拟申报项目公示内容

一、项目名称

《工业控制系统网络安全工程实验室》

二、项目简介

随着工业化与信息化进程的不断交叉融合，越来越多的信息技术应用到了工业领域。目前，工业控制系统已广泛应用于核设施、石油石化、电力、先进制造、水利枢纽、城市轨道交通、城市供水供气供热等工业领域，依靠工业控制系统来实现自动化作业。工业控制系统已经成为国家关键基础设施的重要组成部分，工业控制系统的安全关系到国家的战略安全。由于工业控制系统广泛采用通用软硬件和网络设施，以及与企业管理信息系统的集成，导致工业控制系统越来越开放，并且与企业内网，甚至是与互联网产生了数据交换。攻击工控网络的趋势愈演愈烈，震网、Duqu、火焰、棱镜门等重大事件造成世界范围内的巨大影响，国务院、工信部出台相关文件明确要求：保障工业控制系统安全。但是，我国目前大量的工业控制和工业网络交换领域的设备、技术、软件大量依赖于进口，其核心技术国外对我们实施封锁；工业控制和网络技术发展迅速，产品类型多样，产品功能复杂且工作环境复杂，攻击方法多样，难以对工业控制系统中的网络攻击进行评测。

陕西省工业控制系统网络安全工程实验室是为了应对两化融合而带来的信息安全挑战而建设的高度集成、最贴合生产控制网络实际的研究和检测平台，为直观表现工控、网络设备的可靠性和整体检测分析工控设备及其网络的性能，我单位在整合国外先进技术的基础上提出了陕西省工控网络安全检测及攻防实验室整体解决方案，以解决陕西省内复杂工控和网络设备的检测分析需求，帮助测评中心有效验证工业控制信息空间的稳定。


陕西省工业控制系统网络安全工程实验室项目一是结合重点行业典型和真实工艺流程，搭建仿真测试环境，为进入工业控制系统的产品、设备和系统等提供安全测试和风险评估服务；二是建设工业控制系统风险漏洞信息库，制定量化评价标准，形成测试评估指南；三是开发自动化测试工具集，开展工控安全攻防测试，对相关风险解决方案的有效性提供验证测试。通过建设面向能源、先进制造行业工业控制系统安全可靠的公共技术服务平台，为设备生产商、设备使用者提供高效统一、成熟稳定的安全测试和风险控制服务，构筑我国工业控制系统信息安全的风险防控体系基础，提高我国工业控制系统的抗风险能力。

工业控制系统仿真技术：对工业控制网络从办公网络层、操作管理层、现场控制层、生产控制层、生产执行层进行区域划分，结合工业生产和控制过程，多种生产管理系统和控制系统同时运行。办公网络层包含网关、外界防火墙、企业管理客户端、企业门户等仿真技术；操作管理层包含企业 OPC 防火墙、SCADA 服务企业器、OPC 服务器、活动目录服务器等仿真技术；现场控制层包含生产控制参数配置、设备组态软件控制、主机策略配置等仿真技术；生产控制层包含现场控制设备、工控机等，仿真控制和读取设备生产参数；生产执行层包含操作设备、传感器等仿真技术。

工业控制系统测试攻击技术：通过外网进行专业渗透式攻击技术实现从从工业控制系统外网到进入企业办公网络，以进一步针对工业控制系统主机实行渗透攻击；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；通过恶意代码传播技术对移动存储设备进行渗透攻击后，将其与控制设备、工控主机等进行连接，完成移动设备的渗透测试攻击。

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、基于主机的设备、网络节点设备、与工业过程接口的软件等工控相关设备进行安全检测，评估工业设备的网络健壮性并证明它们满足一整套需求和一致性的标准。

陕西省工业控制系统网络安全工程实验室自建成以来，在工业企业、工控安全厂商、第三方服务机构等单位进行了应用，各单位根据不同需求，对工业控制

系统安全防护设备、控制设备、应用软件、数据安全等内容进行研究测试，为相关单位提供了实验环境，同时扩大了合作交流，提升了测评中心的工业控制系统安全技术能力。

三、客观评价

陕西省工业控制系统网络安全工程实验室自建成以来，与相关安全厂商、工业企业、第三方服务机构等 10 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。实验室的部署与应用取得了良好的经济、社会效益，得到了良好的应用与推广。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；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，相关安全服务年收益预计为 50 万。

