封面报道 Cover Story

全面深化改革，推进中国式现代化

7 月 15 日至 18 日，中国共产党第二十届中央委员会第三次全体会议在北京召开。

这次全会是在新时代新征程上，中国共产党坚定不移高举改革开放旗帜，紧紧围绕推进中国式现代化进一步全面深化改革而召开的一次十分重要的会议。

全会圆满完成了各项议程，审议通过了《中共中央关于进一步全面深化改革、推进中国式现代化的决定》。

为贯彻党的二十届三中全会精神，《中国信息界》特别组织了本期封面报道，与广大读者共同认真学习领会。

《中共中央关于进一步全面深化改革、推进中国式现代化的决定》中新质生产力及数字经济等相关内容解读

一、新质生产力

第 8 条强调“**健全因地制宜发展新质生产力体制机制**”。

推动技术革命性突破、生产要素创新性配置、产业深度转型升级，推动劳动者、劳动资料、劳动对象优化组合和更新跃升，催生新产业、新模式、新动能，发展以高技术、高效能、高质量为特征的生产力。加强关键共性技术、前沿引领技术、现代工程技术、颠覆性技术创新，加强新领域新赛道制度供给，建立未来产业投入增长机制，完善推动新一代信息技术、人工智能、航空航天、新能源、新材料、高端装备、生物医药、量子科技等战略性产业发展政策和治理体系，引导新兴产业健康有序发展。以国家标准提升引领传统产业优化升级，支持企业用数智技术、绿色技术改造提升传统产业。

全会提出，“要健全因地制宜发展新质生产力体制机制”。“这个提法很有新意。”中国科学院科技战略咨询研究院研究员眭纪刚说，全会把体制机制这一属于生产关系范畴的概念与新质生产力结合起来，就是要通过体制机制改革形成新型生产关系，比如塑造更加合理的经济体制、科技体制、创新体系等，为发展新质生产力奠定良好的制度基础。

“因地制宜发展新质生产力的关键在于结合发展实际，释放数据这一生产要素的价值，通过完善数据基础制度，加快综合算力基础设施体系和全国一体化算力网建设，以智能算力激活新质生产力，释放数字经济发展新动能。”浪潮云信息技术股份公司总经理颜亮说。云计算作为新质生产力发展的底座支撑，正在依托大数据、智能技术等新技术逐渐催生出一批新产品、新业态、新模式。

新材料是加快发展新质生产力、扎实推进高质量发展的重要产业方向。“材料科学为新材料产业发展提供了学科基础，未来材料科学的发展，应聚焦于更好地推动新质生产力发展。”上海交通大学材料科学与工程学院院长戴庆说。

为更好地在新材料领域培育新质生产力，戴庆建议，进一步提高基础研究转化为现实生产力的效率，构建以市场为导向的产学研用合作模式，建立具有区域优势的联合研发平台和创新中心，加速科技成果从样品变成产品、形成产业，打通从科技强到产业强、经济强、国家强的通道。

国研新经济研究院创始院长朱克力建议，要健全因地制宜发展新质生产力的体制机制，可以从以下几方面入手。一是建立灵活的政策调整机制，让各地能够根据本土实际情况制定和调整发展策略；二是加强产学研合作，推动科研成果转化和应用，确保科技创新真正服务于地方经济发展；三是优化人才培养和引进政策，为地区经济提供持续的人力资本；四是完善基础设施建设，为产业发展提供良好的硬件环境。通过这些措施，有望构建一个更适应地方特色、更具活力和创新性的生产力发展体制机制，加快实现“新”与“质”的双重飞跃。

二、数据要素

《决定》第三部分“**健全推动经济高质量发展体制机制**”第 6 条强调“**培育全国一体化技术和数据市场**”。

完善要素市场制度和规则，推动生产要素畅通流动、各类资源高效配置、市场潜力充分释放。构建城乡统一的建设用地市场。完善促进资本市场规范发展基础制度。培育全国一体化技术和数据市场。完善主要由市场供求关系决定要素价格机制，防止政府对价格形成的不当干预。健全劳动、资本、土地、知识、技术、管理、数据等生产要素由市场评价贡献、按贡献决定报酬的机制。推进水、能源、交通等领域价格改革，优化居民阶梯水价、电价、气价制度，完善成品油定价机制。

近日，国家数据局局长刘烈宏在国新办举行的“推动高质量发展”系列主题新闻发布会上，介绍推动国家数据事业高质量发展情况时表示：今年是中华人民共和国成立 75 周年，是实现“十四五”规划目标任务的关键一年，也是数据工作夯基垒台、提档加速的重要突破期。下一步，国家数据局将贯彻落实党的二十大和二十届二中、三中全会精神，研究出台我局学习宣传贯彻全会精神的实施意见，总结和运用改革开放以来特别是新时代全面深化改革的宝贵经验，进一步推动数据要素市场化配置改革，统筹数字中国、数字经济和数字社会规划和建设，加快发展新质生产力，加快推进实体经济和数字经济深度融合，加快培育全国一体化数据市场，为中国式现代化建设贡献数据力量。

三、数字经济

第 9 条强调“**健全促进实体经济和数字经济深度融合制度**”。

加快构建促进数字经济发展体制机制，完善促进数字产业化和产业数字化政策体系。加快新一代信息技术全方位全链条普及应用，发展工业互联网，打造具有国际竞争力的数字产业集群。促进平台经济创新发展，健全平台经济常态化监管制度。建设和运营国家数据基础设施，促进数据共享。加快建立数据产权归属认定、市场交易、权益分配、利益保护制度，提升数据安全治理监管能力，建立高效便利安全的数据跨境流动机制。

《决定》第七部分“完善高水平对外开放体制机制”第 28 条强调“**加强绿色发展、数字经济、人工智能等领域的多边合作平台建设**”。

完善推进高质量共建“一带一路”机制。继续实施“一带一路”科技创新行动计划，加强绿色发展、数字经济、人工智能、能源、税收、金融、减灾等领域的多边合作平台建设。完善陆海天网一体化布局，构建“一带一路”立体互联互通网络。

当前，新一轮科技革命和产业变革深入发展，我国实体经济与数字经济融合程度不断加深。“推进产业智能化、高端化和绿色化发展，为健全促进实体经济和数字经济深度融合制度提供了目标指引，以人工智能为代表的数字技术和以数据要素为代表的新型生产要素，则为实体经济转型升级提供了新动能新机遇。”北京理工大学公共管理系主任尹西明说。

在尹西明看来，瞄准产业链供应链薄弱环节，加强数字技术创新和应用赋能，为推进产业数字化和数字产业化“两化协同”提供了重要场景牵引。

“未来，需要进一步建设产业科技创新体系，提升产业科技创新能力，加快场景驱动型国家人工智能创新体系建设；要发挥数字平台企业和数据交易所等的作用，健全数据要素流通交易体系，推动通用人工智能等新一代信息技术和数据要素同制造技术、产业场景融合，为加快发展新质生产力、扎实推进高质量发展注入新动能。”尹西明说，要在确保重点产业链供应链安全可控的基础上，进一步提高产业链供应链韧性。

四、科技体制改革

《决定》第四部分“**构建支持全面创新体制机制**”第 14 条强调“**深化科技体制改革**”。

坚持面向世界科技前沿、面向经济主战场、面向国家重大需求、面向人民生命健康，优化重大科技创新组织机制，统筹强化关键核心技术攻关，推动科技创新力量、要素配置、人才队伍体系化、建制化、协同化。加强国家战略科技力量建设，完善国家实验室体系，优化国家科研机构、高水平研究型大学、科技领军企业定位和布局，推进科技创新央地协同，统筹各类科创平台建设，鼓励和规范发展新型研发机构，发挥我国超大规模市场引领作用，加强创新资源统筹和力量组织，推动科技创新和产业创新融合发展。构建科技安全风险监测预警和应对体系，加强科技基础条件自主保障。健全科技社团管理制度。扩大国际科技交流合作，鼓励在华设立国际科技组织，优化高校、科研院所、科技社团对外专业交流合作管理机制。

五、数字人才

《决定》第四部分“构建支持全面创新体制机制”第 15 条强调“**深化人才发展体制机制改革**”。

实施更加积极、更加开放、更加有效的人才政策，完善人才自主培养机制，加快建设国家高水平人才高地和吸引集聚人才平台。加快建设国家战略人才力量，着力培养造就战略科学家、一流科技领军人才和创新团队，着力培养造就卓越工程师、大国工匠、高技能人才，提高各类人才素质。建设一流产业技术工人队伍。完善人才有序流动机制，促进人才区域合理布局，深化东中西部人才协作。完善青年创新人才发现、选拔、培养机制，更好保障青年科技人员待遇。健全保障科研人员专心科研制度。

强化人才激励机制，坚持向用人主体授权、为人才松绑。建立以创新能力、质量、实效、贡献为导向的人才评价体系。打通高校、科研院所和企业人才交流通道。完善海外引进人才支持保障机制，形成具有国际竞争力的人才制度体系。探索建立高技术人才移民制度。

“推进中国式现代化离不开科技创新，科技创新靠人才，人才培养靠教育，教育、科技、人才三者构成一个完整的逻辑链，因此必须统筹推进教育科技人才体制机制一体改革。”宁波大学校长蔡荣根分析了统筹推进教育科技人才体制机制一体化改革背后的深层次原因。

“推进中国式现代化要靠高素质创新人才，而培养高素质创新人才的基础在教育。”蔡荣根认为，未来基础教育机制改革的取向，应该以培养和激发青少年的好奇心和创造性为主；高等教育应该成为教育科技人才一体化发展的枢纽，深化体制机制改革，应该建设更多有优势特色的高校。

中国科学院科技战略咨询研究院研究员万劲波持有相似的看法。“科技是经济的供给侧，人才是科技的供给侧，教育是人才

的供给侧。教育、科技、人才内在一致、相互支撑。”万劲波说，此次全会提出统筹推进教育科技人才体制机制一体改革，就是要打破教育、科技、人才制度各自改革的边界，将三者融合起来才能真正统筹推进，通过一体化改革实现一体化发展，更好支撑中国式现代化。

中国科学技术发展战略研究院研究员石长慧表示，推进教育科技人才体制机制一体化改革要做好战略规划统筹，在制定教育、科技、人才发展规划时，在发展目标、发展思路和具体举措方面进行统一规划；要完善科教协同育人机制，坚持以科技创新需求为牵引，优化高等学校学科设置，改进中小学科学教育，创新人才培养模式，着力培养造就拔尖创新人才，同时大力推进国家实验室、科研院所、新型研发机构、科技领军企业和高等学校联合培养研究生，在科技攻关一线锻炼培养科技人才。

六、网络治理

《决定》第十部分“深化文化体制机制改革”第 40 条提出“**健全网络综合治理体系**”。

深化网络管理体制改革，整合网络内容建设和管理职能，推进新闻宣传和网络舆论一体化管理。完善生成式人工智能发展和管理机制。加强网络空间法治建设，健全网络生态治理长效机制，健全未成年人网络保护工作体系。

由党建读物出版社和学习出版社联合出版的《党的二十届三中全会〈决定〉学习辅导百问》对此分析说，建立人工智能安全监管制度，是应对人工智能快速发展的必然要求。人工智能作为影响面广的颠覆性技术，可能带来改变就业结构、冲击法律与社会伦理、侵犯个人隐私、挑战国际关系准则等问题，将对政府管理、经济安全和社会稳定乃至全球治理产生深远影响。必须高度重视人工智能可能带来的安全风险挑战，通过加强监管进行前瞻预防与约束引导，最大限度降低风险。

七、网络安全

《决定》第十三部分“推进国家安全体系和能力现代化”第 50 条强调“**健全国家安全体系**”。

强化国家安全工作协调机制，完善国家安全法治体系、战略体系、政策体系、风险监测预警体系，完善重点领域安全保障体系和重要专项协调指挥体系。构建联动高效的国家安全防护体系，推进国家安全科技赋能。

“网络安全、数字安全、智能安全与粮食安全、能源安全一样，是国家安全的重要基石，也是科技链、创新链、产业链的‘底板’。”奇安信集团董事长齐向东说，未来我们将持续锻造网络安全硬实力，力争为国家和社会筑起最坚实的网络安全防线。

改革风正劲，创新潮更涌。改革的催征鼓点再次敲响，今日中国，向着强国建设奋进的脚步愈发铿锵。广大科技工作者将自觉肩负起时代赋予的重任，勇攀科技高峰，挺进科研“无人区”，以实干担当奋力推进中国式现代化。

（摘自新华社、科技日报等媒体报道）

二十届三中全会《决定》解读
——统筹强化关键核心技术攻关

文◆张 泉 宋 晨

7月21日发布的《中共中央关于进一步全面深化改革、推进中国式现代化的决定》提出，深化科技体制改革。优化重大科技创新组织机制，统筹强化关键核心技术攻关，推动科技创新力量、要素配置、人才队伍体系化、建制化、协同化。

党的十八大以来，我国基础研究和原始创新不断加强，关键核心技术实现重大突破，创新主体和人才的活力进一步释放，我国成功进入创新型国家行列。但仍存在创新能力不适应高质量发展要求、关键核心技术受制于人状况没有根本改变等问题。

决定提出，加强国家战略科技力量建设，完善国家实验室体系，优化国家科研机构、高水平研究型大学、科技领军企业定位和布局；改进科技计划管理，强化基础研究领域、交叉前沿领域、重点领域前瞻性、引领性布局。

“我们要不断完善科技创新组织方式和治理体系，加快健全新型举国体制，统筹推进教育科技人才体制机制一体化改革，加强科技创新全链条部署、全领域布局，破解原始创新能力相对薄弱、一些关键核心技术受制于人等突出问题，加快实现高水平科技自立自强，为推进强国建设、民族复兴伟业提供有力支撑。”科技部部长阴和俊说。

决定提出，强化企业科技创新主体地位，建立培育壮大科技领军企业机制；深化科技成果转化机制改革，加强国家技术转移体系建设；加快建设国家战略人才力量，着力培养造就战略科学家、一流科技领军人才和创新团队，着力培养造就卓越工程师、大国工匠、高技能人才，提高各类人才素质。

“近年来，高校在国家创新体系中发挥了重要作用。比如，在量子科技、生命科学、物质科学、空间科学等领域，取得一批重大原创成果。下一步，我们将着力强化高校有目标有组织的人才培养、科技创新和社会服务。”教育部部长怀进鹏说。

（来源：新华社）

新型举国体制助力发展新质生产力

文◆浙商宏观　李　超

《决定》指出，“统筹推进教育科技人才体制机制一体化改革，健全新型举国体制，提升国家创新体系整体效能”。我们认为，新型举国体制是发展新质生产力的重要助力，健全新型举国体制的关键在于深化科技体制改革。其中，健全科技社团管理制度，改进科技计划管理，加强有组织的基础研究，建立企业研发准备金制度，建立职务科技成果资产单列管理制度，深化职务科技成果赋权改革和建立科技保险政策体系等重要方面。

我们认为，健全科技社团管理制度有助于鼓励和规范发展科技类社会团体，有助于新型举国体制加强创新资源统筹和力量组织，深化科技评价体系改革。据民政部统计数据显示，全国科技领域社会组织有 4 万余家，其中，民政部登记全国性社会组织 236 家、国际科技组织 17 家。2023 年底《科技部办公厅 民政部办公厅 中国科协办公厅关于开展促进科技类社会团体发挥学术自律自净作用专项行动的通知》中指出，要“推动科技类社会团体主动承担学术自律自净的职责使命”，“接受委托开展学术调查”，“制定实施学科学术评价规范”和“加大对青年科研人员支持力度”等举措，加强科研作风学风建设，在促进学术自律自净等方面发挥作用。

我们认为，在改进科技计划管理方面，加强有组织的基础研究，是新型举国体制凝聚科技创新能力重点发展新质生产力的着力点。

《决定》指出，要“强化基础研究领域、交叉前沿领域、重点领域前瞻性、引领性布局”，“提高科技支出用于基础研究比重，完善竞争性支持和稳定支持相结合的基础研究投入机制”。我们认为，由于基础研究领域具有投入周期长，研发成果不确定性较大的特点，需要有长期稳定的科技支出投入，相比于企业与个人，政府更具有与之匹配的支出能力，结合我国当前中央与地方的财政现实来看，中央财政在基础研究科技支出上或更为重要，这也是新型举国体制与我国央地财权事权相匹配改革的统一表现。《决定》指出，“完善中央财政科技经费分配和管理使用机制，健全中央财政科技计划执行和专业机构管理体制”。

我们认为，建立企业研发准备金制度有助于强化新型举国体制中的企业科技创新主体地位。研发准备金是企业为保障研发项目的资金需要，在开展研发活动前或研发过程中提前储备的专门用于研发项目、单独核算的资

金。研发准备金制度是指规范研发准备金的形成、使用、核算、信息披露等相关事项的管理措施。此外，对领军企业、专精特新中小企业、中小微企业系统推进也是强化企业科技创新主体地位的体现。

我们认为，建立科技保险政策体系是金融助力新型举国体制发展新质生产力的重要增量。在科技的开发创新与应用中，涉及生产、研发、人员、贸易链、信用链等多个方面，按照时序可大致将科技风险划分为科技研发风险、成果转化风险和市场风险。科技保险有效地分散了研发项目的科技风险，提高了科技研发各方主体对于科技研发的积极性，同时降低了科技研发项目因科技风险而失败的可能，提高了科技研发的效率。具体来看，包括但不限于首台（套）重大技术装备综合保险、重点新材料首批次应用综合保险、软件首版次质量安全责任保险等。

我们认为，建立职务科技成果资产单列管理制度，深化职务科技成果赋权改革，有助于进一步破除制约科技成果转化的制度障碍，激发科研人员创新创业创造活力，促进科技成果落地转化。职务科技成果，是指执行研究开发机构、高等院校和企业等单位的工作任务。《报告》相关内容可以通过科技创新成果的利润共享改革，激发科研人员活力。职务科技成果资产单列管理制度，完善科技成果资产确认、使用和处置等规范化的资产管理，建立健全市场导向的价值评估机制，此前已在河南等地试点，可以进一步破除制约科技成果转化的制度障碍，激发科研人员创新创业创造活力，促进科技成果落地转化。职务科技成果赋权改革，此前已在湖北等地试点，按照规定赋予科研人员职务成果所有权或不低于 10 年的长期使用权。允许高校、科研院所和医疗卫生机构对过往利用单位职务科技成果自主创办企业进行合规整改。推动落实以增加知识价值为导向的收益分配政策。

此外，我们认为，健全新型举国体制，也需要教育科技人才三位一体协同推进。一是，教育综合改革，以科技发展、国家战略需求为导向，“超常布局急需学科专业”。二是，科技体制改革，坚持四个面向，即面向世界科技前沿、经济主战场、国家重大需求和人民生命健康，强化关键核心技术攻关，国家、企业、科技人员三大主体分工明确。在国家层面，科技经费、验证平台和政府采购等是重要的支持方向。“深化科技成果转化机制改革，加强国家技术转移体系建设，加快布局建设一批概念验证、中试验证平台，完善首台（套）、首批次、首版次应用政策，加大政府采购自主创新产品力度。”在科技人员层面，科技人员更大的自主权是关键变量，尤其是在技术路线、经费资源调度和科技成果转化收益分配方面，我们认为这有助于充分激活科技人员创新活力。三是人才发展体制机制改革，重在加快建设国家战略人才力量，呈现梯队明确的特征。《决定》指出，要“着力培养造就战略科学家、一流科技领军人才和创新团队，卓越工程师、大国工匠、高技能人才，一流产业技术工人队伍。”

特别报道——继往开来新气象 谋篇布局再出发 2024 年中国信息协会年中工作会成功召开

文◆中国信息协会

7 月 12 日，2024 年中国信息协会年中工作会在北京成功召开。中国信息协会会长王金平，副会长吴钰、李红、杨志强，监事长廖方宇出席会议，协会各分支机构、杂志社负责人和代表及协会各部门全体工作人员 80 余人参加会议。

王金平会长在会上作 2024 年中国信息协会年中工作报告。王金平以“继往开来，谋篇布局”精炼概括了协会上半年的工作成果，全面回顾了自换届以来，第七届领导班子带领全体干部职工开展的 13 项富有创新和开拓意义的重点工作：加强党的领导、制定战略规划、争取工作支持、健全治理结构、加强内外交流、构建良好生态、重启评选工作、首次参加评估、提升协会影响、维护协会权益、塑造协会品牌、喜迁办公新址、提升管理水平。

王金平在报告中深入分析了协会当前阶段的实际情况和外部发展环境，对协会未来的核心导向提出了“1234”的发展思路，即 1 个基调、2 个认识、3 大战役、4 大业务，强调“新起点、新征程、新辉煌”应成为协会全体成员共同追求的主基调。

王金平强调，协会全体成员要深刻领会和理解“脱钩管理”以及“信息时代”的深层含义，统一思想认识，增强市场敏锐度，强化协会的核心竞争力；在协会内部倡导“一家人、一条心、一盘棋、一起干”的团结协作精神，让会员单位、分支机构、地方信息协会都能感受到

强烈的归属感，努力构建全国信息行业组织的大系统，汇聚各方力量，形成协同发展的格局，共同推动我国信息化事业发展；在继续巩固和深化协会传统业务的同时，要全力攻坚“保留评比表彰”“实现评估预期”“解决遗留问题”三大战役，聚焦成果评选、政策咨询、标准制定、国际交流四大战略性业务。

会上，王金平对协会下半年工作进行了细致部署。王金平指出，要坚定不移地用习近平新时代中国特色社会主义思想凝心铸魂、武装头脑、指导实践、推动工作，不断加强党建引领，深化学习教育，从大视野、全方位、新角度谋划协会党建工作；在内部建设方面，要不断夯实基础管理，在战略规划、管理效率、品牌价值、渠道拓展、会员服务等方面持续发力，构建专业高效的协会秘书处；在业务发展方面，要主动求新求变，不断强化分支机构管理与赋能机制，做好协会品牌活动策

划、培训、评价、赛事、行业交流合作等工作。王金平强调，协会上下要认清形势，坚定高质量发展的信心不动摇，不等不靠、主动出击，以顽强的作风、切实的举措，全力落实协会工作部署，确保全年目标任务圆满完成。

王金平会长的工作报告不仅是对协会上半年工作的总结与回顾，更是对未来发展的殷切期许与规划部署。报告明确了协会的前进方向，提供了清晰的行动指南，激发了协会全体成员的信心和斗志，引领协会持续创新、锐意进取，迈向更高的台阶。

会议由副会长兼秘书长李红主持。参加会议的分支机构和杂志社代表对协会年中工作报告给予高度认同，纷纷表示工作成果令人倍感振奋、催人奋进。

在交流发言环节，市场研究业分会会长赵新宇围绕“数据洞察”话题分会应对行业变化的工作创新实践；通用航空分会会长王砥详细汇报了第三届低空经济大会的筹备进展与低空经济发展前景；粮农信息分会会长张雪重点介绍了分会开展人社部职业技能等级认定工作和参与编制《中国数字粮食发展报告－仓储部分》的工作情况和心得体会；营商环境专委会执行会长斯兰介绍了专委会在推进标准化工作、组织定制化培训等方面的具体举措和取得的成效；产业互联网分会副会长兼秘书长张健作为新成立分支机构代表，详细介绍了分会筹备工作经验和成立以来开展的主要工作、取得的成果，《中国信息界》杂志社社长尚进介绍了探索期刊数字化转型以及全媒体平台优化调整的工作规划和进展情况。交流发言不仅展示了各分支机构和杂志社所取得的工作成绩，也表达了他们对未来工作的

热切期待和坚定信心。

协会副秘书长兼会员与对外交流部主任张凤英就《中国信息协会分支机构管理办法（2024年修订稿）》《中国信息协会会员与会费管理办法（试行）》进行了说明，详细阐述了两个管理办法的修订内容和实施细则，让各分支机构更好地理解并遵循执行。

为贯彻落实中央社会工作部、民政部有关规定和要求，依法合规开展协会各项工作，强化内部管理，明确各部门、分支机构、杂志社等责任单位的工作任务，实现协会整体工作目标，协会制定了2024年任务责任书，要求各责任单位结合自身实际情况，制定切实可行的实施计划，扎实落实各项工作，持续强化各责任单位的主体意识、责任意识。

会上，王金平会长代表协会分别与各分支机构、杂志社负责人签订《2024年中国信息协会任务责任书》，体现了协会对自身建设、各责任单位所承担任务的严肃态度和加强内部治理的坚定决心。协会将按照任务责任书要求，监督和敦促全体成员共同努力、积极行动，依法合规开展工作，实现协会整体工作目标和持续健康发展。

