

平顶山学院能源互联网信息安全实训平台项目供货与 安装合同

甲方：平顶山学院（采购方）

乙方：北京热月教育科技有限公司（供货方）

经过招标，甲乙双方充分协商，特订立本合同，以便共同遵守。

一、合同标的

双方根据招标文件及其补充文件、成交供应商的投标响应文件及其澄清文件和甲方政府采购项目明细表等确定合同标的（清单附后，甲乙双方须在清单上盖章）。

二、合同价格

大写人民币：玖拾柒万伍仟叁佰元整

小写人民币：¥ 975300.00

三、交货时间及地点

1. 乙方在签订合同后 30 日历天内按照合同约定产品的功能、数量及甲方的需求送达甲方指定地点安装、调试并培训完毕，完成、调试时乙方应提前与甲方联系。

2. 乙方自定运输方式，自付费用自担风险将合同标的送达甲方指定地点并完成安装调试。

3. 设备安装过程中的安装风险由乙方承担；

4. 本项目价格包含设备费用及安装过程中所需的配套材料、安装施工和垃圾清运等费用。

四、技术规格

1. 乙方依据甲方招标技术要求，并满足标的清单中的规定，为甲方开发软件产品，乙方提供的产品的技术规格有国家标准的应符合现

行国家标准，无国家标准的应符合部颁标准或行业标准，依据甲方招标技术要求，满足招标响应文件中的参数偏离承诺，满足甲方正常教学科研使用需求。

2.乙方保证提供的产品是最新且稳定的正品，软件安装符合有关标准。交付材料应包含产品清单、软件安装介质和安装指南、软件著作权证书、质量合格证、保修卡、软件操作和使用说明书等一系列保证产品质量和正常使用的全套中文使用及维护手册。

3.根据应用系统的业务特点及学校需求，建立应用系统全面指标化的可视化数据分析大屏，能够根据不同角色展示不同的数据内容，且支持多级数据下钻特性。

五、施工要求

本项目属交钥匙工程，乙方负责甲方相关实验室的环境改造。项目施工辅材辅料应按以下相关要求提供：

1.所有电源线均为绝缘阻燃包覆，铜芯。小功率纤芯不低于 2 平方铜线、独芯；大功率纤芯根据实际情况使用不低于 6 平方独芯铜线；超大功率使用多股铜芯电缆；电源线不允许通过接线延长。

2.墙插、排插等辅材外壳为绝缘阻燃材料，内置导电接触金属片均为铜质；地插等类似辅材均为绝缘防水型。所有墙插、排插等要求均不低于国家标准(GB 1002-2024)或行业标准。

3.所有网线不低于国标六类无氧铜网线。

4.所有穿线管、屏蔽管等辅材要求均不低于国家或行业标准。

5.HDMI 高清线为双屏蔽且信号传输速率不低于 4K/30Hz，超过 25 米时使用光纤 HDMI 高清线。

6.所有信号线、外置电源线均要穿管安装。

7. 所有音频线等相关线材均需穿管，管材必须为绝缘电磁屏蔽管。
8. 所有线材、辅材入场施工前，需经甲方确认后方可施工；所有用电设备无明确要求不接地的需要全部接地。
9. 乙方负责清理因施工产生的垃圾至市政指定清运点或学校方圆 5 公里之外合法倾倒点。
10. 所用材料应不低于国家规定环保标准（无国家标准的应不低于行业相关环保），且无毒无味。

六、附件、配件

按产品所附使用说明书及清单执行；包括在促销等特别期间承诺提供的附件、配件。

七、售后服务

1. 质量：质保期五年，自验收合格签字之日起计算。质保期内乙方免费维修、更换设备零配件，免费对软件维护（修复、优化、升级、调试）、二次开发等，且保证维护期间软件能够正常使用；每学期不少于 1 次主动上门进行技术支持与维护。未按约定完成上门进行技术支持与维护义务的，质保期相应顺延，缺一次顺延六个月，以此类推，顺延期间乙方照常承担全部质保责任。质保期外维修只收取零配件成本费用，不收维修费；免费对软件维护（含功能错误修正或修改、修复系统安全漏洞），免费提供电话及网上在线服务和技术支持。软件终身免费升级。终身免费提供系统全生命周期内的 BUG 及安全漏洞消除、相关库（包含但不限于病毒库、各种特征库等）的升级与服务。

2. 技术培训：按照招标文件中要求及投标响应文件中承诺，乙方免费对甲方（不限人次数）进行技术培训，保证甲方人员能够熟练独立操作，主要内容包括但不限于产品的原理及功能、操作使用、维护、

保养、常见问题及解决办法等内容。培训结束后，乙方要对被培训人员考核，同时发放培训合格证。

3.对于产品出现的问题，乙方在接到甲方通知后 0.5 小时内响应，24 小时内排除故障；软件系统安全缺陷要求 20 分钟响应，12 小时内解决问题。一切费用由乙方承担。

4.根据甲方的要求终身免费提供全量数据和接口；终身免费提供与相关系统对接，并保证对接系统的正常使用；甲方在使用乙方所供软件产品中出现问题需乙方指导解决时，乙方应及时给予解决。

5.质保期内重大故障无法及时排除时，乙方在 20 分钟内提供备品备件供甲方使用，且每发生一次，其质保期相应延长 30 天。如给甲方带来重大损失的，乙方承担损失费用。

八、验收及异议

1.乙方供货、安装调试完毕，甲方经过试用后根据实际验收情况签发验收报告，验收时甲方可邀请第三方参与验收过程；

2.甲方在验收中，如果发现有与合同规定不符的，应在 3 天内向乙方提出书面异议，不签发验收报告；并同时将该书面异议送达有关部门；甲方未按规定期限提出书面异议并且签发验收报告的，视为甲方放弃自己的权利。乙方在接到甲方书面异议后，应在 3 天内予以纠正，并对纠正情况以书面形式告知有关部门，否则视为无效。乙方在纠正过程中产生的费用由乙方承担。乙方不积极按照甲方要求予以纠正的，甲方有权解除合同，并不支付任何费用。

九、付款方式

乙方在供货安装调试完毕后，向甲方提交合同总金额 5% (¥48765.00 元) 的银行履约保函，保函有效期自履约保函开具之日

起至质保期满后 3 个月止,担保范围涵盖本合同项下全部售后服务及质量保证责任。提交符合约定的银行履约保函是甲方启动本项目正式验收的前置条件;乙方未提交合规银行履约保函前,甲方有权不予组织正式验收。甲方试用无质量问题且验收合格后,乙方开具增值税专用发票,甲方支付 100% 货款。在保函有效期满且双方无异议后退还保函。

十、违约责任

1.乙方不能在合同约定的时间内按照甲方的要求完成设备、软件的开发和安装(含提供全量数据和数据字典等)、调试(含系统对接和安全漏洞修复等)和培训的或因不可抗力的原因不能按时全部按照甲方的要求完成设备、软件开发、安装(含提供全量数据和数据字典等)、调试(含系统对接和安全漏洞修复等)和培训的,且未能在不可抗力发生后提供书面证明材料的,10 日以内按照合同金额的 0.5%每日向甲方支付违约金,超过 10 日按合同金额的 1%每日向甲方支付违约金,超过 20 日未完成供货者,甲方除了有权要求乙方支付违约金之外,且有权解除合同,并向乙方索赔由此造成的损失。

2.乙方所交标的功能、品牌、型号、规格、质量等不符合合同规定的,甲方有权拒绝接收,并按违约处理,同时按照超期完成项目缴纳违约金,且承担由此给甲方带来的损失,甲方有权解除合同。

3.乙方未按甲方要求提交银行履约保函的,经甲方书面催告 7 个日历天内仍未补正、更换合规银行履约保函的,乙方应按合同总金额 0.5%每日向甲方支付违约金;若乙方逾期超过 30 日仍未能提供合规银行履约保函,视为乙方根本违约,甲方有权单方解除本合同,乙方须承担由此给甲方造成的全部损失。

4. 甲方验收合格后应及时办理付款手续并向乙方支付货款。

5. 甲乙双方的任何一方由于不可抗力的原因导致无法履行合同的，应在不可抗力发生后及时向对方通报不能履行或不能完全履行的理由，并提供相应的证明材料。允许延期履行、部分履行或者不履行合同，并根据情况可部分或全部免予承担违约责任。

6. 乙方若未按照合同约定进行售后服务，甲方有权通知银行进行索赔。

十一、其他

1. 本合同如发生纠纷，甲乙双方协商解决，协商不成时，约定由平顶山仲裁委员会仲裁。

2. 本合同自签章之日起生效，甲乙双方均不得随意变更或解除合同。

3. 标的软件产品需部署到甲方本地服务器；软件产品甲方有权永久免费使用、迁移、安装，乙方须免费提供技术支持；乙方承担对甲方的保密义务，包括但不限于对系统架构、部署情况、数据、策略、参数等的保密义务。规范操作甲方数据，不得越权或越界操作；乙方未经授权不得查询、获取、存储、传输用户方数据，不得向第三方泄露用户方数据。

4. 软件产品调试、运行过程中，乙方应根据甲方需求及时纠正不符合本合同参数要求和国家、行业标准要求的部分，实施升级完善；按照甲方需求实现与现有信息化相关子系统或数据的对接，并承担与第三方对接合作的费用。

5. 系统中使用的软件产品或组件必须符合国家有关知识产权的相关法律法规。乙方保证提供甲方使用的软件不侵犯第三方的知识产

权，不影响甲方的正常使用。因侵犯第三方知识产权所发生的纠纷及法律责任全部由乙方承担，因此导致影响甲方使用或造成甲方损失的，乙方应当赔偿甲方。

6. 根据等保相关政策，配合甲方完成有等保测评需要的项目的主要系统的等级保护定级与测评。

7. 本合同自签订之日起生效，合同执行期间，甲乙双方均不得随意变更或解除合同。合同如有未尽事宜，须经双方共同协商，做出补充规定，补充规定与本合同具有同等效力。本合同一式六份，甲方四份，乙方两份。

需方（甲方）：平顶山学院

代表人：



供方（乙方）：北京热月教育科技有限公司

代表人：

王海龙



地 址：河南省平顶山市新城区未来路南段

开户银行：中国银行平顶山分行营业部

账 号：257290314413

纳税人识别号：124100004168469074

电 话：0375-2657656

日 期：2026年8月28日

地 址：北京市昌平区超前路17号十纪科技大厦副楼601室

开户银行：招商银行股份有限公司北京昌平支行

账 号：110965766310001

纳税人识别号：91110114MA01BL5U2N

电 话：17600308816

日 期：2026年8月28日

附件 1. 供货清单

序号	产品名称	品牌	规格型号	生产厂家	产地	数量	单位	单价 (元)	总价 (元)	备注
1	高性能服务器	xFusion	2288H V5	东莞记忆存储科技有限公司	广东省 东莞市	3	台	61000.00	183000.00	制造商： 超聚变数字 技术有限公司
2	交换机	HUAWEI	S5735-S48T4E-V2 :100-240VAC, 50~60Hz, 3A	惠州迈腾伟业科技发展有限公司	广东省 惠州市	3	台	8500.00	25500.00	制造商： 华为技术有限公司
3	信息安全数字孪生靶场平台	赛博梦工厂	赛博梦工厂学习平台 V1.0/赛博梦工厂实训平台 V1.0/赛博梦工厂竞赛平台 V1.0/赛博梦工厂靶场平台 V1.0	北京热月教育科技有限公司	北京	1	套	226000.00	226000.00	
4	网络安全基础资源包	赛博梦工厂	赛博梦工厂实训资源包 V1.0	北京热月教育科技有限公司	北京	1	套	112800.00	112800.00	
5	实网攻防资源包	赛博梦工厂	赛博梦工厂综合场景资源包 V1.0	北京热月教育科技有限公司	北京	1	套	240000.00	240000.00	
6	工控能源安全场景演练资源包	赛博梦工厂	赛博梦工厂工控场景资源包 V1.0	北京热月教育科技有限公司	北京	1	套	188000.00	188000.00	
金额：人民币（大写） 玖拾柒万伍仟叁佰元整；									（小写）¥ 975300.00 元	

