缓冲安全区，实现与智能电网的信息交互。

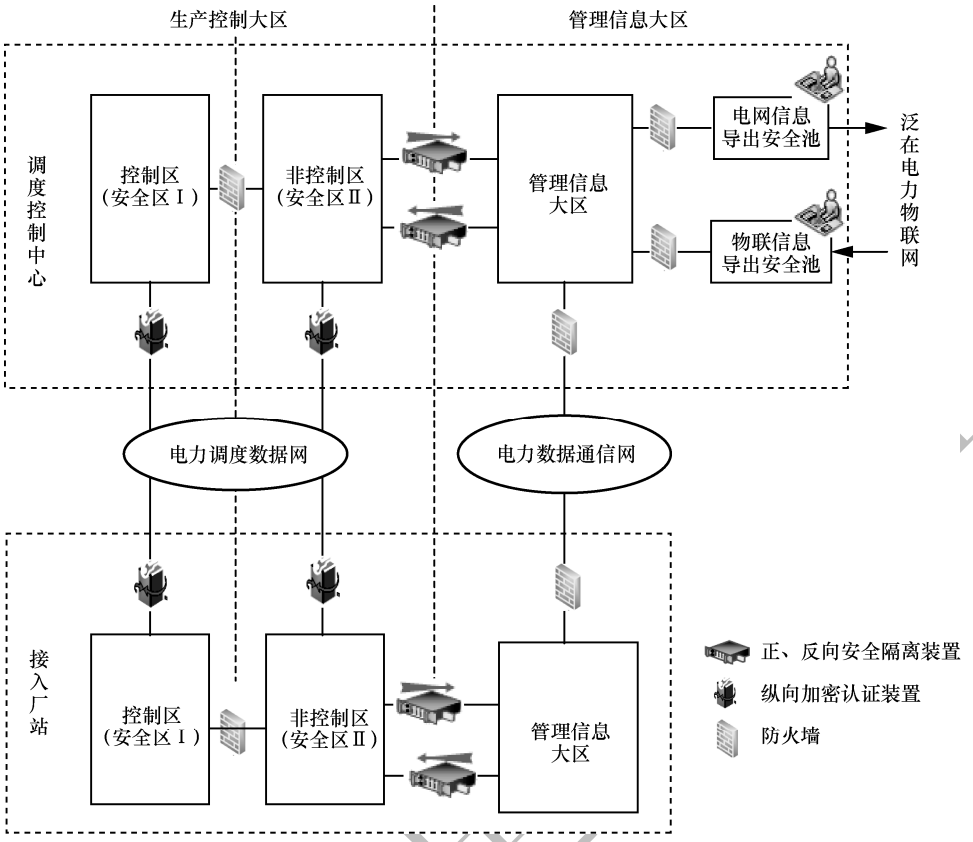


图 4　智能电网信息安全防护

泛在电力物联网的纵向业务可根据业务的重要程度、实时性要求、可靠性要求、安全等级等划分 VPN，确保各类电力业务对网络 QoS 的差异化要求。各类业务的 VPN 通道均应设置相应的纵向认证加密装置，确保各类信息数据的安全传输和业务认证。

综合安全方面，泛在电力物联网边界部署入侵检测装置及时监视泛在电力物联网网络传输状态，发现可疑传输时发出警报或者采取主动反应措施。同时还需部署内网安全日志审计，实现记录和跟踪网络运行状态，监测、记录用户各种信息、网络安全事件等安全审计功能。泛在电力物联网信息安全防护体系如图 5 所示。

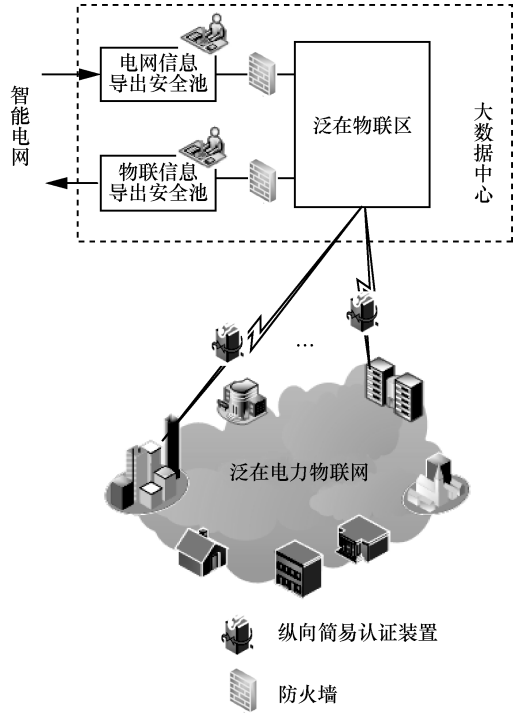


图 5　泛在电力物联网信息安全防护

4　结束语

能源互联网信息安全的重点在于智能电网与泛在电力物联网互联边界的横向防护、泛在电力物联网自身纵向防护，应从信息系统、网络系统、恶意代码防范、安全设备、容灾备份、物理环境、安全策略、安全管理等方面进行全面规划，综合考虑能源互联网安

全可靠和共享开放的这两个互相制约因素，评估网络可承受的安全风险，构建可行、经济、可靠的安全防护体系。能源互联网架构下的安全防护体系，应在确保智能电网现有安全系统防护强度的基础上，重点研究两网边界防护，综合考虑泛在电力物联网的安全性和开放性，构建庞大网元前提下和复杂网络环境下能源泛在物联的大安全构架体系。

参考文献：

[1] 邹春明, 郑志千, 刘智勇, 等. 电力二次安全防护技术在工业控制系统中的应用[J]. 电网技术, 2013,37(11):3227-3232.

[2] 李文武, 游文霞, 王先培, 等.电力系统信息安全研究综述[J]. 电力系统保护与控制, 2011, 39(10): 140-147.

[3] 国家市场监督管理总局 .电力监控系统网络安全导则[Z]. 2018

人民邮电出版社

智能化语音监控系统在群堆电厂的应用

邝豪，高小岩
（中国广核电力股份有限公司信息技术中心，广东 深圳 518124）

摘　要：随着核电自主化、专业化、国际化的快速发展和集团信息化水平的不断提高，核电的语音通信系统在日常生产及应急情况下发挥着关键作用。为了保障该系统的安全、稳定、可靠运行，结合多年运维经验，成功建设了群堆电厂模式下的智能化语音监控系统，具体介绍了系统平台架构、系统工作模式等，实现了语音通信系统统一领导、统一规划、统一标准、统筹投资、统一建设、集中运维的“五统一集”目标，提升了语音通信系统运维管理能力。

关键词：群堆电厂；智能化；监控；可靠性；五统一集

1　引言

随着集团在国内外业务的快速发展，群堆电厂下的语音通信系统对日常行政办公、生产、应急越来越重要。同时，语音通信系统本身也在群堆电厂中不断地扩建，现已建成系统超过 20 套，设备数量超过 4 000 台（包含服务器、媒体网关、相关板卡等），形成了两个双冗余、高可靠的汇接中心，向外覆盖集团国内外的各个核电基地、各个分公司及办事处，但是，该系统目前没有监控手段，在实际运维管理过程中会出现很多问题。

- 整个专业模块处于“救火”状态，只能被动地提供支持，没有提供主动的服务。
- 无相关告警数据，发现问题困难，定位故障原因缓慢，很难实现持续性评估工作。
- 群堆下的运维和业务的保障工作无法达到有效统一，地域分散、设备繁多，缺少对语音业务运行状态的监控手段，无法进行对系统集中直观的监控和管理。

以上问题严重影响了语音通信系统的可靠性管理。因此，建立一套智能化的、高质量的语音监控系统，能够提升系统的稳定性，有效整合集团群堆电厂下的语音通信资源，真正实现“五统一集”目标。

2　群堆电厂智能化语音监控系统概述

2.1　系统概述

群堆电厂智能化语音监控系统是结合核电特殊性开发设计的一套监控系统，该系统拥有强大的智能化数据分析引擎和解决方案提供功能，管理员发现告警后仅需按照解决方案进行处理，同时该系统提供语音资源采集分析，可以通过多方式、多维度的数据分析，进行集中展示、集中分发。智能化语音监控拓扑如图 1 所示。

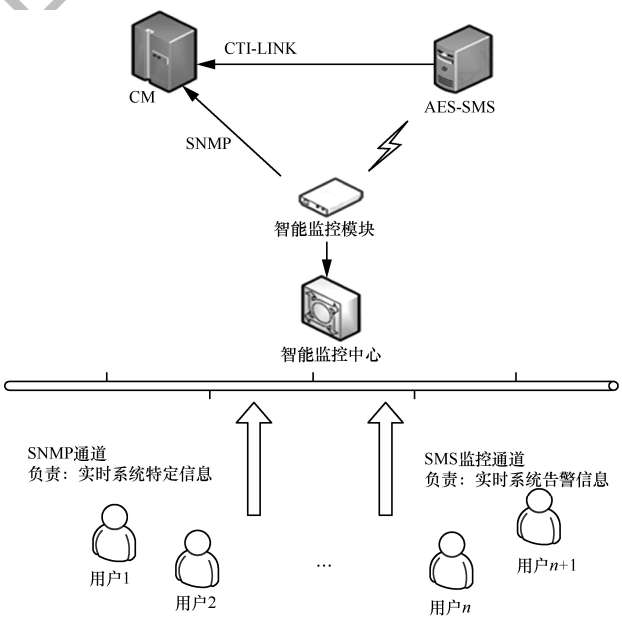


图 1　智能化语音监控拓扑

2.2　系统平台架构

群堆电厂下的智能化语音监控系统，设计架构从低到高可以分为 7 层，如图 2 所示，具体介绍如下。

人民邮电出版社

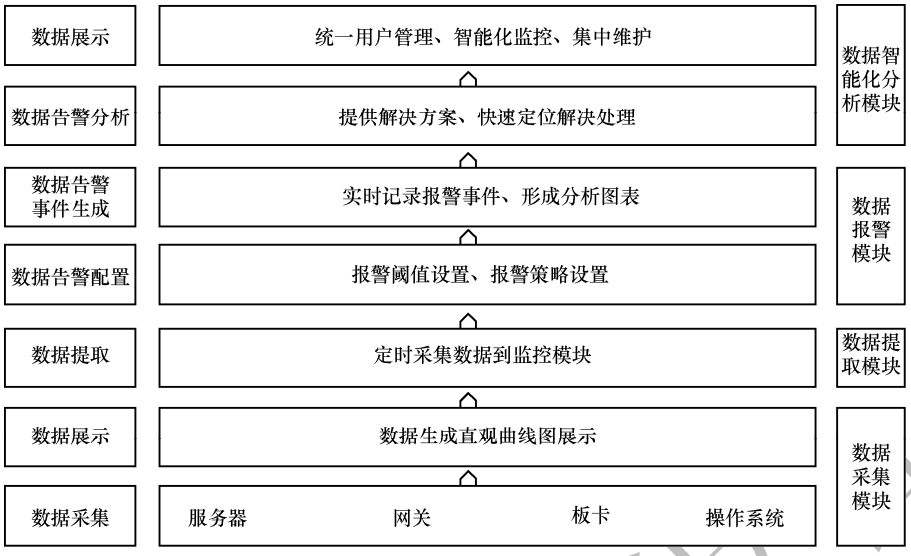


图 2　智能化语音监控系统架构

- 数据采集层：位于最底层，主要采集服务器数据、媒体网关数据、用户板卡数据、操作系统数据等，然后将采集到的数据进行规范化，并进行存储。
- 数据展示层：位于第二层，是一个 Web 展示界面，主要是将数据收集层获取到的数据进行统一展示，展示的方式可以是各种图形，通过将数据图形化，给管理员提供数据趋势，并作为管理员排查问题或解决问题的依据。
- 数据提取层：位于第三层，主要是对数据采集层采集到的数据进行统一处理，提取需要的数据发送至监控报警模块，这个部分是监控和报警两个模块的衔接点。
- 告警规则配置层：位于第四层，主要是根据第三层获取到的信息按规定格式进行报警规则配置、报警阈值配置、报警联系人配置和报警方式的配置等。
- 告警事件生成层：位于第五层，主要是对报警事件进行实时记录，并将报警信息写入数据库，同时将报警结果形成规定的分析报表，以统计一段时间内的故障率和故障发生趋势。
- 数据告警分析层：位于第六层，主要是将数据库的告警记录采用智能化数据分析引擎对告警进行分析，并提供详细的解决方案。
- 用户展示管理层：位于最顶层，是一个 Web 展示界面，主要是对监控统计结果、报警故障结果进行多方式、多维度的展示。