本次年中工作会的召开，既是对协会秘书处、各分支机构及杂志社上半年工作的总结，也是对协会2024年总体发展规划与战略布局的再动员。

在党的二十届三中全会即将召开之际，协会将以年中工作会为契机，认真落实中央社会工作部、民政部工作部署和要求，积极学习并深入贯彻党的二十届三中全会的精神，确保思想统一、齐心协力，汇聚全协会的力量，以更加饱满的热情和坚定的斗志，全力以赴做好下半年各项工作。让我们携手并进，在新征程上勇往直前，以实际行动向共和国75周年华诞献礼，共同为国家信息化事业发展谱写新的篇章！

科技创新

Technical Innovation

习近平总书记在党的二十大报告中强调，完善科技创新体系。坚持创新在我国现代化建设全局中的核心地位，加快实现高水平科技自立自强。以国家战略需求为导向，集聚力量进行原创性引领性科技攻关，坚决打赢关键核心技术攻坚战。

科技已经成为当今世界发展的核心驱动力，它深刻地影响了人类生活的各个方面，促进了社会进步和经济繁荣。我们身处一个数字化、智能化、信息化的时代，科技已经深入到我们生产生活的方方面面，成为人类生存和发展的必需品。中国高度重视科技创新工作，坚持把创新作为引领发展的第一动力。它不仅可以帮助人们更高效地完成工作任务，更重要的是，它正在推动全球范围内的创新、跨界合作和知识分享，为人类未来的发展探索出一条光明的道路。

科技创新
Technical Innovation

基于项目编码技术的科技项目群管理应用

文◆国网上海市电力公司经济技术研究院 顾嘉凤 吴恩琦 李奕婵 李 永

引言

随着“碳达峰、碳中和”目标的稳步推进与新型电力系统构建的加快实施，科技项目已成为公司科技创新的主阵地，是落实“双碳”工作部署，全面建设新型电力系统的重要着力点。近年来，公司科技项目的数量不断增多、规模持续扩大，项目之间的关系也愈发交错复杂，孤立地管理任何项目都难以取得组织层面的技术突破。只有基于战略层面开展科技项目群管理，系统梳理科目关系、科学统筹项目、有效分配组织资源，才能更好地实现公司科技创新的目标。

项目编码是指通过制定一套规则和约定，为项目分配或创建一种特定的识别码、编号或标识符。本研究根据公司科技项目的特点，提出了一种以线分类法为主、面分类法为辅的科技项目混合编码方法，用于标识和分类公司的科技项目，为科技项目群的组建与跟踪管理提供重要支持。

1 编码原理与原则

本研究以国内现行相关规范及信息化技术为基本设计原理[1]，采用线分类法为主，面分类法为辅的混合分类法，进行科技项目编码体系的设计。在设计过程中，本研究以科技项目编码的唯一性和永久性，以及公司科技创新智慧平台的连通性与可扩充性为出发点，对项目编码体系进行设计。

唯一性：单个项目编码不得重复，项目各模块编码也不得与自身项目及其他项目中的同类模块重复，确保项目群中所有模块编码存在且唯一。

永久性：编码一旦赋予某个项目模块，即永久有效，不因模块信息的变化而变更。

科技创新智慧平台连通性：指单个项目模块所含字符码及属性信息可以在各个项目、项目各个阶段以及各参与方之间进行无障碍流通，在平台上流转时可实现有效继承。

可扩充性：在项目实施阶段，如果出现原项目中不存在的模块，可基于原定规则进行新模块的扩充。

2 编码思路与模型

对于一个完整的科技项目编码体系，应使科技项目编码最大限度地承载各种属性信息，其中应包括管理属性、类别属性、技术属性、成果属性。管理属性是指项目的组织结构属性，包括项目的承担单位与合作单位；类别属性则是指该项目的类型，包括项目类型与项目类别；技术属性应包含项目的技术类别及关键技术；成果属性应包含项目的成果类型、成果层次等信息。科技项目编码结构如表 1 所示，将该体系框架按照管理、类别、技术、成果等属性进行结构化分解，以此实现众多科技项目的定义、识别、创建和使用。作为基础性标准，该体系还应确保各项目实施关联方、各阶段和各项任务之间对于编码成果（模型及其信

【作者简介】顾嘉凤（1992—），女，上海人，本科，研究方向：电气工程。
【通讯作者】吴恩琦（1988—），女，山东章丘人，硕士研究生，研究方向：技术经济及管理、能源电力经济。

表 1 科技项目编码结构

属性	结构
管理属性	承担单位－合作单位
类别属性	项目类型－项目类别
技术属性	技术类别－关键技术
成果属性	成果类型－成果层次

息）能够实现信息交换共享、模型整合和应用协同。

本编码体系由项目管理属性代码组、项目类别属性代码组、项目技术属性代码组、项目成果属性代码组 4 个代码组构成。为合理地对科技项目进行编码，研究梳理了科技项目属性（见表 2）。

表 2 科技项目属性

属性		结构
管理属性	承担单位	浦东公司、市区公司、市北公司、市南公司、松江公司、嘉定公司、青浦公司、奉贤公司、金山公司、崇明公司、长兴公司、超高压分公司、电缆公司、建设公司、物资公司、信通公司、电科院、经研院、客服中心、培训中心
	合作单位	久隆咨询、久湛科技、上海交大、柒志科技、朗新科技、杭途科技、武汉大学等
类别属性	项目类型	科技项目
	项目类别	基础共性技术、专业应用技术、专业管理技术、跨领域融合技术、决策支持技术、前沿技术、应用理论
技术属性	技术类别	/
	关键技术	/
成果属性	成果类型	论文 / 专利 / 标准 / 著作 / 奖项
	成果层次	北大核心、南大核心、中国科技核心、CSCD、社科院核心、SCI、SSCI、EI、其它 / 发明专利、实用新型专利、外观设计专利 / 国标、行标、地标、企标 / 专著、独著、合著 / 国奖、地市奖、行业奖、企业奖

由于科技项目申报过程中填写的技术领域颗粒度较粗，本研究将通过文本挖掘的方式先识别科技项目的技术主题[2]，获取科技项目的技术属性，再进行统一编码。最终获得的科技项目编码由四组代码及半角下划线“_”组成，如项目管理属性代码组－项目类别属性代码组－项目技术属性代码组－项目成果属性代码组。

3 技术主题识别

科技项目的技术主题识别是指通过挖掘科技项目名称获得科技项目的主题。本研究以 2022 年公司 90 个举手制科技项目的名称为数据源，使用 BERTopic 主题识别模型获取技术主题，步骤如下。

（1）嵌入科技项目名称数据。将科技项目的名称输入一个基于英语 BERT 的模型，利用双向 Transformer 结构计算研究内容的词向量。

（2）降维 + 聚类。分别将每个科技项目名称的词向量输入 HDBSCAN，可以自动推荐最优的簇类结果。HDBSCAN 输出的聚类数量即为最终提取的各个科技项目名称的技术主题数量。

（3）创建技术主题表示。使用 TF-IDF 评价每个词对每个 HDBSCAN 聚类的重要性，对主题进行提取和精简，以提高最大边缘关联词的一致性。最终获取每个主题中的重要单词。

（4）根据技术主题划分科技项目数据。根据不同技术主题的主题词在每个科技项目名称中出现的频率，计算科技项目名称与主题的匹配程度。

经过训练得到科技项目的 7 个技术主题，即电力数字技术、智能传感技术、“双碳”服务技术、运营管理技术、大数据分析技术、电力治理技术、人工智能技术（见表 3）。表 3 包括技术主题名称、每个技术主题除去粗粒度关键词后的 10 个代表性关键词以及每个技术主题的科技项目数量。

表 3 科技项目技术主题

技术主题名称	代表性关键词	数量
电力数字技术	数字孪生、数字化、可视化、电网需求评估、碳足迹监控分析、多元负荷、交互式、云协同、变电站监控、自动验收	15
智能传感技术	物联网、定位技术、信号自动监听、传感器、电缆故障、档案管理、电缆终端、地下管廊孔位监测、输变电设备、户外 GIS 设备	15
“双碳”服务技术	碳市场、电力市场、耦合机制、仿真研究、碳排放计量、优化模型、碳排放权、碳测算、链路机理、虚拟电厂	15
运营管理技术	增值服务运营、优质供电、优化运行、需求潜力分析、HPLC 技术、市场协同、物联、电源结构转型、博弈交互、仿真研究	7
大数据分析技术	大数据分析、多源数据、信息模型、数据增值、预测分析、质量评价、数据融合、数据画像、数据监测、智慧应用	13
电力治理技术	电能质量治理、系统性治理、仿真模拟算法、配网协议、资源池优化、库存分级耦合、线路跳闸压减技术、柱上断路器控制器、校验系统、智能管控	13
人工智能技术	人工智能、机器学习、AI 技术、文本挖掘、知识图谱、智能交互、图像识别、神经网络算法、智能辨识、智能推荐	12

4 项目自动编码

经过 BERTopic 主题模型训练提取技术主题后，对科技项目的所有属性代码进行统一编码，并建立科技项目编码清单。具体规则如下。

（1）项目管理属性代码，由承担单位与合作单位组成，采用 4 位数字表示。其中，承担单位从浦东公司到培训公司代码为 01 ~ 20，合作单位如久隆咨询、久湛科技等，根据公司供应商库可从 01 依次编码。

（2）项目类别属性代码组，由项目类型与项目类别组成，采用 1 位字母和 1 位数字表示。其中，字母 T 表示科技项目，数字 1 ~ 7 分别表示基础共性技术—应用理论。

（3）项目技术属性代码组，由技术类别与关键技术组成，采用 4 位数字表示。其中，技术类别从电力数字技术到人工智能技术代码为 01 ~ 07，各个技术类别下的关键技术代码为 01 ~ 10。例如，电力数字技术类别下的数字孪生代码为 01，可视化代码为 02，以此类推。

（4）项目成果属性代码组，由成果类型与成果层次组成。每种成果类型和成果层次分别采用 1 位字母和 1 位数字表示，含多种成果的项目可自由拓展。其中，J 表示论文，1 ~ 9 分别表示北大核心—其它；P 表示专利，1、2、3 分别表示发明专利、实用新型专利、外观设计专利；S 表示标准，1 ~ 4 分别表示国标、行标、地标、企标；B 表示著作，1 ~ 3 分别表示专著、独著、合著；A 表示奖项，1 ~ 4 分别表示国奖、地市奖、行业奖、企业奖。

不同组代码之间用半角下划线“_”连接；同一组代码中，相邻层级代码之间依照顺序编制。根据科技项目编码清单，可以自动得到如项目“地下电缆故障定位去干扰自学习神经网络算法研究”的编码为“0301–T01–0707–J9P1S3A3”。

5 科技项目群管理应用

5.1 组建项目群

以拟开展科技项目的相关管理属性、类别属性、技术属性和成果属性等为导向组建项目群，有利于项目群内部项目之间的协同管理，便于群内各项目的各类资源调配，优化项目实施周期，提高项目承接能力，协调技术团队配置，汇总编制总结报告，并做好项目成果维护移交等事务。利用科技项目编码，可以将属性编码相同的项目自动组建为科技项目群。例如项目“地下电缆故障定位去干扰自学习神经网络算法研究”的编码为“0301–T01–0707–J9P1S3A3”，项目“基于文本挖掘的技术标准智能辨识技术研究及应用”的编码为“1701–T02–0704–JP2S1A1”。根据编码，可知这两个项目的合作单位、技术类别相同，因此能够组建在一个项目群中。

5.2 跟踪管理项目群

科技项目编码清单用于记录所有科技项目及其对应的编码，项目群成员可以快速查找和定位特定科技项目。在科技项目群管理过程中，项目群成员可以根据项目编码生成报告，以便在项目群级别了解项目的进展、风险和绩效。同时，通过聚合和分析项目编码相关的数据，项目群成员可以更好地理解项目群的状态和趋势。此外，在科技项目群管理过程中，存在新科技项目的加入或项目的变更，而灵活的项目编码体系能够容纳这些变化，同时保持项目群管理的一致性。

结语

本研究综合考虑了科技项目的管理属性、类别属性、技术属性和成果属性，提出了一种以线分类法为主，面分类法为辅的科技项目混合编码方法。研究借助资料收集法、BERTopic 主题提取法，系统地梳理了科技项目的属性内容，并定义了科技项目的各个属性代码。管理人员可对照科技项目编码清单对科技项目进行编码。利用科技项目编码，可以实现科技项目群的自动组建、快速查找与定位、跟踪管理与灵活应对，提高科技项目群管理的可视性和效率，对开展科技项目群管理具有重要意义。

引用

[1] 张静.问卷调查中评价类问题的自动编码方法及其应用[D].天津:天津商业大学,2022.

[2] 刘智锋,王继民.社会科学数据集的跨学科性研究——以CHARLS和CGSS数据集为例[J].现代情报,2023,43(9):165-177.

大数据时代人工智能在远程网络通信技术中的创新应用研究

文◆中电科大数据研究院有限公司 林 辉 余 楷

引言

在大数据时代，人工智能技术在远程网络通信领域显示出了较好的应用潜力，特别是在网络安全和管理效率方面。通过深入探究人工智能在异常流量检测、智能运维、故障溯源以及网络优化等方面的应用，研究突显了人工智能如何提升网络通信系统的响应速度和安全性。此外，研究还涵盖了人工智能在智能化网络配置、自动化故障恢复、数据流量和带宽优化、网络安全监测、物联网通信以及远程诊断与维护的创新应用。该技术的集成不仅优化了网络资源的管理，还强化了网络的可靠性和安全防护能力。

1 人工智能技术概述

人工智能技术涉及诸多算法和计算模型，核心技术包括机器学习、深度学习和自然语言处理。机器学习技术使计算机系统能够基于经验数据进行预测和决策，无须进行明确的程序编写。深度学习技术作为机器学习的分支，模拟人类大脑的神经网络结构，通过多层处理和抽象能力，使计算机能够从数据中学习复杂模式。该技术不仅在图像和语音识别领域取得了革命性进展，还极大地推动了自动驾驶和机器人技术的发展。自然语言处理技术使计算机能够理解和生成人类语言，提供了从客户服务到全自动翻译系统的广泛应用。

在网络通信领域，人工智能的核心技术被应用于智能监控系统，实现对网络行为的实时监控和管理，有效预防网络攻击和系统故障。通过大数据分析，系统能够识别出潜在的异常模式，及时响应各种网络安全挑战。此外，人工智能技术在提高网络资源利用效率和优化网络配置方面也显示出巨大潜力，通过精确调控网络流量和自动配置网络资源，提高了网络服务的质量和用户体验。

2 人工智能在网络安全中的应用

2.1 异常流量检测

异常流量检测是通过应用人工智能技术实现对网络流量的实时监控和异常识别。该过程通常依赖于机器学习和深度学习算法，其中常见的方法是使用基于统计模型的异常检测。假设，网络流量数据可以表示为一个时间序列 $\{x_t\}$，在正常情况下，这些数据服从某种已知的概率分布 $P(x_t|\theta)$，其中 θ 是模型参数。当网络流量异常时，这些数据的概率分布会偏离正常情况。通过计算每个时间点的异常评分 $S(x_t)$，可以检测出异常流量。异常评分的计算公式如下。

$$S(x_t) = -logP(x_t \mid \hat{\theta})c^2 \qquad (1)$$

式（1）中，$\hat{\theta}$ 是通过历史正常数据估计的参数。较高的 $S(x_t)$ 值表明数据点 x_t 偏离正常分布，判定为异常流量。

机器学习模型，如支持向量机（SVM）和随机森林（Random Forest），通过学习正常与异常流量的特征，进一步提高检测的准确性。深度学习模型尤其是自编码器（Autoencoder），通过重建误差来识别异常流量，自编码器训练时使重建正常流量时的误差最小，对于异常流量则有较大的重建误差。此外，递归神经网络（RNN）和长短期记忆网络

【作者简介】林辉（1985—），男，天津人，本科，研究方向：大数据、信息化。

（LSTM）在处理时间序列数据时表现出色，能够捕捉流量随时间变化的复杂模式，进一步提升检测性能。

2.2 智能运维

智能运维（Intelligent Operation and Maintenance，简称 IOM）是应用人工智能技术优化网络系统管理和维护的实践。在智能运维领域，人工智能主要通过预测性维护、自动化故障处理和资源优化配置来提高运维效率和系统可靠性。预测性维护通过机器学习模型预测设备故障和系统性能下降的可能性，允许运维团队在问题发生前就采取措施，减少系统停机时间和维护成本。例如，通过分析历史数据中的性能指标和故障记录，机器学习模型能够识别出故障发生的先兆，如温度异常升高或硬件性能持续下降。自动化故障处理通过自然语言处理和专家系统，实现故障诊断和问题解决的自动化，简化了问题解决流程并缩短了恢复时间 [1]。

2.3 故障溯源

在人工智能的帮助下，故障溯源过程变得更加自动化和智能化。通过采用深度学习和模式识别技术，故障溯源系统能够从海量的监控数据中迅速识别故障源。这一过程通常包括多个步骤，即数据收集、特征提取、故障诊断和故障定位。

（1）数据收集阶段。系统通过各种传感器和日志收集器持续监控网络状态，收集与网络性能相关的各种指标，如流量数据、错误率、响应时间等。（2）特征提取阶段。利用机器学习算法，如主成分分析（PCA）或自动编码器，从原始数据中提取出有助于故障诊断的特征。（3）故障诊断阶段。采用分类算法如支持向量机（SVM）或神经网络，对提取的特征进行分析，识别出潜在的故障模式。（4）故障定位阶段。系统利用诊断结果，通过算法确定故障的具体位置和原因，指导维护团队进行快速响应。

2.4 网络优化

随着网络规模的不断扩大和网络流量的日益增加，传统的网络管理方法已经难以满足高效和灵活管理的需求。人工智能技术的引入，特别是机器学习和优化算法的应用，增强了网络优化的能力。机器学习模型能够根据历史数据和实时流量情况预测网络流量的趋势，提前调整网络配置，如调整路由策略和带宽分配，以适应预期的流量变化。此外，优化算法如遗传算法和粒子群优化算法被用来求解复杂的网络优化问题，如负载均衡和能源消耗最小化。这些算法能够在多个目标和约束条件下，找到最优或近似最优的网络配置方案。通过实时监控网络状态和自动调整网络参数，AI 驱动的网络优化不仅提高了网络资源的使用效率，还保证了网络用户的服务质量 [2]。

3 人工智能在远程网络通信技术中的创新应用

3.1 智能化网络配置管理

在传统网络设置中，配置管理通常依赖于网络管理员的手动干预，不仅耗费时间，还容易出错，尤其在大规模和复杂的网络环境中更是如此。引入人工智能后，智能化网络配置管理系统能够自动识别网络设备的状态和性能，自动应用最优配置。采用高级算法分析历史配置数据和网络性能指标，预测最佳的网络配置设置。例如，使用决策树、神经网络或强化学习模型，系统能够学习最有效的配置以及在特定情况下应如何调整配置以优化性能和资源利用率。此外，这些智能系统还可以实时监控网络状态，自动调整配置以适应网络负载变化和连接需求，减少网络故障的风险，提高网络的可靠性和弹性。这种智能化的配置管理方法尤其适用于数据中心、云计算环境和大型企业网络，其中网络设备众多且配置需求频繁变化。通过减少人为干预和自动优化配置，不仅提升了网络管理的效率，还改善了网络服务的整体质量和用户体验。

3.2 自动化故障恢复系统

自动化故障恢复系统利用机器学习算法来监测网络操作，实时检测和诊断潜在的故障或性能下降问题。一旦检测到问题，系统可以自动启动预设的恢复流程或使用从以往经验中学到的最佳实践来尝试修复问题。例如，通过分析网络故障历史和维护日志，深度学习模型可以识别故障模式并推荐相应的恢复策略，包括重新收集路由流量数据、重启服务或更换硬件配置。在更复杂的情况下，自动化故障恢复系统还能进行因果推理，确定故障的根本原因，并实施长期解决方案以防止问题再次发生。这种自动化的故障响应和恢复机制对于保持网络的持续可用性至关重要，尤其是在对时间敏感的商业环境中，如金融服务和在线交易平台。此外，随着物联网和智能设备在日常运营中的普及，自动化故障恢复系统在管理这些设备的网络连接和性能方面也显示出巨大的潜力，确保服务不间断和用户体验的连续性。

3.3 数据流量和带宽优化

数据流量和带宽优化是通过利用预测分析和实时数据处理，人工智能算法能够动态调整网络带宽分配和流量管理策略。例如，机器学习模型可以根据历史流量数据和用户行为模式预测网络高峰时段，提前调整路由策略和带宽资源。此外，深度学习网络被训练以识别和优化数据传输路径，减少延迟并避免拥塞，尤其是在多跳网络中。递归神经网络（RNN）特别适用于处理序列数据，能够预测未来流量趋势并实时更新网络配置[3]。

3.4 增强网络安全监测

增强的网络安全监测是利用人工智能技术识别和防御网络威胁的关键应用，包括从基础的入侵检测到复杂的行为分析。人工智能系统通过整合和分析来自网络各个部分的数据，提供全面的安全状态视图。例如，通过实时分析网络流量、用户行为和应用活动，AI 系统可以迅速识别出异常模式，昭示着安全威胁的存在。网络安全监测中的人工智能应用如表 1 所示，展示了一个网络安全监测系统中的常见指标和人工智能模型的应用。该技术的实现依靠于复杂的数据处理和高级算法，使系统不仅能够响应已知的威胁，还能够适应新出现的挑战。通过不断学习和适应网络环境变化，人工智能增强的网络安全系统提供了一种动态的防御机制，更好地提高了网络的安全水平，这对于保护关键基础设施和敏感数据尤为重要[4]。

表 1 网络安全监测中的人工智能应用

指标类型	描述	AI 模型应用
流量异常	流量突然增加或减少	使用异常检测算法如孤立森林
用户行为分析	登录地点、时间异常	应用聚类分析和异常点检测
应用层行为	应用程序行为模式变化	深度学习模型分析应用行为
网络性能	网络延迟和数据包丢失	时间序列预测模型

3.5 优化的物联网通信

人工智能通过高级的数据分析和自动化决策支持系统，能够实现物联网设备之间的优化通信，降低延迟，提高数据传输的可靠性。这一过程包括使用机器学习算法对设备间的通信模式进行建模和分析，以便识别和预测网络中的拥塞点，并自动调整数据流以避免这些问题。例如，通过实施神经网络和强化学习算法，系统能够学习从历史通信失败中恢复，自动调整传输协议和路由选择以优化未来的传输效率。此外，人工智能还能够在设备故障预测、能源消耗优化以及安全漏洞检测等方面发挥作用，通过持续监控和实时分析，为物联网设备提供智能化的维护和管理，提升整个物联网系统的性能和稳定性。

3.6 远程诊断与维护

远程诊断与维护是通过先进的监测和分析工具提供及时的技术支持和问题解决方案，减少物理访问需求。在这一过程中，人工智能系统通过集成的传感器数据和实时网络监控信息，迅速识别和诊断网络中的问题或性能下降。利用深度学习算法，如卷积神经网络和递归神经网络，分析复杂的数据模式，预测潜在的故障并提前警告用户或服务提供者。自动化的故障诊断工具可以解析大量的日志文件和性能数据，通过模式识别技术确定故障的具体原因，智能推荐系统则可以提供修复建议或自动执行某些维护任务[5]。此外，人工智能驱动的远程诊断系统还能进行自我学习和适应，随着时间推移不断提升诊断准确性和维护效率，不仅大幅度提升了网络维护团队的工作效率，还优化了资源分配，确保了网络服务的持续性和可靠性，特别是在金融服务、医疗保健和制造业。

结语

人工智能技术已经成为远程网络通信领域的重要推动力。通过对网络安全的持续加强，异常流量检测、智能运维和故障溯源等功能的实现展示了 AI 的实际应用价值。同时，人工智能在物联网通信、远程诊断与维护等方面的创新应用正在重塑网络管理和优化的传统方法，提升了网络系统的自适应能力和操作效率。不仅提高了网络服务的质量和可靠性，还为未来网络技术的发展趋势提供了新的方向，预示着更加智能化和自动化的网络运维与安全管理模式。

引用

[1] 赵笛杉.大数据时代计算机远程网络通信技术创新研究[J].科技视界,2023,13(35):74-76.

[2] 刘小钧,张勇,陈艳.大数据时代计算机远程网络通信技术创新[J].山西电子技术,2022(4):64-65+69.

[3] 贺明华.计算机远程网络通信技术应用研究[J].科技创新与生产力,2022(5):139-141.

[4] 郑秀毅.大数据时代计算机远程网络通信技术变革分析[J].电子元器件与信息技术,2021,5(5):59-60.

[5] 牛晓丽.大数据时代的计算机远程网络通信技术探析[J].电脑编程技巧与维护,2021(3):73-74+153.

