郑州电力高等专科学校网络安全实训基地建设项目包 2:能源互联网工控安全实训设备采购合同

合同编号（买方）：

合同编号（卖方）：

买　　方：　郑州电力高等专科学校

卖　　方：　河南东进信息技术有限公司

签订日期：

签订地点：　郑州电力高等专科学校

目 录

第一部分　合同协议书

买方：郑州电力高等专科学校

卖方：河南东进信息技术有限公司

鉴于买方拟向卖方采购网络安全实训基地建设项目包2：能源互联网工控安全实训设备（货物名称）（简称“合同货物”），且卖方同意向买方供应上述合同货物，买卖双方就合同货物的采购订立本协议。

一、词语含义

本协议中所用词语的含义与通用合同条款和专用合同条款中相应词语的含义相同。

二、合同组成部分

下列文件为合同的组成部分：

1. 双方在合同履行过程中达成的纪要、协议等文件；
2. 合同协议书及其附件；
3. 中标（签约）通知书(如有)；
4. 专用合同条款及其附件；
5. 通用合同条款；
6. 招标文件和投标文件（如有）；
7. 构成合同的其他文件。

上述组成合同的各项文件应互相解释，互为说明。如有不一致，解释合同文件的优先顺序按照上述文件所列顺序为准。

上述各项合同文件包括合同当事人就该项合同文件所作出的补充和修改，属于同一类内容的文件，应以最新签署的为准。卖方承诺除偏差表释明外已完全响应买方招标文件，若发生投标文件与招标文件不一致的，则买方有权选择以招标文件或投标文件为准。

在合同订立及履行过程中形成的与合同有关的文件均构成合同文件组成部分，并根据其性质确定优先解释顺序。

三、合同标的

买卖双方在合同中约定的合同货物名称、规格型号、数量等见附件1《已标价合同货物清单》。

四、合同价格与支付

1.本合同价格为人民币（大写）壹佰肆拾捌万壹仟捌佰元整（¥1481800.00）（含税）。其中，不含税价人民币壹佰叁拾壹万壹仟叁佰贰拾柒元肆角叁分（大写）（¥1311327.43），增值税税率13%，增值税税额170472.57元。具体价格构成见《已标价合同货物清单》。若国家出台新的税收政策，合同约定税率与国家法律法规及税务机关规定的税率不一致时，对于尚未完成结算且未开具增值税税率发票的部分，按照国家法律法规及税务机关规定的增值税税率调整含税价格，价格调整以不含税价为基准。

2．合同价格支付

项目经甲方验收通过后，卖方凭到货验收单、100%合同价格的增值税专用发票办理支付申请手续，乙方需向甲方提交合同金额的5%额度的履约保证金保函。履约保证金保函应为中国注册的具有担保经营业务资格的银行或有关金融机构开具的保函。银行或有关金融机构保函有效期应与质保期保持一致。甲方在收到履约保证金保函后60日内，向乙方支付合同金额的100%。

（1）合同价格为人民币10万元（含本数）及以下的，卖方凭到货验收单、100%合同价格的增值税专用发票办理支付申请手续，买方在申请手续办理完毕后30个工作日内（境外支付的，延长30个工作日）支付全部合同价款。

（2）合同价格为人民币超过10万元的，卖方凭到货验收单、100%合同价格的增值税专用发票办理支付申请手续，买方在申请手续办理完毕后30个工作日内（境外支付的，延长30个工作日）支付95%的合同价款。

合同价款的5%作为履约保证金，保证期间自合同生效之日起至项目验收合格后7日内。保证期满，并无质量问题或质量问题及时解决后，卖方办理支付申请手续。买方在申请手续办理完毕后30个工作日内（境外支付的，延长30个工作日）支付全部履约保证金。

合同货物验收合格后，卖方可向买方提交履约保证金保函（保险）（格式见附件），申请等额替代履约保证金。履约保证金保函应为中国注册的具有担保经营业务资格的银行或有关金融机构开具的保函。买方在收到履约保证金保函后应向卖方支付履约保证金。银行或有关金融机构保函有效期应与保证期保持一致。

双方一致同意，卖方在保证期内，未按本合同约定或买方要求及时解决合同货物质量问题，买方有权扣除履约保证金，或兑付履约保证金保函（保险）。

五、交货

1. 交货时间：_合同签订后40日。具体交货日期按照附件1《已标价合同货物清单》规定执行。

2. 交货地点：郑州电力高等专科学校指定地点。具体交货地点按照附件1《已标价合同货物清单》规定执行。

六、质量保证

合同货物的质量保证期为从合同货物通过验收后6个月。其他关于质量保证的约定见通用合同条款、专用合同条款。

七、承诺

1. 卖方承诺按合同约定向买方提供符合要求的合同货物和服务。

2. 未经买方同意，卖方不得将本合同项下的债权（合同价款及其他权利）转让给任何第三方、向任何第三方提供担保或者办理保理事项。如买方同意卖方将本合同项下的应收账款债权转让、质押或者办理保理，买方应及时确认卖方的应收账款债权确权请求。卖方应收账款债权确权请求中应当列明转让或用于担保的应收账款的范围、金额等应收账款信息，同时明确告知买方应收账款的受让方、被担保方及其指定的应收账款收款账户等。

