科技进步奖公示

# 项目名称

基于智能感知的电网全域网络安全技术研究及应用

# 提名单位

云南电网有限责任公司

# 提名等级

三等奖

# 主要知识产权目录

| **序号** | **知识产权（标准）类别** | **知识产权（标准）具体名称** | **国家**  **（地区）** | **授权号（标准编号）** | **授权（标准发布）日期** | **证书编号（标准批准发布部门）** | **权利人（标准起草单位）** | **发明人（标准起草人）** | **发明专利（标准）有效状态** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 发明专利 | 一种数据安全运行在线监测系统 | 中国 | ZL202210281677.1 | 2023.09.12 | 第6321076号 | 云南电网有限责任公司信息中心 | 谢林江；杭菲璐；郭威；张振红；罗震宇；陈何雄；毛正雄；李寒箬；梅东晖；何映军 | 有效 |
| 2 | 发明专利 | 一种网络安全的预测分析方法及系统 | 中国 | ZL202210924828.0 | 2024.03.22 | 第6811966号 | 云南电网有限责任公司信息中心 | 谢林江；吕垚；向华伟；杭菲璐；张振红；李寒箬；廖莹璐；颜颖；刘玉婷；胡健 | 有效 |
| 3 | 发明专利 | 一种网络攻击行为的识别方法及识别系统 | 中国 | ZL202210365374.8 | 2024.04.19 | 第6922337号 | 云南电网有限责任公司信息中心 | 谢林江；杭菲璐；郭威；张振红；罗震宇；陈何雄；毛正雄；李寒箬；何映军 | 有效 |
| 4 | 发明专利 | 一种基于openresty的数控引流方法、系统 | 中国 | ZL202111358372.8 | 2024.07.30 | 第7239291号 | 云南电网有限责任公司信息中心 | 杭菲璐；谢林江；时燕；郭威；李寒箬；张振红 | 有效 |
| 5 | 软件著作权 | 信息安全运维监测指标看板系统 | 中国 | 2022SR0050537 | 2022.01.10 | 软著登字第9004736号 | 云南电网有限责任公司信息中心 | / | 有效 |
| 6 | 软件著作权 | 基于威胁情报的互联网用户画像识别系统 | 中国 | 2022SR0051682 | 2022.01.10 | 软著登字第9005881号 | 云南电网有限责任公司信息中心 | / | 有效 |
| 7 | 软件著作权 | 基于openresty的数据引流系统 | 中国 | 2022SR0056047 | 2022.01.10 | 软著登字第9010246号 | 云南电网有限责任公司信息中心 | / | 有效 |
| 8 | 软件著作权 | 安全事件自动化编排调度系统 | 中国 | 2022SR0062282 | 2022.01.11 | 软著登字第9016481号 | 云南电网有限责任公司信息中心 | / | 有效 |
| 9 | 软件著作权 | 深度安全防御分析系统 | 中国 | 2022SR1119226 | 2022.08.12 | 软著登字第10073425号 | 云南电网有限责任公司信息中心 | / | 有效 |
| 10 | 软件著作权 | 威胁响应链编排平台 | 中国 | 2022SR1135928 | 2022.08.15 | 软著登字第10090127号 | 云南电网有限责任公司信息中心 | / | 有效 |