基于情感化设计的智能工具 App 设计研究 *

文◆湖南工业大学　刘聪仪　李岢澹　谷彤彤　田　飞

引言

2023 年，中国各地政府为持续应对日益加剧的老龄化现象[1]，针对三孩政策实施了多种激励措施，这一举动被社会各界评价为能有效推动各方面完善配套措施、保障育龄妇女生育权利、为家庭生育三孩提供法治保障的务实之策[2]。该政策为针对儿童群体的智能化 App 发展带来了巨大商机。目前，AI 人工智能技术已经逐步应用于数字化照片管理，并致力于改进数字化照片管理中的不足。该研究以现有智能相册优点为基础，为 AI 相册应用开发提供新方向。

1 研究背景

情感化设计是一种顺应或唤起用户内心情感需求的设计理念，旨在让用户产生积极的用户体验与行为。从消费者的角度来看，产品的形式不仅要符合人体工程学和心理学的标准，还要具有情感化元素。这意味着在满足理性需求的同时，也要使操作过程变得更加有趣。随着智能设备的普及，情感化设计也日益受到重视，并逐渐应用到各种应用程序中。

本文基于“以人为本”的设计理念[3]，深入分析移动网络背景以及少子化社会环境下，父母用户在使用相册 App 时，对子女真实感受与情感建立过程，通过合理的分析与设计，实现在感性层面上为用户带来持久价值的目标。

2 情感化 AI 人工智能相册 App 体系构建

为深入了解用户的情感需求和市场智能相册类 App 的具体使用情况，本次调查运用了用户访谈法和问卷调研法，针对目标用户在情境设定下的选择性反馈进行筛查，并对现有信息化应用产品进行分类分析。

2.1 前期调研

2022 年 7 月—8 月，以线上方式展开问卷调查分析，本次调查中，最终发出问卷 202 份，收回 197 份，其中有效问卷 186 份。目标用户对产品需求态度调研如表 1 所示。

表 1 目标用户对产品需求态度调研

题项	样本量	肯定 / 前者	否定 / 后者	一般 / 中立
1. 您使用过照片管理类软件吗?	186	73	113	0
2. 您有为整理孩子照片的烦恼吗?	186	123	54	9
3. 如果有一个相册 App，能自动挑选并集合您小孩的所有照片，对您来说有用吗?	186	111	60	15
4. 您更愿意手动筛选孩子照片，还是借助人工智能自动挑选?	186	132	14	40
5. 您认为在相册管理 App 中加入智能时间轴设计会不会让您更方便地筛选出照片?	186	126	28	32
6. 您喜欢通过游戏式体验引导您更好地使用 App 吗?	186	97	23	66
7. 这个 App 还能自动归类社会实践或奖状照片，有用吗?	186	109	40	37

调研结果显示，多数用户面临的问题总结如下。常用相册软件难以自动关联孩子的成长阶段和相应分类，导致查找如“家庭阅读”“体育锻炼”等特定场景照片时效率低下；用户因隐私顾虑对 AI 技术的信任度不高；市面上缺乏针对儿童定制且以相册为核心功能的应用。

2.2 中期调研

以实地用户调研和结构化的问卷调查数据为核心依据，深入剖析现

*【基金项目】2022 年湖南省大学生创新创业训练计划项目（S202211535048）；湖南省大学生创新创业训练计划项目（S202211535088）

【作者简介】刘聪仪（2002—），女，黑龙江哈尔滨人，本科，研究方向：工业设计。

【通讯作者】田飞（1980—），男，陕西宝鸡人，硕士，副教授，研究方向：数字产品与交互设计。

有市场中同类产品的竞争态势，提炼出具有鲜明代表性的标签化用户画像，为后续产品设计优化与策略制定提供有力支持。

全方位了解用户需求，选取问卷中的典型问题，针对研究结果得出以下总结（见图 1）。

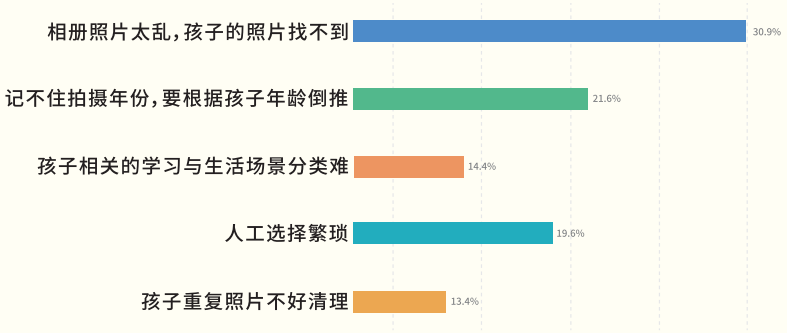


图 1 典型问题分析

设计人员从时间线构建用户行为旅程，整合为完整的相册 App 使用流程，细致标注各阶段用户情感变化，绘制成情绪体验图。明确用户追求的互动感受，即时反馈 AI 智能分拣需求。用户旅程分析如图 2 所示。

通过分析市场和用户反馈，融合游戏元素，使照片管理更富趣味且高效。团队综合考虑功能结构、页面设计和交互逻辑，推进至高保真原型和 UI 切图制作阶段的进程，加速产品迭代。

3 情感化 AI 人工智能相册 App 创新策略

相册智慧管理 App 应着重将情感化设计融入产品 [4]。本文立足国内儿童市场智能相册 App 的发展现状，从产品的使用方式层级出发 [5]，分视觉、交互、技术、情感 4 个层面对 AI 人工智能相册 App 提出情感化设计创新策略分析。

3.1 视觉层面——童趣、清晰的界面框架处理

为适应儿童特性，相册管理设计应考虑其行为和心理特点，因现有时间线排序不便，故转向更符合家长习惯的智能时间轴与情境分类法。设计围绕时间、年龄、学段 3 层展开，为儿童打造跨年龄段、多样化情景的相册管理系统。

3.2 交互层面——游戏化模式

为解决 App 上传资料复杂、用户易被广告干扰以及面对冗长指引感到不悦的问题，采用游戏化设计革新引导流程。首次使用的用户会体验到一种融入了趣味互动的游戏化引导，通过“熊猫选选”小游戏抛掷照片来挑选样本，使其在享受乐趣的同时快速熟悉产品功能。

3.3 技术层面——隐私技术

本研究借助苹果 Testflight 收集数据，并通过问卷验证需求产出高保真设计方案。利用苹果 Vision 框架研发保护隐私的人脸识

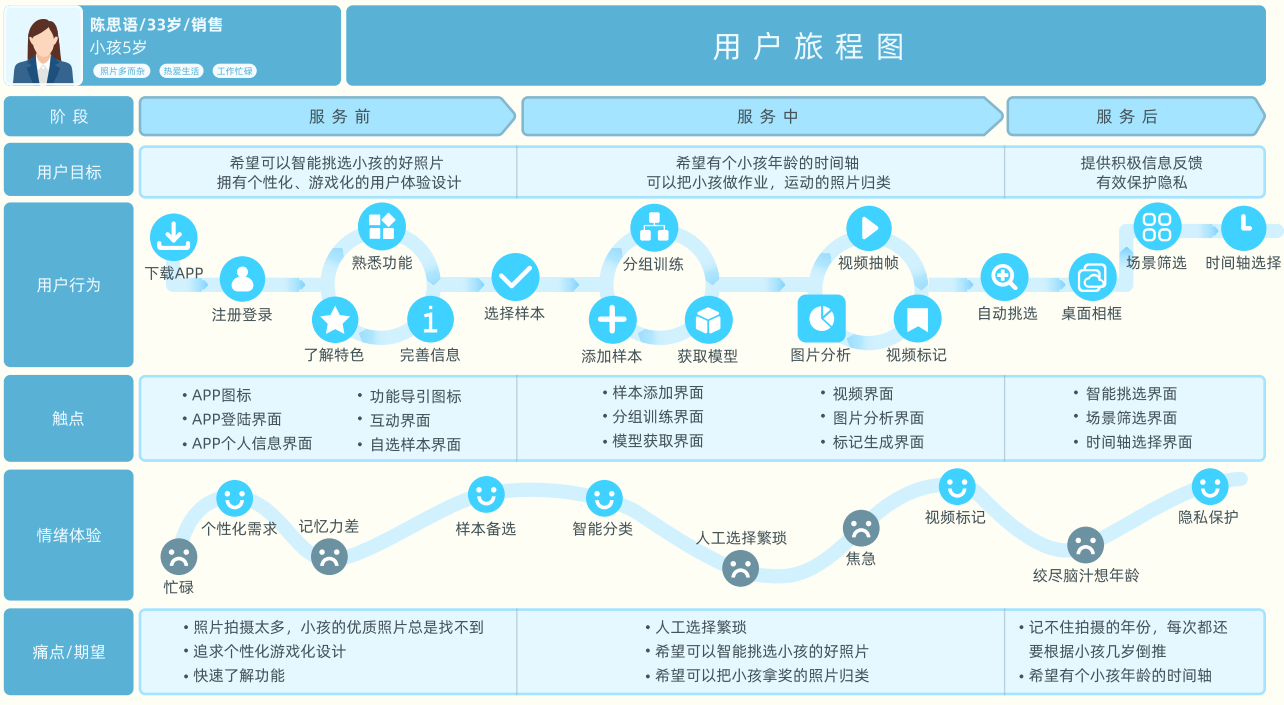


图 2 用户旅程分析

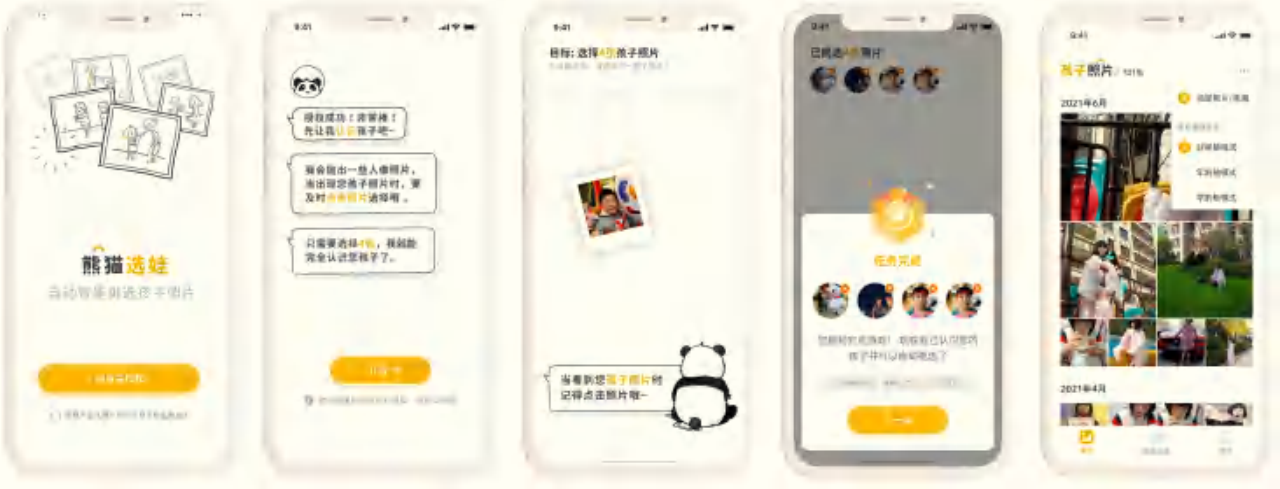


图 3 添加自选样本界面

别技术[6]，实现“自动挑选儿童照片”功能，确保照片和面部信息不上传云端，保障用户隐私安全。

3.4 情感层面——人工智能服务于情感化产品

本次 App 设计超越传统功能实用主义，侧重于提升用户情感价值体验，利用温馨的卡通形象和视觉元素，加深情感联结，增强用户忠诚度。本产品创新性地将情感化设计理念融入每个细节，采用 AI 智能分拣技术，根据时间、地点、人物等因素智能归类高质量照片，解决家庭相册混乱无序的问题。

4 情感化 AI 人工智能相册 App 整体设计方案

4.1 体验设计与提升

设计方法利用产品中的知识产权（IP）角色“熊猫”来识别并分析 4 张儿童的面部图像。系统利用深度学习算法对这些图像进行特征提取和归纳，在用户的照片库中自动识别出与儿童相关的隐藏图像，从而实现儿童图像的自动突出显示功能。 该产品基于苹果公司的官方 Vision 框架进行开发，训练了一种无需网络连接即可运行的离线人脸识别模型。这种设计不仅提高了系统的可用性，还增强了用户隐私的保护。

4.2 产品设计与创新

在设计层面，产品团队采用了以实现情感化设计的方式，不仅提供了高效的技术功能，还向用户传达了人工智能技术的温暖和关怀。

在实际建设过程中，用户登录 App 后，开启首次使用授权，添加自选样本后，通过识别模型训练算法获得模型。之后遍历相册首次自动挑选分类出目标人物照片与视频，搜索是否存在新增或修改的样本，并进行智能检查，添加自选样本界面如图 3 所示。用户为平台提供实时服务信息传递，情感化互动式服务的 App 系统性构建也为儿童相册管理系统注入了更多活力。

结语

熊猫选娃 App 是在三孩政策背景下，开发出的让家长与孩子成长轨迹情感关联的情感化数字产品，产品为人们带来更佳的用户体验，也为解决社会问题作出了有益的尝试。本研究以情感化需求为理论基础，立足国内儿童市场的智能相册 App 的发展现状，通过情感化设计中的本能层、行为层、反思层作为产品开发策略的基础，借用游戏化策略，深入探讨智能相册 App 的设计开发路径，以期为今后的儿童类数字产品发展提供借鉴意义。

引用

[1] 倪泰乐,冉然,祁娜,等.就诊等待服务APP适老化设计研究[J].包装工程,2022,43(22):125-133.

[2] 常进锋,刘畅.建设生育友好型社会的现实困境与优化路径——以福利多元主义为视角[J].德州学院学报,2023,39(5):95-99+110.

[3] 向莉君.坚持以人为本增进民生福祉[J].当代贵州,2024(9):12-13.

[4] 郝玉瑶,詹云.基于沉浸式体验的博物馆APP设计路径[J].湖南包装,2022,37(4):147-150.

[5] 周明.产品使用方式行为层级建构[J].装饰,2016(5):136-137.

[6] 傅滨桢,孔敏,刘朝宗.对人脸识别技术在开放教育考试中应用的思考[J].福建开放大学学报,2024,(3):30-33.

基于高血压检测记录 App 设计流程的 App 设计师转化用户体验模式研究

文◆马德里康普顿斯大学美术系　马　骁　尤金尼奥·巴格尼奥·科麦斯
卡斯蒂利亚拉曼却大学文学系　司雅娣

引言

随着信息技术的迅速发展，互联网应用极大地改变了人类的生产和生活方式。自 21 世纪以来，智能手机开始大规模普及，随之而来的是依附于智能手机的应用程序（App）行业的兴起，为人们的生活带来了各种便利。在 App 设计行业中，经验丰富的设计师可以凭借自己积累的设计能力有效处理和解释接收到的用户体验信息，从而提出完整的设计方案。然而，对于欠缺经验的设计师，他们转化用户体验的方式是否相同仍没有确切答案。本研究计划采用深入访谈法和口语分析法进行研究。通过深入访谈采集初始用户体验数据，然后使用口语分析法对受访设计师在设计手机 App 过程中从接收用户体验到设计完成的口头表达进行分析和整合，以获取不同经验的 App 设计师转化用户体验的模式。通过直观的方式展现他们转化模式的差异，有助于 App 设计公司制定新进设计师的培训和设计师的晋升标准。

在设计 App 产品时，设计师必须以用户为中心，关注用户与手机 App 之间的互动关系以及 App 在现实世界中的作用和用户体验。Pahl 和 Beitz 提出，在用户体验设计的过程中，从界定任务到概念设计再到具体设计和细节设计，概念设计阶段尤为关键，需要提出原则性解决方案 [1]。而不同资历的设计师在处理用户体验信息方面存在差异，了解这些差异并通过直观方式呈现，为新进设计师的培训和晋升提供重要参考。

1 理论研究

1.1 用户体验

用户体验（User Experience）是由认知心理学家 Donald Norman 提出的概念，指用户在使用特定产品、系统、服务时所产生的行为、情绪和态度。Hassenzahl 认为，用户体验包括用户接触产品和服务的过程中建立的感受和认知。根据 ISO 9241–210 的定义，用户体验涉及用户在使用或预期使用产品、系统、服务时所产生的感受和行为反应，包括使用的前、中、后期，并涵盖情绪、信仰、偏好、感受、生理和心理反应、行为，甚至成就感 [2]。简而言之，用户体验是用户与产品互动过程中的整体体验，包括使用前、中、后的所有感受，并受到系统、用户和使用情境 3 个因素的影响。Kankainen 认为，用户体验是在特定目标下，用户有动机的行动所产生的心理结果，过往的经验和期望会影响当前的用户体验，而当前的用户体验也会带来更多的经验和期望的修改 [3]。

提升产品界面的用户体验需要融合技术、心理学、设计和人机工程学等各个领域的知识，以用户为中心进行设计。在这种方法中，常用“易用性”这个词来描述产品（如 App、网站或其他项目）适合人们使用的品质。也

【第一作者简介】马骁（1990—），男，江苏扬州人，博士研究生在读，研究方向：用户体验设计 / 设计思维转化模式。
【第二作者简介】司雅娣（1993—），女，河北石家庄人，博士研究生在读，研究方向：隐喻思维 / 语义学。
【第三作者简介】尤金尼奥·巴格尼奥·科麦斯（Eugenio Bargueño Cómez）（1953—），男，西班牙马德里人，博士，教授，研究方向：设计表现系统 / 图像塑性表达。

就是说，产品应满足用户的需求，让他们工作或娱乐更为方便，从而达到自己的目标。易用性与用户体验密切相关，是衡量用户体验要素的重要指标。简而言之，一个易用的产品应该具备 5 个特点，即易学（用户能够迅速掌握使用方法）、高效（使用该产品能够提高用户的工作效率）、好记（用户在一段时间后再次使用时无需重新学习即可使用）、少错（减少用户操作错误，且一旦发生错误，用户能够容易纠正）以及满意（用户在使用产品时感到愉快和满意）。

1.2 用户体验设计

Hassenzahl 最早提出了用户体验模型，从设计者和用户两个角度出发，关注了不同的元素。设计者在设计产品或服务时，通过产品的内容、外观、功能等传达特定的产品特点。产品本身有两种属性，一是实用性，二是趣味性。实用性关注产品的功能和易用性，而乐趣性则关注用户与产品的互动，带来的感觉和体验。当用户使用产品时，他们会结合自己的期望来评价产品，决定它是否吸引人，同时也会产生不同的情绪体验。此外，Hassenzahl 还强调了用户的心理因素。用户体验具有主观性，不同的人会有不同的感受，而同一个人在不同情境下的体验也会有所不同，甚至会随着时间而改变。因此，综合考虑这些因素，设计出更符合用户需求和期望的产品十分重要。

用户体验要素是由 Garrett 提出的概念，它将用户体验的构建分为 5 个层级，即策略层（明确用户需求和网站目标，为设计提供指导）、范围层（确定功能规格和内容需求，概括所需提供的功能和信息内容）、结构层（整合信息，设计交互界面和信息结构，规划网站的使用路径）、框架层（通过视觉化方式设计界面、信息和导航，通过布局和图像设计帮助用户理解信息）和表面层（打造网站的最终外观，使其视觉上吸引人）[4]。5 个层级从抽象到具体，指导着设计师构建用户体验。最初这些概念用于网站设计，但也适用于移动应用等其他领域。这些层次相互影响，从核心到细节逐步发展，每个层级都有其独特的重点和目标。设计师在设计过程中应充分考虑这些层次，以确保用户能够获得良好的体验。

1.3 用户心智模型

心智模型最初由 Kenneth 提出，他认为，心智模型就是人们大脑里对周围世界的一种理解方式和思考过程。它来源于经验和想象力，能够推测、预测和做出反应，以应对各种情况。Susan 则认为，这种模型基于人们对事物的认知、想象和过去的经历，帮助人们理解世界并制定解决问题的方法。它是基于不完整信息、过去的经验和直觉的一种假设，影响人们的行为和决策 [5]。同时，Norman 给出了这种模型的几个特点，如不完整性（人们对事物的心智模型通常不完整，缺少一些重要信息）、有限性（人们在运用心智模型时，经常会受到限制，无法充分利用它们）、不稳定性（人们经常会忘记心智模型的一些细节，尤其是长时间没有使用它们之后）、没有明确的界限（类似的心智模型经常会混淆不清，边界不够清晰）、不科学（有时候人们会采取不太理性的方式，即使知道这些方式并不正确）和简约（人们倾向于采取更简单的行动方式，以减少心智负担）[6]。从设计角度来看，人们将心智模型分为心智模式、设计模式和系统印象，它们相互作用，影响着人们对事物的理解和行为。

1.4 人机界面设计

人机界面（Human-Computer Interaction，简称 HCI）就像是人与机器之间的互动，是一个封闭的系统，人主动输入指令，机器接受后进行信息输出，然后不间断地运作形成一个循环。Preece 认为，人机界面的系统是机器通过接口传递给用户的，刺激感知器官接收信息，传递给大脑进行信息处理，然后由大脑发布指令控制肢体触点进行机器操作，而机器再通过接口回馈给用户 [7]。

在设计互动系统时，首先要了解用户的需求，确定系统的使用目标，即主要用于开发新的应用系统或者对现有系统进行更新 [8]。Preece 等指出，在设计互动系统时，应评估系统的操作是否简便易学、是否能够有效地使用以及是否能给用户带来愉快的体验。因此，使用性目标是为了让用户更轻松地使用系统，提高他们的工作效率，其中主要包括有效性、迅速性、安全性、功能性、易学性和易记性 [9]。

2 研究方法与实验设计

由于手机 App 种类繁多，各种收集类 App 之间的用户体验差异很大，因此本研究选择了比较常见的“高血压检测记录 App”作为研究对象。且据统计，截至 2017 年，我国 60 岁以上流动人口高血压患病率为 31.92%[10]，已严重危害人类健康，而高血压主要通过记录测量数据来观

察和调节。因此，手机软件商城中涌现出大量血压记录类 App，设计师对这种记录类 App 也有一定了解，在设计时能够更全面地理解产品。因此，本研究以使用“高血压检测记录 App”的用户体验作为设计师获取设计信息的来源。

在整个研究过程中，首先采用深入访谈法对用户体验进行研究，采集用户在使用过程中的体验，然后请不同资历的 App 设计师利用已有的用户体验进行 App 设计，并结合设计师在实验过程中的描述，采集本研究所需要的信息，对设计师在手机 App 设计过程中用户体验转化为设计思路的方法做出合理推断，再比较得出不同资历 App 设计师转化用户体验模式的异同。

验证阶段让另外一组 3 位不同资历的 App 设计师进行设计实验，以验证转化模式的可靠性。整个实验步骤规划分为 3 个阶段。

（1）用户体验研究与采集。此阶段采用深入访谈法，深入了解高血压患者在自我血压监测和记录过程中的经验和情境，包括工具、记录项目和社交层面，为设计实验提供参考。

（2）基于用户体验的设计实验。在此阶段，选取一组 3 位不同工作资历的 App 设计师，根据提供的高血压患者用户体验，分析并选择合适的用户体验，解释其选择的原因，再根据提供的 App 样本对血压检测记录 App 进行再设计，同时绘制概念草图并详细说明设计构想。最后对设计师进行简要访谈，以获取设计过程中概念细节。

（3）对比验证阶段，此阶段将邀请另一组 3 位不同资历的 App 设计师参与相同实验。他们将根据相同的用户体验和素材进行设计，分析其概念草图和口头记录，以探索他们的转化模式与前组是否相同。这有助于确保研究的可信度和说服力，并确认设计模式的普适性。

2.1 用户体验研究与采集

此阶段将深入研究和采集高血压患者的使用经验。探讨高血压患者对血压记录的需求，并仔细观察他们在测量和记录血压时的方法和流程。同时，记录用户高血压的原因和背景。实验的对象是 40 ~ 70 岁的高血压患者，根据最新的高血压诊疗标准，将年龄段分为儿童与成人高血压诊断标准 [11]。鉴于儿童在实验中表达方面的限制，故选择高血压高发的中老年人群作为研究对象。通过这种方式，了解不同年龄段的用户在使用现有 App 时的用户体验，并分析这些结果作为设计师进行设计的依据。