3.买方按合同约定向卖方支付合同价款。

八、争议解决

双方发生争议时，应首先通过友好协商解决；协商不成的，向买方所在地有管辖权的人民法院提起诉讼。

九、生效

本合同经双方法定代表人（负责人）或其授权代表签署并加盖双方公章或合同专用章之日起生效。合同签订日期以最后一方签署并加盖公章或合同专用章的日期为准。

十、份数

本合同一式 陆 份，买方执 肆 份，卖方执 贰 份，具有同等法律效力。

（以下无正文）

签 署 页

买方：郑州电力高等专科学校

（盖章）

法定代表人（负责人）或

授权代表（签字）：

签订日期：2024.7.16

地址：

联系人：王晓燕

电话：037162275802

传真：

Email：

开户银行：中国工商银行股份有限公司郑州东区支行

账号：1702021619217077791

统一社会信用代码：12410000416047531G

卖方：河南东进信息技术有限公司

（盖章）

法定代表人（负责人）或

授权代表（签字）：

签订日期：2024.7.16

地址：：郑州市二七区桃源路45号院6号楼3单元25号

联系人：魏艺伟

电话：18537186101

传真：037186560956

Email：13703927255@126.com

开户银行：中国建设银行股份有限公司郑州金海支行

账号：41001511010050271955

统一社会信用代码：914101033961580490

附件1：已标价合同货物清单格式

序号	货物名称	货物描述	单价（含税）（人民币元）	单价（不含税）（人民币元）	单位	数量	合同价款（含税）（人民币元）	合同价款（不含税）（人民币元）	税率	交货期	交货地点
1	工业控制单元	和利时 LE5109	41200.00	36460.18	套	1	41200.00	36460.18	13%	自合同签订生效之日起40日历天	郑州电力高等专科学校指定地点
2	工业控制防火墙	和利时工业防火墙系统 HOLLiSec-IFW-1000	162000.00	143362.83	套	1	162000.00	143362.83	13%		
3	工业控制漏洞扫描系统	绿盟工控漏洞扫描系统 ICSSCANNX3-S	202000.00	178761.06	套	1	202000.00	178761.06	13%		
4	工业控制漏洞入侵防御系统	绿盟工控入侵检测系统 IDS-ICSNX3-HD2000	81600.00	72212.39	套	1	81600.00	72212.39	13%		
5	工业控制内部网络监控与审计系统	和利时工业网络安全审计系统 HOLLiSec-SAS-1000	158000.00	139823.01	套	1	158000.00	139823.01	13%		
6	工业终端安全管控软件	和利时终端安全卫士 HOLLiSec-AGS	15000.00	13274.34	套	1	15000.00	13274.34	13%		
7	工业仿真组态软件	和利时工业仿真组态软件 HollyView	27800.00	24601.77	套	1	27800.00	24601.77	13%		
8	电力安全动态仿真沙盘	东进定制	276000.00	244247.79	套	1	276000.00	244247.79	13%		
9	工业控制交换机	迪普 LSW2300-8GT2GP-I	26000.00	23008.85	套	1	26000.00	23008.85	13%		
10	OPC server 软件	和利时 HollySyS	5700.00	5044.25	套	1	5700.00	5044.25	13%		

11	机柜	图泰 42U	3500.00	3097.34	套	1	3500.00	3097.34	13%		
12	工业互联网安全渗透系统	东进网络攻防实训系统 Dojin-Adpt	483000.00	427433.62	套	1	483000.00	427433.62	13%		
总计	/	/	/	/	/	/	1481800.00	1311327.43	13%		

附表2：能源互联网工控安全实训平台技术参数及要求

	货物名称	规格参数
1	工业控制单元	（1）CPU 模块:CPU314C-2PN/DP;存储卡:≥128K; I/O 模块:≥数字量输出模块（16DO）；导轨:编程电缆: MPI-USB 编程电缆; （2）CPU 模块:M340;开关量输入模块:≥16 点;开关量输出模块:≥16 点;模拟量输入模块:≥4 点;PLC 电源模块：CPS3500; （3）PLC：2 路 DI，光电隔离。可兼做 2 路高速计数或 1 路差分编码器计数；太网接口≥1 个；支持 modbus/tcp 和 104 规约；串口≥3 个；220VAC 供电；通讯串口≥2 个，DO 继电器输出≥16 路；CP1L 系列，集成数字量输入输出通道。