附件 2. 产品名称及参数

序号	名称	投标技术参数
1	高性能服务器	1. 性能指标 1) 产品类型: 2U 机架式服务器, 性能满足 120 人实践教学同时使用, 国产品牌, 标配原厂导轨; 2) 处理器: 配置 2 颗 Intel 6252 处理器, 单颗处理器 24 核, 主频 2.1GHz; 3) 内存: 配置 8 条 32G DDR4 内存, 支持 24 内存插槽; 4) 存储: 配置 6 块 960GB SSD 硬盘, 最大可插入 8 块 2.5/3.5 英寸热插拔硬盘; 5) 网卡: 本次配置 4 个千兆网口, 2 个万兆光口(含多模模块), 支持灵活 LOM 插卡; 6) RAID 卡: 配置 8 通道 RAID 卡, 2G 缓存, 支持 RAID0/1/5/10/50/60; 7) IO 扩展: 支持 8 个 PCIE 插槽, 支持 1 个 OCP 专用 PCIE 插槽; 8) 电源风扇: 配置 2 个热插拔电源, 功率 900W, 配置 4 个冗余双转子风扇, 风扇转速自动调节。 2. 服务指标 提供五年硬件保修服务; 提供投标商加盖公章的售后服务承诺函, 同时提供硬件厂家加盖公章的项目授权书和售后服务承诺函。
2	交换机	1. 性能指标 1) 硬件性能: 整机交换容量 1.36Tbps; 转发性能 207Mpps, 满足指标要求; 2) 单台端口: 48 个千兆电口, 4 个万兆 SFP+口, 满足指标要求; 3) 支持本地镜像 (SPAN) /远端镜像 (RSPAN) 镜像和 ERSPAN 等多个镜像观察端口, 可以对网络流量进行分析以采取相应管理维护措施; 4) MAC 地址表最大支持 32K 个 MAC 条目, IPv4 路由表容量最大 8192 个 FIBv4 条目, 整机最大 ARP 地址表 4000; 5) 安全特性: 用户分级管理和口令保护、支持 CPU 保护功能、支持防止 DOS、ARP 攻击功能、ICMP 防攻击、支持 IP、MAC、端口、VLAN ID 的组合绑定、支持端口隔离、端口安全、Sticky MAC、支持过载保护等, 可以保护交换机在各种环境下稳定工作。 6) 支持 VRRP、VRRP6、ECMP; 支持 RIP、RIPng、OSPF、OSPFv3、IS-IS、IS-ISv6、BGP、BGP4+等增强三层路由协议; 7) 支持 ERPS 以太环保护协议, 测试收敛时间≤19.89ms, 满足 50ms 要求; 8) 支持 WebMaster 解决方案, WebMaster 是内嵌式本地化管理平台, 支持拓扑自动发现, 拓扑、网元、设备告警等整网可视, 对交换机, AR, AP 统一管理, 无需额外部署网管平台。整网界面化操作, 可实现向导式业务创建、整网一键批量升级、设备免配置替换、网元自动认证纳管、误联线环路检测和自动破坏等能力, 一台设备即可实现整个园区网络可视、可管、可控。 2. 服务指标 提供五年硬件保修服务; 提供投标商加盖公章的售后服务承诺函, 同时提供硬件厂家加盖公章的项目授权书和售后服务承诺函。
3	信息安全数字孪生靶场平台	1. 实训平台基础系统 (管理员用户) 1) 用户与权限管理 ①系统具备用户与权限管理功能, 能够完成教师和学生账号的创建、批量导入及统一管理操作; ②系统具备账号增、删、改、查及密码重置功能; ③系统具备角色权限配置功能, 能够设置学生、教师、管理员等不同角色权限。

	2) 资源管理 ①系统具备教学资源管理功能，能够完成课程资料、实验手册、PPT、视频等资源的上传、更新与管理操作； ②系统具备资源分类管理功能。 3) 课程管理 ①系统具备课程管理功能，能够为教师账号授予课程创建权限； ②系统能够完成课程计划制订、课程公开或私有模式切换设置。 4) 系统监控与维护 ①系统具备平台运行状态监控功能，能够实时监测服务器性能、网络状况、用户并发数等关键指标； ②系统具备日志查看与分析功能，能够追溯用户操作记录。 5) 考试管理 ①系统具备考试管理功能，能够完成试卷模板创建、试卷公开或私有属性设置、题目分值设置、考试时间设置及考场安排操作； ②系统具备成绩统计与报表生成能力。 2. 实训学习子系统（学生端用户） 1) 课程学习功能 ①系统具备课程筛选与查询功能，能够依据关键字完成课程筛选操作； ②系统具备分类查看功能，能够清晰地展示课程名称、课程作者、课程简介、理论及实验数量等信息； ③系统具备实验指导书查阅功能，指导书内容能够包含实验目的、实验内容、实验步骤等。 2) 实验操作功能 ①系统具备实验环境操作功能，能够在Web虚拟桌面中完成文本双向复制粘贴操作及文件上传操作； ②系统具备多种虚拟化仿真模板调用功能，包括虚拟防火墙、路由器、交换机等； ③系统具备实验报告编辑功能，能够完成实验图片插入操作。 3) 学习进度与能力展示功能 ①系统具备学习进度查看功能，能够支持学生实时查看课程学习进度； ②系统能够通过雷达图等图形化方式展示学生学习情况。 4) 考试参与功能 ①系统具备考试参与管理功能，能够在试卷页面展示已答、未答、当前进度等状态； ②系统具备成绩授权查看功能。 3. 授课管理子系统（教师端用户） 1) 教学资源与课程管理子系统 ①系统具备课程体系管理功能，能够完成课程体系的配置与管理操作； ②系统具备岗位体系管理功能，能够完成职业岗位体系课程的设置与管理操作； ③系统具备实训课程管理功能，能够完成课程体系管理、课程管理及章节管理操作。 2) 网络安全资源库管理子系统 ①系统具备知识库管理功能，能够完成知识库资源的新增、删除、修改、查询操作，知识内容能够涵盖前沿技术、攻防技术、安全技术等多维度网络安全资源； ②系统具备漏洞库管理功能，能够完成漏洞库资源的新增、删除、修改、查询操作；漏洞信息内容能够包括漏洞风险评级、漏洞类型、漏洞介绍、漏洞利用方式、POC及受影响产品等信息。 3) 教学过程管理子系统 ①系统具备教学任务下发功能，能够支持教师将课程、班级、作业等学习任务
--	---

	分配至指定目标； ②系统具备考核管理功能，能够支持教师阶段性下发考核任务，并能够完成考核内容及方式设置； ③系统具备班级与人员管理功能，能够支持教师对班级及学生进行新增、删除、修改等操作。 4) 教学质量审核管理子系统 ①系统具备考核任务审核功能，能够完成学生考核或评估任务的审核操作； ②系统具备实验审核功能，能够完成学生实验结果的批改操作。 5) 网络安全仿真实训子系统 ①系统具备场景仿真管理功能，能够完成虚拟场景创建、管理及运行操作，并能够构建仿真网络环境、安全设备及靶机环境。 二、靶场管理系统 1) 资源监控管理子系统 ①系统具备资源统计功能，能够对系统中主机、网络、虚拟机等资源进行统计； ②系统具备资源存量监控功能，能够监控CPU存量、内存存量、存储量、虚拟机存量、容器存量及IP存量等资源信息。 2) 虚拟化环境管理子系统 ①系统具备虚拟机配置功能，能够完成虚拟机内存大小及CPU核数配置操作； ②系统具备虚拟机磁盘配置功能，能够完成磁盘容量及驱动模式配置操作。 3) 平台运维与权限管理子系统 ①系统具备后台任务管理功能，能够查看后台任务、执行进度及执行结果；系统具备后台任务筛选与查询功能； ②系统具备登录日志管理与操作日志管理功能； ③系统具备用户与角色权限管理功能，能够完成用户信息与角色权限配置操作。 4) 攻防裁决管理子系统 ①系统具备目标裁决功能，能够编辑评估裁定规则，能够执行判定操作，能够将随机Flag推送至靶标指定磁盘位置，并支持防作弊机制。 5) 靶场平台竞技任务管理子系统 ①系统具备比武演练任务配置功能，能够根据实训任务要求完成参赛队伍与配套比武演练资源的配置操作，配置内容包括竞赛名称、竞赛开始时间及持续时长、竞赛LOGO、竞赛模式、竞赛规则、竞赛场景（试卷）、参赛队伍等信息； ②系统具备比武演练任务常规管理功能，能够完成任务的新建、删除、编辑、查询、下发等操作。 6) 靶场平台试卷赛题管理子系统 ①系统具备赛题常规管理功能，能够完成赛题新增、删除、编辑、查询、预览等操作； ②系统具备赛题信息编辑功能，能够完成赛题名称、类型、题目入口、宿主机、场景等信息的编辑操作； ③系统具备宿主机管理功能，能够完成宿主机的上传、查询、编辑、删除等操作； ④系统具备试卷创建与配置功能，能够通过整合赛题完成试卷创建操作，试卷信息能够包含名称、描述及试卷内题目配置等内容。 7) 靶场平台人员队伍管理子系统 ①系统具备队伍信息常规管理功能，能够完成队伍信息新增、删除、编辑、详情查看、查询等操作；队伍信息能够包含队伍名称、描述、队伍logo、队伍成员列表等； ②系统具备队伍信息批量处理功能，能够完成队伍信息批量导入或批量删除操作； ③系统具备队伍数据导入导出功能，能够完成队伍信息导入、导出操作，并能够在界面提供导入模板下载功能，导入文件格式为Excel。
--	--

