高等学校科学研究优秀成果奖（科学技术）科学技术进步奖公示材料

项目名称	工业互联网信息安全关键技术与应用
提名单位	北京科技大学
主要完成人情况	1 陈红松（教授）、2 郝志强（研究员）、3 吕翊（高工）、4 龙国东（高工）、5 黄海峰（工程师）、6 刘刚（高工）、7 黄敏（高工）、 8 王方立（工程师）、9 王昭顺（教授）、10 颉靖（高工）、11 梁雄伟（高工）、12 黄锋（高工）、13 陈雪鸿（高工）、14 张冬艳（副教授）、15 韩延鹏（工程师）、16 宋锐（工程师）、17 冯全宝（工程师）、18 王春霞（副研究员）
主要完成单位	1 北京科技大学、2 国家工业信息安全发展研究中心、3 太极计算机股份有限公司、4 北京威努特技术有限公司
项目简介	工业互联网是新一代信息技术与制造业深度融合的产物，我国大量传统制造企业对网络攻击缺乏必要的感知和防控能力。本项目将深度学习算法、微弱信号检测、工控系统漏洞挖掘技术、工控系统漏洞评估技术与物联网、云计算、大数据、人工智能等新兴信息技术结合，构建新一代工业互联网一体化主动安全防护体系。主要创新点如下： 1.基于深度学习和时频域联合分析的工业无线网络流量异常与攻击检测方法 2.工业控制系统安全漏洞高效挖掘与数据分析方法 3.工业控制系统资产高精度识别及漏洞评估技术与工具 4.支持多源异构泛在接入的边云协同的工业互联网平台技术 该成果获授权发明专利 9 项，软件著作权 7 项，发表论文 11 篇，制定国家标准 4 项，行业标准 2 项，出版专著 3 部。近三年产生直接经济效益超过 2.4 亿元，引领了我国工业互联网信息安全及平台建设。本项目相关核心技术及产品服务于中共十九大、两会、上合峰会、一带一路峰会、中非合作论坛、G20 峰会等国家重大活动的网络安全保障工作，产生了良好的社会效益。

主要知识产权和标准规范等目录（不超过 10 件）

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
论文	Bayesian network based weighted APT attack paths modeling in cloud computing	中国		2019-5-18		北京科技大学	亚伦、陈红松、王昭顺	
论文	A novel Low-rate Denial of Service attack detection approach in ZigBee wireless sensor network by combining	中国		2019-3-5		北京科技大学，铁道警察学院，国家信息中心，哈尔滨	陈红松、孟彩霞、单志广、傅忠传、巴拉特	

	Hilbert-Huang Transformation and Trust Evaluation					工业大学，美国普渡大学		
论文	基于循环神经网络的无线网络入侵检测分类模型构建与优化研究	中国		2019-6-16		北京科技大学	陈红松，陈京九	
发明专利	一种无线传感器网络路由层低速洪泛攻击的检测方法	中国	201610725730.7	2019-02-15	3253290	北京科技大学	陈红松	有效
发明专利	一种云计算环境下数据对象的访问控制方法及系统	中国	201610982386.X	2019-09-10	3521285	北京科技大学	陈红松	有效
发明专利	基于工控协议漏洞挖掘用户自定义方法	中国	201510492939.9	2019-04-19	3342780	北京威努特技术有限公司	曾光、黄敏、赵宇、龙国东	有效
发明专利	基于工控协议模糊测试的数据分层生成方法	中国	201610872299.9	2019-02-15	3255186	广东电网有限责任公司电力科学研究院、北京威努特技术有限公司	梁智强、胡朝辉、林丹生、李书杰、黄曙、伍晓泉、胡海生、王方立	有效
发明专利	一种模糊测试数据流的管理方法	中国	201610872307.X	2019-06-25	3431467	广东电网有限责任公司电力科学研究院、北京威努特技术有限公司	胡朝辉、梁智强、林丹生、李书杰、黄曙、伍晓泉、胡海生、王方立	有效
发明专利	一种工业网络异常中断的检测方法	中国	201610262770.2	2019-03-15	3292541	北京威努特技术有限公司	韩延鹏、黄敏、龙国东	有效
发明专利	生成 rest 服务和 rest 实现的方法及对应的设备	中国	201310288983.9	2017-02-08	2370367	北京慧点科技有限公司	姜晓丹、吕翊、黄海峰、韩国权、杜胜、张晓辉	有效