		1.硬件规格 （1）机架 1U 硬件设备；8 个 RJ45 千兆电口（支持 2 对 Bypass）1 个串口；4 个千兆光口（不含光模块）2 个 USB 口；2 个扩展插槽；可扩展 8 个千兆光口或者电口。 2.性能要求 （1）吞吐量 6Gbps；整体延迟≤ 200us；并发会话 100 万以上；每秒新建会话 1 万/s；BYPASS 切换时间≤3s。平均无故障时间 10 万小时以上；散热方式：无风扇；冗余电源。 3.支持分布式部署，支持集中策略管理；支持自管理、支持安全管理平台统一管控。 4.支持通用协议 HTTP、HTTPS、FTP、IMAP、POP3、SMTP、IM、NNTP、IMAPS、POP3S、SMTPS、TELNET、DHCP、ODBC、SNMP、Syslog 等。支持定义应用协议检查模块，形成应用防护模板； 5.支持工控协议包含但不仅限于 Modbus、OPC Classic、OPC UA、DNP3、IEC 60870-5-104、S7、CIP 等多种工控协议，针对工业协议支持细粒度的访问控制。 6.具备 Ping flood、SYN flood、UDP flood、DNS flood、TearDrop 攻击、Land 攻击、Ping of Death 攻击检测与防护。支持 flood 检测与端口扫描检测，支持 TearDrop 攻、Land 攻击、超大 ICMP 数据攻击； 7.具备对系统 CPU、内存和硬盘使用情况进行监视，对系统核心服务运行状态进行监视； 8.具备白名单支持针对协议的数据过滤，包括但不限 HOLLiAS MACS V6、MACS V7、Modbus-TCP、OPCDA、OPCUA、IEC104、IEC61850MMS、MELSEC-Q、DNP3、CIP、CIP_PCCC、S7COMM、S7COMM-PLUS、BACnet、EtherCAT、EtherNet/IP、FINS、Ovation 等多种工控协议； 9.具备工业协议深度学习，按工业协议查看学习结果关键操作，防火墙在学习模式下，所学习的数据会对应到相应的学习结果一键生成防护模板。 10.工业控制防火墙产品具备公安部信息安全产品检测中心、公安部计算机信息系统安全产品质量监督检验中心和国家网络与信息系统安全产品质量监督检验中心联合出具的检测报告。

		1.硬件指标 1U 标准机架式，含交流单电源，1 个 RJ45 串口，1 个 GE 管理口，具备 6 个 10M/100M/1000M 自适应以太网电口扫描口，1 个接口扩展槽位，硬盘 1T。 2.性能指标 （1）工业控制漏洞扫描系统并发扫描主机数 60，扫描速度 800 ip/h，并发任务数 10；授权 IP 扫描数量：无限； （2）工业控制漏洞扫描系统对工业控制系统提供专业的漏洞检测和分析。 3.功能要求 （1）工业控制漏洞扫描系统漏洞扫描支持的协议类型包含但不仅限于 Modbus TCP、S7、DNP3、Profinet、Ethernet/IP、IEC104、BACnet、Fox、FINS、Melsec-Q、ECOM、PCWorx、ProConOs、SNMP、Crimson、IEC61850-MMS、IEC61850-GOOSE 等； （2）支持传统扫描对象，且支持工控系统的扫描，工控系统漏洞数量不少于 850 个； （3）支持针对未知漏洞进行漏洞挖掘的能力，能够发现系统可能存在的未公开的安全隐患。支持传统扫描对象，且支持工控系统的扫描； （4）支持工控网络拓扑自动生成，支持工控系统扫描策略设定。已提供系统自动生成的工控网络拓扑图截图，拓扑图上应该对资产信息进行标识，如网卡类型，系统厂商等； （5）支持针对未知漏洞进行漏洞挖掘的能力，可以通过 fuzzing 方法进行系统未知漏洞挖掘，发现系统可能存在的未公开的安全隐患； （6）提供对资产风险的多次分析能力，能有效地分析网络整体和主机的漏洞分布和风险的趋势； （7）传统漏洞知识库漏洞信息不少于 220000 条，提供详细的漏洞描述和对应的解决方案描述；漏洞知识库与 CVE、CNCVE、CNNVD、CNVD 等主流标准兼容； （8）提供备份恢复机制，能够对系统创建还原点对系统进行备份和还原； （6）提供专门针对 DNS 服务的安全漏洞的检测，包括 DNS 投毒等漏洞检测能力。 （7）产品具备符合 GB/T 37954-2019《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》增强级的产品检测报告； （8）工业控制漏洞扫描系统产品具备（缺项视为不满足）《国家信息安全测评信息技术产品安全测评证书 EAL3+ 级别》、《计算机信息系统安全专用产品销售许可证（增强级）》、《计算机软件著作权登记证书》、《国家信息安全漏洞库（CNNVD）兼容性资质证书》。