	8) 竞赛接入与环境隔离子系统 ①系统具备参赛指引与访问保障功能,能够使参赛队伍/选手依据“参赛手册”访问选手Web客户端及赛题环境; ②系统具备实体终端接入能力,能够支持参赛队伍/选手通过实体PC接入竞赛环境; ③系统具备队伍隔离功能,能够为每支队伍提供专属题目场景,实现队伍之间环境隔离。 9) 选手竞赛交互子系统 ①系统具备选手端竞赛信息展示功能,能够在选手Web客户端界面展示竞赛倒计时、公告信息、实时战况信息、竞赛轮次及时长信息、所在队伍得分及排名信息、所有参赛队伍积分榜单信息; ②系统具备赛题查看与提交功能,能够让参赛队伍/选手通过Web客户端查看题目并提交答案或Flag; ③系统具备动态Flag反作弊功能,能够实现题目Flag动态生成。 10) 赛事管理与公告发布子系统 ①系统具备公告管理功能,能够支持管理员完成公告新增、删除、编辑、查询、发布等操作; ②系统具备公告定向发布功能,能够支持管理员对所有队伍发布全员可见公告,或对指定队伍单独发布信息; ③系统具备赛题状态监控与维护功能,能够支持管理员对赛题开启/关闭状态进行监控,并能够完成赛题详情查看与编辑操作;编辑内容能够包括题目名称、题目内容描述、题目附件配置等。 11) 裁判判分与竞赛管理子系统 ①系统具备人工判分与调整功能,能够支持管理员对队伍/选手分数进行人工判定与调整,并能够在调整时记录操作原因及调整后的分数值; ②系统具备赛题批改与人工补交功能,能够支持裁判针对指定队伍/选手的指定题目进行批改,以应对答案正确但无法自行提交的情况; ③系统具备违规处置功能,能够支持管理员对正在参赛且违规的队伍/选手进行禁赛处置。 12) 竞赛环境运维管理子系统 ①系统具备竞赛环境运维管控功能,能够支持管理员对队伍/选手虚拟机环境进行开机、关机、创建快照、重启等操作。 13) 竞赛展示与数据分析子系统 ①系统具备大屏展示功能,能够展示比武演练基本信息、赛题攻克情况、赛队得分情况、排行榜、队伍得分详情、整体分数走势等信息; ②系统具备竞赛数据统计功能,能够统计答题记录、队伍得分记录、失分记录等信息。 14) 网络拓扑场景构建子系统 ①系统具备构建过程分步骤管理与独立保存功能,能够实现构建过程各步骤独立保存; ②系统具备可视化网络拓扑构建功能,能够支持管理员通过网络拓扑构建组件以拖拽方式构建多级网络场景,并能够同步编辑场景基本信息、附加信息等; ③系统具备多人协同场景构建功能,能够支持管理员多人协同构建场景并进行拼接组网,以满足大规模复杂网络构建需求。 15) 靶标资源配置管理子系统 ①系统具备靶标环境动态调整与场景分发功能,能够动态调整靶标环境并实现一键场景分发; ②系统具备场景编辑与资源关联功能,能够对靶标资源、拓扑资源进行调用与相互关联,并能够完成场景的增删改查操作; ③系统具备拓扑节点与靶机资源关联配置功能,能够在关联及模板制作环节将节点关联至靶机,并能够完成基本属性、网卡信息、服务信息等相关信息配置。
--	--

	16) 场景验证与运行管理子系统 ①系统能够在场景自测及保存环节对建立的场景进行单节点开机、联网开机、资源释放、设备重启等验证操作,并能够将验证通过的场景持久化保存至系统场景库; ②系统具备场景全生命周期管理功能,能够对系统现存场景完成查询、浏览、启动、复制、编辑、删除等操作。 17) 场景扩展与模板管理子系统 ①系统具备场景动态构建与增量式构建功能,能够实现对场景的动态扩展与增量调整; ②系统具备模板克隆与拓扑数据管理功能,能够完成模板克隆、拓扑数据管理与调用操作。 18) 实验场景管理子系统 ①系统支持管理员根据培训要求,自定义创建个性化的实验场景; ②系统支持对实验场景的虚拟机进行设置,以及对场景内不同区域的网络连通性进行设置; ③系统具备环境隔离功能,实验环境满足完全隔离,即学员在进行实验操作时场景之间不可进行数据交换。 19) 虚拟资源管理子系统 ①系统支持KVM虚拟机资源和容器类虚拟资源等虚拟资源类型,并支持不同类型虚拟资源的混合组网; ②系统具备虚拟机资源监控功能,能够监控虚拟机的内存使用率、CPU使用率、磁盘使用率、网络I/O等资源占用情况; ③系统具备虚拟机管理功能,支持创建、删除、查询、重启、关闭、克隆、远程桌面连接及接入、虚拟机网卡配置、虚拟机磁盘配置等操作。 20) 靶标资源管理子系统 ①系统支持为靶机设置Flag信息,包括Flag值、分类、附件、描述等其他信息; ②系统支持对系统中存储的靶机进行常规管理,包括查看、开机、关机、重启、克隆、编辑、删除等操作; ③管理员能够对靶标母版进行克隆和继承改造,形成新的靶标母版。 21) 资源库与镜像管理子系统 ①系统支持对靶标资源库进行常规管理,包括新增、查看、删除、编辑、检索等功能; ②系统支持对QCOW2 格式的虚拟机镜像及docker容器镜像进行管理; ③系统支持虚拟镜像常规管理,包括镜像上传、镜像删除、镜像查看等。 22) 镜像生成与终端管理子系统 ①系统支持虚拟机镜像生成,包括两种生成方式:一是基于系统已有虚拟机模板,快速生成新的虚拟机镜像;二是用户自定义镜像; ②系统支持查看指定账号下所注册的所有终端(操作机)的列表,并可对其进行开机、关机、重启、打开控制台、删除等操作; ③系统支持通过浏览器接入到终端内部,可对终端内部的软件、文件等进行操作,并保存终端状态。 23) 虚实结合设备管理子系统 ①系统具备网络安全设备的虚实结合功能,支持在场景中添加实体设备; ②系统支持添加、查看和删除实体设备信息; ③系统支持配置实体设备的基本信息,包括设备名称、设备型号、设备参数、IP地址、MAC地址、网关、操作系统、登录用户密码等信息。 24) 攻防工具资源管理子系统 ①系统内置攻防工具库,支持对工具进行常规管理操作,包括新增、删除、编辑、查询等; ②系统支持对工具内容、工具分类、工具简介等信息进行编辑; ③系统支持对工具进行分类管理,并能够自定义工具的种类。
--	---

	25) 任务管理子系统 ①系统具备理论试题、CTF任务、场景任务等单一类型或多种任务类型的综合管理功能，能够完成网络靶场挑战与任务的规划、设计与执行，并能够提供单人训练与团队训练模式； ②系统能够完成虚拟环境设计与配置，包括网络拓扑、虚拟机设置、靶标环境部署、应用程序和服务配置等； ③系统能够完成复杂环境布置，以实现多场景、多维度挑战设置，覆盖Web漏洞类、协议类、密码学及特定行业场景等。 三、系统资源包 1) 靶标资源： ①系统内置白板操作系统及应用服务靶标，包含操作系统、网站服务器组件、邮件服务器组件、数据库软件和数据库的连接工具等； ②系统内置公共漏洞靶标，包括但不限于文档类漏洞、浏览器类漏洞、数据库类漏洞、网络设备类漏洞、移动终端类漏洞、web类漏洞等； ③系统内置安全设备靶标，包括VPN、IPS、WAF、防火墙、交换机、IDS设备、安全审计等。采购人在使用过程中，不存在任何形式的隐性消费或二次收费。 2) 漏洞库资源： ①系统内置漏洞信息库，支持对POC、EXP管理； ②系统提供 1000 个高质量漏洞数据（包含漏洞验证代码，远程代码执行验证poc，本地代码执行验证poc，web漏洞代码验证poc，DDOS相关漏洞验证poc等）。 3) 知识库资源： ①系统内置 400 篇高质量信息安全及网络攻防相关知识文章，如Bypass绕过、内网渗透、渗透技巧、工具技巧、经验总结知识类方向，配合用户快速开展基础知识累积； ②系统内置 40 篇最佳实践领域与实战技战法，包含红队技战法（全域信息收集与攻击面测绘、高精度漏洞利用与权限获取、内网穿透与权限体系控制、社会工程学专项攻击和AI赋能的自动化攻击）和蓝队技战法（互联网暴露面收缩与加固、全流量与多维度威胁检测、自动化事件响应与溯源反制、反社会工程学与安全意识建设和AI赋能的新一代防御体系）。 4) 工具库资源： ①系统内置 100 个工具资源，覆盖Webshell管理工具、爆破工具、代理工具、代码审计工具、恶意行为系统检测工具、解密工具、漏洞检测工具、漏洞利用工具、漏洞扫描工具、密码破解工具、免杀工具、目录爆破工具、逆向破解工具、数据库管理工具、网络协议工具、信息搜集工具、资产探测工具、子域名搜集工具、字典生成工具等资源。采购人在使用过程中，不存在任何形式的隐性消费或二次收费。 5) 理论任务资源： ①系统提供理论任务 4000 个，覆盖云安全、密码学、工控安全、安全防护、安全运维、主机安全、法律法规、网络安全等网络安全理论知识，其中工控理论任务资源 200 个。 6) CTF竞赛任务资源： ①系统提供 100 道CTF题目，题目类型包含：Web、Crypto、misc、PWN和reverse等主要方向。 7) 可视化展示管理 ①系统支持按需展示实时攻防信息、成绩趋势、实时排行、能力标签、攻防日志、所得分数等信息，支持活动开始倒计时功能，支持成绩趋势查看要求以折线图方式展示得分趋势变化。 四、平台系统更新与故障响应服务 1) 故障响应服务 ①乙方承诺提供 5 年的平台系统运维与更新服务，并出具盖有乙方公章的承诺函；
--	--

		②乙方承诺在接到故障通知后 10 分钟内进行远程响应，技术人员通过电话、远程登录等方式初步判断故障原因；若无法远程解决，技术人员将在 2 小时内到达现场进行处置；由平台系统故障导致的核心业务完全中断，乙方承诺在 12 小时内解决，若无法按时解决，乙方提供备用机直至问题解决。 2) 平台系统更新 ①在服务期内，服务商提供每年 4 次的平台系统更新服务，包含安全更新、质量与性能更新、兼容性更新等。
4	网络安全基础资源包	1. 网络安全课程资源包 网络安全课程资源包（内含课程讲授视频、课程PPT、课程练习题、教学案例资料等课程资源）覆盖以下课程，总学时不低于 1000 课时，具体课程至少包括：（交付时至少包含如下课程的 80%，交付一年内如下课程需要 100%包含） 《信息安全导论》：48 课时 《应用密码学》：64 课时 《Web安全》：64 课时 《渗透测试技术》：48 课时 《内网渗透测试技术》：32 课时 《逆向工程》：64 课时 《电子数据取证技术应用》：48 课时 《网络安全编程》：48 课时 《运维开发与自动化》：64 课时 《编程基础与代码安全》：32 课时 《网络安全设备配置与管理》：32 课时 《网络安全攻防演练技术》：32 课时 《漏洞挖掘与代码审计技术》：64 课时 《Linux与网络运维》：64 课时 《Linux系统管理》：48 课时 《网络协议安全》：32 课时 《数据库基础与安全》：32 课时
		《Linux系统架构》：96 课时 《AI大模型与安全攻防》：32 课时 《应急响应实战》：32 课时 《工业控制系统与工业网络基础》：32 课时 《工控系统漏洞分析与安全防范》：32 课时 《数据安全治理》：32 课时 《零信任与新型网络安全架构》：32 课时 《网络安全攻防实践（CTF）》：64 课时 2. 网络安全实验资源包 实验资源包括 250 套活体漏洞配套实验，实验内容涵盖以下类型：SQL 注入、跨站脚本攻击、文件上传漏洞、文件包含漏洞、RCE 漏洞、逻辑漏洞、反序列化漏洞等，其中支持CVE编号的实验 150 套。（每年根据一线应用实际，对资源包进行扩展与更新 4 次。）
5	实网攻防资源包	1. 金融行业安全防护综合实验场景 1) 行业化网络环境仿真指标 ①实验场景按照金融行业典型网络环境部署，能够模拟金融科技企业业务架构； ②实验场景网络架构采用 4 级分域设计； ③实验场景划分DMZ区、生产区、办公区和子公司区等多种功能区域，并支持区域间网络隔离与访问控制配置功能。 2) 业务系统与漏洞风险仿真指标 ①在实验场景DMZ区构建Windows Server服务器及门户网站，同时设置了后台登录入口、设置弱口令、Shiro反序列化漏洞以及接口未授权访问漏洞；