3　群堆电厂智能化语音监控系统设计

3.1　系统工作模式

系统采用多重架构，提供了 B/S 的访问模式，节省安装客户端的动作，提升了用户体验。系统拥有灵活、高效的采集引擎，通过对象识别、采集并发及针对的厂商扩展脚本，可准确、可靠地提供语音设备交互服务。系统利用 ICMP、ARP、SNMP、CLI 等标准进行语音设备探测和信息采集，对发现的语音设备对象进行识别、分析、保存，形成统一的设备资源库，并在此基础上进行拓扑计算，生成物理等不同层次的拓扑结构。

通过主动（ICMP、SNMP、CLI）与被动（Trap）两种方式，系统可以从设备上获得各类性能指标和流量数据，经过长时间数据的跟踪记录，最终挖掘分析生成各种报表，展现所需要的事件和资源情况，以提供合理的评估与决策。

在对群堆电厂语音系统的不间断实时监测中，系统能够收集针对服务器、网关、板卡及终端的各种事件，关联所有符合故障特征的相关事件，并利用智能化数据分析引擎，最终在故障发生前或故障发现时发出正确告警，提供相应的解决方案，便于管理人员高效、及时地定位并解决问题。

3.2　事件分析管理

系统通过独立算法，对群堆电厂下系统数据进行统一比对分析、合并，并统一展示。

通过对事件进行过滤、归并、相关性分析、传递

等分析处理，同时对分析的每一条告警提供解决方案，并将处理过程及经验反馈保存在数据库中。

对事件的严重级别加以分类，并分别通知相关人员。故障管理模块可实时监控语音设备运行过程中的异常，并形成初步的原因分析通知到运维管理员。

3.3 资源管理

系统集中继、呼叫量和媒体资源等监测管理于一体，支持 SNMP、Syslog、CLI（Telnet、SSH、WMI）监测，拥有多种监测器，提供对整个语音业务的 7×24 h 不间断监控。

（1）强大监测插件体系

无需二次开发，通过监测插件，不断增加监测器数量，扩展监测范围与内容。众多监测器工作独立，互不影响，保证整个监测体系的稳定运行。

（2）灵活的监测时间调度机制和智能化的监测阈值模型

自定义监测时间与监测阈值，形成多样化、组合型监测策略，满足复杂环境下不同的监测任务要求。

（3）资源趋势分析能力展现

多方式、多维度的资源自由组合，集中展现资源情况及资源趋势。

3.4 报表管理

系统提供性能、告警、状态、资源多个角度的统计和分析报表。

（1）全面的性能与告警报表

对监测数据的自动汇聚、抽取、分析，提供基础架构性能与告警、资源比较、指标排名、指标趋势等各类层次化统计分析报表。从业务运行状态到微观性能指标，自定义查询业务应用系统及其关联资源的当前和历史运行情况。

（2）业务运行报表

支持按业务的方式对业务应用可用性、MTTR 和 MTBF 进行统计。

（3）节点报表

支持按节点的方式对其监测数据进行汇总分析，提供基础架构性能指标趋势等各类层次化统计分析报表，并支持自定义时间段进行查询。

（4）“所见即所得”的报表

支持报表收藏功能和订阅。支持导出为 Excel、PDF 文件和立即发送报表到指定 E-mail 邮箱，还能够为不同的用户订阅相关报表，自动定时发送到指定 E-mail 邮箱，提供系统优化、决策分析和业务规划的量化参考。

4 价值点

综上所述，智能化语音监控系统在群堆电厂的应用中，具有如下优势。

（1）群堆电厂下众多分散系统和设备的集中管理

通过将众多分散在群堆电厂下的语音通信设备配置在集中监控平台中，将各语音系统配置数据、状态数据、资源数据等进行集中管理及展示，使群堆下各电厂运维人员清晰、及时地了解系统设备的状况，实时反馈拓扑的变化情况，使通信运维人员能够快捷地对问题做出响应和处理，提高语音通信系统集中管理能力。

（2）提升决策层的决策能力

该系统通过智能数据采集，实时对群堆电厂下所有系统数据（包括资源、性能、运行信息等）进行多维度、多方式分析处理，对比展现，为未来系统发展提供决策支持。同时，这些数据分析，也能共享到群厂的各业务部门及相关管理人员面前，让他们实时了解系统运行状况、资源使用状况。

（3）智能化语音监控的强大故障分析能力支撑

原始“按程序操作模式”的系统运维方法已不适用于群堆电厂的大数据、精细化运维，因此建立以强大故障分析工具为支撑的运维管理平台，不仅提供能告警及通知功能，更重要的是对每条告警数据进行大数据分析后提供对应的解决方案，维护人员只需按照对应解决方案处理，减少维护人员分析成本，降低人员因失误操作带来的业务影响，最终提高了工作效率。

5 结束语

群堆电厂下众多分散设备运维管理的质量对核电厂的日常生产、核应急至关重要，系统告警的及时、有效处理也终将决定着设备的运维管理质量。因此，设计应用一套智能化、高质量的语音监控系统是保证语音设备安全、稳定必不可少的工具，该监控系统秉承“一次把事情做好”的理念，对比业界优秀设计方案，结合核电群堆电厂的特殊要求，实现了语音通信系统统一领导、统一规划、统一标准、统筹投资、统一建设、集中运维的“五统一集”目标，提升了语音通信系统运维管理能力。

人民邮电出版社

参考文献：

[1] 陈兵, 李俊娥, 聂剑平, 等. 电厂实时监控信息系统的设计与应用[J]. 电力系统自动化, 2003 (8).

[2] 袁桂丽, 王田宏, 金慰刚, 等. 厂级信息监控系统 SIS 的研究与应用[J]. 电站系统工程, 2004 (5).

[3] 丁巧林. 浅谈如何提高电力通信语音业务可靠性[J]. 大观周刊, 2012(2).

[4] 刘权. 基于 CMDB 的网管系统业务可用性监控平台的设计与实现[J]. 电信工程技术与标准化, 2012(2).

[5] 潘安群. 一种基于规则的网络安全事件关联分析方法研究[D]. 武汉: 华中科技大学, 2007.

人民邮电出版社

基于改进蚁群算法的云计算用户任务调度算法

罗斯宁，王化龙，李弘宇，彭蔚
（中国能源建设集团广西电力设计研究院有限公司，广西 南宁 530004）

大摘要：云计算技术可以根据需要执行高计算密集型任务。目前，大多数信息技术（IT）行业已经迁移到基于云计算的框架，以服务其客户。云计算框架通过3 个不同的层次提供服务，即基础设施层、平台层和应用程序层，支持消费者的即时按需需求（如数据存储、计算能力、高带宽等）。企业和个人可以通过虚拟化技术提供的方式使用这些服务。目前，已经存在许多趋势云提供商，如 Amazon EC2、Google、HP 和 IBM 等，其中资源根据客户要求进行虚拟化，并作为“按使用付费”的服务水平协议（SLA）进行提供。云计算可以实现很多功能，如灵活的资源存储库、可扩展和动态的按需服务、基于消费和服务质量（QoS）的服务定价等。

在云计算系统中，资源管理起着重要作用，目的是处理由服务提供商提供的资源池，进行配置和分配任务。云计算系统中资源管理的主要部分是任务调度程序，通过优化算法优化“虚拟机（VM）”的预配置，在逻辑资源中分配用户任务提高任务调度过程的性能。任务调度是云计算中非常关键的问题，其中涉及智能搜索和决策，为每个用户任务找到最佳的虚拟机。

本文在经典蚁群算法的基础上进行改进，在考虑算法快速收敛的同时满足虚拟机的负载均衡。在标准蚁群算法中，启发因子 β 是一常数，算法运行的初始阶段，信息素函数的值不变，信息素函数对蚂蚁选择的概率影响程度较小，而在信息素函数通过不断地局部更新，对获得最终解的影响程度不断增加，所以令启发因子 β 转化为随算法迭代次数变化的减函数：

$$\beta(i) = b^{1/i} \qquad (1)$$

其中，b 为常数，i 为算法当前迭代的次数。

在算法的初始阶段，i 值较小，β 值较大，蚂蚁首要经由启发函数来选择路径，当算法不断迭代，i 值增大，β 值减小，同时路径上的信息素浓度增大，信息素函数对蚂蚁选择路径的影响增强，这样可以提高信息素函数的指导作用，有利于找到最优解。

为了减少虚拟机过载情况，实现在任务分配过程中的虚拟机负载均衡，本文对信息素函数更新过程进行改进，加入信息素调整因子 δ：

$$\delta = 1 - ((C_j - C_{avg}) / \sum_{j \in VM} C_j) \qquad (2)$$

其中，C_j 是虚拟机在上一次迭代中的运行时间 VM_j，C_{avg} 是所有虚拟机运行时间平均值，即 $C_{avg} = \sum_{j \in VM} C_j / m$。信息素函数更新方法改进为：

$$\tau_{ij}(t+n) = (1-\rho) \times \tau_{ij}(t) + \sum_{k=1}^{m} \Delta\tau_{ij}^{k}(t) \times \delta \qquad (3)$$

信息素函数在更新的过程中加入了虚拟机负载状况的影响，当虚拟机的负载程度过大时，δ 值减小，信息素函数减小，当进行下一次迭代时，虚拟机被分配任务的概率也随之减小，从而实现负载均衡。

仿真平台选择云计算仿真平台工具 Cloudsim，为了验证本文算法的调度效率和负载均衡的实现，实验在相同条件和环境下进行，并与 Cloudsim 自带的经典蚁群调度算法的任务分配结果进行比较。一方面，当虚拟机面临更严重的负载时，本文算法能够用更少的时间完成任务的调度，具有更高的调度效率。另一方面，采用改进蚁群算法执行任务时，计算节点的任务分配标准偏差较低，表明节点的负载均衡度较高。因此，本文算法在负载均衡方面也达到了一定的效果。

本文提出了一种基于改进蚁群算法的用户任务调度算法，以解决虚拟机中的任务调度问题。通过对标准蚁群算法的改进，在最小化整体完工时间的同时实现任务调度时间的减小和负载均衡。仿真结果表明，通过该算法的任务调度不仅缩短了任务调度时间，同时实现了任务负载均衡。

关键词：云计算；任务调度；负载均衡

人民邮电出版社

5G 技术在配电网电流差动保护业务中的应用

吕玉祥，杨阳，董亚文，汪玉成
（国网信息通信产业集团安徽继远软件有限公司，安徽 合肥 230088）

大摘要：智能配电网建设随着国家电网公司“三型两网”战略的实施，正不断向网格化、多源化的配电物联网方向发展，分布式电源、储能、电动汽车、“三站合一”、“配电物联网”等建设直接关联配电网的安全稳定运行，使得配电网由单电源辐射形状向多电源复杂供电网络转变，而已有的配电网故障处理方式难以满足智能配电网建设的快速自愈需求。

第五代通信系统（5G）为泛在电力物联网建设提供了 eMBB（增强型移动宽带）、mMTC（海量物联网通信）以及 uRLLC（超高可靠与低时延通信技术）三大应用场景，不仅能够解决配电网典型电流差动保护业务应用难题，同时也能够支撑多类型泛在电力物联网业务。