研究对象选定了 4 名高血压患者，受测者的年龄范围在 40 ~ 70 岁之间，男女各两名，并且都有血压记录的经验。用户体验受测者均须符合以下条件。

（1）血压持续或非同日三次收缩压≥ 140mmHg 和 / 或舒张压≥ 90mmHg，并经过专科医生诊断患有高血压的患者。

（2）被诊断出高血压的时间超过一年。

（3）均有血压测量以及记录的经验。

通过深入访谈法与受测者进行焦点式访谈，并邀请受测者就现有的智能手机上的高血压检测记录 App，探讨其在记录过程中的不足之处。访谈的过程是受测者与研究人员进行一对一的深度访谈，时间大约为 1.5 ~ 2 小时之间，事先通过电话筛选合适的测试对象，并请受测者携带平时用于测量血压的仪器。

2.2 基于用户体验的设计实验

在完成用户体验研究与采集阶段后，进入设计实验阶段。本阶段实验的对象是两组，分别为 3 位不同工作年限和资历的 App 设计师。

实验的步骤共分为两个阶段、4 个步骤，两个阶段分别为实验阶段和对比验证阶段；4 个步骤分别为实验前说明、用户体验评估、绘制概念草图以及实验后访谈。

实验 4 个步骤的详细内容如下。

（1）实验前说明。协助受测设计师了解本实验的运作流程，在进行受测前，根据准备的问题清单向受测设计师进行完整的说明。

（2）用户体验评估。受测设计师在理解实验说明后，针对提供的用户体验进行参考和评估。该阶段的主要目的是了解受测设计师如何参考、评估、挑选和使用用户体验。这部分可以从设计师的语言记录中了解设计师如何根据已有的 App 模型，选择他们认为重要的用户体验，评估它们的重要性，并将其用于设计工作中。

（3）绘制概念草图阶段。此阶段是受测设计师绘制概念草图的过程，请受测设计师利用本实验提供的用户体验，设计出 2 ~ 3 组血压记录的 App 模型。为了辅助实验分析，在受测设计师发展各个设计方案时，希望能从中获得有用的信息，包括想法来源于哪些用户体验、概念草图的特色以及草图特色与用户体验的关系。设计师在设计的过程中要时刻表达自己的想法，便于捕捉语

言中的设计思维，遇到不清晰的设计步骤可以在实验后要求设计师追加解释。

（4）设计实验后对设计师的访谈。实验后会对受测设计师进行一系列较为简单的访谈，以近似聊天的方式向受测设计师提出一些问题，希望从较轻松的访谈氛围中得到设计师如何使用用户体验发展设计构想的意见，并进一步补充实验中未收集到的信息或预期外的信息。

2.3 对比验证阶段

在验证阶段，邀请另外一组3位不同工作年限和资历的App设计师参与相同的设计实验。他们会被要求根据相同的用户体验，使用相同的素材进行设计，并仔细分析他们的概念草图和口头记录，试图总结出他们转化用户体验的模式。通过对这些模式的验证，可以确保此次研究的可信度，进一步提高研究的说服力和可靠性。同时，这种交叉验证的方法也有助于确认设计模式的普适性。

3 分析准则

将设计实验产出的3组案例，若干有效页面经过界面评估原则和现有归纳依据的分析之后，定义出以用户体验转化为设计概念的模式类型，以下针对各类型的分析准则进行介绍。

本研究定义了四大类型设计概念的构成因素，分别是操作提醒、信息提醒、规范提醒和情景重现。

3.1 操作提醒

操作提醒的判别准则是操作方式经验提醒的分析标准。通过对照用户体验，分析出不同类型操作提醒的转化模式。

3.2 信息提醒

信息提醒的判别准则包括信息聚焦化、切换信息和对应信息的要素。在解析概念草图时，将针对不同的信息强化方式进行区分，同时参照用户体验，分析出信息提醒的转化模式。

3.3 规范提醒

规范提醒的判别准则是屏蔽目标要素。在分析草图的过程中，将参照这个要素分析其中的概念表达，并根据用户体验，分析出属于规范提醒的转化模式。

3.4 情景重现

情景重现的判别准则在于用户在使用产品时产生的心理联想与界面的呼应。在分析应用元素的概念表达时，将参照此要素剖析，并根据用户经验，分析出属于情景重现的转化模式。

这些准则将有助于更清晰地理解设计概念的构成要素，从而为设计实践提供更有针对性的指导和建议。

4 App设计师转化用户体验的方法

本实验选取的第一组3位受测App设计师，分别具有五年、三年和一年的工作经验。通过对受测设计师概念草图、口语记录中概念转化类型的分析，统计其使用转化类型的频率，依据分析准则，可得出以下7种转化模式。

4.1 操作提醒转化法步骤之一

（1）分析用户在App中的操作模式，并将其与可反馈的功能对应起来。

（2）根据操作对应的功能反馈，思考常见的操作方式。

（3）以现有的App功能为基础，将用户操作经验等元素融入新的设计中。

4.2 操作提醒转化法步骤之二

（1）分析用户在App中的操作模式，并将其与可反馈的功能对应起来。

（2）根据操作对应的功能反馈，构想常见且普及的图形或造型元素。

（3）以现有可实现的App功能为基础，将用户操作经验等元素融入新的设计中。

4.3 信息提醒转化法步骤之一

（1）确定用户需要的信息反馈和操作过程中的重点内容。

（2）对这些信息进行放大处理，使用鲜艳的颜色和独立的图形等方式增强吸引力。

（3）在设计中加入操作的反馈，以引导用户更顺利地使用App。

（4）以实际可实现的App功能为基础，提出设计概念。

4.4 信息提醒转化法步骤之二

（1）确定用户操作和操作反馈之间的对应关系。

（2）对这些对应特征进行特殊处理，加强用户对其的认知。

（3）以需要反馈提示的内容和实际App使用情境为基础，提出设计概念。

4.5 规范提醒转化法步骤之一

（1）确定用户在操作中的步骤以及它们与目的信息的对应关系。

（2）通过点击后对其他信息进行遮蔽或模糊处理的方式进行设计。

（3）利用点击后的不同反馈，以实际可实现的 App 功能为基础，提出设计概念。

4.6 规范提醒转化法步骤之二

（1）确定用户在使用过程中对于使用性认知不清晰的部分。

（2）通过对信息进行特殊处理，让用户能够预测到信息的作用性，以便正确操作。

（3）利用不同的提示方式，以实际可实现的 App 功能为基础，提出设计概念。

4.7 情景重现转化法步骤

（1）深入了解用户在操作 App 过程中的意图。

（2）借助感同身受的方式联想用户在使用过程中所处的环境和遇到的问题。

（3）以实际可实现的 App 功能为基础，将环境特点或操作中遇到的问题呈现在设计中。

研究分析得出的转化方法旨在帮助 App 设计师在设计过程中使用用户体验中的信息来辅助设计概念的生成。尽管研究中得出的用户体验并不能代表所有用户体验的表达方式，但通过对第一组 3 位不同资历的设计师的转化模式分析，确实发现了四大类转化模式在快速有效地转化为设计方案方面的作用，且资深设计师使用转化模式的完整度均优于资历较浅的设计师。再经由与对照组 3 位不同工作年限和资历的受测 App 设计师实验结果分析之后，得到的结果基本符合第一组的结论，因此转化模式的分析结果基本可信。

结语

本研究通过两组不同工作资历的 App 设计师，将用户体验转化为设计理念的方法进行了比较和分析，提出了四大类转化模式，即“操作提醒”“信息提醒”“规范提醒”和“情景重现”。这些转化模式在不同资历的设计师间存在一定差异，但都旨在帮助设计师更好地理解如何将用户体验融入设计中。对资历尚浅的设计师和设计系的学生而言，这些研究成果提供了一个参考标准，帮助他们意识到与资深设计师在转化用户体验方面的差距，并提高自己的设计水平。对所有设计师而言，这些模式的提出有助于更好地自我定位，并与资深设计师相互学习，完善设计方法，从而提升设计质量。同时这些模式也有助于 App 设计公司制定新进设计师的培训和晋升标准。

引用

[1] Pahl G,Beitz W,Feldhusen J,et al.Engineering Design—A Systematic Approach[M].3.London:Springer,2007.

[2] Hassenzahl M.The Thing and I:Understanding the Relationship Between User and Product[M].Blythe M A,Overbeeke K,Monk A F,et al, Dordrecht:Kluwer Academic Publishers,2003:31-42.

[3] Kankainen A.Thinking Model and Tools for Understanding User Experience Related to Information Appliance Product Concepts[D].Helsinki University of Technology,2002.

[4] Garrett J J.The Elements of User Experience:User-Centered Design for the Web[M].Berkeley: New Riders,2002.

[5] Susan C.Cognitive Science and Science Education[J].American Psychologist,1986,41(10):1123-1130.

[6] Norman D. Some Observations on Mental Models[M].Gentner D,Stevens A L,New Jersey:Lawrence Erlbaum Associates,1983 :7-14.

[7] Preece J.A Guide to Usability: Human Factors in Computing[M]. 1.London:Pearson,1993.

[8] Sharp H,Rogers Y,Preece J.Interaction Design:Beyond Human-Computer Interaction[M]. 2.Hoboken:John Wiley & Sons, 2007.

[9] Preece J,Rogers Y,Sharp H.互动设计[M].陈建雄,台北:全华科技图书股份有限公司,2006.

[10] 李亚杰,李剑波,莘军龙,等.老年流动人口高血压和糖尿病患病现状及与自评健康的相关性研究[J].中国慢性病预防与控制,2022,30(5):381-384.

[11] 娄东辉,陆强,史文宗,等.秦皇岛市儿童应用中国和美国儿童高血压诊断标准的比较[J].中华高血压杂志,2012,20(8):733-737.

电力工程自动化中人工智能技术的应用研究

文◆国网山西省电力公司信息通信分公司　牛娜娜　万雪枫

引言

在我国计算机科技迅速发展的当下，人工智能技术能够通过对人的意识认知、逻辑思维能力进行模拟，建立仿真程度极高的AI应用模型。将该技术应用于各行各业的生产中，可以最大限度降低人工成本，提高作业的专业水平。特别是在电力工程中，人工智能技术的融入不仅可以优化电力控制模型，还能推进智能化设备操控和精准机械施工，细化实际工作运行参数的调节，最大限度地削弱意外带来的不利影响，从而推动自动化发展趋势的基础目标达成。本文从清晰认知人工智能技术概述的前提出发，深入探讨人工智能技术在电力工程中的概念和应用意义，进一步推进电力工程中人工智能技术的应用和研究进程，在设备故障诊断、强化现场管控、完善网络识别、构建级别权限等方面，实现有效的创新尝试，旨在为相关人员提供新的思考角度，进一步推动现代电力工程建设迈向全新的转型方向。

1 人工智能技术

1.1 优化控制模型

在原有的电力工程中，作业人员需要运用各种控制模型，实现整体项目的流程运转。应用人工智能技术可以更高效地优化控制模型。通过模拟历史模型的需求分析，结合先进的技术，对模型进行改良，实现功能上的扩展，从而减少使用的模型数量。针对模型使用中存在的一些问题，如运行加载数据时间长、无法中途变更需求以及限制严重等，人工智能技术的运用可以推动动态模型编程的建立。新型模型突破了原有形式的束缚，能够极大降低误差值，提高流程适配度，减少员工的工作压力。

1.2 推进智能操控

在电力工程的设备运行期间，工作人员需要定期查看作业状态，关注实践情况，避免其脱离自动化轨迹，失去控制。因此，项目运转期间对人工的需求较高。推动人工智能技术的普及和应用，可以更有效地实现流程的智能操控，提高机械辅助能力，进一步实现全面监测和精准预警，及时发现故障原因，并重点解决问题环节。

1.3 精准设备施工

使用人工智能技术对设备进行施工调控，可以显著提高设备施工的准确性，控制机械变动性，使其在规定区间内浮动。设备使用期间会产生磨损，磨损程度的严重级别会影响设备作业的精确度。通过智能化控制系统，能够依据精准记录的设备作业数据，推断磨损程度，进行效率评估，并针对设备问题，实施合适的处理手段。

1.4 细化参数调节

在电力工程施工期间，设备如出现设置偏差，传统的解决措施是选择专业的技术人员进行参数调节，但调整结果难以得到有效保证。然而，通过在作业中应用智能技术，可以及时解决简单问题。AI能够根据案例备用库中记载的信息，对关联参数进行细化调节，加强数据使用的扩展管理，提升电力工程的整体自动化水平。

2 电力工程中人工智能技术的实际应用研究

2.1 设备故障诊断

2.1.1 运行状态监控

在日常的电力设备工作中，人工智能技术需要对设备的实际运行状态进行动态监控。通常以智能与人工相结合的方式共同实现状态监控，

【作者简介】牛娜娜（1990—），女，山西太原人，研究生，研究方向：信息技术、人工智能。

通过对智能系统设置定期检查设备状态的任务，结合员工随机抽查监控信息的校验方式，进一步确保工程实施的安全性。

2.1.2 智能分析故障原因

运用智能技术，依据状态监控信息，以历史数据和当前状态信息实现资料整合。从案例库中搜索相对应的实况记录，如存在模糊检测结果，则判断其与记录问题的相似度。若相似度基本一致，则按照记录的问题产生原因进行分析，并给出最终结论；若相似度吻合程度低，则判断其为新问题，应新建文档，记录产生时间、情况、涉及环节，并在问题数据库中备案[1]。备案后，将该问题记录上传至技术人员维修平台，标注新问题的类别，并尝试性列举其余相似数据，为技术人员提供参考。

2.1.3 优化处理手段

技术人员可以通过智能系统对设备问题的判断和分析，结合自身的专业知识，对问题现象进行仔细观察，从而更高效地确认其真实的产生原因[2]。在设备维修、养护方面，智能系统起到了重要的辅助支持作用，有助于进一步提升处理效率和准确性。以变压器故障为例，传统的处理手段需要收集变压器中的气体，并逐一进行实验分析，以此得到诊断结果。该流程不仅会延长作业时间、浪费人力资源，而且诊断结果的精确度也存在较大差异。而利用智能系统，可以实现对变压器状态的实时监测和数据分析，快速准确地定位故障，从而大大优化处理流程。

2.2 强化现场管控

2.2.1 简化计算模型

在电力工程的作业流程中，维护其正常的工作状态，需要加强对相关的动态参数关注，强化现场管控。通过对作业现场设备和作业人员的管控，可以进一步确保工程自动化的顺利进行。运用人工智能技术，可以简化实际运行中的计算模型，实现更精准的参数调控。然而，模型应用过多会加大设备负荷，增加作业时长[3]。因此，应用智能系统进行有效管控，迫在眉睫。

2.2.2 提高容错标准

人工智能技术在电力工程中的运用，能够加强现场管控，提高计算模型的精准度，进而优化容错能力，使建设、监测、养护质量都能得到显著提升。高标准的作业系统容错能力能够减少偏差数据带来的不利影响。通过合理对比运行数据和标准数据，可以降低内部变量的关系复杂度，帮助作业人员更好地掌握设备的使用技巧，从而加强安全操作性能。

2.2.3 控制模糊响应

模糊数据响应是人工智能技术针对电力工程运营数据总量进行高效搜索、计算的重要组成部分。通过简化原有的工程自动化运行系统，构建精确的动态响应程序，并利用关联变量，完成整体流程的操控。在现场管控中，应用模糊响应能力，可以实现对整个项目建设范围的检测，推荐应急措施，并处理环节需求变更申请，从而推动工程自动化向高质量转型发展。

2.3 实现远程遥控

2.3.1 监控界面直观化

使用智能技术构建全新的远程遥控体系，以信息技术的最新成果应用为基础，实现监控界面直观化，帮助安检人员对整体系统的运行状态形成全方位、多角度的观察和认知意识。人工智能自动化的监控信息整理能力将重要的数据进行分类，形成更直观的图或表，展示给安检人员，为后续管理层实施的决策提供真实可靠的依据。

2.3.2 遥控开关高效化

在应用人工智能技术实现遥控开关高效化的情况下，工作人员要严格遵循安全规范和施工建设图纸，科学合理地利用远程遥控技术操作设备开关，实现规范作业。远程操作设备开关可以降低人工成本，优化流程细节，提升操作的专业化程度。

2.3.3 实时数据精准化

基于远程遥控技术，不仅能够传输电力工程作业数据，还能实现信息监控，将收取、发送的数据，在中央控制中心的后台储备库进行备注。备注通常包括类型（接收/发送）、时间（起始时间、传输时长、完成时间）、信息分类（故障检修/变更申请/业务回复）以及内容（具体事项）等。借助人工智能技术，推动远程遥控技术落实，进一步实现实时数据的精准化操作，为工程施工提供有效的信息支持。

2.4 完善网络识别

2.4.1 辨识非线性操作

针对网络识别技术进行优化，增强非线性操作的辨识能力，能够推进网络模型的简化发展进度。由于非线性操作具有难以明确阐述的特性，在面对网络化控制申请时，网络识别能力能够以此构建出适合的网络化控制模型，实现系统基础功能，得到灵活地应用和拓展。基于当前最优的选择条件，实施电力系统导入请求，并在充分利用大数据提升其自身的适应性和自主性的基础上，深化流程的优

化与应用，以期模拟基础的人类思维模拟，强化过程控制成效[4]。

2.4.2 升级大数据处理

电力企业应对电力工程中的自动化进行升级，包括提高网络的识别、分析技术，以及提升大数据的处理效率。以工程作业时期内的记录数据和技术人员的检修报告等为基础，为应用最新人工智能技术做好前期准备。

2.4.3 加强智能搜索、检测

通过数据网络控制技术，设置智能故障征兆的收集与分析机制。从作业平台系统中的设备信号状态和工作情况中定向采集，搜索关键词，实现模型模拟预判断和处理。人工智能技术中的大数据基础为后续技术人员在进行现场设备调控提供了依据，并通过模拟检测为技术人员提供高真实性的问题产生原因。此外，网络识别技术基于正常工作状态的监控信息，判断非线性操作，审查违规权限申请和异常状态警告，并提供详细的解析，进一步完善强大的后备辅助支撑。

2.5 构建级别权限

2.5.1 推动流程审核

在自动化的电力工程中，为确保作业流程的审核准确有效，需要设计一套完整、有效、精确的流转计划。在核心数据处理和重要需求报备更改时，智能系统必须获得管理层的权限命令。如果没有命令，系统无法依照更改需求的档案进行整体或部分工程结构的运行模式变更。在中央控制中心的计算机底层，应明确设计员工权限，包括管理员权限、技术人员权限、维修人员权限、安检人员权限等，确保业务流程的审核能够依照级别和权限高低进行。通过不同权限系统用户端口的核实操作，系统可以，根据批复结果处理申请内容或报告。

2.5.2 明确责任归属

设置智能系统内部的权限机制后，可以确定各部门成员的责任归属，避免事故爆发后，无法进行追责处理，延误工程的交付工期。人工智能技术可以根据不同部门需求，构建专业的系统平台，确保不同需求能够定向输送到对应管理层账号系统中。例如，测量人员主要负责工程进度调查。在调查期间，若发现作业问题或安全隐患，员工需要在智能系统中，使用个人的测量人员账号及时反馈问题。智能系统会将该反馈记录上传至相关部门管理人员的待处理界面，等待管理层根据问题的严重程度，通过会议形式决定具体处理措施。一旦处理措施确定，智能系统会将详细的责任清单下发至环节负责人账号中，并以红色感叹号作为加急标注，催促其尽快办理该业务。

通过人工智能技术的深化应用，能够有效解决责权归属问题。对于工程现场或监控随机抽查中发现的安全风险，智能系统将通过层级的动态数据传输功能调动相关资料，并针对具体事宜确定核心问题，提高数据分析和处理能力，确保通过智能系统平台，实现大事开会，小事通知，无事报备的“三件事”要求。

2.5.3 精细业务列表

在电力工程作业系统实现自动化的基础上，需要进一步细化员工的业务列表。基于此，面对电力企业承包的各类工程，应按照该工程的管理现状、任务指标等，将其划分为多个小组类别。例如，管理人员的系统可以划分为多个应用模块，如当前项目（类型、人员构成、基本要求、建设现状、工期）、库存管理（材料、设备、供应商）、维修管理（当职人员、后备小组、任务进程）、日程表（待处理、已处理、复核）等。其中，当前项目可以切换为其他项目，同时关联板块的信息也会随之更新。

结语

随着人工智能技术应用水平的不断提升，其对电力工程自动化建设产生决定性的影响，增加了工程建设现有的经济效益和社会效益。通过智能技术，电力工程建设能够实现实时监控和定期检测，一旦发现设备出现异常现象，系统能依据运行状态表现，分析产生原因，并为技术人员提供适合的维修方案。智能系统的运用强化了现场管理，实现了专业化生产，并推动了遥控技术和权限审核技术的广泛应用，助力电力企业大幅降低资金损耗，促使其在新时期实现持续、稳定的发展。

引用

[1] 张卫斌.人工智能技术在电气工程自动化中的应用研究[J].河北农机,2023(7):67-69.

[2] 彭乐伟.人工智能技术在电气工程自动化中的应用研究[J].光源与照明,2021(2):107-108.

[3] 王光明.电气工程自动化中人工智能技术的应用[J].湖北农机化,2020(12):155-156.

[4] 易汉鹏.智能技术在电力工程自动化中的应用[J].电子技术,2023,52(12):340-341.

基于双目视觉的智能小车避障方法研究 *

文◆贵州师范学院　莫章洁　邓　睿

引言

随着技术发展，扫地机器人、无人物流车等智能小车的应用得到快速普及，小车避障技术也得到重视。目前，常见的避障方案有基于超声测距的避障技术、基于红外测距的避障技术和基于激光雷达的避障技术[1,2]。前两者难以准确检测到如三脚架等具有镂空结构的复杂结构物体的距离，而后者则成本较高。基于此，本文提出一种基于双目视觉的智能小车避障方法。实验结果表明，此方法可有效实现小车前方障碍物检测功能。

1 双目视觉模型

双目视觉是利用两个相机，从不同角度采集同一三维场景的二维图像，再从两张二维图像中根据三角测量原理，获取三维场景中感兴趣目标相对于相机的纵深信息的视觉测量系统[3,4]。双目视觉模型如图 1 所示，即水平布置左右两个相机的双目视觉深度测量系统模型。

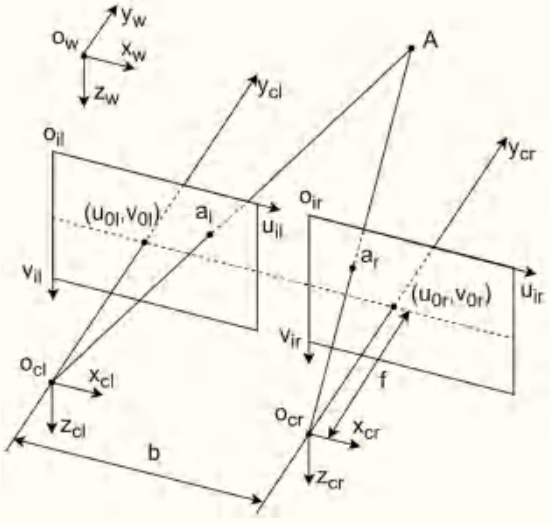


图 1 双目视觉模型

双目视觉模型主要包含以下 3 个组成部分。

（1）左相机坐标系 o_{cl}–$x_{cl}y_{cl}z_{cl}$ 和右相机坐标系 o_{cr}–$x_{cr}y_{cr}z_{cr}$。两个坐标系的原点 o_{cl} 和 o_{cr} 分别为两个相机的光心，光心之间的连线称为基线，其长度记为 b。y_{cl} 轴和 y_{cr} 轴分别为左相机和右相机的光轴。两个光轴互相平行且朝向相机前方。在实际应用中，习惯令左相机为主相机，因此，以左相机坐标系作为双目相机坐标系。

（2）左相机图像坐标系 o_{il}–$u_{il}v_{il}$ 和右相机图像坐标系 o_{ir}–$u_{ir}v_{ir}$。两个坐标系平面垂直于相机坐标系的光轴，其原点 o_{il} 和 o_{ir} 分别为各自相机成像平面的左上角。为了计算和分析方便，将其由相机光心的后方旋转平移至相机前方。u_{il} 轴和 u_{ir} 轴在一条直线上且平行于基线。两个相机的焦距相等，记作 f。光轴 y_{cl} 和 y_{cr} 与各自成像平面的交点为投影中心，其坐标参数分别为 (u_{0l},v_{0l}) 和 (u_{0r},v_{0r})。

（3）A 是三维场景中的一个点。它在左相机成像平面和右相机成像平面上的投影分别为 a_l 点和 a_r 点。为描述 A 点的空间位置信息，人为设定一个世界坐标系 o_w–$x_wy_wz_w$。此时，A 点的空间位置信息由其在世界坐标系中的坐标参数约束。因为世界坐标系和双目相机图像坐标系之间可通过刚体变换进行转换，所以 A 点在世界坐标系和双目相机坐标系中的坐标参数具有一一对应关

