陕西省科学技术进步奖提名书

（2022 年度）

一、项目基本情况

奖励类别： 社会公益类　　成果登记号： 9612016Y0320

项目名称	项目名称	基于工业大数据的网络安全态势感知技术研究与应用		
	公布名（专用项目）			
主要完成人		赵首花，杨帆，杨向东，杨帆，高瑞		
主要完成单位		陕西省网络与信息安全测评中心		
是否国家秘密技术项目		否		
项目密级		非密	定密日期	
保密期限(年)			定密机构(盖章)	
学科分类名称	1	系统安全	代码	5207020
	2	信息安全工程	代码	5207045
	3	网络安全	代码	5207025
所属国民经济行业		互联网信息服务		
所属陕西省重点发展领域		信息产业及现代服务业		
任务来源		省级计划		
具体计划、基金的名称和编号： 陕西省2016年两化融合专项资金项目（工业控制系统网络安全工程实验室项目）				
已呈交的科技报告编号：				
授权发明专利（项）		0	授权的其他知识产权（项）	2
项目起止时间		起始： 2016年1月1日	完成： 2018年5月31日	

陕西省科学技术奖励工作办公室制

二、提名单位意见

（适用于单位提名）

提名者	陕西省电子学会		
通讯地址	西安市雁塔区太白南路2号西安电子科技大学	邮政编码	710071
联 系 人	杜娟	联系电话	13619213782
电子邮箱	sxsdzxh@163.com	传　　真	029-81891405

提名意见：

工业控制系统信息安全监测平台基于工业大数据的网络安全态势感知技术设计开发，集全域联网工控感知、在线监测、综合分析、威胁评估、态势呈现和通报预警于一体，通过识别工业互联网工控组件，利用大数据分析引擎等相关组件关联分析各类工业控制系统安全威胁及事件，可视化呈现我省工业控制系统信息安全现状，感知整体安全态势。

该平台自建成以来，协助陕西省工业和信息化厅开展工业互联网安全检查和工业互联网安全监测等相关工作，根据历年安全检查和互联网监测结果，及时通报存在问题和安全隐患。协助主管部门和工业企业完善工业控制系统安全管理、安全监控、风险发现、事件通报、应急响应等工作机制，健全工业控制系统信息安全保障体系。

该技术研究成果荣获2项实用新型专利，荣获2019年度数字陕西建设优秀成果和最佳实践案例，荣获2022年度陕西省电子学会科学技术二等奖，项目参与人利用研究成果参编工信部工业信息安全产业发展联盟(国家工业信息安全发展研究中心)编制的《工业互联网安全白皮书(2020)》，参与制定国家标准2个(《工业控制系统安全防护技术要求和测试评价方法》《工业控制系统信息安全防护能力成熟度模型》)，权威期刊发表技术论文7篇，在成果转化方面取得了良好的成效。

鉴于该项目技术创新和应用成效等情况，同意推荐为2022年度陕西省科学科技进步类三等奖。

提名该项目为陕西省科学技术进步奖三等奖。

声明：本单位遵守《陕西省科学技术奖励办法》及其实施细则的有关规定，承诺遵守评审工作纪律，所提供的提名材料真实有效，且不存在任何违反《中华人民共和国保守国家秘密法》和《科学技术保密规定》等相关法律法规及侵犯他人知识产权的情形。如产生争议，保证积极调查处理。如有材料虚假或违纪行为，愿意承担相应责任并接受相应处理。

法人代表签名：　　单位（盖章）

年　　月　　日　　年　　月　　日

提名项目奖励等级意向（由项目组填写）

一等奖	
二等奖	
三等奖	√

说明：省科学技术进步奖一、二、三等奖项目，实行按等级标准提名、独立评审表决的机制。提名单者应严格依据省科学技术奖的标准条件，说明提名项目的贡献程度及等级建议。“提名一等奖”评审落选项目不再降格参评二等奖，“提名二等奖”的评审落选项目不再降格参评三等奖。项目组与提名单位沟通后，做出提名等级意见；提名项目正式提交后，提名等级建议不得变更。请在相应栏打“√”进行选择，并由第一完成人签字确认。

软科学标准计量科普类项目请勾选“二等奖”或者“三等奖”。

第一完成人签字：

年　　月　　日

三、项目简介

随着“两化”深度融合，工业控制系统越来越多地采用通用协议、通用软硬件，利用互联网等公共网络连接，使得针对工业控制系统的攻击行为大幅增长，面临的信息安全问题日益突出。震网、Duqu、火焰、棱镜门等重大信息安全事件造成世界范围内的巨大影响。就目前形势下，我国大量的工业控制设备、技术、软件仍依赖国外，难以对工业控制系统中的网络攻击进行识别、分析与评价，网络安全态势目前仍处于“看不清、防不住、攻不克”的尴尬窘境。

基于工业大数据的网络安全态势感知技术研究与应用，以工业控制系统、工业控制组件为主要研究对象，以全域联网工控感知、在线监测、综合分析、威胁评估、态势呈现和通报预警为主要研究内容，研发了工业控制系统指纹探测技术，通过指纹解析引擎判断目标工业组件存活状态和基本信息，利用工控应用探测引擎抓取工业组件参数，定位和识别；通过工业控制系统漏洞 POC 探测技术，识别工业控制系统、工业控制组件安全漏洞，设计漏洞验证过程及方法，自动化检测工控应用安全漏洞利用和复现情况；通过工业控制系统测试攻击技术，搭建测试靶场和测试蜜罐，复现内外网渗透测试过程，解决了工业控制系统信息收集、定位与识别、漏洞验证、内外网渗透测试模拟、工具测试与测试环境复现困难等相关问题。

利用工业控制组件搜索引擎技术、工业控制系统指纹探测技术、工业控制系统漏洞 POC 探测技术、工业控制系统测试攻击技术和工业控制系统安全检测技术等创新技术研究，设计并开发了工业控制系统信息安全监测平台（工业组件识别、工业数据采集、大数据分析、在线监测、风险识别、数据可视化）、能源化工业工业控制系统安全测评仿真平台（技术研究、攻防展示、应急演练、仿真测试、协议分析、培训教学）等业务平台，为我省网络安全保障工作提供支撑服务。