	②实验场景生产区部署了多台服务器,认为内置了数据库弱口令与中间件漏洞等风险点,便于后续信息获取; ③子公司区域内的主机已部署安全防护机制,操作前须先利用免杀技术规避检测,绕过后方可执行后续任务。 3) 内网渗透与攻防路径训练指标 ①实验场景办公区部署了Windows 7/10/11 混合终端以及AD域来模拟员工使用的终端设备,并内置浏览器插件漏洞、弱口令终端、凭证泄露、漏洞提权、永恒之蓝等风险点; ②本实验场景中,攻击路径设计如下:首先从门户网站切入,利用Web漏洞获取初始访问权限,继而以该主机为跳板,尝试进入AD域,获得基础权限后深入内网测试环境,随后借助各类漏洞或弱点实现横向移动,最终通过办公终端渗透至子公司,达成对整个网络环境的完整控制; ③实验场景包括信息收集、漏洞利用、权限提升、横向渗透及持久化控制等能力的综合训练内容。 4) 验证评价与资源配套指标 ①实验场景包括多级Flag校验机制,用于验证渗透链路的完整性和攻击效果。场景内置Flag数量为10个,分布在各个功能域; ②场景配套内容有场景描述、Flag获取任务描述、网络拓扑、演示视频、标准答案及复现报告等资料。 2. 政府系统安全防护综合实验场景 1) 行业化网络环境仿真指标 ①实验场景包括政府门户网站及其配套网络环境的仿真; ②实验场景网络架构分域共分为4级; ③实验场景包括DMZ区、生产区、办公区、核心区等多种功能区域,并支持区域间网络隔离与访问控制配置。 2) 业务系统与漏洞风险仿真指标 ①DMZ区部署的政府门户网站中,内置了后台弱口令与文件上传GetShell漏洞,且管理入口未加隐藏,直接暴露; ②生产区通过部署生产服务器来模拟正常的生产环境,人为设置了Fastjson反序列化、RCE漏洞、容器环境逃逸等漏洞; ③核心区部署运维终端来模拟政府办公环境,内置密码保存、RDP登录凭证泄露等风险; ④办公区部署了SQLServer数据库、域控服务器、邮件服务器用于存储敏感信息,存在数据库弱口令、zerologon域控漏洞、域内hash横向移动风险,便于进一步深入利用。 3) 内网渗透与攻防路径训练指标 ①实验场景以门户网站Web漏洞为起点,通过生产服务器的漏洞进一步深入利用,最终尝试解密RDP凭证侵入办公区后跳板进入核心区,获取重要数据; ②实验场景包括了信息收集、漏洞利用、权限提升、横向移动及持续控制等攻防能力的训练内容。 4) 验证评价与资源配套指标 ①实验场景包括多级Flag校验机制,用于验证渗透链路的完整性和攻击效果。场景内置Flag数量为8个,分布在各个功能域; ②场景配套内容有场景描述、Flag获取任务描述、网络拓扑、演示视频、标准答案及复现报告等资料。 3. 教育行业安全防护综合实验场景 1) 行业化网络环境仿真指标 ①实验场景包括教育机构典型网络环境的整体仿真; ②实验场景网络架构分域共分为4级; ③实验场景包括DMZ区、生产区、分校办公区、分校生产区等多种功能区域,并支持区域间网络隔离与访问控制配置。
--	--

	2) 业务系统与漏洞风险仿真指标 ①DMZ区部署了校园门户系统, 设置了文件上传漏洞及后台弱口令漏洞; ②生产区设置了web业务系统, 预置RCE漏洞及容器逃逸环境; ③生产区设置了Windows7/10/11 混合终端, OA系统来模拟学校人员使用的电脑, 存在文件上传GetShell漏洞、浏览器凭据泄露及SMB弱口令风险; ④分校区办公区设置了弱口令及SMB溢出漏洞, 存在最终靶标。 3) 内网渗透与攻防路径训练指标 ①本实验场景设计了一条完整攻击路径: 首先利用校园门户后台的弱口令突破外围防线, 进而通过容器逃逸技术获取内网访问权限, 随后, 借助域内账户的弱口令缺陷, 横向移动至核心生产区域, 持续渗透扩张, 最终攻入分校区的业务系统, 实现对整体网络环境的完全控制。 ②实验场景包括了信息收集、漏洞利用、权限提升、横向移动及持续控制等攻防能力的训练内容。 4) 验证评价与资源配套指标 ①实验场景包括多级Flag校验机制, 用于验证渗透链路的完整性和攻击效果。场景内置Flag数量为8个, 分布在各功能域; ②场景配套内容有场景描述、Flag获取任务描述、网络拓扑、演示视频、标准答案及复现报告等资料。 4. 医疗行业安全防护综合实验场景 1) 行业化网络环境仿真指标 ①实验场景包括医院信息系统及基础网络环境的仿真; ②实验场景网络架构分域共分为4级; ③实验场景包括互联网访问域、业务服务域、办公管理域、核心数据控制域等多种功能区域, 并支持区域间网络隔离与访问控制配置。 2) 业务系统与漏洞风险仿真指标 ①互联网访问区域向外部开放了医院门户网站与远程预约平台, 提供患者信息交互入口, 集成了敏感信息泄露、文件上传及JWT鉴权等典型web漏洞; ②业务区域内部署了内部OA办公系统及内网测试服务环境, 并支持基本的业务操作逻辑; ③办公区主要模拟企业内部员工使用的办公终端, 这些终端分布在独立子网中, 与生产区通过部分主机跨网卡联通, 用于还原内网深度渗透路径; ④核心数据区配置了集成永恒之蓝漏洞的Windows域控制器, 参训人员的最终目标是获取DC域控权限及核心数据。 3) 内网渗透与攻防路径训练指标 ①实验场景设置了一条从门户网站进入, 结合Web漏洞拿下首个入口, 进入OA系统获取基础权限后深入内网测试环境, 利用系统漏洞与中间件弱点实现横向移动, 最终通过办公终端渗透到域控系统, 实现完整网络控制的完整攻击路径; ②实验场景包括了信息搜集、漏洞利用、权限提升、横向移动及持续控制等攻防能力的训练内容。 4) 验证评价与资源配套指标 ①实验场景包括多级Flag校验机制, 用于验证渗透链路的完整性和攻击效果。场景内置Flag数量为8个, 分布在各功能域; ②场景配套提供的内容包括场景描述、Flag获取任务描述、网络拓扑、演示视频、标准答案及复现报告等资料。 5. 电信行业安全防护综合实验场景 1) 行业化网络环境仿真指标 ①实验场景包括电信运营商典型网络环境的整体仿真; ②实验场景网络架构分域共有4级; ③实验场景包括DMZ区、生产区、办公区、子公司区等多种功能区域, 并支持区域间网络隔离与访问控制配置。 2) 业务系统与漏洞风险仿真指标
--	--

	①DMZ区部署短信服务入口，存在ActiveMQ默认口令、后台任意文件上传等多个漏洞； ②生产区部署了nacos系统，存在默认口令漏洞； ③办公区部署了AD域及证书服务环境，其中存在ADCS ESC1 漏洞以及SSH私钥泄露问题。攻击者可利用上述漏洞获取服务器及域管理员权限，进而引发内网横向移动及域控沦陷的安全风险； ④子公司区部署了应用服务器以及财务数据库存储了公司的要数据，存在敏感信息泄露风险。 3) 内网渗透与攻防路径训练指标 ①本实验场景的攻击路径设计如下：以短信服务入口的文件上传漏洞为初始突破点，获取生产区主机控制权限，随后利用生产区已存在的漏洞横向进入AD域环境，借助ADCS的ESC1 漏洞获取域管理员权限；继而通过SSH私钥泄露问题获取子公司服务器控制权限，最终成功访问财务数据库，实现对整体网络环境的全面控制。 ②实验场景包括对信息搜集、漏洞利用、权限提升、横向移动及持续控制等攻防能力的训练内容。 4) 验证评价与资源配套指标 ①实验场景包括多级Flag校验机制，用于验证渗透链路的完整性和攻击效果。场景内置Flag数量为8个，分布在各功能域； ②场景配套提供内容为场景描述、Flag获取任务描述、网络拓扑、演示视频、标准答案及复现报告等资料。 6. 工业控制行业安全防护综合实验场景 1) 行业化网络环境仿真指标 ①实验场景包括工业控制典型网络环境的整体仿真； ②实验场景网络架构分域共有4级； ③实验场景包括互联网访问区、DMZ区、生产控制区、办公区等多种功能区域，并支持区域间网络隔离与访问控制配置。 2) 业务系统与漏洞风险仿真指标 ①互联网访问区设置了web访问入口，存在弱口令及后台任意文件上传等多个漏洞； ②DMZ区放置了存在Redis未授权访问漏洞的场景数据库； ③生产控制区部署了域控环境和Tomcat系统，存在弱口令、文件上传漏洞和Everything未授权访问漏洞，可通过域控主机进行横向移动； ④生产控制区放置了PLC程序图纸，学生可通过程序逆向解密获取目标flag； ⑤办公区模拟了存在黄金票据漏洞的企业内部用户的办公终端。 3) 内网渗透与攻防路径训练指标 ①实验场景的攻击路径设计如下：首先从Web访问区入手，获取DMZ区数据库机器的控制权；继而利用生产控制区Tomcat系统的相关漏洞，获取主机权限并进一步攻入域环境；在域内通过信息收集，借助哈希传递技术实现横向移动；最后利用黄金票据获取办公区机器的最终权限，实现对整体网络环境的全面控制。 ②实验场景包括了信息搜集、漏洞利用、权限提升、横向移动及持续控制等攻防能力的训练内容。 4) 验证评价与资源配套指标 ①实验场景包括多级Flag校验机制，用于验证渗透链路的完整性和攻击效果。场景内置Flag数量为7个，分布在各功能域； ②场景配套内容有场景描述、Flag获取任务描述、网络拓扑、演示视频、标准答案及复现报告等资料。
--	--