按照基本业务应用类型对泛在电力物联网承载的业务进行分类，可以将现有承载业务类型分为：生产控制类业务、数据采集类业务以及状态监测类业务。

5G 与智能电网结合形成了“5G+”智能电网新的垂直应用研究领域，对智能分布式配电自动化、毫秒级精准负荷控制、低压用电信息采集、智能配电巡检、分布式电源等业务进行 QoS 指标分析，形成不同指标（如时延、可靠性、带宽、安全性等）需求下的 5G 应用场景建议方案。

在配电网电流差动保护业务方面，由于其优越的速动性、灵敏性和选择性在配电网建设中广泛应用，而现有应用方法多采用专用光纤通道、230MHz/1.8GHz 电力无线专网等通信技术承载实现，但上述方式存在成本高、稳定性差、实时性低等多样化问题。

采用 5G 通信技术结合北斗授时同步技术，提出配电网电流差动保护信号同步应用方案，将配电主站、差动保护装置、配电自动化终端等进行有序串联。

将 110 kV 变电站之间的常用联络线作为 5G 配电网电流差动保护场景进行方案设计，为该线路环网柜分别配置了电流差动保护、测控装置和 5G CPE 通讯模组，同时将电流差动保护以两端考虑，每个智能配电终端分别采集两侧 CT 的各相电流以及零序电流，各自计算被保护线路的差动电流和制动电流，并通过 5G 基站及核心网电力 uRLLC 切片，对发生区内故障，2 个智能配电终端的差动保护逻辑各自动作，保护分别动作出口，实现配电网电流差动保护应用。

在结合 5G 典型应用场景 eMBB 的电网管理业务中，以智能电网变电站巡检监控业务为应用场景，将监控摄像头作为业务信息采集终端，将摄像头与 5G CPE 设备连接，接入 5G 通信网，并在后端现场利用 eMBB 切片，实现 360° 全景视频监控及远程 VR 头显应用，解决现有通信网无法满足实时、大带宽数据流传输难题。

在国家电网公司“三型两网”战略的实施背景下，电力企业不仅需要充分利用自建私有网络，同时也需要结合业务 QoS 指标利用新兴通信技术，本文分析了智能电网业务通信需求与 5G eMBB、mMTC 以及 uRLLC 三大应用场景的适配性，提出了典型业务场景的应用策略，并针对配电网电流差动保护业务应用场景，设计了同步应用方式及组网应用架构，同时针对电力管理业务场景，通过 eMBB 技术分析了变电站巡检视频监控业务应用方式，提出了“5G+”视频监控与 VR 互联的应用解决方案。对“5G+”技术应用于电力生产业务与管理业务场景具有一定的指导和参考意义。

关键词：智能配电网；差动保护；5G

人民邮电出版社

电力潜在敏感客户预测的大数据方法应用

陈小峰，赵雅迪,张利鹏，朱峰
（北京国网信通埃森哲信息技术有限公司，北京 100032）

大摘要：随着现代经济和社会的快速发展，传统的电力行业机制已经不能满足市场需要。电力体制改革的不断深化、电网企业的公用性、基础性和服务性等社会特性愈加明显，一方面承担着服务地方经济发展、提高人民生活品质的重要政治和社会责任;另一方面，消费者心理需求从低级的生理、安全需求逐渐提升至寻求情感归属和尊重的需求。国家电网公司提出“三型两网，世界一流”的战略目标，推动泛在电力物联网建设，供电企业需要寻求科学依据、拓展服务深度广度，增强面向客户的服务能力建设，不断深化机制建设、持续强化现场管理，实现企业与客户之间的高效沟通，提升客户满意度。

为了改善服务质量，提高运维效率，企业开始从数据中寻找客户因停电、电费而发生投诉、咨询等行为的影响因素，提前做好预防措施和服务准备工作，提高工作质量和服务水平。随着信息技术的发展，国内开始使用数据挖掘技术分析海量数据并试图寻找引起敏感行为发生的影响因素。大数据方法作为实现泛在电力物联网的重要基础，已经被应用到电工领域的许多专业中去解决一些重要问题，更充分发挥公司数据价值，实现大数据智能分析、多源大数据治理与跨领域智能分析，主动培育大数据运营、大数据征信等新兴业务。严宇平等运用逻辑回归、决策树等数据挖掘技术，建立了客户停电敏感度预测模型，试验证明运用逻辑回归算法的效果比决策树算法好，同时分析了客户特征，为供电企业加强客户停电差异化管理提供了支持，但对指标的建设未过多描述。赵会茹等在对云南省 150 户农民调研的基础上，采用因子分析法和 Logistic 回归模型，分析了影响电力普遍服务受助个体诉求的主客观因素，并重点分析了主观影响因素的作用机理。随着服务业务工单量的不断增多，对文本挖掘技术在电力领域中应用的需求也在不断提升。吴刚勇等通过文本分类分析,构建文本分类器模型,实现对“热点词频”在不同业务中的分布情况研究，并根据结果开展相应改进措施。邹云峰等建立 95598 工单文本自动分类的模型，通过验证实现 95598 工单文本快速精准地自动分类，为分析供电服务对客户的用电诉求的影响提供依据和数据基础。

为了进一步加深对客户隐性特征以及诉求的认识和理解，本文以客户服务工单中的投诉业务为切入点，运用统计方法和数据挖掘算法对指标进行了梳理并构建投诉倾向客户模型，基于工单内容运用文本挖掘方法得出了停电投诉占总投诉业务的比率最大的结论，通过决策树算法筛选识别计划停电敏感潜在客户，将有助于电力企业准确辨识停电敏感度高的客户，有针对性地进行服务资源调度，充分做好应对措施；同时提供差异化停电服务，降低客户停电抱怨的概率，减少投诉压力，提升服务精度。

关键词：投诉工单；数据挖掘；熵权法；决策树

人民邮电出版社

基于回归分析的迎峰度夏用电量分析方法

陈雨泽[1]，李磊[2]，方学民[2]，刘建[1]，赵加奎[3]，刘玉玺[1]，左松林[4]
（1. 国网信息通信产业集团有限公司，北京 100085；2. 国家电网公司，北京 100031；
3. 国家电网有限公司大数据中心，北京 100031；4. 国网安徽省电力有限公司，合肥 340001）

大摘要：电力行业迎峰度夏期间电力客户用电需求达到高峰，电力企业供电压力陡增。为确保电网设备安全、平稳运行，有效缓解用电高峰期的紧张局面，需要提前根据天气情况对迎峰度夏期间的电力负荷、日用电量等指标进行定量分析，使电网公司对即将到来的用电高峰进行充分的准备。此外，掌握迎峰度夏期间公司供电区域用电、售电情况，了解迎峰度夏期间公司营销营业相关业务的运行特点还能够对公司营销营业的后续工作开展提供很好的借鉴。

本文提出一种迎峰度夏期间日用电量的量化分析方法。首先分析日用电量与日最高气温间的相关性。利用日用电量数据与其经营区域内日最高气温数据进行基于皮尔森相关系数的相关性分析，用量化的方法检查数据间的相关关系。之后，利用回归分析算法对日用电量与日最高气温之间建立函数关系，以日最高气温为输入，日用电量为输出，采用最小二乘法进行函数参数拟合。解得拟合函数参数后，根据可决系数评判拟合函数的拟合程度，即日用电量分析方法的有效性，可决系数在 0.5 以上表示使用该函数进行日用电量分析效果较好。

本文利用 2015 年迎峰度夏期间国家电网公司经营区域内 23 个电力公司的日用电量数据与其经营区域内日最高气温数据进行分析。首先对各电力公司进行日用电量与日最高气温的相关性分析，可得到较强的正相关关系，且在日最高气温高于一定值后，日最高气温越高日用电量越大。然后，利用各电力公司 2015 年 6 至 8 月日用电量与日最高气温数据通过回归分析算法建立函数关系，先对日最高气温相同的样本所对应的日用电量数据取平均值作为创建函数关系的新样本，目的是将不同日期的日用电量数据均衡化，使取平均值后的日用电量与短期经济变化无关。然后，以日最高气温为输入，日用电量为输出，利用最小二乘法进行函数参数拟合。再利用可决系数评判拟合函数的拟合程度。对各电力公司日用电量与日最高气温的拟合函数计算可决系数可知，利用本文提出的拟合方法可以较好地量化电力公司迎峰度夏期间日用电量随日最高气温变化的关系。利用某电力公司 2015 年 6 月 1 日—8 月 25 日的日最高气温和日用电量函数关系，计算 8 月 26 日—8 月 28 日的日用电量预测值，误差分别为 0.22%、1.75%、3.42%，预测精度较高。

本文提出了一种电力公司迎峰度夏期间日用电量的分析方法，通过对日用电量数据与日最高气温数据之间建立的函数关系得到了日用电量随最高温度变化的定量分析结果。通过实证研究发现，迎峰度夏期间电力公司的日用电量与其经营区域内日最高气温之间存在较强的正相关，经过函数拟合，其函数关系均呈二次或一次函数关系，且存在一个阈值使日最高气温高于该阈值时日用电量随日最高气温的增长而增加。实验结果表明，利用该方法建立的函数关系在电力公司迎峰度夏期间气温发生变化时能够很好地对日用电量的变化情况进行量化，并能够对未来几天的日用电量进行预测，为电网设备迎峰度夏期间的安全运行提供数据支撑，对电力公司充分做好迎峰度夏准备工作、提高营销营业管理水平具备一定指导意义。此外，在电力公司迎峰度冬期间，也可以采用类似方法对用电量的变化情况进行量化。

关键词：用电量；迎峰度夏；皮尔森相关系数；回归分析；最小二乘法

人民邮电出版社

基于调度自动化系统的低压分布式光伏电站接入估算模型

马大燕，谢祥颖，那峙雄，沈文涛，孟凡腾
（国网电子商务有限公司， 北京 100053）

大摘要：分布式光伏发电并网规模的激增，对配网规划、电网的安全运行带来了诸多挑战。因而，电网调度部门需要根据光伏电站的发电功率曲线制定调度和检修计划，合理调度投切电源、消纳负荷、检修电网，并进一步协调电网运营商制定发电计划和检修计划，提高各级电网光伏消纳能力。因此，分布式光伏的数据采集与统计管理得到了电力行业的高度重视。

目前，调度端未实现分布式光伏数据实时采集全覆盖，且采集不完整、频度低。针对这些问题，本文提出台区估算法作为一种低压分布式光伏电站实时采集的辅助手段，通过适当算法估算可实现低压分布式光伏电站的全面接入。估算原理如下：基于接入调度自动化系统的 10 kV 及以上高压台区的光伏电站实时发电出力，拟合发电功率曲线，获取该台区所在区域的装机容量单位 kW 的分布式光伏发电功率曲线；根据同一区域 9 km×9 km 网格低压 380 V/220 V 分布式光伏电站的装机容量，估算低压分布式光伏电站发电功率曲线；最后对实测值和估算值进行误差分析，验证模型的准确性。

以 H 省某地 10 kV 高压台区某光伏电站和同一区域网格 400 V 低压台区某光伏电站采用上文提到的台区估算法进行处理，步骤如下。

（1）400 V 低压台区分布式光伏电站的功率曲线：用电信息采集系统通过智能电表采集光伏电站的发电侧、上网侧的电流、电压、功率、电量等信息，每天等时间间隔（15 min）采集 96 次，光伏云网通过 ETL 程序从各网省营销基础数据平台获得该光伏电站的发电量信息，每天等间隔采集 n 次，获得该光伏电站一天内电量序列 Q，$Q=(q_1, q_2,\ldots, q_n)$，利用最小二乘法，m 阶拟合该光伏电站的电量函数 q_x：

$$q_x = \sum_{j=0}^{m} h_j x^j \qquad (1)$$

$$x_i = \frac{24}{n} \times i，\ 1 \leqslant i \leqslant n \qquad (2)$$

其中，x 为测量时刻，x_i 为第 i 次测量的时刻，x_j 为 x 的 j 次幂，h_j 为第 j 阶拟合系数。

通过对电量微分计算得到该光伏电站的发电功率曲线 z_x，$z_x = \frac{\sum_{j=0}^{m} h_j x^j}{\partial x}$，此曲线可以近似看做此电站的实时功率曲线。