应用推广情况：以上关键技术的研究，一是落实国家政策文件，建立健全工业控制系统信息安全通报工作机制，协助主管部门开展信息通报和风险预警工作，提高我省工业控制系统信息安全应急处置水平和防护能力；二是协助主管部门，对辖区内重点领域工业企业进行安全检查，指导区域内的工业企业制定工控安全防护策略与措施，保障工业控制系统安全；三是定期开展工业控制系统网络安全培训工作，提高党政机关、企事业单位公章人员对工业控制系统网络安全的认识，加强攻击入侵手段的了解与学习，培养工控安全专业人才，为工控安全战略部署、规划制定、决策咨询、重大问题提供智力支持和技术支撑。

科研院所、工业企业、第三方服务机构等组织与我中心建立了良好合作关系，根据不同需求，应用工业控制系统信息安全监测平台、能源化工业工业控制系统安全测评仿真平台等业务平台，开展工业控制系统安全防护设备、控制设备、应用软件、数据安全等相关测试研究工作，加强了合作交流，促进了工作开展，为后续我省工业控制系统安全保障体系建设夯实业务基础。

经济收益情况：基于工业大数据的网络安全态势感知技术得到了良好的应用与推广，取得了一定的经济和社会效益。工业控制系统信息安全监测平台、能源化工业工业控制系统安全测评仿真平台等业务平台自建成以来，主要以服务社会公众为主，免费向省内中小企业开放，及时公布监测数据及高危漏洞，协助中小企业进行自查和整改。针对有特殊需求的企业，提供工业控制系统仿真模拟实验、工业控制系统风险评估、工控系统漏洞进行研究测试等方服务，促进我省工业企业健康可持续发展。

四、主要科技创新

1. 主要科技创新

一、工业控制组件搜索引擎

工控组件搜索引擎通过 IP 探查、域名反查来识别部署在互联网上可用的工控组件，识别组件后，通过爬虫技术访问工业控制应用，爬取应用组件信息，与普通搜索引擎区别在于，爬虫抓取的不仅限于应用内容，涵盖被探测应用组件的关键特征（例如 cookies，server，x-powered-by 等）信息，特殊 URL 或文件 MD5 信息，最终通过与指纹库的比对识别应用组件。

通过上述关键技术研究与应用，解决了工业控制组件探测与识别困难等问题，发表技术论文 3 篇（对应附件 1-7、附件 1-9、附件 1-10），授权专利 1 项（ZL202021185781.3，对应附件 1-1）。

二、工业控制系统指纹探测技术

工控系统指纹探测技术主要包括服务器指纹探测和应用指纹探测。服务器指纹探测主要探测应用程序响应头部数据、应用文件类型、应用异常响应、服务端口标识回显等指纹信息，通过指纹解析引擎来判断目标应用的操作系统、WEB 服务器软件、WEB 脚本语言等信息及相应版本型号。应用指纹探测技术基于持续收集应用指纹信息，通过比对自动化识别应用响应基本信息、HTML 页面信息、特殊 URL 信息、系统文件 MD5 哈希值信息等。

通过上述关键技术研究与应用，解决了工业控制系统基本信息收集、定位和识别困难等问题，发表技术论文 2 篇（对应附件 1-4、附件 1-5），授权专利 1 项（ZL202021185781.3，对应附件 1-1）。

三、工业控制系统漏洞 POC 探测技术

工业控制系统漏洞 POC 引擎在识别 URL 后启动工控应用探测引擎，工控应用探测引擎负责抓取 URL 头部信息和网页信息，经特征匹配后识别工控应用具体名称和版本型号，工控应用识别引擎进一步结合工控应用漏洞库，查询该工业应用所有历史漏洞信息，利用应用漏洞验证引擎调用漏洞验证程序，检测被探测工控应用是否真实存在安全漏洞。

通过上述关键技术研究与应用，解决了工业控制系漏洞复现与验证过程信息的收集困难等问题，发表技术论文 3 篇（对应附件 1-5、附件 1-6、附件 1-8），授权专利 1 项（ZL202021185781.3，对应附件 1-1）。

四、工业控制系统测试攻击技术

通过外网渗透式攻击技术实现从工业控制系统进入企业办公网络，通过内网渗透测试技术对工业控制系统中的主机节点、开放的服务端口、控制设

备等进行渗透攻击；通过恶意代码植入渗透测试技术，连接工控主机和控制设备，利用工控主机进行非授权访问和操作，完成移动设备的渗透测试攻击。

通过上述关键技术研究与应用，解决了工业控制系统内外网渗透测试模拟、工具测试与测试环境复现困难等问题，发表技术论文 3 篇（对应附件 1-4、附件 1-8、附件 1-9），授权专利 1 项（ZL202021185755.0，对应附件 1-2）。

五、工业控制系统安全检测技术

通过工业控制系统安全检测技术对嵌入式设备、主机设备、网络节点设备、接口软件等工控相关组件进行安全检测，评估工业设备的网络健壮性，验证协议和标准的一致性。

通过上述关键技术研究与应用，解决工业控制系统关键设备健壮性安全检测等相关问题，发表技术论文 3 篇（附件 1-6、附件 1-7、附件 1-8），授权专利 1 项（ZL202021185755.0，对应附件 1-2）。

2. 科技局限性

经过共同努力，基于工业大数据的网络安全态势感知技术研究与应用项目取得了较好的社会和经济效益。主要研究对象为常见的、市场占有率高的工控产品，针对小众厂商的产品和系统，缺乏有效的技术分析手段，研究范围受到一定限制，转化成果无法实现全面覆盖。目前基于工业大数据的网络安全态势感知技术设计开发的业务平台、芯片和主要零部件依赖国外产品，国产化率低，存在一定安全风险。随着我国工业控制领域技术能力的提升，国产化率将会进一步提高，逐步实现自主可控。