作为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，实验室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，通过实验室建设，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。

四、应用情况

建设陕西省工业控制系统网络安全工程实验室构建了完整的贴合现场运行环境的工业控制网络系统，工控设备的网络安全可靠性分析离不开具体的网络环境和工业过程，通过合理规划以实现不同品牌、型号工控设备的互联，并提供组态软件实现实时监控、远程操作环境，建立针对不同厂家、不同工业控制协议和设备的专业的漏洞挖掘系统，协助测评人员开展工业控制网络安全风险评估、工控设备和系统的漏洞挖掘及脆弱性分析、工业控制网络病毒行为研究、工业安全协议设计和系统仿真、以及工业控制网络安全防护技术研究，直观反映工控设备在企业网络中被恶意攻击和病毒侵袭的可能、分析工控设备的运行状态及其在整个企业网络中的输入输出、验证设备的检测结果和存在的安全风险。

截止目前，测评中心通过以工业控制系统网络安全工程实验室为基础，与相关安全厂商、工业企业、第三方服务机构等 10 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、开放的端口 9 个，相关测试数据在持

续发现中。

近年来，为了推进工业控制系统网络安全产业发展，测评中心从以下几个方面开展业务应用推广：

1、开展企业安全检查：协助地方工业和信息化主管部门，指导区域内的工业企业制定工控安全防护实施方案，对工业控制系统应用企业以及工业控制系统规划、设计、建设、运维、评估等方面进行安全检查，涉及安全软件选择与管理、配置和补丁管理、边界安全防护、物理和环境安全防护、身份认证、远程访问安全、安全监测和应急预案演练、资产安全、数据安全、供应链管理、责任落实等检查内容，结合工业控制系统网络安全工程实验室对检查中发现的安全风险在实验环境中进行测试，是否对生产系统的可用性造成影响，以帮助工业企业在实际生产环境中能够顺利加强安全防护措施。

2、组建工控安全风险通报成员单位：受省工信厅委托，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）》，建立健全工业控制系统信息安全通报工作机制，协助开展信息通报和风险预警等工作，逐步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。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，结合工业控制系统网络安全实验室仿真环境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。

3、组织实施安全培训：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。

4、召开用户答谢会议：每年定期召开客户答谢会议，通过“答谢会”形式，宣传工业控制系统网络安全研究及业务开展情况，宣扬企业文化和企业价值，让新老客户了解我们的工业控制系统网络安全服务能力和水平，与客户展开深入沟通交流、交换意见、为现有工业控制系统网络安全项目的落实和下一步合作意向打下坚实基础，通过答谢会进一步推广工业控制系统网络安全服务形式和内容。

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	北京神州绿盟科技有限公司	工控安全技术	工控安全服务	2016年10月至今	关倩倩/18602988133
2	陕西电子工业研究院	工控安全技术	工控安全服务	2016年9月至今	雷亚龙/15009266628
3	上海三零卫士信息安全有限公司	工控安全技术	工控安全服务	2016年10月至今	穆喜产/18700417139
4	北京威努特技术有限公司	工控安全技术	工控安全服务	2016年12月至今	宁大鹏/17782836657
5	陕西思科锐迪网络安全技术有限公司	工控安全技术	工控安全服务	2017年8月至今	黄旭/18990559267
6	远江盛邦（北京）网络安全科技股份有限公司	工控安全技术	工控安全服务	2017年1月至今	徐讯飞/18602998596
7	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	2016年12月至今	王玉婷/15229394696
8	西安通软软件科技有限公司	工控安全技术	工控安全服务	2016年12月至今	黄女士/15309263314
9	西安恒联软件科技有限公司	工控安全技术	工控安全服务	2016年12月至今	杨女士/18792967057
10	陕西省网络与信息安全测评中心	工控安全技术	工控安全服务	2016年8月至今	杨帆/13299060822