*【基金项目】贵州省普通高等学校青年科技人才成长项目（黔教合 KY 字 [2022]297 号）
【作者简介】莫章洁（1987—），男，贵州贵阳人，硕士研究生，研究方向：检测技术与自动化装置。

系。进一步，A 点的空间位置信息可由其在双目相机坐标系中的坐标参数描述。

若已知 A 点分别在左、右相机成像平面上的投影点 a_l 和 a_r 的坐标参数 (u_{al},v_{al}) 和 (u_{ar},v_{ar})，以及相机焦距 f、基线长度 b，左、右相机投影中心坐标参数 (u_{0l},v_{0l}) 和 (u_{0r},v_{0r})，则可根据三角测量原理，用式（1）解算出 A 点在双目相机坐标系中的坐标参数 $(x_{acl},y_{acl},z_{acl})$。

$$\begin{cases} x_{acl}=\dfrac{b\left(u_{al}-u_{0l}\right)}{u_{al}-u_{0l}+u_{0r}-u_{al}} \\ y_{acl}=\dfrac{b\left(v_{al}-v_{0l}\right)}{u_{al}-u_{0l}+u_{0r}-u_{al}} \\ z_{acl}=\dfrac{b\cdot f}{u_{al}-u_{0l}+u_{0r}-u_{al}} \end{cases} \quad (1)$$

2 相机标定与图像校正

上述双目视觉模型要求左、右相机光轴平行，左、右相机图像坐标系的 u_{il} 轴和 u_{ir} 轴在一条直线上。现实中，很难通过精确摆放相机的位置和姿态达到这个条件。为了使左右相机生成的图像满足这个条件，应求解左、右相机之间的位姿关系参数，再根据位姿关系参数对左、右相机生成的两幅图像进行后期立体校正。上述双目视觉模型还要求两个相机的成像平面与各自光轴垂直，但是，由于相机镜头装备工艺的限制，很难做到精确垂直，导致成像结果容易存在畸变。此外，对三维场景中某一点的空间位置信息的解算依赖于相机焦距 f、基线长度 b 以及投影中心坐标 (u_{0l},v_{0l}) 和 (u_{0r},v_{0r}) 等相机参数。

为求解上述参数，本文使用“张正友标定法”进行相机标定。该方法的基本原理是首先拍摄一组包含棋盘格图案的特殊图片，每张图片含有多个已知世界坐标系坐标参数的特征点。其次在拍摄的图片中识别这些特征点及其在图像坐标系中的坐标参数。最后根据这组图像中各特征点的世界坐标系坐标参数和图像坐标系坐标参数以及两个坐标系之间坐标参数的转换关系，解算出相机内部参数、畸变参数和左、右相机之间的位姿关系参数 [5]。

3 特征点检测与匹配

基于双目视觉测量双目相机视野范围内某个点在双目相机坐标系中的坐标参数，应首先获取该点同时在左相机图像坐标系和右相机图像坐标系中的坐标参数。使用 ORB 特征点检测算法实现特征点检测。该算法速度相对于经典的 SIFT（Scale-Invariant Feature Transform）算法和 SURF（Speeded Up Robust Features）算法可分别提高 100 倍和 10 倍，适合应用于嵌入式实时检测领域。

在对左相机图像和右相机图像的特征点检测后，应对其进行匹配，找出一组在两幅图像中均存在的特征点。为了确保每一轮匹配的精度，本文对两幅图像的特征点进行暴力匹配后，使用 RANSAC（RANdom SAmple Consensus，随机抽样一致）算法对匹配结果进行筛选。该算法利用两幅图像间单应性变换的一致性原理，对不符合单应性变换结果的特征点暴力匹配结果进行舍弃，以提升匹配的准确性。

4 障碍物检测

基于特征点检测与匹配方法可得到同时存在于左相机图像和右相机图像的多个特征点，以及特征点在左相机图像坐标系和右相机图像坐标系中的坐标参数。将这些参数代入式（1）可计算出特征点在双目相机坐标系中的坐标参数。

对于小车避障，应获取的信息是小车前方规定的区域内是否存在障碍物。根据小车的尺寸人为设定前方规定区域的边界。例如，规定双目相机坐标系中，x=250mm 的平面、x=−150mm 的平面、y=200mm 的平面，y=0mm 的平面，z=200mm 的平面，z=−200mm 的平面，一共 6 个平面围成的区域为规定区域。其中，将垂直与 x 轴的平面设定为 x=250mm 和 x=−150mm 是因为使用双目相机的左相机坐标系作为双目相机坐标系，该相机原点相对双目相机的中点向左平移约 50mm。接下来，将特征点的坐标参数与规定区域阈值进行比较，当特征点的坐标参数同时满足条件 −150mm<x<250mm、0mm<y<200mm、−200mm<z<200mm 时，判定为小车前方规定区域存在障碍物，反之则判定前方规定区域无障碍物。

5 实验与验证

为了验证基于双目视觉的智能小车避障方法的可行性，基于 OpenCV 开发了“基于双目视觉的智能小车避障系统”软件。并在桌面上搭建了实验场景。场景中以三脚架作为双目相机载具，模拟智能小车。场景中还摆放了眼镜盒、水杯、包装盒等物品，用于模拟障碍物。并且，为了测量障碍物与双目相机的实际距离，在桌面上铺设了坐标纸，实验场景如图 2 所示。

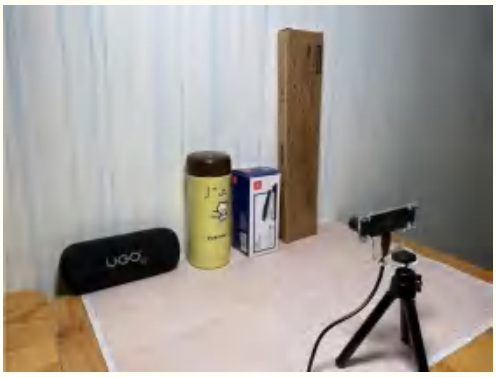


图 2 实验场景

首先，对双目相机进行标定，并对双目相机生成的图像进行校正。其次，启动系统，点击“基于双目视觉的智能小车避障系统”软件界面上的“开始检测障碍”按钮。再次，系统成功检测到了双目相机两幅图像中的特征点，并对特征点进行了成功匹配。同时，系统对三维场景中的障碍物进行了检测，无障碍时系统的检测结果如图 3 所示，系统检测结果为“无障碍”。初始状态下，眼镜盒等物品与双目相机的距离约等于 250mm，不在约束的“双目相机前方规定区域”内，因此检测结果与实际情况相符。

在保持其他物品位置不变的情况下，改变水杯的位置，将其移动到距离双目相机 150mm 处，即将其移动到约束的“双目相机前方规定区域”内。此时，系统依然能成功检测到双目相机两幅图像中的特征点，

图 3 无障碍时系统的检测结果

图 4 有障碍时系统的检测结果

并对特征点进行成功匹配，有障碍时系统的检测结果如图 4 所示，系统检测障碍物的结果显示为“有障碍”，与实际情况相符。

由实验结果可看出，基于双目视觉的智能小车避障方法能够较准确测量出双目相机前方规定区域内的障碍物，满足扫地机器人、无人物流车等智能小车应用场景的需求。

结语

基于双目视觉的智能小车避障方法使用双目相机采集的两幅环境图像，对图像中的 ORB 特征点进行检测、匹配和筛选。根据双目相机模型计算特征点在双目相机坐标系中的坐标参数。最后将特征点的坐标参数与规定区域阈值进行比较，判断双目相机前方规定的区域内是否存在障碍物。实验结果表明，该方法能够准确实现障碍物的检测，满足常规智能小车避障应用需求。

引用

[1] 王梓光.基于单目视觉的实时6DOF位姿定位手柄设计[D].成都:电子科技大学,2021.

[2] 吕伟康.基于FPGA的水下超声波测距系统设计[J].机械工程与自动化,2024(1):165-167.

[3] 孙立帅,王明泉,郝利华,等.基于双目视觉的无人机飞行高度测量方法研究[J].测试技术学报,2020,34(6):470-474.

[4] 侯禹光.基于双目视觉的手持式结构光测量技术研究[D].吉林:吉林大学,2023.

[5] 黄及远,李敏,谢兵兵,等.双目视觉关键技术研究综述[J].制造业自动化,2023,45(5):166-171.

基于信息安全技术的智能电网建设研究

文◆南方电网数字平台科技（广东）有限公司　全文举　梁子键　覃健峰

引言

智能电网的安全运转对于电力事业的发展具有深远意义。伴随着智能电网的建设，网络环境在电力体系运转中居于关键地位，潜在隐患因素侵入智能电网的概率也在增加。在智能电网建设中合理应用信息安全技术已成为重要课题。基于此，本文主要概括智能电网背景，探索信息安全技术的运行机制以及在智能电网中的应用策略。

1 智能电网安全现状概述

1.1 智能电网网络结构分析

智能电网系统由发电站、变电站和配电站系统组成，网络环境是数据调度网络。关于智能电网的网络模块，涉及生产控制区域以及信息管理区域两大部分。此前遇到的发电站等自动控制系统和数据调度网络都属于生产控制区域，而信息管理区域则涵盖了电力企业各个业务领域的管理系统[1]。具体而言，在生产控制大区内的发电自动化系统中，包括RTU、智能仪表、开关、SCADA系统等组成部分，实现了智能电网设备监控、运行状态监控、远程通信等多种功能。在变电站自动化系统中，包括一次化的智能设备，并对二次化设备进行网络分层，实现数字化电压、电流等参数的采集，做到信息集成与网络共享。关于配电自动化系统，涵盖了馈线管理以及配电管理两方面。以数据采集系统、配电信息系统和需求侧管理系统为依托，实现24h不间断远程监控与操作效果，智能电网运行更协调。同时，数据调度网络承载了数据信息传输的任务，并调度指挥指令。

1.2 智能电网的特点

第一，智能电网具有实时性、连续性的特征。控制系统应确保各类指令要素及时到达目标设备，同时保证电能生产连续。第二，在智能电网的生产网络中，不应有多余的软件，确保网络带宽资源应用高效，体现主机应用软件单一性特征。第三，智能电网高度集中，发电厂、供电公司等组织机构，都要听从智能电网的统一调度。第四，智能电网设备复杂多样，包括光、温湿度传感器、机械装置等多种设备，各个设备之间密切关联，体现出设备多样性特征。第五，智能电网中的认证机制不足。直接引入无线网络，则会增加控制设备暴露的概率，并带来安全隐患。

1.3 智能电网安全隐患分析

第一，由于智能电网业务相对特殊，无法为控制系统打安全补丁，会影响部分业务[2]。同时，部分电网业务容易被杀毒软件识别，干扰部分业务的正常开展。第二，部分工业控制系统存在后门。虽然后门的存在降低了系统维护的难度并提升便利性，但是访问权限过大，容易为工业控制系统带来额外的威胁。第三，目前我国应用的工业控制系统多来自国外，其中会存在间谍程序。程序窃取智能电网数据后，基于无线网络发送数据。而且，智能电网系统的电磁屏蔽效应不足，对间谍程序的识别能力较弱。第五，智能电网工业控制系统的硬件和软件存在缺陷，测试过程中，部分节点问题被掩盖。

2 智能电网中的信息安全技术

2.1 入侵检测技术

在智能电网中，建立高级测量体系（Advanced Infrastructure，AMI）并形成AMI网络，具体组成部分有智能电表、集中器、计量服务器、通信网络等，是外部因素侵入的重点。目前，常见的AMI网络攻击包括基于连接的攻击、基于设备的攻击。因此，必须应用相应的检测方法，并

【作者简介】全文举（1979—），男，河北迁安人，本科，助理工程师，研究方向：计算机。

关注误用、异常和规范等方面[3]。由于基于规范的检测成本较高，目前多采用基于误用和异常的检测模式。其中，基于误用的检测模式，应重点关注对特征代码库的匹配情况，并且只能检测已知的攻击行为。由于AMI网络系统属于新兴事物，对应的不是传统的攻击手段，可见基于误用的检测模式并不可靠。基于异常进行检测时，应收集智能电网用户行为并建立用户模型，利用机器学习方法，分析用户的活动行为。如果行为不符合正常模型，则判定为行为异常。可见基于异常的检测模式，能够适应AMI网络的应用特征。

第一，在检测恶意代码入侵现象时，可以根据信息熵以及ARM指令的统计特征，完成可执行代码的检测任务。但是，软件一旦被感染控制，经过字节置换处理，就能逃避检测。在实际操作中，可以提取4个不相关特征，基于SVM进行数据训练测试，有效提升检查精度[4]。第二，针对DDoS攻击，应利用智能电表以及网络协议中的漏洞。应对DDoS攻击时，主要历经攻击防护与攻击检测两个阶段。在DDoS攻击发起前，应维护系统并完善协议安全等级，做好资源分配与审计工作。在攻击检测阶段，应关注攻击源并采取可靠的措施，如利用贝叶斯蜜罐博弈模型，提升攻击行为的检测效率并降低能源消耗。第三，关于电量数据欺骗的应对，应注意用户用电量与时间、位置和用户性质之间的联系。在提取上述要素的特征后，借助SVM区分正常数据和异常数据，或者根据不同的时间维度明确统计特征，随后利用PCA降维法与机器学习方法进行检测，增强对用户窃电的应对能力。

2.2 漏洞挖掘技术

基于智能电网的特征，一般从系统、终端与协议3个层次进行漏洞挖掘。系统通过污点传播分析、渗透测试等机制，验证仿真系统并检测发掘漏洞。关于终端设计，以Python语言的Fuzz开源框架为依托，发掘PLC、智能终端、继电保护等组件的漏洞，深入分析工控系统存在的问题。借助模糊测试机制，分析智能电网协议并检测攻击行为的特征。

在漏洞挖掘进程中，通常要同时使用多种挖掘技术。常见的漏洞挖掘技术只能应对浅层的漏洞，或者进行简单的分析。若能综合应用模糊测试以及符号执行方式，那么就能够找到二进制中的漏洞。模糊测试方式能够挖掘出智能电网公有协议中的漏洞，在综合应用隐马尔科夫、统计算法的基础上，形成优化重构法，让漏洞挖掘机制更加完善。同时，借助心跳检测的存活检测机制以及一致性的检测方法，判别被测系统的状态。在结合符号执行机制后，由模糊器探索兴趣路径，由此形成预约控制效应并增强系统性能。

检测漏洞后，还要验证漏洞。借助漏洞验证机制，挖掘并验证漏洞，分析漏洞的情况以及影响程度，避免漏洞漏报，使漏洞排查结果更准确。以智能电网系统漏洞为基础，设计攻击脚本并研发相关工具。以典型的电力工控实验环境为依托，明确漏洞检测以及攻击验证的具体程序。漏洞验证工具开发进程中，应用到Java语言和Python语言脚本。根据漏洞的构造原理，成功触发漏洞。关于识别已知漏洞的方面，采用CNVD、CNNVD等公开的漏洞库。关于挖掘潜在漏洞的方面，首先是建立测试用例，借助模糊测试方法进行测试，其次进行风暴测试以及协议完整性测试，最后是弱口令检测。测试漏洞后，开发相关脚本以及攻击验证的工具，如拒绝服务漏洞验证、远程控制漏洞验证、信息获取漏洞验证等。

2.3 隔离交换技术

隔离交换技术是传统防火墙技术的升级，通过在智能电网中部署安全隔离交换设备，有效提升智能电网的安全性能。借助网络安全隔离交换机制，切断内外部网络的联系，及时阻断不同网络环境之间的数据交换。服务器负责保护智能电网的内部网络，从根本上避免数据库与操作系统被外部因素入侵[5]。在内部网络环境中访问外网时，亦不会导致信息泄露现象。此外，通过数据交换平台机制，充分满足数据交换的业务需求。在智能电网安全隔离与信息交换技术的模型架构体系中，终端用户的访问行为以及对智能电网的运行监控过程，都在内部网络中进行。在内外部网络交互体系中，涵盖了缓存的交换处理以及安全保障机制。在安全保障体系中，融合了边界隔离、入侵检测、安全审计、身份鉴别等模块。在内外部网络的交互进程中，纳入了网络防病毒体系，以便及时检测数据交换进程中的病毒要素，最终满足智能电网在数据交换进程中的安全交互需求。

2.4 安全态势感知和预测技术

安全态势感知与预测是智能电网信息安全机制的重要组成部分。例如，构建多维度安全事件的关联分析模型，适应智能电网中的设备应用领域、出厂厂家、型号等要素差异巨大的特征，以及数据采集标准不一致的现象。在整合多元异构的数据并存储

后，基于安全事件的关联分析机制，有效融合上述数据，由此分析出潜在的异常活动以及网络攻击意图。分析多源数据后，通过聚类、分类、关联等处理，获得更高层次的安全态势信息。在智能电网业务环境中，利用多维事件安全分析机制，能够从资产关联、逻辑关联、时间序列等角度进行关联[6]。同时，依托聚类算法、累积概率等机制，形成智能电网异常的识别模型，由此增强异常行为的识别能力以及网络安全预警的性能。另外，基于攻击场景的攻击链识别模型也是典型应用。依托恶意代码防护技术以及知识图谱技术，构建了攻击链的识别模块，增强对恶意代码与攻击链的监测识别能力。在网络攻击行为中深入发掘，绘制形成网络攻击链条，作为安全事件溯源的依据。基于大数据技术检索原始日志，评估攻击行为对智能电网的影响，以及安全体系的防御效果，同时体现出攻击全过程，帮助工作人员及时定位潜在的风险因素，有效弥补传统人工评价风险的短板。此外，立足于攻击链，能够建立智能电网安全处置图谱，开发智能电网安全事件的自动响应处置体系。一旦智能电网遭受攻击，借助自动匹配机制，自动形成网络安全的应急预案，由此提升智能电网安全事件的处理效率。

3 智能电网关键信息安全技术应用探索

在信息安全技术的应用分析阶段，以智能电网的调度系统为例，探索信息安全技术的应用方式。借助调度系统，及时掌握智能电网各个运行阶段的隐患，并借助技术防护效应，避免数据信息泄露，降低智能电网的运行事故概率。在电网调度控制前期，通常隔离开系统网络与广域网，让全部设备软件在独立的环境中工作。伴随着电网的智能性不断上升，电网与终端的交互也愈发丰富，传统的隔离策略与防护体系难以为继。因此，应引入边界防护、安全等级防护等多种防护机制。

3.1 防护策略分析

在划分智能电网子系统的基础上，合理应用横向隔离方式保护系统，让智能电网运维进程更简易。依托各个子系统特性，做好数据传输的安全保护工作，并加大相关软件的开发力度，增强系统安全监控性能。随后，从安全防范与安全认证的角度出发，构建安全保护体系，进而监控智能电网数据运转全过程，降低人员主观因素对数据操作的影响。接下来，借助风险识别机制，让安全防御更主动。由于智能电网规模不断扩大，数据类型愈发复杂，借助安全态势与感知思想，综合发挥软件与硬件技术的优势，及时预测并杜绝智能电网运行中的危险因素，让安全保护系统更可靠。

3.2 基于可信技术建立主动防御体系

可信技术的应用意味着计算结果吻合预期，而且计算过程足够顺畅，确保数据信息安全可靠。关于“可信技术”的应用，就是在智能电网的硬件环境中建立一个受信任保护的网络。一旦外部因素侵入到智能电网，调度系统能够自动响应，由此形成自动化防御体系。可信计算平台的应用，实现了智能电网监控可视化。在智能电网调度控制系统的服务器内部，实现了可信加密模块的可信引导。依托信任链，让数据要素安全传输到操作系统，确保操作系统稳定工作。同时，从静态和动态两个角度，保证数据信息完整。静态完整性的评价是在保证检测度量完整性的基础上，确保智能电网系统可靠；动态完整性则关注系统数据以及代码段，评价量度是否可靠，由此评价智能电网是否可信，同时优化控制机制。

结语

信息安全技术的应用，对于智能电网的建设与发展具有深远意义。未来将继续加大智能电网建设中的信息安全技术探索力度，让智能电网体系更加稳定和谐，更好地服务全社会用电以及电力事业的发展进程。

引用

[1] 李志强.智能电网面临的安全隐患及防范策略[J].大众用电,2023,38(3):52-54.

[2] 田昊.智能电网信息安全风险及防范对策探究[J].中国管理信息化,2022,25(24):93-95.

[3] 方嘉祥.智能电网信息安全及新技术研究综述[J].科技与创新,2022(4):21-25.

[4] 严彬元,刘俊荣,周琳妍.智能电网信息安全与网络结构优化路径[J].网络安全技术与应用,2020(11): 131-132.

[5] 程杰,尚智婕,胡威,等.智能电网信息系统安全隐患及应对策略[J].电气应用,2020,39(4):99-102.

[6] 张佳发.信息安全技术在智能电网中的应用[J].通信电源技术,2020,37(2):153-154.

基于 5G 技术的卫星空天地一体化网络安全研究

文◆广州广哈通信股份有限公司　邱　涛　张聚明　杨　光

引言

针对形势复杂多变的网络安全环境开展系统性的保障工作，已成为目前网络管理严峻形势的迫切需要。同时，卫星网络的诊断、发现和预警网络安全事件很难通过单一数据源和传统空间数据类型实现，因此 5G 技术的发展给卫星空天地一体化网络安全提供了新的思路。

1 卫星空天地一体化网络简介

卫星空天地一体化网络是指通过卫星、无人机、地面基站和终端设备的协调工作，实现广泛覆盖、无缝连接的网络体系 [1]。该网络利用 5G 技术的高速率、低延时和大连接优势，整合天地多种资源，提供高效稳定的数据传输服务。其应用涵盖广泛，从应急救援、远程监控到全球范围的应用，极大提升了信息传递的可靠性和实时性，为各类应用场景提供了坚实的技术支持。

2 空天地一体化监测体系

空天地一体化监测体系是通过集成天基、空基和地基监测手段，实现全方位、多层次的综合监测网络。该体系包括卫星监测、无人机监测和地面监测 3 个主要部分。卫星监测主要利用高轨和中低轨卫星进行大范围、全天候的环境和网络安全监测。空基监测通过无人机和其他临空设备，提供灵活、高精度的实时监测，特别适用于灾害现场、交通枢纽等重点区域的监控。地面监测则由宏蜂窝、微蜂窝和皮蜂窝基站组成的地面网络来实现，采集和传输地面终端设备的数据，确保信息的快速汇集和处理。在数据处理方面，利用 5G 技术和大数据分析平台，快速处理和分析来自不同监测设备的大量数据，生成精准的监测报告和预警信息。

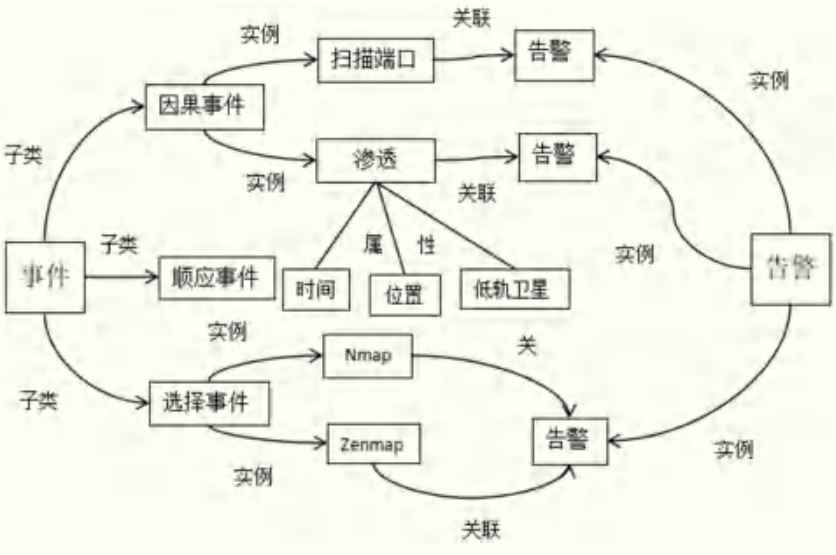


图 1 天地一体化网络的网络安全知识图谱

3 网络安全测绘方案

3.1 网络安全知识图谱构建技术

网络安全知识图谱构建技术是一种通过集成和关联多源信息，建立系统性、结构化网络安全知识体系的方法。天地一体化网络的网络安全知识图谱如图 1 所示，该图谱将各种安全事件分为 4 类，即回溯事件、脆弱事件、预警事件和活跃事件，每类事件又细分为子类，并通过实例

【作者简介】邱涛（1977—），男，湖北武汉人，硕士研究生，工程师，研究方向：5G 核心网设计与网络解决方案。

进行具体化。在知识图谱中，扫描事件和暴露事件通过关联节点进行连接，表示不同事件间的联系和影响。具体的安全工具如 Nmap 和 Zenmap，被用来进行事件的检测和分析，它们的功能性被映射到特定的安全事件中[2]。结合 5G 技术知识图谱将传统的静态安全信息转化为动态的、可操作的安全知识，通过对事件的分类和关系的构建，使网络安全管理人员能够快速识别潜在威胁并采取有效的防御措施。

3.2 无人机信息采集

无人机信息采集是空天地一体化监测体系中的关键组成部分，无人机信息采集示意图如图 2 所示。无人机群在空中网络中执行多种任务，包括实时监测、数据收集和传输。无人机通过在近空平台系统内飞行，能够灵活地应对不同的监测需求，并将采集到的数据迅速传输至地面站。不同层次的网络架构如 GEO、MEO 和 LEO 卫星构成了空间网络，提供大范围的监测和覆盖。高空平台系统和无人机群则组成了近空网络，进行高精度的实时监测。地基系统则通过地面蜂窝网络完成数据的接收和处理[3]。通过 5G 技术，无人机群在近空平台系统中执行实时监测和数据采集任务。无人机利用 5G 的高速传输和低延时特性，将采集的数据迅速传输至地面站，实现高精度监测。

图 2 无人机信息采集示意图

3.3 跨域攻击溯源安全

利用 5G 技术的高速率和低延时特性，该技术可以实时监测和分析来自不同领域的攻击行为。通过卫星、无人机和地面网络的协同工作，构建起一套全面的监测和溯源体系。卫星负责大范围的初步监测和数据采集，无人机在近空平台系统中提供高精度的实时监控，地面网络则通过 5G 技术实现快速的数据传输和处理。这一体系能够快速定位攻击源头，分析攻击路径，并追踪攻击者的活动轨迹。跨域攻击溯源安全能够有效应对复杂多变的网络攻击，提高空天地一体化网络的整体安全性，确保各类通信和数据传输的稳定与安全。

结语

空天地一体化网络安全体系通过融合天基、空基和地基资源，利用 5G 技术构建了全面、实时、高效的监测和防护机制。通过卫星、高空平台系统和无人机群，实现了广覆盖、高精度的监测，确保在复杂环境和紧急情况下，快速采集和传输数据。网络安全知识图谱构建技术为系统提供了结构化、安全性的基础，提升了应对复杂安全事件的能力。无人机信息采集利用 5G 技术的高速传输和低延时特性，保证了数据的实时性和准确性。跨域攻击溯源安全通过协同监测和溯源分析，有效应对网络攻击，提升了网络的整体安全性。5G 技术为空天地一体化网络安全提供了坚实的技术支持。

引用

[1] 刘昊昱.卫星与5G融合的网络架构设计与优化[J].无线互联科技,2024,21(1):21-23.