主要完成人情况表

姓　　名	陈红松	性别	男	排　　名	1	国　　籍	中国
技术职称	教授			最高学历	研究生	最高学位	博士
工作单位	北京科技大学						
完成单位	北京科技大学						
对本项目主要科技创新的贡献： 主要科技创新的贡献对应创新点一，提出面向大规模工业互联网的网络安全异常流量检测体系架构，提出基于深度学习和时频域联合分析的工业无线网络流量异常与攻击检测方法，可实现对大规模工业无线网络流量异常检测与攻击源定位。通过产学研用一体化合作创新模式，为国家工业互联网安全关键技术研发、国家工业信息安全漏洞库建设及人才培养做出积极贡献。科技贡献的支撑材料为论文、授权发明专利。							

姓　　名	郝志强	性别	男	排　　名	2	国　　籍	中国
技术职称	研究员			最高学历	研究生	最高学位	硕士
工作单位	国家工业信息安全发展研究中心						
完成单位	国家工业信息安全发展研究中心						
对本项目主要科技创新的贡献： 主要科技创新的贡献对应创新点三，在工业控制系统信息安全防护能力评估工具的总体方案设计、业务流程设计、各模块具体方案设计等方面给予了关键指导和审核把关；在工业控制系统信息安全防护能力评估工具的开发过程中统筹协调内外多方资源，确保项目能够按时间节点高质量完成；此外，还牵头制定了工业控制系统信息安全防护能力评估工具的具体评估流程。贡献对应创新点三，指导并审核工业控制系统资产高精度识别及漏洞评估技术与工具，支撑材料为著作《工业信息安全发展报告 2017-2018》。							

姓　　名	吕翊	性别	男	排　　名	3	国　　籍	中国
技术职称	高级工程师			最高学历	研究生	最高学位	硕士
工作单位	太极计算机股份有限公司						
完成单位	太极计算机股份有限公司						
对本项目主要科技创新的贡献： 主要科技创新的贡献对应创新点四，提出了支持用户按需使用的制造资源智能优化、管理与控制理论和方法，研发了一批相关集团企业制造资源服务管控工具。同时负责研究成果在工业互联网平台上集成应用，实现了基于集团型用户边云协同模式下的安全可控的工业互联网平台。推动工业互联网平台在企业的广泛应用，成功实践提供了丰富的经验及案例支撑。授权发明专利《生成 rest 服务和 rest 实现的方法及对应的设备》作为支撑材料。							

姓　　名	龙国东	性别	男	排　　名	4	国　　籍	中国
技术职称	高级工程师			最高学历	本科	最高学位	学士
工作单位	北京威努特技术有限公司						
完成单位	北京威努特技术有限公司						
对本项目主要科技创新的贡献： 主要科技创新贡献对应工业控制系统安全漏洞高效挖掘与数据分析方法，提出了可扩展的工控系统漏洞挖掘随机模糊测试软件框架，通过分层方法降低变异测试数据的无效数据量，提升了模糊测试变异数据的生成效率和可用性，主持研发工控漏洞挖掘平台和安全监测审计产品，相关科技创新成果获得 6 项授权发明专利。							

姓　　名	黄海峰	性别	男	排　　名	5	国　　籍	中国
技术职称	工程师			最高学历	本科	最高学位	学士
工作单位	太极计算机股份有限公司						
完成单位	太极计算机股份有限公司						
对本项目主要科技创新的贡献： 主要科技创新的贡献对应创新点四，创新提出了支持用户按需使用的制造资源智能优化、管理与控制理论和方法，研发了一批相关集团企业制造资源服务管控工具。同时负责研究成果的集成，实现了基于集团型用户边云协同模式下的安全可控的工业互联网体系。在项目成果转化及推广阶段，先后推动了电力、油气、化工、煤炭、冶金、交通、水利等多个领域的应用推广，为工业互联网平台在企业的广泛应用提供了丰富的经验及案例支撑。有已授权发明作为支撑材料，《生成 rest 服务和 rest 实现的方法及对应的设备》。							

姓　　名	刘刚	性别	男	排　　名	6	国　　籍	中国
技术职称	高级工程师			最高学历	本科	最高学位	学士
工作单位	太极计算机股份有限公司						
完成单位	太极计算机股份有限公司						
对本项目主要科技创新的贡献： 主要科技创新的贡献对应创新点四，主导工业互联网平台整体架构设计，对平台时序数据库、工业大数据模型及算法库等重点方向进行技术攻关。提出了基于集团型用户边云协同模式下的工业互联网体系，并参与了工信部发布的工业互联网平台白皮书的讨论和编制。在项目成果转化及推广阶段，先后完成了水电、风电、化工等多个领域的应用推广，为工业互联网平台在能源行业的广泛应用提供了丰富的经验及案例支撑。基于项目应用成果，作为第一作者发表论文《基于工业互联网的水电设备安全预警系统设计》，作为共同作者发表论文两篇《抽水蓄能电站信息安全合规性的量化评价方法研究》、《电力企业融合型应用系统建设的研究与实现》。							