另外，该项目是基于当前的技术和产品建立，但网络安全技术发展很快，安全问题层出不穷，因此为保持系统的可用性，我们需要定期更新相关技术。

五、客观评价

一、“基于工业大数据的网络安全态势感知技术研究与应用”科技查新项目于 2022 年 6 月 13 日委托教育部科技查新工作站开展，完成于 2022 年 6 月 22 日。（科技查新报告编号：202236000L290083）结论：经检索并对相关文献分析对比结果表明：上述国内的相关文献报道分别涉及到该查新项目的部分研究内容，但除该委托项目组发表的文献外，国内均未见与该查新项目查新点相同的文献报道。（附件 6-7）

查新点：基于工业大数据分析和态势感知技术，研究了一个包含指纹探测、漏洞 POC 探测、攻击测试的工业控制系统信息安全监测平台。

检索到国内公开发表的中文文献 178 篇，去掉重复文献后，剩余文献 126 篇；相关文献 66 篇，其中密切相关文献 12 篇。（密切相关文献 1 为该委托人课题组成员发表）

查新结论：该查新委托项目研究基于工业大数据分析和态势感知技术，研究了一个包含指纹探测、漏洞 POC 探测、攻击测试的工业控制系统信息安全监测平台。通过指纹解析引擎判断目标工业组件存活状态和基本信息，利用工控应用探测引擎抓取工业组件参数，定位和识别，利用 POC 漏洞验证引擎调用漏洞验证程序，检测被探测工控应用是否真实存在安全漏洞，通过外网渗透式攻击技术实现从工业控制系统进入企业办公网络，通过内网渗透测试技术对工业控制系统中的主机节点、开放的服务端口、控制设备等进行渗透攻击，解决了工业控制系统信息收集、定位与识别、漏洞验证、内外网渗透测试模拟、工具测试与测试环境复现困难等相关问题。经检索并对相关文献分析对比结果表明：上述国内的相关文献报道分别涉及到该查新项目的部分研究内容，但除该委托项目组发表的文献外，国内均未见与该查新项目查新点相同的文献报道。

二、基于工业大数据的网络安全态势感知技术应用于工业控制系统信息安全监测平台，平台建设完成后，经工业和信息化部电子科学技术情报研究所进行测试，于 2017 年 5 月 28 日出具软件测试报告（ ETIRISTC-BG-1708-V2.0），测试结论：本次测试依照开发需求和用户使用手册分别对监测平台的各部分功能进行了测试。测试结果表明，各项测试用例运行通过，符合项目需求，达到验收标准。（附件 2）

本次测试对 “工业控制系统信息安全监测平台”的功能性进行了全面测试，具体到监测平台的各个部分而言:1、监测平台的前端界面部分采用常用的 Web 架构方式,界面简单直观、易操作，界面的链接、导航、快捷键和登录等各项功能正常。2、监测平台的 “工控设备指纹识别 ”部分可以准确地扫描相应工控设

备的基本信息。3、监测平台的“自定义扫描任务”部分在下发 (指定)任务条件下(例如:设备的端 口扫描、服务名扫描、地理位置扫描、厂商扫描以及地理位置扫描等),能够正确、快速地进行任务扫描。4、监测平台的 “数据的自定义搜索”部分检索功能正常,可以准确、快速地检索出自定义条件下的相关数据 (例如:设备标签信息、厂商信息、地理位置信息等)。5、监测平台的“后台扫描搜索”部分能够对互联网进行扫描,准确获取暴露在全球互联网上相关工控设备的数据信息,就国内而言,已通过该平台扫描发现的工业控制系统及设备多达30万余个。6、监测平台的 “分类统计功能”能够正确地对扫描到的工控设备按照端 口、协议、类型、厂商等类别进行细分与统计 ,同时也可 以按照国家地区进行分类统计 并定位 。7、监测平台的数据库采用 mongodb 非关系型数据库,支持数据分片及分布式存储,可支持磁盘阵列。

综上所述,本次测试依照开发需求和用户使用手册分别对监测平台的各部分功能进行了测试。测试结果表明,各项测试用例运行通过,符合项目需求，达到验收标准。

三、基于工业大数据的网络安全态势感知技术设计开发的“工业控制系统信息安全监测平台”于 2021 年 4 月完成了陕西省科学技术厅的科技成果登记，经批准，同意登记（批准登记号：9612021Y0854）。（附件 4）

四、基于工业大数据的网络安全态势感知技术设计开发的“能源化工业工业控制系统安全测试仿真平台”于 2019 年 11 月获得 2019 数字陕西优秀案例。（附件 6-4）

五、2018 年 4 月，省工信厅组织相关专家组，对《工业控制系统网络安全工程实验室建设项目》进行了验收，并出具验收意见，验收结论：1、项目的验收资料完整，符合验收要求;2、项目建设完成了能源化工仿真平台、工控信息安全监测平台以及支撑网络环境建设等内容，符合项目申报书的建设内容;3、项目通过系统试运行，稳定可靠，达到了建设的预期目标;4、经陕西中陕会计事务所有限责任公司关于陕西省网络与信息安全测评中心工业控制系统网络安全工程实验室项目专项资金专项审计报告，专项资金使用合理。验收组同意该项目通过验收。（附件 2）

六、基于工业大数据的网络安全态势感知技术研究与应用（工业控制系统网络安全态势感知技术与应用）项目荣获 2022 年度陕西省电子学会科学技术二等奖。（附件 6-9）

六、应用情况和效益

1．应用情况

截止目前，测评中心以与相关安全厂商、工业企业、第三方服务机构等 30 余家单位合作，对工业控制系统中的设备安全、网络安全、应用安全、主机安全、数据安全等多项内容进行研究。

1.安全检查。协助陕西省工信厅对西安市、宝鸡市、咸阳市、铜川市、渭南市等全省 11 个地市开展陕西省工业控制系统信息安全检查工作。在 2017-2021 年之间，利用仿真平台、安全监测平台等相关技术手段，每年对全省 11 个地市开展工业控制系统信息安全检查工作，累计检查 401 家重要工业控制系统运营单位，涉及重要工业控制系统 2835 套，涵盖煤化工、石油石化、电力能源、工业制造等多个重要领域，发现安全风险 2531 个，通过安全检查，帮助企业识别安全隐患，降低安全风险，避免重大安全事件的发生，加强了对工业企业工业控制系统信息安全工作的指导，提升了工业互联网创新发展安全保障能力和服务水平。每年根据检查结果，出具工业控制系统安全检查报告，上报主管部门省工信厅。**（佐证材料：附件 5-1、附件 5-2、附件 5-3、附件 5-4）**