[2] 高菲.卫星天地一体化网络势如破竹——第十二届卫星学术年会在京召开[J].卫星应用,2016(3):84-85.

[3] 王蛟,曲艳华.空天地一体化网络流量检测技术研究[J].中国信息化,2024(5):62-63.

基于人工智能的计算机应用软件开发技术

文◆山西工程职业学院　王晓红

引言

随着计算机应用软件需求的增多，人们对计算机应用软件的开发提出了新的要求，传统的开发技术存在诸多问题，难以保障计算机应用软件的功能。以人工智能为基准的计算机应用软件开发更为便捷。未来的计算机应用软件开发中需要继续推广人工智能新技术。基于此，本文从人工智能环境下计算机应用软件的开发困境着手，重点分析应用软件开发中的人工智能新技术，以期为实际工作提供技术指导。

1 基于人工智能技术的计算机应用软件开发现存困境

1.1 语言习惯偏好

人工智能技术下计算机能够模拟人的行为进行相应操作，完成各项任务，提高工作效率和质量。针对计算机应用软件开发这一复杂性工作，人工智能技术较为适用。人工智能环境下开发计算机应用软件时，应考虑使用群体的语言习惯，若未考虑这一方面，则会导致计算机应用软件的开发效果不佳，软件功能和操作等无法满足使用者的需求。同时，软件用户具有个体差异，用户来自不同国家，有各自的语言表达习惯，在开发应用软件时应充分考虑个体差异，增强软件的语音识别功能[1]。

1.2 人机互动

利用人工智能技术作为开发计算机应用软件的核心技术，应保障软件强大的人机交互特性，使用户与计算机之间能高效互动，一旦计算机接收到用户的相关需求指令，应立即进入智能化操作模块。市场上一些计算机应用软件的人机互动能力较差，系统接收的词汇量较少，智能化模块在数据分析、提取方面效率不高，导致数据处理耗时长，是计算机应用软件开发的一大难点。

2 基于人工智能的计算机应用软件开发原则及路径

2.1 开发原则

2.1.1 确保软件技术可行性

计算机应用软件有其指定的使用对象，在设计软件架构以及功能等方面应从使用对象的角度来考虑。只有保障计算机应用软件的性能以及功能等与用户需求相一致，方可体现软件对实际工作的价值。为此，人工智能下的计算机应用软件开发中，相关人员应贯彻技术可行性原则，在开发阶段引入多样化、先进性技术，提前调查用户需求。例如，开发人员应提前与用户群体沟通，分析用户群体对软件的功能、操作等特殊要求，使开发人员在此前提下优化软件架构，并设计多种界面模式[2]。

2.1.2 确保软件运维便捷性

针对计算机应用软件开发，需要多部门、多岗位人员高度配合，方可达到开发目标。初期阶段，开发人员应获取用户对计算机软件界面、功能等方面的需求，并围绕需求设计软件架构。当基本的设计工作结束后，为检验计算机应用软件的安全性、实用性，应展开一系列系统测试，依据测试过程以及结果调整软件参数或者运行程序。基于人工智能技术开发计算机应用软件时，应遵循软件便捷运维原则，提高应用软件的运行水平。即使软件在运维过程中发生异常，智能化模块也能快速启动故障预警及排查机制，确定故障位置，并进行自检、自查或者由人工修复故障。

【课题】山西省教育科学“十四五”规划2022年度课题“高职院校人工智能专业的建设”（GH-220096）
【作者简介】王晓红（1972—），女，山西介休人，硕士研究生，副教授，研究方向：人工智能、计算机网络。

2.2 开发路径

2.2.1 实现循环网络与多层感知技术融合

计算机应用软件开发引入人工智能技术，应采用人工智能网络技术。在当前的技术条件下，人工智能网络技术广受关注，在很多领域都有相对成功的应用。从根本上分析，人工智能网络是一种模拟人脑神经结构的分布式处理技术，应用该技术时将设置若干信息处理单元模块，且各模块具有一定的独立性，在一定的条件下能够高度协同。一旦智能网络接收到指令，将自动处理该指令，并依据处理结果完成相应的操作。同时，人工智能网络在信息处理方面具有显著优势，能够在短时间内调动多种算法来处理海量数据，从数据中提取出关键信息。基于人工智能的计算机应用软件开发中，应注意保持循环网络与多层感知技术的高度融合，以保护、整合、筛选以及利用数据，一旦发现数据异常，智能化模块立即扫描数据并标记异常数据，以便后续人工排查和处理问题。

2.2.2 配置网络空间及感知网络

计算机应用软件开发中采用人工智能代理技术，此技术能够实时感知软件的各方面情况，采集到环境等信息后再由智能化模块执行相应的指令。网络安全方面应用人工智能代理技术，能够识别不法分子对系统的入侵行为，并同步采集不法分子的入侵时间等数据。利用人工智能代理技术，根据需求重新配置网络空间，实时关注环境情况，决定是否需要启动网络保护。因此，任何情况下利用人工智能技术开发计算机应用软件时，都应配置网络空间及感知网络，快速识别和处理网络风险。

3 计算机应用软件自动化开发方法

3.1 组件开发

为达到预期的开发目标，应率先开发组件。具体来说，专业人员应遵循一定的标准将应用软件拆分为多个部分，获取若干系统组件，此后对每一系统组件开展详细化开发。一方面，开发人员应以用户需求为前提进行开发。另一方面，应着重分析软件的类型，据此选择最优的自动生成方式。开发组件时应重点关注以下方面，一是整合大量的已有信息，将信息集成到专门的数据库系统中，保障组件自动生成阶段的全部数据均存储于数据库中。二是优化组件自动生成程序，规范执行此程序，完成组件的自动生成任务。三是针对关键组件中的重点参数，应调整个别参数。四是完成测试环节，评估组件性能，依据测试结果完成修复。

3.2 流程设计

流程是影响计算机应用软件开发效果的重要方面。为开发出符合用户需求的计算机应用软件，应重点关注流程设计方面。借助自动化、人工智能等新技术开发计算机应用软件，直接由自动化、智能化模块取代人工来进行软件功能等的开发和优化。针对各种类型的计算机应用软件，开发之前应了解软件的运行流程，从效率、安全等角度减少不必要流程，增强不同流程之间的衔接性。

3.3 系统安装

应用软件的开发工作结束后，应引入自动化、智能化技术进行安装，此过程中只需要安排少量人员负责监督，一旦发现问题，应尽早处理。多年来应用软件自动化开发技术虽有一定的应用，但还存在诸多的技术问题，并不能实现完全自动化安装。通过人工监督可保持人工与自动化模式的高度结合，由人工处理自动化模块无法处理的安装问题。在计算机系统中安装各类应用软件时，应关注格式转换方面，保障系统与软件的兼容性，以发挥软件的功能优势。

4 人工智能下的计算机应用软件开发技术及其应用

4.1 人工智能神经网络技术

人工智能神经网络为典型的智能化技术，此技术参考了人脑的神经构成和分布，相当于大规模的并行分布处理器。面对较为复杂的问题，应利用人工智能神经网络构建针对此问题的神经网络，在该网络中设置若干信息处理模块。每一信息处理模块负责特定范围和类型的数据，在数据量庞大的情况下，不同信息处理模块应相互协同，通过各种运算、分析方法筛选数据，为软件运行提供有效保障。相对来说，人工智能神经网络的运算能力强大，网络流程度高。如果用户对运算效率等有严格规定，那么可以采用该技术。人工智能神经网络不仅具备数据运算功能，还具备强大的数据存储、组织信息能力，可模仿人脑的思考过程。另外，神经网络的结构特征决定了其强大的安全防护作用。原有信息系统的安全防护能力交叉，即使采取多种网络安全技术，仍会面临数据丢失、泄漏等问题。而神经网络可实时存储数据，能从根本上提高数据安全性，无论是数据存储还是传输过程，都能营造安全条件。同时，智能化模块能够精准识别数据、网络、设备等方面所面临的风险，实现预警和防控。计算机软件运行期间，神经

网络技术能够迅速检测软件的各类入侵信息，一旦入侵软件中存在安全风险，则可快速识别风险并立即拦截。通常而言，为提高神经网络的数据处理、风险识别能力，在开发计算机应用软件时应保持入侵检测、循环网络、多层感知等技术的融合，构建更为完善的入侵检测神经网络系统。

4.2 人工智能专家系统技术

将专家系统应用于计算机应用软件开发过程中，可提高软件的入侵检测能力，如专家系统可实时监测、智能分析用户的操作行为等。一旦用户存在异常入侵问题，专家系统可自动调取相关数据，判定是否为异常入侵，启动预警。例如，专家系统中的 NIDIS 技术，此技术能够在入侵检测环节发挥重要作用，具体的工作中应采用新型统计计算方法，检验评估用户每一次的操作行为。NIDIS 系统中包含各类入侵场景编码，其中融合了诸多统计学方式。系统中存储有用户的各种操作行为数据，相应模块遵循一定的规则来评估数据和分类数据，并依据有关算法计算数据之间的关联性，构建模型。模型中存储有用户的权限以及特征数据，还包含用于监测用户行为的子系统，在这些构成部分的高度配合下实现了随时分析用户行为的目的 [3]。

4.3 人工免疫技术

人工免疫技术是人工智能的典型技术。目前我国逐步构建了较为完善的计算机网络，在网络体系中包含了大量的数据，增大了计算机网络的管理难度。例如，缺乏全面化管理及控制，在运行计算机软件时面临异常入侵，一旦网络安全防护不足，必将影响软件信息安全。当应用人工免疫技术后，计算机软件的防护能力显著增强，不仅能够准确识别病毒，还能够快速杀毒和修复系统，为用户创造良好的软件操作环境，减少内外部因素对软件的负面影响，维护软件中的数据完整性和准确性。

通过科学应用人工智能新技术，在相对复杂的互联网环境中保障计算机软件的运行安全。同时，人工智能模块还可以自动检测软件的入侵行为，查杀病毒，以免计算机应用软件被异常入侵。计算机应用软件中采用人工免疫技术，可在否定选择、克隆选择、基因库方面发挥作用。以基因库为例，计算机应用软件运行阶段，基因库能够实时分析入侵检测的基因片段，保障软件对病毒的识别与防控能力，并将病毒数据存储于软件基因库，后续一旦面临相同的软件，智能化模块能够自动调取基因库中的数据进行对比，识别病毒。现阶段的网络环境下，病毒种类日渐增多，计算机应用软件中采用人工免疫技术，可提升软件运行水平。

4.4 人工智能 Agent 技术

分布式人工智能技术应用于计算机系统中，人工智能 Agent 技术起着关键作用。与其他技术相比，Agent 技术可自动执行各种任务，但在具体的工作中应配备各种类型的传感器，由传感器自动采集环境信息，评估计算机应用软件的运行环境。人工智能 Agent 技术可实时感知计算机软件所处的环境状态，以自身对环境的评估结果为参考完成自我调节，执行任务命令。由于人工智能 Agent 技术的发展现状，其在安全防护方面该技术的优势明显，能够自动感知、识别和处理环境中的安全风险。近年来人工智能 Agent 技术的相关理论日渐增多，产生了大量的技术实践，增强了此技术的环境感知能力。计算机应用软件方面应用 Agent 技术时，应结合软件类型和运行特点，合理选用 Agent 插件。Agent 插件作用于安全防护的功能对比如表 1 所示。

表 1 Agent 插件作用于安全防护的功能对比

功能	功能详情	常规防护系统	安装 Agent 插件
漏洞管理	系统软件漏洞	无	有
	CMS 漏洞	只检测	检测 + 修复
基线检查	高危风险配置检测	无	有
异常登录	异地登录 / 暴力破解	有	有
Webshell 检测	网站后门查杀	只检测	检测 + 处理
主机异常	异常行为分析	无	有
	异常网站链接	无	有

结语

计算机应用软件开发中人工智能技术具有显著优势。为提高人工智能环境下的计算机应用软件开发水平，应结合应用软件的类型和操作要求，合理规划开发路径，做好技术组合。未来，计算机应用软件开发应继续推广和创新人工智能技术。

引用

[1] 冯景利.基于人工智能的计算机应用软件开发技术应用分析[J].信息记录材料,2022,23(9):189-191.

[2] 张海玉.基于人工智能的计算机应用软件开发技术研究[J].软件,2022,43(5):82-84.

[3] 安永刚.计算机应用软件的需求分析与开发[J].数字技术与应用,2022,40(7):166-168.

网络安全视角下的国产化 OA 办公系统部署与防护策略研究

文◆河北省财政厅　伍均玺
河北省财政厅一体化运维中心　胡冬梅

引言

在当今的信息时代，国产化 OA 办公系统在企业中发挥着越来越重要的作用。本研究旨在从网络安全视角出发，探讨如何部署和加强国产化 OA 办公系统的防护策略。首先，通过分析当前网络安全威胁形势和国产化 OA 系统存在的潜在安全风险，提出相应的部署与防护策略。其次，探讨身份认证、访问控制、数据加密、漏洞修复等方面的具体防护措施。最后，提出完善安全审计和合规性管理、持续加强安全意识培训等建议，以期提升国产化 OA 办公系统的整体安全性。

1 国产化 OA 办公系统的发展现状

国产化 OA（办公自动化）系统是指在国内独立开发、定制或适配的办公自动化软件系统，具有符合国内办公需求、便于维护升级、适应国内法规的特点。近年来，随着我国信息化建设的不断推进，国产化 OA 办公系统在企业和组织中得到了广泛应用并取得了长足发展。

国产化 OA 办公系统在功能上不断完善，逐渐拓展至办公流程管理、文档管理、协同办公、移动办公等多个领域，满足了用户多样化的办公需求。在技术上，国产化 OA 系统逐步实现了与国际先进水平接轨，表现出更高的性能、更好的用户体验和更强的扩展性。此外，国产化 OA 办公系统在安全性方面也取得了显著加强。

2 网络安全的基本概念

网络安全是保护计算机系统、网络系统和数据免受未经授权的访问、修改、破坏或泄露的一系列措施和技术的总称。在数字化时代，网络安全的重要性愈发凸显，由于大量的个人、企业和政府数据都存储在网络上，任何安全漏洞都会导致严重的后果。网络安全涉及防范各种类型的攻击，包括但不限于计算机病毒、木马、网络钓鱼、勒索软件等。这些攻击会导致数据丢失、个人隐私泄露、系统瘫痪等严重后果，因此需要采取相应的防御措施 [1]。同时，网络安全也包括保护网络通信的安全性，确保数据在传输过程中不被窃取或篡改，涉及加密技术、安全通信协议等手段，防止黑客或恶意攻击者截取和篡改数据。此外，网络安全还包括访问控制、身份认证等技术，确保只有授权用户才能访问特定的资源和数据，防止未经授权的访问和数据泄露。

3 国产化 OA 办公系统部署与防护技术分析

3.1 国产化 OA 办公系统架构与特点

国产化 OA 办公系统作为一种针对国内办公需求开发的软件系统，具有独特的架构和特点。其架构通常包括前端界面、后台服务、数据库等组成部分，并围绕办公场景提供全面的功能支持。国产化 OA 办公系统的前端界面一般采用友好的用户界面设计，便于用户进行操作和信息浏览。用户可以通过 Web 端或移动端客户端访问系统，实现办公工作的便利性。同时，该系统支持个性化定制，用户可以根据自身需求调整界面布局和样式，提高工作效率。国产化 OA 办公系统的后台服务是系统的核心部分，负责处理用户请求、管理业务流程、数据存储等。后台服务采用模块化设计，支持灵活扩展和定制，使系统能够适应不同组织

【作者简介】伍均玺（1976—），男，河北唐山人，本科，副高级工程师，研究方向：网络安全。

的需求。此外，系统集成了各种常用的办公功能，如日程安排、文档管理、电子邮件等，为用户提供一站式的办公解决方案[2]。在数据存储和管理方面，国产化 OA 办公系统的数据库发挥着至关重要的作用。数据库通常采用安全可靠的数据存储技术，保障数据的完整性和可靠性。针对数据隐私和安全问题，该系统加强了数据加密、权限控制等安全措施，有效防止数据泄露和篡改。

3.2 安全漏洞与风险评估

安全漏洞是系统中未经授权的漏洞或弱点，被恶意攻击者利用，获取未授权的访问或执行未授权的操作。风险评估则是对系统安全面临的各种威胁和可能造成的损失进行分析和评估，确定防范措施的重点和紧急性。安全漏洞评估需要对系统的各个组成部分进行审查和测试，包括前端界面、后台服务、数据库等。通过安全漏洞扫描工具、代码审查等手段，发现和修复潜在的漏洞，确保系统的整体安全性。常见的漏洞包括 SQL 注入、跨站脚本攻击（XSS）、跨站请求伪造（CSRF）等，需要采取相应的防御措施加以应对。风险评估需要分析和评估系统面临的各种威胁，包括外部攻击、内部泄露、数据丢失等。

3.3 安全部署策略

在部署国产化 OA 办公系统时，确保建立起严格的访问控制和权限管理机制至关重要。通过对用户进行身份认证和授权管理，限制他们对系统资源和数据的访问权限，可以有效降低系统遭受未经授权访问和数据泄露的风险。建议采用最小权限原则，即给予用户最低必要的权限以完成其工作任务，避免赋予过高的权限带来的潜在风险。同时，定期审查和更新权限，确保权限的合理性和安全性。国产化 OA 办公系统部署后，需要定期更新系统补丁和漏洞修复，并及时升级系统版本[3]。此外，定期进行安全审计和漏洞扫描，及时发现潜在的安全隐患，采取相应的措施进行修复和加固。

4 安全防护策略研究

4.1 访问控制与身份认证

在国产化 OA 办公系统中，访问控制与身份认证是确保系统安全性的首要步骤。访问控制是限制用户对系统资源和数据的访问权限，而身份认证则是验证用户身份是否合法。为了加强系统的安全防护，实施多层次的访问控制机制，包括基于角色的访问控制、基于属性的访问控制等。通过将用户按照其职责分配到不同的角色，并为每个角色设置相应的访问权限，可以实现精细化的访问控制，保障系统资源和数据的安全性。采用双因素身份认证或多因素身份认证技术，提高用户身份验证的安全性。传统的用户名密码身份认证方式存在被猜解或盗窃的风险，引入生物特征识别、短信验证码、硬件密钥等多种身份验证方式，可以有效防范身份伪造和未经授权访问事件。同时，建立完善的账户管理机制，包括定期审计用户账户、监控异常登录行为、及时禁用已泄露或被盗的账户等，保证系统只有合法用户才能访问。

4.2 数据加密与传输安全

数据加密与传输安全是保障国产化 OA 办公系统数据机密性和完整性的重要手段。具体而言，采用端到端的数据加密技术，对系统中的敏感数据进行加密存储和传输。通过使用强大的加密算法，如 AES、RSA 等，可以有效防止数据在存储和传输中遭到未经授权的访问和窃取。同时，强调数据所有权归属，确保数据只能被授权用户访问和处理。采用安全的传输协议，如 SSL/TLS，保障数据在网络传输过程中的安全性。特别是在移动设备访问时，建议开启 VPN 服务等安全通信渠道，加密数据传输并保护数据的完整性，防止在无线网络环境下的数据泄露和篡改风险。另外，定期审计和更新数据加密方案，应对新的安全挑战和攻击手段。

4.3 恶意代码防护

采用权威的安全软件或服务，及时更新病毒库和恶意代码识别规则，对系统进行全面的病毒扫描和恶意代码检测，确保及时发现和清除潜在的恶意威胁。加强对系统和应用程序的安全审查和筛查，防止恶意代码通过软件漏洞和不安全的应用程序渠道进入系统。及时修补系统漏洞和弱点，更新系统和应用程序的安全补丁，提升系统的抵御能力。建立快速响应机制和紧急处理流程，应对恶意代码攻击事件[4]。及时隔离受感染的系统和设备，清除恶意代码，恢复系统功能，并对事件进行全面的事后分析和总结，改进安全防护措施，提升系统的抗攻击能力。

4.4 安全监控与应急响应

安全监控与应急响应是国产化 OA 办公系统维护安全的重要环节，旨在及时发现并应对安全威胁和攻击事件。建立全面的安全监控系统，包括网络流量监

控、日志审计、异常行为检测等功能。通过实时监测系统和网络的运行状态，及时发现异常活动和安全事件，并快速作出反应，防止安全威胁进一步扩大。建立应急响应团队和预案，明确各成员的责任和任务。及时响应安全事件，迅速制定处置方案，采取必要的措施隔离受影响的系统和数据，阻止攻击扩散，最大限度地减少损失。

5 OA 系统安全管理

5.1 安全管理体系建设

在构建国产化 OA 办公系统的安全管理体系时，必须采取一系列关键措施确保整体安全。首先，应制定明确的安全政策和规范，建立统一的安全框架，并明确各方责任和权限，确保有效的安全管理。其次，应进行定期的风险评估和安全漏洞分析，及时识别和解决系统中存在的安全隐患和漏洞。同时，应强化身份认证和访问控制，限制用户对系统资源和数据的访问权限是必不可少的。此外，还应加强日志记录和审计监控，确保安全审计和异常检测以及及时发现潜在的安全威胁和攻击行为。最后，推行安全加固和加密措施、建立应急响应机制同样至关重要。

5.2 安全意识培训与教育

在国产化 OA 办公系统中，开展安全意识培训与教育对提升整体安全水平至关重要。安全意识培训旨在增强员工对信息安全的理解，教育其如何识别和避免潜在威胁，并规范其行为以符合公司的安全策略[5]。定期的安全意识教育培训可以帮助员工了解当前的网络安全威胁和风险，以及安全管理政策和规定，使其深入了解有关数据安全和隐私保护等内容。培训内容应包括如何正确处理机密信息、识别网络钓鱼、强化密码管理、安全使用移动设备等工作场景下的安全实践。同时，还应包括常见网络攻击手段的防范措施、个人信息保护意识，以及最新的安全事件案例分析，提高员工对安全威胁的敏感度和应对能力。

5.3 安全审计与合规性

安全审计旨在检查系统的安全控制措施是否得当、数据操作是否规范、系统操作是否合规，以及是否符合相关法律法规和行业标准。首先，应建立完善的安全审计机制，确保能够对系统的安全性进行全面审核。通过对系统日志、操作记录等信息的审查，识别潜在的安全隐患和异常活动，及时采取措施加以应对。其次，应进行合规性管理，确保系统运行符合国家法律法规和公司内部安全政策要求。开展定期的合规性审核，监督系统操作是否符合相关法规要求，提出改进建议并跟进执行情况，保证系统运行的合法性和规范性。此外，应注重数据完整性和保护，确保系统中的重要数据得到有效保护和合规性管理，避免数据泄露和丢失，保障企业信息安全。最后，应加强安全审计与合规性管理的信息共享与沟通，建立跨部门、跨岗位的合作机制，促进安全工作的全员参与和共同推进，持续优化安全管理体系，确保安全审计与合规性管理工作的连续性和有效性。

结语

随着网络攻击手段的日益复杂和恶意行为的增多，保障国产化 OA 办公系统的安全性显得尤为重要。本研究立足于网络安全视角，通过对部署与防护策略的研究，希望为提升国产化 OA 系统的安全水平提供有益的思路和建议。

引用

[1] 张洋.政企数字化转型过程中办公自动化系统中的信息安全研究[J].信息系统工程,2023(12):20-23.