		1.硬件规格 （1）1U 标准机架式，含交流双电源；USB 接口≥2 个，Console 口≥1 个，管理口≥1 个，配置≥6 个千兆电口，≥4 个 SFP 插槽；≥1 个接口扩展槽； 2.性能要求 （1）系统网络吞吐量 2Gbps，最大并发连接数 30 万；检测能力 600Mbps，并发会话数 20 万，能够对工业控制系统提供入侵检测、工业协议识别和事件告警。 3.功能要求 （1）工业控制漏洞入侵防御系统内置入侵特征库数量达到 1 万条，其中工控物联威胁特征达到 300 条，并针对工控系统攻击的识别及防护可持续升级； （2）支持被动资产识别，支持识别类型达到常见的 100 种； （3）支持至少 20 种工控协议的深度解析，包含但不限于（缺项视为不满足）：Modbus TCP、OPC Classic、OPC_UA、CIP、Ethernet/IP、S7_COMM、S7 plus、IEC61850 MMS、OMRON_Fins、DNP3 等； （4）支持工业行为分析，内置各工业协议的敏感操作功能码，对相关行为告警； （5）支持常见拒绝服务攻击阈值配置，包含但不限于（缺项视为不满足）PING Flood 、UDP Flood、SYN Flood 等；支持 PortScan 防护、PINGSweep 防护、ARPSpoof 防护； （6）支持流量分析功能，支持流量异常检测，可进行速率突变检测、无流量检测，检测内容包含且不限于阈值、升速、降速等； （7）系统支持 6500 种协议及应用识别，其中具备 100 种工控协议识别；具备 10 种流媒体协议识别；具备 6 种摄像头识别；具备 15 种数据库识别；具备 37 种 5G 协议识别； （8）系统支持入侵检测，能够针对 IT 系统攻击进行识别及防护。 （9）系统具备符合 Q/GDW 10941-2018 《入侵检测系统测试要求》、CEPRI-C-TX2-1015-01/2020《渗透测试检测方法技术文件》标准的中国电力科学研究院出具的检测报告； （10）系统具备（缺项视为不满足）安全操作系统、计算机软件著作权登记证书、符合 GA/T1485-2018《信息安全技术工业控制系统入侵检测产品安全技术要求》增强级的产品检测报告。

		1.硬件规格 工业控制内部网络监控与审计系统为 1U 标准机架式，6 个 RJ45 千兆电口，1 个串口，2 个 USB 接口，2 个扩展插槽； 2.性能指标 网络吞吐量 4Gbps，平均无故障时间≥10 万小时；内存 16G，硬盘 1T； 3.功能要求 （1）工业控制内部网络监控与审计系统具备通过流量分析识别系统中通信链路，利用基于对网络通信数据的实时分析，自动以拓扑图的形式直观展示工控网络中各个设备节点之间的通信连接情况，提供可视化的异常展示与告警，如 IP、MAC、设备种类、设备厂商、设备型号等； （2）计系统能够对工控网络中的所有活动提供协议和流量审计。支持协议包含但不限于（缺项视为不满足）：IEC60870-5-104、Modbus TCP、IEC61850、S7Comm、S7Comm-Plus、DNP3、MMS、EtherNet/IP、CIP、OPC-DA、OPC-UA、OMRON-FINS、HOLLiAS-MACS 等众多工业协议字段级的深度解析，有效实现在线监测审计分析； （3）系统具备工业网络入侵检测。基于丰富的规则库，可通过对网络流量数据的分析，发现网络异常行为或攻击行为，包括漏洞 ID、名称、危害等级等详细信息； （4）系统具备按协议类型进行流量统计，从工控协议和网络协议角度，展现流量使用情况，支持（统计占用流量最大的资产和通信关系）TOP10，具备和安管平台统一管控，远程下装策略管理等。 （5）系统支持对工控系统通信流量特征的学习，学习通信关系信息，形成五元组基线，判断新增通信关系。 （6）计系统具备公安部信息安全产品检测中心、公安部计算机信息系统安全产品质量监督检验中心和国家网络与信息系统安全产品质量监督检验中心联合出具的检测报告。