2.漏洞通报。为进一步贯彻落实《工业控制系统信息安全行动计划（2018-2020 年）》，陕西省工信厅建立健全工业控制系统信息安全通报工作机制，测评中心协助开展信息通报和风险预警等工作，2017 年 8 月，经省工信厅授权，利用安全监测平台等技术手段扫描全省互联网近 500 万个 IP 地址，识别出符合工业控制系统网络指纹特征的 IP，搜索暴露在全省互联网上的重要工业控制系统基本信息，研究分析在线工业控制系统的安全风险。通过平台对全省水、电、气、热等关键基础设施控制系统及能源、钢铁、石化、有色等关键领域重要工业控制系统及其相关业务系统开展持续性保护性安全监测，及时发现存在的高危网络安全风险，掌握全省工业控制系统网络安全态势。2018 年至 2021 年间，每季度出具漏洞通报信息，累计发布漏洞通报 17 份，发布各类工控设备厂商安全漏洞 355 个，指导各级单位开展相关整改工作。测评中心联合多家工业控制系统安全服务单位及时排查风险，结合基于工业大数据的网络安全态势感知技术研究与应用对相关漏洞进行验证分析，提出相应的安全解决方案，整改安全隐患，提高工业企业安全防护能力。**（佐证材料：附件 5-6、附件 5-7、5-8）**

3.安全培训。定期与相关安全厂商技术人员开展工业控制系统网络安全培训工作，培训内容涉及安全意识、安全操作、安全管理、安全技术、安全测试等，通过培训提高相关人员对工业控制系统网络安全的认识，加强攻击入侵手段的了解与学习，联合培养工控安全专业人才，为工控安全战略部署、规划制定、决策咨询、重大问题提供智力支持和技术支撑，有效提高客户安全防护的意识，促进业务深度合作的意向达成，在技术研发、技能竞赛、标准推广、公共服务等工作中，促进技术交流、加强信息沟通，形成产学研用高效联动的发

展格局。业务平台自应用以来，每年协助省工信厅，定期开展专项培训，培训内容主要包括，安全意识、安全操作、安全管理、安全技术、安全测试等相关内容，累计开展工业控制系统专项安全培训 5 次，累计参训人员 1200 余人，为我省工业控制系统网络安全意识培训、技能培养、实践操作培训等方面做出重要贡献。**（佐证材料：附件 6-5、附件 6-6）**

4.安全研究。业务平台自应用以来，与党政机关、科研院所、工业企业、第三方服务机构等 30 余家单位合作，对工业控制系统中的设备安全、网络安全、应用安全、主机安全、数据安全等多项内容进行研究，对工业控制系统安全防护产品的可用性、有效性进行测试，通过检测技术累计发现协议漏洞 540 条、控制设备漏洞 19 个、开放端口 9 个，相关测试数据在持续发现中。**（佐证材料：附件 2）**

主要应用单位情况表

序号	单位名称	应用的技术	应用的对象及规模	应用起止时间	单位联系人/电话
1	陕西省工业和信息化厅	工控安全技术	工控安全服务	2017 年 8 月至今	/
2	陕西电子工业研究院	工控安全技术	工控安全服务	2017 年 9 月至今	/
3	陕西省信息化工程研究院	工控安全技术	工控安全服务	2017 年 1 月至今	/
4	陕西渭河工模具有限公司	工控安全技术	工控安全服务	2019 年 5 月至今	/
5	陕西凌云电器集团有限公司	工控安全技术	工控安全服务	2018 年 10 月至今	/
6	陕西中认信安技术服务有限公司	工控安全技术	工控安全服务	2019 年 1 月至今	/
7	西安航天自动化股份有限公司	工控安全技术	工控安全服务	2019 年 9 月至今	/
8	西安创赛福机电科技有限公司	工控安全技术	工控安全服务	2020 年 3 月至今	/
9	西安千诺机电设备有限公司	工控安全技术	工控安全服务	2020 年 3 月至今	/
10	西安正昌电子股份有限公司	工控安全技术	工控安全服务	2019 年 1 月至今	/

2．经济效益和社会效益

一、经济效益

工业控制系统信息安全监测平台（工业组件识别、工业数据采集、大数据分析、在线监测、风险识别、数据可视化）、能源化工业工业控制系统安全测评仿真平台（技术研究、攻防展示、应急演练、仿真测试、协议分析、培训教学）等业务平台为工业控制系统网络安全测试研究工作、工业控制系统风险评估及漏洞通报工作提供了基础支撑。

在工业控制系统风险评估工作中，通过对企业工业控制系统数据采集后的仿真模拟实验，针对普通规模的工业控制系统，开展工业控制系统风险评估服务。在工业控制系统漏洞通报中，对公开发布的工控系统漏洞进行研究测试，同时对未知漏洞进行挖掘并提交相关设备厂商。

相关业务平台的建设，一方面承担国家工业控制系统设备、安全防护产品验证测试等工作，协助评估设备的安全性、可用性，以节省检测成本，缩短对产品的认证周期。另一方面，承担工业企业在解决工业控制系统所存在的安全风险时，无法建立符合生产环境的离线测试环境，帮助企业进行仿真环境测试，以减少企业采取的安全防护措施成本，提升企业工业控制系统的安全防护能力，保障工业控制系统的安全运行，降低因网络安全所带来的生产风险。

基于工业大数据的网络安全态势感知技术得到了良好的应用与推广，取得了一定的经济和社会效益。工业控制系统信息安全监测平台、能源化工业工业控制系统安全测评仿真平台等业务平台自建成以来，主要以服务社会公众为主，免费向省内中小企业开放，及时公布监测数据及高危漏洞，协助中小企业进行自查和整改。针对有特殊需求的企业，提供工业控制系统仿真模拟实验、工业控制系统风险评估、工控系统漏洞进行研究测试等方服务，促进我省工业企业健康可持续发展。