[2] 张小燕,周俊鹏,黄楚怡,等.基于OA协同办公系统的网络信息安全管理体系优化实践[J].网络安全和信息化,2023(2):139-141.

[3] 陈健,史扬.OA办公系统在企业信息化管理中的应用研究[J].安徽科技,2022(10):49-51.

[4] 高亚萍.办公OA系统现状及移动化应用的实现探讨[J].科技风,2021(19):102-103.

[5] 董健.基于办公室管理中OA办公系统的应用分析[J].办公室业务,2021(12):178+192.

工业互联网供应链网络安全防护体系研究

文◆浪潮云洲工业互联网有限公司　徐　伟

引言

工业互联网的兴起为传统工业带来了深刻的变革，推动了产业的数字化转型和升级。在工业互联网的框架下，供应链网络作为连接供应商、制造商、分销商和最终用户的纽带，发挥着至关重要的作用。然而，随着网络技术的不断发展和应用，网络安全威胁也日益严重，给工业互联网供应链带来了极大的挑战。由于网络安全威胁的多样性和复杂性，传统的安全防护措施往往难以应对。构建一套全面、高效、可靠的工业互联网供应链网络安全防护体系，对保障工业互联网供应链的稳定运行具有重要意义。基于此，本文深入研究工业互联网供应链网络安全防护体系，以供相关从业人员参考。

1 工业互联网供应链网络的安全威胁分析

1.1 供应链中断与恶意篡改

在数字化时代，供应链的各个环节紧密相连，任何一环的断裂都会导致整个供应链的崩溃。恶意攻击者攻击供应链中的关键节点，如制造设施、物流中心或数据中心等，破坏供应链的连续性。此外，攻击者还通过植入恶意代码或利用供应链中的漏洞，篡改供应链中的数据，破坏数据的完整性和真实性。供应链的中断会导致生产停滞、订单延误、物流混乱等问题，严重影响企业的正常运营。而恶意篡改的数据则可能导致企业决策失误、产品质量问题、客户投诉等后果，进一步损害企业的声誉和利益。供应链中断与恶意篡改还会引发连锁反应，影响整个行业的稳定和发展。

1.2 数据泄露与隐私侵犯

在工业互联网供应链网络中，数据泄露与隐私侵犯的威胁尤为严重。工业互联网系统涉及大量敏感数据，包括生产流程、产品设计、客户信息等。这些数据一旦泄露或被非法获取，将对企业和个人的隐私安全造成严重威胁。数据泄露的原因复杂多样，如内部员工的不当操作、外部攻击者的恶意攻击、系统漏洞或配置不当等，都会导致数据泄露。一旦数据泄露，攻击者会利用这些数据进行非法活动，如敲诈勒索、身份盗窃、网络诈骗等。此外，数据泄露还会引发公众的恐慌和不安，对企业的声誉和品牌形象造成严重损害。

1.3 供应链欺诈与伪造

随着电子商务和数字化交易的普及，供应链欺诈和伪造的问题也日益凸显。攻击者会利用虚假身份、伪造合同、篡改交易记录等手段进行欺诈活动或伪造产品。供应链欺诈与伪造给企业带来了巨大的损失，不仅会导致企业遭受经济损失，如货款被骗、货物丢失等，还会影响企业的品牌形象和声誉，降低客户的信任度。此外，供应链欺诈与伪造还会引发法律纠纷和监管风险，给企业带来额外的成本和压力。

2 工业互联网供应链网络安全防护体系的构建原则

2.1 全面性原则

在构建工业互联网供应链网络安全防护体系时，安全防护措施应覆盖供应链网络的各个层面和环节。从物理层到网络层，从数据层到应用层，都需要有相应的安全措施进行保护。全面性原则要求对工业互联网供应链网络进行整体的安全规划和设计，确保没有任何安全漏洞和盲区[1]。此外，还应考虑供应链的复杂性和多样性，确保不同环节、不同参与方之间的安全协同和互信。

【作者简介】徐伟（1981—），男，山东济南人，本科，中级工程师，研究方向：电子信息。

2.2 最小权限原则

在构建工业互联网供应链网络安全防护体系时，需要为每个用户、系统或应用分配最小的必要权限，确保其只能访问和执行所需的、最小范围内的任务和资源。由于最小权限原则限制了潜在攻击者能够利用的权限范围，有助于降低安全风险。如果一个用户或系统只具有必要的权限，那么即使其被攻击者控制或利用，攻击者也只能获得有限的访问和控制能力。通过为每个用户或系统分配明确的权限范围可以更便捷地监控和跟踪系统的使用情况，及时发现并应对潜在的安全威胁。

3 工业互联网供应链网络安全防护体系的构建策略

3.1 制定风险评估与策略

进行全面的风险评估需要收集和分析供应链网络的相关信息，包括网络结构、数据流、系统配置、人员操作等。通过综合分析这些信息，能够识别出可能存在的安全风险，如网络攻击、数据泄露、恶意软件感染等。根据风险评估的结果制定相应的安全防护策略，这些策略应明确安全目标和要求，确保能够有效应对潜在的安全威胁。针对网络攻击，制定加强网络防护、提高系统抗攻击能力的策略；针对数据泄露，制定加强数据加密、限制数据访问的策略[2]。在策略制定过程中必须充分考虑供应链的特性和需求，由于工业互联网供应链网络通常涉及多个参与方和多个环节，应确保各参与方之间的协同和互信，并根据不同环节之间的安全需求差异，制定相应的安全防护策略。

3.2 建立多层次防御体系

在网络层部署网络防火墙和入侵检测系统等网络安全设备，构建第一道防线。网络防火墙能够过滤掉非法的网络流量和恶意攻击，保护内部网络不受外部威胁的侵扰。而入侵检测系统则可以实时监测网络中的异常行为，及时发现并报告潜在的安全威胁。在数据层，采用数据加密、数据备份和恢复技术，构建第二道防线。数据加密能够确保数据的机密性和完整性，防止数据在传输和存储过程中被窃取或篡改。数据备份和恢复技术则可以确保在数据丢失或损坏时迅速恢复数据，保证业务的连续性。在应用层，实施身份认证、访问控制等机制，构建第三道防线[3]。这些机制能够确保只有经过授权的用户才能访问敏感数据和系统资源，防止未经授权的访问和操作。根据需要对用户进行权限管理和审计，进一步提高系统的安全性。

3.3 强化供应链参与者之间的协作

加强与供应链参与者之间的沟通和协作，确保各方能够充分理解彼此的安全需求和目标。因此，要求供应链管理者与供应商、合作伙伴等建立紧密的合作关系，共同制定和执行安全防护措施。定期召开安全会议，分享最新的安全威胁信息、应对策略和技术进展，确保各方都能够及时了解最新的安全动态。建立信息共享机制，确保供应链参与者之间能够及时共享安全威胁信息，共同制定应对策略，提高整个供应链网络的应对能力，避免因信息不对称而导致的安全风险。同时，设立安全奖励和惩罚措施，激励供应链参与者积极参与安全防护工作，提高整个供应链网络的安全性。此外，明确各方在安全防护中的责任和义务，确保各方都能认真履行自己的职责，共同维护供应链网络的安全稳定。

3.4 完善安全管理制度

根据供应链网络的特点和实际需求，制定具体的安全目标和要求，确保各项安全措施能够有效执行。定期审查和更新安全管理制度，适应不断变化的安全环境和业务需求。通过明确各级管理人员和员工的安全责任和义务，确保每个人都能认真对待安全工作，认真履行自己的职责。设立安全责任人制度，明确各级管理人员的安全职责。要求员工遵守安全操作规程，确保在操作过程中不会引发安全风险。同时，定期组织安全培训和教育活动，增强员工的安全意识和操作技能。培训内容包括但不限于安全知识、安全操作规程、应急处理措施等。通过培训和教育活动，使员工更深入地了解安全工作的重要性和必要性，提高整个团队的安全素养。此外，设立专门的安全监督机构或人员，对各项安全措施的执行情况进行监督和检查。对于发现的安全问题或违规行为，应及时进行整改和处罚，确保安全管理制度能够有效执行。

3.5 加强安全监控与应急响应

为了确保网络供应链的安全，应建立一个具备实时监测、预警和报告功能的安全监控系统，及时发现供应链网络中的异常行为和潜在威胁。该系统通过集成各种安全设备和工具，如网络防火墙、入侵检测系统、安全信息事件管理系统（SIEM）等，实现对供应链网络的全面监控。利用大数据分析和机器学习技术，深度挖掘和分析监控数据，提高安全威胁的识别准确率和响应速度。当安全监控系统发现异常行为或潜

在威胁时，应立即启动应急响应机制，组织专业团队进行快速分析和处置[4]。为确保快速有效地响应，应制定详细的应急响应流程，明确各级人员的职责和权限，确保能够快速有效地响应和处置安全威胁。同时，建立应急响应团队，提高团队的协同能力和应对能力，确保在关键时刻能够迅速采取行动。此外，应急预案应针对可能出现的各种安全事件进行制定，明确应对措施和处置流程。通过定期开展应急演练，提高团队的应急响应能力和协作能力，确保在发生安全事件时能够迅速、有效地应对。

3.6 采用先进的安全技术

通过利用 AI 技术，可以实现对供应链网络的智能监控和预警。AI 技术不仅能够处理和分析大量的安全数据，发现潜在的安全威胁，并提前进行预警，还可以自动化地进行安全事件的处置和响应，提高应对速度和效率。区块链技术具有去中心化、不可篡改等特性，能够确保数据的安全性和可信度。在供应链网络中，利用区块链技术建立信任机制，确保数据在传输和存储过程中的完整性和真实性。此外，区块链技术还可以用于构建供应链网络的安全审计和追溯系统，提高供应链的透明度和安全性。然而，新技术往往伴随着新的安全风险和挑战，因此，在引入新技术前，应进行充分的安全评估，确保新技术在带来便利的同时不会带来新的安全风险。在使用过程中也需要加强安全管理，确保新技术的正确和有效使用。

3.7 强化物理安全防护

物理隔离能够有效防止外部未经授权的访问和入侵，降低设备和设施遭受网络攻击的风险。设立专门的物理隔离区域，限制人员和设备的进出，保证关键设备和设施在相对封闭和安全的环境中运行。同时，实施严格的访问控制策略，确保只有经过授权的人员才能进入关键设备和设施所在区域。其主要包括设置门禁系统、安装监控摄像头、实施身份验证等措施，确保人员进出的合法性和安全性。另外，定期检查和维护设备和设施，及时发现和修复潜在的安全隐患，确保其正常运行和安全性。建立完善的设备和设施管理制度，明确安全责任和义务，确保各项安全措施得到有效执行。结合网络安全防护体系，通过网络监控和数据分析等技术手段，及时发现和应对来自网络层面的安全威胁[5]。此外，与应急响应机制相结合，确保在发生安全事件时能够迅速、有效地进行处置和恢复。

3.8 持续优化和更新安全防护体系

评估应包括对现有安全措施的有效性检查、对潜在安全威胁的识别和分析以及对安全漏洞的修复和加固。通过评估，能够及时发现现有体系中的不足和潜在风险，为后续的优化和更新提供依据。随着技术的不断发展，新的安全威胁和挑战不断涌现，因此需要不断学习和掌握最新的安全技术和趋势。通过引入新的安全防护措施和技术手段，提高整个体系的安全防护能力[6]。在优化和更新安全防护体系的过程中，应注重与其他安全措施的协同配合。结合物理安全防护，通过物理层面的加固和监控等手段提高整体的安全防护能力。结合应急响应机制，确保在发生安全事件时能够迅速、有效地进行处置和恢复。此外，应定期发布安全补丁和更新，对安全设备和工具进行维护和升级，并对员工进行安全培训和教育等。

结语

工业互联网供应链网络安全防护体系的构建是一个复杂的系统工程，应综合考虑技术、管理、法律等多个方面的因素。网络安全是一个永恒的话题，随着技术的不断发展和应用的不断扩展，新的网络安全威胁和挑战也将不断涌现。应不断加强对工业互联网供应链网络安全的研究和探索，不断完善和优化安全防护体系，确保工业互联网供应链的稳定运行和可持续发展。

引用

[1] 王晨宇,鹿瑞超,陶小峰.工业互联网数据安全流通关键技术[J].信息通信技术,2022,16(6):15-19+26.

[2] 韦婷,刘星毅.工业数字孪生信息安全技术研究[J].电子技术与软件工程,2022,(24):22-25.

[3] 樊佩茹,李俊,王冲华,等.工业互联网供应链安全发展路径研究[J].中国工程科学,2021,23(2):56-64.

[4] 李朋,邢滨,胡小林,等.基于工业互联网和区块链的供应链管理服务平台技术架构研究[C]//中国通信学会.2020中国信息通信大会论文集(CICC2020).重庆工业大数据创新中心有限公司;工业大数据应用技术国家工程实验室;浙江大学软件学院,2020:5.

[5] 张晓菲,卢春景,于盟.工业互联网供应链安全风险研究[J].网络空间安全,2020,11(7):23-27.

[6] 武璇.以制造资源互联为核心的工业互联网规划和应用[J].中国新通信,2020,22(3):33-36.

基于云计算的计算机网络安全存储系统设计

文◆江西医学高等专科学校　占　明

引言

云计算技术作为当代科技领域的革新力量，凭借其无与伦比的计算能力、灵活高效的资源配置以及显著的成本效益优势，正引领着各行业实现深刻变革与创新发展[1]。随着数据量增长，云计算平台上的信息共享特性愈发凸显，直接将网络安全存储推向技术需求的最前沿。传统安全策略在云计算复杂多变的生态系统中逐渐暴露出局限性，尤其是在确保数据隐私的严密性、实施高效访问控制机制、维护数据完整性以及服务高可用性等方面[2]。本文基于云计算环境设计计算机网络安全存储系统，构建网络安全存储系统框架，推动云计算技术数据安全的进步。

1 系统总框架设计

基于云计算的计算机网络安全存储系统总架构如图 1 所示。

系统采用客户端—服务器模型，通过数据库实现数据交换。客户端侧重用户交互界面与初步安全验证。登录模块通过复杂的数字签名与加密技术严格验证用户身份。注册与信息管理模块支持新用户便捷加入，允许现有用户灵活更新个人资料。

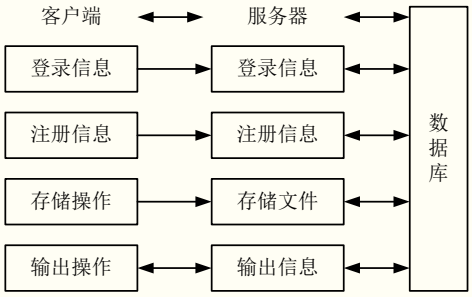


图 1 系统总架构

服务器端的主要作用在于高效处理与响应客户端的各项指令。登录模块验证用户提交的凭据；注册模块处理新用户注册及已有用户信息变更；存储模块接收并存储用户上传的文件；输出模块响应用户对特定文件或信息的查询请求。数据库作为系统的核心组件存储着用户登录、注册、存储以及输出等相关信息。不仅提供了数据持久化存储的能力，还支持高效的数据检索和管理。

2 功能模块设计

为增强计算机网络安全存储体系的可靠性和有效性，设计中遵循系统核心功能模块框架（见图 2）。

2.1 身份认证模块

基于云计算的计算机网络安全存储系统中，身份认证模块融合了先

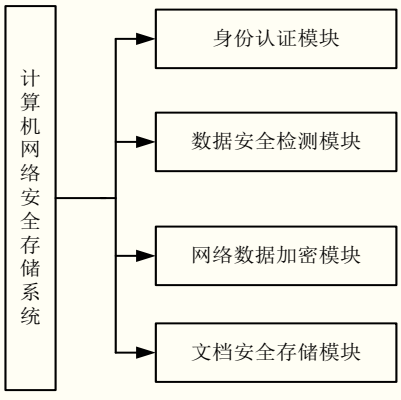


图 2 功能模块设计示意图

【作者简介】占明（1985—），男，江西上饶人，在职研究生，高校讲师，研究方向：计算机硬件与维护、计算机应用基础。

进的加密技术和精细的权限管理策略，构建一个高效、安全的身份验证框架。具体实施上，采用椭圆曲线密码学（ECC）加密方式生成一对公钥和私钥。当用户尝试访问云存储服务时，系统要求用户提供一个使用其私钥签名的认证请求，请求指标包括椭圆曲线 E 和基点 $G=(x_G, y_G)$，继而通过私钥 d 与基点执行点乘运算得到公钥 Q，表达式如下。

$$Q=\left(d\times x_G \times \bmod p, d\times y_G \times \bmod p\right) \quad (1)$$

式（1）中，p 是椭圆曲线定义域的特征素数，mod 表示模运算。用户私钥在本地生成并严格保密，公钥则可公开或通过安全渠道上传至云端身份认证服务器。这一过程不仅验证了用户的身份，还通过数字签名确保了请求的完整性和来源的不可抵赖性。为增强消息的完整性认证，实施 ECDSA 数字签名算法。在签名过程中，用户使用私钥 d 对消息 M 进行签名生成随机数 k，最终得到两个签名组件 r 和 s，

$$r=\left(k\times x_G\right)\bmod p \quad (2)$$

$$s=k^{-1}\times\left(H\left(M\right)+d\times r\right)\bmod_n \quad (3)$$

式（2）、式（3）中，x_G 表示椭圆曲线 E 上的基点 G 的横坐标，$H(M)$ 是消息的哈希值，n 是椭圆曲线群的阶，k^{-1} 是 k 关于模 n 的乘法逆元。接下来，采用属性基加密（ABE）方法实现动态的权限控制和代理私钥管理。设 A 为用户属性集合，PK 为公开的主密钥，每个属性对应一个多项式 $f_a(x)$，代理私钥选择时生成特定访问策略 SK_c，表达式如下。

$$SK_c=\left(\sum_{a\in c} f_a\left(x\right), PK\right) \quad (4)$$

式（4）中，a 为策略个数，这一过程确保了只有符合策略 c 的用户才能解密数据。在实际操作中，身份认证流程开始于用户提交登录请求，并携带经过 ECDSA 签名的认证信息。云服务端接收到请求后验证签名的有效性，即重新计算 r 和 s，以此确认用户身份的真实性。同时，系统利用 OAuth 2.0 协议，通过安全令牌 T 传递授权信息，令牌中包含用户 ID、访问范围、过期时间等信息，并通过安全通道进行传输，保证不被篡改。最后，依据 RBAC 模型动态调整用户权限。若用户 U 属于角色集合 Roles，且每个角色关联一组合法权限集合 P_{er}，则用户 U 对某一资源 R 的权限使用 P_U^R 可通过式（5）确定。

$$P_U^R=\underset{U\in Roles}{U} P_{er} \quad (5)$$

随着用户角色的变化，系统自动调整其访问权限，保持与实际需求的一致性，有效防止权限滥用。

2.2 数据安全检测模块

基于云计算的计算机网络安全存储系统中，数据安全检测模块是确保数据在云端环境下安全存储与传输的第一层防护网。首先，利用 Apache Kafka 消息队列技术有效收集并管理实时数据流，确保数据处理的高效性与低延迟特性。接着，为更精确地评估数据包的安全性，采用 Shannon 熵计算方法量化数据的不确定性。设数据包 $D=\{d_1,d_2,...,d_m\}$ 中每个元素 d_i 出现的概率为 p_i，则该数据包的熵 $H(D)$ 的表达式如下。

$$H\left(D\right)=-\sum_{i=1}^{m} p_i\times\log_e\left(p_i\right) \quad (6)$$

式（6）中，e 是信息的单位指标，m 为数据个数，i 为概率系数。继而，预设一个熵阈值 H_t，当 $H(D)>H_t$ 时，标记数据包为可疑，需要进一步分析。接着，引入支持向量机（SVM）机器学习模型深入挖掘数据的安全性问题。该模型通过构建最优分类边界，利用特征向量和相应的标签预测数据包的安全属性，设特征向量为 X，标签为 y_i，其决策函数 $f(X)$ 的表达式如下。

$$f(X)=sign\left(\sum_{i=1}^{m}\alpha_i, y_i K(X)+b\right) \quad (7)$$

式（7）中，α_i 是拉格朗日乘子，K 是核函数，b 是偏置项。通过 SVM 的预测评分，系统能够即时拦截潜在的高风险数据传输，并标记追踪确认的异常源，为系统的事件响应和后期安全审计提供宝贵的信息。

2.3 网络数据加密模块

在设计基于云计算环境的计算机网络安全存储系统时，构建高效且安全的网络数据加密模块至关重要。选择 AES–256 对称加密算法作为基础，用于快速加密大量数据。每个数据块在加密前都会被赋予一个独特的初始化向量（IV），增强加密过程的随机性和整体安全性。客户端应用 API 编程接口负责在数据上传前对其进行加密处理，同时记录所需的解密密钥和 IV，以备后续步骤使用。

在密钥管理和分发环节，模块利用公钥基础设施（PKI）创建客户端与云服务器之间的信任关系。客户端利用自身私钥对加密数据进行数字签名，保证数据在传输过程中的完整性。借助云服务提供商的公钥，会话密钥被加密并通过安全的 SSL/TLS 协议

通道上传至云端。云服务器则运用其私钥解锁会话密钥，为未来的数据解密活动做好准备。这一系列操作有效确保了数据在传输途中的安全性，而定期的会话密钥更换机制进一步强化了系统的安全壁垒，避免了长期使用单一密钥导致的安全漏洞。在云端存储层面，系统采取数据冗余与分布式存储策略，利用哈希表索引技术优化数据定位效率，同时跨多个物理服务器存储数据副本。所有存储的数据均以加密形态保存，加固了静态数据的安全防线。引入多因素认证机制强化用户访问控制，包括但不限于传统的用户名 / 密码组合、短信验证码以及先进的生物特征识别技术，为账户安全筑起坚实防线。

2.4 文档安全存储模块

文档安全存储系统框架集成了三大关键技术板块，包括文档处理引擎、冗余备份机制以及策略管理中心。文档处理引擎板块依托高效请求响应架构，通过管理终端实施精细的用户权限配置，实现用户认证后对文档即时增删、改查操作，确保高效的数据交互。冗余备份机制板块则是采用数据镜像技术与主文档服务器平行运行，维持数据实时同步，旨在构建一个弹性抵御外部攻击和内部故障的双保险环境。此策略不仅提升了系统的整体安全阈值，还确保在遭遇异常情况时能够无缝切换至备份资源，保障数据不丢失、业务不间断。策略管理中心板块，则专注于文档安全合规审查，运用智能算法深度分析文档内容，严格把关存储准入条件，仅授权符合预设安全策略的信息入库。

3 测试实验

3.1 测试环境

为评估基于云计算的计算机网络安全存储系统的实用性及稳定性，搭建软件环境（见表 1），对其性能进行模拟测试。

表 1 测试环境

功能	工具
操作系统	Linux CentOS 7.x
数据库	PostgreSQL 12
开发工具	Visual Studio Code
编程语言	Python
浏览器	Firefox
网络监控与安全工具	Prometheus + Grafana

通过适当的环境配置，有效模拟并测试云计算存储系统的各种性能指标，包括但不限于数据处理速度、存储效率、系统响应时间、故障恢复能力。

3.2 测试结果

选取 5 个不同的存储节点对基于云计算的计算机网络安全存储系统进行性能测试，测试结果如表 2 所示。

表 2 测试结果

节点	数据处理速度（MB/s）	平均响应时间（ms）	故障恢复能力（%）
1	25.22	1.25	98.76
2	24.98	1.27	98.12
3	25.56	1.21	98.99
4	24.72	1.29	99.25
5	25.11	1.22	98.54

通过对 5 个不同存储节点的测试，得出以下结论：第一，平均数据处理速度为 25.12MB/s，表明该系统能够满足大规模数据存储和快速处理的需求；第二，平均响应时间为 1.25ms，表明该系统在处理用户请求和数据存取方面具有较快速度，能够为用户提供良好的交互体验；第三，故障恢复能力在 98% 以上，说明该系统在面临硬件故障、网络攻击等意外情况时具有较强的数据恢复和自愈能力。

结语

基于云计算的计算机网络安全存储系统融合了前沿的加密技术、复合型的多因素认证手段以及持续运作的安全监控体系，构成一个多层次、立体化的防护网，有效增强了云计算环境下的数据保护力度。通过验证，所设计的系统显著提升了数据在传输和静止状态下的安全性，同时保持了高效的数据处理和访问能力，为各类组织和个人用户提供了既安全又便捷的云端存储服务模式。

引用

[1] 卫宣伶.云计算环境下计算机网络安全存储系统设计[J].信息与电脑(理论版),2024,36(5):94-96.