		1.工业终端安全管理软件具备6个工业控制终端安全永久授权，兼容工业常用Windows系统。加固方式包括安全配置、授权管控、采用专用软件强化操作系统访问控制能力、以及配置安全的应用程序的要求，制定主机加固的技术标准、方案和管理策略； 2.支持终端本地气泡静默弹窗告警功能。当执行非法操作产生告警信息时，终端会进行静默气泡弹窗告警提示； 3.软件服务端支持B/S架构管理模式，提供对授权客户端登录终端界面管理，提供白名单功能包含但不限于，支持阻止蠕虫、脚本、木马等类型病毒，白名单机制可以有效拦截已知、未知病毒、木马及其他恶意软件，保证系统内生安全；提供对USB存储设备进行的外设访问控制；兼容工业常用系统； 4.具备兼容Windows XP、Windows 7、Windows 10、Windows Server 2016 、CentOS 7.9 mini/CentOS 7.9 DVD等主流Windows与Linux操作系统； 5.支持系统安全管理设置：如页面超时时间，最大登录次数，用户锁定时间，密码长度，密码有效期和复杂度等，支持“三权分立”的管理模式，使得系统中的不同角色各司其职，相互制约，共同保障系统的安全； 6.具备日志存储阈值设置，日志转存配置根据配置的IP和端口进行原始日志的转发，日志备份、导入导出，日志详细查询包括接收时间、终端名称、终端IP、终端位置、告警类型等信息。 7.具备终端上的程序只有在白名单中才能运行，不在白名单的程序将拒绝执行（白名单拦截、USB存储设备禁用、系统双因子认证）； 8.具备白名单在终端软件安装时可自动扫描本地执行程序形成白名单，不在白名单的程序将被拒绝执行； 9.具备白名单机制可以有效拦截已知、未知病毒、木马及其他恶意软件（包括文件类型、文件路径、状态）等，保证系统内生安全； 10.具备白名单机制可有效止.exe、.dll、.com、.ocx、.js、.java 等工控应用常见程序类型 ； 11.软件具备对白名单列表信息的查找、追加、删除、保存等操作（包括文件名称、文件类型、文件路径、目录、状态）等，支持文件添加及导出； 12.软件具备安全策略，包括工作模式切换（包括允许。拦截。审计）、例外路径（包括文件路径、目录）、例外进程（对关键进行进行包含，防止关键进行在运行过程中被强制关闭、停止）、USB外设管控（支持对USB存储设备使用进行控制，未授权设备无法使用，可实现USB存储设备的读、写权限控制）等； 13.软件具备防护、审计、透明等多种工作模式，各种模式具备开关控制，可以灵活适应各种工况的需要，保证现场系统稳定可靠运行； 14.软件具备记录提取的程序文件数码特征值，程序启动时自动校验核对文件特征值，阻止被篡改的同名文件启动，保证授权文件的添加运行； 15.软件具备中华人民共和国公安部颁发的《计算机信息系统专用产品销售许可证》（“文件加载执行控制”、“访问控制”）、计算机软件著作权登记证书资质； 16.软件具备公安部信息安全产品检测中心、公安部计算机信息系统安全产品质量监督检验中心和国家网络与信息系统安全产品质量监督检验中

		1.技术要求 （1）工业仿真组态软件能满足与所提供工业控制单元通信的要求，组态软件与所提供工业控制单元可完成实验平台的不同组合； （2）工业仿真组态软件功能模块包含但不限于 1)实时数据库；2)设备通讯服务程序；3)HMI 画面；4)网络通讯程序；5)接口 SDK；6)Web 应用服务；7)关系数据转储；8)数据转发；9)扩展组件等功能模块； 2.软件要求 （1）工业仿真组态软件系统结构组态包括管理器、符号编程、下载和调试程序、组态分布式 I/O 等； （2）提供集成互通承诺函。

		1.电力安全动态仿真沙盘尺寸不小于2000mm*1200mm*3000mm（宽*高*长）； 2.电力安全动态仿真沙盘展示场景包含发电、变电、配电、输电及用电等，每个场景符合工业现场实际情况，并且有真实的设备、管道、仪表和工艺流程； 3.电力安全动态仿真沙盘发电行业仿真包括风力发电系统、光伏发电系统、火力发电系统等； 4.电力安全动态仿真沙盘包括变电、输电、配电和用电的整个流程的工艺和构筑物，有灯光展现，能看到安全事故的效果，并且可以一键恢复。 5.电力安全动态仿真沙盘模型底座造型设计现代、时尚、简约；模型高度设置保证人在模型前观看时略微仰视为宜。底座高度约700mm(包含底盘厚度)；模型底座颜色、风格与现代模型水平一致。方便拼装、更新、维护；声、光、电、水等系统的设备设施在底座内，同时对电器、电路的安全、散热等进行设计处理；沙盘底座的材质在选择上要考虑耐腐蚀、不易变形、工业感强、易打理，长时间使用不掉漆等。 6.电力安全动态仿真沙盘把现代的光、电技术溶入本项模型之中，在主体建筑中及路灯、地灯、庭院灯、园林设置柔和自然的灯光，并采用各种手法创造出独特的夜间观赏效果。用不同颜色的光源来体现不同区域，把不同区域的功能分别开来，丰富的视觉效果。采用多路不同的灯光来表现项目所要反映的几大核心内容：餐饮、交通、教育、医疗、金融、地标、配套等。 7.跨平台数据中转器能实现工业互联网平台（工控平台、管理平台等）和工业控制安全平台（态势感知、知识图谱等）的数据互通共享； 1）具备实时双向转换IT、OT侧数据，并可对接通用SCADA平台，实现功能安全和网络安全的双监控；（已提供系统功能截图并加盖原厂商公章）。 2）IT侧数据转发OT侧支持Syslog、HTTP、OPC UA、Modbus数据上报；（已提供系统功能截图并加盖原厂商公章）。 3）OT侧数据转发IT侧支持通过ModbusTCP、OPC UA、HTTP、UDP、MQTT协议转发，支持采集的数据写入数据库（SQL Server）。 4）支持（CPU：4核、内存：8GB）、每秒1000条处理。 5）支持在linux、windows操作系统上部署，跨平台可运行； 6）支持在虚拟机环境上部署运行； 7）提供集成互通承诺函。