二、社会效益

通过工业控制系统信息安全监测平台、能源化工业工业控制系统安全测评仿真平台等业务平台的监测，发现我省重点行业中工控系统网络安全漏洞，为其加固整改提供建议，提高其整体网络安全防护水平，并与重点企业建立沟通的桥梁，定期下发安全漏洞风险，并提供各种咨询、建议、培训等服务，以表明测评中心具备按照相应认可资质开展工业控制系统网络安全检测和服务的技术能力。

工业控制系统信息安全监测平台、能源化工业工业控制系统安全测评仿真平台等业务平台，是陕西省两化融合建设的一部分，为充分提高资源的社会效益，更好地满足信息的交叉和整合，平台既服务于单位测试研究工作，又服务于两化融合产

业安全，并尽可能实现资源配置的最优化，通过该技术的研究与应用，以推动陕西省两化融合建设的发展，增强测评中心的市场竞争能力，赢得政府部门、社会各界的信任。

与国内相关工业控制系统产品认证机构合作，最大限度地利用基于工业大数据的网络安全态势感知技术研究与应用及相关业务平台现有设备资源，提高了设备利用率，按照合作要求对相关的工业控制系统设备、安全防护产品进行测试，协助完成相关认证工作，加强了双方在产品认证方式方法的交流，提升了技术能力，为建立新的工业控制系统整体安全防护认证体系奠定了基础。

工业企业在生产环境中无法直接对存储安全风险的工业控制系统进行漏洞检测，基于工业控制系统信息安全监测平台、能源化工业工业控制系统安全测评仿真平台等业务平台，模拟搭建仿真测试环境，帮助企业及时发现生产环境中工业控制系统的漏洞，并通过合理的解决方案修复生产环境中的漏洞，提升企业工业控制系统的安全防护能力，保障工业控制系统的网络安全。

七、主要知识产权和标准规范等目录（限10条）

序号	知识产权类别	知识产权具体名称	国家(地区)	授权号	授权日期	证书编号	权利人	发明人
1	实用新型专利	一种工业大数据交换处理用便于放置的主机服务器	中国	ZL202021185781.3	2020年12月22日	12183068	陕西省网络与信息安全测评中心	杨帆；赵杨鲁汪宝玉首花东军；；；；向红春龙；白玉；高瑞；魏玉峰
2	实用新型专利	一种工业大数据服务处理用具有散热功能的主机服务器	中国	ZL202021185755.0	2020年12月22日	12177031	陕西省网络与信息安全测评中心	杨帆；赵杨鲁何宝玉首花东军；；；；向红松龙；白玉；高瑞；张敏
3	其他	工业互联网平台安全白皮书(2020)	中国	2020年工业互联网平台安全白皮书	2020年12月04日	国家工业信息安全发展研究中心；工业信息安全产业发展联盟	陕西省网络与信息安全测评中心	杨帆
4	论文	工业控制系统信息安全风险评估研究与分析	中国	网络空间安全 2017年第08卷第08-09期 第58页	2017年09月01日	网络空间安全	陕西省网络与信息安全测评中心	杨向东；马卓元；赵首花
5	论文	基于工业控制系统信息安全检查方法的研究	中国	工业控制计算机 2018年第31卷第10期 第1页	2018年10月25日	工业控制计算机	陕西省网络与信息安全测评中心	杨帆；高瑞；李俊；魏玉峰；杨瑞超
6	论文	工业控制系统安全检查工作现状分析及对策研究	中国	工业控制计算机 2019年第32卷第10期 第52页	2019年10月25日	工业控制计算机	陕西省网络与信息安全测评中心	杨向东；何果；赵首花；杨帆；李丹
7	论文	工业控制系统的安全现状分析研究	中国	工业控制计算机 2019年第32卷 第11期 第97页	2019年11月25日	工业控制计算机	陕西省网络与信息安全测评中心	赵首花；闫育芸；何果；杨向东
8	论文	基于分布式思想构筑面向化工行业的工业互联网安全堡垒	中国	工业控制计算机 2020年第33卷第4期 第68页	2020年04月25日	工业控制计算机	陕西省网络与信息安全测评中心	杨帆
9	论文	工业互联网发展应用分析探究	中国	工业控制计算机 2020年第33卷第8期 第12页	2020年08月25日	工业控制计算机	陕西省网络与信息安全测评中心	赵首花；闫育芸

10	论文	基于工业互联网平台数据安全评估的设计	中国	工业控制计算机 2021年 第34卷 第5期 第1页	2021年05月25日	工业控制计算机	陕西省网络与信息安全测评中心	杨帆；闫育芸；魏玉峰；杭萧

承诺：上述知识产权无争议且为本项目独有，未曾在往年国家科学技术奖励项目、往年其他省部级（政府）科学技术奖励项目和本年度其他陕西省科学技术奖提名项目中作为支撑材料出现。用于提名陕西省科学技术奖的情况，已征得未列入项目主要完成人和主要完成单位的权利人（专利指发明人）的同意，有关知情证明材料均存档备查。

第一完成人签名：

八、主要完成人情况表

姓　　名	赵首花	性别	女	排　　名	1	国　　籍	中国
出生年月	1982年11月23日			出 生 地	咸阳市	民　　族	汉族
身份证号	610404198211235529			归国人员	否	归国时间	
技术职称	高级工程师			最高学历	研究生	最高学位	硕士
毕业学校	陕西师范大学			毕业时间	2010年07月01日	所学专业	计算机科学与技术
电子邮箱	zhaoshouhua@sntec.org.cn			办公电话	029-88319550	移动电话	13992823960
通讯地址	陕西省西安市雁塔区茶张路1号省信息化中心19层					邮政编码	710065
工作单位	陕西省网络与信息安全测评中心					行政职务	安全服务部部长
二级单位	无					党　　派	群众
完成单位	陕西省网络与信息安全测评中心					所 在 地	陕西
						单位性质	行政机关或其他事业单位
参加本项目的起止时间	自 2016年01月01日　至 2018年05月31日						