五、主要知识产权和标准规范等目录

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	论文	工业控制系统信息安全风险评估研究与分析	中国	CN10-1421/TP	2017 年 8 月 1 日	《网络空间安全》2017 年第 08-09 期	陕西省网络与信息安全测评中心	杨向东、赵首花
2	论文	工业控制系统安全隐患和防护分析	中国	CN51-1567/TN	2018 年 9 月 1 日	《数字化用户 》2018.09 第 24 卷第 09 期	陕西省网络与信息安全测评中心	李俊、杨睿超、杨帆

3	论文	基于工业控制系统信息安全检查方法的研究	中国	CN32-1764/TP	2018 年 10 月 1 日	《工业控制计算机》2018 年底 31 卷第 10 期	陕西省网络与信息安全测评中心	杨帆、高瑞、李俊

六、主要完成人情况

姓　　名	杨　帆	序号	第【1】完成人
行政职务	总工程师	技术职称	高级工程师
工作单位	陕西省网络与信息安全测评中心		
完成单位	陕西省网络与信息安全测评中心		
对本项目主要学术和技术创造性贡献	规划实验室建设方案，设计工业控制系统安全仿真平台、安全防护平台、安全检测平台功能架构，规划设计实验室网络环境，提出了工业控制安全仿真系统的建设要求，重点研究了工业控制安全仿真系统石油开采和集输工艺的设计与实现。		

姓　　名	赵首花	序号	第【2】完成人
行政职务	部长	技术职称	工程师
工作单位	陕西省网络与信息安全测评中心		
完成单位	陕西省网络与信息安全测评中心		
对本项目主要学术和技术创造性贡献	起草项目研究报告、实施方案等相关技术文档，负责工业控制系统安全仿真平台的研究与应用，规划平台控制系统，设计原油集输控制和管道控制模块，实现能源开发、采油系统、储运系统的模拟仿真还原，重点研究平台控制模块的设计与实现。		

姓　　名	杨向东	序号	第【3】完成人
行政职务	技术研究总监	技术职称	工程师
工作单位	陕西省网络与信息安全测评中心		
完成单位	陕西省网络与信息安全测评中心		

对本项目主要学术和技术创造性贡献	研究能源行业的攻击手段和方法，设计模拟仿真攻击过程。编写运行控制程序，实现正常运行、系统攻击、恢复初始状态的远程控制，重点研究设备故障、运行停滞、安全事故等模拟环境的设计与实现。

姓　　名	杨帆	序号	第【4】完成人
行政职务	无	技术职称	工程师
工作单位	陕西省网络与信息安全测评中心		
完成单位	陕西省网络与信息安全测评中心		
对本项目主要学术和技术创造性贡献	工业控制系统安全防护技术研究，设计安全防护平台渗透测试模块，研究工控通用协议控制方法，开展安全防护策略和工控协议的安全性测试验证等相关工作。		

姓　　名	高瑞	序号	第【5】完成人
行政职务	项目总监	技术职称	工程师
工作单位	陕西省网络与信息安全测评中心		
完成单位	陕西省网络与信息安全测评中心		
对本项目主要学术和技术创造性贡献	设计规划工业控制系统安全仿真平台沙盘模型，完成油井生产现场、生产站点、集输控制管道和化工原料储存等真实生产环节模型的工艺设计，重点研究工业控制系统安全仿真平台灯光展示效果及模块设计。		

姓　　名	李俊	序号	第【6】完成人
行政职务	无	技术职称	助理工程师
工作单位	陕西省网络与信息安全测评中心		
完成单位	陕西省网络与信息安全测评中心		
对本项目主要学术和技术创造性贡献	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。		

姓　　名	李丹	序号	第【7】完成人
行政职务	无	技术职称	工程师
工作单位	陕西省网络与信息安全测评中心		
完成单位	陕西省网络与信息安全测评中心		
对本项目主要学术和技术创造性贡献	工业控制协议研究，研究 DNP3 协议控制方法，开展安全防护策略和工控协议的安全性测试验证等相关工作。		