（2）10 kV 光伏电站实时数据的参数建模：调度自动化采集系统对此光伏电站进行数据采集，每天采集 n 次，获得一天内该台区的实时发电功率序列 Y，$Y=(y_1, y_2,\ldots, y_n)$，利用最小二乘法，m 阶拟合该台区光伏发电的功率函数曲线 y_x：

$$y_x = \sum_{j=0}^{m} k_j x^j \qquad (3)$$

$$x_i = \frac{24}{n} \times i，\ 1 \leqslant i \leqslant n \qquad (4)$$

其中，x 为测量时刻，x_i 为第 i 次测量的时刻，x^j 为 x 的 j 次幂，k_j 为第 j 阶拟合系数。

由此，估算低压台区同一区域 9 km×9 km 网格同一天装机容量 N kW 光伏发电功率函数为 j_x：

$$j_x = N \times \frac{\sum_{j=0}^{m} p_j x^j}{M \times 1000} \qquad (5)$$

结合上述案例，通过 j_x 对 z_x 的误差分析，得到估算值与实测值偏差基本控制在 8%以内，从而验证了台区估算法进行低压分布式光伏电站接入估算模型的正确性。

针对装机容量较小的 380 V/220 V 低压分布式光伏电站，台区估算法作为一种数据实时采集的辅助手段，在允许误差范围内可实现在运 380 V/220 V 分布式光伏光伏全部接入调度自动化系统管理。

关键词：分布式光伏；台区估算法；出力估算；电力调度 [1]

基金项目：国家重点研发计划资助项目

人民邮电出版社

基于多模型融合的电网故障抢修时长预测

潘坚跃[1]，吴懿臻[2]，徐汉麟[1]
（1. 国网浙江省电力有限公司杭州供电公司， 浙江 杭州 310009;
2. 浙江华云信息科技有限公司，浙江杭州 310008）

大摘要：电网故障的分析和预测是电网自动化和智能化中的重要一环。由于电网故障种类繁多、原因复杂，电网故障的分析和预测较为困难，尤其对电网故障抢修时长的预测更加困难。随着智能电网的建设，调度自动化水平不断提高，信息采集系统的功能不断强大，已有众多学者展开对电网故障预测的研究。已有的研究多从电网内部收集的信息作为预测依据，如电压、电流、功率等指标，这些指标某种程度上反映了电网的运行状况，但忽略了天气、人为破坏等外部因素。本文从历史的故障抢修工单出发，依据多种内外部指标，对电网故障的抢修时长进行预测。

本文研究数据来自电力系统服务热线——95598热线系统。主要数据是抢修人员现场抢修完毕后，反馈系统的故障抢修工单。故障反馈工单数据是由抢修人员手动输入的半结构化数据，需要将数据进行格式化处理。数据包括 H 市 2016 年 3 月—2019 年 2 月所有故障抢修工单，共 21 万余条记录。除了内部电网故障数据外，还采集了公开的气象、地理、节假日等外部数据。影响故障抢修时长的因素众多，为了发现影响抢修时长的相关因素，分析了包括环境因素(温度等天气状况)、抢修人因素(抢修队、抢修人等)、发生时间、故障所在位置、故障类型等。发现平均抢修时长与平均气温有很强的相关性，随着气温的上升平均抢修时长也呈上升的趋势；故障发生时间也会影响故障的抢修时长，发生在凌晨以后的故障平均抢修时长较长，发生在白天的故障平均抢修时长较短；此外对故障类型、是否发生在节假日、发生区域、不同的抢修单位和抢修人等进行分析，发现这些因素都会对抢修时长产生一定影响，因此可根据以上影响因素对故障的抢修时长进行预测。

故障抢修反馈工单是抢修人员手动输入的，这导致部分异常数据存在。在实验过程中，需要先对异常数据进行清洗。为了更精准的预测故障的抢修时长，尽可能减少潜在的未知因素对抢修时长预测的影响，将抢修时长以 15 min 为单位进行重新计算，在预测时也以 15 min 为单位进行预测。对输入的特征数据进行清洗，排除异常数据，使用清洗后的数据进行特征工程建设，找出适合特征分别输入到基于集成学习的预测模型 XGBoost、 LightGBM 以及基于深度学习的预测模型的 LSTM 中进行建模。

对单个模型分别进行训练，并进行模型参数的调优。采用平均绝对误差（mean absolute error,MAE）作为主要的性能评价指标，LightGBM 平均绝对误差值为 1.21，XGBoost 为 1.52，LSTM 为 1.23，单个算法中 LightGBM 的效果最佳。分别训练完 3 种算法后，需要将 3 种算法输出结果根据权重进行融合。根据多次实验结果，经过分析给出 LightGBM、XGBoost 和 LSTM 的权重分别为：0.65、0.15 和 0.2 时输出的加权结果较好，预测最好结果的 MAE 为 1.15，时长预测以 15 min 为单位，对应的抢修时长误差大致为 17.25 min。

实验表明，多模型融合的抢修时长预测模型相比单模型更加准确，可以为电力抢修调度的智能化提供更加有效地支撑。

关键词：电网故障；抢修时长；LSTM；LightGBM；XGBoost

人民邮电出版社

基于知识图谱的泛在电力物联网安全可视化技术

余洋，朱少敏，卞超轶
（北京启明星辰信息安全技术有限公司，北京 100193）

大摘要：泛在电力物联网是能源革命和信息通信技术相互融合的产物，是产业互联网在电力行业的具体体现和应用落地。泛在电力物联网逐步向着“数据采集+集中控制+区域自治”的模式转变，终端由单一功能型转向综合服务型，以开放型业务中台和数据中台方式提供以客户为中心的快速业务服务模式，面临着更为复杂的安全威胁和风险。随着综合能源服务、互联网金融等新业务的蓬勃发展，在安全交互等方面对现有防护体系提出了更高的要求。泛在电力物联网“人—机—物”安全互动和海量信息的高效快速处理需求，需要开展基于可视化的全场景网络安全分析和防护体系建设，有效应对新业务发展带来的安全风险。同时泛在互联对精准智能防护提出更高的要求，各类物联设备的可视性、“云雾中心”的监测感知精准性有待进一步提升，而安全分析是达成上述愿景的前提。安全分析本质上是从现有安全数据中提取威胁情报，并综合分析的过程。然而随着泛在电力物联网网络规模增大，安全数据的量及种类激增，导致安全分析的过程越来越复杂，难度越来越大，尤其体现在异构数据的情报聚合问题上。网络安全可视化技术可以把不可见的、看似毫无关联的告警信息转换成直观的、便于理解的内外部威胁情报，方便网络安全管理人员对海量告警事件精准分析，从而快速有效地感知网络态势，判别网络异常和攻击，是泛在电力物联网全场景安全防护的重要新技术手段。

给出了基于知识图谱的安全分析架构图，整个架构大致分为 3 层，包括数据采集层、数据预处理层和安全分析层。数据采集层的作用是采集构建知识图谱所需的原始安全数据。数据预处理层负责安全数据的进一步加工，通过采集层采集的数据大多是结构化的文本数据，为使安全分析更加有效，需要对这些数据进行进一步加工处理，从而获得更深层次的知识。安全分析层基于预处理的数据，构建安全分析知识图谱，安全分析层可以制定查询规则，用来查询异常行为、异常实体，同时可以基于已有的风险评估模型进行资产的风险评估。

通过 3 种安全场景，阐述安全分析知识图谱的构建过程。

构建样本同源性知识图谱，安全数据可以从多角度体现样本的同源性，例如不同样本具有相同的回连服务器，就可以认为样本之间具有同源关系。通过分析恶意样本数据，建立恶意样本数据的本体，获取恶意样本的共有属性，构造恶意样本知识图谱，将样本间的同源性通过图形进行展示。

构建威胁狩猎知识图谱，威胁狩猎是威胁的搜索和关联过程，然而，仅仅发现孤立的异常行为，已不能满足当前的需求。为了阻止威胁造成的影响，深入地分析威胁，需要分析威胁的扩散路径。而知识图谱能够很好地表达这种路径结构。通过抽取安全数据中的关键属性，将安全数据知识图谱化，从而发现安全数据间的依赖关系，进而进行有效的安全溯源和威胁分析。

构建攻击图知识图谱，攻击图能够反映主机间脆弱性关系，也是分析攻击路径和进行风险评估的有效手段，使用攻击图对威胁建模，进而将攻击图知识图谱化，构建孤立威胁间关系，构造威胁的可能扩散路径，从而分析攻击路径和攻击意图。

关键词：泛在电力物联网；安全可视化；威胁情报；知识图谱；网络安全态势

人民邮电出版社

电力企业基于 RPA 技术助力财务智能化应用实践

全文举[1]
（南方电网数字电网研究院有限公司，广东 广州 510623）

大摘要：通过研究流程自动化技术在电力行业的应用，实现借助数字化手段替代人工执行的重复性任务和工作流程，解决低附加值业务岗位产出问题，夯实财务管理模式转型基础，对提升电力企业精益管理水平和财务管理效能，具有重大现实意义和必要性。

RPA（robotics process automation）即机器人流程自动化，作为一种具备操作高效、数据准确性高、安全性高及可拓展、部署灵活等多种应用优势的软件自动化工具，可通过预先设定的程序操作指令模拟人工作业处理流程标准化工作，达到加速业务流程流转并减少人力投入目的，实现财务管理的自动化和智能化，从功能优势和效益两方面同时促进电力企业改革，实现数字化转型。

RPA 相比人工操作，能根据规则进行无差别化业务处理，提高电力企业财务数据质量、业务效率及数据准确性，规范电力企业财务管理，其每一个操作流程还能生成详细的日志记录以供后期查询审核，合规性强，能满足财务数据存储需求及加强财务风险管控。同时易于部署和可定制化流程解决方案的特点，能有效降低成本，提高财务流程规模化的灵活性，还能优化财务人员结构和工作内容。

RPA 在财务领域应用前景十分广阔，其在财务领域的业务处理适用性主要体现在：（1）基础类会计，包括报销、制单、整理核对和传递单据等简单、高重复性会计工作；（2）管理类会计，包括核算、制表、统计和报表汇总等会计工作；（3）财务专家，主要涉及财务管理过程中的问题描述、诊断、分析、验证等工作，这主要建立在管理会计领域的成熟应用之上。未来随着技术发展与进步，RPA 会持续在财务管理和分析类领域为企业创造更大价值。

RPA 辅助企业财务管理，能为电力企业带来管理效益和经济效益。（1）管理效益：RPA 通过优化操作复杂、规范性差、运行风险较高的繁琐流程，高效利用数据资源，提高工作效率，减少用人成本，可降低企业管理和运营成本，提高运营效率；提升和优化管理者思维模式，推动企业管理转型，全面提升企业管理水平、财务支持决策能力、资源配置能力、风险管控能力、协同服务能力，深化和加强企业财务管理、财务风险控制监督、财务标准化管理；通过代替基础性工作，促进财务工作重心转移，优化人力资源配置，促进财务人员职能转型，优化管理结构。（2）经济效益：RPA 能满足特殊业务需求在短时间内多任务、多平台海量处理数据要求， 7 天 24 小时运行，能保持持续稳定高效作业，极大提升业务流程响应速度，缩短处理周期，且准确率高，大大提升工作效率和质量，节省人力成本；同时 RPA 可连接多系统数据流，低成本实现各业务系统集成，综合提升企业管理水平和运营效率。