# 主要论文、专著发表情况

| **序号** | **论文、专著名称** | **刊名、出版社** | **通信作者/第一责任人、第一作者** | **刊期、刊号** | **页码** |
| --- | --- | --- | --- | --- | --- |
| 1 | Performance Evaluation of Data-Centric Networks Based on Parallel and Distributed Architectures for Machine Intelligence Research | Parallel Processing Letters  World Scientific Publishing Company | 谢林江 | Vol. 33, No. 03, 2340006 (2023)  ISSN (print): 0129-6264  ISSN (online): 1793-642X | 2340006 -(1-21) |
| 2 | Data-centric Networking with Parallel and Distributed Architecture Performs Performance Analysis to Protect Critical Infrastructure in the Future Power System Network Based on IoT | Parallel Processing Letters  World Scientific Publishing Company | 谢林江 | Vol. 33, No. 03, 2340005 (2023)  ISSN (print): 0129-6264  ISSN (online): 1793-642X | 2340005- (1-21) |
| 3 | Research on the Application of Network Security Defence in Database Security Services Based on Deep Learning Integrated with Big Data Analytics | International Journal of Intelligent Networks  KeAi Communication Co., | 杭菲璐 | Volume 5, 2024  ISSN: 2666-6030 | 101-109 |
| 4 | Construction of Power System Network Security Defense Behavior Decision-Making Model Based on Artificial Intelligence Technology | Scalable Computing: Practice and Experience  West University of Timisoara | 杭菲璐 | Vol. 25 No. 4 (2024)  ISSN: 1895-1767 | 2614-2620 |
| 5 | Research and Design of an Automated Security Event Analysis and Handing Framework Based on Threat Intelligence | Scalable Computing: Practice and Experience  West University of Timisoara | 廖周缘、谢林江 | Vol. 25 No. 3 (2024)  ISSN: 1895-1767 | 1872-1881 |
| 6 | 新型电力系统智能化深度安全防御体系构建 | 《科技创新与应用》  黑龙江省创联出版有限公司 | 谢林江 | 第13卷第6期2023年2月（下）  ISSN: 2095-2945 | 128-131 |
| 7 | 自动化技术在终端管理中的应用 | 《电子技术》  《电子技术》杂志编辑部 | 张振红 | 第52卷第6期2023-06  ISSN: 1000-0755 | 150-151 |
| 8 | 计算机主机风险的自动化控制技术分析 | 《集成电路应用》  《集成电路应用》编辑部 | 廖周缘 | 第40卷第5期2023-05  ISSN: 1674-2583 | 138-139 |