对本项目技术创造性贡献：

对工业控制组件搜索引擎、工业控制系统测试攻击技术、工业控制系统安全检测技术做出了创造性贡献。科技创新：工业控制系统安全检测技术、工业控制系统测试攻击技术、分布式存储技术、海量数据清洗技术。成果：实用新型专利“一种工业大数据交换处理用便于放置的主机服务器”，附件1-1；实用新型专利“一种工业大数据服务处理用具有散热功能的主机服务器”，附件1-2；技术论文《工业控制系统的安全现状分析研究》，附件1-7；技术论文《工业互联网发展应用分析探究》，附件1-9；技术论文《工业控制系统信息安全风险评估研究与分析》，附件1-4；技术论文《工业控制系统安全检查工作现状分析及对策研究》，附件1-6。

曾获科技奖励情况：

曾获2012年度陕西省科学技术奖，项目名称：陕西省政府网站绩效评估研究及应用，奖励等级：叁等，证书编号：2012-3-112-R3；

曾获2018年度陕西省电子学会科学技术奖，项目名称：陕西省互联网网站云防御及追踪平台，奖励等级：贰等，证书编号：SD-2018-2-3-R2；

声明：本人同意完成人排名，遵守《陕西省科学技术奖励方法》及其实施细则的有关规定，承诺遵守评审工作纪律，保证所提供的有关材料真实有效，且不存在任何违反《中华人民共和国保守陕西省密法》和《科学技术保密规定》等相关法律法规及侵犯他人知识产权的情形。如产生争议，保证积极配合调查处理。如有材料虚假或违纪行为，愿意承担相应责任并接受相应处理。承诺该项目是本人本年度提名的唯一项目。

本人签名：

年　　月　　日

完成单位声明：本单位确认该完成人情况表内容真实有效，且不存在任何违反《中华人民共和国保守国家密法》和《科学技术保密规定》等相关法律法规及侵犯他人知识产权的情形。如产生争议，愿意积极配合调查处理工作。

工作单位声明：本单位对该完成人被提名无异议。

单位（盖章）

年　　月　　日

姓　　名	杨帆	性别	男	排　　名	2	国　　籍	中国
出生年月	1976年04月27日			出 生 地	宝鸡市	民　　族	汉族
身份证号	610302197604270015			归国人员	否	归国时间	
技术职称	正高级工程师			最高学历	研究生	最高学位	硕士
毕业学校	西北工业大学			毕业时间	2005年05月31日	所学专业	计算机科学与技术
电子邮箱	yangfan@sntec.org.cn			办公电话	029-89381939	移动电话	13572138689
通讯地址	陕西省西安市雁塔区茶张路1号省信息化中心19层					邮政编码	710065
工作单位	陕西省网络与信息安全测评中心					行政职务	总工程师
二级单位	无					党　　派	中国共产党
完成单位	陕西省网络与信息安全测评中心					所在地	陕西
						单位性质	行政机关或其他事业单位
参加本项目的起止时间	自 2016年01月01日　至 2018年05月31日						

对本项目技术创造性贡献：

对工业控制系统指纹探测技术、工业控制系统漏洞POC探测技术、工业控制系统测试攻击技术、工业控制系统安全检测技术做出了创造性贡献。

主要科技创新：工业控制系统生产仿真技术、工业控制系统安全检测技术、工业控制系统测试攻击技术、分布式存储技术、海量数据清洗技术。

研究成果：应用案例“能源化工工业控制系统安全测试仿真平台”，附件6-4；实用新型专利“一种工业大数据交换处理用便于放置的主机服务器”ZL202021185781.3，附件1-1；实用新型专利“一种工业大数据服务处理用具有散热功能的主机服务器”ZL202021185755.0。

曾获科技奖励情况：

曾获2012年度陕西省科学技术奖，项目名称：陕西省政府网站绩效评估研究及应用，奖励等级：叁等，证书编号：2012-3-112-R5

曾获2015年度陕西省科学技术奖，项目名称：云计算安全关键技术验证与攻防平台，奖励等级：贰等，证书编号：2015-2-056-R7

声明：本人同意完成人排名，遵守《陕西省科学技术奖励方法》及其实施细则的有关规定，承诺遵守评审工作纪律，保证所提供的有关材料真实有效，且不存在任何违反《中华人民共和国保守陕西省密法》和《科学技术保密规定》等相关法律法规及侵犯他人知识产权的情形。如产生争议，保证积极配合调查处理。如有材料虚假或违纪行为，愿意承担相应责任并接受相应处理。承诺该项目是本人本年度提名的唯一项目。

本人签名：

年　　月　　日

完成单位声明：本单位确认该完成人情况表内容真实有效，且不存在任何违反《中华人民共和国保守国家密法》和《科学技术保密规定》等相关法律法规及侵犯他人知识产权的情形。如产生争议，愿意积极配合调查处理工作。

工作单位声明：本单位对该完成人被提名无异议。

单位（盖章）

年　　月　　日

姓　　名	杨向东	性别	男	排　　名	3	国　　籍	中国
出生年月	1987年05月05日			出 生 地	宝鸡市	民　　族	汉族
身份证号	610321198705050015			归国人员	否	归国时间	
技术职称	工程师			最高学历	研究生	最高学位	硕士
毕业学校	四川大学			毕业时间	2016年06月01日	所学专业	软件工程
电子邮箱	yangxiangdong@sntec.org.cn			办公电话	029-88319550	移动电话	15829730621
通讯地址	陕西省西安市雁塔区茶张路1号省信息化中心19层					邮政编码	710065
工作单位	陕西省网络与信息安全测评中心					行政职务	技术研究总监
二级单位	无					党　　派	群众
完成单位	陕西省网络与信息安全测评中心					所在地	陕西
						单位性质	行政机关或其他事业单位
参加本项目的起止时间	自 2016年01月01日　至 2018年05月31日						

对本项目技术创造性贡献：

对工业控制系统测试攻击技术、工业控制系统安全检测技术做出了创造性贡献。

主要科技创新：工业控制系统安全检测技术、工业控制系统测试攻击技术、分布式存储技术、海量数据清洗技术。

研究成果：实用新型专利“一种工业大数据交换处理用便于放置的主机服务器”ZL202021185781.3，附件1-1；实用新型专利“一种工业大数据服务处理用具有散热功能的主机服务器”ZL202021185755.0，附件1-2；技术论文《工业控制系统信息安全风险评估研究与分析》，附件1-4；技术论文《工业控制系统安全检查工作现状分析及对策研究》，附件1-6；技术论文《工业控制系统的安全现状分析研究》，附件1-7。