		1.交换容量≥128Gbps，包转发率≥15Mpps； 2.固化端口≥8个千兆电口，≥2个千兆光口； 3.支持16KMAC表项、支持VLAN、STP、RSTP、ACL、QOS等功能； 4.支持静态路由、RIP、OSPF； 5.支持广播风暴抑制、组播风暴抑制和未知单播抑制； 6.具备工信部《电信设备进网许可证》。
		1. OPC server软件能实现各工业设备数据采集、集成和通信； 2.OPC server软件能够连接不同类型、不同厂家的设备，将其数据转化为统一的格式； 3.提供集成互通承诺函。
		机柜符合ANSI/EIA RS-310-D、IEC297-2、DIN41491：PART1、DIN41494：PART7、GB/T3047.2-92标准，兼容ETSI标准。

		1.系统要求 （1）工业互联网安全渗透系统包含攻击套件资源包支持主流攻击，能形象展示攻击效果，内容包含但不限于Modbus协议篡改、U盘攻击、木马植入攻击等。 2.系统实训教学管理需求 （1）总体要求提供以下功能包含但不限于（缺项视为不满足）： 实训教学管理包括实训课程管理、组课排课、考试管理、作业管理、在线课堂、工业互联网安全职业技能、虚拟组件管理、场景设计、拓扑场景等； （2）工业互联网安全渗透系统教师和管理员可以选择章节快速组课，课程可设置显示/隐藏。支持教师排课，即授权课程给班级，为课程添加学习的班级，授权的课程在相应班级的教学空间显示； （3工业互联网安全渗透系统支持自定义虚拟组件即虚拟机，设置组件分类和规格；支持上传组件的权限自动划分，不同权限的角色只允许上传和管理自己的组件；组件支持上传新增和快速新增；在组件管理页面支持对上传的组件进行参数设置包括网络连接、磁盘类型、开机密码等；上传好的组件支持开机测试，组件开机可连接互联网下载软件或者通过web页面直接本地上传安装包到组件中。 （4）工业互联网安全渗透系统场景设计支持创建场景拓扑。不同角色创建的场景自动划分权限，只允许创建和管理自己的场景；场景设计至少包括终端、服务器、交换机、路由器等组件，以拖拽和划线方式实现组件拓扑组网；组件支持设置IP地址，路由器支持设置路由；创建好的场景支持另存场景，启动场景后可在线测试，支持对场景中虚拟机开机、关机、保存到当前模板、另存模板操作；支持设置场景中某虚拟机为场景入口，场景入口虚拟机在前台启动场景后显示； （5）工业互联网安全渗透系统在线课堂教师可选中某个班级作为在线课堂，支持在网页上实时监控学员实操过程，支持在网页上直接操作学员的虚拟机进行实操演示和故障排除，老师的操作过程学员在网页上同步显示； 3.系统实训教学内容需求 工业互联网安全渗透系统实训教学内容总实验数量800；课程内容包含但不限于安全基础、web安全、工业互联网渗透测试、内网安全、安全运维、安全意识等； 4.工业互联网安全渗透系统实训靶标提供虚拟化终端靶标，终端靶标数量50种；靶标涉及的漏洞类型应涵盖栈溢出、堆溢出、整型溢出、格式化字符串溢出、反序列化、权限提升、远程代码执行、任意文件上传等； 5.工业互联网安全渗透系统固件漏洞提供可利用固件漏洞靶标，包括CPU、显卡等，数量2种；交付内容包漏洞验证代码（poc），可利用漏洞利用代码（exp），漏洞说明文档（漏洞危害等级、复现/利用的难易程度、适用环境、漏洞类型、触发方式、利用条件、Shellcode功能等漏洞描述）及科目操作文档（含漏洞复现过程、成因分析等）；

第二部分 通用合同条款

1. 合同标的

1.1 卖方向买方供应的货物的名称、品牌、规格型号、数量等见《已标价合同货物清单》。

1.2 卖方应向买方提供全新的、技术水平先进的、质量可靠的货物，并保证该货物未侵犯任何第三方的合法权利（包括但不限于知识产权），详细要求见“技术规范书”。

1.3 卖方提供的货物应符合国家或行业技术标准，生产厂家的技术标准高于国家或行业技术标准的，卖方应按生产厂家技术标准执行。

1.4 卖方应提供与货物安装使用相关的技术资料和技术服务。

1.5 卖方保证其依照本合同向买方交付的合同货物没有任何权利瑕疵，合同货物上不存在任何抵押、质押、留置等担保物权、任何第三方知识产权，不存在任何性质的附属或者限制性权益，也不存在被任何政府机关或者司法机关查封、扣押、冻结的情形。卖方对货物享有合法完整的所有权、知识产权及其他相应的权利。卖方依照本合同交付合同货物、提供服务及履行其他本合同项下的义务不会违反其组织章程，不会超越经营范围和方式，并不会违反与任何第三方达成的协议、承诺、任何政府部门或者司法/仲裁机构对其的要求。卖方保证买方不会因为合同货物侵犯任何知识产权而被提起索赔、指控或请求，否则，卖方应当就买方因此遭受的损失（包括但不限于直接损失、间接损失、律师费、诉讼费或仲裁费等）承担全部赔偿责任。