在某种程度上，RPA 是一把双刃剑。企业在 RPA 运用中同时也需关注其系统风险、操作风险、信息安全风险和人员管理风险等风险管控。例如系统更新升级或发生意外，出现不兼容情况，或自然灾害、系统故障等意外情况；例如财务操作人员轮换或调离岗位，导致误操作；例如错误使用方式或恶意访问产生信息泄露风险；财务人员学习负担和沟通成本，产生的业务运营风险等等。

管理者应重视 RPA 深入企业日常工作带来的各类风险，加强风险管控，以积极开放的心态迎接 RPA 带来的变化，以促进电力企业的数字化、智能化转型。本文介绍了 RPA 技术在电力企业财务领域的应用，明确了 RPA 在数字化转型中的功能优势和影响，探索了 RPA 技术为电力企业带来的管理效益和经济效益，为电力企业的数字化、智能化转型提供一定的参考依据。

关键词：RPA；电力企业；财务机器人；数字化转型；智能化应用

人民邮电出版社

泛在电力物联网无线网络规划

马 跃，李炳森，胡全贵
（北京国网信通埃森哲信息技术有限公司，北京 100032）

大摘要：网络建设，规划先行。泛在电力物联网建设前需要对各种技术体系、电力业务应用场景充分分析，文中重点讨论的是在何种电力业务场景使用何种无线技术，以高质量的网络支撑泛在电力物联网的建设。

泛在电力物联网无线物联网技术包括电力无线专网、运营商公网、LPWA（low-power-wide-area）技术等。

泛在电力物联网无线网络规划分为承载业务需求分析、泛在电力物联网规模估算、泛在电力物联网站址规划、泛在电力物联网网络仿真、工程参数规划 5 个阶段。

承载业务需求分析是泛在电力物联网无线网络规划的基础。不同电力业务的带宽需求、时延要求、并发率、安全性要求等不尽相同；同时，不同电力业务的地形地貌环境、部署位置等也存在较大差异。需要根据承载业务需求选取最适合的无线系统，并合理地规划系统架构和设备位置，才能更好地满足泛在物联网建设目标。

泛在电力物联网规模估算的目的是从无线信号覆盖和网络容量两个角度分别测算需要建设的站点数，取两者的较大值为泛在电力物联网的网络规模。一般建设前期，侧重覆盖目标，容量需求较小，随着终端（用户）数量的上升及其对速率要求的提升，后期逐渐向容量目标倾斜。覆盖目标和容量目标都需要满足，根据计算结果判断是容量受限还是覆盖受限。

泛在电力物联网站址规划根据完成的泛在电力物联网规模估算，确定基站选址方案，基站工程参数配置，以完成泛在电力物联网站址规划。在选址方案周边选取距离最新的电力物业位置，原则上，实际电力物业位置与基站选址方案距离＜500m，若 500m 内没有合适的电力物业，则在该方案地址采用新建杆塔方式。

泛在电力物联网网络仿真通过软件进一步评估规划方案是否可以满足覆盖及容量目标，对不满足建设目标的区域，则需对规划参数进行调整，以满足建设要求。

泛在电力物联网工程参数规划主要考虑频率规划问题，其他参数可根据仿真结果和工程实际情况进行微调。频率规划方面，泛在电力物联网只能使用国家批准的频段，频谱资源较少，主要需要考虑频率干扰问题。

根据对多种无线技术体制在覆盖、容量、组网模式等方面的特点与不同，及其对不同泛在电力物联网应用场景的适配性，确定泛在电力物联网无线物联网技术应用场景。

泛在电力物联网无线网络规划是建设泛在电力物联网之前的重要步骤，何种业务场景使用何种无线技术直接决定泛在电力物联网的网络质量。本文提出的泛在电力物联网无线网络规划方法，充分分析了电力无线专网、5G、NB-IoT、LoRa 等无线技术体制在覆盖、容量、组网模式等方面的特点与不同，并论证其对控制类、采集类等不同泛在电力物联网应用场景的适配性，为泛在电力物联网的建设提供了一定的参考。

关键词：泛在电力物联网；网络规划；专网；LPWA；5G

人民邮电出版社

基于国网商旅大数据融合背景的用户画像构建框架

张长浩[1]，余志勇[2]，周振[2]，石瑞杰[1]，王新勇[1]
（1. 国网电子商务有限公司，北京 100053；2. 国家电网有限公司，北京 100031）

大摘要：基于大数据分析的商旅计划决策是掌控差旅动态、制定差旅规范的重要组成部分。基于国网商旅信息数据，针对出差过程中出行方式的优化选取、酒店住宿的个人喜好，构建一种用户画像框架技术，实现快速、准确识别敏感客户群体。首先针对用户不同特性采用双通道建模方式预测用户敏感程度；其次围绕业务审批、差旅控制、酒店评价、时间特征、数值特征等类型刻画用户，构建用户多源特征体系；最后充分利用商旅数据多源性，创建基于双层 Xgboost 的多视角融合模型，提升分类精确率，并通过对比实验验证方法的有效性。

国网商旅客户信息是基础数据，用户每次出行均针对目标地点的变化，变更出行方式，根据目标地点按照目标距离、星级、评价、舒适度等选择推荐酒店。通过统计发现，全年查阅标准次数少的用户较多，相应敏感度占比较小，将其定义为低活跃度用户；而多次查阅标准用户较少，但敏感度占比较大，将其定义为高活跃度用户。低活跃度用户与高活跃度用户特性存在明显差异，主要表现在：

（1）用户画像刻画角度不同。对于低活跃度用户，重点刻画、关注标准关键内容；而对于高活跃度用户，系统重点计算搜索频率和浏览时间等相关联系等；

（2）用户特征构造方式不同。低活跃度用户仅有极少的搜索记录，相应数据项目取值较少，而高活跃度用户则对应多条相应数据记录，同一项目对应多个取值信息。

围绕国网商旅客户信息建立业务审批信息、差旅控制信息、财务结算信息 3 个不同维度构建特征群，围绕用户类别特征、数值特征、聚类特征、文本特征、时间特征、统计特征等多种特征类型对用户敏感度进行刻画。

以多种视角的方式构建数据特征，构建国网商旅用户信息表多源特征体系。提出一种基于双层 Xgboost 的多视角融合模型，有效利用多源特征，解决高维特征的问题，Xgboost 是一种经过优化的提升树模型，具有任务通用性高、运行速度快的优点[6]，广泛应用于数据挖掘和机器学习中。

数据采用国网商旅 2018 年全年用户数据，包括业务审批、差旅控制、票务预订、酒店评价等信息。计算数据表中字段与用户敏感度之间的基尼指数，结合用户数据完整性因素，最终确定差旅管理、预算控制、报销流程三类信息的业务类型编码、单位编码、预定方式、结算方式等字段用于特征提取。

选用 F1-score 作为结果评价指标，F1-score 是分类问题的一个衡量指标，是精确率（precision）和召回率（recall）的调和平均数，只有精确率和召回率两者都取较高数值时 F1-score 才能得到较高得分。首先计算 precision， precision 为被分类器判定为正例的正样本的比重；recall（召回率 / 查全率）指被预测为正例的占总的正例的比重。最后计算各个类别下的 F1-score 平均值，得到最终评测结果。

在分析和挖掘国网商旅用户数据的基础上，提出构建用户画像多视角融合框架模型，该框架可以快速、准确识别商旅敏感用户。通过分析商旅用户特征，采用双通道建模算法对低活跃度用户与高活跃度用户分别预测，提出多种特征数据提取方法，构建商旅用户多源特征体系；提出了基于双层 Xgboost 的多视角融合模型解决具有多源特征的高维特征问题，并通过实验证明了方法的有效性，为精确识别商旅敏感用户提供了重要的参考依据。

关键词：用户画像；多视角学习；模型融合

人民邮电出版社

风电场电力监控系统网络安全威胁防控体系

丁伟
（南方电网科学研究院有限责任公司，广东广州 510663）

大摘要：风电场电力监控系统网络安全事件的频发，严重威胁电厂和电网的安全。为了有效提升风电场电力监控系统网络安全水平，防止并网电厂的网络安全威胁通过调度数据网向电网侧蔓延，确保厂网两侧电力监控系统的安全可靠运行，有必要开展风电场接入调度数据网网络安全风险分析和安全威胁管控体系研究,对保障风电场和电网的安全稳定运行具有重要作用，并将对涉网发电企业规划、设计、建设及运维等工作具有指导意义。

首先，根据对目前风电场电力监控系统安全防护现状、日常督查检查和发生的相关异常事件的分析，从结构安全、本体安全、安全管理、安全应急和基础设施物理安全方面对风电场电力监控系统网络安全的主要风险进行分析。

然后，从安全防护、安全监测、接入管控、安全管理四个方面归纳总结了针对风电场电力监控系统的安全威胁防控方案，其中安全防护和安全监测从电厂提高自身安全防护水平出发，接入管控和安全管理调度机构技术监督职责角度出发。

安全防护。从主机、网络和应用 3 个方面进一步提升风电场电力监控系统的安全防护能力，从而抵御各种网络攻击和恶意代码感染。主机防护，生产控制大区各业务系统服务器、工作站的操作系统皆应采取恶意代码防护措施，并定期进行病毒库的更新。同时应经过安全加固，对于电力监控系统中的关键服务器进行软件升级、补丁安装前进行安全评估和测试验证。网络防护，租用运营商专线与集团远程集控中心通信应落实纵向加密认证措施。应用防护，开展电力监控系统源代码审计研究，系统上线前对应用系统源代码预置漏洞或恶意代码检测。

安全监测。建立对风电场电力监控系统外网互联、网络流量、设备运行状态等多层次的综合监测，全面掌握风电场电力监控系统的安全状况。外网互联监测，在电场内生产控制大区易发生跨区互联的业务系统部署外网互联监测程序，周期性测试外网联通情况，从而实现对网络边界非法访问、跨区互联等违规情况的监测。网络流量监测，通过对生产控制大区内网络流量进行实时监测，对异常 IP、异常通信等情况进行识别、报警和分析，从而发现非法外联、异常网络应用和通信行为。 设备监测，对风电场内生产控制大区网络设备、安防设备及主机类设备的运行日志及操作情况进行集中监控及审计分析，包括运行状态信息 、配置信息、配置流量传输信息及安全告警信息，从而判断系统是否存在故障或异常。

接入管控。为了避免电厂侧的网络安全风险向调度侧蔓延，在调度侧采取接入管控措施。通过在调度侧实行接入管控，划分独立的电厂 VPN，并实施点对点的路由控制，可有效抵御电厂侧的网络安全风险通过调度数据网向调度侧蔓延。

安全管理。新建、改扩建电厂，严格落实涉网电力监控系统网络安全实施方案的审查及并网验收工作，在电力监控系统新建或重大改造后开展投运前的网络安全等级保护测评和电力监控系统安全防护评估工作。对于已投运电厂，按流程严格管控涉网电力监控系统网络安全结构、安全策略变更，防范未经调度机构批准的涉网电力监控系统网络结构或安全策略变更，变更后的网络结构和安全策略应及时完成在对应调度机构的备案。

基于实际情况探讨了风电场电力监控系统所面临的安全风险，从安全监测、安全防护、接入管控和安全管理四个方面归纳总结了风电场电力监控系统安全防护体系，并深入分析了未来全面提升电力监控系统安全性的关键技术，以提升风电场电力监控系统安全防护水平，确保厂网两侧的安全稳定运行。

关键词：风电场；电力监控系统；安全风险；安全监测；接入管控

人民邮电出版社

无实时网络下约定式运算的控制研究和应用

张正峰
（广东电网有限责任公司电力调度控制中心，广东广州 510600）

大摘要：如果一个远端物体是长期固定位置的，远端物体应无需自己把定位信息告知业主方与租赁方，可以通过业主方通知租赁方。如果在边远山区、无信号的地下停车场中，远端物件无后台联网，即便有移动信号覆盖，也都需要业主到场进行交接，这就限制了物联网覆盖范围。所以，被联网管理的物品的后台通信和其定位的需要与否都值得研究，对不同的“物”是否可进行有区分的按通信需求联网和“对话”。目前固定的远端物体共享经济的技术方案都存在同一个问题：远端物件必需纳入互联网的网络部署或网络基础建设，远端物件必需随时在线以便接收业主方的控制。