6	工控 能源 安全 场景 演练 资源 包	1. 电力领域工控安全综合实验场景 1) 业务场景仿真指标 ①本场景以某工业园区 10kV 配电站房为蓝本，按配电自动化业务流程建模。站房内设 10kV I 段母线及 901—904 四回馈线，配变#1 (1000kVA)、配变#2 (800kVA) 及 4×50kvar 无功补偿电容器组。场景复现业务链路：遥测——由配变监测终端 (TTU) 采集三相电压、电流、有功功率及功率因数，周期上送主站；遥信——采集 901—904 断路器分合位置、弹簧储能、事故总等状态信号；遥控——主站可对断路器执行分/合闸远程操作并收到执行回令；遥调——主站按电压越限策略对无功补偿电容器组执行自动投切。下图给出了站房内“信息采集—传输处理—决策控制—执行反馈”的完整“四遥”业务链路。 ②实验场景运行于 10kV 配电网 SCADA 系统远程监测与控制仿真环境之上：管理层部署 FreeSCADA 配电自动化主站 (192.168.10.5)，通过工业以太网 (VLAN10) 经工控防火墙接入安全接入区的边缘控制网关 (Modbus TCP, 端口 502)；网关完成 Modbus TCP 与 Modbus RTU 协议转换后，经 RS-485 总线 (9600bps, 8N1) 下联现场设备层的配变监测终端 TTU、断路器模拟器与馈线终端 FTU；同时保留 4G/5G 无线公网接入通道，模拟配电终端异构通信方式。主站通过安全 I 区边界的纵向加密认证装置 (SM2/SM3/SM4 国密算法) 接入调度数据网；I 区数据经横向单向隔离装置单向摆渡至安全 II 区发布。全场景在虚拟化平台上 1:1 仿真运行，在仿真环境中即可完成远程监测与控制全过程操作。 ③场景对配电自动化核心业务功能逐项仿真：①配变电压监测——TTU 输入寄存器 30001—30003 实时存放 A/B/C 相电压 (分辨率 0.1V)，主站以 2s 周期轮询刷新；②线路电流采集——寄存器 30004—30006 存放三相线路电流，配合 30007 有功功率、30008 功率因数形成完整遥测量；③故障跳闸控制——主站保护逻辑或人工遥控向断路器模拟器下发跳闸指令 (Modbus 功能码 0x05 写线圈)，断路器执行分闸并经离散输入 10001—10008 反馈分/合位置与 SOE 事件；④无功补偿投切——主站按电压越限 (40001 过压定值/40002 欠压定值) 自动投切电容器组，构成遥调业务闭环。 ④场景内置完整的非法入侵攻击路径：攻击者位于管理信息区 (渗透测试终端，Kali 192.168.50.66)，利用边界防火墙策略缺陷 (如放行的 RDP 3389/SNMP 161 端口) 突破管理网与生产网边界，渗透至安全 I 区工程师站，继而通过默认凭据或组态软件漏洞登录配电自动化主站 (FreeSCADA 服务器)，获得监控画面的完整操作权限。入侵过程的每一步均在靶场闭环环境内进行，与外网物理隔离。 ⑤场景支持两类典型电力攻击的仿真演练：(1) 监测数据篡改——攻击者在渗透至生产网后，向 TTU 保持寄存器 40001 写入篡改值 (如将过压定值由 2200 改为 2500 触发误告警)，或在 Modbus TCP 通信路径上实施中间人篡改，使主站收到伪造遥测数据；(2) 控制指令伪造——攻击者利用 Modbus 协议缺乏认证的固有缺陷，直接向 RS-485 总线上的断路器模拟器 (从站地址 0x02) 伪造跳闸/合闸指令 (功能码 0x05 写线圈 0x0001—0x0004)，造成断路器误分/误合，模拟实际电网中的误操作事故。攻击效果可通过主站监控画面与断路器状态反馈实时观察。 2) 配电自动化系统架构指标 ①实验场景按“管理层—控制层—现场设备层”三级架构模型设计：管理层由工业控制主机 (FreeSCADA 主站)、工程师站、历史数据服务器经工业交换机汇聚，运行配电监控与数据管理业务；控制层由工控防火墙与边缘控制网关构成，承担安全隔离与 Modbus TCP/RTU 协议转换、数据转发职能；现场设备层由配变监测终端 TTU、断路器模拟器、馈线终端 FTU 经 RS-485 总线 (Modbus RTU) 接入。在该三级简化架构之上，场景进一步叠加了安全 I 区/安全接入区/安全 II 区/管理信息区的四区安全分区设计，形成“三级业务架构+四区安全架构”的复合模型。 ②管理层部署工业控制主机 1 台 (配电自动化主站，192.168.10.5)，运行 Fr
---	---------------------------------------	--

eeSCADA监控组态软件。主机提供 10kV 一次系统单线图监控画面：左侧为站房一次接线实时图（断路器分合位置着色显示、配变运行参数随动刷新），右侧为遥测量表、遥信量表、遥控/遥调操作面板与实时告警栏，底部状态栏显示当前用户、前置机与通信通道状态。全部数据展示与遥控/遥调指令下发均经该主机完成，操作留痕可审计。

③控制层设置 ICG-5200 边缘控制网关（上联 192.168.20.10，下联 192.168.30.1）。网关以太网侧运行 Modbus TCP Server（端口 502）响应主站轮询；串口侧 COM1 以 RS-485（9600bps，8N1，Modbus RTU Master）轮询现场设备；内置 TCP↔RTU 从站映射表（CH1→TTU 从站 0x01、CH2→断路器从站 0x02、CH3→FTU 从站 0x03），实现双向协议转换与数据转发；同时集成 4G/5G 无线拨号模块，模拟配电终端无线公网接入。

④现场设备层部署 TTU-3000 配变监测终端模拟器（192.168.30.10，Modbus RTU 从站地址 0x01），基于 OpenPLC Runtime 构建，程序符合 IEC 61131-3 标准。终端以输入寄存器 30001—30008 模拟三相电压、电流、有功功率、功率因数采集（遥测），以离散输入 10001—10008 模拟开关位置与告警信号（遥信），以保持寄存器 40001—40004 存放过压/欠压/过流保护定值，兼容标准 Modbus RTU 协议（9600bps，8N1）。

⑤现场设备层部署 BRK-400 断路器模拟器（192.168.30.11，Modbus RTU 从站地址 0x02），仿真 901—904 四台馈线断路器。模拟器以线圈 0x0001—0x0004 接收主站遥控分/合闸指令（功能码 0x05 写单线圈/0x0F 写多线圈），执行分合闸动作后以离散输入反馈分位/合位遥信及 SOE 事件（分辨率 2ms），并记录完整的控制指令接收日志（报文原文可查），真实复现“指令接收—机构动作—状态反馈”的遥控业务闭环。

3) 安全分区与纵深防御指标

①场景在管理层（安全 I 区）与控制层（安全接入区）边界部署 ICFW-900 工控防火墙，开启基于 Modbus 协议的工业白名单防护；内置 Modbus TCP 深度包检测（DPI）引擎，按“源地址—目的地址—功能码—寄存器范围”四元组配置访问规则，仅放行 0x01/0x02/0x03/0x04（读）、0x05/0x06/0x0F/0x10（写）等业务必需功能码，其余功能码（如 0x08 诊断码）默认拒绝并告警。防火墙同时划分 192.168.10.0/24 与 192.168.20.0/24 两个隔离网段，实现管理层与控制层的边界隔离。

②场景网络互联关系为：管理层与控制层之间采用工业以太网互联，按 VLAN 划分隔离（VLAN10——管理层主站区 192.168.10.0/24，VLAN20——控制层接入区 192.168.20.0/24），工控防火墙部署于两网段边界，执行跨网段访问控制；控制层与现场设备层之间采用 RS-485 串行总线连接（Modbus RTU，9600bps，8N1），边缘控制网关完成以太网侧 Modbus TCP 与串口侧 Modbus RTU 的双向协议转换，同时保留 4G/5G 无线公网链路模拟配电终端异构接入。工控防火墙将生产网络划分为 192.168.10.0/24 与 192.168.20.0/24 两个隔离网段，与拓扑中 VLAN10/VLAN20 划分一一对应。

③配电自动化主站系统按网络安全等级保护 2.0 定级为第三级（依据 GB/T 22039-2019 及国能安全〔2015〕36 号文要求），场景内置了对应的技术措施并在课程中逐项演练：访问控制——主站账户三权分立、最小权限分配、登录失败锁定与操作员口令策略；入侵防范——工程师站/主站部署主机白名单与 EDR，与边界工控防火墙 DPI 检测联动；安全审计——操作日志、遥控操作记录、通信审计日志留存 6 个月，支持 SOE 事件追溯；数据完整性校验——遥测报文 CRC+HMAC 校验、组态文件哈希基线比对、SOE 记录防篡改。

④场景严格采用“安全分区+纵深防御”架构，划分为四个逻辑区域：安全 I 区（生产控制区，192.168.10.0/24）部署配电自动化主站、工程师站、历史数据服务器；安全接入区（192.168.20.0/24）部署边缘控制网关与 4G/5G 无线模块；安全 II 区（非控制生产区，192.168.40.0/24）部署 Web 发布服务器与故障录波工作站；管理信息区（192.168.50.0/24）部署办公终端与 EMS/ERP

	服务器。区域边界由专用安全设备隔离：I区与接入区之间为工控防火墙，I区与调度数据网之间为纵向加密认证装置，I区与II区之间为横向单向隔离装置，管理信息区与生产大区之间为边界防火墙。场景内置6个核心靶标：靶标1 配电自动化主站（FreeSCADA服务器）、靶标2 边缘控制网关、靶标3 工控防火墙、靶标4 配变监测终端TTU、靶标5 纵向加密认证装置、靶标6 横向单向隔离装置，各靶标均内置独立漏洞与攻防科目。 ⑤依据《电力监控系统安全防护规定》（国家发改委14号令，2024年修订版）对配电网异构通信的新增要求，场景在安全I区与现场设备层之间设立安全接入区（192.168.20.0/24，VLAN20），作为无线公网、光纤专网等异构通信方式接入内外网之间的统一缓冲地带：4G/5G无线模块与光纤专网链路统一汇聚至安全接入区，经边缘控制网关进行协议转换与接入控制后，方可经工控防火墙进入安全I区，杜绝外部通信链路直连生产控制区。 4) 工业控制安全攻防训练指标 ①场景攻击面覆盖从网络边界到物理设备的完整攻击链，内置8个攻防演练科目（编号与下图红色攻击路径一一对应）：a. 边界突破与横向渗透——从管理信息区钓鱼/弱口令突破边界防火墙，横向渗透至安全I区；b. 纵向加密认证绕过——在调度数据网链路实施证书伪造与中间人攻击；c. Modbus协议攻击与数据篡改——构造异常功能码、篡改寄存器定值；d. 配电终端恶意控制——伪造分合闸指令造成断路器误动；e. 勒索病毒——模拟勒索载荷加密组态与工程文件并演练应急响应；f. SCADA服务器权限获取与持久化——提权、植入后门、痕迹清理；g. DoS/DDoS攻击——对Modbus 502端口与协议转换进程实施泛洪与畸形报文攻击；h. APT全链路攻击——按kill chain完整模拟“初始入侵—立足—提权—侦察—横向—目标达成”，并以虚假站端状态上报阻碍调度协调。每个科目均可在靶场内闭环演练并支持红蓝角色互换。 ②靶标1（配电自动化主站）内置上述全部训练内容：a. 默认凭据——主站运行系统保留出厂默认账户admin/admin123，可使用弱口令字典爆破登录，登录成功即获得含遥控/遥调权限的完整监控画面操作权；b. XAML组态文件缺乏完整性校验——主站组态画面文件（station_main.xaml）加载时无数字签名与哈希校验，可通过工程师站共享目录直接篡改遥测绑定地址，重启后画面显示伪造数据；c. 异常Modbus报文缺乏输入验证——主站前置机对诊断功能码（0x08）、超长度报文、越界寄存器写请求不做输入验证，可通过Wireshark抓包对比正常轮询与攻击报文，观察从站异常响应与定值被篡改的全过程。 ③靶标2（边缘控制网关）内置四类训练内容：a. Telnet/SSH弱口令——网关开放23/22端口，出厂账户root/admin123未强制修改，可爆破登录获得设备shell（BusyBox环境），进而读取/etc/shadow并离线破解；b. 固件未签名验证——网关固件升级接口不校验数字签名，可刷入植入后门的篡改固件实现持久化控制；c. 协议转换层缺乏报文合法性校验——modbus_gw转换进程对报文长度、功能码范围不做校验，获得网关权限后可篡改TCP↔RTU映射表劫持数据流；d. 无线接入面缺乏设备认证——4G APN接入无设备证书认证，任意获知APN参数的模块均可入网，可演练非法接入与链路监听。 ④靶标3（工控防火墙）内置三类训练内容：a. 验证防火墙规则有效性——对照业务需求审查“源—目的—功能码—寄存器范围”规则表，使用Modbus探测脚本逐条验证规则是否按预期放行/拒绝；b. 绕过DPI检测的报文构造——通过TCP分片重组、未覆盖功能码（0x08 诊断码）、功能码混淆等构造技术绕过深度包检测，观察攻击报文穿透防火墙直达从站；c. 规则配置疏漏导致的穿透——规则表中对工程师站写操作未限制写入值域、对诊断功能码未做覆盖等疏漏可被利用，通过对比防火墙日志（无告警）与从站实际状态（定值已被改写），理解“配置即安全”的防御要点并修复规则。 ⑤靶标4（配变监测终端TTU）内置三类训练内容：a. 缺乏写保护——终端保持寄存器写保护开关默认关闭、写操作无访问口令，可直接以功能码0x06将过压保护定值40001由2200篡改为2500，触发保护误动告警；b. 固件升级接
--	---