2. 合同价格

本合同价格指卖方将合同货物运到合同约定交货地点并履行完毕其他合同义务所需的全部费用，包括但不限于合同货物价款及包装费、保险费、各种税费、运杂费、卸车费、技术资料费、安装调试费、培训费、技术服务费等。

买方有权从任何一笔应向卖方支付的价款中扣除卖方按合同约

定应向买方支付的违约金、赔偿金或其他费用。

3. 交货

3.1 卖方应按照买方指定的时间、地点和方式向买方交付本合同项下的货物。

卖方应将技术资料（包括但不限于货物安装、使用所需的图纸及合格证书）两套随货物一并提交买方，否则视同延迟交货处理。

3.2 卖方负责货物运输，并承担由此发生的所有费用。

3.3 货物的实际交货日期以符合合同要求的货物包括备品配件，到达合同约定的交货地点为准。

3.4 卖方承担货物交付给买方之前的损毁、灭失等一切风险。

3.5 卖方物资发货须以买方或买方指定单位统一发送的送货通知单为准，否则不予结算。

3.6 卖方在收到买方指定单位发出的物资交货通知书后的3个工作日内需将物资运输计划以电子邮件或文本形式提交至买方指定单位。卖方未按期向买方交付运输计划的，每迟交1日，应向买方支付合同价格0.05%的违约金。

3.7 卖方在货物到达现场完成物资交接相关手续之后，应在3个工作日内将到货验收单送至买方指定单位，每迟交1日，应向买方支付合同价格0.05%的违约金。

4. 包装与标记

4.1 卖方交付的所有合同货物均应符合相关包装储运指示标志的规定，按照国家主管机关最新的规定进行包装，满足长途运输、能承受水平受力、垂直受力、多次搬运、装卸、防潮、防震、防碎等包装要求。卖方应在外包装上注明产品名称、型号并应按照合同货物的特点，按需要分别加上防冲撞、防霉、防锈、防腐蚀、防冻、防盗的保护措施。合同货物包装前，卖方应负责按照买方要求进行合同货物身份码标签的下载、制作和赋码，并在指定平台进行身份码信息维护，按部套进行检查清理，不留异物，并保证零部件齐全。

4.2 合同货物严禁使用松木做包装材料（包括松木包装箱、线缆

盘、垫木、固定支架等）。如使用其它木质包装材料，卖方应在发货前通知买方，并到当地森林检疫部门办理《植物检疫证书》。该证书必须随货同行，作为附随资料交付买方，并作为到货验收和入库凭据之一，否则买方有权拒收，且每批货物卖方应向买方支付不低于5000元的违约金。

5. 到货检验

5.1 货物到达交货地点后，买方将对货物的包装、外观及数量进行检验，货物检验合格后，由买方出具到货验收单给卖方。如发现货物非因买方原因有任何损坏、缺陷、短少或不符合合同约定的质量标准和规范的情况，卖方应在接到买方通知后，尽快修理、更换，或补齐短缺部件，并承担相关费用。

5.2 上述检验为现场的到货检验，现场检验未发现问题或卖方已按索赔要求予以修理、更换，或补齐短缺部件，均不减轻或免除卖方按合同约定所应承担的质量责任。

6. 安装和质量保证

6.1 货物由卖方根据卖方提供的技术资料、检验标准、图纸及说明书进行安装，买方提供配合。

6.2 如果货物安装过程中，由于卖方原因需要进行检查、试验、再试验、修理或更换，卖方应承担进行上述工作所需的费用。

6.3 合同货物安装完毕后，卖方应按照买方通知参加验收并办理相关手续，卖方未按照买方通知参加验收的，视为卖方认可验收结果。合同货物通过验收并不能免除卖方在质量保证期内对合同货物应尽的责任和义务。

6.4 卖方承诺对所提供的货物提供 6 个月（含本数）的质量保证，质量保证期自合同货物通过最终验收之日起计算。国家法律、法规等规定的质量保证期长于卖方承诺的质量保证期的，适用国家法律、法规等规定。在货物质量保证期内，由于卖方责任需要修理、更换有缺陷的设备或部件导致货物停运或货物存在缺陷影响正常运行时，货物的质量保证期自卖方消除该缺陷后重新计算，由此产生的所

有损失由卖方承担。如在质量保证期内发现设备或部件出现缺陷但不影响货物的正常运行，经维修或更换后的设备或部件的质量保证期重新计算。在货物质量保证期终止之前，卖方对所提供货物实行“三包”服务。