七、主要完成单位及创新推广贡献

单位名称	陕西省网络与信息安全测评中心	序　号	第【1】完成单位

陕西省网络与信息安全中心成立于 2009 年 3 月，是具有独立法人资格的事业单位，是专业从事网络安全服务的第三方权威机构，是我省网络安全和信息化建设的支撑单位。根据批复，主要职责为网络与信息系统安全测评，网络与信息系统安全保障体系的设计及咨询服务，信息安全等级保护和风险评估技术支持与服务，网络与信息安全应急响应与救援，网络与信息安全技术与管理培训，网络与信息安全相关应用技术研究等。

对本项目科技创新和推广应用情况的贡献：

科技创新：

1. 工业控制系统生产仿真技术。对工控网络从办公网络层、操作管理层、现场控制层、生产控制层、生产执行层进行区域划分，结合工业生产和控制过程，实现多种生产管理系统和控制系统同时运行。

2. 工业控制系统测试攻击技术。通过外网进行专业渗透式攻击技术实现从工控系统外网到进入企业办公网络，以进一步针对工控系统主机实行渗透攻击；通过内网渗透测试技术对工控系统中的主机节点、开放的服务端口、控制设备等进行渗透攻击；通过恶意代码传播技术对移动存储设备进行渗透攻击后，将其与控制设备、工控主机等进行连接，完成移动设备的渗透测试攻击。

3. 工业控制系统安全检测技术。通过工控系统安全检测技术对嵌入式设备、基于主机的设备、网络节点设备、与工业过程接口的软件等工控相关设备进行安全检测，评估工业设备的网络健壮性并证明它们满足一整套需求和一致性的标准。

推广应用：

目前实验室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、客户答谢等多种形式开展，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，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。

八、完成人合作关系说明

本项目完成人杨帆、赵首花、杨向东、杨帆、高瑞、李俊、李丹均属陕西省网络与信息安全测评中心同一单位。第一完成人杨帆任总工程师，为项目总负责人；赵首花、杨向东、杨帆、高瑞、李俊、李丹均为中心同一部门，同一课题组。本项目合作时间 2016.01-2018.04，完成人共同完成本项目，具有共同知识产权，共同获奖等。

本项目完成人杨帆、赵首花等共同获得 2012 年度陕西省科学技术三等奖“陕西省政府网站绩效评估研究及应用”（2012-3-112-R5）。

本项目完成人杨向东、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）；李俊、杨帆等合著完成了“工业控制系统安全隐患和防护分析”论文（《数字化用户》2018 年第 9 期）；杨帆、高瑞、李俊等合著完成了“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）；高瑞、李俊合著了 “工业私有云安全防护体系研究与分析”论文，（《工业控制计算机》2019 年 5 月）；杨向东、赵首花、杨帆、李丹合著了“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）。

九、经济效益和社会效益

1.经济效益

工业控制系统网络安全工程实验室的建设为开展工业控制系统网络安全测试研究工作提供了基础环境，为测评中心开展工业控制系统风险评估及漏洞通报工作提供实验支撑。实验室自建成以来，与相关安全厂商、工业企业、第三方服务机构等 10 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。

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，相关安全服务年收益预计为 50 万。

利用工业控制系统网络安全工程实验室仿真环境，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。

2.社会效益

陕西省工业控制系统网络安全工程实验室是为了应对两化融合而带来的信息安全挑战而建设的高度集成、最贴合生产控制网络实际的研究和检测平台。是构建完整的贴合现场运行环境的工业控制网络系统，合理规划以实现不同品牌、型号工控设备的互联，并提供组态软件实现实时监控、远程操作的任务环境。建立针对不同厂家、不同工业控制协议和设备的专业的漏洞挖掘系统，协助测评人员开展工业控制网络安全风险评估、工控设备和系统的漏洞挖掘及脆弱性分析、工业控制网络病毒行为研究、工业安全协议设计和系统仿真、以及工业控制网络安全防护技术研究。

通过陕西省工业控制系统网络安全工程实验室的建设，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。

陕西省工业控制系统网络安全工程实验室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，实验室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，通过实验室建设，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，最大限度地利用工业控制系统网络安全工程实验室现有设备资源，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，通过工业控制系统网络安全工程实验室仿真环境搭建符合企业生产业务的测试环境，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。