口缺乏认证——终端Web固件升级接口(/update)无需登录、不校验固件签名,可直接POST刷入篡改固件;c.支持广播报文——终端响应从站地址 0x00 的广播请求,以广播Report Slave ID (0x11)即可一键枚举RS-485 总线上全部从站设备指纹(型号+固件版本),为后续定向攻击提供情报。

⑥靶标 5 (纵向加密认证装置)内置三类训练内容:a.证书伪造攻击——装置信任链中残留自签名测试证书(PD-GATE-TEST),可伪造调度端证书(CN=PD-DISP-01)通过证书校验;b.加密隧道中间人攻击——在调度数据网链路实施ARP欺骗立于隧道中间位置,截获SM2 密钥协商报文,并利用装置未校验时间戳的缺陷重放历史认证报文通过认证;c.策略配置绕过——利用运维遗留的“紧急旁路策略”与未启用的CRL吊销列表,以明文通道直连I区主站 502 端口,使SM4 隧道加密形同虚设。演练从“部署了加密”与“形成了有效加密保护”的差距出发,强化对纵向认证机制的深度理解。

⑦靶标 6 (横向单向隔离装置)内置三类训练内容:a.验证隔离强度——由安全II区向安全I区发起反向端口扫描与会话建立尝试,验证物理单向隔离“无TCP会话、无回程路由”的强度;b.尝试反向渗透路径——尝试源端口伪装、摆渡协议夹带、管理口绕行等多种反向渗透思路,均无法建立反向通道,从对抗中理解物理单向的技术原理;c.利用摆渡数据残留的攻击面——装置摆渡缓存目录未做安全清除,残留历史同步数据备份(hist_sync_*.db.bak),可从残留数据中还原I区完整点表与运行数据,认识摆渡数据全生命周期管理的重要性。

5) 实训教学与资源配套指标

①电力场景实训内容共计 40 学时(20 个实训单元×2 学时),覆盖“基础认知—协议基础—流量分析—攻防实战—防御配置—综合考核”六个模块,其中 8 个攻防科目与场景攻击链一一对应。每个实训单元均配套按课程内容的演示视频文件(MP4),视频与场景靶标、实训手册同步使用。

②电力场景配套教学资料:a.场景描述——《电力领域工控安全综合实验场景说明书》,含业务背景、四区架构、6 个靶标的设备清单、网段规划、寄存器/点表定义;b.Flag获取任务描述——8 个攻防科目各设独立Flag任务(任务编号DL01—DL08),每份任务书含任务目标、前置知识、操作步骤、注意事项、考核标准五段式内容,Flag值埋设于靶标文件系统、寄存器与日志中;c.网络拓扑——四区架构拓扑图、三级架构图、攻击链拓扑图全套(见本文件各章节附图,源文件随包交付);d.演示视频——20 个按课程改名的MP4 演示视频(见表 5-1 及图 5-1),覆盖全部实训单元与 8 个攻防科目操作全过程;e.标准答案——《电力场景Flag标准答案册》,含每个Flag的获取路径、关键命令与预期回显;f.复现报告——《电力场景综合复现报告》模板及样例,含场景描述、攻击时间线还原、受影响资产清单、防御改进建议四个固定章节,供学生考核与教师评阅使用。上述资料均以电子文件形式随场景资源包整体交付。

2. 煤炭领域工控安全综合实验场景

1) 工业控制业务仿真指标

①实验场景以煤矿井下主运输煤系统为原型,基于胶带输送机(带式输送机)启停控制与故障监测仿真环境构建。场景完整复现“井底煤仓—给煤机—主运胶带机—转载胶带”的运煤工艺流程,由井下PLC控制器(192.168.20.10)作为控制核心,地面控制层集控系统通过MRP工业环网与井下PLC通信,实现对胶带运输机的远程启停控制与运行状态、故障信号的实时监测。全部仿真在虚拟靶场平台内闭环运行,与生产网络物理隔离。

②场景对胶带输送机核心业务功能逐项仿真:a.启停操作——调度操作站/地面集控服务器下发启机、停机、急停指令,经MRP环网到达井下PLC,PLC控制主运胶带机启停并反馈运行状态;b.速度监测——速度传感器模拟器(从站 0x03)实时采集带速(正常 2.42m/s),带速低于设定值 70%持续 5 秒触发打滑报警;c.超温报警——温度传感器模拟器(从站 0x04)监测驱动滚筒温度,达到 80℃阈值即触发超温报警、联动声光报警器并连锁停机;d.跑偏报警——

	一跑偏传感器模拟器（从站 0x05）检测胶带偏移量，一级跑偏（偏移>5cm）报警提示、二级跑偏（偏移>10cm）联锁停机。 ③场景内置两类典型攻击的仿真演练：a. 非法控制运输机运行——攻击者经办公网络渗透至地面控制层，利用集控服务器RDP弱口令（administrator/Coal@123）非法登录后，以集控服务器为跳板向井下PLC伪造远程启机/停机/急停控制指令（EtherNet/IP CIP写服务），在无调度员操作、无操作票记录的情况下远程操控运输机运行状态；b. 屏蔽故障报警——攻击者通过篡改传感器上送寄存器值（将超温 84.6℃改写为 76.2℃）、丢弃报警上送报文、旁路PLC保护联锁逻辑等方式，使超温/跑偏故障“隐身”，集控画面无报警、声光报警器不动作、联锁停机不执行，设备带病运行。攻击过程与防护效果可在集控画面“屏蔽前后对比”中直观呈现。 2) 工业控制架构设计指标 ①实验场景按“地面控制层—井下控制层—现场设备层”三级架构模型设计：地面控制层由工业控制主机、地面集控服务器、调度操作站、视频监控联动主机经地面汇聚交换机组成，承担远程监控、集控管理与调度操作职能；井下控制层由井下PLC控制器与六台工业环网交换机（MRP介质冗余环网）组成，承担控制逻辑运算与井上下数据可靠传输职能；现场设备层由配变监测终端、断路器模拟器、速度/温度/跑偏传感器模拟器、声光报警器模拟器经RS-485 现场总线（Modbus RTU）接入井下PLC。在三级架构基础上，场景还在地面控制层与井下控制层边界部署工控防火墙，形成“三级业务架构+边界安全防护”的复合设计。 3) 地面控制层设备部署指标 ①地面控制层部署工业控制主机 1 台（192.168.10.10），安装煤矿胶带运输集控组态软件。主机提供主运输煤工艺流程监控画面：左侧为工艺流程实时图（煤仓存量、给煤机、主运胶带运行方向与托辊/滚筒状态、传感器数值随动刷新），右侧为运行参数表（带速、运量、滚筒温度、电机电流/电压、班产量）、设备状态汇总表、调度操作面板（启动/停止/急停/报警确认）与实时报警栏，底部状态栏显示当前用户、集控服务器与井下链路状态。运输机状态远程监控与启停操作均经该主机完成，操作留痕可审计。 ②地面控制层部署两类集控设备：a. 地面集控服务器（192.168.10.20）——集成煤炭产量计量（瞬时运量 486t/h、本班累计产量 2417t、班报自动生成）、设备运行状态汇总（主运/转载/备用胶带机、给煤机、各保护传感器投退状态集中展示）、视频监控联动（报警事件自动弹出对应摄像头画面，如 2 号转载点烟雾报警联动CAM-07）等功能；b. 调度操作站（192.168.10.30）——提供调度员人机操作界面，支持皮带机启停操作（启动/停止/急停按钮）、故障报警确认、运行参数调整（带速上限等定值修改），所有操作按调度权限控制并生成操作记录。两类设备的界面功能均在集控界面右侧“设备状态汇总”“调度操作”“实时报警（视频联动）”三个面板中完整体现。 4) 井下控制层设备部署指标 ①井下控制层设置井下PLC控制器 1 台（192.168.20.10，基于OpenPLC Runtime构建，程序符合IEC 61131-3 标准），作为胶带运输机控制核心。PLC以 50ms扫描周期循环执行控制程序（belt_main.st结构化文本+protection_chain 梯形图）：通过Modbus RTU总线采集速度、温度、跑偏传感器数据，执行保护联锁逻辑（超温≥80℃、二级跑偏、急停任一触发即停机并联动声光报警），通过EtherNet/IP与地面控制层通信，接收启停控制指令并上送设备运行状态。支持程序上传下载、在线变量监视与强制表操作。 ②井下控制层设置六台 IES-6300 工业环网交换机（SW2—SW7）组成MRP介质冗余环网：SW2 作为环网管理器（Ring Manager），SW3—SW7 作为环网客户端，环网采用千兆光纤互联；当环网任一单点链路故障时，管理器在 50ms内重构环路，保障地面控制层与井下PLC之间通信不中断（30 天运行记录中环网收敛 1 次，为计划内光纤插拔测试）。SW5 下接井下PLC，SW7 经工控防火墙上联地
--	--