曾获科技奖励情况：

曾获2018年度陕西省电子学会科学技术奖，项目名称：陕西省互联网网站云防御及追踪平台，奖励等级：贰等，证书编号：SD-2018-2-3-R2；

曾获2022年度陕西省电子学会科学技术奖，项目名称：工业控制系统网络安全态势感知技术与应用，奖励等级：贰等，证书编号：SD-2022-2-4

声明：本人同意完成人排名，遵守《陕西省科学技术奖励方法》及其实施细则的有关规定，承诺遵守评审工作纪律，保证所提供的有关材料真实有效，且不存在任何违反《中华人民共和国保守陕西省密法》和《科学技术保密规定》等相关法律法规及侵犯他人知识产权的情形。如产生争议，保证积极配合调查处理。如有材料虚假或违纪行为，愿意承担相应责任并接受相应处理。承诺该项目是本人本年度提名的唯一项目。

本人签名：

年　　月　　日

完成单位声明：本单位确认该完成人情况表内容真实有效，且不存在任何违反《中华人民共和国保守国家密法》和《科学技术保密规定》等相关法律法规及侵犯他人知识产权的情形。如产生争议，愿意积极配合调查处理工作。

工作单位声明：本单位对该完成人被提名无异议。

单位（盖章）

年　　月　　日

姓　　名	杨帆	性别	男	排　　名	4	国　　籍	中国
出生年月	1990年01月10日			出 生 地	西安市	民　　族	汉族
身份证号	610125199011012515			归国人员	否	归国时间	
技术职称	工程师			最高学历	大学本科	最高学位	学士
毕业学校	西安邮电大学			毕业时间	2013年07月01日	所学专业	信息安全
电子邮箱	yangfan11@sntec.org.cn			办公电话	029-88319550	移动电话	13299060822
通讯地址	陕西省西安市雁塔区茶张路1号省信息化中心19层					邮政编码	710065
工作单位	陕西省网络与信息安全测评中心					行政职务	无
二级单位	无					党　　派	群众
完成单位	陕西省网络与信息安全测评中心					所 在 地	陕西
						单位性质	行政机关或其他事业单位
参加本项目的起止时间	自 2016年01月01日　至 2018年05月31日						

对本项目技术创造性贡献：

主要对工业控制系统漏洞POC探测技术、工业控制系统测试攻击技术做出了贡献。科技创新：工业控制系统生产仿真技术、工业控制系统安全检测技术、工业控制系统测试攻击技术。成果：应用案例“能源化工工业控制系统安全测试仿真平台”附件6-4；标准规范工业互联网平台安全白皮书（2020）附件1-3；技术论文《基于工业控制系统信息安全检查方法的研究》附件1-5；技术论文《基于分布式思想构筑面向化工行业的工业互联网安全堡垒》附件1-8；技术论文《基于工业互联网平台数据安全评估的设计》附件1-9；国标《工业控制系统安全防护技术要求和测试评价方法》附件6-8；国标《工业控制系统信息安全防护能力成熟度模型》附件6-9。

曾获科技奖励情况：

曾获2018年度陕西省电子学会科学技术奖，项目名称：陕西省互联网网站云防御及追踪平台，奖励等级：贰等，证书编号：SD-2018-2-3-R2；

曾获2022年度陕西省电子学会科学技术奖，项目名称：工业控制系统网络安全态势感知技术与应用，奖励等级：贰等，证书编号：SD-2022-2-4

声明：本人同意完成人排名，遵守《陕西省科学技术奖励方法》及其实施细则的有关规定，承诺遵守评审工作纪律，保证所提供的有关材料真实有效，且不存在任何违反《中华人民共和国保守陕西省密法》和《科学技术保密规定》等相关法律法规及侵犯他人知识产权的情形。如产生争议，保证积极配合调查处理。如有材料虚假或违纪行为，愿意承担相应责任并接受相应处理。承诺该项目是本人本年度提名的唯一项目。

本人签名：

年　　月　　日

完成单位声明：本单位确认该完成人情况表内容真实有效，且不存在任何违反《中华人民共和国保守国家密法》和《科学技术保密规定》等相关法律法规及侵犯他人知识产权的情形。如产生争议，愿意积极配合调查处理工作。

工作单位声明：本单位对该完成人被提名无异议。

单位（盖章）

年　　月　　日

姓　　名	高瑞	性别	男	排　　名	5	国　　籍	中国
出生年月	1981年08月31日			出 生 地	西安市	民　　族	汉族
身份证号	610104198108310010			归国人员	否	归国时间	
技术职称	工程师			最高学历	大学本科	最高学位	学士
毕业学校	中国人民解放军空军工程大学			毕业时间	2005年06月30日	所学专业	计算机科学与技术
电子邮箱	gaorui@sntec.org.cn			办公电话	029-88319550	移动电话	13359212227
通讯地址	陕西省西安市雁塔区茶张路1号省信息化中心19层					邮政编码	710065
工作单位	陕西省网络与信息安全测评中心					行政职务	项目总监
二级单位	无					党　　派	群众
完成单位	陕西省网络与信息安全测评中心					所在地	陕西
						单位性质	行政机关或其他事业单位
参加本项目的起止时间	自 2016年01月01日　至 2018年05月31日						

对本项目技术创造性贡献：

工业控制系统网络环境的部署与研究，规划工控实验网络环境，划分企业管理、工厂管理、工业控制、仪器仪表等安全层级，重点研究工业控制系统网络安全设备的应用于部署。

主要科技创新：工业控制系统测试攻击技术、工业控制系统安全检测技术、分布式存储技术、海量数据清洗技术。

研究成果：实用新型专利“一种工业大数据交换处理用便于放置的主机服务器”ZL202021185781.3，附件1-1；实用新型专利“一种工业大数据服务处理用具有散热功能的主机服务器”ZL202021185755.0，附件1-2；技术论文《基于工业控制系统信息安全检查方法的研究》，附件1-5。