无实时网络下约定式运算的控制的核心思想就是，在远端物件无网络状态下，采用定时约定机制和业主手中的虚拟锁镜像同步运算获得相同的密匙用于远端物件的开启关闭。约定时间内正常结束或逾期不正常结束已使用过的密匙都为过期，同步跳到下一个加解密算法和密匙核对，提供输入的文字或图案是含有密匙和租约的必要信息，提供关闭时的输入的租约信息错误的话也得不到正确的关闭密码，远端物件和业主手中的虚拟锁所知租约信息内容作为下一个制密原料通过镜像同步的加密算法制作出只有两者所知密匙。

根据无实时网络下约定式运算的控制思想构建了一种远端非联网加密算法约定的约时开关装置，包括本端密码运算器和远端非联网开关装置。

本端密码运算器包括本端微控制器及分别与本端微控制器电连接的本端键盘、本端显示屏和本端存储器；本端微控制器用于根据业主通过本端键盘输入的含有约时信息的明文生成开启加密字符串，并控制本端显示屏进行显示。

远端非联网开关装置包括远端微控制器及分别与远端微控制器电连接的远端键盘、远端显示屏、远端存储器、继电器组及连接在继电器组输出端的电控锁件；远端微控制器用于对共享资源临时使用人通过远端键盘输入的开启加密字符串进行解密，并通过继电器组开启电控锁件或共享资源物件，还用于在租赁约定截止时间或租赁实际结束时间，通过继电器组关闭电控锁件或共享资源物件。远端非联网开关装置还包括闭合传感器、状态检测器和凭条打印机；闭合传感器用于检测电控锁件的闭合状态并通过状态检测器发送给远端微控制器，以使远端微控制器在电控锁件闭合时，控制凭条打印机打印凭条。打印凭条上记载有租赁约定使用时间、租赁实际结束时间及租赁实际结束时间所对应的电控锁件闭合状态。远端非联网开关装置还包括与远端微控制器电连接的远端二维码扫描器和远端蓝牙模块，远端二维码扫描器用于扫描由业主提供给共享资源临时使用人的，包含开启加密字符串或关闭加密字符串的二维码并发送给远端微控制器。

一种远端非联网加密算法约定的约时开关装置，就是一种受密码控制开启使用和结束使用的控制电源开合的装置，密码的加密算法和循环机制只由业主和该种远端非联网加密算法约定的约时开关装置私密设定，受密码控制开启使用和结束使用，无需以业主方为服务中心与远端物件和租赁方都有联网的远程通信，只需利用业主方与租赁方建立的远程通信进行密码的传递，密码是可读可输入的字符串，所述的远程通信甚至涵盖传统的书信方式。

在研究无网络状态下的定时约定机制和镜像同步运算获得密匙的基础上，提出基于密码控制、非实时虚拟通信和按约定计算密匙的逻辑控制方法，能很好地适用于智能锁或开关在无实时通信网覆盖下的动态认证以及开关工作，建立一种无实时通信网络下的“密控网”，既可作为物联网技术在无通信覆盖情况下的有益补充，也可作为固定地点的远端物件按计算次序移交管理权或使用权，而无需建设后台通信网络以及等候期的通信费用支出。

关键词：远端非联网；加密算法；约定；约时

广东电网电力调度控制中心版权所有

基于量子通信的电力业务调度算法

于卓智，张叶峰，韩冰洋，陈文伟，王栋
（北京中电飞华通信股份有限公司，北京 100070）

大摘要：随着电网的不断发展壮大，承担着电网控制、运维信息的电力通信系统也在不断复杂化。电力通信系统的安全与电网安全密切相关，特别是以特高压电网为核心、各级电网协调发展的坚强智能电网建设，对通信系统传输的安全性和可靠性提出了更高要求，并且由于计算机处理能力的不断提高，尤其是量子计算机的发展，传统加密方法的安全性正受到越来越严峻的挑战。基于单光子不可再分原理、海森堡不确定关系、测量塌缩原理和量子不可克隆定理等量子物理学基本原理，通过量子加密技术实现密钥的分发并结合“一次一密”的密码体系可以实现理论上的绝对安全性，因此，将量子加密应用于电力通信系统以提高其通信的安全性和保密性有着重要的意义。

目前由于技术水平的限制，量子密钥的成码率较低，在按照传统单队列“先入先出”的顺序进行加密时，业务的时延要求往往难以得到保证，而电力通信网中的电力业务大多对时延要求敏感。基于此，本文提出一种基于区分服务模型的业务队列调度算法LD-WFQ 算法对电力业务进行调度，按照业务的时延要求将业务划分到不同队列中，通过调度器进行调度，决定业务接受量子加密服务的顺序，对量子加密带宽进行分配。

现有队列调度算法多针对业务队列的权值进行动态调整，通过改变各业务队列所占加密带宽实现时延的均衡，但缺乏对业务超时率进行有针对性地控制和优化的调度算法，本文算法通过对业务队列中待加密数据分组在队列调度系统中的转发时延进行估计，优先处理即将超时的待加密数据分组，降低量子加密超时率。

待加密数据分组在队列调度系统中的时延包括数据分组停留在队列调度系统中的时间和加密后发送该数据分组的时延。加密后发送数据分组的时延可直接通过数据分组本身的大小和经典信道的传输速率计算得到，数据分组停留在队列调度系统中的时间则可进一步分为待加密数据分组从进入系统到到达所属队列队头的时间、数据分组到达队头后直到被选择出队的时间和生成加密所需量子密钥的时间三部分，其中，数据分组从进入系统到到达所属队列队头的时间可由调度器进行记录，生成所需密钥的时间则仅仅取决于量子密钥的生成速率，而数据分组到达队头后直到被选择出队的时间则可根据加密所需密钥量、空闲队列结合、队列权值和量子密钥生成率进行估计。

调度器每次进行调度时，首先估算各队列队头数据分组的预计转发时延，若均小于对应的转发时延要求，则按照 WFQ 算法进行调度，而若有数据分组的预计转发时延大于其时延要求，则对该数据分组进行优先调度，避免其因为超时而加密失败。

仿真结果表明，本文算法通过估计待加密数据分组的预计耗时，优先调度即将超时的待加密数据分组，能够有效降低待加密数据分组的加密超时率，虽然算法的优先调度机制将不可避免地造成其他队列中待加密数据分组的转发时延增加，但不会造成更高优先级队列中数据分组超时率的增加，能够在可控的范围内以转发时延为代价降低数据分组加密超时率，提高量子密钥的有效利用率，这也在一定程度上缓解了量子密钥成码率低的问题，相比 WFQ 算法有更加优越的性能。

关键词：电力系统量子通信；量子密钥分发；队列调度；WFQ 算法；超时比率

人民邮电出版社

基于组合密钥的智能电网多源数据安全保护

高建，王立城，余梦月，庞建民，宋国瑞
（北京智芯微电子科技有限公司，北京 102200）

大摘要：电力通信网是电力系统的重要基础设施，部署了数量庞大、分布广泛的各类业务终端、通信终端，其数据安全关系着整个电网的安全稳定运行。对于点多面广、环境开放的各类终端，安全防护措施相对薄弱。并且攻击者能够通过终端迂回攻击主站，造成更大范围的安全威胁

传统密码学的安全性基于数学算法的计算复杂度，随着分布式计算和量子计算机的愈加成熟，已不能保证密钥的绝对安全性。适应室外充电站、站所终端 DTU、配变终端 TTU、馈线终端 FTU、智能电表等终端特点，从而实现点多面广的智能配用电、分布式能源接入的终端数据安全传输的广泛应用，针对配用电终端所需的大量密钥需求，更安全、高效、可靠地响应业务安全的需求，具有重要实用价值。

提出一种适用于配用电业务的密钥分片组合应用方法，方案是利用初始密钥作为种子密钥，通过分片和组合技术，将这些种子密钥映射成大量的对称密钥，以实现大量终端的数据加密通信，弥补密钥生成分发速率较低的缺陷，满足点多面广的配用电终端所需的大量高安全性密钥的需求。

首先进行密钥分片，方法是把一个密钥分成 m 个不同的片组，称为 m 个子秘钥，设定共有 n 个密钥，经分片后形成的子密钥资源数量 $L=mn$。然后把这些片或片组的子密钥进行唯一标识，用于密钥的组合从而生成对应的密钥。密钥分片方式可采用两段至多段的方式，优选地采用两段或三段的方式。

通过密钥因子矩阵依次随机从集合 R 中选取与分片数量对应的没有重复的元素，组合生成密钥。密钥因子矩阵的元素可由服务器采用硬件随机数发生器生成方法或软件系统的伪随机数产生 Hash 函数生成，密钥因子矩阵 TK 表示。矩阵的行表示组合密钥的每一段包含的密钥变量，矩阵的列表示组合密钥的段数，设矩阵为 i 行 j 列的密钥因子矩阵，$i=mn$，$j=m$，i 行是从子密钥集合中选取的有效子密钥，j 列表示组合密钥运算的段数。用 Hash 函数将密钥片标识映射成矩阵的行和列，再提取矩阵的行与列所对应的密钥因子来进行组合，即生成相对应的密钥。

针对配用电终端数量大、分布广的特点，提出一种基于组合密钥的密钥生成技术。该方案采用初始密钥作为种子密钥，以较少密钥组合大量相异的密钥，解决密钥有限和大量终端需求数量的问题，保障终端设备都能共享足够的安全密钥。由于采用了组合的思想来实现对称密钥的一次一变，具有良好的安全优势，可对种子密钥进行有效的保护。密钥因子矩阵经过组合产生大量的共享密钥，从而使得较小的存储空间可存储大量的密钥，有利于降低大量密钥所需的存储空间受限问题，具有应用简单、可扩展性好的特征，适用于点多面广的大规模配用电终端网络。

关键词：配用电大数据；通信安全；多源数据；密钥分片组合

水电部电力出版社

基于电力大数据的经济景气指数分析

刘玉娇[1]，宋坤煌[2]，王 向[3]

（1. 国家电网有限公司大数据中心，北京 100031；2. 国网信通亿力科技有限责任公司，福建 福州 350003；
3. 国网能源研究院有限公司，北京 102209）

大摘要：随着电力信息化的日益完善，电力企业积累了大量的电力大数据，大数据相关技术发展正在改变电力企业的管理方式。景气是对研究对象发展状况的一种综合性描述，用于说明研究对象的活跃程度。景气分析是一种经济周期的统计分析方法，利用月度或者季度数据经济统计序列，分析研判经济发展在周期性波动中所处的阶段，能够为政府经济政策决策及实施提供参考。

本文基于全社会用电量、行业用电量、居民用电量、业扩报装容量等电力数据和外部经济数据，提出一种基于 X13-ARIMA 季节调整算法的电力景气指数模型，并开展应用验证，实现从电力视角看经济的目标。

宏观经济状况可能影响和反映行业的发展走势，行业用电量指标和行业经济指标可以反映行业的发展状态，采集 2013 年 1 月-2019 年 3 月全国及分省分行业月度电量数据、业扩报装容量数据、工业增加值月度数据开展景气指数分析。

确定与行业相关的经济指标后，对采集的电力数据进行预处理，计算行业月度电量、业扩月度报装容量同比增长率，并进行完整性检查，对缺失值进行填补，对 2018 年前后细分行业分类不一致的数据，根据新旧行业对应关系表进行整合。进一步采用时差交叉相关系数法，验证行业月度电量、业扩月度报装容量同比增长率与经济指标的先行、一致或滞后关系

对电量、业扩报装容量增长率序列采用 X-13-ARIMA 算法进行季节调整，获取 TC 循环趋势项。为了进行季节性调整，通常假定时间序列由 4 个主要部分组成：趋势周期部分、季节部分、日期效应部分和不规则部分。