# 主要完成单位情况

| **序号** | **单位名称** | **联系人** | **联系电话** | **法定代表人** | **通讯地址** | **统一社会信用代码** | **排名** | **对本项目科技创新和应用推广情况的贡献** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 云南电网有限责任公司 | 黄山珂 | 15508770526 | 甘霖 | 云南省昆明市拓东路73号 | 915300007134058253 | 1 | 本单位为项目统筹和总体负责单位。负责项目立项、总体研究方向、目标、技术路线、知识产权申报、论文编制等方面的指导和把关，帮助总结形成自动化数据聚合监测及智能化风险预测方法、安全事件智能防御及联动处置和反制对抗方法、告警自动化多维分析研判和智能化态势感知决策方法、人机协同运营和智能化联动治理方法等成果。负责项目进度、技术监督及质量管理，负责项目组织协调、总结、检测和验收，统一协调提供研究成果部署所需南网云节点、算力、存储等资源，统筹研究成果在省地两级示范应用和监督管控，并在云南电网范围内各级单位进行推广应用。 |
| 2 | 云南电网有限责任公司信息中心 | 杭菲璐 | 13608885700 | 朱兴柯 | 云南省昆明市西山区海宏路云南电网有限责任公司滇池路基地信息中心 | 915300007902753582 | 2 | 本单位为项目主导、技术路线及总体架构设计、理论研究、关键技术研究、数据分析验证、成果部署实施的主要完成单位，并负责成果示范应用和推广。  本单位围绕监测预警、分析研判、处置对抗、运营管控开展研究，创新自动化数据聚合监测及智能化风险预测、告警自动化多维分析研判和智能化态势感知决策、安全事件智能防御及联动处置和反制对抗、人机协同运营和智能化联动治理等关键技术。  本单位部署了省级平台，推动成果在各级单位开展示范应用。通过示范应用，统一处理和分析全省网络安全数据，并接入本单位终端1403台、安全系统113套，开展溯源反制600余次、全省指令联动226次，实现了“智能防御、省地联动”防御目标，形成人机协同作战的防御新模式，有效提升中心网络安全保障能力、协同效率和深层次威胁防御水平，降低了安全防御投入和运营人力成本，取得了良好的应用效果。 |
| 3 | 西南林业大学 | 代飞 | 13908715148 | 王卫斌 | 云南省昆明市盘龙区白龙寺300号 | 125300004312044009 | 3 | 本单位为项目设计、理论指导和技术指导的主要完成单位。  本单位聚焦于能源行业数字化转型中的全域网络安全防御技术，针对电网海量安全数据监测难、告警分析难、事件处置效率低、协同运营治理能力不足等痛点，指导项目组围绕监测预警、分析研判、处置对抗、运营管控等方面开展相关研究，帮助形成自动化数据聚合监测及智能化风险预测方法、告警自动化多维分析研判和智能化态势感知决策方法、安全事件智能防御及联动处置和反制对抗方法、人机协同运营和智能化联动治理方法等成果。 |
| 4 | 云南电网有限责任公司昆明供电局 | 颜丽渊 | 13808707015 | 叶盛 | 中国（云南）自由贸易试验区昆明片区官渡区太和街道办事处吴井路98号 | 9153000091652092XA | 4 | 本单位为项目实施单位、测试单位和成果示范应用单位。  本单位主要配合完成了项目成果体系的落地实施及测试、试运行工作，并将相关结果反馈至设计单位进一步完善和改进，对自动化数据聚合监测及智能化风险预测方法、告警自动化多维分析研判和智能化态势感知决策方法、安全事件智能防御及联动处置和反制对抗方法、人机协同运营和智能化联动治理方法等成果的形成有测试和实施贡献。  本单位将项目最终成果应用于内部安全运营日常工作中，通过示范应用，接入本单位终端5322台、安全系统43套，配合完成全省指令联动226次，实现了“智能防御、省地联动”防御目标，形成人机协同作战的防御新模式，有效提升本单位网络安全保障能力、协同效率和深层次威胁防御水平，降低了安全防御运营人力成本，取得了良好的应用效果。 |
| 5 | 云南云思科技有限公司 | 刘建顺 | 15288240767 | 周春英 | 云南省昆明市官渡区彩云北路大都摩天2期1301 | 915301110569509106 | 5 | 本单位为项目技术研究、系统研发、数据分析验证和测试的主要完成单位，并负责项目成果运维。  本单位按照总体设计要求，围绕监测预警、分析研判、处置对抗、运营管控开展技术研究，完成了安全数据中台、安全能力中台、安全管控中台、安全运营中台等的研发构建，通过安全数据中台提供大数据集成能力，通过安全能力中台提供自动化编排能力、安全关联分析能力、智能化能力，通过安全管控中台提供设备集中管控和自动调用能力，通过安全运营中台的统一指挥管控及联动治理能力，形成基于人机协同和智能防御的电网全域网络安全技术平台。负责收集分析各示范应用单位测试和试运行结果，根据结果进行系统性能测试和优化，对自动化数据聚合监测及智能化风险预测方法、告警自动化多维分析研判和智能化态势感知决策方法、安全事件智能防御及联动处置和反制对抗方法、人机协同运营和智能化联动治理方法等成果的形成有积极贡献。 |