曾获科技奖励情况：

曾获2018年度陕西省电子学会科学技术奖，项目名称：陕西省互联网网站云防御及追踪平台，奖励等级：贰等，证书编号：SD-2018-2-3-R2；

曾获2022年度陕西省电子学会科学技术奖，项目名称：工业控制系统网络安全态势感知技术与应用，奖励等级：贰等，证书编号：SD-2022-2-4

声明：本人同意完成人排名，遵守《陕西省科学技术奖励方法》及其实施细则的有关规定，承诺遵守评审工作纪律，保证所提供的有关材料真实有效，且不存在任何违反《中华人民共和国保守陕西省密法》和《科学技术保密规定》等相关法律法规及侵犯他人知识产权的情形。如产生争议，保证积极配合调查处理。如有材料虚假或违纪行为，愿意承担相应责任并接受相应处理。承诺该项目是本人本年度提名的唯一项目。

本人签名：

年　　月　　日

完成单位声明：本单位确认该完成人情况表内容真实有效，且不存在任何违反《中华人民共和国保守国家密法》和《科学技术保密规定》等相关法律法规及侵犯他人知识产权的情形。如产生争议，愿意积极配合调查处理工作。

工作单位声明：本单位对该完成人被提名无异议。

单位（盖章）

年　　月　　日

九、主要完成单位情况表

单位名称	陕西省网络与信息安全测评中心				
排　　名	1	法定代表人	白晓军	所 在 地	陕西
单位性质	行政机关或其他事业单位	传　　真	029-88317698	邮政编码	710065
通讯地址	陕西西安高新区茶张路1号省信息化中心十九层				
联 系 人	李严	单位电话	029-88319550	移动电话	17778957519
电子邮箱	liyan@sntec.org.cn				

对本项目科技创新和应用推广情况的贡献：

本项目为陕西省网络与信息安全测评中心独立完成，对本项目科技创新和推广应用情况的贡献包括科技创新:

1.工业控制组件搜索引擎

2.工业控制系统指纹探测技术

3工业控制系统漏洞POC探测技术

4.工业控制系统测试攻击技术

5.工业控制系统安全检测技术推广应用:

目前基于工业大数据的网络安全态势感知技术研究与应用在我省的应用推广主要靠工业企业安全检查、工控风险漏洞通报、工控安全培训等多种形式开展，其推广应用的目的是为了发现我省重点行业中工控系统网络安全漏洞，为其加固整改提供建议，提高其救体网络安全防护水平，并与重点企业建立沟通的桥梁，定期下发安全漏洞风险，提供咨询、培训、测试等服务，帮助企业解决工控安全问题，以减少企业采取的安全防护措施成本，提升企业工业控制系统的安全防护能力，保障工业控制系统的安全运行，降低因网络安全所带来的生产风险。

声明：本单位同意完成单位排名，遵守《陕西省科学技术奖励方法》及其实施细则的有关规定，承诺遵守评审工作纪律，保证所提供的有关材料真实有效，且不存在任何违反《中华人民共和国保守国家密法》和《科学技术保密规定》等相关法律法规及侵犯他人知识产权的情形。如产生争议，保证积极配合调查处理。如有材料虚假或违纪行为，愿意承担相应责任并接受相应处理。

法定代表人签名：　　单位（盖章）

年　　月　　日　　年　　月　　日

附表 1

完成人合作关系说明

本项目完成人赵首花、杨帆、杨向东、杨帆、高瑞均属陕西省网络与信息安全测评中心同一单位。第一完成人赵首花任安全服务部部长，为项目总负责人；赵首花、杨帆、杨向东、杨帆、高瑞均为中心同一项目组。本项目合作时间2016.01-2018.05，完成人共同完成本项目，具有共同知识产权，共同获奖等。

本项目完成人赵首花、杨帆、杨向东、高瑞共同获得了“一种工业大数据交换处理用便于放置的主机服务器”实用新型专利（ZL202021185781.3）（附件 1-1）；赵首花、杨帆、杨向东、高瑞共同获得了“一种工业大数据服务处理用具有散热功能的主机服务器”实用新型专利（ZL202021185755.0）（附件 1-2）。杨向东、赵首花等合著完成了“工业控制系统信息安全风险评估研究与分析”论文（《网络空间安全》2017 年第 08-09 期）（附件 1-4）；杨帆、高瑞等合著完成了“基于工业控制系统信息安全检查方法的研究”论文（《工业控制计算机》2018 年底 31 卷第 10 期）（附件 1-5）；杨向东、赵首花、杨帆等合著了“工业控制系统安全检查工作现状分析及对策研究”论文（《工业控制计算机》2019 年 10 月）（附件 1-6）；赵首花、杨向东等合著完成了“工业控制系统的安全现状分析研究”论文（工业控制计算机 2019.11）（附件 1-7）；杨帆、赵首花等合著了“基于工业互联网平台数据安全评估的设计”论文（《工业控制计算机》2020 年 8 月）（附件 1-10）。

第一完成人签名：

完成人合作关系情况汇总表

序号	合作方式	合作者/项目排名	合作起始时间	合作完成时间	合作成果	证明材料
1	共同知识产权	赵首花/1、杨帆/2、杨向东/3、高瑞/5	2019.3	2020.11	一种工业大数据交换处理用便于放置的主机服务器	附件 1-1
2	共同知识产权	赵首花/1、杨帆/2、杨向东/3、高瑞/5	2019.3	2020.11	一种工业大数据服务处理用具有散热功能的主机服务器	附件 1-2
3	论文合著	杨向东/3、赵首花/1	2017.5	2017.8	工业控制系统信息安全风险评估研究与分析	附件 1-4
4	论文合著	杨帆/4、高瑞/5	2018.3	2018.7	基于工业控制系统信息安全检查方法的研究	附件 1-5
5	论文合著	杨向东/3、赵首花/1、杨帆/4	2019.8	2019.10	工业控制系统安全检查工作现状分析及对策研究	附件 1-6
6	论文合著	赵首花/1、杨向东/3	2019.8	2019.10	工业控制系统的安全现状分析研究	附件 1-7
7	论文合著	杨帆/4、赵首花/1	2021.3	2021.5	基于工业互联网平台数据安全评估的设计	附件 1-10

承诺：本人作为项目第一完成人，对本项目完成人合作关系及上述内容的真实性负责，特此声明。

第一完成人签名：