季节性调整程序分为两个步骤，第一阶段称为预调节。预调整的目的是选择一个 ARIMA 误差最能描述原始序列特征的回归模型。所选模型用于调整序列的确定性影响，并扩展时间序列分解过程中使用的具有回溯性和预测性的序列。预调整的阶段主要包括未观察到的成分如何相互关联。

第二阶段将预先调整的序列分解为未观察到的组件。根据确定性效应调整后的序列分解为 3 个未观察到的部分：趋势周期、季节性和不规则性。第一阶段确定的调整因素（日期效应、异常值等）被分配到各自的成分，以便最终将原始序列完全分解为最终趋势周期、季节、日历和不规则成分。季节性调整序列作为没有季节和日历效应的序列获得。

季节性调整的目的是识别和估计时间序列的不同组成部分，从而更好地了解时间序列中的基本趋势、业务周期和短期运动。季节性调整提供了对宏观经济序列当前发展的补充，允许在不受季节和特定日期影响的情况下比较经济的周期发展，在货币供应量等经济领域有广泛的应用。由于天气和社会因素，一年内经济变量受系统性和经常性的模式影响，通常被称为季节性模式（或季节性）。当季节性变化主导原始序列（或季节性未调整序列）的周期性变化时，很难识别非季节性影响。而长期运动、周期性变化或不规则因素，通常代表重要的经济信号。从电力数据角度上看，由于天气、产业周期性影响，用电数据表现出明显的季节周期性特征，通过季节调整能够抽取电力数据中的循环周期成分，保证基于电力数据的经济景气指数构建更加可靠。

本文将经济学领域的景气指数模型引入电力经济景气指数领域，研究了景气指数的筛选及构建过程，创新采用了 X13-ARIMA 季节调整算法用于电力景气指数模型的分析研究，通过构建季节调整模型对用电量序列进行了趋势循环项拆分，结合工业增加值等外部经济数据，构建电力经济景气指数，并基于用电量数据进行了实例验证。验证结果表明，该方法能科学有效地利用电力数据模拟经济趋势。

关键词：景气指数；电力大数据；时间序列；季节调整算法

人民邮电出版社

电力大数据安全治理体系

朱洪斌[1]，安龙[2]，杨铭辰[3]

（1. 国家电网有限公司大数据中心，北京 100031; 2. 国网山西省电力公司信息通信分公司，山西 太原 030021; 3. 国网陕西省电力公司西咸新区供电公司，陕西 西咸新区 712000）

大摘要：为促进数据安全合规使用、保障业务安全稳定运行，依据国家数据安全相关法律法规要求，以数据安全为核心，设计了电力大数据安全治理体系，全面提升数据全生命周期的安全保障能力，推进数据安全攻防、检测、评估、监测等技术的研究应用，对内对外提供数据安全服务。

电力大数据安全治理的要求包括：（1）数据收集时，应遵循“合法、正当、必要”的原则，公开收集使用规则，明示收集信息的目的、方式和范围，并经被收集者同意。采取必要的安全技术手段和管控措施，对收集到数据进行完整性和一致性校验，跟踪记录数据收集获取的过程，确保数据收集过程的可追溯性。（2）数据内部传输和外部传输应采用不同的加密、签名、鉴别、认证等机制对传输中的数据进行安全管理，防止传输过程中的数据泄露。建立传输通道前，对传输两端的主体身份进行鉴别和认证，确保数据传输双方是可信任的。（3）格按照国家数据安全要求，加强大数据中心内部数据存储安全保护。采取认证鉴权、访问控制、加密、安全审计等安全措施，做好数据存储保护。依据数据级别做好数据备份策略，确保备份与恢复功能，保证数据的高可用性和灾难可恢复性。（4）用核心业务支撑平台实现数据的统一分析处理，对外不提供明细数据，仅提供经脱敏或加工后的数据，防止敏感数据泄露。加强对重要数据使用行为的识别、监控和预警，并签订相应安全职责及保密协议。（5）对数据导入导出，结合业务需求和数据分级明确数据导入导出策略与规范，严格安全评估及授权审批流程。针对数据共享，明确数据共享范围和安全管控措施。针对数据发布，依据国家法律法规建立数据发布审核制度，各专业自行明确数据发布的内容、范围、规范以及发布者与使用者的权利和义务。（6）明确数据销毁工作责任，制定数据销毁策略和管理制度。根据数据安全分级和场景需要，确定数据销毁手段和方法，确保销毁数据不可复原。（7）制定数据安全事件应急预案，明确各岗位职责及应急处置策略和流程，确保发生安全事件时能及时响应并开展处置工作，记录事件内容，评估事件影响。

电力大数据安全治理平台通过数据权限统一管控、安全策略集中管理、基于虚拟数据库的数据安全分发、灵活的数据防护能力以及数据使用过程中的安全监控等措施，实现大数据中心对外提供数据服务过程中的涵盖数据采集、传输、存储、使用、交换、销毁等全过程的安全管控。电力大数据安全治理平台主要分为 4 层：数据交互层、数据服务层、数据存储层和数据接口层。数据交互层负责接收用户或者应用的输入，并将输出通过各功能或者结果返回给用户或者应用；数据服务层负责数据申请、脱敏、使用、回收等数据全生命周期的管理，将数据从下发到回收形成一个端到端的闭环管理；数据存储层负责将数据系统的用户信息、权限信息、敏感信息、使用信息、监控信息以及系统运行日志等存储到数据库；数据接口层负责与数据源之间的交互。

通过分析电力大数据面临的安全挑战，设计了电力大数据安全治理体系，通过研发电力大数据安全治理平台对电力大数据安全治理管控进行了实践验证，通过验证表明，电力大数据安全治理平台有效健全了数据安全管控机制，构建了数据安全合规技术支撑和安全运营服务能力，稳步提升了大数据中心整体数据安全管控能力。

关键词：电力大数据；数据安全；安全管理；治理体系

人民邮电出版社

电网机巡图像分析框架与深度学习方法

李远宁[1]，宁柏锋[2]，董召杰[1]
（1.南方电网数字电网研究院，广东 广州 510000；2. 深圳供电局有限公司，广东 深圳 518000）

大摘要：随着智能制造与物联网技术的发展，无人机已被电网企业广泛应用于输电线路巡视检查。与人工巡检相比，无人机巡检具有工作高效便捷、不易受地域影响、安全可靠性高等优点。无人机巡检在电网企业的广泛应用，也产生了大量的巡检图像数据亟需分析与处理。目前，机巡图像自动化分析方法主要可以划分为人工特征分析方法和深度学习方法两种。人工设计特征分析方法只能针对特定场景与目标分析，其泛化能力还有待进一步提升。深度学习方法自主学习数据深层次抽象特征，具有较强的检测性能与泛化能力，是人工神经网络的重要分支。

本文基于深度学习方法设计了一套从用户数据样本归集、兴趣内容标注、模型训练、内容分析与自动标注到用户评价反馈的闭环 U2U 分析框架。在训练阶段，首先对接机巡作业管理系统，实现用户历史数据归集，并结合输电线路缺陷分析报告开展机巡图像数据的兴趣部件与缺陷手工标注，最终形成企业级机巡图像训练样本库，为不同图像深度学习模型训练提供支撑，基于 U2U 分析框架可以进一步应用和探索适用于机巡图像分析应用场景的机器视觉分析方法。在测试与应用阶段，借助机巡图像分析模型对增量数据进行自动标注，实现兴趣部件的自动检测，并生成缺陷隐患报告，用户围绕分析结果进行评估，并将最终确认结果反馈给样本库，从而实现训练样本的不断补充与完善。相应地，基于增量更新地训练样本库，不断优化机巡图像分析模型，从而缓解个别部件训练样本不充分带来的影响。

针对机巡图像多尺度多目标分析，本文首先采用 Faster R-CNN 验证探索深度学习方法的在多尺度多类别兴趣对象检测的有效性与泛化能力。Faster R-CNN 以 VGG16 为预训练卷积网络（共有 13 个卷积层，4 个池化层），提取输入图像 1/16 的特征图并提交 RPN 和 ROI（region of interest）池化层进行处理。RPN 是一个全卷积网络，用于生成候选选兴趣对象区域。ROI 池化层将候选兴趣对象区域对应的特征块映射成一个固定尺度的特征向量，作为下一层全连接层（full connected layer, FC）的输入。全连接层通过 softmax 函数计算每个 ROI 特征向量的具体兴趣部件的概率，同时对候选兴趣区域边框回归获得更精确的目标框。

以 Faster R-CNN 为代表的 two-stage 分析方法对象检测与定位的准确率上存在优势，但其分析与处理速度上难以满足实时分析要求。因此，本文进一步验证与探索 SSD 在实时机巡图像分析的效果，SSD300 采用 VGG16 为基础网络，修改全连接层 FC6 和 FC7 为卷积层 conv6 和 conv7，移除 FC8 和所有 dropout 层，额外添加 4 个卷积层用于构造特征金字塔。SSD300 在 6 个特征图的每个点上构造不同尺寸的锚点信息框（anchor box），每个 anchor box 都输出兴趣部件的置信度和相对于默认框的位置偏移量。多尺寸的特征图配合多尺寸的 anchor box，基本可覆盖机巡图像中各种形状和尺度的兴趣目标，从而达到对原图多尺度分析的效果。

为进一步提升机巡图像分析对兴趣部件尺度变化的适应，我们利用 K-means++聚类分析方法对兴趣对象锚点信息框进行设定。根据实验分析兴趣部件的目标框长宽比集中在 1:1~4:1 之间，Faster R-CNN 和 SSD 通过 anchor box 捕捉兴趣目标的形状和尺度变化。使用 K-means++聚类分析方法对应 anchor scale 分别为 [8,18,39,61,81,102,113]。考虑到机巡图像分析中小尺度目标较多，因此在后续实验中选取前 5 个 scale，对特征图上每个滑动窗口的不同 scale 生成长宽比分别为 1:1、1:2、1:4、2:1、4:1 共 25 个候选 anchor box。

实验证明针对兴趣部件样本有限、尺度不一、背景复杂等问题，将 Faster R-CNN 和 SSD 模型应用到 U2U 分析框架，可精确检测机巡图像中出现的玻璃绝缘子、复合绝缘子、防震锤、均压环、屏蔽环等部件，为后续更大规模的缺陷检测及系统化应用提供基础。通过聚类分析方法自动化设定 Faster R-CNN 中的 anchor box 参数，可以有效提高分析模型对多尺度部件的适应性与检测精度。

关键词：智能电力系统；深度学习；多部件检测；无人机

人民邮电出版社

电力通信网省地集约化监控运行支撑系统架构及关键技术

杨志敏，洪丹轲，黄昱
（中国南方电网电力调度控制中心，广东广州 510525）

大摘要：电力通信网是电力系统的重要组成部分，是电网安全生产和企业经营管理的基础保障性资源，在电网安全生产和电网公司数字化转型中，电力通信网发挥越来越重要且不可替代的作用。以南方区域为例，电力通信网按照统一调度、分级管理的原则分为主干通信网、省通信网和地区通信网。

随着技术的发展，信息与通信系统集约化运维逐渐成为发展方向。为解决地区通信网监控不到位的系统性风险，南网公司组织实施了以省为单位，依托并做大中调通信调度团队开展省地两级通信网集约化监控工作，具体包括集中监视、集中监视+应急控制、常态化控制 3 种模式。

为支撑通信网集约化监控运行工作，本文基于现有的通信网属地化监控系统，对系统架构和关键技术进行研究。系统架构方面以中调通信调度台为信息枢纽，打通省地两级通信网与中调通信调度台的实时运行信息、实时控制指令等监控信息流。关键技术方面研发了安全高效运行的综合监视技术、网管集约技术和跨层资源调度技术，为集约化监控模式下中调通信调度员安全、高效履职提供技术保障。