# 主要完成人情况

| **序号** | **姓名** | **性别** | **技术职称** | **最高学历** | **工作单位** | **联系电话** | **排名** | **对本项目科技创新和应用推广情况的贡献** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 杭菲璐 | 男 | 正高级工程师（正高） | 硕士研究生 | 云南电网有限责任公司信息中心 | 13608885700 | 1 | 项目总负责人，负责把握项目总体方向与研究目标，总体负责技术架构设计、技术路线设计、总体方案制定、组织并主导关键技术攻关，对自动化数据聚合监测及智能化风险预测方法、安全事件智能防御及联动处置和反制对抗方法、告警自动化多维分析研判和智能化态势感知决策方法、人机协同运营和智能化联动治理方法等创新成果有主导和主要研究贡献。 |
| 2 | 谢林江 | 男 | 正高级工程师（正高） | 本科 | 云南电网有限责任公司信息中心 | 13759551905 | 2 | 项目研究负责人，负责技术路线执行、场景策划、关键技术攻关、统计分析改进，对自动化数据聚合监测及智能化风险预测方法、安全事件智能防御及联动处置和反制对抗方法、告警自动化多维分析研判和智能化态势感知决策方法、人机协同运营和智能化联动治理方法等创新成果有主要研究贡献。 |
| 3 | 向华伟 | 男 | 高级工程师（副高） | 本科 | 云南电网有限责任公司信息中心 | 15925150092 | 3 | 项目管理负责人，负责方案评估、进度管控、协调组织、实施应用推进、评价改进，对提出自动化数据聚合监测及智能化风险预测方法、提出安全事件智能防御及联动处置和反制对抗方法、提出告警自动化多维分析研判和智能化态势感知决策方法、提出人机协同运营和智能化联动治理方法等创新成果有方向指导和参与研究贡献。负责协调成果体系在信息中心的部署应用，并统筹推进项目成果在各级单位试点示范应用。 |
| 4 | 吕垚 | 男 | 工程师 | 硕士研究生 | 云南电网有限责任公司 | 13759128957 | 4 | 项目管理人员，负责项目研究方向指导、资源协调、应用推广，对提出自动化数据聚合监测及智能化风险预测方法、提出安全事件智能防御及联动处置和反制对抗方法、提出告警自动化多维分析研判和智能化态势感知决策方法、提出人机协同运营和智能化联动治理方法等创新成果有方向指导和参与研究贡献。负责协调成果体系南网云节点、算力、存储等资源，推动成果覆盖省地两级应用。 |
| 5 | 白彪 | 男 | 高级工程师（副高） | 硕士研究生 | 云南电网有限责任公司信息中心 | 13769919996 | 5 | 项目管理人员，负责项目指导、统筹协调、应用评估、改进方向指导，对提出自动化数据聚合监测及智能化风险预测方法、提出安全事件智能防御及联动处置和反制对抗方法、提出告警自动化多维分析研判和智能化态势感知决策方法、提出人机协同运营和智能化联动治理方法等创新成果有方向指导和参与研究贡献。负责成果推广应用过程和机制运转情况的监督管控。 |
| 6 | 吴玮 | 女 | 高级工程师（副高） | 硕士研究生 | 云南电网有限责任公司信息中心 | 13769179629 | 6 | 项目管理人员，负责项目指导、统筹协调、应用评估、改进方向指导，对提出自动化数据聚合监测及智能化风险预测方法、提出安全事件智能防御及联动处置和反制对抗方法、提出告警自动化多维分析研判和智能化态势感知决策方法、提出人机协同运营和智能化联动治理方法等创新成果有方向指导和参与研究贡献。负责成果推广应用过程和机制运转情况的监督管控。 |
| 7 | 代飞 | 男 | 教授 | 博士研究生 | 西南林业大学 | 13908715148 | 7 | 项目技术负责人，负责项目理论研究指导、技术指导，对提出自动化数据聚合监测及智能化风险预测方法、提出安全事件智能防御及联动处置和反制对抗方法、提出告警自动化多维分析研判和智能化态势感知决策方法、提出人机协同运营和智能化联动治理方法等创新成果有理论方法和技术指导贡献。 |
| 8 | 胡健 | 男 | 工程师 | 硕士研究生 | 云南电网有限责任公司信息中心 | 18787469692 | 8 | 项目研究人员，负责项目研发、实施、统计分析、改进、应用推广，对自动化数据聚合监测及智能化风险预测方法、告警自动化多维分析研判和智能化态势感知决策方法等创新成果有参与研究贡献。负责成果技术体系在应用单位的推广实施及实施效果的跟踪管控。 |
| 9 | 廖周缘 | 男 | 工程师 | 本科 | 云南电网有限责任公司信息中心 | 15925102141 | 9 | 项目研究人员，负责项目研发、测试、实施、改进，对自动化数据聚合监测及智能化风险预测方法、安全事件智能防御及联动处置和反制对抗方法等创新成果有参与研究贡献。负责成果技术体系推广应用实施效果的跟踪管控。 |