	面控制层，实现地面与井下数据可靠传输。 5) 现场设备层设备部署指标 ①现场设备层部署配变监测终端模拟器 (192.168.30.10, Modbus RTU从站地址 0x01)，模拟胶带输送机驱动电机供电回路的电压、电流数据采集：输入寄存器存放三相电压 (6.08kV侧)、电机电流 (286.5A) 等电量参数，经RS-485总线 (9600bps, 8N1) 兼容标准Modbus RTU协议上送井下PLC，为电机运行状态监测与过流保护提供数据基础。 ②现场设备层部署断路器模拟器 (192.168.30.11, Modbus RTU从站地址 0x02)，模拟胶带输送机供电回路断路器：以线圈地址接收井下PLC下发的跳闸/合闸指令 (功能码 0x05)，执行分合闸动作后以离散输入反馈分位/合位遥信及事件记录，真实复现“跳闸指令接收—机构动作—运行状态反馈”的控制闭环。 ③现场设备层部署速度传感器模拟器SP-300 (192.168.30.12, 从站 0x03, 量程 0-4.0m/s) 与温度传感器模拟器TP-450 (192.168.30.13, 从站 0x04, 量程 0-150℃)：速度传感器以寄存器 30011 实时输出胶带带速，支撑打滑检测 (低于设定值 70%持续 5 秒报警)；温度传感器以寄存器 30013 实时输出驱动滚筒温度，达到 80℃阈值触发超温报警并连锁停机。两类传感器的实时数值、寄存器映射与总线通信过程见图运行界面。 ④现场设备层部署声光报警器模拟器AL-900 (192.168.30.15, Modbus RTU从站地址 0x06)：以控制线圈 0x0011 接收井下PLC下发的故障报警指令 (超温、二级跑偏、急停联动触发)，执行声光报警动作，并以离散输入 10031 反馈报警器动作状态，构成“故障检测—报警下发—动作执行—状态反馈”的完整报警联动链路。同时现场层还部署跑偏传感器模拟器DV-120 (从站 0x05)，提供一级报警/二级停机两级跑偏保护信号。 6) 工业通信与网络安全防护指标 ①场景在地面控制层 (管理层) 与井下控制层 (控制层) 边界部署工控防火墙 (192.168.10.1/20.1)，开启工业协议白名单防护：内置EtherNet/IP与Modbus TCP深度包检测 (DPI) 引擎，仅放行地面集控服务器、调度操作站至井下PLC的CIP读写服务与Modbus业务功能码，其余协议与端口默认拒绝并告警；防火墙划分 192.168.10.0/24 与 192.168.20.0/24 两个网段，实现管理层与控制层的边界隔离。下图为防护部署拓扑 (绿色高亮框为防火墙部署位置)。 ②场景地面控制层与井下控制层通过MRP工业环网互联：六台工业环网交换机 (SW2—SW7) 组成介质冗余环，SW2 为环网管理器，单点链路故障时 50ms内自愈，保障井上下通信连续性。井下PLC与现场设备通过RS-485 现场总线 (Modbus RTU, 9600bps, 8N1) 连接，六类现场设备 (从站 0x01—0x06) 统一挂接总线。环网交换机全部开启端口隔离 (Port Isolation)：传感器接入口划入隔离组，仅允许与上联口通信、组内端口互访禁止，并配置广播风暴抑制 (64kbps)、组播抑制 (128kbps) 与未知单播丢弃，有效防范广播风暴沿环网横向扩散。 ③实验场景内置 4 个核心靶标，覆盖指标要求的全部八类训练内容：靶标 1 地面集控服务器 (192.168.10.20) ——内置RDP弱口令 (administrator/Coal@123)，用于非法登录、远程控制指令注入攻击演练 (以服务器为跳板向井下PLC伪造启停/急停指令)；靶标 2 井下PLC控制器 (192.168.20.10) ——编程口 (EtherNet/IP 44818) 无会话认证，用于PLC漏洞利用 (未授权上传/下载程序)、控制逻辑篡改测试 (篡改超温连锁阈值、强制表压制报警输出)；靶标 3 工控防火墙——用于防火墙规则有效性验证、端口扫描测试、绕过DPI的报文构造训练；靶标 4 声光报警器及传感器链 (192.168.30.12—30.15) ——用于传感器数据篡改 (改写温度寄存器屏蔽超温信号)、故障信号屏蔽测试 (丢弃报警报文/旁路连锁逻辑)、报警器拒动测试。另支持环网拓扑攻击 (伪造MRP_Test帧触发环网重构、组播风暴注入)，并可对比验证端口隔离的防护效果。各靶标训练界面如下。 靶标 1：非法登录集控服务器与远程控制指令注入演练界面 (含报警屏蔽前后
--	--

	对比)。 靶标 2/3/4: PLC 漏洞利用与逻辑篡改、环网拓扑攻击、传感器数据篡改演练界面 7) 实训教学与资源配套指标 ①煤炭场景实训内容共计 40 学时 (20 个实训单元×2 学时), 覆盖“基础认知—协议基础—设备认知—编程进阶—组态认知—攻防实战—防御配置—应急处置—综合考核”九个模块, 其中攻防实战模块与场景 4 个核心靶标的训练内容一一对应。每个实训单元均配套按课程内容改名的演示视频文件 (MP4); ②煤炭场景按“六件套”标准配套完整教学资料: a. 场景描述——《煤炭领域工控安全综合实验场景说明书》, 含运煤工艺背景、三级架构、4 个靶标的设备清单、网段规划、寄存器/点表定义与MRP环网配置说明; b. Flag获取任务描述——围绕 4 个核心靶标设置独立Flag任务 (任务编号MT01—MT08), 覆盖非法登录、指令注入、PLC逻辑篡改、环网攻击、传感器篡改、报警屏蔽等科目, 每份任务书含任务目标、前置知识、操作步骤、注意事项、考核标准五段式内容; c. 网络拓扑——三级架构图、MRP环网拓扑图、攻击路径拓扑图; d. 演示视频, 覆盖全部实训单元操作全过程; e. 标准答案——《煤炭场景Flag标准答案册》, 含每个Flag的获取路径、关键命令与预期回显; f. 复现报告——《煤炭场景综合复现报告》模板及样例, 含场景描述、攻击时间线还原、受影响资产清单、防御改进建议四个固定章节。 上述资料均以电子文件形式随场景资源包整体交付, 可直接投入教学使用。 3. 水利领域工控安全综合实验场景 1) 工业控制业务仿真指标 ①场景完整复现小型水库单孔闸门控制业务: 超声波液位计实时采集库水位并以 4-20mA信号输出 (信息采集), 经模拟量输入模块SM331 转换为工程量后送入PLC模拟机进行逻辑运算 (传输处理), PLC按水位联锁策略生成闸门升降指令, WinCC上位机提供监视、报警与操作界面 (决策控制), 4 台电动闸阀执行升降动作并回送开度反馈形成闭环校核 (执行反馈)。当库水位达到 45m限值时触发超水位报警, 联动视频弹窗并自动提升闸门泄洪; 场景同时支持模拟非法控制闸门启停、篡改水位数据等攻击情形, 用于攻防对抗教学。 ②实验场景基于小型水库单孔闸门升降控制与水位监测仿真环境, 通过PLC模拟机控制 4 个电动闸阀执行器。 ③WinCC运行画面以工艺流程图方式呈现水库、闸室、四孔闸门及下游河道, 实时显示库水位 23.60m (对应回路电流 11.55mA)、各闸门开度、24 小时水位趋势曲线及报警/事件窗口, 画面刷新周期 500ms, 与PLC通过S7Comm协议保持通信。 ④实验场景可通过WinCC模拟非法控制闸门启停、篡改水位数据等场景。 2) 工业控制架构设计指标 ①场景采用“控制层—现场设备层”二级架构模型设计。控制层 (192.168.10.0/24) 部署WinCC组态服务器、工程师编程站、操作员站、视频监控主机、域控服务器、渗透测试终端 (Kali) 及PLC模拟机, 各节点经工业以太网交换机 (VLAN10) 互联; 现场设备层部署超声波液位计与 4 台电动闸阀执行器, 通过 4-20mA模拟量信号与PLC的SM331/SM332 模块硬接线连接。架构层次清晰、设备角色明确, 便于学生理解水利工控系统的信息流与控制流。 3) 控制层设备部署指标 ①控制层部署PLC模拟机 1 台 (S7-300 软PLC, 192.168.10.100), 承担水位联锁判断、闸门联动控制、操作互锁等逻辑运算与数据处理任务, 程序块包含OB1 主循环、FB1 水位联锁、FB2 闸门控制、DB1 工艺参数、DB2 报警参数。工
--	--

程师编程站（STEP7 环境，192.168.10.20）用于PLC程序编写、上传下载与在线监视；上位机组态服务器（WinCC，192.168.10.10）与操作员站（WinCC RT，192.168.10.30）提供水位监视、闸门操作、报警管理等人机交互界面。

②实验场景通过SIMATIC Manager—S7_Reservior模拟，在控制层部署上位机组态服务器、工程师编程站、操作员站等，提供水位监视、闸门操作、报警管理等人机交互界面。

4) 设备层设备部署指标

①现场设备层设置超声波液位计模拟器1台（位号LT-101），量程0-50m、盲区0.30m、分辨率1mm，输出4-20mA标准信号接入SM331模拟量输入模块（换算关系 $I=4+16 \times H/50$ ，当前水位23.60m对应11.55mA），并提供信号冻结、叠加干扰、阶跃突变等教学注入模式，用于“传感器信号干扰/虚假数据注入”攻防科目。

②现场设备层设置电动闸阀执行器模拟器4台（位号GV-101~GV-104），接收PLC模拟量输出模块SM332的4-20mA升降指令（4mA=全关、20mA=全开），执行动作后回送4-20mA开度反馈形成闭环校核，指令-反馈偏差大于5%时触发“执行器故障”报警；支持现场/远程切换与检修挂牌，可模拟非法控制指令下发与设备误动作等攻击情形。

5) 工业通信与网络安全防护指标

①控制层内PLC模拟机与WinCC监控主机、工程师编程站通过工业以太网互联，采用S7Comm协议（TCP 102端口）进行数据读写与程序上下载；PLC与现场设备之间通过SM331/SM332模拟量模块以4-20mA硬接线连接，不经过网络。访问控制方面，场景依赖WinCC权限管理与Windows域策略实现分级分权管控。

②控制层依赖WinCC的权限管理（操作员/工程师/管理员三级角色，闸门操作须“操作员确认+管理员授权”双因子）和Windows域策略（统一账户管理、口令复杂度、登录审计、操作日志集中留存180天）进行访问控制。

③场景内置4个核心靶标：靶标1为WinCC组态服务器（监控软件非法登录、画面篡改攻击演练），靶标2为PLC模拟机（PLC程序上传下载攻击、逻辑篡改测试），靶标3为水位测量回路（传感器信号干扰、虚假数据注入测试），靶标4为闸门执行器（非法控制指令下发、设备误动作测试），完整覆盖指标要求的8项训练内容。

6) 实训教学与资源配套指标

①水利场景实训内容共40学时（20个课程单元×2学时），涵盖场景认知、设备实操、组态编程、攻防演练、安全防护与综合考核六个递进层次，课程单元与靶标、攻防科目一一对应（详见随附《水利场景实训课程列表.xlsx》）。每个攻防科目均提供录制的演示视频（共20讲，与课程单元同名），学员可按视频复现完整攻击过程。

②场景按指标要求配套提供六类教学资料：

- 场景描述：水库闸门控制业务背景、工艺流程、设备清单及网络规划说明；
- Flag获取任务描述：每个攻防科目的任务目标、Flag位置与获取条件说明；
- 网络拓扑：场景总体拓扑、业务链路拓扑、攻击链拓扑及防护体系拓扑；
- 演示视频：20讲实操录屏，覆盖全部攻防科目与设备操作；
- 标准答案：各科目攻击命令、脚本参数、预期结果及评分要点；
- 复现报告：含操作步骤、截图证据、结果分析与防护建议的标准报告模板。。

二、配套课程资源

1. 靶场场景与课程资源须实现内容配套，形成理论—实践闭环。

1) 课程内容与靶场场景一一对应

①靶场场景中涉及的工控协议，须提供对应的通信设备和协议交互环境；学生可在靶场协议交互环境中抓取并解析真实的Modbus TCP/S7Comm报文，观察主站对TTU寄存器30001-30008的周期轮询、写寄存器报文的逐字节结构，以及异常写入。