安全高效运行的综合监视技术。该技术实现运行信息可靠采集、根原因告警压缩、异构告警归一化，最终筛选出需要值班调度员确认处理的标准化根告警推送至中调通信调度台。技术要点包括以下 3 方面。

• 信息采集方面，通过地网监视模块转发和集中监视模块从地区网管直采双方式实现实时运行信息可靠采集；中调集中监视模块对直采数据处理完成的根告警，与地调监视模块转发的根告警进行比较与合并，有效防止告警疏漏；双数据互为校核，防止监视信息流缺漏。

• 异构告警处理方面，结合电力通信网特性，分析推演每一种告警所反映的设备技术问题对电力通信网可靠性的影响，规范化重定义告警信息，形成告警归一化处理规则库。通信网监视模块运用该规则库对网管报送的原始异构告警逐条进行映射，输出归一化的规范告警。

• 根原因告警压缩方面，对海量告警信息进行实时压缩并自动筛选根告警，推送给中调通信调度员处理。根原因告警压缩技术主要包括告警压缩与根告警分析两个步骤：一方面从告警间是否存在父子关系、是否存在重复频闪关系等维度对告警进行去重压缩，留下无重复的父告警；另一方面从告警时间、告警对象、影响的业务等维度进行关联性和因果性分析，过滤出根告警。

网管集约技术。以设备厂商为边界，以省为单位，将省地通信网同厂商设备网管进行整合，全省用一套网管服务器、多个客户端实现全省同厂商全部设备统一管理。在中调主备调部署主备网管服务器，管理全省同厂商的网络设备，主备服务器实时热备运行。网管客户端属地化按需布设，分权分域控制权限，实现本地区通信网设备的控制操作。特殊方式可手动切换至属地化网管方式运行，与集中网管方式形成应急备用。

跨层资源调度技术。通信资源数据属地化录入和维护，全省统一展示分析与本地展示分析，实现一份数据同源、多方使用。中调通信调度员在省资源管理系统发起资源调配工作，设置目标、参数和约束条件，省资源系统进行可行性分析后，向地网资源系统发出资源调配指令、参数和约束条件，地网资源系统根据要求自动生成地网资源调配方式，反馈给省资源系统，完成资源跨层调配互操作，实现在中调资源管理模块中对所属地区通信资源的统一调度。保障中调通信调度员对地区通信网资源安全、可靠、高效率调度。

随省地电力通信网集约化监控工作推进，系统架构及关键技术在南方区域通信网监控系统改造中得到广泛应用，结果表明系统架构适合并高效支撑省地电力通信网集约化监控模式安全运行，提升了安全运行质量和运行工作的技术水平。

关键词：电力通信网；集约化；技术支撑系统；通信网监控

人民邮电出版社

230 MHz 电力无线通信技术的优化研究

赵训威，白杰，丁高泉，相里瑜
（国网信息通信产业集团有限公司，北京 102211）

大摘要：230 MHz 频段主要有两段共 7 MHz 合计 278 个载波可供电力无线应用。在这 7MHz 里，有 43 个零散分布频点已被其他行业占用，故电力行业总共可以使用 235 个离散分布的载波频点，其中，能够连续分配的最大频点数为 41 个。

230 MHz 电力无线专网技术目前主要有两种制式：LTE-G 与 IoT-G，两者均基于 LTE/NB-IoT 技术。针对 230 MHz 频段离散频率资源进行设计，主要区别在于空口无线参数设计，包括帧结构、时频资源结构、FFT 点数、子载波间隔及由此衍生出的调度控制机制等。

LTE-G/IoT-G 目前均是按照各个载波单独处理，包括频域资源子载波映射、IFFT、FIR 滤波以降低对邻带干扰、上采样与中频滤波等。每个载波单独处理，都有各自的保护带。在分配多个连续载波资源时，这些保护带不能传输有效数据，会造成这部分频率资源浪费，频谱利用率不高，影响业务速率。

设计一种优化基带频域资源映射与中频的方法，在降低运算量复杂度的同时提高频谱利用率，其原理如下。

• 分配给终端连续占用的载波子带，不再单独进行单个载波的基带频域资源映射与滤波处理，而是把连续占用载波组合作为整体带宽资源进行资源映射与滤波处理，仅在整体带宽的两侧预留保护带。

• 自适应 FFT 与滤波处理，针对不同连续带宽分配，对应采用不同 FFT 点数与 FIR 滤波器系数。

采用优化设计方案后，原来多个连续载波中间的保护带宽部分，就可以用于有效的基带频域子载波映射，从而提高了频谱效率；另外，多个连续载波资源映射后，仅需要进行一次 FFT 运算与 FIR 滤波处理，相比现在每个载波都需要单独进行处理，优化方案的运算量大大降低。

根据无委的频率规划使用表，电力占用的频率资源，最多可以分配连续的 41 个载波，故存在连续分配 1～41 个载波/子带的情况，需要在此约束下分别设计针对 LTE-G 和 IoT-G 的具体优化方案，内容包括：根据优化设计原理重新设计不同连续带宽所对应的参数，考虑到提高频谱占用率，同时减小 FIR 滤波器阶数，按照频谱占用率不超过 96%的原则，分别计算有效子载波个数 N_{sc}、保护带大小、FFT 点数、基带采样速率，并根据这些参数计算频谱利用率和业务速率可提高的百分比。

以 LTE-G 为例，可计算出 LTE-G 的优化设计参数如下。

• 分配两个连续子带时，子载波个数 N_{sc} 为 23，单侧保护带为 2 kHz，频谱占用率为 92%。

• 分配连续子带个数 N_{sb} 为 3~40 时，子载波个数 $N_{sc} = 12\times N_{sb}$，单侧保护带为 $0.5\times N_{sb}$，频谱占用率为 96%。

• 分配连续子带个数 N_{sb}= 41 时，子载波个数 $N_{sc} = 12\times N_{sb} = 492$，单侧保护带为 20 kHz，频谱占用率为 96%。

• 分配连续子带个数 N_{sb} 为 1~5 时，FFT 点数为 64，基带采样速率为 128 ks/s。

• 分配连续子带个数 N_{sb} 为 6~10 时，FFT 点数为 128，基带采样速率为 256 ks/s。

• 分配连续子带个数 N_{sb} 为 11~20 时，FFT 点数为 256，基带采样速率为 512 ks/s。

• 分配连续子带个数 N_{sb} 为 21~41 时，FFT 点数为 512，基带采样速率为 1024 ks/s。

LTE-G 采用优化设计方案后，频谱利用率从 88%提高到 96%，传输速率可提升 9.09%。

同样，可以计算出 IoT-G 采用优化设计方案后的具体参数如下。

• 分配连续子带个数 N_{sb} 为 1~2 时，FFT 点数为 16，基带采样速率为 60 ks/s。

• 分配连续子带个数 N_{sb} 为 3~4 时，FFT 点数为

人民邮电出版社

32，基带采样速率为 120 ks/s。

• 分配连续子带个数 N_{sb} 为 5~9 时，FFT 点数为 64，基带采样速率为 240 ks/s。

• 分配连续子带个数 N_{sb} 为 10~19 时，FFT 点数为 128，基带采样速率为 480 ks/s。

• 分配连续子带个数 N_{sb} 为 20~38 时，FFT 点数为 256，基带采样速率为 960 ks/s。

• 分配连续子带个数 N_{sb} 为 39~41 时，FFT 点数为 512，基带采样速率为 1920 ks/s。

IoT-G 采用优化设计方案后，其频谱利用率从 90% 提高到 95.46%，传输速率可提升 6.07%。

优化设计方案增加了分配带宽资源组合的过渡带比例，从而降低了滤波器设计难度，减小了运算量；LTE-G 运算量减小 77.46%，IoT-G 运算量减小 16.18%。

国家电网公司正在推动两种技术制式的标准统一，吸取两种技术制式的优点并进一步优化设计，同时考虑采用一些 5G 先进技术来完善 230 MHz 电力无线专网标准，以促进产业链的集中培育与壮大。

整体上，电力无线专网在优化系统设计时，尽可能考虑最大化重用现有产业链，充分利用已成熟的各个环节，降低终端、系统设备研发与网络部署成本，相比公网，主要的差别在于射频、中频与基带处理。

关键词：LTE 230；连续子带；频域资源映射；中频滤波

人民邮电出版社

一种可量化的云计算平台安全评估模型

许剑，靳莉
（北京中电飞华通信技术有限公司，北京 100071）

大摘要：随着云计算技术的不断发展，云服务日益普及，越来越多的组织开始使用云服务。但是涉及云服务的安全和隐私问题仍然需要多方面的考虑，比如可信身份验证、适当的授权、数据安全和隐私。对于同一个云，其云用户、管理员和访问者很难掌握可访问和可管理资源的整体安全情况，如果采用不同的服务，安全状况会更加复杂。因此，本文提出了一种基于一致的 API 访问不同云的可量化安全评估模型。

一个安全可量化评估模型包括安全可视化显示模块、安全漏洞数据库、安全扫描引擎、恢复引擎、安全评估模型、模型建立模块和模型维护模块。

安全可量化评估模块从计算安全集、存储安全集、网络安全集、运维安全集、应用安全集等方面定义了安全项目集合和可量化评估方法。评估系统模型可以根据监控资源的规模部署在单个服务器上，也可以作为一个集群部署在多个服务器上。

评估系统的安全扫描引擎扫描用电用户的安全集合，包括计算安全、存储安全、网络安全、维护安全、应用安全等不同安全项目的得分。扫描可采用串行或并行方式执行，并根据评价模型的定义对每个资源给出一个评分。对于一个云，总体安全性的可量化评估结果为 0 到最大值（最大值为 1、10 或 100）。

安全类型集合及其指标：一个安全评估模型是由 $P=\{P_1,P_2,P_3,P_4,\cdots,P_N\}$ 等安全字段组成的集合。P_i 代表计算安全集合、存储安全集合、网络安全集合、维护安全集合、应用程序安全集合之一。

一个 P_i 包含不同的安全检查指标 P_{ij}，如物理服务器 OS、VM OS、容器系统和其他漏洞项。

安全评估过程：定义用电用户作为 UP 访问的资源集合。UP_i 对应于 P_i，P_i 定义了扫描 UP_i 所需的检查项。每个用户的资源视图都是全局资源视图的一个子集，拥有最高权限的管理员的资源视图是全局资源视图。安全扫描引擎根据安全评估模型对用户资源视图进行扫描，可以通过串行或并行方式扫描检查项 P_{ij}，并给出一个实际的 US_{ij} 得分。

云安全视图是用电用户云资源视图各种检查项的实际安全得分。管理员可以获取与总云对应的全局安全视图。为了提高一个用户对其云安全的关注程度，采用了“一票否决”的策略来降低一个云存在严重漏洞时的得分。

否决策略与用户的安全视图相对应，总分之和是全局可量化的分数。通过利用直接总结、平均或“一票否决”策略计算总得分，在否决策略中，如果一个关键检查项的得分低于阈值，即 L_{ij} 为 0，则 US_i 为 0。

修复安全漏洞：当用电用户选择修复扫描的漏洞时，安全修复引擎将调用与 P_{ij} 对应的 O_{ij}。O_{ij} 是针对不同安全漏洞的修复规则对应的一个环节。维修引擎将对安全漏洞进行串行或并行修复。

对于一个管理员或普通用电用户，安全系统调用修复引擎修复安全漏洞，如下载补丁、更改配置、关闭服务或端口等。该安全修复引擎可以对漏洞进行静默修复，也可以通过用户界面与用户交互。修复后的发动机工作结束后，安全评估模型根据固定的结果给出一个新的评分。

针对单云和多云环境，提出了一种可量化的安全评估方法。可量化的评估模型为不同的云用户实现用电信息安全评估。通过可视化图形显示某云的动态安全扫描评分，引导用户修改配置、改进操作、修复漏洞，从而提高整个云平台的安全性。

关键词：云计算；可视化；可量化评估；安全可视

人民邮电出版社