姓　　名	黄敏	性别	男	排　　名	7	国　　籍	中国
技术职称	高级工程师			最高学历	研究生	最高学位	硕士
工作单位	北京威努特技术有限公司						
完成单位	北京威努特技术有限公司						

对本项目主要科技创新的贡献： 主要科技创新贡献对应创新点二，在工控安全白名单、漏洞挖掘、监测审计、安全防护技术领域提出新型技术创新，已获得授权发明专利 4 项和外观设计专利 1 项。参编 1 项国家标准《信息安全技术 物联网感知层网关安全技术要求》（GB/T 37024-2018）、2 项地方标准《风力发电工业控制系统安全基本要求》（DB43/T 1347-2017）和《城市轨道交通控制系统信息安全通用要求》（DB43/T 1310-2017）。

姓　　名	王方立	性别	男	排　　名	8	国　　籍	中国
技术职称	工程师			最高学历	本科	最高学位	学士
工作单位	北京威努特技术有限公司						
完成单位	北京威努特技术有限公司						
对本项目主要科技创新的贡献： 主要科技创新贡献对应工业控制系统安全漏洞高效挖掘与数据分析方法，主导国内首款工控漏洞挖掘设备的设计开发工作，设计开发了国内先进的 FUZZ 引擎，创新性的提出了模糊测试的数据分层测试方法，针对协议特性，可以通过分层的方式来实现协议的模糊测试，有效解决了模糊测试的数据空间及状态空间爆炸问题；提出了横向多字段关联纵向状态关联的解决方案，有效解决了 FUZZ 测试无效用例过多的问题；创新性的提出了测试数据流的管理方法，此方法很好的解决了大量数据流创建带来的时间开销问题，保证测试用例发送的时效性。相关科技创新成果获得 3 项授权发明专利。							

姓　　名	王昭顺	性别	男	排　　名	9	国　　籍	中国
技术职称	教授			最高学历	研究生	最高学位	博士
工作单位	北京科技大学						
完成单位	北京科技大学						
对本项目主要科技创新的贡献： 主要科技创新的贡献对应创新点一，提出面向工业互联网的加密勒索软件及异常流量检机制，提出以 Web 为中心的加密注入攻击及检测方法。科技贡献的支撑材料为论文。							

姓　　名	颉靖	性别	男	排　　名	10	国　　籍	中国
技术职称	高工			最高学历	研究生	最高学位	硕士
工作单位	国家工业信息安全发展研究中心						
完成单位	国家工业信息安全发展研究中心						
对本项目主要科技创新的贡献： 主要负责工业控制系统信息安全防护能力评估工具的总体架构设计，以及该评估工具中的工业控制系统资产管理模块、《工业控制系统信息安全防护指南》符合性评估模块、统计分析系统、工业控制系统软硬件风险漏洞库四大模块的技术架构设计。贡献对应创新点三，支撑材料是论文《美国网络攻防技术发展及其推进举措》。							

姓　　名	梁雄伟	性别	男	排　　名	11	国　　籍	中国
技术职称	高级工程师			最高学历	本科	最高学位	学士
工作单位	太极计算机股份有限公司						

完成单位	太极计算机股份有限公司
对本项目主要科技创新的贡献： 主要科技创新的贡献对应创新点四，作为核心角色设计 TECO 工业互联网平台工业大数据、建模和分析系统，集成 hadoop、kafka、flume、spark 等大数据技术和微服务架构、容器等开发运行技术，开发了融时序库、MPP 库、非结构化库为一体的工业大数据库，实现了可视化、交互式的模型构建和运行系统。在成果推广应用中，提出并实现基于任务的特征值计算方法，为基于大数据的模型运算准备预处理数据，显著缩短模型运行时间，并成功运用到电力、水利等企业的监测预警应用中。基于项目实践成果，作为共同作者发表论文一篇《基于工业互联网的水电设备安全预警系统设计》。	

姓　　名	黄锋	性别	男	排　　名	12	国　　籍	中国
技术职称	高工			最高学历	本科	最高学位	学士
工作单位	国家工业信息安全发展研究中心						
完成单位	国家工业信息安全发展研究中心						
对本项目主要科技创新的贡献： 主要负责工业控制系统信息安全防护能力评估工具的总体架构设计，并从工业企业资产录入与管理、工业控制系统软硬件漏洞匹配、符合情况测试、评估报告生成方面，完成了该评估工具的具体业务流程设计。贡献对应创新点三，支撑材料《国防电子热点 2018》。							