②提供课程大纲与靶场场景对应关系表，逐项标注每个课程模块对应的靶场设

	备、靶标编号和攻击/防御科目。 ③提供课程大纲与靶场场景对应关系表，逐项标注每个课程模块对应的靶场设备、靶标编号和攻击/防御科目。 2) 课程资源配套完整性 ①课程体系共四阶段 160 课时：基础阶段 40 课时、进阶阶段 50 课时、实战阶段 50 课时、考核阶段 20 课时，各阶段课时均满足指标要求，课时分配见表。 ②每门课程均配备对应的实验指导书与PPT课件：PPT课件共 77 讲，覆盖全部 160 课时；实验指导书按阶段分册共 5 册。 ③考核试题库试题总量 500 道，其中单选题 260 道、多选题 120 道、判断题 80 道、实操题 40 道，配套答案解析、组卷模板与评分表。 ④按要求制作课程大纲、课时分配表、实验指导书封面及目录页、试题样本。 3) 课程架构设计 ①课程按“工控安全基础—工控安全进阶—场景驱动实战—专项练习与考核”四大模块设计，下设 16 个子模块，遵循“认知→破坏→防护→对抗”的递进逻辑，模块构成见表。 4) 理论课件阶段、模块分别制作 ①按要求设计：基础阶段课包含知识点讲解、配套动画、随堂测试题。 ②按要求设计进阶阶段课件：增加案例驱动的教学设计——每个知识点配套一个真实或仿真的安全事件案例，如乌克兰电网被攻击事件。 ③按要求设计实战阶段课件：作为任务书和参考手册使用，包含攻防科目的完整任务描述、操作步骤截图和注意事项。 5) 实训任务手册 ①攻防科目配备独立的实训任务书，统一采用“五段式”结构：任务目标、前置知识、操作步骤、注意事项、考核标准。另外包含科目名称、建议课时数、对应靶标和难度等级。 6) 配套工具与资源包 ①配套工具资源包共 12 项，覆盖仿真软件（FreeSCADA、WinCC Basic）、PLC 模拟器（OpenPLC Runtime、Modbus Slave）、协议分析工具（Wireshark、Modbus Poll）、漏洞扫描工具（Nessus Essentials、OpenVAS）、模糊测试工具（Boofuzz）、逆向分析工具（Ghidra、Binwalk）及 8 套课程定制靶场虚拟机镜像，由工具资源包管理器统一部署与授权管理。 ②攻击脚本库：攻击脚本库按“Modbus攻击脚本集、配电终端交互脚本、S7 协议脚本、辅助工具脚本”四类组织，共 12 个脚本：Modbus攻击脚本集含 modbus_read.py、modbus_write.py、modbus_fuzz.py、func08_probe.py；配电终端交互脚本含rtu_force.py、ttu_tamper.py、coil_control.py；辅助工具脚本含ics_scan.py、pcap_evidence.py、restore.py等。脚本采用Python编写、逐行注释，供学生在靶场闭环环境内复现攻击过程。
--	--

备注：

软件的非功能要求：

本要求为所有标包的通用要求。

（一）验收要求

最终验收在用户现场进行。

由甲方组织验收小组，根据《平顶山学院信息化建设项目验收实施细则（试行）》的流程展开验收。验收时甲方可邀请第三方参与验收过程。

（二）系统集成要求

我校已完成智慧校园私有云平台 and 软件基础平台（数据中台、业务中台和双端门户）的建设工作。本项目所购系统必须基于学校私有云平台进行部署，并根据学校需要与学校智

慧校园软件基础平台实现对接或集成，以便实现学校对系统的统一管理，同时给学校师生使用提供便利。

1. 统一身份认证集成：本项目所购系统需按照《平顶山学院信息化建设规范》的统一身份认证集成要求，实现用户（教师和学生）的统一身份认证和单点登录。

2. 服务集成：本项目所购系统的用户常用的 PC 端功能需集成到学校网上服务大厅。

3. 数据集成：本项目所购系统需要按照《平顶山学院信息化建设规范》的统一数据调用规范和统一数据汇聚要求，实现组织机构、院系、专业、班级、教职工基本信息、学生基本信息等与数据中台保持一致，同时将应用系统的全量数据（结构化数据、非结构化数据）和数据字典提供给数据中心。

4. 乙方必须向我校开放全量数据（数据库形式）并按照我校要求提供相应的数据字典（文档形式）；根据用户方对接需要，无条件免费向用户方开放所需数据接口；日后扩充各种点位时，提供免费接入授权且数量无限制；开放接口和授权的费用须包含在报价内。

5. 所有的数据库建立、数据格式、各种功能定制等，均必须遵守平顶山学院信息化建设规范的要求，符合平顶山学院数据标准规范的要求，接受平顶山学院信息化领导小组的业务指导；充分考虑与平顶山学院的数据格式互通，严禁形成数据孤岛。

6. 乙方应根据我校需求提供与上级管理部门的业务系统对接的服务，方便数据上报和信息共享。

7. 系统各项集成所需费用应包含在投标总报价内，项目实施时学校不再承担由此产生的其它任何费用。

8. 根据应用系统的业务特点及学校需求，建立应用系统全面指标化的可视化数据分析大屏，能够根据不同角色展示不同的数据内容，且支持多级数据下钻特性。

（三）技术与性能要求

1. 开发技术：系统开发框架基于 B/S 架构，基于跨平台语言规范的多层体系结构。采用成熟的、符合技术标准的服务器、中间件产品。数据库支持 SQL Server 2008 r2、Oracle 11、Mysql 5 及以上版本。服务器操作系统支持市场主流的 Windows、Linux、国产操作系统。

2. 稳定性：系统架构设计合理，结合必要的集群、热备等手段，保证系统不间断运行。系统用户数量不受限制。系统可以全天候 7*24 天不间断运行，不会因为程序错误导致响应失败或者系统崩溃。数据库设计要保证实现数据高效查询检索、数据更新及数据调用。

3. 响应时间：一般时段响应时间不超过 1.5 秒，高峰时段不超过 4 秒；一般数据查询响应时间不超过 1 秒钟，一般固定表格制表不超过 5 秒钟，复杂统计汇集表格不超过 2 分钟。后台数据批处理时间应在 2 小时内完成。

4. 兼容性：系统应保证 Windows 8 及其以上版本、MAC、Harmony 客户端的正常使用，浏览器兼容 IE9 及其以上版本，并同时兼容非 IE 内核浏览器，如谷歌、火狐、搜狗等。

5. 安全性：确保应用系统源代码安全，无漏洞。提供较为完善的数据加密机制，非必要不进行明文传输，确保数据存储和按照信息系统安全等级保护二级及以上标准进行建设。系统正式上线前应通过有资质的第三方安全检测机构的安全测评，并出具测评报告。在需要时配合学校完成安全测评、等保测评等工作，并对产生问题进行无条件免费修复或整改。

6. 可审计：系统具备日志跟踪与分析功能，提供详尽的用户操作日志，提供丰富的查询方式，供追溯和追责。

7. 可靠性：系统运行稳定可靠，充分考虑冗余问题，要在系统设计范围内保证随着系统数据量的增加，系统性能不出现显著下降。

8. 可扩展性：系统架构设计可满足业务变化引起的系统功能升级，具有良好的扩展性与二次开发能力。为保证系统的易用性和可操作性，在系统中应为不同类型用户专门设计符合其操作习惯的界面和操作流程，确保系统的简单易用。

9. 易维护性：采用代码维护、公式调整、参数配置等手段，确保用户可自行维护系统基础设置数据项。系统采用纯 B/S 结构，系统升级和日常维护只需要在服务器进行即可。

10. 易操作性：系统设计符合业界通用规范和习惯用法，满足非专业用户的日常使用。

(四) 安全合规要求

1. 要求提供系统全生命周期内的 BUG 及安全漏洞消除、提供相关库（包含但不限于病毒库、各种特征库等）、新软件版本的升级与服务，由生产商提供承诺函；

2. 愿意承担对业主方的保密义务，包括但不限于对系统架构、部署情况、数据、策略、参数等的保密义务；

3. 规范操作用户方数据，不得越权或越界操作；未经授权不得查询、获取、存储、传输用户方数据，不得向第三方泄露用户方数据；

4. 根据等保相关政策，配合业主完成有等保测评需要的系统的主要系统的等级保护定级与测评；

5. 系统中使用的软件产品或组件必须符合国家有关知识产权的相关法律法规；投标方保证知识产权的合法性并承担可能侵权的责任；

6. 本项目需要使用的操作系统、数据库、数据库备份软件、第三方中间件等，在项目部署时按需提供针对校方永久授权的正版软件，费用包含在总投标价中。

(五) 商务及服务要求

1. 现场演示及测试：项目中标后三日内，提供主要设备厂方针对本项目的授权、产品原厂售后服务承诺函、产品授权等材料；业主对任何响应内容存疑时，可随时（原则上为中标通知书生效后的一周内、合同签订之前）要求对所提供的方案的任意功能在项目实施现场进行功能演示与测试，投标方必须无条件配合。如果与投标响应文件存在不符、功能不能实现、不能按要求对接现有系统、要求改变现有系统状态（如整体或部分替换、拆除、改变使用方式、改变配置等）、无法满足设计规范、不符合系统实施方案的要求等，任何一种情况均以虚假应标处理，采购人有权终止合同签订流程，追究投标方违约责任，由此所产生的一切费用及项目延误造成的一切损失由投标人全部承担，并可以由后续中标候选人顺序中标。

2. 除明确说明内容外，所有响应细节中有关“支持”等响应描述，当用户方对“支持”等内容有具体需求时，乙方均应当无条件免费提供满足用户方相应需求的服务。

3. 质保服务：本项目须提供 5 年免费质保服务（主要设备及核心软件原则上为原厂质保）。质保期内，中标人负责对软件系统进行维护和迁移，并且保证每学期主动上门维护一次，不再向用户收取任何费用。质保期后中标人提供的产品，采购人有权永久免费使用、迁移、安装。软件版本、各种升级库终身免费更新；系统漏洞和各种 BUG 终身免费修补。须提供产品原厂使用授权函和售后服务承诺函。

4. 日后若扩展软硬件时，产品报价不得高于此次投标价格。

5. 故障处置：一般系统故障（包括漏洞修复）须在 2 小时内做出有效响应，24 小时内解决；特殊复杂的系统故障（包括漏洞修复）须 48 小时内解决；若需现场解决故障的，服务人员必须在 5 小时内到达学校。

6. 技术及使用培训：免费提供所购软件中文版的操作说明书、相关技术资料及培训资料。免费提供每年不少于 2 次的现场培训或集中培训，并提供各种类型培训与个性化指导。

7. 费用范围：本项目为交钥匙工程，项目预算已包含项目实施过程中的所有费用。投标方应充分考虑项目实施过程中各环节的费用，并包含在投标总报价中，项目实施中不得以任何理由增加费用。

8. 交货期：**合同规定时间内完成安装**（含提供全量数据和数据字典等）、调试（含系统对接和安全漏洞修复等）、培训完毕，并提供软件著作权证书。

9. 乙方须建立完善的长期技术支持和售后服务管理体系和服务队伍，为配合用户使用提供全方位的技术支持工作。项目经理必须为自有在册固定人员，合同生效一周内必须到岗，项目完成验收前非不可抗力不得中途更换；必要时，根据甲方的需求派驻技术人员和项目经理驻场；项目经理到岗时不得同时兼任其他项目的成员。