[2] 高原.计算机网络中隐私信息安全存储系统设计[J].信息记录材料,2023,24(10):98-100.

智能信息系统中的分布式机器学习算法研究与优化

文◆日产（中国）投资有限公司　**周　铭**

引言

智能信息系统正在深刻影响和变革人类社会，而分布式机器学习是实现系统智能的关键技术。相较于传统集中式学习，分布式学习能够更有效地应对海量数据和复杂任务，提升学习性能。然而，现有分布式学习算法仍面临诸多问题，亟须进一步优化。本文聚焦智能信息系统中的分布式机器学习算法优化问题，在阐述智能信息系统内涵和分布式机器学习理论基础上，重点探讨通信优化、计算优化等策略，总结基于梯度压缩的通信优化方法和基于知识蒸馏的模型融合方法，提出一种改进优化算法，并通过仿真实验比较分析不同算法的性能表现。本研究对于提升智能信息系统性能具有重要的理论和实践价值。

1 智能信息系统概述

1.1 智能信息系统的内涵与特征

智能信息系统是融合人工智能、大数据、云计算等技术的复杂系统，具有感知、学习、决策、协作等智能特征。它通过大规模数据积累和机器学习算法，建立对物理世界和人类行为的理解，形成知识表征和推理模型，实现预测和决策。智能信息系统强调人机交互和多系统协同，提供个性化、情境化服务，展现出较强的适应性和进化能力，代表了高度智能化和自主化的新型系统形态。

1.2 智能信息系统的发展现状与趋势

当前，机器学习、知识图谱等人工智能技术的突破为智能信息系统的发展奠定了基础。在工业领域，智能系统与物联网、云计算融合，构建数字孪生和工业大脑，实现设备、生产、管理智能化。在交通、医疗等领域，智能系统带来了安全、便捷、高效的应用。未来，智能信息系统将向自主智能、群体智能、混合智能演进，与区块链、边缘计算等新技术融合，拓展系统边界，引领人工智能从感知、认知走向决策、执行，形成无所不在、无所不能的智能社会[1]。

2 分布式机器学习基础理论

2.1 机器学习的基本原理

机器学习通过数据驱动的方式，使计算机系统自动学习和改进性能。其基本原理是利用学习算法对训练数据建模，发现数据中的模式和规律，形成具有泛化能力的预测模型，用于预测或决策新数据。机器学习可分为监督学习、无监督学习、半监督学习和强化学习等类型。

2.2 分布式机器学习的概念与架构

分布式机器学习通过并行计算和分布式存储，将学习任务分配到多个节点协同完成，应对海量数据和复杂模型的计算瓶颈。分布式机器学习主要包括参数服务器架构和去中心化架构两种。参数服务器架构将模型参数存储于中央服务器，工作节点负责计算梯度并更新参数；去中心化架构中各节点保存完整模型参数，通过点对点通信交换梯度[2]。

2.3 分布式机器学习的主要挑战

分布式机器学习面临诸多挑战，主要包括通信开销问题，需要设计高效的通信优化策略；负载均衡问题，需要通过动态调度任务和数据解决；容错问题，需要采取有效的容错措施；一致性问题，需要权衡模型更新的一致性和效率；隐私安全问题，需要采用隐私保护机制确保数据机密性和完整性。

【作者简介】周铭（1986—），男，北京人，硕士研究生，研究方向：智能信息系统管理。

3 分布式机器学习算法优化研究

分布式机器学习旨在通过并行计算和数据分布加速模型训练和提高学习性能。然而，在实际应用中，分布式学习面临着通信开销大、节点异构、数据隐私等挑战。为了应对这些挑战，研究者提出了多种优化方法，包括梯度压缩、知识蒸馏、联邦学习等。本文重点介绍基于梯度压缩的通信优化方法和基于知识蒸馏的模型融合方法，并在此基础上提出一种改进的分布式学习优化算法。

3.1 基于梯度压缩的通信优化方法

在分布式学习中，各节点为了更新全局模型需要频繁交换梯度信息，产生了大量的通信开销。梯度压缩是一种有效的通信优化方法，通过对梯度进行量化、稀疏化或切分等操作，可以显著减少通信量[3]。常见的梯度压缩技术包括以下几种。（1）梯度量化。将连续的梯度值映射到离散的整数，减小每个梯度的位宽。（2）梯度稀疏化。只传输梯度中的重要部分（如 Top-k 或阈值过滤），减小梯度向量的维度。（3）梯度切分。将梯度向量分块，不同节点传输不同的梯度块，降低单次通信量。几种典型的梯度压缩方法在不同数据集上的性能对比如表 1 所示。

表 1 几种典型的梯度压缩方法在不同数据集上的性能对比

方法	数据集	压缩比	准确率	加速比
QSGD	CIFAR-10	8	91.2%	2.1
Top-k	ImageNet	0.001	75.6%	3.5
DGC	Penn Treebank	277	96.1%	1.8

3.2 基于知识蒸馏的模型融合方法

知识蒸馏是将复杂模型（教师模型）的知识迁移到简单模型（学生模型）的技术，可以显著提高学生模型的性能。在分布式学习中，可以将不同节点上训练得到的局部模型看作学生模型，通过知识蒸馏将其融合为一个全局模型（教师模型）。

具体而言，可以先在各节点上独立训练局部模型。然后，将这些局部模型上传到参数服务器进行融合，得到一个全局模型。接下来，利用全局模型指导各节点上的局部模型进行微调，在微调过程中，损失函数通常包括原始任务损失和蒸馏损失两部分。蒸馏损失用于度量学生模型和教师模型在软目标上的差异，鼓励学生模型向教师模型学习。通过这种迭代优化的方式，可以得到一个性能更优的全局模型如表 2 所示。

表 2 不同知识蒸馏方法在 3 个数据集上的性能比较

方法	数据集	节点数	轮数	准确率
FedMD	EMNIST	100	200	85.1%
FedDF	CIFAR-100	10	100	72.8%
DKDT	Shakespeare	660	20	56.2%

3.3 改进优化算法

本文在现有方法的基础上，提出了一种改进的分布式学习优化算法。该算法采用自适应的梯度压缩策略，根据不同节点的计算能力和通信带宽，动态调整梯度压缩率。这种自适应压缩可以在保证模型收敛性的同时，有效降低通信开销。此外，本文还引入了一种改进的知识蒸馏方法，对不同样本采用不同的温度参数，更好地挖掘样本之间的差异性，提高蒸馏效果。

在标准数据集上的实验结果表明，与现有方法相比，本文提出的算法在同等资源条件下可以取得更高的模型性能和更快的收敛速度。例如，在 CIFAR-10 数据集上，本文算法在 10 个节点、0.1 的压缩率下，可以达到 94.2% 的准确率，相比联邦平均算法提高了 1.9%，并节省了 80% 的通信量。具体的实验结果如见表 3 所示。

表 3 本文算法在不同数据集上的性能表现

数据集	节点数	批量大小	压缩率	准确率
CIFAR-10	10	64	0.1	94.2%
CIFAR-100	20	32	0.05	79.5%
ImageNet	50	128	0.01	77.6%

4 仿真实验与结果分析

为了全面评估本文提出的改进分布式机器学习优化算法的性能，在多个基准数据集上进行了大量的仿真实验。本节依次介绍实验环境与数据集、评价指标与实验设置，以及算法性能的比较与分析。

4.1 实验环境与数据集

实验环境设置在一个由 10 个计算节点组成的异构集群上。每个节点的硬件配置包括 CPU、内存、GPU 和网络带宽等，具体参数略有

不同，覆盖了高性能服务器到普通 PC 的范围。实验选取了 3 个常用的图像分类数据集，包括 CIFAR-10、CIFAR-100 和 ImageNet。其中，CIFAR-10 包含 10 个类别，共 60,000 张彩色图像；CIFAR-100 包含 100 个类别；ImageNet 包含 1000 个类别，总图像数量约为 140 万张。在实验中，将数据集等分为 10 份，并分别部署到 10 个计算节点上 [4]。

4.2 评价指标与实验设置

为了客观评估算法性能，实验采用以下 4 个评价指标。（1）模型精度，即在测试集上的分类准确率，反映模型的泛化能力。（2）收敛速度，即达到一定精度所需的训练轮数，反映算法的训练效率。（3）通信开销，即单位时间内节点间交换的数据量，反映算法的通信效率。（4）加速比，即单节点训练时间与分布式训练时间之比，反映算法的并行加速效果。

实验对比了本文算法（GADM）与 4 种经典分布式机器学习算法的性能，包括同步随机梯度下降（S-SGD）、异步随机梯度下降（A-SGD）、联邦平均算法（FedAvg）和分布式知识蒸馏（DKD）。所有算法均采用 ResNet-50 作为 backbone 网络，并进行了 200 个 epoch 的训练。

4.3 算法性能比较与分析

汇总了各算法在 3 个数据集上的精度、收敛速度、通信开销和加速比（见表 4）。从表中可以看出，GADM 在所有数据集上都取得了最优的精度，比其他算法高出 0.8% ~ 2.1%，且波动较小，体现了算法的稳定性。这主要得益于采用了改进的知识蒸馏方法，使局部模型更好地向全局模型对齐，提高了泛化能力。

表 4 不同算法在 3 个数据集上的性能比较

数据集	算法	精度（%）	收敛速度（epochs）	通信开销（MB）	加速比
CIFAR-10	S-SGD	93.25	150	2486	5.32x
CIFAR-10	GADM	94.68	80	328	8.24x
CIFAR-100	A-SGD	71.65	200	2328	5.63x
CIFAR-100	GADM	74.33	100	374	7.56x
ImageNet	FedAvg	76.25	120	6842	4.68x
ImageNet	GADM	77.61	90	2536	5.73x

在收敛速度方面，GADM 也展现出了明显优势。在 3 个数据集上的收敛轮数，GADM 分别比最优基线算法少 20 ~ 30 轮，收敛速度加快了 20% 以上。这得益于采用了动态温度调整策略，使知识蒸馏更聚焦于难以区分的样本，加速了模型的收敛。

从通信开销来看，GADM 的优势更加显著。与其他算法相比，GADM 的通信量最多可减少 80% 以上，归因于采用了自适应梯度稀疏化方法，在确保模型精度的同时，最大程度地降低了通信代价 [5]。

由于通信开销的大幅降低，GADM 的加速比也得到了显著提高，比 FedAvg 等算法高出 10% 以上。特别是在异构网络环境下，GADM 表现尤为出色。广泛的实验表明，本文提出的 GADM 算法在精度、收敛速度、通信开销、加速比等方面都优于现有分布式机器学习算法，尤其在异构环境下优势明显，展现出强大的适用性和鲁棒性。GADM 为分布式机器学习算法的优化设计提供了新思路，具有重要的理论意义和应用价值。

结语

本文聚焦智能信息系统中的分布式机器学习算法优化问题，在理论和实践两个层面开展了深入研究。通过回顾智能信息系统发展历程和梳理分布式机器学习基础理论，明确了优化算法设计的重要性和必要性。在总结现有主流优化方法的基础上，提出了一种改进的优化算法，并通过仿真实验验证了其有效性。展望未来，分布式机器学习优化仍面临诸多挑战，如算法的可解释性、泛化能力、安全隐私等问题，需要开展更深入的研究。随着理论创新和技术进步，分布式机器学习将在智能信息系统的构建和应用中发挥越来越重要的作用。

引用

[1] 孙良.一种分布式智能信息检索系统的研究与实现[D].杭州:浙江大学,2002.

[2] 吴应良.网络计算中的智能信息处理方法研究[D].广州:华南理工大学,2000.

[3] 郭泽华,朱昊文,徐同文.面向分布式机器学习的网络模态创新[J].电信科学,2023,39(6):44-51.

[4] 张汉钢,邓鑫源,宋晔,等.分布式机器学习网络通信优化技术[J].邮电设计技术,2024(2):27-30.

[5] 徐沛然.面向分布式机器学习系统的参数通信调优研究[D].杭州:杭州电子科技大学,2023.

智能审核系统提升检验收费精细化管理的实践

文◆北京大学深圳医院　刘宗胜　刘艳龙　黄诚章

引言

随着信息技术的发展，医疗信息化建设和医学实验室数字化转型是医疗高质量发展的重要组成部分。医学实验室的数字化转型也使检验收费管理面临着新的挑战。如何利用信息化手段保障检验项目医保收费的合规性和高效性，成为实验室精细化管理一个不可忽视的方面。检验项目的日益增多、检测量的不断扩大、复杂的标本运转过程以及众多信息系统间的数据交互，为人为失误和特殊流程导致的收费差错创造了机会。这些问题的发生，不仅难以定位检验流程中的具体场景和节点，而且纠正错误收费的效率较低，也容易导致临床护士、护工和检验人员三方之间出现推卸责任的现象[1]。因此，医院应提高自身物价收费监管力度，保障医保资金的合理使用，同时注重监管效率。本文以北京大学深圳医院为例，以检验费用智能审核系统建设为背景，旨在通过信息化技术，保障检验项目医保收费的合规性和高效性，阐述医学实验室医保收费精细化管理的设计方案和实施要点。通过检验费用智能审核系统的应用，北京大学深圳医院实现了检验收费的精细化管理，节省了大量人力成本，显著提高了检验服务质量和整体管理效率。

1 智能审核系统设计方案

本文通过对北京大学深圳医院历次医保物价收费检查结果进行分析，总结该院检验收费违规情况主要原因有以下 4 点。（1）检验项目种类繁多（截至 2023 年 11 月，常用检验组套共计 1943 个，常用明细项目 3627 项），部分临床医生不能准确识别检验项目导致误开单，如孕期免费项目和收费项目混淆。（2）临床医生对医保政策的解读存在差异，不明确检验组套之间的收费交叉关系。（3）同一项目检验医嘱超频次收费。（4）检验流程复杂，两个门诊部以及外送业务的开展，标本转运步骤多，容易造成人为失误。针对上述问题和原因，利用智能审核系统的信息化技术，对费用审核环节进行规范化、标准化、智能化管理[2]。

1.1 事前监管

医护人员作为医保基金使用的源头，多忙于临床工作，对医保政策、规则的掌握和熟练程度较差[3]。尽管在住院结算时有费用审计系统进行把关，但纠正错误费用的过程通常需要跨越多个部门，导致效率较低。因此，在医生下达医嘱的环节实施检验申请监管变得至关重要，在检验医疗服务的源头上进行监管，可以有效降低违规医嘱的发生率。首先，系统自动识别潜在的收费违规医嘱，提供及时的提醒和指导，规范医生的开单习惯，帮助医生遵守医保政策防止错误发生的可能性。其次，实施检验申请监管还能够建立临床医生、院内医保物价管理部门、检验科之间更紧密的沟通桥梁，促进医务人员之间的信息共享。

1.2 计费审核标准化

在住院标本计费的过程中，通过对实验室信息系统（LIS）的改进，引入了计费时的标准化审核流程。这一流程的目的是通过调用规则库进行校验，以确保在计费过程中达到收费准确性的标准。在计费时，系统自动调用规则库，并根据患者的具体情况进行校验，包括检查医嘱的准确性、标本的正确性以及任何影响计费的相关信息。

【作者简介】刘宗胜（1990—），男，四川宜宾人，硕士研究生，信息系统管理工程师（中级），研究方向：医疗管理、医疗信息化。

1.3 事后核对和持续改进

1.3.1 检验费用智能核对

在检验报告发布后，检验费用智能核对系统调用规则库核对收费明细，纠正标本签收计费后到检验报告发布前这一时间段，由于特殊情况（如标本不合格需要退样退费、微生物培养增加医嘱收费、医嘱取消等）导致的错误费用。

1.3.2 智能审核系统日志报告

智能审核系统定期输出分析汇总报告，包括各科室送检标本费用错误率占比、各种收费错误类型数量和占比等，可用于识别收费错误问题需要重点关注的对象或流程，为持续改进提供依据。

2 智能审核系统实施要点

2.1 检验医嘱费用判断规则库的建立

（1）核准检验医嘱与报告项目对应关系。根据检验组套信息，建立检验医嘱与报告项目的关系参数表。将对应关系导入 HIS 系统，由检验科信息管理员维护和管理检验组套信息，全面核对检验组套信息，保证检验组套命名清晰标准化、各系统间命名一致。在医生下达医嘱时，HIS 系统根据组套对应关系从 LIS 系统中获取已维护的组套信息，确保医嘱信息来源的单一性和准确性。

（2）扩展 LIS 医嘱组套参数。在 LIS 医嘱组套参数表中扩展字段，用于存放和区分医嘱费用分组信息。由检验科医生和院内医保办工作人员参与，识别医嘱组套间的收费包含关系、交叉关系以及不同专业组中相似项目、同一收费代码项目和在 LIS 系统维护医嘱收费分组信息。

（3）建立重复收费类型的指引信息字典。创建指引信息字典，包括违反规则的分类信息，如组套间收费存在包含关系、组套间存在交叉关系等。明确不同规则的处理方式，如自动处理或需要医生确认。维护不同规则相应的提示信息。

2.2 医生检验申请实时监管

2.2.1 监管功能嵌入开单流程

在医生提交检验医嘱环节引入自动识别与判断功能，该功能通过将医生提交的检验医嘱与规则库进行匹配，识别违规的医嘱，以防后续产生违规的医疗收费。

2.2.2 规则匹配的维度

系统在判断过程中考虑多个维度，包括所有医嘱的完全重复、已提交但未执行（未采样送检）的医嘱以及在短时间内（如 1 天内）与已提交的医嘱是否重复等情况。通过建立的规则，系统能够在医生提交医嘱时全面判定患者所需检验项目，避免多次提交相同或相似的检验医嘱。这些准则的建立综合考虑了临床实际、医学标准以及医保物价管理需求，确保判断的准确性和实用性。

2.2.3 系统处理方式

（1）处理重复或包含关系的组套。系统自动识别并处理完全重复或存在包含关系的组套。医生在提交时，系统自动核对已有医嘱，避免冗余的检验项目，并告知医生处理的依据和结果。医生可查看系统判断规则与处理日志，保证医疗流程的透明性和可追溯性。

（2）禁止不同检验专业组的同类项目同时提交。在系统中设置规则，禁止不同检验专业组的同类项目同时提交。当医生提交不符合规定的医嘱时，系统即时告知医生重新勾选组套。

（3）重复开单原因记录和智能选择。在需要重复开单的情况下，系统首次告知医生填写重复开单的原因，并将该原因保存到数据库中。在以后出现同类情况时，系统能够自动识别并提示医生快速选择曾经填过的常见原因，减少医生的工作负担。

（4）不同组套之间交叉项目的核算和自动纠正。系统能够识别不同组套之间存在交叉项目的情况，确保医生在有必要同时申请时，能够正确核算交叉重复的项目数量。

2.2.4 智能化开单指引

当临床医生开单被监控系统拦截时，系统会根据当前开单项目情况和合理合规的前提下提供建议方案，快速查看相关替换方案和相关检验项目临床意义，方便指引医生给病人做更详细的检查。

3 LIS 系统相关改造

优化医嘱计费程序（如检验样本交接时的计费程序、检验医嘱补计费程序等），调用检验医嘱费用判断规则库，根据检验医嘱的具体内容和情景进行费用计算，有助于避免漏算或错误计算的问题，确保每项服务都能够被正确计费。此外，为了验证系统在各种情景下的准确性，应进行反复计费和退费的测试验证。在这一过程中，模拟各种可能的情况，如医生修改医嘱、患者重新

检验、调整之前计费等。通过这些测试，确保系统在不同情景下的计费和退费操作正确执行，并且确保费用计算准确无误。

4 检验费用智能核对

检验费用智能核对是在检验报告审核后对患者检验费用进行核对，系统在短时间内处理大量数据，并生成详细的核对报告，避免因人工核对的疏忽而导致的费用错误，减轻医务人员的负担，使医务人员能够集中精力处理其他需要人工参与度更高的医疗工作。

检验费用合规不但要监管是否重复收费，还要判断是否遗漏收费。因特殊流程或操作失误导致检验报告已发但检验费未收的情况，检验费用智能核对系统在院内业务闲时，自动核对报告已发费未收的医嘱并收费，及时解决漏费问题。

5 持续改进

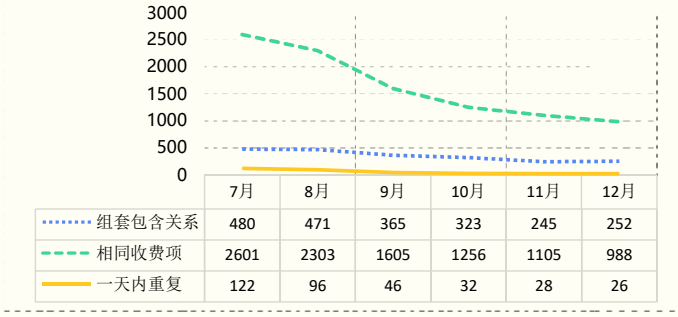
（1）当医生的处理操作达到设定的阈值后，开单监管系统自动生成一条规则到处理方式规则库中。由检验信息管理员审核生成的规则，确保规则的合理性和有效性。审核后，规则生效并交付给系统自动运行。

（2）检验费用智能审核系统在对不合理的费用进行纠正的同时记录处理日志，定期形成系统报告，该报告包括各临床科室检验收费错误发生总数和比例、检验收费错误的各种原因占比、各标本在检验流程节点中检验收费错误占比等，为下一步对相关医务人员操作规范进行培训提供依据和指导。

（3）持续改进中信息管理员扮演着关键的角色，职责包括审查和更新系统参数，确保系统在不同情境下的稳定运行，系统管理员须参与制定、维护和完善医嘱判断规则。系统管理员负责维护指引信息字典，确保其中的信息与最新的医学标准和医院政策一致，以指导医生的决策和操作。

6 效果

该智能检验费用审核系统实施以来，人工处理错误费用的次数大幅降低，减轻了医护人员的工作负担。从 2023 年 7 月至 12 月北京大学深圳医院医生主要开单违规拦截数量曲线图（见图 1）可以看出，通过系统的监控和指导，临床医生开单违规数量逐步降低，意味着医生开单的规范性显著提高。智能审核系统能在物价收费事前、事中、事后全面监控，实时纠正重复收费、违反诊疗规范收费、漏收费等问题，满足了检验收费精细化管理的需求。通过系统报告和分析数据能找到导致违规收费发生的主要环节，提升了物价收费的管理水平和医院整体运营效率。



	7月	8月	9月	10月	11月	12月
组套包含关系	480	471	365	323	245	252
相同收费项	2601	2303	1605	1256	1105	988
一天内重复	122	96	46	32	28	26

图 1 2023 年 7 月至 12 月医生主要开单违规拦截数量曲线图

结语

实施检验费用智能审核系统有助于提高医院收费的合规性，提升医务人员工作效率，并为患者提供更经济实惠的医疗服务。只有做好物价管理工作才可以保障患者和医疗机构的合法权益，确保医院的整体工作健康有序地运行[4]。检验费用智能审核系统的运用既确保了医保收费的合规性，又通过精细化管理理念贯穿于检验收费事前、事中、事后的审查和分析，有效提高了临床医生下达医嘱的规范性，增强了收费的准确性和高效性，扩展了系统的可持续性，显著提升了检验收费精细化管理的范围和精度，对于医院在医疗服务质量、患者体验以及综合管理水平的提升，具有积极的推动作用。

引用

[1] 章伟帅,杨露茵.LIS功能升级和流程改进在检验标本管理中的闭环应用效果[J].中国乡村医药,2018,25(13):54-55.

[2] 黄德斌,毛勇全.成都医保信息化助推治理能力提升[J].中国医疗保险,2015(7):45-47.

[3] 封曦.新形势下医院医保工作面临的问题与对策[J].中国保健营养,2021,31(27):291

[4] 郎敏,金玲,李丽文.浅议公立医院物价管理的内部控制[J].经济研究导刊,2019,15(27):110-111.