6.5 卖方承诺货物的寿命期限不少于 三 年。因卖方设计、材料或工艺的原因造成货物存在缺陷或出现故障的，卖方应按买方要求免费修理或更换有缺陷的设备或部件。

6.6 在从货物运至交货地点之日起至质量保证期结束之日的期间，如发现卖方提供的货物有缺陷或故障，不符合本合同约定时，买方有权选择且卖方须采取以下补救措施：

6.6.1 对不符合合同约定的货物进行修理，以使其符合合同要求，费用由卖方承担。除非买方同意，修理工作应在 30 天内（含本数）完成。

6.6.2 以符合合同要求的货物更换不符合要求的货物，费用由卖方承担。除非买方同意，更换应在 30 天内（含本数）完成。

6.6.3 买方将有缺陷的货物退还卖方，卖方负责将被退还的货物运出安装现场。在此种情况下，卖方应退还已收取的货款并承担买方支出的安装、拆卸、运输、保险及购买替代品所发生的额外支出等费用。

6.7 卖方提供给买方的货物不得侵犯第三人的权利，卖方应保证买方在使用该货物或其任何一部分时免受第三方提出侵犯其任何专利、注册的设计、版权、商标或商品名称或其他知识产权工业设计权的起诉及索赔。若买方受到此类索赔或起诉，其责任及给买方造成的一切损失由卖方承担，买方有权解除合同，同时卖方应向买方支付合同总额的 10%的违约金。

7. 违约责任

7.1 卖方不履行本合同义务或者履行义务不符合约定的，买方有权要求卖方承担继续履行、赔偿损失和/或支付违约金等违约责任。

7.1.1 卖方违反合同约定迟延交货的，买方有权按迟交货物金额

的1‰/天向卖方主张迟延交货违约金。

7.1.2 卖方未按合同第6.6.1、6.6.2条约定时间履行修理、更换等义务的，买方有权按合同价格的1‰/天向卖方主张违约金。

7.1.3 由于卖方货物质量或迟延交货等原因导致买方工程不能按期投入使用的，每逾期一天，卖方应向买方支付合同价格0.1%的违约金。

7.1.4 在质保期内，由于卖方设计、材料、制造缺陷造成货物无法正常使用的，每发生一次卖方应向买方支付合同价格2%的违约金。

7.1.5 发生以下情况之一时，买方有权解除合同，并可要求卖方退还买方已支付的全部（或部分）合同价款；在第（1）、（2）和（4）种情况下买方同时有权要求卖方支付全部（或部分）合同价款20%的违约金：

（1）卖方提供的货物完全不能使用；

（2）卖方明确表示无法供货或买方有合理理由认为卖方无法供货；

（3）卖方应支付的违约金总额达到合同价格的20%；

（4）卖方出现违约行为，经买方通知后在限定时间内仍不改正的。

买方终止合同的，有权以依其认为适当的条件和方式购买与本合同项下货物类似的货物，由此发生的额外费用由卖方承担。

7.1.6 卖方按合同约定应支付的违约金低于给买方造成的损失的，并应就差额部分向买方进行赔偿。

7.1.7 未经买方同意，卖方将本合同项下的应收账款债权转让、质押或者办理保理的，卖方应按照合同价格的 10 %向买方支付违约金。

7.2 买方逾期支付合同价款的，应就逾期部分向卖方支付按合同订立时全国银行间同业拆借中心公布的1年期贷款市场报价利率计算的逾期付款违约金。

8. 不可抗力

8.1 本合同中不可抗力是指不能预见、不能避免并不能克服的客观情况，包括但不限于自然灾害、战争、武装冲突、社会动乱、暴乱或按照本条的定义构成不可抗力的其他事件。

8.2 任何一方由于不可抗力而影响本合同义务履行时，可根据不可抗力的影响程度和范围延迟或免除履行部分或全部合同义务。但是受不可抗力影响的一方应尽量减小不可抗力引起的延误或其他不利影响，并在不可抗力影响消除后，立即通知对方。任何一方不得因不可抗力造成的延迟而要求调整合同价格。

8.3 受到不可抗力影响的一方应在不可抗力事件发生后 2 周内（含本数），取得有关部门关于发生不可抗力事件的证明文件，并以传真等书面形式提交另一方确认。否则，无权以不可抗力为由要求减轻或免除合同责任。

8.4 如果不可抗力事件的影响已达 120 天或双方预计不可抗力事件的影响将延续 120 天以上（含本数）时，任何一方有权终止本合同。由于合同终止所引起的后续问题由双方友好协商解决。

9. 适用法律

本合同的订立、解释、履行及争议解决，均适用中华人民共和国法律。

10. 争议解决

本合同争议解决方式见合同协议书。

11. 合同生效

本合同生效条件见合同协议书。

12. 份数

本合同份数在合同协议书中约定。

13. 保密

双方及其各自的雇员、代理人对对方提供的无论何种形式的客户信息、技术信息、价格、报价、折扣及其他资料、市场及产品信息承担保密的责任，不得以任何形式向第三方披露上述保密信息。本部分规定在本合同终止后仍然有效。