姓　　名	陈雪鸿	性别	女	排　　名	13	国　　籍	中国
技术职称	高工			最高学历	研究生	最高学位	硕士
工作单位	国家工业信息安全发展研究中心						
完成单位	国家工业信息安全发展研究中心						
对本项目主要科技创新的贡献： 主要负责工业控制系统资产管理模块的具体设计和功能研发工作。贡献对应创新点三，支撑材料为沦为《国家标准<信息安全技术 工业控制系统安全控制应用指南>导读》。							

姓　　名	张冬艳	性别	女	排　　名	14	国　　籍	中国
技术职称	副教授			最高学历	研究生	最高学位	博士
工作单位	北京科技大学						
完成单位	北京科技大学						
对本项目主要科技创新的贡献： 主要科技创新的贡献对应创新点一，提出面向工业互联网移动设备入侵检测算法，提出移动节点攻击行为分析及检测方法。科技贡献的支撑材料为论文-《Optimization of traditional Snort Intrusion Detection System》、《User Behavior Analyses in Mobile Personal Livecasts》。							

姓　　名	韩延鹏	性别	男	排　　名	15	国　　籍	中国
技术职称	工程师			最高学历	研究生	最高学位	硕士

工作单位	北京威努特技术有限公司
完成单位	北京威努特技术有限公司
对本项目主要科技创新的贡献： 主要科技创新贡献对应工业控制系统安全漏洞高效挖掘与数据分析方法，参与国内首款主机应用白名单软件产品开发，创新性的提出白名单技术替代传统杀毒软件的黑名单技术进行主机防护，该技术更加适用工业场景，有效解决工业主机面对的未知安全威胁问题。相关科技创新成果获得 2 项授权发明专利。	

姓　　名	宋锐	性别	男	排　　名	16	国　　籍	中国
技术职称	工程师			最高学历	本科	最高学位	学士
工作单位	太极计算机股份有限公司						
完成单位	太极计算机股份有限公司						
对本项目主要科技创新的贡献： 主要科技创新的贡献对应创新点四，负责 TECO 工业互联网平台边缘计算端的架构设计与应用实践，对工业互联网平台边缘计算架构在水轮发电机机组状态评价及故障诊断等领域进行技术攻关。作为共同作者发表论文《基于工业互联网的水电设备安全预警系统设计》。							

姓　　名	冯全宝	性别	男	排　　名	17	国　　籍	中国
技术职称	工程师			最高学历	研究生	最高学位	硕士
工作单位	北京威努特技术有限公司						
完成单位	北京威努特技术有限公司						
对本项目主要科技创新的贡献： 主要科技创新贡献对应工业控制系统安全漏洞高效挖掘与数据分析方法，在不改变工控系统的前提下，使用智能学习技术辅助生成 OPC 协议的安全规则，安全规则包含基于 TCP/UDP 协议的 OPC 协议操作。某些场景可使用内置只读规则省略学习过程直接达到防护工业系统的目的。发明一种支持 OPC 协议实现双机热备的方法、装置以及通信终端，解决基于 OPC 协议的工业控制系统部署的防火墙无法实现双机热备的问题。相关科技创新成果获得 1 项授权发明专利。							

姓　　名	王春霞	性别	女	排　　名	18	国　　籍	中国
技术职称	副研究员			最高学历	研究生	最高学位	博士
工作单位	北京威努特技术有限公司						
完成单位	北京威努特技术有限公司						
对本项目主要科技创新的贡献： 主要科技创新贡献对应工业控制系统安全漏洞高效挖掘与数据分析方法，负责国际标准 IEC62443-3-3《工业通信网络 系统安全要求和安全等级》(GB/T 35673-2017)国标转化工作，目前该项标准已发布并实施。IEC62443-3-3 由 ISA99 委员会第四工作组的第 2 任务组与 IEC TC65/WG10 一起合作制定的，本标准规定了与 IEC 62443-1-1 中所描述的 7 个基本要求相关的控制系统详细技术要求，包括定义了控制系统安全能力等级要求，本标准是工业自动化控制领域最重要的基础标准之一，使用者包括资产所有者、系统集成商、产品供应商、服务供应商、合规性管理机构。参编国家标准《信息安全技术 工业控制系统漏洞检测产品技术要求及测试评价方法》（GB/T 37954-2019），该标准已发布并实施。							